Estudio de Factibilidad Técnica de Integración, Estudio y Diseño de Telecomunicaciones

Producto 3
Documentación de diseño preliminar

DISTRIBUCIÓN					
Interno			**Externo**		
División	**Nombres**	**Nº**	**Compañía**	**Nombres**	**Nº**
Airtel	Aldo Giraudo	1	SPD	Tania Macuer V.	1
Airtel	Patricio Boric	1	SPD	Camila Beltrán O.	1
			SPD	Patricio Urriola	1
			SPD	Miguel Fernández F.	1
Airtel	Archivo	1	SPD	spd-partes@interior.gob.cl	1

APROBACIONES			
Funciones	**Nombres**	**Fecha**	**Firma**
Autor	P. Boric	3-06-24	
Revisor	A. Giraudo	3-06-24	
Rep. de Calidad			
Gerente de Proyecto			
Cliente			

REVISIONES										
Rev. Nº					**Por**	**Capítulos Modificados**	**Descripción**	**Causa**	**Fecha**	**Rev. Por**	**Aprob. Por**
1	.	0	.	0	PBS	Todos	Emisión de Documento	Emisión	03-06-24		
2	.	0	.	0	PBS	Todos	Se ajusta de acuerdo a observaciones menores de la SPD e información adicional recibida.	Observaciones de la SPD.	25-06-24		
3		0	.	0	PBS	2.1 Diseño de interconexión e integración, pág. 6.	Se mencionan los municipios y donde se encuentra la información en forma detallada.	Observaciones de la SPD.	10-07-24		

Revisión 3 . 0 . 0
Referencia Informe producto 3 Rev. 3
N° de páginas 34

Contenido

Confidencialidad

El presente documento y/o anexos se proporcionan en respuesta a una solicitud de la parte que la recibe y ésta entiende y acuerda que:

a) Proteger el carácter y propiedad confidencial de lo proporcionado.
b) El presente documento y/o anexos solamente es para uso interno del receptor.
c) Distribuir o comunicar el presente documento y/o anexos solo a los funcionarios que tienen la directa relación con este, informándoles el carácter confidencial del mismo.

De forma análoga a lo anterior, los consultores de AIRTEL y ZAGREB se comprometen a que toda la información que se reciba de parte del cliente será tratada en forma confidencial.

1. Alcances del estudio

La Subsecretaría de Prevención del Delito del Ministerio del Interior y Seguridad Pública, en adelante la Subsecretaría o SPD indistintamente, contrató el servicio denominado "Estudio de Factibilidad Técnica de Integración, Estudio y Diseño de Telecomunicaciones" según lo señalado en las bases de Licitación ID: 654478-2-LE24, la que fue adjudicada mediante Resolución Exenta N° 580 del 12 de marzo de 2024.

De acuerdo con lo establecido en las bases técnicas de la licitación el presente estudio considerará:

a) Evaluación de las infraestructuras tecnológicas existentes en 14 comunas de la RM (Santiago, Estación Central, Quinta Normal, Independencia, Recoleta, Cerro Navia, Lo Prado, Renca, Conchalí, Quilicura, Huechuraba, Colina, Lampa y Til Til.)
b) Evaluación de las infraestructuras tecnológicas existentes en:
   - Delegación Presidencial Regional Metropolitana de Santiago. Gobierno Regional Metropolitano de Santiago.
   - Concesión Acceso Nororiente a Santiago.
   - Concesión Américo Vespucio Oriente: Tramo El Salto - Príncipe de Gales.
   - Concesión Sistema Américo Vespucio Norponiente: Tramo Avenida El Salto - Ruta 78. Autopista Central: Concesión Sistema Norte - Sur.
   - Costanera Norte: Concesión Sistema Oriente - Poniente.
   - Túnel San Cristóbal: Concesión variante Vespucio El Salto - Kennedy. Mall Arauco Quilicura.
   - Mall Plaza Norte. Estadio Santa Laura
   - Supermercados (por definir) y estacionamientos (por definir)
c) Realizar visitas a terreno para levantamiento.
d) Identificación de requerimientos técnicos para la integración e interconexión de los sistemas de cámaras de vigilancia a CENCO u otra dependencia que permita la coordinación de la televigilancia en Santiago centro, desde las instituciones anteriormente descritas.
e) Análisis de las opciones de conectividad y transmisión de datos.
f) Estimación de costos de implementación y operación.
g) Identificación de riesgos y mitigaciones.
h) Análisis de la normativa legal y de seguridad aplicable.

Como resultado del estudio encomendado, se entregarán varios informes que resumirán los hallazgos, conclusiones, recomendaciones y cualquier otro aspecto relevante para proporcionar una comprensión completa de los resultados del estudio obtenidas durante el proceso de investigación. Estos informes corresponden a los siguientes entregables:

Producto 1: Informe "Reporte de situación actual"

- Recopilación de información técnica existente (Cantidad - Software - hardware).
- Análisis de la infraestructura de telecomunicaciones actual.
- Evaluación de la capacidad y condiciones de los equipos de transmisión y recepción de datos.

Producto 2: Informe "Reporte de factibilidad técnica"

- Evaluación de requerimientos de ancho de banda.
- Análisis de alternativas de conectividad (fibra óptica, inalámbrico, satelital, etc.).
- Estudio de la topología de red necesaria.
- Disponibilidad de operadores de servicios de telecomunicaciones para lograr la interconexión.
- Identificación de puntos críticos y propuesta de soluciones.

Producto 3: Informe "Documentación de diseño preliminar"

- Diseño de interconexión e integración.
- Especificaciones técnicas del diseño de interconexión.
- Plan de integración con los sistemas de televigilancia existentes.
- Propuesta de equipamiento y software necesarios.

Producto 4: Informe "Presentación ejecutiva para la toma de decisiones".
Resumen ejecutivo de los contenidos incorporados en los productos 1, 2 y 3, además de un archivo de presentación (PowerPoint o similar) de los resultados informados en los reportes de los productos 1, 2 y 3.

Producto 5: Informe "Propuesta de roadmap para la implementación del proyecto".
Propuesta de implementación del proyecto considerando:

- Actividades de habilitación de espacios y equipamiento para el desarrollo del proyecto
- Plazos de ejecución
- Costos de ejecución
- Ruta crítica para la ejecución de las actividades
- Carta Gantt de la propuesta de roadmap para la iniciativa.

Este informe corresponde al entregable número tres de la consultoría, consistente en el Informe “Documentación de diseño preliminar" en su versión número 2, en la que se agrega información que a la fecha de entrega de ese informe no estaba disponible.

Para un mejor entendimiento de este informe se recomienda que este sea revisado considerando los otros documentos entregados, por su carácter complementario y a que mucha de la información contenida en ellos está directamente relacionada entre sí.

2. Documentación de diseño preliminar

En este capítulo se desarrolla todo lo relacionado con el producto 3, en particular el informe de reporte de factibilidad técnica para el proyecto SITIA, de acuerdo con el siguiente detalle:

2.1. Diseño de interconexión e integración.

En primer lugar, antes de abordar las opciones de diseño del sistema integrado, es conveniente explicar la situación actual, la cual a grandes rasgos consiste en múltiples sitios (de municipalidades y privados) de concentración de cámaras de video vigilancia y salas de monitoreo. Cada uno de estos sitios tiene diversos componentes, entre los cuales se pueden mencionar los siguientes:

- Múltiples cámaras de video de distintos tipos desplegadas en los puntos de interés que contienen los sensores ópticos que efectúan la captura de imágenes de video.
- Codificadores para comprimir las señales de video y utilizar de esta forma menor ancho de banda. Normalmente los codificadores o códecs están incorporados en las cámaras de video.
- Medios de transporte de la señal de video de las cámaras hacia el punto de concentración. El medio mayoritario utilizado son enlaces de MMOO punto a punto o multipunto, y en algunos casos enlaces de fibra óptica.
- Switches que actúan como concentradores de las señales de video. En la mayoría de las municipalidades el punto de concentración corresponde a una comisaría de carabineros[1] y desde allí se envían todas las señales para ser replicadas en una sala de monitoreo de la municipalidad, salvo en cuatro casos[2] en que el monitoreo se realiza en la misma comisaría.
- Sistemas de almacenamiento de las señales de video.
- Uno o más sistemas de gestión de video VMS (por sus siglas en inglés (Video Management Software) que corresponden a una aplicación de software que permiten monitorear y gestionar una gran cantidad de cámaras de video IP desde cualquier ubicación y que residen además en un servidor conectado a la red o también puede ejecutase como un servicio en la nube.
- Como alternativa al VMS, puede existir un NVR (Network Video Recorder), que es un dispositivo especializado que habilita un sistema de cámaras de video en red, para una cantidad relativamente pequeña de cámaras. Los NVR están diseñados para grabar y almacenar video de las cámaras en red y, por lo general, no requieren instalar ni mantener ningún software.
- Sistemas de analítica, que existen en algunos casos y que facilitan el procesamiento de las imágenes de video con diferentes aplicaciones como lectura de placas patentes (LPR), reconocimiento de vehículos y de personas (rostros).
- Sistemas de visualización y despliegue para el monitoreo de las señales de video. Estos sistemas se encuentran en las salas de monitoreo, donde hay operadores que revisan las imágenes, pudiendo existir más de una sala por institución.

[1] Esto ocurre en las municipalidades de Renca, Independencia, Quinta Normal, Recoleta, Lampa, Estación Central, Huechuraba, Cerro Navia y Quilicura. Mayores detalles en la tabla 3 del informe 1 revisión 3.
[2] Municipalidades de Recoleta, Lampa, Estación Central y Quilicura.

En la gran mayoría de los casos, estos sistemas en la actualidad existen en forma aislada en cada institución, con las excepciones de la Municipalidad de Santiago que dispone de una interconexión dedicada vía fibra óptica con CENCO, y de algunas municipalidades que se interconectan con CENCO vía Internet en modalidad de plan piloto y con condiciones algo más limitadas. La figura siguiente muestra esta situación en forma esquemática, sin detallar la totalidad de las componentes:

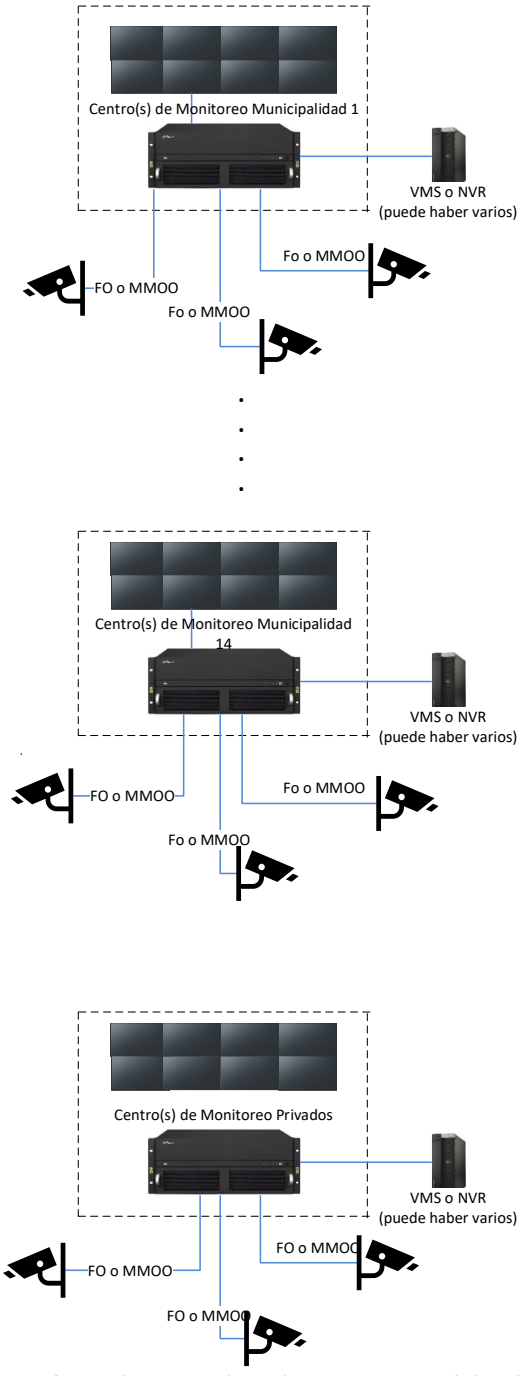

Figura 1 esquema referencial de la situación actual municipalidades y privados

2.1.1. Diseño de interconexión

Para la interconexión de todas las entidades que forman parte de este proyecto se han considerado distintas opciones, siendo una de ellas la de conectar todos los puntos de concentración a una red IP / MPLS a través de un servicio a ser contratado a un operador de telecomunicaciones que ofrezca la cobertura y condiciones de calidad a todos los puntos requeridos.

El acceso desde cada punto de concentración a la red IP / MPLS del operador debiera ser preferentemente en fibra óptica, y se incluiría también el CENCO como un punto más de esta red privada MPLS con un enlace de mayor capacidad para soportar todas las capacidades agregadas. De ser necesario, para lograr la disponibilidad requerida se pueden habilitar enlaces de acceso redundantes a la red MPLS, obteniendo así una mayor resiliencia del sistema en los puntos más débiles del sistema que son precisamente los accesos de última milla (entre la red y el punto de concentración), adicional a la que provee la misma red que cuenta con rutas internas alternativas.

Esta es la opción preferente recomendada, situación que debe ser validada una vez que se disponga de la información solicitada a algunos operadores en cuanto a factibilidad técnica, condiciones y costos de esa solución.

La figura siguiente muestra un esquema de estas interconexiones:

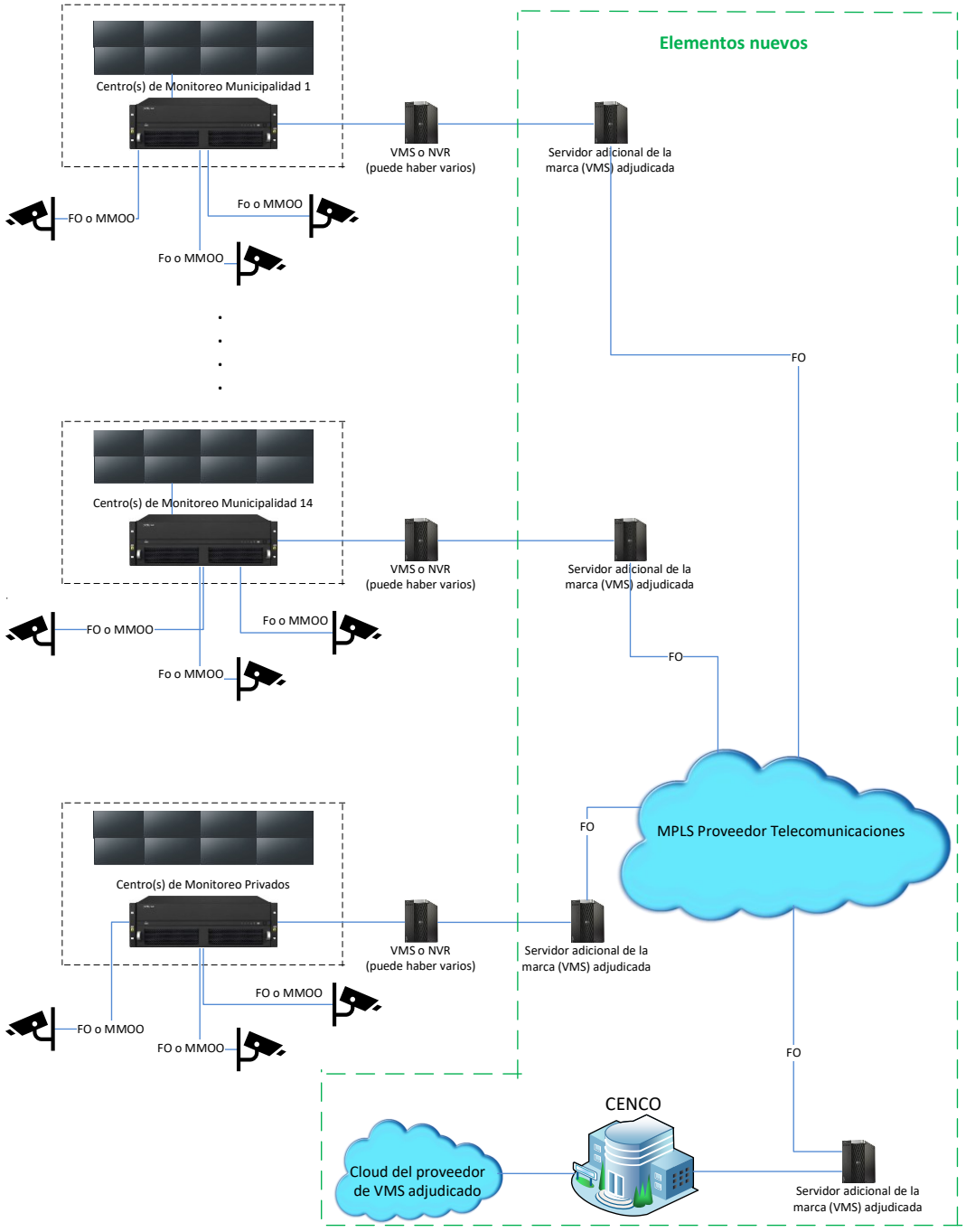

Figura 2 esquema diseño interconexión vía MPLS

Como opción se puede considerar otra solución para la interconexión entre los múltiples puntos, a través de accesos individuales a Internet en cada punto de concentración.

El servicio de acceso a Internet que se requiere contratar debe reunir características especiales que se detallan en el punto siguiente “Especificaciones técnicas del diseño de interconexión”. Es importante destacar que no es adecuada cualquier conexión a Internet, sino que deben cumplirse las especificaciones respectivas para asegurar un funcionamiento óptimo y evitar riesgos de ciberseguridad que podrían comprometer la seguridad de todos los sistemas involucrados.

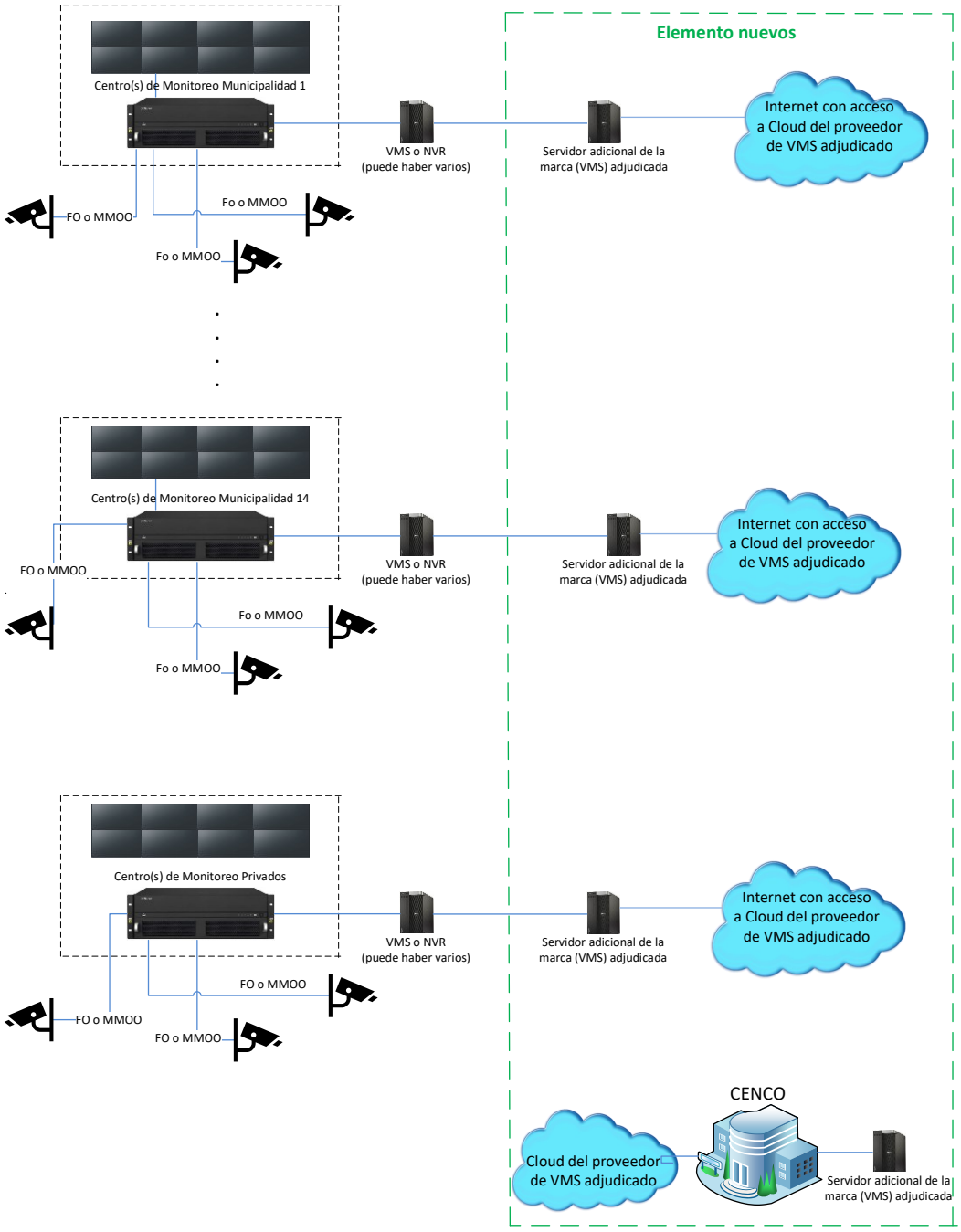

Figura 3 esquema diseño interconexión vía Internet

Como ya se mencionó, la alternativa preferente recomendada es la de la interconexión vía MPLS y la decisión final deberá tomarse en función de las respuestas de factibilidad técnica y costos de los operadores de telecomunicaciones. Puede ser válido adoptar una configuración mixta, sobre todo para las comunas más alejadas como Til Til, Lampa, o Colina donde la oferta de cobertura de red MPLS puede ser menor. Al respecto, ya se adelantó en el informe 2 que para la comuna de Colina es más complejo contar con rutas alternativas en una de las dependencias de esa comuna.

2.1.2. Diseño de integración

Por integración nos referimos a cómo se combinan y coordinan los diversos sistemas y componentes de hardware y software existentes de los diversos sistemas de videovigilancia para funcionar desde una plataforma centralizada.

Recordemos que no existe una única solución dado que cada fabricante o integrador posee distintas formas de hacer la integración.

La integración de múltiples sistemas de videovigilancia independientes en CENCO puede presentar diversas dificultades tanto de índole económicas, técnicas y organizacionales.

En cuanto a la índole técnica se puede señalar que la principal corresponde a la Interoperabilidad de diversos sistemas.

Dada la inexistencia de uniformidad en las soluciones que han adoptados las diversas municipalidades y organizaciones privadas, existen cámaras, equipos, software de diferentes fabricantes y emplean diferentes protocolos de comunicación (ONVIF, RTSP, etc.), formatos de compresión de video (H.264, H.265, MJPEG, MPEG4), de almacenamiento (G64X, MP4, AVI, etc.) y organización de los datos, lo que complejiza la integración ya que en general los software de visualización y gestión de video (VMS) de los diversos fabricantes de por si no hablan entre ellos, por lo cual se requiere una aplicación de mayor jerarquía que permita la integración de múltiples aplicaciones y dispositivos, que no siempre es factible en su totalidad, sino que puede ser limitada con algunos fabricantes.

En la siguiente figura se puede apreciar en forma esquemática los principales elementos que de alguna forma -hardware y/o software- se deben integrar, y además se incluyen los posibles equipos o software adicionales que deberían agregarse para esta integración.

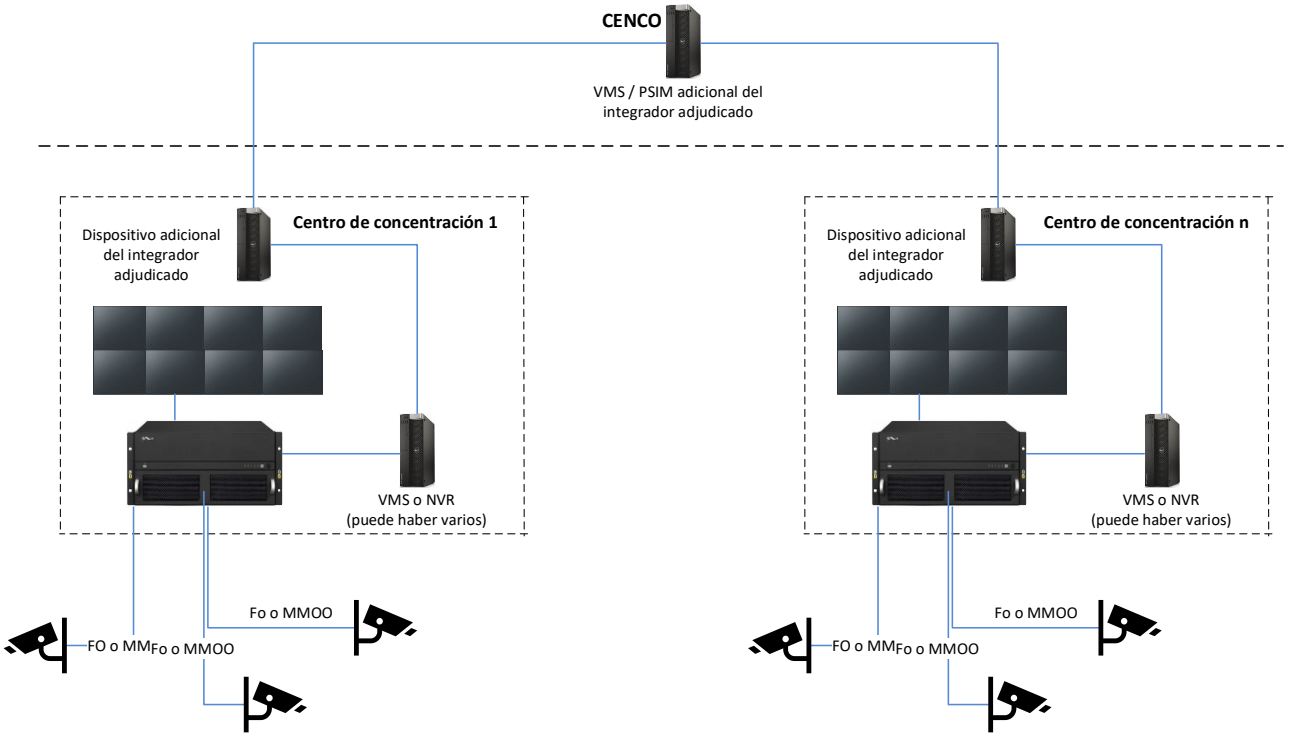

Figura 4 esquema diseño elementos principales a integrar

Como solución a la problemática anteriormente descrita, los fabricantes optan por distintas filosofías, arquitecturas y topologías para realizar la ansiada integración por lo cual no es posible diseñar una propuesta concreta sin que se defina una marca en particular, lo cual coarta la posibilidad de competencia entre ellos. Por ende, más que diseñar una solución particular se han definido funcionalidades, bloques constitutivos y necesidades a satisfacer que es lo que se expone a continuación.

Especificaciones para la integración

La plataforma de consola a ser instalada en las dependencias centrales de CENCO debe cumplir al menos con lo siguiente:

- Generalidad

Una plataforma central del tipo multiusuario con un software que unifique información crítica, en tiempo real y almacenado, de flujos de video, voz, meta datos y datos - provenientes de dispositivos o aplicaciones, de múltiples marcas, tales como VMS, cámaras y almacenamiento de diversos sitios- para generar una visión integral en situaciones de seguridad y emergencia proporcionando una visión completa e inmediata de los eventos en desarrollo proveyendo control y gestión en forma centralizada e inteligencia para la toma de decisiones.

- Conexiones Físicas

Debe existir compatibilidad y conexión con la red de transporte que en términos generales serán a dispositivos switches y routers necesarios para gestionar el tráfico de datos.

- Software de Unificación, Gestión y Control de Video

Debe asegurarse de que todas las cámaras y dispositivos sean compatibles con el software de gestión y visualización que se vaya a emplear de forma de tener acceso al streaming de video y data de la cámara.

Debe asegurarse la mayor cantidad de integración con las diversas marcas y versiones de software de Gestión de Video (VMS) existentes. En caso de que no exista dicha factibilidad, debe proponer una alternativa de solución técnica y económicamente viable. Lo anterior es importante dado que, dependiendo de la filosofía del proveedor, la analítica como detección de movimiento, análisis de video, alertas, etc. podría ser extraída localmente desde los VMS sin que se adicionen algoritmos o infraestructura para estas funcionalidades específicas.

Debe permitir y ser compatible con procesamiento mayoritario de analítica generada en el borde para disminuir los requerimientos de ancho de banda de la red de transporte que llega a CENCO.

Debe proporcionar una interfaz de usuario personalizable de acuerdo con los derechos de cada usuario, otorgando permisos, restringiendo funciones que al menos permita monitorear, controlar todas las cámaras y dispositivos, eventos y metadata desde una plataforma consolidada.

Debe proporcionar capacidades para acceder y gestionar el sistema desde dispositivos móviles o remotos.

Debe proporcionar capacidades para configurar acciones automáticas basadas en eventos específicos, tales como enviar alertas o activar grabaciones y otros.

Debe proporcionar capacidades de implementación de algoritmos de IA para análisis avanzado de video ya sea en forma local, como en el borde, en la cámara en forma independiente o simultánea.

Debe proporcionar capacidad de escalabilidad tanto horizontal (añadiendo más cámaras y dispositivos) como verticalmente (mejorando la capacidad de procesamiento y almacenamiento) a medida que crezcan las necesidades de videovigilancia de los actuales, o expansiones a nuevas organizaciones.

El sistema debe proporcionar a través de interfaces gráficas, como Dashboards, diversas informaciones de métricas tales como cantidad de dispositivos conectados, espacio en disco y otros de utilidad para de la salud del sistema.

El sistema debe mantener registros (logs) de las diversas acciones realizadas por los usuarios, estado del sistema, registro de eventos, alarmas y otros.

- Protocolos y Estándares

Debe asegurar la operación e integración con protocolos estándares como ONVIF para asegurar la interoperabilidad entre dispositivos de diferentes fabricantes, al igual que con protocolos de transmisión de video tales como RTSP, HTTP.

- Integración con Otros Sistemas

Debe permitir Integración futura con diversos sistemas tales como: sensores, alarmas, GPS, mapas GIS georreferenciados, capas de información varias, video wall, etc. entregando respuestas automáticas a eventos específicos de acuerdo con reglas preestablecidas.

Debe permitir la funcionalidad de interconexión con base de datos de Carabineros, Gendarmería, Registro Civil u otros que se determinen.

- Redundancia y Resiliencia del Sistema

Debe asegurar que el sistema de video vigilancia esté siempre disponible mediante la implementación de redundancias en hardware y software.

- Seguridad Cibernética

Debe proveer distintas herramientas, estrategias y/o dispositivos para la protección de la red y los datos y sistema de autenticación y control de acceso, uso de VPN.

El sistema debe permitir la autenticación de usuarios para ocasiones en que sea necesario monitorear, realizar ciertas tareas en el software de monitoreo y administración.

Mayores detalles sobre seguridad cibernética se incluyen en el punto 2.4.1

Otros

Si bien lo siguiente no corresponde a las funcionalidades del sistema a implementar, igualmente son aspectos importantes que deben ser considerados al momento de seleccionar el proveedor

- DRP

Debe desarrollarse un plan detallado para la recuperación del sistema en caso de desastres naturales, ciberataques u otros eventos catastróficos los cuales deberán ser compatibilizados con los existentes en Carabineros.

- Experiencia

El proponente deberá demostrar experiencia en la implementación de integración con múltiples marcas y plataformas, de tamaño similar al de este proyecto.

- Soporte

El proponente deberá contar con soporte local en la ciudad de Santiago y acceso directo con el fabricante de la solución implementada.

2.2. Especificaciones técnicas del diseño de interconexión.

A continuación, se incluye una propuesta inicial de especificaciones técnicas para el servicio de interconexión, las cuales deberán ser ajustadas a las definiciones de alcances que se adopten posteriormente, como por ejemplo relación completa de sitios con direcciones donde se requieren los servicios, valores específicos de anchos de banda por cada sitio, niveles de servicio y otros[3].

Dado que se ha recomendado la solución de red IP / MPLS, se ha privilegiado las especificaciones técnicas para esa tecnología, sin embargo, igualmente se agregan algunas especificaciones para el caso que se utilicen accesos Internet.

2.2.1. Servicio de conectividad IP / MPLS

- Aspectos generales

El servicio de conectividad IP / MPLS deberá soportar comunicación de datos bajo protocolo IP MPLS y poseer los mecanismos y dispositivos necesarios para asegurar calidad de servicio (QoS) efectiva de extremo a extremo, de acuerdo con los estándares vigentes del mercado, los que deberán ser informados, especificados y detallados por el proponente como parte de su oferta.

El servicio mayoritario para transportar será el de señales de video en tiempo real en diferentes formatos, pudiendo agregarse otros servicios como voz, mensajería, imágenes fijas, metadata, y señales de control.

La conexión a todos los sitios de acuerdo con el “Anexo Direcciones y BW Red Transporte v2.xlsx” en que se definen estos puntos será a través de la red MPLS redundante del proveedor de servicios, con conexiones preferentemente en fibra óptica o inalámbricas con enlaces dedicados de uso exclusivo, desde el nodo más cercano del proveedor hacia las dependencias del cliente.

Se deben evitar accesos satelitales, debiendo privilegiar el proponente subcontratar enlaces terrestres a otros proveedores, donde no cuenten con cobertura.

Los anchos de banda ofrecidos para cada dependencia deben ser simétricos 1:1 (velocidad de subida igual a la velocidad de bajada), y estar garantizados extremo a extremo sin aplicarles ninguna

[3] Si bien no ha sido suministrada toda la información por parte de los participantes en el estudio, esto no afecta a la arquitectura y especificaciones de la red de transporte ya que a lo más podría variar la cantidad y capacidad de algunos sitios. Para suplir la falta de información se han considerado en esos casos, capacidades equivalentes a las de los sitios en que se dispone de esa información.

tasa de compartición, incluyendo los accesos, según los valores mínimos que se incluyen en el mismo anexo ya citado, y garantizados para cada sitio. En todo caso, la asignación del ancho de banda contratado por tipo de servicio podrá ser modificada de acuerdo con el comportamiento de la red observado en el tiempo.

El proponente debe contar con una cobertura propia de red MPLS y accesos locales igual o superior al 70% de todos los sitios del cliente indicados en el anexo ya citado. Los sitios restantes deberán ser contratados por el proponente a través de acceso de terceros, haciéndose cargo de su provisión y mantenimiento. El proponente deberá informar en su Oferta Técnica, qué sitios cuentan con cobertura propia o con recursos de terceros.

Además, el proponente deberá indicar en su propuesta los parámetros técnicos de tasa de pérdida de paquetes, jitter y retardo que garantiza para los diferentes servicios, los que deben ser igual o mejores que los siguientes:

Parámetro	Voz	Video	Datos
pérdida de paquetes	0,10%	0,10%	0,50%
retardo (*)	20 ms	20 ms	N.A.
jitter	6 ms	6 ms	N.A.

(*) salvo enlaces satelitales

Al menos en el sitio central CENCO, el proponente deberá contar con dos accesos por rutas diferenciadas incluyendo idealmente ingresos diferentes al edificio mismo, cada una de estas rutas con la capacidad de cursar todo el tráfico agregado, de acuerdo con lo que se señala en el anexo ya citado. Estas rutas diferenciadas deberán ser detalladas por el proponente, señalando si estas rutas serán con medios propios o de terceros y entregando un diagrama del recorrido de ellas.

Para los sitios restantes, el proponente podrá o no contar con accesos duplicados, lo que se diseñará para cumplir con el nivel de servicio exigido.

El proponente adjudicado deberá informar con detalle las rutas de acceso a cada sitio demostrando el recorrido diferenciado entre los accesos principales y secundarios.

Como una forma de cumplir con la disponibilidad, el proponente podrá ofrecer respaldos en la modalidad de SD-WAN para los enlaces que estime conveniente, sin que esto signifique costos adicionales a la propuesta económica.

Todo el equipamiento para instalar en las dependencias de CENCO deberá cumplir las normas internas de esa institución definidas en el Anexo correspondiente. En particular este equipamiento deberá ser rackeable y contar con fuentes de poder redundantes.

El proponente adjudicado deberá asegurar la integridad, independencia y privacidad de los enlaces que considere el servicio hasta la capa de acceso de cada dependencia del cliente, implementando para ello las políticas más apropiadas, tales como encriptación de la WAN, túneles de seguridad o alguna otra propuesta de parte del proponente. El proponente deberá declarar los controles de

seguridad para evitar amenazas de suplantación, alteración de datos, divulgación de información no autorizada, denegación de servicio, aumento de privilegios, o escuchas no autorizadas.

La red WAN IP / MPLS debe ser sólida, escalable, funcional, flexible, administrable, redundante y de alta disponibilidad, acorde a las características solicitadas por el cliente, para estos efectos el proponente deberá disponer de la tecnología necesaria para que el servicio cumpla con los siguientes requerimientos:

• Calidad de servicio: La red WAN IP / MPLS debe contar con calidad de servicio (QoS) para soportar multiservicios (Video, Voz, Datos prioritarios).

• Escalable: La red WAN IP / MPLS debe soportar y permitir aumentar la cantidad de sitios y la configuración de nuevos anchos de banda que satisfagan el incremento proyectado en el tráfico, sin afectar los niveles de servicios ni la continuidad operacional.

• Alta disponibilidad: La red WAN IP / MPLS debe considerar las redundancias necesarias en todo su trazado y arquitectura, para asegurar efectivamente el cumplimiento de los niveles de servicios exigidos. Adicionalmente los enlaces redundantes deben asegurar rutas y accesos independientes.

• Solidez: La red WAN IP / MPLS debe estar basada en equipamiento nuevo de alta calidad, probado, y con soporte técnico certificado local.

• Funcionalidad: La red WAN IP / MPLS debe permitir la incorporación de funcionalidades que apoyen aspectos de seguridad y de administración.

- **Niveles de servicio**

El nivel de servicio más importante es la disponibilidad mensual de cada punto. En este aspecto hay que tomar decisiones, ya que en general cuanto más alto sea el nivel de servicio requerido, mayor será el costo del servicio ya que los proveedores para poder asegurar los niveles más altos deberán incurrir en infraestructura adicional. Se pueden proponer otros SLAs, pero el de disponibilidad es el más importante.

A manera de referencia, las figuras siguientes muestran algunos valores típicos de disponibilidad mensual por cada punto y la infraestructura requerida en cada caso.

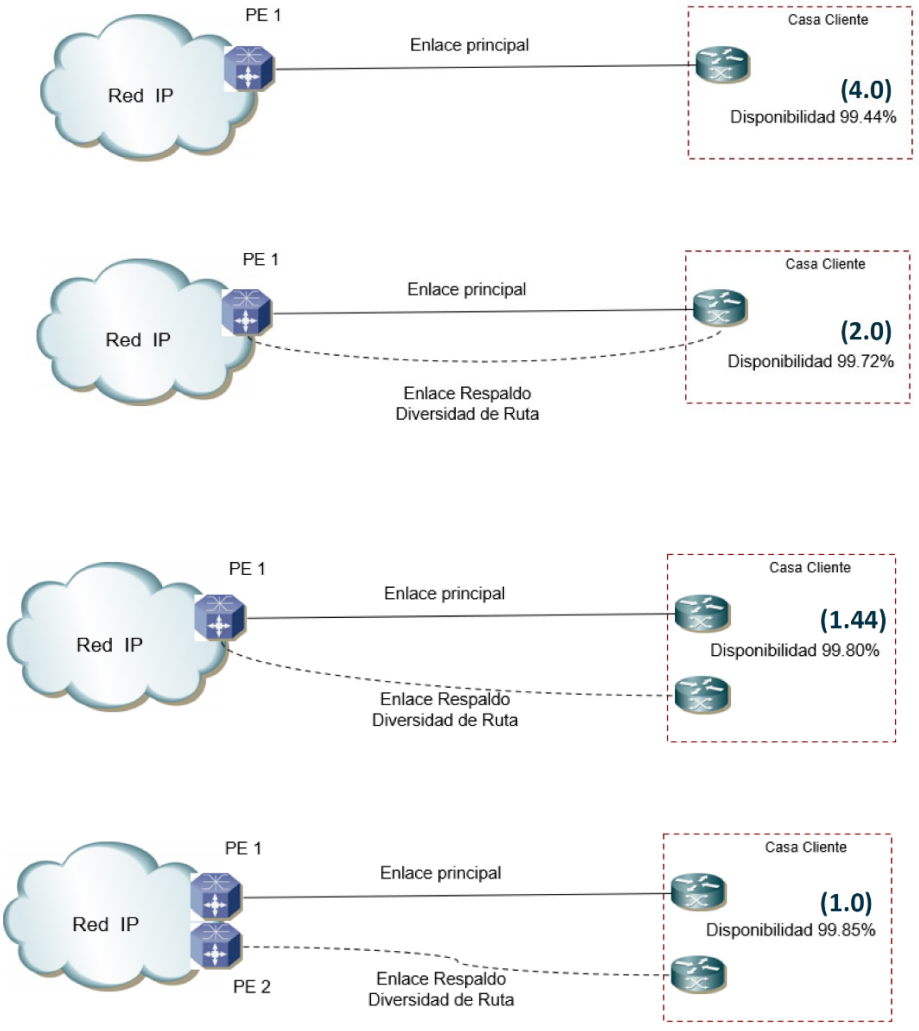

Figura 5 Valores típicos de disponibilidad y sus configuraciones asociadas

El nivel de disponibilidad de 99,4% mensual (que equivale a 4,32 horas de indisponibilidad acumulada en el mes) es el básico y no incluye ninguna redundancia. Otros operadores ofrecen 99,5% por defecto.

Luego viene un nivel algo mayor de 99,72% (que equivale a 2 horas de indisponibilidad acumulada en el mes), y que requiere al menos un enlace de respaldo con diversidad de ruta en el sitio remoto, compartiendo el equipo terminal.

Para una disponibilidad mayor, de 99,8% (que equivale a 1,44 horas de indisponibilidad acumulada en el mes), se requiere además que ambos enlaces tengan equipos diferentes en el sitio remoto.

Por último, subir a 99,85% (que equivale a 1,08 horas de indisponibilidad acumulada en el mes), se requiere además duplicar el equipamiento de red, es decir cada acceso duplicado deberá contar con equipos terminales distintos en el lado red y en el lado sitio remoto.

Estos valores son ligeramente distintos entre diferentes operadores, y además se pueden considerar otros escenarios adicionales.

La recomendación es definir una disponibilidad mensual en los sitios remotos de 99,5% y de al menos 99,85% para el sitio central CENCO. La SPD debe confirmar estos valores o proponer otros alternativos.

También es importante precisar la forma de medir estas disponibilidades, ya que en ese aspecto existe mucha variedad entre los distintos operadores, y suelen agregar muchas exclusiones por robo de cables, cortes de energía y otras causas, lo cual termina causando que casi nunca asumen la responsabilidad de una interrupción.

Una posible propuesta sería la siguiente:

El proponente deberá garantizar una disponibilidad mensual igual o superior a los valores indicados a continuación, según el tipo de sitio:

Sitio central (CENCO)	99,85%
Sitio remoto	99,5%

Independientemente del origen de una falla (sea ésta de enlace, de equipo, de software, de servidor externo, lógica o cualquiera otra que no sea responsabilidad del cliente), si éste no tiene acceso al uso del servicio, esto se contabiliza para la indisponibilidad. Igualmente se considerarán como de responsabilidad del proponente, las fallas ocasionadas por interrupción del suministro de energía (salvo las que ocurran en dependencias del cliente), o por robos de cables y equipos, o por daños causados por accidentes.

Un servicio se considerará indisponible cuando esté totalmente interrumpido o también cuando su capacidad binaria o alguno de sus parámetros asociados (latencia, jitter, pérdida de paquetes) se encuentren degradados en un 10% o más con respecto a los valores especificados como nominales.

En el caso de servicios suministrados por medio de accesos o equipos duplicados, no se considerará indisponible el servicio si algún elemento redundante se encuentra fuera de servicio o con funcionamiento defectuoso, siempre y cuando otro elemento de similares características absorba la carga y funcionalidades del elemento fallado o defectuoso, permitiendo así que el cliente tenga acceso al servicio de telecomunicaciones respectivo sin experimentar degradación alguna.

Los tiempos de indisponibilidad se contabilizarán desde el momento que se notifique la falla o sea detectada por los sistemas de monitoreo propios del proponente, hasta que se acepte como solucionada por el cliente. Los tiempos de los múltiples eventos de indisponibilidad del mismo servicio se suman en un mes calendario para calcular el tiempo final de indisponibilidad.

- **Operación, gestión y reportes**

Para la gestión y control de todos los servicios y enlaces solicitados, el proponente deberá ofertar un servicio de administración de la red IP / MPLS que incluya en el respectivo equipamiento de comunicaciones, las capacidades necesarias para satisfacer los requerimientos de monitoreo detallados a continuación.

El proponente deberá poner a disposición del cliente un portal para que éste pueda tener acceso, con las debidas medidas de seguridad, a un sistema de monitoreo “en tiempo real” que supervise y mida los parámetros principales de cada uno de los servicios contratados, como por ejemplo indicadores de tráfico o uso de ancho de banda por cada enlace (entrada y salida), retardo, jitter, pérdida de paquetes, etc. La herramienta debe mostrar en forma gráfica el tráfico medio tanto de salida como de entrada, medido en ventanas de 10 minutos, para las últimas 24 horas, además de los perfiles de tráficos medios horarios para la última semana, perfiles de tráfico medio diario para el último mes y para el último año. Esta herramienta deberá desplegar la información de tal forma que pueda visualizarse en la escala adecuada de acuerdo con los rangos contratados con una precisión de un 5%, y ser exportable a archivos Excel o similares, para análisis y procesamiento adicionales.

El proponente deberá incluir la instalación, mantenimiento, actualización, administración y operación de todos los elementos incluidos en este servicio.

Además, el proponente deberá proveer la capacitación necesaria al personal del cliente designado para realizar las labores de supervisión.

Anualmente el proponente estará obligado a proporcionar las actualizaciones tecnológicas concernientes al software y firmware aplicables a los equipos provistos para la prestación de los servicios contratados, considerando que las actualizaciones permitan una mejor administración, mayor seguridad, y compatibilidades de equipos para los servicios contratados. El cliente resolverá aceptar, postergar o desestimar dichas actualizaciones.

El proponente supervisará los servicios ofrecidos a través de un sistema de gestión de tráfico, supervisión de operación y mantenimiento 7x24 debiendo señalar explícitamente en la oferta, los siguientes aspectos relacionados con su capacidad de gestión de los servicios suministrados:

- Centro de gestión de tráfico y capacidades de enrutamiento, supervisión, operación y mantenimiento.

- Capacidad de reasignar tráficos en forma dinámica.

- Informes y reportes mensuales de gestión relacionados con el uso real de la red, calidad obtenida y otras estadísticas que estarán disponibles para el cliente. Estos reportes deberán contener y desplegar información similar a la disponible en el portal antes descrito, de tal forma que pueda visualizarse en la escala adecuada de acuerdo con los rangos contratados con una precisión de un 5%, y ser exportable a archivos Excel o similares, para análisis y procesamiento adicionales.

- Dichos informes se deberán elaborar para cada servicio e incluirán en cada caso valores globales (todos los sitios) e individuales (por cada sitio) cuando corresponda, señalando entre otros:

La disponibilidad mensual global y por sitio.

uso real de ancho de banda de subida y bajada, y parámetros de calidad como pérdida de paquetes, latencia y jitter. Para todos estos valores se indicarán valores promedio y extremos (mínimos y máximos) del mes, por servicio y recinto cuando corresponda.

El detalle y formato de estos informes se convendrán con el proponente adjudicado.

El proponente deberá disponer de un servicio de monitoreo, seguimiento, soporte y solución de fallas de todos los servicios otorgados que opere de forma continua 7x24. El proponente deberá contar con un número de acceso telefónico con atención 7 x 24 para recibir y registrar los requerimientos efectuados por el cliente, además de permitir su seguimiento y solución satisfactoria (cierre). Además, deberá proveer un sistema vía web que permita la comunicación de fallas o eventos a resolver por parte del proponente, el que deberá permitir efectuar el seguimiento de la solución y análisis de tiempos de solución de fallas y entregar estadísticas de gestión. Dentro de la oferta técnica, el proponente deberá considerar aspectos de soporte y mantenimiento, además de capacitación a personal técnico del cliente basado en la ciudad de Santiago.

Se requiere que el oferente adjudicado mantenga un registro de todos los eventos que afecten la continuidad operativa de los servicios contratados, este debe ser llevado en formato de informe mensual, tanto a nivel ejecutivo como a nivel de detalle, en formato Excel.

2.2.2. Servicio de conectividad vía Internet

En el caso que se decidiera emplear accesos de Internet en vez de la red IP / MPLS, ya sea en forma parcial o total, se deberán considerar las siguientes especificaciones:

- El servicio de Internet deberá contar con 64 IP públicas continúas configuradas en una red máscara 25, con anchos de banda para los accesos al sitio central (CENCO) y a los sitios remotos que se detallan en el anexo correspondiente.

- Todos estos anchos de banda deberán ser simétricos y con tasa de agregación de 1:1 según las capacidades que se indican en el “Anexo Direcciones y BW Red Transporte v2.xlsx”. En el caso del sitio central CENCO el servicio deberá contar con dos accesos en alta disponibilidad.

- Se deberá asegurar además el acceso a los servicios cloud de proveedores como AWS, MS Azure y Google Cloud entre otros.

- Los accesos a los sitios remotos deberán ser vía VPN site to site.

- Para la interconexión de los VMS a Internet debe incluirse un cortafuegos o firewall. Esta conexión deberá configurarse en lo posible exponiendo solo el componente para acceso a Internet del servidor y ubicándolo en una zona desmilitarizada (DMZ) con cortafuegos en ambos lados.

- El componente para acceso a Internet del servidor del VMS se deberá instalar en una DMZ y en una computadora con dos interfaces de red: una para comunicación interna y la otra para el

acceso a Internet. Esto permite a los usuarios de clientes Internet conectarse al servidor con una dirección IP pública, sin comprometer la seguridad o disponibilidad de la red VMS.

- En caso de existir previamente conexiones a Internet en determinados sitios, se privilegiará el separar la infraestructura existente de la nueva que se contrate. De ser necesario compartir algún elemento se deberán implementar VLANs separadas para aislar los tráficos administrativos existentes de los generados por este sistema.

- Para el tráfico internacional el proponente deberá Indicar los proveedores Tier 1 internacionales a través de los cuales se brindará el servicio de conectividad internacional y las respectivas capacidades que dispone la conectividad de cada ISP con cada uno de ellos.

- Se deberá suministrar un diagrama de interconexión de los ISP ofertados con los proveedores Tier 1 internacionales y otro diagrama con la interconexión en los puntos de llegada internacionales hacia los principales backbones y NAPs (Network Access Point) en USA y Europa, e informar acerca de:

    - Ancho de banda utilizado en cada tramo de la interconexión internacional
    - Punto de acceso internacional hasta el cual garantiza el ancho de banda provisto
    - Nivel de redundancia del servicio
    - Tiempos de activación del respaldo.
    - Diagrama de conectividad que ilustre las salidas internacionales del proponente, incluyendo respaldos.

- La latencia observada en cada uno de estos servicios, a nivel nacional deberá ser menor a 10 milisegundos, y a nivel internacional deberá ser menor a 150 milisegundos.

2.3. Plan de integración con los sistemas de televigilancia existentes.

A continuación, se desarrolla un posible plan que considera las diversas etapas que se visualizan en el proyecto desde el inicio a su puesta en marcha, pasando por todas las actividades intermedias

- **Definiciones Previas**

Con objeto de disminuir la incertidumbre a los proveedores que realizaran la integración, y que finalmente ellos las traspasan a precio, es importante que antes de un llamado a licitación se encuentre definido:

- Cantidad total de cámaras a integrar en CENCO (considerar posible ampliación).
- Catalogar y cuantificar las cámaras que requieren analítica (considerar posible ampliación y/o instalación de cámaras especiales para propósitos particulares).
- Si existirá o no acceso de cámaras de los vecinos.
- Qué tipo de analítica se realizará.
- Quien realizara las interconexiones a la red de transporte.
- Cantidad de operadores en CENCO. Esta información influye en varios aspectos, como el ancho de banda requerido, cantidad de posiciones, licencias (concurrentes y declaradas)

- Puntos/puerta de interconexión en cada municipio y organización privada.
- Señalar modelos, marcas y versión de cada dispositivo en especial el de los VMS.
- Señalar capacidad de almacenamiento deseado incluyendo otras especificaciones deseadas de la materia.
- Identificar los requerimientos de seguridad, tales como necesidad de cifrado y autenticación, para la transmisión, almacenamiento y tratamiento de los videos.
- Definir si se efectuarán reemplazos de algunos componentes existentes, como cámaras, enlaces de MMOO, servidores, VMS, etc. Lo anterior considerando que en algunos casos un reemplazo puede ser más costo eficiente que agregar módulos para asegurar la compatibilidad.
- Definir niveles de los servicios que se contraten en modalidad de arriendo, como la red IP / MPLS, acceso a Internet, etc. Entre estos parámetros se incluyen disponibilidad mensual, tiempos de reposición, facilidades de gestión y reportes, redundancia y otros aspectos.
- Especificaciones para el soporte de la plataforma integrada tanto en CENCO como en los puntos remotos, tiempos de respuesta, soporte de segundo y tercer nivel
- Facilidades de integración con desarrollos de analítica propios
- Escalabilidad para futuros crecimientos
- Plazos máximos de implementación, y horizonte del proyecto

- Licitación

- Confección de bases de licitación tanto generales como técnicas.
- Publicación de las bases.
- Realizar de presentación del proyecto a los que retiraron las bases.
- Periodo de preguntas y respuestas sobre la licitación.
- Recepción y evaluación de ofertas.
- Adjudicación.

- Inicio de Implementación

- Reunión de inicio con proveedor para definir o confirmar, entre otros parámetros, contactos, canal de comunicaciones, objetivos, plazos, procedimientos varios (calidad, no conformidades, seguridad, medio ambiente, etc.).
- Confección de ingeniería de Ingeniería de detalle por parte del proveedor.
- Aceptación de la Ingeniería de detalle.

- Instalación

- Montaje del hardware (Dispositivo de extracción y Analítica de video, Dispositivos de Red, Servidores de Análisis, Almacenamiento, Elementos de Seguridad) en cada punto.
- Montaje del hardware (Consola de Monitoreo, Consola de Análisis, Almacenamiento, Elementos de Seguridad, Dispositivos de Red) en CENCO.

- Configuraciones

- Integrar/habilitar en VMSs y/o cámaras con equipos adicionados.
- Configurar y verificar la red de trasporte para asegurar una transmisión eficiente.
- Configuración de servidores y otros componentes del sistema de extracción en cada punto.
- Configuración de servidores y otros componentes del sistema de monitoreo central en CENCO.
- Implementar las medidas de seguridad como firewalls y VPNs
- Configurar alertas y notificaciones según los requerimientos de seguridad.
- Integrar el software de análisis de video para funciones avanzadas etc.

Nota: eventualmente se deberán hacer cambios en la programación actual de algunos VMS para que operen con protocolos estándar como ONVIF, RTSP, etc., lo que implicara la colaboración de la empresa que brinda soporte a la municipalidad u organización.

- Pruebas y Validación

- Pruebas de Funcionamiento (transmisión de video, almacenamiento, calidad de video y la latencia, calidad de analítica, etc.).
- Pruebas de Seguridad.
- Sintonía fina (ajustes y optimización de configuraciones según los resultados de las pruebas.

- Capacitación

- Capacitación general al personal para que entienda qué se adicionó a su sistema, cómo opera, cuidados, responsable del sistema frente a problemas, etc.
- Capacitación al personal operador en el uso de la plataforma, en procedimientos varios y en las políticas de seguridad.

- Marcha Blanca

- Período de prueba o de funcionamiento preliminar del sistema antes de entrar a la fase de explotación

- Documentación

- Entrega del proveedor de documentación detallada de la instalación y configuración del sistema (as built).
- Entrega por parte del proveedor de manuales de usuario.
- Entrega por parte de SPD (o quien corresponda) políticas para el acceso y uso del sistema y procedimientos para el manejo de incidentes, la revisión de grabaciones y su distribución.

- Aceptación el sistema

• Validación y aprobación del sistema por usuarios finales y los stakeholders.

- Explotación del sistema

• Entrada en producción del sistema proporcionando los resultados previstos.

- Mantenimiento

• Dar inicio al plan de mantenimiento preventivo y evolutivo de software y hardware.
• Dar inicio al sistema de monitoreo y detección de fallas del sistema para informar al proveedor y resolver los problemas rápidamente.

2.4. Propuesta de equipamiento y software necesarios.

A continuación, se entrega una propuesta de posible equipamiento y software necesarios, los cuales pueden varias según la solución específica, ya que en algunos casos se pueden integrar algunos equipos en uno solo, o bien una determinada funcionalidad se puede presentar separada en múltiples equipos.

También se común que diversos fabricantes denominen en forma distinta a determinados dispositivos, por lo tanto, esta lista debe considerarse como referencial.

2.4.1. Equipamiento en CENCO

Todo el equipamiento que se instale en CENCO debe satisfacer la normativa interna de esta institución, como por ejemplo los equipos deben ser rackeables, contar con fuentes de poder redundantes, uso de VPN y otras normativas de seguridad.

Se recomienda solicitar a CENCO formalmente la lista de esos requerimientos específicos para incluirlos en las especificaciones finales de las bases de licitación.

En el centro de control deberían estar presente al menos las siguientes funcionalidades en forma integrada o unitaria.

Consola de Monitoreo.

Corresponde a la interfaz de usuario (GUI) que permite la visualización en tiempo real y consolidada de videos, eventos y datos capturados por las cámaras y sensores desplegados en terreno y eventualmente la que es personalizable para mostrar la información y los controles más relevantes según las necesidades del operador. La consola típicamente se encuentra constituida por software

especializado, procesadores y monitores individuales y video wall que permiten el monitoreo de los múltiples streaming de video y datos.

Además, debería brindar capacidades de automatización que permiten la configuración de alertas y notificaciones basadas en reglas predefinidas, visualizar mapas, GPS, eventos y otros. (no todos los fabricantes pueden hacer todo lo mencionado).

Debe mostrar a través de interfaces gráficas, como Dashboards, informaciones tales como espacio en disco, cantidad de dispositivos conectados y generar alarmas al alcanzar ciertos niveles de almacenamiento.

Debe ser capaz de recibir y controlar entradas y salidas de alarma de dispositivos como cámaras, dispositivos de entrada-salida, de manera que permita iniciar eventos manualmente o recibir señales de intrusión o sistemas de control de acceso.

Debe permitir la importación de mapas en diferentes formatos y ser compatible con servicios de mapas inteligentes como Bing, Google y mapas de OpenStreetMap, permitiendo mapas GIS georeferenciados, como shapefiles, dibujos CAD (DWG / DXF) y permitir la construcción de diseños de múltiples capas.

Los mapas inteligentes deben permitir la visualización de íconos para alarmas, dispositivos de entrada, micrófonos, vista previa de video, permitir el control integrado de micrófonos y entradas de dispositivos, posicionar iconos rápida y fácilmente, enlaces directos a otros sitios en caso de múltiples sitios.

Debe permitir que las imágenes de las cámaras de sitios diferentes puedan ser visualizadas en el sistema central.

Consola de Análisis.

Corresponde a herramientas centralizadas para para análisis avanzado de video pudiendo emplear distintos algoritmos, inteligencia artificial y machine learning.

Dependiendo si la analítica se realiza en el centro de acopio del video o bien en CENCO, esta consola debe poseer la posibilidad de trabajar con metadata de personas y vehículos y los subfiltros correspondientes. También debería incorporar la capacidad de poder hacer reconocimiento de placas (LPR), reconocimiento de marcas y modelos (MMR), detección de movimiento, reconocimiento facial, seguimiento entre cámaras, análisis de comportamiento, búsquedas de similitudes, detección de Objeto Olvidado (OLB), seguimiento de objetos (OT), caída de personas (PF), detección de armas y otros para aquellos casos que no exista analítica en borde.

El sistema debe admitir cámaras con el protocolo estándar RTSP (Protocolo de Transmisión en Tiempo Real) y con ONVIF.

El sistema debe procesar videos para obtener metadatos para búsqueda, alerta y revisión estadística.

Almacenamiento.

El almacenamiento se realizará preferentemente en los sitios remotos para disminuir los requerimientos de ancho de banda, manteniendo el uso de los sistemas de almacenamiento existentes cuando ello sea factible.

El sistema centralizado accederá a los almacenamientos remotos en forma directa cuando ello sea posible, lo que ocurrirá generalmente en los casos en que los sistemas remotos sean de la misma marca del nuevo sistema central. En caso contrario se deberán instalar y habilitar los medios necesarios (hardware y software) para acceder al almacenamiento remoto de otras marcas desde el sistema central.

Eventualmente podría existir alguna infraestructura de almacenamiento centralizada o en la nube, incluyendo bases de datos para metadatos y archivos de video según la filosofía del fabricante y para los datos que se consideren más relevantes y que requieran acceso local.

Algunas especificaciones del sistema de almacenamiento local son las siguientes:

Debe ser totalmente compatible con la grabación digital simultánea de múltiples canales de video y audio y permitir la grabación continua por un mínimo de 30 días.

Debe permitir que el cliente que se conecta al servidor solicite imágenes en vivo a una velocidad de fotogramas diferente y a una resolución inferior a la configuración de grabación, optimizando el funcionamiento de los equipos de los operadores.

Debe ser compatible para la detección automática de modelos de cámaras al instalarlos en el servidor de grabación.

Debe estar equipado con tecnología de grabación segura y de alta velocidad con compatibilidad de imágenes JPEG o secuencias MPEG4, H.264 y H.265, incluido el audio.

Debe permitir la función de bloqueo de evidencia, es decir, permitir que se evite la eliminación de una evidencia específica presente en el sistema independientemente del tiempo de grabación del sistema, incluso después de alcanzar el tiempo máximo de retención de imágenes predefinido.

Debe permitir al operador crear marcadores (bookmarks) de forma manual para insertar comentarios en imágenes que puedan convertirse en evidencia importante dentro del sistema, y también en modalidad automática, mediante la activación de reglas previamente creadas en el sistema.

Debe identificarse fácilmente en la grabación a través del icono de identificación del marcador y tener la opción de buscar a través de marcadores dentro del software cliente de monitoreo.

La evidencia caracterizada como marcador debe tener un tiempo de almacenamiento diferente al tiempo de grabación normal.

Elementos de Seguridad.

A continuación, se entregan las principales recomendaciones de seguridad que son aplicables a los dispositivos en CENCO, a los equipos y software en los sitios remotos y a la red de transporte entre ambos, por lo que la responsabilidad de estas medidas puede estar dispersa a lo largo de diversos sistemas. Por esta razón es muy importante que el responsable del proyecto cumpla con el rol de velar por la seguridad en forma integral y en las diversas instancias ya indicadas.

En el caso de la red de transporte, las medidas de seguridad deben ser aplicadas con mayor rigurosidad en el caso de emplear en forma parcial o total accesos Internet, ya que por su naturaleza es una red esencialmente insegura, y expuesta a ataques de terceros, amenazas de denegación de servicios y otros. En cambio, la red MPLS es una red privada en la que el operador adopta determinadas medidas de seguridad y el riesgo es mucho menor, lo que no impide que igualmente sea conveniente tomar ciertas precauciones.

Toda la comunicación en ambas direcciones entre CENCO y los sitios remotos debe realizarse de forma cifrada. Una recomendación al respecto es el empleo del protocolo HTTPS que es un tipo de cifrado que ayuda a impedir que terceros se apoderen de la comunicación de una cámara de vídeo y del cliente o servidor VMS. El sistema HTTPS utiliza un cifrado basado en la seguridad de textos para crear un canal cifrado (cuyo nivel de cifrado depende del servidor remoto y del navegador utilizado por el cliente) más apropiado para el tráfico de información sensible que el protocolo HTTP, con lo cual se consigue que la información sensible (usuario y claves) no pueda ser usada por un atacante que haya conseguido interceptar la transferencia de datos de la conexión, ya que lo único que obtendrá será un flujo de datos cifrados más difíciles de descifrar.

Todos los servidores deben contar con el software de base actualizado, realizar escaneos de vulnerabilidades, contar con logs de eventos, mantener los puertos de comunicación innecesarios cerrados.

Todas las aplicaciones deben utilizar la última versión del framework de todos los sistemas implementados, contar con identificadores únicos para usuarios, y disponer de gestión segura de las credenciales.

Se deberán utilizar Firewalls para la protección de la red y los datos y sistema de autenticación y control de acceso, y uso de VPN.

Se deberá disponer de una solución de monitoreo de seguridad de los sistemas a través del SOC, la que puede implementarse con recursos propios o de mismo integrador.

Se deberá disponer de una solución de monitoreo de la integridad de carpetas y archivos.

La solución de integración deberá cumplir con los estándares definidos en FIPS 140-2 (Federal Information Processing Standard).

El integrador o sus representadas deberá estar certificado en la norma ISO 27001

Se deberá contar con una solución de NGAV (Antivirus de Próxima Generación) y EDR (Detección y Respuesta de Endpoints) para los servidores y estaciones de trabajo a implementar en CENCO.

Se deberá disponer de una solución de inventario y de gestión de parches para mantener el entorno siempre actualizado y controlado, reduciendo los riesgos tecnológicos y controlando el uso de software y hardware de las plataformas.

Se deberá disponer de una solución de gestión de vulnerabilidades, que es una práctica de seguridad que permite identificar, evaluar y remediar posibles fallas de seguridad en dispositivos, redes y aplicaciones para reducir los riesgos de ciberataques e infracciones dentro de la organización. Esta solución debe usarse en los servidores de la solución y las estaciones de trabajo en CENCO.

Empleo de Firewall de próxima generación (NGFW), que es un dispositivo de seguridad de red que monitorea el tráfico entrante y saliente, bloqueando o permitiendo paquetes específicos de acuerdo con reglas de seguridad definidas, filtrando el tráfico de red para una mayor protección contra amenazas internas y externas. Una de sus características es la VPN - Red Privada Virtual, que mantiene una conexión integrada, privada y segura, utilizando un túnel encriptado entre dispositivos en una red, protegiendo la información contra agentes externos. Esta implementación es altamente recomendable en el caso de usar accesos Internet.

Empleo de una solución WAF (Firewall de aplicaciones web), que protege las aplicaciones web contra ataques maliciosos, exposición de datos no autorizada y tráfico de Internet no deseado, evitando varios tipos de amenazas que pudieran comprometer la continuidad del negocio.

En los sitios remotos asignar VLANs para las cámaras y VMSs separadas del resto de los equipos de usuarios.

Emplear el protocolo de autenticación IEEE 802.1X en los switches y cámaras, el cual garantiza que el switch se comunique con la cámara y no con algún equipo extraño a la red.

Dispositivos de Red aportados por el proveedor de servicio

Equipos tales como Switches y/o Router gestionados del tipo empresariales de alta capacidad, velocidad e interfaces de red adecuados al medio de transporte seleccionado permitiendo así una gestión eficiente del tráfico de red.

En el caso de los routers que van en CENCO, estos deben contar con puertos GEthernet, soportar protocolos MPLS y SDWAN, gestión cloud, VPN, fuentes de poder redundantes, hot swapping, entre otras características.

2.4.2. Equipamiento en los sitios remotos

Equipos de red

- Los routers que se instalen en los sitios remotos por parte del proveedor pueden utilizar puertos de menor capacidad según el ancho de banda que deban soportar en cada caso

específico, y en general requieren menor procesamiento que los del sitio central, mientras que el resto de las otras características son similares.

- Por el lado de los equipos que son provistos por los usuarios (municipalidades y otras organizaciones) para el caso de MPLS se debe disponer como un mínimo de un switch con la cantidad de puertas suficientes, administrables, con soporte para VLANs, PoE, y soporte de protocolo 802.1x.

- Si se utilizará Internet como acceso, para la interconexión debe incluirse un firewall que deberá configurarse en lo posible exponiendo solo el componente para acceso a Internet del servidor y ubicándolo en una zona desmilitarizada (DMZ) con cortafuegos en ambos lados.

Sistemas de video en municipios y organismos privados

Tanto los municipios como los organismos privados ya cuentan con sus propios sistemas de videovigilancia con más o menos facilidades según lo que han adoptado de acuerdo al proveedor o proveedores que han seleccionado.

Dado que son sistemas existentes y algunos de ellos con contrato de mantenimiento, es complejo introducir modificaciones en ellos por lo cual se sugiere en vez de intervenirlos, colocar hardware y software adicionales con las siguientes funcionalidades:

Dispositivo de extracción y Analítica de video:

Servidor dedicado o NVR inteligente con software adecuado para realizar or un lado, la interconexión con el sistema existente permitiendo la extracción de video desde las cámaras o VMS y/o del sistema de almacenamiento y que permita hacer la analítica de video requerida y/o integre los metadatos de las cámaras / VMS, y por el otro lado envíe la información y flujos a CENCO.

Servidores de Análisis

Servidores dedicados para el análisis de video con capacidades de procesamiento gráfico de acuerdo con el tipo y cantidad de analítica a realizar en forma local.

Almacenamiento

Si es que el proveedor no puede ingresar al sistema de almacenamiento de imágenes existentes por ser de un formato propietario, deberá colocar su propio sistema para ir almacenando la totalidad de las capturas.

3. Conclusiones

En este informe se entrega la documentación de diseño preliminar del proyecto de interconexión e integración de los sistemas de video vigilancia existentes en 14 comunas de la zona centro norte de la región metropolitana y en otras instituciones en esas mismas comunas.

Para el diseño de la interconexión e integración se describe en primer lugar la situación actual y luego se analizan distintas opciones de interconexión, recomendándose adoptar la interconexión a través de la red IP /MPLS. A continuación, se entregan las especificaciones técnicas del diseño de interconexión para esas opciones.

Luego se analizan las características y desafíos que impone la integración de los diversos sistemas en operación para lo cual existen diferentes alternativas y estrategias que son adoptadas por los distintos fabricantes e integradores de plataformas para consolidar un sistema único de gestión y visualización de video, incorporándole además funcionalidades de analítica e inteligencia artificial. Esto se pudo ratificar en reuniones sostenidas con diversos integradores y fabricantes y análisis de la documentación técnica especializada, lo cual se produce entre otras razones por la carencia de estándares de integración, a diferencia de lo que ocurre en el mundo de las telecomunicaciones.

Con el fin de no excluir en forma temprana del proceso de licitación a ninguno de estos integradores o fabricantes, se privilegió la elaboración de especificaciones funcionales para la integración, dejando abierto a que los futuros proponentes escojan la arquitectura más adecuada que cumpla los objetivos del proyecto y considerando las opciones más costo eficientes disponibles en su portafolio de productos. Esto permitirá ampliar la oferta posterior de soluciones a ser recibidas en el proceso de licitación.

En el documento también se incluye un plan de integración con los sistemas de televigilancia existentes, detallando las etapas y actividades desde las definiciones previas, especificaciones de detalle, proceso de licitación y adjudicación, implementación y puesta en marcha, hasta la entrada en operación del nuevo sistema.

Por último, se incluye una propuesta de equipamiento y software necesarios para el proyecto, detallando las principales funcionalidades de estos componentes.

Se puede concluir que este es un proyecto factible, pero que presenta cierta complejidad por la diversidad de equipos y sistemas en operación, que involucra a múltiples actores y roles, que requerirá diversas adecuaciones y mejoramientos en parte de la infraestructura existente, en especial en el sector municipal.

4. Anexos

En la tabla siguiente se indican los anchos de banda que se han aproximado a los enteros superiores de múltiplos de 100 Mbps., según los criterios explicados en el producto 2, capítulo 2.1. (es decir, imágenes de alta resolución Full HD o 1080p y entre 20 a 30 FPS que se visualizan en forma simultánea, para lo cual se ha estimado un ancho de banda de 4 Mbps. por cámara que asegura obtener esa calidad en la mayoría de las situaciones que corresponden a iluminación estándar y con nivel de detalle y grado de movimiento moderados).

La cantidad de cámaras considerada corresponde en el caso de las municipalidades al 50% del total existente en ellas, mientras que para las organizaciones privadas se consideró una cantidad estándar que corresponde a las cámaras que visualizan ambientes exteriores e ingresos.

N°	Comuna u Organización	Dirección Monitoreo	Propuesta total cámaras propias en visualización simultánea en CENCO	BW Sugerido (Mbps)
1	Santiago	Dirección Seguridad Municipalidad Erasmo Escala 2612	345	2.000
2	Renca	Dirección Seguridad Municipalidad (Dorsal 1317), Renca	29	200
3	Independencia	Dirección Seguridad Municipalidad (Pasaje Nueva Colon 1073, Independencia)	23	100
4	Quinta Normal	Carrascal 4447, Quinta Normal	50	200
5	Tiltil	Av. Arturo Prat 200, Tiltil	0	0
6	Lo Prado	Los Copihues 5849, Lo Prado	48	200
7	Recoleta	6 Comisaría (Gavilán 1980).	16	100
8	Lampa	59 Comisaría (Sargento Aldea 1100, Lampa)	18	100
9.1	Estación Central	58 Comisaría (Antártica 4701)	22	100
9.2	Estación Central	21 Comisaría (Ecuador 4050)	20	100
10	Huechuraba	Municipalidad (Premio Nobel 5555, Huechuraba).	41	200
11	Cerro Navia	45 Comisaría Carabineros (Los Conquistadores 7350, Cerro Navia)	9	100
12	Quilicura	49 comisaría Carabineros, Cabo primero Carlos Cuevas Olmos 256, Quilicura	46	200

N°	Comuna u Organización	Dirección Monitoreo	Propuesta total cámaras propias en visualización simultánea en CENCO	BW Sugerido (Mbps)
13	Conchalí	Dirección Seguridad Municipalidad Augusto Ossa 3069, Conchalí	44	200
14.1	Colina	General San Martín km. 28 s/n, Colina	58	300
14.2	Colina	El Valle s/n (frente a la Shell), Colina	25	100
14.3	Colina	General San Martín Km. 31, Esmeralda, Colina	8	100
15	COPSA	No entrega Información	No entrega Información.	Sin Información.
16	Concesión Acceso Nororiente a Santiago.	No entrega Información	30	200
17	Concesión Américo Vespucio Oriente: Tramo El Salto - Príncipe de Gales.	No entrega Información	30	200
18	Autopista Vespucio Norte	No entrega Información	30	200
19	Autopista Central	No entrega Información	30	200
20	Costanera Norte: Concesión Sistema Oriente - Poniente.	No entrega Información	30	200
21	Túnel San Cristóbal: Concesión variante Vespucio El Salto - Kennedy.	No entrega Información	30	200
22	Cámara de Centros Comerciales	No entrega Información	No entrega Información.	Sin Información.
23	Mall Arauco Quilicura	Av. Bernardo O'Higgins 581, Quilicura.	NA	NA
24	Mall Arauco Estación	Av. Libertador Bernardo O'Higgins 3250, Estación Central	30	200
25	Mall Arauco Buenaventura	San Ignacio 500, Quilicura	30	200
26	Mall Plaza Norte		30	200
27	CENCOSUD-Costanera Center	No entrega Información	30	200
28	Delegación Presidencial Regional Metropolitana de Santiago.	Morandé N° 93, Santiago	4	100
29	Gobierno Regional Metropolitano de Santiago.	Morandé N° 93, Santiago	No entrega Información.	Sin Información.
30	Gremio- Supermercados (ASACH)	No entrega Información	No entrega Información.	Sin Información.
31	Cencosud (Jumbo, Santa Isabel)	No entrega Información	30	200
32	SMU (Unimarc, Alvi, Mayorista 10 y Super10)	No entrega Información	30	200
33	Tottus	No entrega Información	30	200

N°	Comuna u Organización	Dirección Monitoreo	Propuesta total cámaras propias en visualización simultánea en CENCO	BW Sugerido (Mbps)
34	Walmart (Líder, Express de Líder, Lider.cl, SuperBodega Acuenta y Central Mayorista)	No entrega Información	30	200
35	Estadio Santa Laura	Santa Laura 1291, Independencia	30	200
36	SABA	No entrega Información	No entrega Información.	Sin Información.
37	Carabineros CENCO	Catedral 1337 Edificio Centenario	NA	10.000
	Totales		**1.256**	**17.400**

Esta misma información se entrega como planilla Excel “Anexo Direcciones y BW Red Transporte v2.xlsx” que debiera ser informado a un posible proveedor.