Respuestas a consulta ciudadana temas de medios de comunicación

Consultas empresa AUTER:

Observación N°1: Revalidación de la solución de conectividad seleccionada por desfase temporal entre evaluación e implementación
Desde el punto de vista de ingeniería, los criterios técnicos definidos en el instructivo parecen adecuados para la selección inicial de tecnologías de comunicación.
Sin embargo, se observa que en proyectos evaluados como medidas de mitigación, puede existir un desfase importante entre la evaluación original y la implementación efectiva. Durante ese período, las condiciones técnicas, urbanas, comerciales u operacionales pueden cambiar, afectando la viabilidad de la solución inicialmente seleccionada.
Esto puede ocurrir tanto en tecnologías inalámbricas, por cambios en línea de vista, obstrucciones, interferencias o saturación del espectro, como en fibra óptica u otras tecnologías, por variaciones en cobertura, factibilidad técnica, disponibilidad de red, permisos, postación, canalizaciones, costos o condiciones de implementación.
Por lo anterior, se consulta si el instructivo contempla un mecanismo de revalidación técnica de la solución de conectividad seleccionada al momento del inicio efectivo del proyecto, especialmente cuando haya transcurrido un período relevante desde la evaluación original. Dicha revalidación permitiría confirmar si la tecnología definida sigue siendo viable bajo las condiciones reales existentes o si corresponde actualizar la solución propuesta.

Respuesta:
"En relación con el eventual desfase temporal en la ejecución de la solución de conectividad, se deben diferenciar dos instancias del proceso:

1. ***Etapa de evaluación del IMIV:*** *Cuando el desfase transcurre entre la aprobación del Informe de Mitigación de Impacto Vial (IMIV) y la materialización del proyecto, las medidas de mitigación se definen de manera general enfocándose en el qué hacer y no en el cómo hacer. Esto se debe a que:*
    - *Los plazos entre la aprobación del instrumento y su ejecución pueden extenderse por varios años, por lo que una definición tecnológica prematura podría volver no factible la solución por cambios en el entorno, o privar al proyecto de avances tecnológicos más eficientes.*
    - *En la etapa conceptual del IMIV no se cuenta con los antecedentes de detalle ni con el nivel de ingeniería para definir la solución técnica definitiva.*
2. ***Etapa de proyecto ejecutivo y aprobación UOCT:*** *Cuando el desfase se da entre la aprobación técnica del proyecto de comunicaciones por parte de la UOCT y la ejecución de las obras, aplica lo dispuesto en el* ***Capítulo 4 (Sección 4.1.1 "Objetivos") del Manual de Señalización de Tránsito****. De acuerdo con esta normativa, la aprobación otorgada por la UOCT tiene una* ***vigencia de 1 año****.*

Si transcurrido ese plazo no se ha iniciado la construcción de las obras, el interesado debe reingresar los antecedentes a la UOCT para una nueva revisión y aprobación. Esta revalidación permite actualizar los estudios y confirmar que la solución propuesta sigue siendo técnicamente viable según las condiciones operacionales y del entorno vigentes. Adicionalmente, si durante el desarrollo de los trabajos se detectan condiciones no

previstas en la aprobación original, es posible ingresar las modificaciones correspondientes para su ajuste técnico."

Observación N°2: Incorporación de soluciones 4G/5G con Internet y VPN para tráfico de alto volumen
Se observa que el instructivo no considera explícitamente el uso de tecnologías 4G/5G con conexión a Internet e implementación de VPN CLOUD como alternativa de conectividad, sólo considera conexión M2M Privadas
Se estima conveniente permitir esta posibilidad, especialmente en aplicaciones que requieren transmitir grandes volúmenes de datos, como video, cámaras de tránsito u otros sistemas similares. Lo anterior, debido a que los enlaces M2M tradicionales no están diseñados comercial ni técnicamente para este tipo de tráfico permanente o de alto volumen.
En particular, la transmisión de video sobre enlaces M2M puede generar costos operacionales significativamente superiores, pudiendo encarecer de manera relevante la operación mensual y hacer económicamente inviable la solución. En estos casos, podría evaluarse el uso de planes de banda ancha móvil (planes BAM) u otros equivalentes, que suelen estar más orientados al consumo intensivo de datos. Sin embargo, al utilizar conectividad móvil con acceso a Internet, resulta necesario incorporar mecanismos de seguridad adecuados, tales como VPN, cifrado, control de accesos y segmentación de red , etc.
Adicionalmente, si no se desea depender de servicios de VPN en la nube o provistos por terceros, el instructivo podría considerar como alternativa la habilitación de un enlace dedicado a Internet en la UOCT, protegido mediante firewall perimetral y un servidor VPN propio, permitiendo establecer comunicaciones seguras entre los dispositivos remotos y la plataforma central.
Por lo anterior, se solicita reevaluar esta exclusión y/o que el instructivo proponga alguna alternativa factible económica y técnicamente al día de hoy sin sacrificar políticas de ciberseguridad.

Respuesta:
"*Previamente no se habían considerado a fondo los dispositivos de CCTV, estación de conteo o mensajería variable en el caso de conexión por red móvil, y se consideró correcta la observación sobre la inclusión de otros medios de conexión aparte de los M2M para estos casos, ya que se necesitaba otra solución para transmitir grandes volúmenes de datos.*

Dicho eso, se ampliaron las opciones en el instructivo para este tipo de conexión, incluyendo actualmente APN privado o corporativo, servicios M2M/IoT y Banda Ancha Móvil (BAM). Además, se ampliaron las características de seguridad para que concuerden con las nuevas opciones incluidas."

Observación N°3: Revisión de exigencia de latencia para radioenlaces
Se observa que el instructivo establece exigencias de latencia para radioenlaces que podrían resultar muy restrictivas en ciertos escenarios de implementación.
En particular, si el sistema de control de tránsito de la UOCT (según instructivo) es capaz de operar adecuadamente con latencias del orden de 100 ms cuando se utilizan soluciones basadas en routers 4G, exigir una latencia máxima de 10 ms para un radioenlace podría entenderse como un estándar de excelencia técnica deseable, pero no necesariamente como una condición estrictamente indispensable para asegurar la continuidad operacional del servicio. Si bien una baja latencia es un atributo positivo y recomendable, no todos los enlaces inalámbricos pueden garantizar permanentemente valores cercanos a 10 ms, especialmente considerando factores como distancia, condiciones de propagación, interferencias, topología de red, cantidad de saltos, equipamiento utilizado y condiciones propias del entorno urbano. Por lo anterior, se solicita evaluar la posibilidad de incorporar mayores tolerancias en los criterios de latencia

exigidos para radioenlaces, o bien establecer rangos diferenciados según el tipo de aplicación, criticidad del servicio y comportamiento real requerido por el sistema de control de tránsito. De esta forma, se evitaría descartar soluciones técnicamente viables que, aun no cumpliendo con una latencia de 10 ms, sí podrían operar de manera estable y segura dentro de parámetros compatibles con la continuidad operacional del servicio.

Respuesta:
"Revisando nuevamente el apartado de latencia para radioenlace y considerando el análisis hecho en esta observación, se considera correcto de que el exigir una latencia menor a 10 ms en este ámbito puede resultar muy restrictivo en innecesario en este ámbito ya que los equipos igualmente pueden tener una comunicación efectiva con una latencia mayor, por lo que se decidió cambiar este parámetro de 10 a 50 ms para ajustarlo a un valor más permisivo."

Consultas empresa KAPSCH:

Recomendación 1: Incorporación de una Matriz de Criticidad de Servicios

Resumen
Se recomienda incorporar una clasificación simple de criticidad de los servicios conectados (alta, media y baja), que permita adaptar los requisitos técnicos según el impacto operacional.
En qué consiste
- Definir disponibilidad requerida por tipo de sistema.
- Definir latencia y jitter esperados.
- Indicar cuándo se recomienda redundancia.
- Relacionar criticidad con seguridad y monitoreo.

Justificación
El instructivo actual evalúa tecnologías, pero no formaliza la criticidad de los servicios. La Ley N.º 21.663 establece requisitos asociados a prevención, respuesta y continuidad, por lo que una clasificación de criticidad ayuda a aplicar medidas proporcionales.
Referencia:
https://nuevo.leychile.cl/navegar?idNorma=1202434&idParte=10496231&idVersion=2222-02-02
Ubicación sugerida en el documento actual
Sección 5.1 Inicio del Proceso y sección 6 Consideraciones Generales.
Respuesta:
"Se valora la recomendación. Para efectos de este instructivo, la criticidad relevante corresponde a la de las intersecciones semaforizadas. Actualmente, los distintos centros de control de la UOCT clasifican las intersecciones según su nivel de importancia en la red vial; sin embargo, cada centro aplica sus propios criterios de categorización, por lo que no existe una clasificación única a nivel nacional.
Por lo anterior, la incorporación de una clasificación de criticidad en el instructivo se considerará como parte de la mejora continua del documento, una vez que se unifiquen los criterios de categorización de intersecciones entre los distintos centros de control. En esa instancia se evaluará su vinculación con los requisitos técnicos de los medios de comunicación."
Recomendación 2: Requisitos mínimos de ciberseguridad

Resumen
Se recomienda definir un estándar mínimo de seguridad aplicable a todos los medios de comunicación, sin imponer soluciones complejas o de alto costo.
En qué consiste
- Uso de redes privadas o túneles cifrados según criticidad.

- Segmentación lógica entre control, video y gestión.
- Restricción de accesos desde internet público.
- Autenticación robusta para accesos remotos.
- Registro básico de eventos e inventario de activos.

Justificación

La Ley N.º 21.663 y la normativa publicada por ANCI establecen obligaciones de prevención, reporte, respuesta y gestión de incidentes.

Referencias:

https://nuevo.leychile.cl/navegar?idNorma=1202434&idParte=10496231&idVersion=2222-02-02 ; https://anci.gob.cl/normativa/ ; https://anci.gob.cl/normativa/instrucciones/

Ubicación sugerida en el documento actual

Nueva subsección dentro de 6 Consideraciones Generales, con aplicación transversal a todas las tecnologías.

Respuesta:

"Se acoge la recomendación. Si bien el instructivo ya exige, para cada tecnología, enlaces cifrados o con acceso controlado y conexiones que no transiten por internet público (APN privado, MPLS o red privada del integrador), estas exigencias se encuentran dispersas en las tablas de cada sección. Adicionalmente, tal como se indicó en la respuesta a la Observación N°2 de AUTER, se ampliaron las características de seguridad asociadas a las nuevas opciones de conexión por red móvil.

Por lo anterior, se incorporará en la sección 6 una nueva subsección "Requisitos mínimos de ciberseguridad", de aplicación transversal a todos los medios de comunicación, que considerará como mínimo:

– Conexión mediante redes privadas (APN privado, MPLS, enlace propio) o túneles cifrados (VPN), sin exposición directa de los dispositivos de terreno a internet público.

– Segmentación lógica (por ejemplo, mediante VLAN) entre el tráfico de control semafórico, el de video y el de gestión de equipos.

– Acceso remoto a los equipos sólo a través de los mecanismos autorizados por la UOCT, con credenciales individuales, eliminación de contraseñas por defecto y deshabilitación de servicios no utilizados.

– Registro de eventos de los equipos de comunicación y entrega de un inventario de activos (ver respuesta a la Recomendación 4).

Cabe señalar que las políticas específicas de ciberseguridad, así como la gestión y reporte de incidentes, corresponden a la UOCT en el marco de las obligaciones que la Ley N.º 21.663 y las instrucciones de la ANCI establecen para la institución. Por ello, el instructivo fijará requisitos mínimos que los mandantes y contratistas deberán cumplir, sin perjuicio de las directrices adicionales que la UOCT defina para la integración a su red."

Recomendación 3: Protocolo de Pruebas de Aceptación de Enlaces

Resumen

Se recomienda establecer un conjunto mínimo de pruebas técnicas obligatorias para todos los enlaces de comunicación, incluyendo el medio principal y los tramos necesarios de cableado estructurado.

En qué consiste

- Pruebas generales: latencia, jitter, pérdida de paquetes, disponibilidad, rendimento (throughput) y multicast, cuando es requerido.
- Pruebas operativas: reconexión ante fallas, monitoreo remoto, acceso seguro y alarmas.

- Pruebas por tecnología: fibra con OTDR y potencia óptica; radio con RSSI/SNR; móvil con RSRP/RSRQ/SINR; enlace dedicado con validación de SLA.
- Cableado estructurado: certificación de continuidad, atenuación y desempeño, considerando ANSI/TIA-568, ISO/IEC 11801 e IEEE 802.3 como estándares técnicos de referencia. Este punto es especialmente útil cuando se ocupe cableado UTP/SFTP en tramos exteriores cortos.

Justificación

El instructivo actual no considera explícitamente los tramos de cobre, los cuales suelen ser puntos críticos de falla. Incorporarlos asegura el desempeño real del enlace completo. La Ley General de Telecomunicaciones reconoce las telecomunicaciones por línea física, radioelectricidad, medios ópticos u otros sistemas electromagnéticos, por lo que la validación del enlace debe considerar todos sus componentes.
Referencia: https://www.leychile.cl/navegar?idNorma=29591

Ubicación sugerida en el documento actual

Sección 6.1 Entrega de documentación técnica y sección 6.2 Periodo de marcha blanca.

Respuesta:

"Se acoge parcialmente la recomendación. El instructivo ya exige certificaciones de enlace por filamento para fibra óptica y certificación de pruebas de aceptación para enlaces dedicados (sección 6.1), y la recepción de obras se rige por el "Procedimiento de inspección de obras de semaforización" (sección 6.2), documento en el cual corresponde detallar los protocolos de prueba.
No obstante, se considera pertinente que el instructivo explicite un conjunto mínimo de pruebas, las que deberán ser ejecutadas y acreditadas por el mandante, a través del contratista o consultor que utilice el instructivo para la selección e implementación del medio de comunicación. La UOCT no realizará pruebas de validación de los enlaces, siendo responsabilidad de quien implementa la solución asegurar que esta cumple con los requisitos establecidos. En consecuencia, se incorporará una nueva sección 6.3 con las siguientes pruebas mínimas:
– Pruebas generales para todos los enlaces: latencia, jitter, pérdida de paquetes y rendimiento (throughput), verificando el cumplimiento de los valores definidos para la tecnología seleccionada, y pruebas de multicast cuando el sistema lo requiera.
– Pruebas por tecnología: fibra óptica con OTDR y medición de potencia óptica; radioenlace con RSSI y SNR medidos en terreno; red móvil con RSRP, RSRQ y SINR en el punto de instalación; y enlace dedicado con validación de los parámetros comprometidos en el SLA.
– Tramos de cableado estructurado de cobre (UTP/FTP/SFTP): certificación de continuidad, atenuación y desempeño, tomando como referencia las normas ANSI/TIA-568 e ISO/IEC 11801.
– Pruebas operativas: verificación del acceso remoto seguro hacia la red de la UOCT, reconexión automática ante caídas del enlace y correcta recepción de alarmas.
La disponibilidad del enlace, al ser un indicador que requiere un período de observación, deberá ser acreditada por el mandante durante el período de marcha blanca."

Recomendación 4: Monitoreo, inventario y sincronización horaria

Resumen

Se recomienda establecer capacidades mínimas de operación continua mediante monitoreo, trazabilidad e integración horaria.

En qué consiste

- Monitoreo de disponibilidad, latencia, pérdida, estado de equipos y niveles de señal.
- Inventario de equipos, direcciones IP, SIM, firmware, ubicación y responsable asociado.
- Sincronización horaria mediante NTP para consistencia de eventos, alarmas y registros.

Justificación

La capacidad de detectar, reportar y analizar incidentes depende de contar con trazabilidad, monitoreo e información horaria confiable. Esto se relaciona con la Ley N.º 21.663 y las instrucciones generales de ANCI sobre gestión de incidentes.
Referencias:
https://nuevo.leychile.cl/navegar?idNorma=1202434&idParte=10496231&idVersion=2222-02-02 ; https://anci.gob.cl/normativa/instrucciones/
Ubicación sugerida en el documento actual
Nueva subsección dentro de 6 Consideraciones Generales.
Respuesta:
"Se acoge parcialmente la recomendación. El monitoreo de los enlaces y equipos de comunicación integrados a la red es realizado por la UOCT desde sus sistemas centrales, por lo que el instructivo no exigirá a los mandantes plataformas de monitoreo propias. Sin embargo, se considera necesario asegurar que los equipos instalados permitan dicha supervisión y que la UOCT cuente con la información necesaria para la trazabilidad de los activos. En consecuencia, se incorporará en la sección 6 lo siguiente:
– Los equipos de comunicación deberán permitir su gestión y monitoreo remoto (por ejemplo, mediante SNMP u otro protocolo compatible con las plataformas de la UOCT), incluyendo estado del equipo, disponibilidad y niveles de señal cuando corresponda.
– Junto a la documentación técnica de la sección 6.1, se deberá entregar un inventario de los equipos instalados que incluya, al menos: marca, modelo y número de serie, versión de firmware, direcciones IP, identificación de la SIM (cuando corresponda), ubicación y responsable de la mantención.
– Los equipos deberán permitir sincronización horaria mediante NTP con la fuente de tiempo que indique la UOCT, de manera de asegurar la consistencia de eventos, alarmas y registros."

Recomendación 5: Compatibilidad normativa y electromagnética

Resumen
Se recomienda asegurar el cumplimiento de normativa radioeléctrica y evitar interferencias con sistemas críticos ITS y de peaje.
En qué consiste
- Uso de bandas autorizadas y parámetros permitidos.
- Control de potencia, canalización radioeléctrica y coordinación espectral.
- Verificación de interferencia con sistemas de cobro electrónico automático de peaje.
- Documentación de permisos o autorizaciones SUBTEL cuando corresponda.

Justificación
El espectro radioeléctrico está regulado por la Ley General de Telecomunicaciones. Adicionalmente, la Resolución Exenta N.º 791/2024 establece condiciones técnicas para bandas 2,4 GHz y 5 GHz, incluyendo prioridad de sistemas de cobro electrónico automático de peaje en la banda 5.795–5.815 MHz.
Referencias:
https://www.leychile.cl/navegar?idNorma=29591 ;
https://www.bcn.cl/leychile/navegar?i=1202982 ; https://www.subtel.gob.cl/normas-tecnicas/
Ubicación sugerida en el documento actual
Sección 5.3 Evaluación de Radio Enlace, sección 5.6 Evaluación de otras tecnologías y sección 6.1 Documentación técnica.
Respuesta:
"Se acoge la recomendación. El instructivo ya contempla, en el paso 6, la elección de banda o licencia, la coordinación de espectro y la ausencia de impedimentos normativos como criterios de aceptación, y en la sección 6.1 se solicita documentación emitida por SUBTEL. Sin embargo,

se explicitarán estos requisitos de la siguiente forma:
– En el Informe de Factibilidad Geométrico-Radioeléctrica (paso 5) y en la evaluación de otras tecnologías (paso 9), se deberá indicar la banda de operación, la potencia y la canalización utilizadas, acreditando que se ajustan a la normativa técnica vigente de SUBTEL y que los equipos cuentan con la certificación u homologación correspondiente.
– Cuando el radioenlace se ubique en las cercanías de pórticos de cobro electrónico de peaje (incluidos sistemas de flujo libre), se deberá verificar y documentar la ausencia de interferencia con dichos sistemas, considerando la prioridad que la normativa les otorga en la banda 5.795–5.815 MHz.
– En la sección 6.1 se precisará que el permiso o autorización de SUBTEL se exigirá cuando corresponda según la banda utilizada; para bandas de uso libre se deberá acreditar el cumplimiento de la norma técnica aplicable."