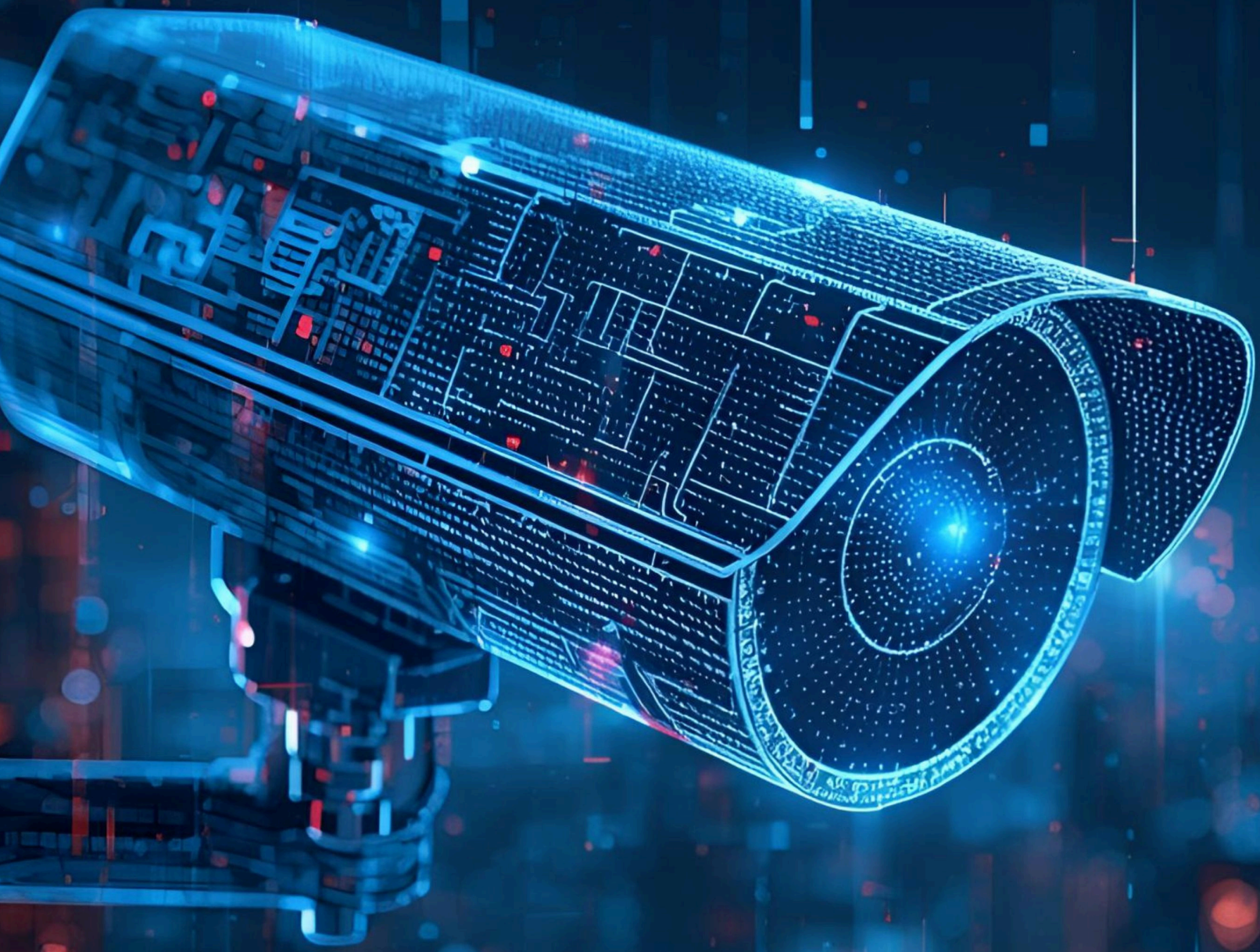
Guía Integral de Sistemas de Teleprotección Inteligente



Teleprotección Inteligente
Transformando la seguridad con tecnología

Proyecto apoyado por: CORFO

Un proyecto de: FUNDACIÓN país digital

ÍNDICE
DE CONTENIDOS

Guía Integral de Sistemas de Teleprotección Inteligente [1]

Introducción

Este documento forma parte de las mesas de trabajo “Teleprotección Inteligente: Transformando la Seguridad con Tecnología”, iniciativa apoyada por CORFO, desarrollada por Fundación País Digital en colaboración con Fundación Paz Ciudadana. **Tiene como propósito entregar orientaciones prácticas y criterios técnicos que permitan fortalecer la calidad, eficiencia e interoperabilidad de los sistemas de teleprotección que se implementan en los territorios.** Su contenido se ha enriquecido gracias al trabajo colaborativo en mesas técnicas con municipios, proveedores, actores del sector público y expertos en seguridad, buscando avanzar hacia un modelo más estandarizado, sostenible e inteligente.

Objetivos clave de los sistemas de teleprotección

Visión directa

Cámara capta alcance completo de vista perimetral

La teleprotección cumple un rol importante en las estrategias de prevención del delito y la violencia. A nivel comparado, es posible identificar evidencia que señala que los sistemas de televigilancia tienen efectos en la delincuencia, donde dicha efectividad en la reducción de delitos se concentraría principalmente en estacionamiento y en ciertos delitos contra la propiedad (por ejemplo, robo de vehículos), aunque sin necesariamente impactar en delitos violentos (Welsch y Farrington, 2008; Piza et al., 2019). Sin embargo, es importante destacar que su efectividad no depende solo de la instalación de dispositivos, sino también de cómo se integran operativamente.

Junto a lo anterior, los sistemas de televigilancia también podrían orientarse a contribuir y solucionar otras problemáticas, por ejemplo: reducir la percepción de temor al delito de la ciudadanía, responder de forma oportuna a emergencias, y entregar evidencia audiovisual útil para investigaciones penales, entre otros.

Estos objetivos sólo pueden alcanzarse plenamente si se articulan de manera efectiva los componentes tecnológicos, humanos y de gobernanza.

1 Este documento ha sido creado bajo una colaboración público-privada y busca ser un material referencial para municipalidades, comunidades vecinales y cualquier organización o empresa. En ningún caso, busca sustituir las “Orientaciones Técnicas de Prevención Situacional, Sistemas de Teleprotección” de la Subsecretaría de Prevención del Delito.

Funciones y ecosistema de las distintas instituciones públicas y privadas

La operación de sistemas de teleprotección inteligente requiere la articulación coordinada de diversos actores públicos, privados y comunitarios. Cada institución cumple funciones específicas que, en conjunto, permiten que estos sistemas sean sostenibles, interoperables y eficaces. A continuación, se describen los principales roles:

Municipalidades: Son responsables de la instalación, operación y mantención de los sistemas de cámaras y monitoreo en su territorio. Definen prioridades locales, administran los centros de monitoreo y articulan las acciones preventivas con otras instituciones.

Carabineros de Chile: Cumple funciones de prevención y respuesta ante delitos. En ciertos casos, puede recibir imágenes en tiempo real o solicitudes de apoyo. La coordinación operativa se canaliza a través de las comisarías y la Central de Comunicaciones (CENCO).

Policía de Investigaciones de Chile (PDI): Cumple funciones investigativas especializadas en delitos complejos. Puede requerir imágenes como evidencia, por lo que se coordinan con unidades como Brigada Investigadora de Robos (BIRO), Brigada de Investigación Criminal (BICRIM) o Cibercrimen, asegurando trazabilidad, integridad de la evidencia y cumplimiento de normativas de protección de datos.

Ministerio Público (Fiscalía): Es la institución encargada de dirigir la investigación penal. Puede solicitar imágenes y registros como evidencia, por lo que se requiere mantener procedimientos de entrega con respaldo documental y trazabilidad.

Ministerio de Seguridad Pública: A través de sistemas como SITIA, iniciativa dependiente de la Subsecretaría de Prevención del Delito, facilita el intercambio de información y la estandarización de plataformas. También contribuye con lineamientos y asesoría técnica.

Gobiernos Regionales y Programas de Seguridad Regional: Financian proyectos de instalación de cámaras, mejoramiento de infraestructura y fortalecimiento de capacidades municipales. En el marco de la Ley N°21.074 y de proyectos que buscan ampliar atribuciones regionales en seguridad, los Gobiernos Regionales podrían asumir un rol más activo en implementar sistemas de monitoreo compartidos y apoyar a municipios con menos recursos y capacidades técnicas.

CSIRT de Gobierno: Es el equipo de Respuesta a Incidentes de Seguridad Informática (CSIRT) que apoya en la prevención, detección y respuesta ante incidentes de ciberseguridad que puedan afectar los sistemas de monitoreo.

Proveedores Tecnológicos: Empresas fabricantes y distribuidoras de cámaras, plataformas de gestión de video y analítica, a través de empresas integradoras, participan en la instalación, soporte técnico y actualización de soluciones.

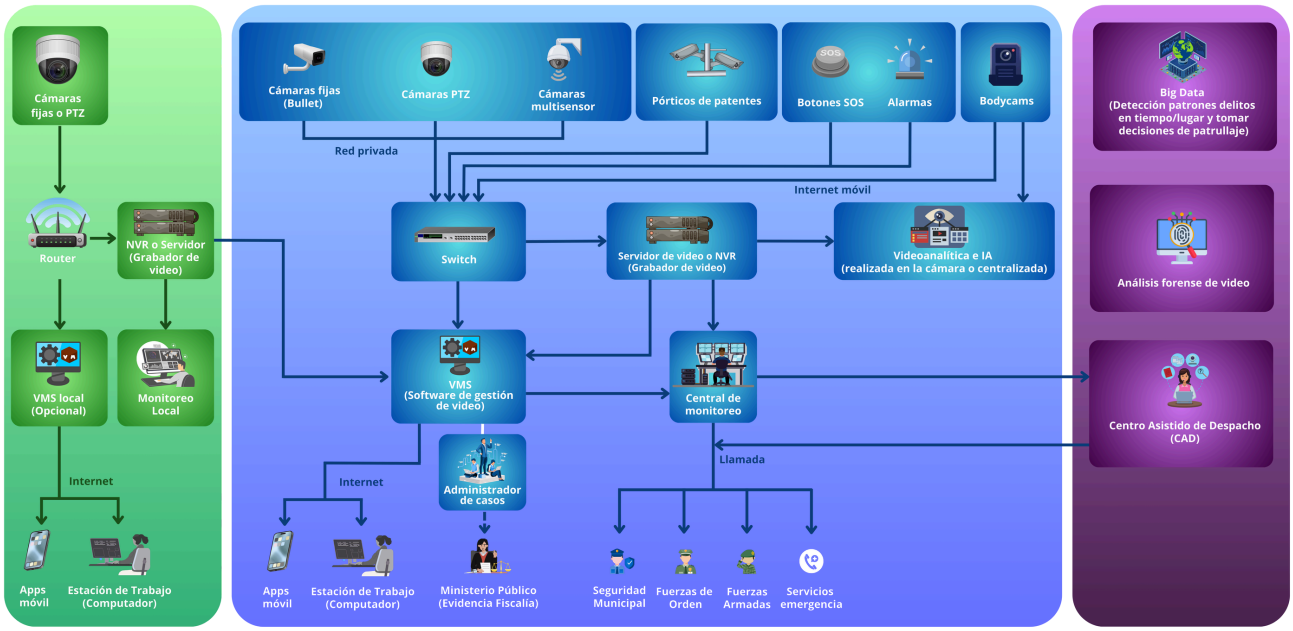
Comunidad y Organizaciones Vecinales: Pueden colaborar en la identificación de puntos críticos, la operación de cámaras comunitarias y la promoción de un uso responsable de la tecnología.

Como síntesis integrada, **el Ministerio de Seguridad Pública lidera los lineamientos, normativas y sistemas nacionales que articulan la teleprotección**. Los Gobiernos Regionales y las Municipalidades gestionan la implementación y operación de las soluciones en sus territorios. Por su parte, Carabineros de Chile y el Ministerio Público cumplen funciones esenciales en la respuesta a emergencias y la investigación penal. Los proveedores tecnológicos aportan capacidades, soporte y actualizaciones de los sistemas. Finalmente, la comunidad y las organizaciones vecinales colaboran en la priorización de zonas críticas, el uso responsable de las tecnologías e, incluso, pueden proveer cámaras privadas que se integren al sistema municipal.

Diagrama de sistemas de teleprotección inteligente

La efectividad de un sistema de teleprotección inteligente no depende únicamente de la instalación de cámaras, sino de su capacidad operativa para ejecutar acciones concretas. Esto incluye el intercambio de información a través de **sistemas interoperables, el uso de inteligencia artificial (IA) para automatizar el monitoreo, y la articulación con nodos regionales que apoyen a comunas con menor capacidad técnica.**

El siguiente diagrama presenta una **visión simplificada de los componentes principales del sistema**, que incluyen: dispositivos periféricos (como cámaras fijas, PTZ [2], multisensor, botones SOS, parlantes y alarmas), equipos de grabación (NVR o servidores), plataformas de gestión de video (VMS), motores de videoanalítica con IA, y canales de interoperabilidad con otros sistemas institucionales. Tiene una división por niveles, iniciando en el nivel comunitario y privado (aprovechando la compartición de cámaras), luego un nivel base de municipios para terminar en un nivel optimizado.



2. Es un tipo de cámara de seguridad o videovigilancia que puede moverse horizontalmente (pan), verticalmente (tilt) y acercarse o alejarse (zoom).

Diseño y formulación de proyectos

El diseño de proyectos de teleprotección debe ir más allá de la simple instalación de cámaras, integrando capacidades institucionales, diagnóstico territorial, criterios técnicos y sostenibilidad operativa. **Esta sección entrega orientaciones prácticas para una formulación estructurada y escalable, aplicable tanto a proyectos municipales como comunitarios.**

1. Capacidades institucionales

Es fundamental contar con una entidad técnica —pública o privada— con capacidad de diseño, coordinación y supervisión del sistema. Esta unidad debe tener competencias en planificación, compras públicas, gestión técnica, interoperabilidad y análisis de datos. En aquellos casos donde el modelo operativo contemple la participación de organizaciones comunitarias o vecinos coordinadores, se recomienda establecer protocolos claros de colaboración, incluyendo canales de comunicación, criterios de interoperabilidad y mecanismos de apoyo técnico. La ausencia de estas capacidades suele explicar fallas en operación o sostenibilidad de los sistemas.

2. Diagnóstico situacional del territorio

Todo proyecto debe partir de un análisis riguroso del entorno, el cual idealmente debe incluir mapas de calor u otras representaciones visuales para identificar patrones delictuales y justificar técnicamente la ubicación de cámaras:

- Identificación de zonas vulnerables o de concentración delictual.
- Condiciones urbanas y cobertura de servicios (electricidad, conectividad).
- Capacidades operativas del municipio: centros de monitoreo, personal disponible, turnos, coordinación con CENCO de Carabineros, PDI y Fiscalía.
- Percepción de seguridad y cohesión social.
- Iniciativas comunitarias o programas previos de prevención.

Este diagnóstico permite orientar la lógica territorial de intervención, apoyando tanto la eficacia operativa como la apropiación comunitaria del sistema. Dado que la delincuencia presenta una alta movilidad y capacidad de adaptación, es clave mantener un análisis continuo del entorno, idealmente complementado con sistemas de analítica preventiva que permitan anticipar patrones delictivos y ajustar el despliegue tecnológico de forma dinámica.
Asimismo, puede ser útil aplicar modelos de clusterización entre municipios, agrupándolos por nivel de desarrollo en seguridad y disponibilidad de recursos. Este enfoque permite homologar criterios y diseñar sistemas ajustados a las capacidades reales de cada comuna, facilitando decisiones de escalabilidad, inversión y apoyo técnico.

3. Diseño tecnológico y escalabilidad

El sistema debe ser modular, permitiendo su expansión sin costos excesivos. Se sugiere:

- Infraestructura preparada para futuras cámaras o sensores.
- Energías alternativas (solar o eólica) en zonas sin factibilidad eléctrica.
- Compatibilidad con sistemas comunitarios o privados.
- VMS interoperables para gestión centralizada.
- Integración de cámaras privadas mediante modelos colaborativos. En algunas comunas existen programas que cofinancian cámaras vecinales para ampliar la cobertura pública.

Al final de esta sección se presentan los componentes clave del sistema, y en capítulos posteriores se detallan las especificaciones técnicas mínimas.

4. Planimetría y especificaciones técnicas

Se debe presentar un plano legible con:

- Georreferenciación (norte, calles, zonas).
- Simbología clara para elementos existentes y propuestos.
- Justificación de ubicación según criterios de seguridad y cobertura.

Las especificaciones deben incluir partidas detalladas, numeradas y asociadas al plano, facilitando comparaciones entre proveedores y reduciendo riesgos de retrasos o rechazos. La ubicación de los puntos de cámara debe considerar los criterios de selección de puntos vulnerables, críticos de delitos o concentraciones delictuales equivalentes en sectores residenciales, para ser consistentes con el diagnóstico situacional, además de que contemple la cobertura completa del sector a intervenir, sin dejar puntos ciegos.

5. Presupuesto detallado

El presupuesto debe:

- Incluir todas las partidas relevantes con cantidades específicas.
- Evitar partidas globales sin desagregación técnica.
- Considerar expresamente permisos eléctricos, municipales u otros necesarios, dado que su tramitación y factibilidad técnica pueden generar retrasos significativos en la planificación del proyecto.
- Incluir los costos de instalación, conectividad, postes, licencias, capacitación y mantenimiento, tanto preventivo como correctivo, ya que este componente es clave para garantizar la continuidad y operatividad del sistema.

La omisión de información completa y debidamente desagregada puede generar retrasos o la no aprobación/adjudicación de la iniciativa.

6. Instalación física y permisos

La instalación debe seguir estándares mínimos:

- Altura de cámaras: desde 2,5 metros en estructuras existentes (postes, edificios).
- Postes nuevos: considerar postes de 9 a 18 metros con brazos de hasta 2,5 m, según cobertura requerida.
- Equipamiento complementario: luminarias, megáfonos o alarmas, según necesidad.
- Gestión de permisos y coordinación con empresas eléctricas o juntas vecinales.
- Evaluar la factibilidad eléctrica en cada punto de cámara solicitado, considerando disponibilidad de energía, carga requerida y condiciones técnicas de conexión.

7. Software y actualización

Se debe prever la actualización de software:

- Preferencia por licencias perpetuas y sistemas interoperables.
- Evaluar la opción de “take-over”, permitiendo que otro proveedor asuma los costos de cambio.
- Monitorear actualizaciones de firmware y compatibilidad con analítica avanzada.

8. Capacitación y gestión comunitaria

Es esencial capacitar a los operadores y responsables vecinales:

- Entregar material de apoyo y protocolos operativos.
- Fomentar la participación comunitaria como corresponsables del sistema.
- Incluir capacitación en ciberseguridad básica y protección de datos.

Junto con esto, la participación comunitaria es un eje fundamental para la legitimidad y sostenibilidad del sistema, involucrando a vecinos en la priorización de zonas, instalación y uso responsable de los sistemas e incluso promoviendo acuerdos colaborativos, como el aporte de electricidad o espacios físicos para la instalación de cámaras.

9. Evaluación continua y sostenibilidad

- Definir indicadores de éxito (delitos prevenidos, tiempos de respuesta, percepción ciudadana).
- Establecer rutinas de monitoreo, auditoría y actualización tecnológica.
- Incorporar mecanismos de revisión participativa para ajustar el proyecto en el tiempo.

10. Componentes del sistema de teleprotección

Cada proyecto debe considerar los siguientes ejes para asegurar un diseño integral:

a) Hardware y despliegue físico:

- Elección de cámaras (fijas, PTZ, multisensor, térmicas) y que la precisión considere un estándar unificado como DORI (Detección, Observación, Reconocimiento, Identificación).
- Infraestructura recomendada: postes de 9 a 18 metros, brazos de hasta 2,5 metros, galvanizado estructural o soluciones mixtas comunitarias.
- Incorporación de dispositivos adicionales: sensores, parlantes, botones SOS, pórticos lectores de patente y bodycams, si corresponde.

b) Plataforma de gestión y analítica:

- Sistemas de gestión de video (VMS) interoperables, con licencias perpetuas y operación continua (24/7).
- Integración de videoanalítica para eventos como: aglomeraciones, robos, intrusiones, zonas prohibidas y detección de comportamiento anómalo.
- Evaluar si el análisis se realiza en el borde (edge) o de forma centralizada en servidores, según capacidad técnica y escalabilidad del sistema.

c) Conectividad y transmisión:

- Uso de fibra óptica como estándar para puntos fijos.
- Enlaces inalámbricos (PTP/PTMP) o redes móviles (4G/5G) para ubicaciones sin cableado o dispositivos móviles.
- Evaluar conexión satelital en zonas rurales donde no existan otras alternativas.
- Se debe considerar la cantidad de puntos unidos por un mismo enlace, ya que pérdidas de transmisión pueden afectar la operación y visualización del sistema. Se recomienda organizar los puntos en pequeños grupos para minimizar este impacto.

d) Ciberseguridad y protección de datos:

- Cifrado en tránsito y en reposo, autenticación robusta, control de accesos y trazabilidad.
- Adecuación progresiva a la Ley 21.719 sobre protección de datos personales.
- Registro de accesos, mecanismos de difuminación y firma digital para integridad de evidencia audiovisual.

e) Continuidad operacional:

- Sistemas de respaldo energético como UPS, baterías, paneles solares y generadores eléctricos, con su respectiva mantención en puntos críticos.
- Planes de continuidad operacional con responsables asignados, procedimientos de respaldo y protocolos de recuperación frente a contingencias.
- Respaldo seguro de información mediante almacenamiento redundante y políticas de retención con trazabilidad.

Esta arquitectura técnica permite construir sistemas escalables, interoperables y sostenibles que se adapten a la realidad operativa de cada comuna.

Hardware y elementos físicos [3]

La realidad de **cada comuna y de las organizaciones comunitarias puede variar significativamente en capacidades técnicas, recursos y contexto urbano.** Esta clasificación de distintos tipos de cámaras y componentes físicos propone orientaciones generales para facilitar la toma de decisiones, estandarizar criterios mínimos y promover sistemas eficientes, seguros y escalables en los distintos territorios.

Uso de brazos

Cámara capta imágenes de la línea divisoria del inmueble

La elección de tecnologías debe considerar atributos como resolución, tipo de lente, iluminación y distancia de cobertura, en función de las condiciones locales. Para orientar esta decisión, se recomienda utilizar la norma internacional IEC EN 62676-4, que facilita la especificación de cámaras según el nivel de detalle requerido.

Esta norma se basa en el modelo DORI, que define cuatro niveles de desempeño según la precisión visual esperada. Cada nivel se relaciona con una densidad mínima de píxeles necesaria para lograr ese grado de precisión, expresada en píxeles por rostro o por metro:

D Detección

Confirma la presencia de una persona o vehículo (4 px/rostro o 25 px/m).

O Observación

Permite apreciar detalles generales como vestimenta o comportamiento (10 px/rostro o 63 px/m).

R Reconocimiento

Identifica si una persona u objeto es el mismo que se ha visto antes (20 px/rostro o 125 px/m).

I Identificación

Entrega nitidez suficiente para una identificación sin ambigüedades (40 px/rostro o 250 px/m).

3 Estas especificaciones fueron elaboradas de acuerdo al proceso de co-construcción entre los participantes de las mesas de trabajo y 3 ejemplos de especificaciones técnicas de términos de referencia de las municipalidades de Hualpén, La Granja y San Felipe, junto con características del Programa Barrio Protegido de la municipalidad de Las Condes.

Sin perjuicio de lo anterior, a continuación se describen las características mínimas recomendadas de tipo de cámaras, iniciando en el nivel comunitario, seguido por un nivel base municipal, y culminando en un nivel optimizado, permitiendo una planificación escalonada y adaptativa del sistema de teleprotección.

Componente Técnico	Nivel Comunitario	Nivel Municipal	Nivel Optimizado	Certificaciones
Cámaras Fijas	Bullet - 4 MP	Bullet VF - 4 MP Full HD (Varifocal)	Bullet VF - 4 MP Full HD (Varifocal)	Certificaciones Base Nivel 2 y 3 IK10, IP66, NEMA 4x
Cámaras PTZ	Mini PT Sin Zoom	PTZ 4 MP - Zoom desde 30x	PTZ 4 MP - Zoom desde 30x	Certificaciones Base Nivel 2 y 3 IK10, IP66, NEMA 4x
Cámaras Multisensor (más lentes)	N/A	Resoluciones 4 MP por lente 90° + PTZ 180° + PTZ 270 ° + PTZ 360 ° + PTZ	Resoluciones 4 MP por lente 90° + PTZ 180° + PTZ 270 ° + PTZ 360 ° + PTZ	Certificaciones Base Nivel 2 y 3 IK10, IP66, NEMA 4x
Cámaras lectoras de placas patentes	N/A	Atributos de vehículo, Color, dirección, Velocidad, Tipo vehículo Velocidad de Captura desde 200 km/h	Atributos de vehículo, Color, dirección, Velocidad, Tipo vehículo Velocidad Captura desde 200 km/h	Certificaciones Base Nivel 2 y 3 IK10, IP66, NEMA 4x
Parlantes	N/A - Incorporado en Cámaras Fijas	IP - >10 w	IP - >10 w	Protocolo SIP u ONVIF

Botones SOS	N/A	SOS Antivandálicos	SOS Antivandálicos	Protocolo SIP u ONVIF
Alarmas	N/A	Centrales Wireless o Cableadas	Centrales Wireless o Cableadas	Protocolos tradicionales como CID o SIA
Bodycams	N/A	2 MP - 4G Compatibles con VMS existente	2 MP - 4G Compatibles con VMS existente	Comunicación por ONVIF o RTSP o RTMP
UAV (drones)	N/A	Compatibles con VMS existente	Compatibles con VMS existente	Comunicación por RTSP o Mavlink
Almacena-miento[4]	Se recomienda NVR para uso básico	Se pueden usar NVR o servidores más avanzados.	Considerar la escalabilidad del sistema (x aumento cámaras)	A nivel municipal, considerar redundancia de alimentación y RAID como mínimo
Tipo de conectividad requerida	30 días Wireless o Cableado (Internet Convencional / P2P)	30 días Wireless o Cableado (Internet Convencional / P2P)	30 días Wireless o Cableado (Internet Convencional / P2P)	
Condiciones de almacena-miento	Mínimo 30 días	Mínimo 30 días con acceso controlado por Municipio o Redundancia	Mínimo 30 días con acceso controlado por Municipio o Redundancia	

4 Si bien no es un estándar, los fabricantes de cámaras indicaron que generalmente existe un servidor de grabación para 150 a 300 cámaras de seguridad.

Este enfoque es generalista así que incluir otros atributos de cámaras, debe ser revisado según las características geográficas de cada comuna. Por ejemplo, en comunas rurales con riesgo de incendios forestales, podría ser clave la incorporación de cámaras térmicas para detección temprana. En comunas costeras, es aconsejable considerar equipamiento con protección anticorrosiva frente a ambientes con alta salinidad.

Software y plataformas de gestión

Los sistemas de teleprotección requieren plataformas que permitan administrar cámaras, coordinar recursos, analizar eventos, generar evidencia y entregar respuestas oportunas ante incidentes. Estas soluciones deben ser interoperables, seguras, escalables y ajustadas a las capacidades de cada municipios, comunidades y actores privados.

En las mesas técnicas se ha identificado una advertencia relevante: es frecuente que en procesos de compra se presenten softwares que aparentan funcionalidades mediante simulaciones o planillas Excel, sin contar realmente con la capacidad de operar bajo condiciones reales. Por ello, se recomienda solicitar pruebas funcionales y operativas verificables, que permitan evaluar si el sistema efectivamente resuelve los desafíos de monitoreo, coordinación y análisis que enfrentan los territorios. Además, incorporar criterios de interoperabilidad, escalabilidad y ciberseguridad en las bases técnicas de adquisición, que se describirán en siguientes secciones de esta guía.

1. VMS (Video Management System)

El VMS es el sistema que permite administrar las cámaras, visualizar en tiempo real, almacenar grabaciones y gestionar alertas. De acuerdo a la revisión con los proveedores VMS de esta mesa, se sugiere que cuente con los siguientes elementos:

- Gestión de cámaras, botones de pánico, bocinas y lectores Placa Patente Única (PPU).
- Compatible con cualquier fabricante de hardware y software.
- Protocolos de comunicación universales.
- Escalable y distribuido.
- Integración con drones y control de acceso.
- Soporte para videoanalítica de terceros.
- Envío de video a terceros.
- Mapas inteligentes integrados.
- Gestor de alarmas incorporado.
- Visualización desde dispositivos móviles.
- Conectividad e interoperabilidad.
- Integración con sistema criminológico e iluminación.

2. CAD (Centro Asistido de Despacho)

El CAD cumple un rol central en la gestión operativa de la seguridad municipal, ya que permite ordenar, coordinar y registrar la respuesta ante distintos tipos de incidentes. Su valor no está solo en recibir alertas, sino en conectar información, recursos disponibles y decisiones operativas en tiempo real. En contextos comunales, permite fortalecer la coordinación entre equipos municipales, fuerzas de orden y otros servicios de apoyo. Por ello, su diseño debe responder a la realidad territorial, institucional y operativa de cada municipio.

- Recibir llamadas, registrar incidentes y priorizarlos geográficamente.
- Despachar móviles en función de disponibilidad, urgencia, tipo de evento y cercanía vía GPS.
- Integrar cámaras de vigilancia, botones SOS, cámaras corporales, alarmas y radios.
- Coordinar acciones en tiempo real con Carabineros, PDI, ambulancias u otros servicios.
- Registrar todos los pasos del procedimiento, generar informes automáticos y asegurar trazabilidad del caso.
- Incorporar evidencia audiovisual útil para Fiscalía y PDI.
- Apoyar la gestión posterior: medidas cautelares, rondas preventivas, seguimiento de casos.
- Generar indicadores clave mediante dashboards y análisis de datos.

Un CAD bien configurado debería adaptarse a la realidad operativa local, con interfaces intuitivas e incluyendo reglas o códigos propios de las fuerzas de orden y gobierno local. Además, debe permitir una operación flexible, escalable e interoperable con distintas tecnologías presentes en el territorio comunal. No es solo una plataforma tecnológica, sino una herramienta estratégica y logística para fortalecer la coordinación, trazabilidad y capacidad de respuesta de la seguridad municipal.

3. Plataformas de videoanalítica e inteligencia artificial

Estas plataformas procesan imágenes para automatizar el análisis de eventos, ya sea en tiempo real o en forma forense. Algunas funcionalidades comunes incluyen:

- Reconocimiento de matrículas (ANPR o LPR) y reconocimiento facial.
- Detección de aglomeraciones, cruce de líneas, objetos abandonados, detenciones prolongadas y cambios de velocidad.
- Definición de zonas de intrusión, análisis de color y conteo de personas o vehículos.
- Generación de alertas configurables y clasificación automática de eventos.

Si bien aquí se presentan algunas funciones, los avances en esta área han llevado a incluir una sección específica en esta guía dedicada exclusivamente al uso de inteligencia artificial en teleprotección.

4. Sistemas big data y análisis forense

Existen sistemas orientados a la revisión posterior de los datos, que permiten:

- Reconstruir eventos mediante revisión de cámaras, audios y registros asociados.
- Correlacionar variables como tiempo, ubicación, placas, personas y reincidencias.
- Generar reportes de tendencias delictuales o recurrencia de eventos.
- Apoyar decisiones estratégicas para patrullajes, focalización de recursos y rediseño territorial de dispositivos.

Este tipo de análisis permite a los municipios tomar decisiones basadas en evidencia, más allá de la operación diaria.

5. Aplicaciones móviles

Se deben incluir porque permiten a funcionarios o actores autorizados acceder al sistema desde terreno. Entre sus funciones están:

- Visualización de cámaras en tiempo real y emisión de alertas georreferenciadas.
- Activación de alarmas y botones SOS.
- Registro de incidentes con imágenes, videos y ubicación.
- Acceso diferenciado según perfil del usuario (inspector, operador, vecino, entre otros).

Estas aplicaciones amplían la cobertura operativa y facilitan la reacción desde múltiples puntos.

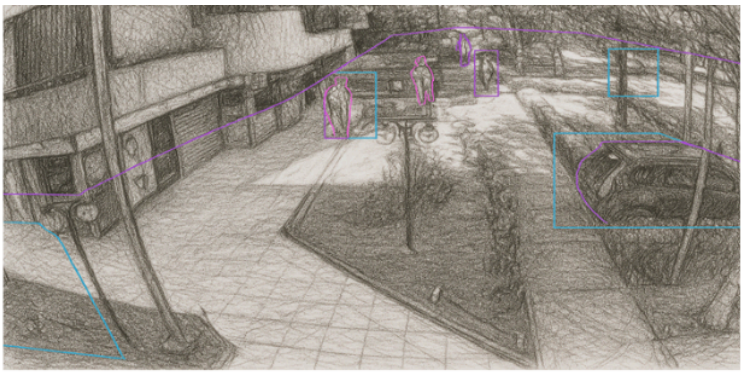
6. Sistemas complementarios

Existen herramientas adicionales que pueden fortalecer la operación del sistema, tales como:

- Sistemas de información geográfica (GIS), para mapear cámaras, zonas críticas y rutas de patrullaje.
- Módulos legales o de gestión de evidencia, que permiten preparar carpetas para entrega a Fiscalía o PDI.
- Paneles de indicadores o sistemas de business intelligence (BI), para evaluar desempeño, carga de operadores o tiempos de respuesta.
- Módulos ciudadanos, que permiten reportar incidentes o activar alarmas desde la comunidad.

En muchos casos, estos sistemas complementarios ya se encuentran integrados como módulos dentro de los propios VMS o CAD, por lo que se sugiere evaluar su funcionalidad antes de optar por soluciones adicionales.

Videoanalítica e inteligencia artificial



Videoanalitica e IA permite mejorar la solución de eventos con distintas analíticas pre-configuradas según el municipio

El Estado y los gobiernos locales tienen la función de velar por la seguridad de sus ciudadanos. Para ello, utilizan tecnologías de videoanalítica e inteligencia artificial que permiten identificar eventos [5] relevantes o situaciones de riesgo, como asaltos, incivilidades u otras emergencias. Para ello, las municipalidades y comunidades deben revisar sus principales problemáticas locales y definir una configuración específica de analíticas, considerando sus prioridades y el entorno urbano.

Los tipos de analítica que se pueden configurar para la gestión de eventos son algunas como las siguientes: vehículo detenido; aglomeración de personas; cruce de muro; cruce de línea; conteo de personas, vehículos y bicicletas; zonas de intrusión o zonas prohibidas; lector de placa patente con análisis forense (cámaras que cubran total o parcialmente las calzadas); identificación de objetos y colores; cambio de velocidad de personas y vehículos; posible robo a vehículo motorizado; detención prolongada de personas, vehículos motorizados y objetos; movimiento de levantamiento de portones. Un ejemplo de lo anterior, podría ser el evento **"robo a vehículo estacionado"**. Una persona permanece cerca de un auto, observa el entorno y sustrae objetos. Para detectarlo se configuran analíticas como detención prolongada, cambio de velocidad, zona de intrusión, reconocimiento de matrícula (ANPR o LPR) e identificación de objetos y colores, facilitando alertas y búsqueda posterior.

Existen también eventos clasificados como "anomalías" - por ejemplo, portonazos o ciertos patrones de comportamiento delictual inusuales - que hoy no pueden identificarse de manera completamente precisa, por lo que su uso debe evaluarse en un proceso continuo de mejora.

A pesar de las limitaciones, la experiencia muestra que estas tecnologías incrementan significativamente la eficiencia operativa: **mediante analítica avanzada un operador puede supervisar hasta 300 cámaras en simultáneo, en comparación con las aproximadamente 40 que se monitorean sin analítica avanzada.**

5 Las municipalidades también usan sinónimos de eventos como alertas o emergencias.

A continuación, se ejemplifican algunas analíticas según el tipo de dispositivo, lo que significa que ya es posible hacer este tipo de configuraciones en los dispositivos:

Tipo de dispositivo	Reconocimiento de matrículas (ANPR o LPR)	Reconocimiento Facial	Atributos[6]	Armas	Cruce de muro
Cámaras Fijas	✓	✓	✓	✓	✓
Cámaras PTZ	✓	✓	✓	✓	✓
Cámaras Multisensor (más lentes)	✓	✓	✓	✓	✓
Pórtico de patentes	✓	✓	✓	✓	✓
Parlantes	✗	✗	✗	✗	
Botones SOS	✗	✓	✗	✗	
Alarmas	✗	✗	✗	✗	
Bodycams	✓	✓			

6 Considera atributos personas (lentes, gorro, enmascarado) y automóviles (marca, modelo, color)

Finalmente, es importante considerar que el procesamiento de inteligencia artificial puede realizarse de dos formas:

- En el borde, directamente en la cámara, donde la capacidad de cómputo es limitada y generalmente admite solo 1 o 2 analíticos simultáneos.
- De manera centralizada, en servidores, NVR o el sistema de gestión de video (VMS), lo que permite mayor escalabilidad y procesamiento más complejo.

La selección del enfoque dependerá de la capacidad técnica, los recursos disponibles y las necesidades específicas de cada municipio.

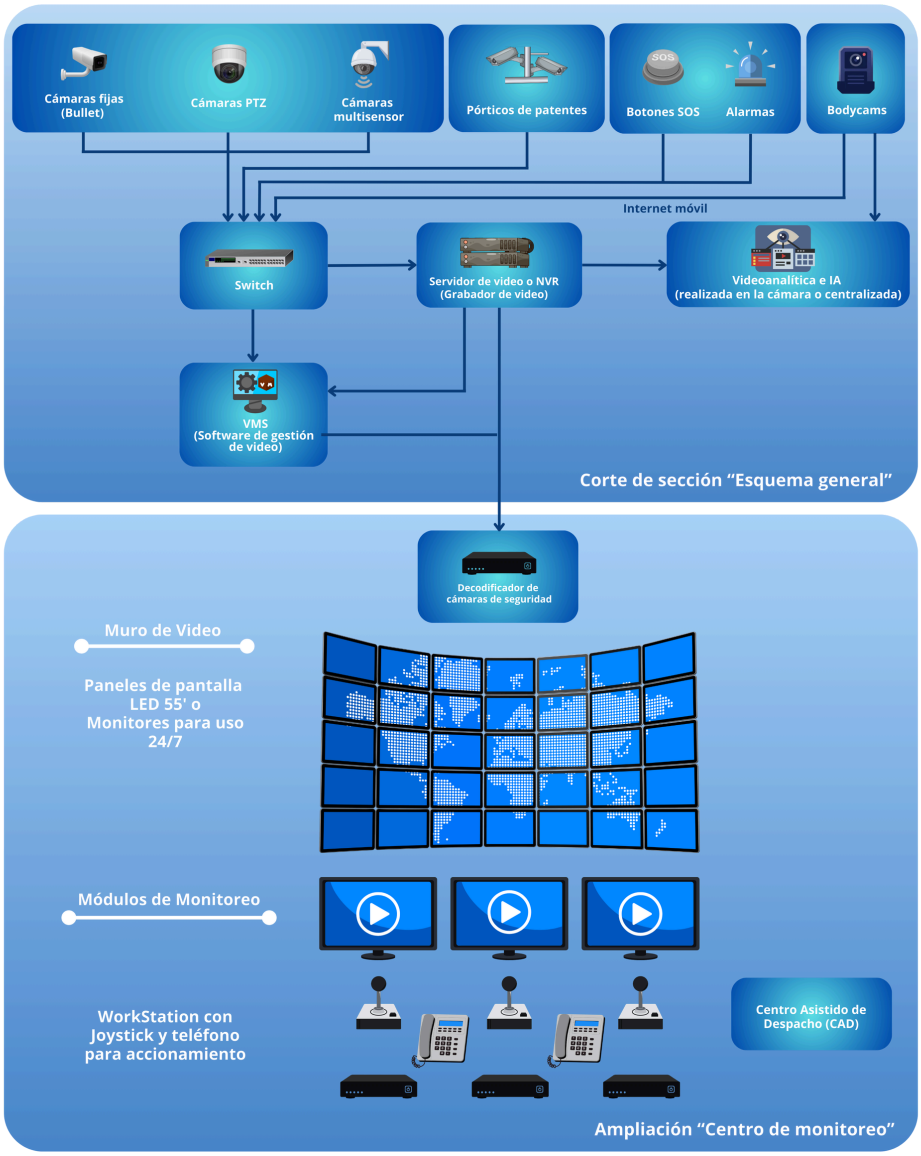
Centros de monitoreo y coordinación operativa

La eficacia de los sistemas de teleprotección depende directamente de la capacidad operativa del centro de monitoreo. **No basta con visualizar imágenes: es fundamental contar con operadores capacitados, conectividad directa con móviles municipales y protocolos claros para la coordinación de respuestas en tiempo real.**

Centro de Monitoreo de Municipalidad del sector sur RM

Se recomienda establecer turnos 24/7, mantener una proporción adecuada entre operadores y cámaras, y asegurar que personal cuente con atribuciones fiscalizadoras, cuando corresponda.

Desde la perspectiva tecnológica, como se ilustra en el esquema general, los distintos tipos de cámaras de vigilancia se conectan a grabadores y software de gestión de video —puede haber varios si existen múltiples plataformas—, los cuales son visualizados en una central que decodifica las imágenes en un muro de pantallas, permitiendo a los operadores gestionar eventos mediante teléfono, radio o directamente en el software Centro Asistido de Despacho (CAD). La infraestructura, especialmente los monitores, debe garantizar una operación continua 24/7.



La integración operativa es tan importante como la tecnológica. Es necesario distinguir las funciones entre las comisarías de Carabineros y la Central de Comunicaciones (CENCO). Aunque algunos municipios han asignado carabineros a sus centros de monitoreo, esta práctica ha demostrado ser poco efectiva. CENCO es la unidad encargada de asignar recursos para emergencias y coordinar el despliegue policial, pero paradójicamente tiene acceso limitado a las centrales municipales, lo que dificulta la eficiencia en la respuesta.

Por ello, se sugiere establecer canales formales de coordinación entre las municipalidades y CENCO, con el fin de articular una respuesta conjunta ante eventos de seguridad y emergencias.

En comunas con menor capacidad operativa, como se mencionó en la sección anterior, en el futuro los gobiernos regionales podrían prestar apoyo a través de centros de monitoreo integrados regionales que respalden a comunas con menor capacidad técnica.

Gestión y custodia de evidencia

Esta sección entrega orientaciones prácticas para asegurar que la evidencia audiovisual generada por sistemas de teleprotección sea útil y válida en investigaciones penales.

- **Plazo de entrega:** Una vez ocurrido y reportado un delito, se dispone de un máximo de 24 horas para remitir los registros a la Fiscalía.
- **Herramientas de gestión:** Se recomienda utilizar un módulo de administración de casos, integrado en el sistema de gestión de video (VMS) o en el sistema de despacho asistido por computadora (CAD). Estas plataformas permiten documentar cada registro, asegurar la trazabilidad y mantener la integridad técnica de la evidencia.
- **Procedimientos de primeras diligencias:** La Policía de Investigaciones (PDI) aplica protocolos establecidos en su Manual de Primeras Diligencias, que incluyen la identificación temprana de víctimas, testigos y responsables, además del aseguramiento inmediato de la evidencia material y audiovisual.
- **Condiciones mínimas de validez:** La mayoría de los fabricantes incorporan mecanismos como marcas de agua o huellas digitales para garantizar que la evidencia audiovisual no ha sido alterada. Para que sea eficiente y admisible, la evidencia debe resguardarse con sincronización horaria, metadatos asociados (fecha, hora, ubicación y responsable de descarga), y protocolos de custodia y respaldo documental.

Interoperabilidad

Para que los sistemas de teleprotección sean sostenibles y útiles a largo plazo, es fundamental que los equipos y plataformas sean interoperables, es decir, capaces de integrarse con otros sistemas y compartir información de manera segura y efectiva.

Por ello, se debe garantizar que los sistemas cumplan con los siguientes requisitos técnicos:

- Compatibilidad con estándares abiertos[7], como el protocolo ONVIF (Open Network Video Interface Forum) en sus distintos perfiles S, T, G y M[8], para asegurar que cámaras, grabadores, software de gestión y herramientas analíticas puedan operar entre sí, sin depender de un único proveedor.

7 En esta sección se menciona como ejemplo el protocolo ONVIF y en la sección Hardware se mencionan otros protocolos de comunicación específicos por tipo de cámara.
8 Información de los perfiles en https://www.onvif.org/profiles/

- APIs y/o SDK abiertas[9] y documentadas, que faciliten la conexión con plataformas municipales, regionales o institucionales, como el sistema SITIA[10] del Ministerio de Seguridad Pública o sistemas de Fiscalía, PDI o Carabineros de Chile.
- Exportación de evidencia con trazabilidad, incluyendo metadatos relevantes (fecha, hora, ubicación, ID de cámara y responsable de descarga), en formatos compatibles con procesos judiciales.
- Sincronización horaria (NTP - Network Time Protocol) y codificación estándar de video para comprimir archivos de video (ej. H.264/H.265) para facilitar la interoperabilidad entre dispositivos y plataformas.
- Priorizar plataformas que faciliten la interoperabilidad y promuevan esquemas abiertos que permitan flexibilidad y autonomía tecnológica.

Dado que muchas municipalidades no cuentan con capacidades técnicas especializadas, se recomienda recurrir a instituciones como el propio Ministerio de Seguridad Pública (vía SITIA), el CSIRT[11] de Gobierno, o centros de investigación académica, para recibir apoyo técnico, evaluaciones de compatibilidad o buenas prácticas de integración.

Ciberseguridad

La seguridad de los sistemas de teleprotección es un componente crítico que debe abordarse desde el diseño e instalación. Todos los equipos y plataformas —incluidas cámaras comunitarias, redes y software de gestión— deben contemplar principios mínimos de ciberseguridad para prevenir accesos no autorizados, manipulación de datos y vulnerabilidades operativas.

Para ello, se debe considerar lo siguiente dentro de la propuesta técnica y posterior capacitación:

- Autenticación y control de accesos: Configuración de usuarios con distintos niveles de privilegio, autenticación robusta y contraseñas seguras.
- Cifrado en todo el sistema: Los datos deben ir cifrados desde las cámaras, borde y transmisión hasta el almacenamiento, usando AES y protocolos seguros como TLS o HTTPS.

9 API abierta se considera como una interfaz de programación de aplicaciones que está disponible para que cualquier desarrollador pueda acceder y utilizarla. Deben seguir buenas prácticas de seguridad como las del OWASP API Security Top 10 (2023): https://owasp.org/API-Security/editions/2023/en/0x11-t10/

10 SITIA (https://www.sitia.gob.cl/) es una iniciativa que busca integrar el potencial de la Inteligencia Artificial (IA) y de las nuevas tecnologías emergentes para la prevención del delito y la seguridad de las personas y de los territorios.

11 CSIRT (https://csirt.gob.cl/) es una unidad dentro de la Agencia Nacional de Ciberseguridad que da respuesta a los incidentes de ciberseguridad del país.

- Cifrado de datos en tránsito y reposo: Usar tecnologías de cifrado robustas y estándares reconocidos para proteger la integridad y confidencialidad del video en redes y dispositivos de almacenamiento.
- Registros y trazabilidad: Mantener registros de acceso y actividad, auditables y protegidos contra modificaciones.
- Política de gobernanza de datos: Incluir orientaciones básicas sobre cómo administrar la información grabada, su retención, privacidad y uso legal.
- Protocolos de respuesta ante incidentes: Proveer una guía inicial de actuación frente a filtraciones o mal uso del sistema.
- Actualización segura de sistemas: Compromiso del proveedor con la entrega de parches y actualizaciones de firmware o software críticos.

Dado que muchos municipios y organizaciones comunitarias no cuentan con capacidades técnicas propias, se recomienda solicitar al adjudicatario la inclusión de un módulo de formación en ciberseguridad básica y, cuando sea posible, vincularse con instituciones especializadas como el CSIRT de Gobierno, la Alianza Chilena de Ciberseguridad, o programas universitarios que entreguen apoyo técnico o guías de buenas prácticas.

Por último, como parte de las capacitaciones, se deben incluir prácticas básicas de ciberhigiene, como el uso de gestores de contraseñas seguras y actualización periódica de contraseñas, identificación de correos o enlaces sospechosos, y la prohibición de instalar software no autorizado. También se debe instruir al personal para reportar comportamientos inusuales y evitar el uso de redes públicas en dispositivos conectados al sistema.

Seguridad de información y protección de datos

Los sistemas de teleprotección tratan datos personales y deben adecuarse a la Ley N°21.719, cuya entrada en vigencia será en diciembre de 2026. Según esta normativa, los datos personales pertenecen a las personas naturales, mientras que municipios y operadores privados, en su calidad de responsables del tratamiento, deben velar por su custodia. Están obligados a garantizar la confidencialidad, seguridad y respeto de los derechos de los titulares, conforme a los principios de licitud, minimización y responsabilidad. Se recomienda iniciar desde ya la adopción progresiva de buenas prácticas, como informar a la ciudadanía sobre la finalidad del monitoreo, el responsable y los canales para ejercer sus derechos. Los datos deberán almacenarse únicamente durante el tiempo estrictamente necesario y, posteriormente, ser eliminados o anonimizados.

12 Con el fin de mitigar posibles vulnerabilidades de seguridad, se sugiere renovar la contraseña cada 90 días.

Se sugiere, cuando sea posible, configurar funciones de difuminación automática de rostros o matrículas, como medida preventiva para reducir riesgos y dar cumplimiento al principio de minimización.
En el caso del reconocimiento facial, que opera mediante algoritmos vectoriales para anonimizar imágenes, se debe garantizar una desanonimización controlada y trazable, aplicable solo en situaciones autorizadas. Además, se recomienda implementar mecanismos de firma digital o huellas criptográficas sobre los archivos originales, a fin de asegurar su integridad y evitar la manipulación de evidencia audiovisual.

Se deben garantizar los derechos de los titulares, conocidos como derechos ARCO (acceso, rectificación, cancelación y oposición), mediante procedimientos formales, accesibles y trazables. La Ley N°21.719 amplía estos derechos a figuras como la portabilidad, el bloqueo y la limitación del tratamiento, según el contexto. Toda cesión de imágenes a Carabineros, PDI, Fiscalía u otros organismos debe estar debidamente justificada, documentada y registrada en la bitácora del sistema.

Es fundamental contar con una política de privacidad, un inventario actualizado de actividades de tratamiento y señalética visible en los espacios vigilados. El personal autorizado debe firmar acuerdos de confidencialidad y recibir capacitación periódica. La protección de datos complementa las medidas de ciberseguridad, incorporando deberes de transparencia activa y respeto de los derechos fundamentales de las personas.

Conectividad de los sistemas y transmisión de video

La transmisión de video y datos en sistemas de teleprotección puede realizarse mediante distintas tecnologías según la disponibilidad de infraestructura, el tipo de equipamiento y los requisitos de operación. **La fibra óptica es la opción más estable y de alta capacidad, recomendada para la mayoría de las cámaras fijas, PTZ, multisensor, pórticos de patente, parlantes y botones SOS.** Los enlaces inalámbricos PTP o PTMP permiten conectar equipos en zonas sin red cableada, mientras que el internet móvil 4G o 5G es especialmente útil para cámaras a bordo, Bodycams y algunos dispositivos en entornos dinámicos. Por su parte, el internet satelital puede utilizarse en áreas rurales donde no existe otra conectividad, principalmente para pórticos de patente y Bodycams con transmisión diferida.

A continuación, se presenta una tabla que muestra la compatibilidad de cada tecnología con los distintos equipos de monitoreo.

Tipo de equipamiento	Fibra óptica	Enlaces inalámbricos PTP o PTMP[13]	Internet móvil 4G o 5G	Internet Satelital
Cámaras Fijas	✓	✓	✗	✓
Cámaras fijas a bordo	✗	✓	✓	✗
Cámaras PTZ	✓	✓	✗	✓
Cámaras Multisensor (más lentes)	✓	✓	✗	✓
Pórtico de patentes (envío flujo de video para procesar dato)	✓	✓	✗	✓
Pórtico de patentes (envío sólo del dato procesado)	✓	✓	✓	✓
Parlantes	✓	✓	✗	✓
Botones SOS	✓	✓	✗	✓
Alarmas	✓	✓	✓	✓
Bodycams para la visualización en vivo y estos flujos graben en VMS	✗	✗	✓	✗
Bodycams para la descarga de videos y enviarlos a un VMS	✓	✓	✗	✓

13 En comunicaciones inalámbricas, PTP (Punto a Punto) y PTMP (Punto a Multipunto) son configuraciones de red. PTP conecta dos ubicaciones, mientras que PTMP conecta un punto central a múltiples puntos remotos.

Energía, Resiliencia y Continuidad Operacional

La continuidad eléctrica y la resiliencia son esenciales en los sistemas de teleprotección, que dependen de energía constante para grabar y transmitir información. Es altamente recomendable contar con respaldo de energía eléctrica UPS en centros de monitoreo con autonomía de al menos 4 horas, baterías de respaldo en cámaras, y paneles solares o generadores portátiles en zonas críticas. Además, es clave establecer rutinas de mantenimiento preventivo y pruebas periódicas de los sistemas de respaldo.

Para asegurar la operación ante cortes prolongados o emergencias, cada municipio debe contar con un Plan de Continuidad Operacional, que defina responsables, procedimientos de registro alternativo, priorización de equipos críticos, resguardo seguro de evidencia y protocolos de restablecimiento de los servicios. Estas medidas permiten mantener la disponibilidad y confiabilidad de los sistemas, incluso en situaciones adversas, fortaleciendo su impacto preventivo y la capacidad de respuesta.

Asimismo, **se deben incorporar medidas de respaldo de información para prevenir la pérdida de registros audiovisuales.** Esto incluye el uso de almacenamiento redundante (como RAID), respaldos automáticos y políticas que aseguren una retención mínima de 30 días con metadatos trazables. Estas medidas permiten mantener la disponibilidad, confiabilidad y valor probatorio de los sistemas, incluso en situaciones adversas, fortaleciendo su impacto preventivo y capacidad de respuesta.

Recomendaciones para compras públicas y gestión de proveedores

Los procesos de licitación deben balancear el criterio técnico con el económico. Se aconseja evaluar la propuesta considerando estándares mínimos, garantías, trazabilidad, conectividad, y calidad del servicio post-instalación.

- Se recomienda incluir niveles de servicio (SLA) definidos que aseguren tiempos de respuesta en caso de fallas, mantenimiento preventivo, y soporte técnico permanente.
- Incluir en la pauta de evaluación que todas las funcionalidades solicitadas en las especificaciones técnicas y administrativas estén operativas, por ejemplo, configuración de las cámaras como videoanalítica o delimitación de sectores (ensombrar segundos pisos de edificios).

- Incluir puntaje adicional en la pauta de evaluación un entrenamiento facilitado por la empresa adjudicataria a una determinada cantidad de funcionarios o vecinos (caso cámaras vecinales).
- El uso de modelos tipo o fichas técnicas referenciales puede facilitar la estandarización entre municipios y acelerar procesos de adquisición.

Participantes

Este trabajo fue posible gracias a los facilitadores de País Digital: Carlos Ibacache, Rita Baeza y Marco Terán, junto con la participación voluntaria de representantes de diversas organizaciones vinculadas con la teleprotección quienes se mencionan a continuación:

Joaquin Ugalde	AChM	Pablo Bahamondez	Ingeniería del Tiempo (CAD)
Ximena Cid	Axis	Andrés Valdés	ISS
Cristobal Cruces	Bosch	Jharold Machillanda	ISS
Mauricio Lara	Bosch	Mario Cortes	Milestone Systems
Darwin Muñoz	Carabinero de Chile	Pedro Guerra	Municipalidad de Lo Barnechea
Miguel Ramírez	Carabinero de Chile	Sebastián Delmas	Municipalidad de Lo Barnechea
José Luis Riffo	Carabinero de Chile	Carlos Pérez	Municipalidad Las Condes
Pedro Herrera	Dahua Technology	Rocío Brizuela	Municipalidad Providencia
Camila Duarte	DIPLADER GORE RM	Graciela Marchant	Municipalidad Puente Alto
Sara Álvarez	DIPLADER GORE RM	Marcos Carrillo	PDI
Iván Soto	Director Programa CEGIR IA	Solange Arredondo	Programa SÉSantiago, GORE RM
Benjamín Barros	Fundación País Digital	Paulina Cataldo	Programa SÉSantiago, GORE RM
Tomás Leal	Fundación País Digital	Claudio Rodríguez	SITIA, Ministerio Seguridad Pública
Paulina Díaz	Fundación Paz Ciudadana	Nicolás Vergara	SITIA, Ministerio Seguridad Pública
Nicolás Muñoz	Fundación Paz Ciudadana	Patricio Urriola	SITIA, Ministerio Seguridad Pública
Jorge Martínez	Genetec	Pablo Bravo	SITIA, Ministerio Seguridad Pública
Eugenio López	Hanwha	Yona Duvauchelle	SITIA, Ministerio Seguridad Pública
Nicolas Steck	Hanwha	Claudio Fuentes	Universidad Diego Portales
Pablo Pizarro	Hikvision	Pedro Valenzuela	Universidad Diego Portales
Claudio Valdebenito	Hikvision	Francisco Soto	VSaaS

Especialmente, se agradece la participación de los expositores Paulina Díaz (Fundación Paz Ciudadana), Benjamín Barros (Fundación País Digital), Graciela Marchant (Municipalidad de Puente Alto), Claudio Fuentes (Universidad Diego Portales), Sara Álvarez y Camila Duarte (GORE RM), cuyas presentaciones ayudaron a la activación de ideas y a las organizaciones Gobierno Regional Metropolitano, Programa SÉSantiago de la Corporación Regional de Santiago y la iniciativa SITIA del Ministerio de Seguridad Pública.

Anexos

Especificaciones Técnicas mínimas

Cámara Fija

- Formato: Bullet, mini Dome y Box con Housing.
- Resolución: 4 MP o superior.
- Cuadros por Segundo: 30 FPS o superior en resolución 4 MP.
- Compresión: H.264 / H.265.
- Estándares: ONVIF Perfil S, G, T, M.
- Almacenamiento: Soporte MicroSD 256 GB o superior (opcional según diseño de storage).
- Longitud Focal: Varifocal (según DORI).
- WDR Real: 120 dB o superior.
- Infrarrojos: Alcance de 50 m o superior (ajustable según diseño).
- Ciberseguridad: Cumplimiento con FIPS o uso de módulos criptográficos TPM.
- Interoperabilidad: Analíticos vía ONVIF Perfil M.
- Analíticos: Clasificación de humanos y vehículos en contexto de ciudad inteligente.
- Certificaciones mínimas recomendadas: IP66, IK10.

Cámara PTZ

- Formato: PTZ Colgante o Sistema de Posicionamiento.
- Resolución: 4 MP o superior.
- Cuadros por Segundo: 30 FPS en resolución 4 MP.
- Compresión: H.264 / H.265.
- Estándares: ONVIF Perfil S, G, T, M.
- Almacenamiento: Soporte para MicroSD 256 GB o superior (uso según criterio de diseño).
- Zoom Óptico: 30x o superior.
- WDR Real: 120 dB o superior.
- Infrarrojos: Alcance de hasta 300 m (opcional según diseño).
- Ciberseguridad: Cumplimiento con FIPS o uso de módulos criptográficos TPM.
- Interoperabilidad: Analíticos vía ONVIF Perfil M.
- Analíticos: Clasificación de humanos y vehículos en contexto de ciudad inteligente.
- Cobertura: Según criterio DORI.
- Certificaciones mínimas recomendadas: IP66, IK10.

Cámara Multi-Sensor 4 Lentes con PTZ

Lentes

- Formato: Multi Sensor (4 lentes fijos).
- Resolución: 4 MP o superior por lente.
- Cuadros por Segundo: 15-30 FPS en resolución 4 MP o superior.
- Compresión: H.264./ H.265.
- Estándares: ONVIF Perfil S, G, T, M.
- Almacenamiento: Soporte MicroSD 256 GB o superior.
- WDR Real: 120 dB o superior.
- Ciberseguridad: Cumplimiento con FIPS o uso de módulos criptográficos TPM.
- Interoperabilidad: Analíticos vía ONVIF Perfil M.
- Analíticos: Clasificación de humanos y vehículos en contexto de ciudad inteligente.
- Certificaciones mínimas recomendadas: IP66, IK10.

PTZ

- Resolución: 2 MP o superior.
- Zoom Óptico: 30x o superior.
- Cuadros por Segundo: 30 FPS en resolución 2 MP o superior.
- Compresión: H.264/H.265.
- Estándares: ONVIF Perfil S, G, T, M.
- Almacenamiento: Soporte MicroSD 256 GB o superior.
- WDR Real: 120 dB o superior.
- Ciberseguridad: Cumplimiento con FIPS o uso de módulos criptográficos TPM.
- Interoperabilidad: Analíticos vía ONVIF Perfil M.
- Analíticos: Clasificación de humanos y vehículos en contexto de ciudad inteligente.
- Certificaciones mínimas recomendadas: IP66, IK10.

Cámara Multi-Sensor sin PTZ

- Formato: Multi Sensor (4 o 5 lentes fijos, sin PTZ).
- Resolución: 4 MP o superior por lente.
- Cuadros por Segundo: 15-30 FPS en resolución 4 MP o superior.
- Compresión: H.264. / H.265.
- Estándares: ONVIF Perfil S, G, T, M.
- Almacenamiento: Soporte MicroSD 256 GB o superior.
- WDR Real: 120 dB o superior.

- Ciberseguridad: Cumplimiento con FIPS o uso de módulos criptográficos TPM.
- Interoperabilidad: Analíticos vía ONVIF Perfil M.
- Analíticos: Clasificación de humanos y vehículos en contexto de ciudad inteligente.
- Certificaciones mínimas recomendadas: IP66, IK10.

Sistema de Lectura de Placas (ANPR/LPR)

Cámara ANPR/LPR

- Formato: Bullet o Box con Housing.
- Resolución: 4 MP o superior a 30 FPS.
- Velocidad de Captura: 120 km/h o superior.
- Tasa de Captura: ≥95% (medible en base a estándares).
- Iluminador: Incorporado, 30 m o superior (IR externo recomendado).
- Almacenamiento: Soporte MicroSD 256 GB o superior.
- Longitud Focal: Varifocal.
- Interoperabilidad: ONVIF o API abierta para extracción de datos.
- Certificaciones mínimas recomendadas: IP66, IK10.

Cámara de Contexto:

Cámara fija de apoyo, instalada junto a sistemas de lectura de placas (ANPR/LPR), cuya función es entregar una visión general del entorno, permitiendo identificar la escena completa y complementar la evidencia asociada a la placa detectada.

- Formato: Bullet o Box con Housing.
- Resolución: 4 MP o superior a 30 FPS.
- Almacenamiento: Soporte MicroSD 256 GB o superior.
- Longitud Focal: Varifocal.
- Certificaciones mínimas recomendadas: IP66, IK10.

Reconocimiento de Placas Vehiculares (ANPR/LPR)

- Compatibilidad regional: lectura de placas de Chile y América (automóviles, motocicletas y carros de arrastre).
- Velocidad de captura: soportar detección de vehículos en movimiento hasta 120 km/h. o superior.

- Multi-pista: lectura simultánea en mínimo 2 carriles.
- Tasa de captura: precisión mínima del 95% en condiciones estándar.
- Detección sin matrícula: identificar vehículos que circulan sin placa.
- Interoperabilidad: exportación de datos a VMS, plataformas de tránsito y sistemas externos mediante ONVIF M o API.
- sistemas externos mediante ONVIF M o API.

Clasificación y Reconocimiento Avanzado de Vehículos

- Clasificación por tipo o tamaño: diferenciación de automóvil, motocicleta, bus, camión, bicicleta, etc.
- Reconocimiento de color del vehículo.
- MMR (Make, Model, Recognition): reconocimiento de marca, modelo, y color del vehículo, alcanzando la mayor precisión posible en condiciones ideales.
- Detección de sentido de circulación, incluyendo alertas de conducción contra el tránsito.
- Generación de metadatos estructurados: registro automático de atributos de cada vehículo para búsquedas rápidas.

Parlantes- Speaker

- Potencia de salida: 7 W o superior.
- Micrófono incorporado.
- Comunicación bidireccional.
- Nivel máximo de presión acústica (SPL): ≥105 dB a 1 metro.
- Soporte para Broadcast en red IP.
- Soporte de audios pregrabados, reproducibles de forma remota o automática.
- Memoria interna o externa para almacenamiento de audios pregrabados.
- Protocolos de interoperabilidad:
  - SIP (para integración con sistemas VoIP).
  - ONVIF (para integración con VMS).
  - VoIP para transmisión de audio sobre redes IP.
- Certificaciones mínimas recomendadas: IP66.

Botones SOS

- Comunicación bidireccional de audio en tiempo real.
- Cámara integrada de mínimo 2 MP para transmisión de video asociada al evento.
- Micrófono incorporado para comunicación de voz.
- Protección anti-sabotaje, con mecanismos de alerta en caso de manipulación indebida.
- Protocolos de interoperabilidad:
  - SIP (para comunicación directa sobre VoIP).
  - ONVIF (para integración con VMS).
  - RTSP (para transmisión de video en tiempo real).

Certificaciones y Normativas

Todos los dispositivos deberán cumplir, según corresponda a su tipología, con las siguientes certificaciones internacionales:

🔹 Protección Física y Ambiental

- IP66 – Protección contra polvo y chorros de agua (conforme IEC 60529 / EN 60529).
- NEMA 4X – Protección anticorrosiva y ambiental, equivalente a IP65/IP66, aplicable a gabinetes y carcasas.
- IK10 – Resistencia contra impactos y vandalismo (conforme IEC 62262 / EN 62262).

🔹 Estándares de Video y Rendimiento

- IEC EN 62676-4 – Estándar internacional para videovigilancia basado en criterio DORI (Detectar, Observar, Reconocer, Identificar).
- ONVIF – Estándar abierto para interoperabilidad de sistemas de videovigilancia, aplicando perfiles:
  - Perfil S (streaming de video).
  - Perfil G (grabación y almacenamiento).
  - Perfil T (video avanzado y H.265).
  - Perfil M (metadatos y analíticos).

🔹 Estándares de Ciberseguridad

- FIPS 140-2 – Validación de seguridad criptográfica.
- TPM (Trusted Platform Module) – Módulos de hardware para encriptación y resguardo de claves.
- Cumplimiento de buenas prácticas internacionales de ciberseguridad en dispositivos de red (ej. actualizaciones seguras, autenticación robusta, cifrado TLS/HTTPS).

🔹 Audio y Comunicación

- SIP (Session Initiation Protocol) – Estándar abierto para comunicación de audio y video sobre IP.
- VoIP (Voice over IP) – Transmisión de voz sobre redes IP.
- ONVIF Audio – Para integración de altavoces y botones SOS con sistemas VMS.

Cuadro comparativo de dispositivos

Características	Detalle	Hardware y elementos físicos					
		Cámaras fijas	Cámaras PTZ	Cámaras Multisensor (más lentes)	Cámaras lectoras de patentes	Parlantes	Botones SOS
Polvo/agua (IP)	Nivel de protección contra ingreso de sólidos y líquidos	IP66	IP66	IP66	IP66	IP66	IP66
Resistencia Vandalismo (IK)	Capacidad de la cámara frente a los impactos físicos	IK10	IK10	IK10	IK10	IK10	IK10
Protección Anticorrosión (NEMA)	Nivel de resistencia a ambientes corrosivos	NEMA 4X	NEMA 4X	NEMA 4X	Según equipo	Según equipo	Según equipo
Objetivo	Propósito o uso principal del equipo	Vigilancia permanente de un sector	Vigilancia detallada de un área y seguimiento	Cobertura 360°, mediante múltiples lentes fijos, reduciendo puntos fijos	Captura de placas y datos vehiculares	Difusión de mensajes en tiempo real	Alerta comunitaria directa
Sugerencia de instalación	Sugerencia de instalación según eficiencia y cobertura	Calles, plazas, exteriores	Avenidas principales, cruces	Intersecciones críticas nuevas	Puntos de control vehicular	Cualquier poste de teleprotección	Tótems o infraestructura municipal
Analíticos sugeridos	Funciones de detección o análisis recomendados para la cámara	Detección de intrusión, conteo de personas y clasificación humano/vehículo con metadata	Detección de intrusión, conteo de personas y clasificación humano/vehículo con metadata	Detección de intrusión, conteo de personas y clasificación humano/vehículo con metadata	Detección de Placas, comparación con base de datos		
Vida útil con mantenimiento	Duración aproximada considerando mantenimiento adecuado	7-10 años aprox.	7-10 años aprox.	7-10 años aprox.	7-10 años aprox.	5-7 años aprox.	5-7 años aprox.

Glosario

- **Algoritmos:** Conjunto de reglas o instrucciones programadas que permiten a un sistema analizar datos y tomar decisiones automáticamente. En teleprotección, los algoritmos permiten reconocer rostros, detectar anomalías o clasificar eventos en tiempo real, especialmente en funciones de videoanalítica.
- **Almacenamiento de Evidencia:** Mecanismos para guardar de forma segura y legalmente válida los registros de video e información crítica captada por los sistemas de vigilancia.
- **Analítica de Video:** Procesamiento automático de imágenes de cámaras para detectar eventos relevantes como movimiento, aglomeraciones, objetos abandonados, etc.
- **Analítica de Video basada en Inteligencia Artificial (IA):** Tecnología avanzada que utiliza algoritmos de aprendizaje automático para interpretar el contenido del video de forma contextual y precisa. Reconoce patrones complejos como personas, vehículos, comportamientos anómalos o situaciones específicas (por ejemplo, un portonazo o una persona corriendo). Tiene mayor capacidad de adaptación al entorno y reduce los falsos positivos. Puede operar en el borde (en la cámara) o de forma centralizada (en servidores).
- **Analítica de Video basada en Píxeles:** Tecnología que detecta cambios en la imagen a partir de variaciones en los píxeles del video. Funciona mediante reglas predefinidas (como detectar movimiento en una zona específica, cruce de líneas o cambios de color) y no interpreta el contenido del video, solo registra que algo cambió. Es útil para tareas simples, como alertar sobre intrusiones, pero puede generar muchos falsos positivos si las condiciones del entorno varían (como sombras, lluvia o animales).
- **ANPR (Automatic Number Plate Recognition):** Término equivalente a LPR, usado principalmente en contextos europeos. Se refiere a la lectura automatizada de matrículas vehiculares mediante analítica de video. Ambos conceptos (LPR y ANPR) se utilizan indistintamente para describir esta capacidad tecnológica.
- **API (Application Programming Interface):** Conjunto de reglas que permite que distintas plataformas o software se comuniquen entre sí. En sistemas de teleprotección, las APIs permiten integrar cámaras, software de gestión, plataformas de análisis y bases de datos, facilitando la interoperabilidad y la personalización de soluciones.
- **Alarmas, Sensores & Comunicaciones:** Incluye sistemas de alarma, detección, y equipos de comunicación (intercom, líneas directas) integrados al centro.
- **Balanceo de Carga:** Técnica que distribuye automáticamente el tráfico de datos o procesamiento entre varios equipos o servidores, evitando saturaciones y mejorando el rendimiento del sistema. En teleprotección, se aplica para gestionar múltiples cámaras o solicitudes simultáneas.

Glosario

- **Cableado & Equipos de Red:** Incluye cables coaxiales, Ethernet, routers y switches, fundamentales para la transmisión de datos.
- **Cámaras Bullet:** Diseñadas para exteriores, con carcasa visible y forma cilíndrica, resistentes al clima y al vandalismo, suelen incluir visión nocturna.
- **Cámaras Covert (Ocultas)**: Diseñadas para vigilancia discreta, aún utilizadas en sistemas modernos.
- **Cámaras Dome:** Tienen forma hemisférica, más discretas, usadas en interiores, resistentes a manipulaciones y con amplio ángulo de visión.
- **Cámaras Fisheye (Ojo de pez):** Capturan imágenes 180° o 360°, útiles para cubrir grandes áreas; requieren software para corregir distorsión.
- **Cámaras PTZ (Pan–Tilt–Zoom):** Permiten movimientos remotos en horizontal, vertical y zoom, ideales para seguir objetivos o cubrir áreas amplias.
- **Cámaras Térmicas:** Detectan radiación infrarroja, útiles en condiciones de baja visibilidad (noche, humo, niebla).
- **CAD (Centro Asistido de Despacho):** Infraestructura tecnológica que coordina la atención y respuesta ante eventos de seguridad detectados por sistemas de teleprotección. El CAD recibe alertas desde cámaras o sensores, las analiza y despacha recursos (como patrullas o equipos de emergencia), operando como eje de comunicación entre distintas entidades (municipios, Carabineros, bomberos, etc.).
- **Centro de Monitoreo:** Instalación desde la cual se supervisan múltiples fuentes de video y datos en tiempo real, operado por personal capacitado para gestionar incidentes.
- **Ciberseguridad:** Conjunto de prácticas y tecnologías que protegen los sistemas y datos de vigilancia ante accesos no autorizados o ciberataques.
- **Clúster de Municipios:** Asociación territorial entre comunas que permite implementar soluciones tecnológicas de vigilancia compartidas para optimizar recursos.
- **Control de Acceso:** Sistemas biométricos, lectores de tarjetas, cerraduras electrónicas, integrados con el VMS y el centro de monitoreo.
- **DVR (Digital Video Recorder):** Sistema que graba video desde cámaras analógicas mediante conexiones coaxiales. Es menos escalable y ofrece menor calidad en comparación con el NVR (Network Video Recorder).
- **Encriptación de Datos:** Técnica para proteger la información durante su transmisión o almacenamiento, evitando accesos indebidos o manipulaciones.

Glosario

- **Estaciones de Trabajo / Consolas:** Computadores con software VMS para operar sistemas, controlar cámaras, gestionar incidentes y verificar grabaciones.
- **Failover:** Mecanismo de respaldo automático que permite que un sistema continúe funcionando si uno de sus componentes falla (como servidores, grabadores o enlaces de red). En teleprotección, asegura la continuidad del monitoreo y grabación ante fallos técnicos.
- **Firewall y Ciberseguridad de Red:** Protección del acceso a la red y videos, esencial ante el riesgo de intrusiones y sabotajes.
- **Gobernanza de Datos:** Marco normativo, técnico y ético que regula el uso, acceso y custodia de los datos generados por los sistemas de teleprotección.
- **Inteligencia Artificial (IA):** Tecnologías que permiten a los sistemas aprender de datos, identificar patrones y tomar decisiones automatizadas. En teleprotección, se usa para analítica de video, reconocimiento facial, entre otros.
- **Interoperabilidad:** Capacidad de distintos sistemas o tecnologías (cámaras, software, sensores, etc.) para comunicarse e integrarse entre sí de forma efectiva.
- Licitación Pública: Proceso mediante el cual las instituciones estatales contratan servicios o compran bienes (como sistemas de vigilancia), de acuerdo con criterios técnicos, económicos y de legalidad.
- **LLM (Large Language Model):** Modelo avanzado de inteligencia artificial capaz de comprender y generar lenguaje natural. Aunque aún emergente en teleprotección, los LLM pueden integrarse para analizar reportes, automatizar respuestas o generar descripciones de eventos desde imágenes o videos.
- **LPR (License Plate Recognition):** Tecnología de reconocimiento automático de placas patentes mediante cámaras y software especializado. Permite identificar vehículos en tiempo real o desde grabaciones, facilitando la detección de vehículos robados, control de accesos o gestión de tránsito. Es una función clave en sistemas de teleprotección urbana.
- **Monitores y Videowall:** Pantallas para visualización en tiempo real. Pueden ser estaciones individuales o videowalls para múltiples operadores.
- **MPLS (Multiprotocol Label Switching):** Tecnología de red utilizada para enviar datos de forma rápida y eficiente por rutas optimizadas. Se aplica en redes privadas de municipios o instituciones que conectan centros de monitoreo, servidores y cámaras en distintos puntos geográficos.

Glosario

- **NVR (Network Video Recorder):** Dispositivo que graba video digital proveniente de cámaras IP a través de una red, ofreciendo almacenamiento de alta calidad y mayor escalabilidad que un DVR.
- **ONVIF (Open Network Video Interface Forum):** Estándar internacional de interoperabilidad para dispositivos de videovigilancia en red (cámaras, grabadores, software, etc.). Permite que equipos de distintos fabricantes sean compatibles entre sí, facilitando la integración, administración y escalabilidad de sistemas de teleprotección.
- **P2P (Peer to Peer):** Tipo de conexión directa entre dispositivos sin pasar por servidores centrales. En cámaras de vigilancia, P2P permite ver video en tiempo real desde una app o navegador, facilitando la instalación remota pero con consideraciones de seguridad.
- **PoE (Power over Ethernet) & Switches PoE:** Tecnología que suministra energía a las cámaras IP mediante el mismo cable de red, simplificando la instalación.
- **RAID (Redundant Array of Independent Disks):** Sistema de almacenamiento que combina varios discos duros para mejorar la seguridad y velocidad del almacenamiento de datos. Se utiliza comúnmente en centros de monitoreo para resguardar grabaciones de video, permitiendo continuidad operativa ante fallos de hardware.
- **Redundancias:** Diseño de sistemas con componentes duplicados o alternativos (como conexiones de red, fuentes de energía o almacenamiento), para garantizar que el servicio no se interrumpa ante fallos. Es clave en sistemas críticos como centros de monitoreo o servidores de video.
- **Resguardo de Datos Personales:** Cumplimiento de normativas legales para garantizar que la información captada por los sistemas de vigilancia respete la privacidad de las personas.
- **RTSP (Real Time Streaming Protocol):** Protocolo que permite la transmisión en tiempo real de video desde cámaras IP a plataformas de visualización o grabación. Es uno de los estándares más utilizados para integrar flujos de video en sistemas de monitoreo.
- **Servidores & Almacenamiento:** Servidores locales o en la nube que almacenan grandes volúmenes de video, utilizando discos preparados para CCTV.
- **SIP (Session Initiation Protocol):** Protocolo de comunicación que permite iniciar, mantener y finalizar sesiones de audio, video o mensajería en tiempo real. En teleprotección, se usa para integrar cámaras con audio bidireccional, botones de pánico, sistemas VoIP u otras plataformas de respuesta remota.

Glosario

- **Teleprotección:** Sistema tecnológico de observación remota que combina cámaras, sensores, plataformas de monitoreo y análisis inteligente de video para vigilar espacios públicos o privados, con el objetivo de prevenir riesgos, detectar incidentes y apoyar la toma de decisiones en seguridad. Esta función integra la vigilancia continua con capacidades de respuesta y coordinación, permitiendo actuar frente a situaciones delictivas o emergencias, y fortalecer la seguridad ciudadana de forma planificada y eficiente.
- **UPS (Sistema de Alimentación Ininterrumpida):** Accesorio esencial para mantener operativos los sistemas en caso de corte eléctrico.
- **VLAN (Virtual Local Area Network):** Red local virtual que permite separar lógicamente distintos dispositivos o servicios dentro de la misma infraestructura física. En teleprotección, se usa para aislar cámaras, servidores y estaciones de trabajo, mejorando la seguridad y el rendimiento de la red.
- **VMS (Video Management System):** Software que permite administrar, visualizar, grabar y recuperar imágenes de cámaras de seguridad. Facilita la integración con otros sistemas como alarmas o analítica.


FUNDACIÓN
país
digital