



El futuro digital
es de todos

MinTIC

USO DEL ESPECTRO RADIOELÉCTRICO PARA SERVICIOS DE SEGURIDAD

Implementación de redes de uso privado para comunicaciones a través de banda ancha móvil para el servicio de seguridad en municipios y ciudades





RESUMEN: “Ciudades seguras”, término usado para referirse a la gama de sistemas que incluyen análisis predictivos y big data, procedimientos de respuesta en tiempo real y sistemas de respuesta a emergencias; soluciones que permiten a los gobiernos y a las fuerzas policiales ampliar y mejorar el servicio público de protección a los ciudadanos.

Este documento presenta una guía a los entes territoriales sobre la implementación de soluciones tecnológicas de este tipo, basadas en el uso de las TIC para servicios de seguridad en sus territorios.



CONTENIDO

INTRODUCCIÓN	4
1. OBJETIVO GENERAL	6
1.1 Objetivos Específicos	6
2. JUSTIFICACIÓN	7
3. NORMATIVIDAD RELACIONADA	8
4. CONDICIONES PARA LA IMPLEMENTACIÓN DE LA RED DE USO PRIVADO PARA SERVICIOS DE SEGURIDAD SOBRE BANDA ANCHA MÓVIL	10
4.1 Consideraciones administrativas	10
4.2 Consideraciones técnicas	11
4.3 Consideraciones logísticas	13
5. CARACTERÍSTICAS GENERALES DE LA RED DE USO PRIVADO PARA SERVICIOS DE SEGURIDAD SOBRE BANDA ANCHA MÓVIL	15
5.1 Flujo funcional	16
5.2 Esquema de implementación	19
5.3 Seguridad de la red	19
6. PRESUPUESTO	20
7. CRONOGRAMA	21



INTRODUCCIÓN

De acuerdo con la Unión Internacional de Telecomunicaciones (UIT), una ciudad inteligente y sostenible es una ciudad innovadora que aprovecha las tecnologías de la información y la comunicaciones (TIC) y otros medios para mejorar la calidad de vida, los servicios urbanos y la competitividad, al tiempo que se asegura de responder a las necesidades de las generaciones presente y futuras en lo que respecta a los aspectos económicos, sociales, medioambientales y culturales¹.

Bajo este concepto se encuentra el de “ciudades seguras”, término usado para referirse a una gama de sistemas que incluyen análisis predictivos y big data, procedimientos de respuesta en tiempo real y sistemas de respuesta a emergencias; soluciones que permiten a los gobiernos y a las fuerzas policiales ampliar y mejorar el servicio público de protección a los ciudadanos.

Lo anterior cobra relevancia en el país, especialmente al considerar su gran concentración poblacional a nivel urbano. De acuerdo con el DANE, el 77,7% de la población en el país vive en cabeceras municipales, 15,2% en el área rural y el 7,1% en centros poblados².

Bajo este contexto surge la necesidad de aportar una guía a los entes territoriales que facilite la formulación de soluciones tecnológicas para ciudades o municipios más seguros en el país. En este sentido, el uso de la banda ancha móvil supone uno de los principales canales de comunicación para fortalecer los servicios de seguridad, por esta razón en este documento se describen soluciones tecnológicas que se pueden implementar sobre la banda de 380 MHz a 398 MHz destinada para este tipo de servicios.

Lo anterior, partiendo desde el uso eficiente del espectro radioeléctrico hasta la implementación de una red de seguridad con monitoreo de zonas específicas, utilizando transmisión de video, llamadas P2P/llamadas de grupo, mensajes multimedia, servicios de información geográfica con el correspondiente almacenamiento de información, que permita la coordinación de las acciones de las fuerzas de seguridad para la identificación de actividades delincuenciales y los actores involucrados en las mismas.

¹ UNIÓN INTERNACIONAL DE TELECOMUNICACIONES. Internet de las cosas y ciudades y comunidades inteligentes. Octubre de 2016.

² Ver <https://www.dane.gov.co/index.php/estadisticas-por-tema/demografia-y-poblacion/censo-nacional-de-poblacion-y-vivenda-2018/donde-estamos>



Es de aclarar que, en esta guía, el alcance del uso en la banda 380 MHz a 398 MHz, está referido a servicios de seguridad mediante redes privadas, entendidas como aquellas destinadas a satisfacer necesidades propias de los usuarios, mas no como redes cuyo objetivo sea la prestación de servicios de telecomunicaciones a terceros. Es decir, redes utilizadas exclusivamente para la función específica de apoyo a los entes territoriales en sus planes o estrategias de seguridad.

Es importante considerar que la solución contenida en este documento no obsta para estudiar, analizar y/o desarrollar otras alternativas, sin embargo, la recomendación principal se basa en el uso de la banda de frecuencia relacionada para redes privadas de seguridad.



1. OBJETIVO GENERAL

Presentar una guía que le permita a los entes territoriales, encargados de la seguridad de la población, desarrollar proyectos de servicios de seguridad basados en el uso de las TIC y a través de la banda ancha móvil para redes privadas.

1.1 Objetivos Específicos

- 1.1.1 Presentar una alternativa de solución tecnológica que apoye los programas de seguridad de los entes territoriales, utilizando redes privadas de comunicaciones.
- 1.1.2 Promover el uso del espectro radioeléctrico en las frecuencias 380 a 398 MHz en el desarrollo de soluciones de seguridad para la protección de los ciudadanos.
- 1.1.3 Proporcionar información de apoyo para la formulación de soluciones tecnológicas orientadas al servicio público de seguridad.



2. JUSTIFICACIÓN

De acuerdo con el “Marco de Convivencia y Seguridad Ciudadana”, expedido por el gobierno nacional en 2019, una de las áreas a priorizar a nivel nacional y por ende a nivel territorial, es la “Tecnología para la convivencia y la seguridad ciudadana”³, bajo el entendido que el uso de la tecnología facilita la oportuna detección del comportamiento criminal o de actividades inusuales, permitiendo a las autoridades desplegar una respuesta más inmediata.

Colombia presenta grandes retos en este sentido, pues tal como fue señalado en la política mencionada *“El número de capturas por delitos que afectan la seguridad ciudadana contrasta con el número de condenas y con la adopción de medidas de aseguramiento privativas de la libertad. La posibilidad que un capturado sea objeto de una medida de aseguramiento de ese tipo es baja y que sea objeto de condena es aún menor. Esta situación se traduce en una alta rentabilidad del delito, en contraste con una baja probabilidad de pagar un costo por su comisión”*⁴.

Y en lo anterior influyen factores de toda índole, sin embargo, en gran medida la identificación oportuna de la conducta y de quien la comete es uno de los obstáculos que no permiten que estas cifras mejoren. En este sentido, en lugares como Singapur, una de las ciudades catalogadas como de las más seguras del mundo, se encuentra que el uso de las TIC ayudó entre los años 2012 y 2016 a resolver más de 1.000 casos de criminalidad⁵.

Así las cosas y con la intención de buscar aportes directos de las TIC en el desarrollo de servicios de seguridad, así como explorando las posibilidades que ofrece la industria, se presenta esta guía sobre las soluciones tecnológicas que, con el uso de los recursos de las telecomunicaciones, contribuyen a promover ciudades más seguras y a una mejor respuesta por parte de las autoridades.

³ MARCO DE CONVIVENCIA SEGURIDAD CIUDADANA. Consultar en https://www.mininterior.gov.co/sites/default/files/politica_marco_de_convivencia_y_seguridad_ciudadana.pdf

⁴ Ibidem

⁵ THE ECONOMIST. Safe Cities Index 2017. Security in a rapidly urbanising worldIndex.



3. NORMATIVIDAD RELACIONADA

De acuerdo con el artículo 17 de la Ley 1341 de 2009, modificada por la Ley 1978 de 2019, el Ministerio de las Tecnologías de la Información y las Comunicaciones tiene como objetivo promover el uso y apropiación de las Tecnologías de la Información y las Comunicaciones entre los ciudadanos, las empresas, el gobierno y demás instancias nacionales como soporte del desarrollo social, económico y político de la Nación.

Así mismo, según el artículo 18, tiene como función apoyar al Estado en el acceso y uso de las Tecnologías de la Información y las Comunicaciones para facilitar y optimizar la gestión de los organismos gubernamentales para prestar mejores servicios a los ciudadanos.

De otro lado, la Unión Internacional de Telecomunicaciones (UIT) ha recomendado, para la región 1 y región 2, de la cual Colombia hace parte, que la banda de 380 - 470 MHz se use para la implementación de redes de Protección Pública y Atención de Desastres (PPDR)⁶, preferiblemente en la banda 380 a 430 MHz según la Recomendación UIT-R M2015-2.

Bajo el anterior contexto, el plan de banda previsto en la Tabla 4 del Cuadro Nacional de Atribución de Bandas de Frecuencias (CNABF) expedido por la Agencia Nacional del Espectro (ANE), atribuyó para el servicio de radiocomunicación móvil, la banda de frecuencias de 380 MHz a 398 MHz, con el principal objetivo de que este recurso sea utilizado para la implementación de redes privadas de comunicaciones móviles de banda ancha en configuración TDD (Duplexación por división de tiempo, por sus siglas en inglés).

Esta actualización se encuentra contenida en la Resolución 105 de 2020, en la que se fijan las siguientes condiciones:

Rango de frecuencias:	380 a 398 MHz
Anchos de Bandas	3, 5 y 10 MHz
Permitido:	
Modo de uso:	Comunicaciones móviles de banda ancha
Método de acceso:	TDD
Restricciones:	Redes privadas (no prestan servicios de comunicaciones a terceros)

En este sentido, se propone que las redes que se establezcan sobre la banda de frecuencias 380 MHz a 398 MHz sean de uso privado para garantizar que las mismas no permitan la

⁶ Resolución 646 UIT (Rev. CMR 15)



prestación de servicios de telecomunicaciones a terceros, de tal manera que las entidades territoriales puedan explotar de la forma más eficiente su uso para soluciones que apoyen los planes de seguridad ciudadana. En segundo lugar, se busca que los servicios TIC sean transmitidos a través de redes de banda ancha móvil para permitir que el uso de internet y de la información que se pueda transmitir por estas redes, puedan utilizar servicios avanzados de video y de comunicación.

De conformidad con lo establecido en la Ley 62 de 1993, los alcaldes y gobernadores son las primeras autoridades de policía de su territorio; así mismo, según lo señalado en el artículo 6, numeral 4 de la Ley 1551 de 2012, les corresponde a los municipios elaborar e implementar los planes integrales de seguridad ciudadana en coordinación con las autoridades locales de Policía.

Adicionalmente, es importante señalar que la implementación de soluciones de este tipo debe garantizar el efectivo ejercicio de los derechos a la intimidad personal, familiar y de habeas data, de acuerdo con lo establecido en el artículo 15 de la Constitución Política, con la Ley 1581 de 2012 y sus decretos reglamentarios.



4. CONDICIONES PARA LA IMPLEMENTACIÓN DE LA RED DE USO PRIVADO PARA SERVICIOS DE SEGURIDAD SOBRE BANDA ANCHA MÓVIL

La implementación de una red de uso privado para servicios de seguridad requiere del cumplimiento de varios aspectos técnicos, logísticos y administrativos, de cara a los objetivos planteados por las entidades territoriales que decidan implementar este tipo de soluciones.

4.1 Consideraciones administrativas

Para la implementación de esta guía por el ente territorial correspondiente, es necesario tener en cuenta la *“Guía metodológica para la formulación, implementación y seguimiento de los Planes Integrales de Seguridad y Convivencia Ciudadana (PISCC)”* en la versión que se encuentre vigente⁷, que para el año 2020 es la elaborada por el Ministerio del Interior, Ministerio de Defensa Nacional, Departamento Nacional de Planeación y Policía Nacional.

Esta guía, en términos generales, recomienda a las autoridades seguir una serie de pasos dentro de su planeación en temas de seguridad consistentes en:

1. Diagnosticar, focalizar y priorizar
2. Formular el plan de seguridad y convivencia
3. Realizar la planeación operativa y financiera
4. Implementar
5. Realizar seguimiento y evaluación

Bajo este esquema, el diagnóstico que se realice, les permitirá identificar las zonas en las que es necesario implementar este tipo de soluciones tecnológicas de acuerdo con aspectos como la densidad poblacional y la comisión de delitos en la zona, entre otros.

Así mismo, la disponibilidad de presupuesto es un factor determinante para la implementación de la solución. La asignación de presupuesto dependerá de la cantidad de zonas a ser cubiertas por el sistema de monitoreo y control, es decir que el presupuesto estará directamente relacionado con el número de cámaras y/o dispositivos utilizados en la

⁷ GOBIERNO DE COLOMBIA. Guía metodológica para la formulación, implementación y seguimiento de los Planes Integrales de Seguridad y Convivencia Ciudadana (PISCC). Versión vigente 2019
https://osc.dnp.gov.co/guia_total.pdf



red a implementar, la capacidad instalada que se requiera en la base de datos y el sistema de gestión. En este aspecto, la guía metodológica citada incluye las diversas fuentes de financiación con que los entes territoriales cuentan para la ejecución de estos planes⁸.

Una vez la red de uso privado para servicios de seguridad esté instalada se debe dimensionar el recurso humano para manejar la operación del sistema, tanto en los ambientes de gestión como en lo relativo a tareas de soporte y mantenimiento, razón por la cual se deben estimar los costos asociados para al menos 5 años posteriores a la puesta en marcha del proyecto, esto último con el ánimo de que la solución sea sostenible. Este aspecto podrá ser parte de la coordinación que las autoridades realicen y que es mencionada en la guía citada⁹.

4.2 Consideraciones técnicas

La primera consideración técnica obedece a las especificaciones de la banda de frecuencia a utilizar en este tipo de proyecto, las cuales corresponden a la banda de frecuencia de 380 MHz y 398 MHz, atribuida para comunicaciones móviles de banda ancha de acuerdo con la Tabla 4 de CNABF. Dada esta condición es mandatorio que los enlaces de microondas o conexiones a redes de transmisión funcionen sobre dichas frecuencias, ya sea sobre infraestructura ya desplegada por otra entidad, por un operador de redes terrestres de telecomunicaciones o sobre infraestructura propia del proyecto.

Respecto a la infraestructura de red se recomienda considerar diferentes opciones respecto a los medios de acceso para la trasmisión de información. En primer lugar, se puede considerar infraestructura propia, lo que implicará una mayor inversión a nivel presupuestal, una segunda opción es hacer instalación de equipos sobre la infraestructura de los operadores terrestres presentes en las zonas seleccionadas, y la tercera opción se basa en el uso de redes de servicios de internet WiFi público si los mismos estuvieran disponibles en las zonas de cobertura de la solución. De cualquier manera y de acuerdo con el modelo de infraestructura seleccionada es fundamental que se puedan garantizar los protocolos de seguridad para la trasmisión y métodos de accesos a la información recolectada por los dispositivos móviles de grabación de audio y video.

También se deben considerar las especificaciones técnicas de los demás elementos utilizados en el despliegue de la solución (remítase a la ilustración 2 e identifique los elementos de hardware que se recomiendan para la implementación). Las cámaras fijas o

⁸ Ibidem, página 19.

⁹ Ibidem, página 18.



los dispositivos móviles deben tener una resolución de alta calidad (HD por sus siglas en inglés) de al menos 1280x720 píxeles, los sistemas de transmisión deben contar con la conectividad apropiada, recomendando al menos canales dedicados de 15Mbps (Megabit por segundo) si se tiene en cuenta la necesidad de hacer streaming en vivo. Una recomendación adicional respecto al ancho de banda es poder contar con simetría en la velocidad de carga y de descarga, lo que indicaría disponer de velocidades de al menos 15 Mbps tanto en uplink como en downlink.

Es importante determinar cuál será el método que se deba utilizar para la compresión del vídeo debido a que serán múltiples cámaras en la zona a ser vigilada y el volumen de datos a ser transmitido será elevado, más aún si selecciona transmitir vídeo en HD. Aunque existen diferentes estándares de compresión es recomendable utilizar como mínimo el estándar MPEG-4 sin que esto limite el uso de otros estándares como MPEG-7, H.264 o H.265¹⁰.

En cuanto a los protocolos, recuerde utilizar los que correspondan a la fase de implantación de la red privada, considere protocolos TCP (Transmission Control Protocol por sus siglas en inglés) para el control del transporte, RTP (Real-time Transport Protocol por sus siglas en inglés) para el transporte en tiempo real sobre comunicación IP, RTCP (Real-time Control Protocol por sus siglas en inglés) para el control en tiempo real, RTSP (Real-time Streaming Protocol por sus siglas en inglés) para hacer streaming en tiempo real y UDP (User Datagram Protocol por sus siglas en inglés) que se utiliza para el transporte de datos de forma rápida y compacta.

El almacenamiento de los datos es un factor determinante en el éxito del sistema de gestión utilizado en el monitoreo y vigilancia de las zonas seleccionadas para la implementación de la red de uso privado de servicios de seguridad, por esta razón es necesario realizar una adecuada selección de los equipos de almacenamiento y de la capacidad de estos. Dependiendo de la cantidad de cámaras y de zonas a ser vigiladas se podría seleccionar desde un DVR (Digital Video Recorder por sus siglas en inglés) para el almacenamiento hasta un disco duro; sin embargo, considerando que la recomendación es monitorear zonas de alto tráfico de personas, se debería entonces utilizar discos duros que ofrecen mayor capacidad de almacenamiento, incluso sería mejor si se utiliza un arreglo de discos (varios

¹⁰ ALVARADO LEÓN, R. H. Diseño e implementación de sistema de video vigilancia con cámaras IP para la ferretería PROINDUPET CIA. LTDA (Bachelor's thesis, QUITO/EPN/2011)



discos) para recolectar la información. Tenga en cuenta que para calcular la capacidad de los discos de almacenamiento puede utilizar la siguiente fórmula¹¹:

Almacenamiento (Gbytes)

$$= \text{Ancho de banda Total} \times \# \frac{\text{segundos}}{\text{semanas}} \times \frac{1\text{Gbits}}{1024\text{Mbits}} \times \frac{1\text{ byte}}{8\text{ bits}}$$

Considere para el cálculo de Ancho de banda Total

$$= \text{Ancho de banda 1} + \text{Ancho de banda 2} + \text{Ancho de banda n (Mbps)}$$

También considere que no es necesario tener la información almacenada durante diferentes meses en el mismo espacio de disco utilizado para la grabación, existen alternativas técnicas que permiten realizar copias de seguridad para ser almacenadas en otros dispositivos, como por ejemplo servidores de respaldo o BackUp. Si su solución contempla el intercambio y/o compartición de información con otras entidades debe incluir un análisis de los métodos tecnológicos para compartir la información requerida.

4.3 Consideraciones logísticas

El desarrollo y puesta en marcha de una solución de seguridad tiene un gran impacto en la sociedad y así mismo representa un gran reto para la entidad que lo desee poner en práctica, parte de esos retos están relacionados con las actividades a nivel logístico en la implementación.

En primer lugar, la selección de las zonas a ser cubiertas por el servicio debe cumplir los objetivos del proyecto y abarcar el mayor número de población beneficiaria, además dichas zonas deben contar con infraestructura TIC que permita el montaje e instalación de los elementos dispuesto para la solución. Considere infraestructura de redes de internet sobre tecnologías móviles, como por ejemplo LTE.

Por otra parte, es necesario establecer la ubicación del centro de gestión y los mecanismos de comunicación con las entidades encargadas de garantizar la seguridad en los diferentes municipios, de tal manera que las reacciones a eventos delictivos tengan alta eficiencia, es decir, el menor tiempo de atención ante cualquier evento.

¹¹ VELASCO SANTAMARÍA, D. A. *Estudio y diseño de una red de video vigilancia local y remota, utilizando cámaras de vigilancia para el monitoreo de seguridad, alerta de intrusión y almacenamiento de video, para la planta de producción de la empresa Romery* (Bachelor's thesis, QUITO/EPN/2013).



En segundo lugar, la comunicación a la ciudadanía es muy importante, las zonas seguras deben permitir a las autoridades tener control y monitoreo permanente, pero también es relevante que las personas conozcan de la ubicación de estas cámaras y así darles herramientas en caso de realizar denuncias y eventuales búsquedas de evidencias de actos delictivos, además, esta información genera una percepción positiva de seguridad y tranquilidad en la comunidad.

En tercer lugar, se encuentra la necesidad de realizar procesos de capacitación a los diferentes actores que utilizarán los sistemas de seguridad. Estos procesos de aprendizaje le apuntan directamente a la apropiación de la tecnología, por eso es necesario capacitar a los operarios del sistema, las autoridades competentes, la ciudadanía beneficiaria del sistema de seguridad, las entidades externas que pudieran hacer uso de la información almacenada por el sistema, entre otros.

Se recomienda incluir en las capacitaciones los procesos técnicos referentes al uso, administración y gestión de la solución tecnológica dirigido a los operadores del sistema. Además, las capacitaciones también deben tener alcance a la comunidad en el sentido de hacer la divulgación y promoción de la solución como un beneficio común, por eso se esperaría que se realicen encuentros con la comunidad para participarles de la existencia de la red y del aporte que ofrece la misma a la convivencia y seguridad de la comunidad.



5. CARACTERÍSTICAS GENERALES DE LA RED DE USO PRIVADO PARA SERVICIOS DE SEGURIDAD SOBRE BANDA ANCHA MÓVIL

La primera característica a resaltar es el concepto de red privada, lo que en este contexto está particularmente orientado a que una solución tecnológica de banda ancha en la banda de frecuencia 380 MHz a 398 MHz, sea de uso exclusivo de las entidades territoriales para la prestación del servicio de seguridad a los ciudadanos. Esto quiere decir en primer lugar, que esta red privada no podrá ser utilizada por terceros, ni comercializada y, en segundo lugar, que la misma debe tener como fin la prestación de un servicio público.

Así mismo tenemos que el uso de la banda ancha permite que la información transmitida por los canales de comunicación establecidos pueda fluir de forma rápida, segura y con calidad. En este sentido y acotando el alcance de la solución a redes de servicios móviles, se busca que la cobertura de la red y la ubicación de los elementos físicos para obtener la información requerida sea más amplia que la que se pudiera lograr con otros tipos de redes. Además, la disponibilidad de coberturas de las redes móviles en las ciudades principales permite cubrir más población con este tipo de soluciones de servicios de seguridad.

De otro lado, se enfoca el servicio a la integración de diferentes dispositivos móviles que permiten la transmisión de vídeo, a través de la utilización de cámaras de vigilancia para efectuar el control y monitoreo de zonas específicas dentro de la región geográfica seleccionada.

Actualmente se disponen de dos tecnologías disponibles en la banda de 380 a 398 MHz, en primer lugar, LTE¹², estándar de Interfaz Radioeléctrica para IMT¹³ del 3GPP¹⁴ y en segundo lugar B-Trunc¹⁵, un estándar de CCSA¹⁶ que es reconocido por la UIT y es una respuesta a las necesidades de transmisión de video, imágenes y datos que el acceso troncalizado de banda angosta tradicional no puede soportar, con el que es posible disponer de estaciones base, terminales de usuario y puntos de acceso con capacidades de transmisión de datos utilizando anchos de banda desde 3 MHz hasta 10 MHz.

¹² Evolución a Largo Plazo, LTE por sus siglas en ingles

¹³ Telecomunicaciones Móviles Internacionales, IMT por sus siglas en ingles

¹⁴ Proyecto Asociación de Tercera Generación, 3GPP por sus siglas en ingles.

¹⁵ ZHANG, Zheming, et al. A Multicast Beamforming Algorithm to Improve the Performance of Group Service for Multicell B-Trunc System. En *International Conference on Artificial Intelligence for Communications and Networks*. Springer, Cham, 2019. p. 120-131.

¹⁶ Asociación China de Estándares Internacionales



5.1 Flujo funcional

Considere al menos los aspectos relacionados en el siguiente diagrama de flujo para la implementación de la solución de seguridad basada en cámaras de seguridad.

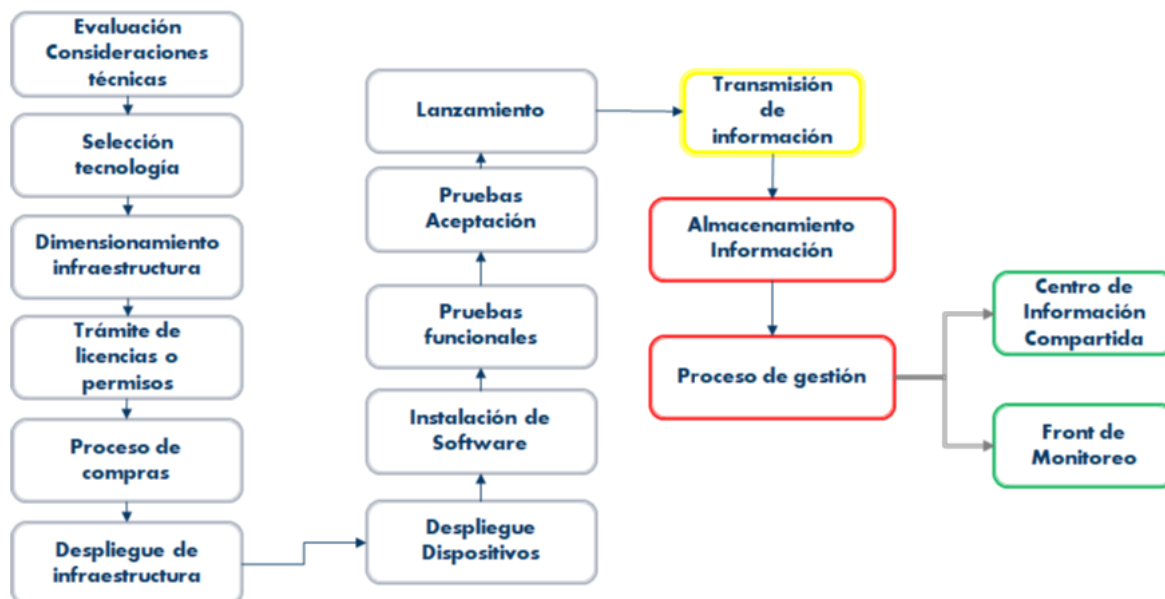


Ilustración 1. Flujo Funcional Red Privada para servicios de seguridad

Fuente: Elaboración propia

Evaluación de consideraciones técnicas: Es importante realizar una valoración técnica de las opciones disponibles para la implementación de este tipo de soluciones no omita ninguna opción y, en cualquier caso, evalúe la infraestructura TIC disponible en las zonas a ser cubiertas por la solución. Una vez cuente con suficientes criterios de evaluación y el resultado de un análisis técnico, seleccione la tecnología a implementar.

Trámite de licencias y permisos: Entre los posibles permisos requeridos para el despliegue y operación de la red, cabe destacar los siguientes: ante el Ministerio de las Tecnologías de la Información y las Comunicaciones, cuando se refiera al uso del espectro radioeléctrico; la Aeronáutica Civil de Colombia, en cuanto al permiso de alturas; la Autoridad Nacional de Licencias Ambientales o las Corporaciones Autónomas Regionales, cuando se requiera



licencia de tipo ambiental; ante los curadores urbanos y las Oficinas de Planeación de los Municipios para las licencias de construcción y/o de ocupación del espacio público y la expedición de los actos administrativos que autoricen la instalación de los elementos de transmisión; ante la Agencia Nacional del Espectro, cuando se traten temas referentes a exposición a campos electromagnéticos en su caso.

Proceso de Compras: En este punto debe tener en cuenta lo señalado en las consideraciones administrativas sobre la *“Guía metodológica para la formulación, implementación y seguimiento de los Planes Integrales de Seguridad y Convivencia Ciudadana (PISCC)”*.

Despliegue Infraestructura: Estime los tiempos de la institución en las zonas seleccionadas para la implementación de la solución, recuerde que en caso de seleccionar infraestructura ya desplegada de alguna otra entidad pública o privada, debe realizar los trámites correspondientes para obtener las autorizaciones de instalación y uso de dicha infraestructura.

Despliegue de dispositivos: Una vez se establezca la zona y/o sector sobre el cual se requiere realizar el monitoreo y control de seguridad establezca la referencia geográfica de la ubicación de las cámaras de seguridad.

Instalación de Software: Las herramientas de software son fundamentales para la gestión y control de las actividades propias de la solución tecnológica, considere todas las fases de instalación del software requeridas para cada uno de los dispositivos y sistemas que hacen parte del proyecto.

Pruebas Funcionales y de Aceptación: Se recomienda realizar al menos dos fases de pruebas para la aceptación de la solución previo al lanzamiento de esta. La primera fase se debe realizar sobre un ambiente controlado y que busque validar la funcionalidad de cada elemento que compone la red, de tal manera que de forma gradual se vayan probando las etapas de la funcionalidad. Posteriormente se sugiere una prueba completa del sistema debido a que la integración de todos los elementos y la interconexión entre estos puede ocasionar fallas que deben ser solucionadas previo a la puesta en servicio.

Transmisión de información: De acuerdo con las características planteadas para esta solución, considere utilizar estaciones base, terminales de usuario y equipos tipo router o puntos de acceso, además de cámaras, alarmas, sensores de movimiento, entre otros, que puedan ser integrados para transmitir información sobre la banda de frecuencia de 380



MHz a 398 MHz utilizando comunicaciones móviles de banda ancha con método de acceso TDD. En este punto es muy importante, tener en cuenta que la transmisión de información (Video/Audio/Información del equipo terminal) debe ser de manera segura hacia un servidor central debido a la sensibilidad de la información que se utiliza en este tipo de soluciones de seguridad.

Almacenamiento de información: La información que sea transmitida hacia el servidor central debe ser almacenada bajo protocolos de seguridad que garanticen la integridad de esta. En el servidor central se debe instalar una base de datos que permita almacenar la información de tal manera que se pueda identificar de manera clara y fácil el origen de esta.

Front de Monitoreo: Consiste en el sistema de gestión y control de las cámaras instaladas en la zona seleccionada para monitoreo. El sistema de gestión debe permitir visualizar las imágenes captadas por las cámaras, controlar el movimiento de estas (acercamientos, primeros planos, rotación, etc.) y gestionar el proceso de almacenamiento de la información.

Centro de información compartida: es importante que el centro de gestión permita que otras entidades puedan acceder a la información almacenada en el servidor central, de acuerdo con la estrategia que al respecto se diseñe en el plan de seguridad del ente territorial. Considere, en cualquier caso, las entidades tendrán acceso a dicha información y los mecanismos de autorización o permiso de acceso a dicha información.

5.2 Esquema de implementación

Se presenta a continuación una arquitectura de referencia de la solución para redes de uso privado para comunicaciones de banda ancha móvil en municipios para el servicio de seguridad. Tenga en cuenta que la arquitectura propuesta permite facilitar el diseño de implementación, sin embargo, cada entidad territorial debe realizar dentro de su proceso de análisis técnico, diseño y adecuación del proyecto la adaptación del mismo.

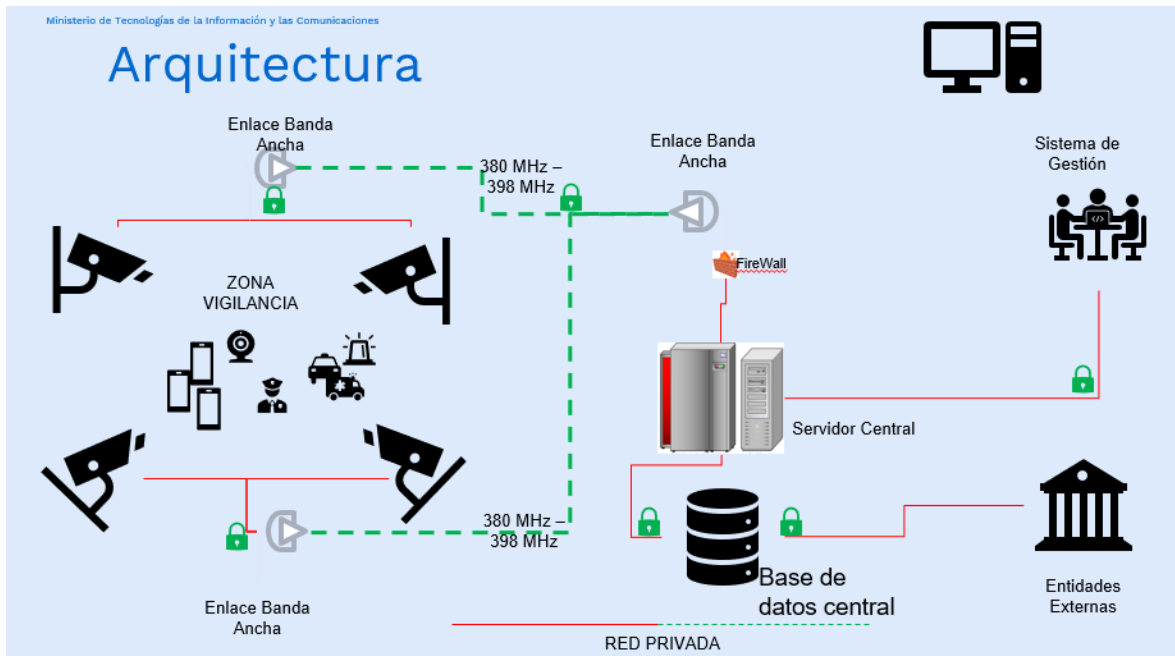


Ilustración 2. Esquema de implementación red privada para servicios de seguridad

Fuente: Elaboración propia

5.3 Seguridad de la red

Teniendo como referencia el esquema de implementación presentado en la ilustración 2, considere todos los aspectos de seguridad¹⁷ para garantizar la integridad de la información que se trasmite en la red privada para servicios de seguridad. Las recomendaciones básicas van orientadas a implementar protocolos de encriptación de video y audio, instalación de elementos de protección como Firewall para el acceso al servidor central y controles de acceso a las bases de datos, tanto para los accesos de los operadores del sistema como para las conexiones de otras entidades.

¹⁷ López, P. A. (2010). *Seguridad informática*. Editex.



6. PRESUPUESTO

Para la estimación del presupuesto se recomienda identificar de manera muy clara el tipo de gasto o inversión a realizar basados en los conceptos de CAPEX (gastos de Capital) y OPEX (Costos de Operación).

Considere en principio incluir dentro del presupuesto los aspectos relacionados con la evaluación técnica de la solución tecnológica a implementar, el dimensionamiento de la infraestructura de red (Antenas Rx y Tx), las cámaras de monitoreo, los elementos activos de red, el software de gestión y los costos de instalación e implementación. Adicionalmente, se deben presupuestar aquellas actividades requeridas para la operación del sistema, el mantenimiento de equipos y del sistema, software y los costos de almacenamiento de información (servidores).

Identifique cualquier otro requerimiento del sistema a nivel de software y hardware, además de las necesidades técnicas para la integración a redes existentes y/o servidores de otras entidades que requieran la información almacenada, incluso si la misma se pudiera consultar en tiempo real.

El costo final de la implementación de los sistemas de seguridad dependerá del estudio de mercado de cada zona a ser beneficiada, de las cotizaciones que realice cada entidad y del proveedor que sea seleccionado, sin embargo, un presupuesto estimado para la implementación de una zona segura (cobrimiento de 8000 personas) incluyendo los costos de mantenimiento para un año, podría estar alrededor de los \$ 450.000.000 COP.



7. CRONOGRAMA

En la Tabla 1 podrá encontrar las actividades generales que se relacionan con la implementación del proyecto, considere incluir las tareas adicionales que identifique en sus estudios de mercado y/o cotizaciones, además estime los tiempos de acuerdo con las actividades incluidas adicionalmente.

Actividad	Tiempo Estimado (Semanas)
Estudio y evaluación técnica	4
Dimensionamiento de infraestructura	3
Proceso de compra de equipamiento	8
Instalación de infraestructura de radios	6
Instalación dispositivos de monitoreo	7
Instalación y personalización del software de gestión	5
Pruebas sistema de comunicación	2
Pruebas sistema de gestión	3
Capacitación personal de operación	2
Prueba piloto del sistema integrado	4
Puesta en producción	1

Tabla 1. Actividades del proyecto

De acuerdo con el análisis técnico y de recursos que realice la entidad territorial para la implementación de este tipo de soluciones, es importante identificar las actividades que deba desarrollar en paralelo.



El futuro digital
es de todos

MinTIC

