UNIVERSIDAD NACIONAL
"SANTIAGO ANTÚNEZ DE MAYOLO"

FACULTAD DE CIENCIAS

ESCUELA ACADÉMICO - PROFESIONAL
INGENIERÍA DE SISTEMAS E INFORMÁTICA

"SISTEMA DE TELEVIGILANCIA UTILIZANDO FIBRA ÓPTICA CON FINES DE SEGURIDAD CIUDADANA PARA EL DISTRITO DE HUARAZ, 2014"

TESIS

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO DE SISTEMAS E INFORMÁTICA

PRESENTADO POR:

Bach. DANTE JHOSEP DE LA CRUZ MAGUIÑA

ASESOR:

Ing. LUIS RUPERTO ALVARADO CÁCERES

HUARAZ - PERÚ

2015

N° Registro: T010

UNIVERSIDAD NACIONAL
"SANTIAGO ANTÚNEZ DE MAYOLO"

FACULTAD DE CIENCIAS

ESCUELA ACADÉMICO-PROFESIONAL
INGENIERÍA DE SISTEMAS E INFORMÁTICA

"SISTEMA DE TELEVIGILANCIA UTILIZANDO FIBRA ÓPTICA CON FINES DE SEGURIDAD CIUDADANA PARA EL DISTRITO DE HUARAZ, 2014"

TESIS

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO DE SISTEMAS E INFORMÁTICA

PRESENTADO POR:

Bach. DANTE JHOSEP DE LA CRUZ MAGUIÑA

ASESOR:

Ing. LUIS RUPERTO ALVARADO CÁCERES

HUARAZ - PERU
2015

Nº Registro: T010

DEDICATORIA

A mis padres por ser razón y motivo de seguir adelante y alcanzar mis objetivos y metas trazadas, enfrentando cualquier adversidad de la vida con perseverancia y coraje.

A mis hermanos por su apoyo moral, siendo un ejemplo en mí vida de hacer bien las cosas con mucho esmero y dedicación.

A mis familiares y amigos quienes creyeron en mí para que yo pueda culminar mi carrera profesional y lograr este sueño que se está haciendo realidad.

Dante Jhosep

AGRADECIMIENTOS

Agradezco a Dios, quien me dio la vida y permitió hacer realidad este sueño, el ser un profesional y por darme la oportunidad de tener un día más de vida junto a las personas que más quiero en este mundo.

Al Ing° Luis Alvarado Cáceres, por su desmedido apoyo en estructurar y guiarme en la tesis.

A nuestra casa superior Universidad Nacional Santiago Antúnez de Mayolo, por albergarnos durante nuestra vida estudiantil y a todos nuestros docentes por brindarnos sus conocimientos y sapiencias para formarnos como buenos profesionales.

Dante Jhosep

PRESENTACIÓN

Señores Miembros del Jurado Calificador:

En cumplimiento con el Reglamento de Grados y Títulos de la Escuela Académico-Profesional de Ingeniería de Sistemas e Informática, Facultad de Ciencias, de la Universidad Nacional Santiago Antúnez de Mayolo, me permito presentar la tesis titulada "***Sistema de televigilancia utilizando fibra óptica con fines de seguridad ciudadana para el distrito de Huaraz, 2014***".

Esta tesis realizada en el área urbano y urbano marginal del distrito de Huaraz contiene paginas preliminares y IX capítulos. En el capítulo I se determina el problema que consiste en el aumento de la inseguridad ciudadana en el área urbana del distrito de Huaraz. En el capítulo II se investigó sobre los antecedentes internacional, nacional y local, así como las teorías que sustentan el presente trabajo. En el capítulo III se define los materiales y métodos utilizados. En el capítulo IV se realiza el análisis y diagnóstico de la situación actual de seguridad ciudadana en el área de estudio. En el capítulo V se plantea el diseño del sistema de televigilancia. En los capítulos VI y VII se plantea la construcción e implementación del sistema de televigilancia. En el capítulo VIII se expone los resultados obtenidos en la investigación. En el capítulo IX se discute los resultados. Finalmente se presenta las conclusiones y recomendaciones.

Se espera que la presente Tesis sea revisada y sustentada para su aprobación.

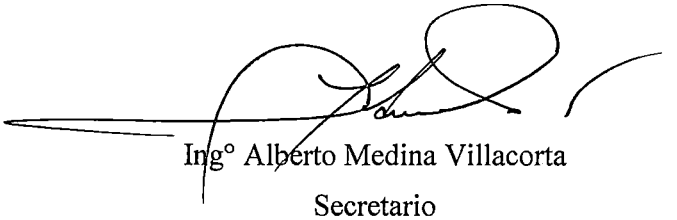
Atentamente,

Dante Jhosep De La Cruz Maguiña

HOJA DE VISTO BUENO

Ing° Rolando Salazar Cáceres

Presidente



Ing° Alberto Medina Villacorta

Secretario

Ing° Luis Alvarado Cáceres

Vocal

RESUMEN

El objetivo es plantear el diseño de sistema de televigilancia con tecnología de fibra óptica para fines de seguridad ciudadana en el 2014, precisando la situación actual y los recursos tecnológicos para este fin, en el distrito de Huaraz. La investigación es de tipo no experimental.

El diseño de la investigación es descriptivo simple. El procedimiento consistió en: definir la población demandante de un servicio de seguridad en óptimas condiciones. Se elaboró el cuadro donde se muestra los puntos álgidos de la delincuencia en el área urbana de Huaraz. Se tuvo en cuenta los actos delictivos y delitos que motivan la inseguridad ciudadana. Se consideró a la población del distrito de Huaraz, urbano y urbano marginal.

Como resultado del análisis causa-efecto, el problema central se define como, insuficiente capacidad de monitoreo, supervisión y control de la seguridad del ciudadano en el distrito de Huaraz y como efecto el atraso en el desarrollo social, cultural, económico y educativo de la Provincia de Huaraz. .

La investigación pretende facilitar el trabajo de los entes de seguridad ciudadana, quedando en propuesta para ser presentada para su implementación.

Palabras clave: sistema de televigilancia, seguridad ciudadana, banda ancha, fibra óptica.

ABSTRACT

The objective is to present the design of remote monitoring system with fiber optic technology for public safety purposes in 2014, specifying the current situation and technological resources for this purpose, in the district of Huaraz. The research is not experimental.

The research design is simple descriptive. The procedure consisted of: defining the applicant of a security service optimally population. Table where crime hotspots shown in the urban area of Huaraz was developed. Criminal acts and crimes motivated insecurity was taken into account. It was considered a district population of Huaraz, urban and urban marginal.

As a result of cause-effect analysis, the central problem is defined as insufficient capacity for monitoring, supervision and control of the safety of citizens in the district of Huaraz and the effect of the delay in the social, cultural, economic and educational development province of Huaraz. .

The research aims to facilitate the work of public safety entities, being in proposal to be submitted for implementation.

Key words: telemonitoring system, public safety, broadband, fiber optic.

ÍNDICE GENERAL

CAPÍTULO I: GENERALIDADES

1.1 Realidad problemática

El distrito de Huaraz en el transcurso de los últimos años ha crecido en forma acelerada, en ese crecimiento ha aumentado la delincuencia, inseguridad, violencia familiar, pandillaje, alcoholismo, etc., por ello para hacerle frente a la inseguridad ciudadana se creó la jefatura de seguridad ciudadana.

En este ámbito es que se realiza una serie de vacíos y deficiencias de la inseguridad ciudadana, motivada por la inefectividad de los agentes de seguridad, tales como: los agentes de seguridad ciudadana, los responsables de las instituciones públicas y privadas que no participan activamente en preservar la tranquilidad pública y lucha frontal contra el incremento delincuencial, que cada vez es más creciente; a pesar que existen normas legales establecidas desde el nivel constitucional, las leyes y reglamentos, que no se aplican con la debida celeridad.

Estos hechos generan la inestabilidad de una vida democrática adecuada, en un Estado de Derecho, en que se observa una debilidad de materia de seguridad ciudadana, en que los agentes no realicen una labor efectiva contra la criminalidad y la delincuencia, que afecta directamente a la tranquilidad ciudadana, de las familias y las instituciones públicas y privadas, en el proceso de desarrollo sostenible necesario, en los momentos actuales.

Asimismo los gobiernos locales y regionales mediante la prestación del servicio de seguridad ciudadana han tratado de fortalecer paulatinamente sus divisiones de Serenazgo con el objetivo de incrementar la presencia de autoridad en las calles y contribuir a atacar el problema de inseguridad, sin embargo aún las acciones y políticas tomadas están siendo insuficientes dado que los resultados se mantienen y no se ven avances al respecto.

En los últimos años el índice delincuencial y violencia se ha incrementado significativamente en el distrito de Huaraz, generándose la necesidad imperiosa de adoptar medidas orientadas a optimizar el servicio de seguridad ciudadana, ampliando su cobertura y mejorando la prestación de servicio.

En la actualidad la Municipalidad Provincial de Huaraz, no dispone de un sistema electrónico de televigilancia en el área urbana, lo que coadyuva el aumento de la inseguridad ciudadana.

En este contexto, se tiene la necesidad de plantear un sistema de televigilancia en la zona urbana del distrito de Huaraz para garantizar su seguridad, lo cual no solo servirá para la seguridad sino que también se podría utilizar para la promoción turística del mismo mediante internet con imágenes en vivo, asimismo disminuir los problemas que afectan la seguridad ciudadana.

1.2 Enunciado del problema

¿Existe inseguridad ciudadana en el área urbana del distrito de Huaraz, por el aumento de delitos cometidos en el 2014?

1.3 Hipótesis

Con la instalación de un sistema de televigilancia que utiliza fibra óptica se mejorará los niveles de seguridad ciudadana en el área urbana del distrito de Huaraz en el 2014.

1.4 Objetivos

1.4.1 Objetivo general

Proponer el sistema de televigilancia utilizando fibra óptica con fines de seguridad ciudadana en el área urbana del distrito de Huaraz en el 2014.

1.4.2 Objetivo especifico

1.4.2.1 Levantar información sobre los sucesos de inseguridad existente en el área urbana del distrito de Huaraz, obteniendo el mapa del delito.

1.4.2.2 Determinar los requerimientos de las tecnologías de banda ancha a ser utilizados para el diseño del sistema de televigilancia, que sirva para minimizar la inseguridad en el área urbana del distrito de Huaraz.

1.4.2.3 Realizar la evaluación económica de las alternativas estudiadas, a fin de ofrecer la mejor solución técnica económica.

1.5 Justificación

El sistema de televigilancia utilizando fibra óptica con fines de seguridad ciudadana en el distrito de Huaraz, se justifica por:

1.5.1 Justificación Operativa

El sistema de televigilancia utilizando la tecnología de fibra óptica mejorara las acciones prevención, protección y estrategias tácticas para la seguridad ciudadana del personal de Serenazgo del área urbano y urbano marginal del distrito de Huaraz, porque permitirá visualizar en tiempo real los diversos delitos o acciones delincuenciales que se van registrando.

1.5.2 Justificación Técnica

La tecnología de fibra óptica en todo el mundo está en constante evolución, y en el área de seguridad se utiliza con mayor frecuencia debido a que su mayor parte de componentes son electrónicos.

La banda ancha en la red, tiene una elevada capacidad para transportar información que incide en la velocidad de transmisión de ésta. Así entonces, es la transmisión de datos simétricos por la cual se envían simultáneamente varias canales de información, con el objeto de incrementar la velocidad de transmisión efectiva.

Los sistemas de comunicación óptica de alta capacidad han posibilitado la gran difusión de las comunicaciones a escala planetaria, tanto desde el punto de vista de diseño del sistema como de sus componentes. Las diferentes técnicas de amplificación óptica y el enorme impacto que estas han tenido en el incremento de la capacidad de transporte de la información de los sistemas modernos de comunicación.

1.5.3 Justificación Económica

Al implementarse el presente proyecto la Municipalidad Provincial de Huaraz, tendrá una disminución significativa por el lado de gastos de operación del personal de Serenazgo, por el menor uso de personal y gastos de combustibles de los vehículos.

1.5.4 Justificación Legal

La propuesta del sistema de televigilancia para fines de seguridad ciudadana se se sustenta en el siguiente marco legal y normativo:

Constitución Política

- Art. 197. "Las municipalidades brindan servicios de seguridad ciudadana, con la cooperación de la Policía Nacional del Perú, conforme a ley".

Leyes

- Ley 27972 Ley Orgánica de municipalidades. Art.85: Las municipalidades brindan servicios de seguridad ciudadana.
- Ley N° 27933 Ley del Sistema Nacional de Seguridad Ciudadana.

Normatividad

- Decreto Supremo N° 012-2003-IN del 07 Oct2003 que aprueba el Reglamento de la Ley del Sistema Nacional de Seguridad Ciudadana.
- Decreto Supremo N° 003-IN del 30 Jun2003 Determina que la Secretaría Técnica – CONASEC es un órgano técnico, ejecutivo y de coordinación, dependiente de la Alta Dirección del MININTER, que por la naturaleza de la función realiza labores de asesoramiento y de ejecución.
- Plan Nacional del Sistema de Seguridad Ciudadana 2013 y su Reglamento (D.S. N° 012-2003-IN).
- Plan Local de Seguridad Ciudadana 2013 de la Municipalidad Distrital de Huaraz.

1.5.5 Justificación Social

El uso del sistema de televigilancia contribuirá combatir la delincuencia de una forma frontal con el anhelo de que el distrito de Huaraz sea un ejemplo modelo en lo que se refiere a la seguridad de las personas, viviendas, locales, así como las que están de visita.

1.5.6 Justificación Profesional

Con el desarrollo de este sistema de televigilancia el tesista está adquiriendo experiencia y conocimiento en el uso de tecnologías de almacenamiento de información (video), fibra óptica y de video cámaras con fines de seguridad ciudadana.

1.6 Limitaciones

La limitación existe por cuanto, este trabajo de investigación, deberá ser avalado por las autoridades de la Municipalidad Provincial de Huaraz para que tomen la decisión de su implementación, para mejorar los bajos niveles de seguridad ciudadana.

1.7 Descripción y sustentación de la solución

Para lograr la instalar el sistema de televigilancia utilizando fibra óptica con fines de seguridad ciudadana en el área urbana del distrito de Huaraz en el 2014, se deberá seguir los siguientes procesos:

- Levantar información de los sucesos de inseguridad en el área urbana del distrito de Huaraz, obteniendo el mapa del delito.
- Determinar los requerimientos de las tecnologías de banda ancha utilizando fibra óptica para el diseño del sistema de televigilancia.
- Realizar la evaluación económica de las alternativas estudiadas, a fin de ofrecer la mejor solución técnica económica.
- Diseñar el sistema de televigilancia utilizando tecnología de fibra óptica en el área urbana del distrito de Huaraz.

CAPÍTULO II: MARCO TEÓRICO

2.1 Antecedentes

A nivel internacional

(Herrera 2012), en su tesis "*Diseño de una red de televigilancia inalámbrica para los equipos que conforman el sistema que ayuda a la navegación aérea en el aeropuerto palo negro de bucaramanga*"... nos define el término Televigilancia como un conjunto de sistemas que permiten la supervisión y el control desde una central de monitoreo, de una o varias instalaciones técnicamente aisladas o distribuidas geográficamente.

(Garcia 1999), en su tesis "*Sistema de comunicaciones por medio de fibra óptica*", indica que en la era moderna todo sistema de comunicación está ligado a la fibra óptica, la cual permite mejorar de gran manera la velocidad.

(Prince 2010), en su investigación "*Las TIC y su relación con la seguridad ciudadana: un marco de análisis a la problemática*" hace referencia que la aplicación de la TIC, y de los diferentes elementos de la compleja sociedad del conocimiento no son un "combo" que se adquiere en el mercado. De todas maneras requiere de una adecuada planificación estratégica previa en la cual se realice la propia situación de las fuerzas de seguridad. También no debemos olvidar que la finalidad de la seguridad ciudadana no es la mantención de un orden sino brindar la posibilidad real del ejercicio pleno de los derechos a los propios ciudadanos construyendo una sociedad cada vez más libre y justa.

(Lledo Real 2003) En su Tesis sobre: "*La seguridad ciudadana como condición de la democracia*". Un enfoque filosófico, existen en la tesis varias líneas argumentales que pretenden concluir en la idea de que la seguridad ciudadana es una condición necesaria para el desarrollo de la Democracia. En primer lugar porque se parte del principio de que sin seguridad, la libertad no existe, y sin

libertad, la Democracia carece de sentido. Para llegar a esta conclusión, se analiza el concepto de seguridad integral, en sus vertientes objetiva y subjetiva; individual y colectiva; pública y privada; interior y exterior; nacional e internacional diferenciándola de otros conceptos, con los que a veces se confunde, como orden público, o sistemas de tolerancia cero ante los delitos. En este análisis surgen una serie de aparentes contradicciones, como el binomio liberta-seguridad; derecho a la seguridad o seguridad de los derechos; prevención o represión de los delitos; el ciudadano como sujeto u objeto de la seguridad; el papel de las Fuerzas y Cuerpos de Seguridad como servidores del Estado o de los ciudadanos etc., que se van analizando en los distintos capítulos. También merece un estudio el propio concepto de Democracia, no sólo en su versión representativa, sino especialmente participativa, llegando a la conclusión de que sin el compromiso político de los ciudadanos, y su participación activa en las políticas públicas, la seguridad ciudadana en su sentido integral no es posible, y por lo tanto, los gobernantes carecen de legitimidad, aunque sean legales, al no contar con la confianza de los ciudadanos. Por último, se esboza un proyecto de organización de la seguridad pública de modo que pueda constituir una garantía de calidad de vida para los ciudadanos.

(Alcino 2005), En su Tesis realizada en la ciudad de Buenos Aires, Argentina, sobre "*La Responsabilidad de la familia y la Escuela frente al problema del pandillaje*", arribó a los siguientes resultados: estudió a una muestra de 420, con un diseño transversal-correlacional; el 89% mostraba hostilidad hacia la policía, el 13% no le temía a la policía y el 7% no respondió; el 90% respondieron "sólo los inocentes trabajan y el 58% no tenían miedo a las instituciones correccionales y el 80% opinó que las comisiones de Seguridad Ciudadana eran inoperantes frente a la fuerza de la pandilla.

(Chipix Notz 2009), En su Tesis sobre: "*Participación de actores sociales en espacios de seguridad ciudadana y prevención del delito*". La seguridad ciudadana en Guatemala, al igual que en los demás países latinoamericanos, principalmente del cono sur, se remontan a la década de los noventa, cuando los fenómenos

políticos, económicos y sociales mundiales contribuyeron a la finalización de guerras civiles, la desmilitarización de sociedades, la aparición y/o fortalecimiento de los sistemas democráticos en muchas sociedades de la región, todo esto permitió la progresiva refundación del pensamiento y actitud social con relación a la prestación de algunos servicios básicos históricamente considerados de competencia exclusiva a los Estados a través de sus gobiernos.

(Guaycha 2005), en la Tesis realizado sobre los países de América Latina, en "*Inseguridad Ciudadana*", concluye que América Latina es la región del mundo de mayor índice de criminalidad. Este índice se mide por la tasa de homicidios ya que es una cifra relativamente fácil de registrar. La criminalidad alta, más de 10 homicidios por cada 100,000 habitantes, se da en las ciudades de El salvador, Guatemala, Otros de criminalidad baja con 0.5 y 5 homicidios por cada 100,000 habitantes como las ciudades de Costa Rica, Chile y Uruguay. Aunque en el Perú el índice de criminalidad es de 12,5 homicidios por cada 100,000 habitantes. Menos que en Brasil que tienen entre 24 y 24.9 homicidios por cada 100,000 habitantes, México que tiene entre 20 y 20,9 homicidios por cada 100,000 habitantes y Colombia que tiene un índice de criminalidad más alto del mundo, con 77 a 77.9 homicidios por cada 100,000 habitantes.

(Carpaneto 2000), en la investigación realizada acerca de "*Las Acciones de los Comités de Prevención y Seguridad Ciudadana en Chile*", informan sobre los resultados obtenidos estudiaron 140 Comités como muestra de estudio, el 98% están conformados por vecinos y usuarios de la comuna; el 91% colaboran con las autoridades municipalidades y carabineros en la prevención de la delincuencia en sus barrios. El 95% de delegados o coordinadores reciben inquietudes de los vecinos y deriva sus problemas al municipio y a los Carabineros. Se percibe un 13% de inseguridad ciudadana en la población.

(Rangel 2009), *"El Delito como factor de Inseguridad ciudadana"* determina: El objeto esencial de la investigación empieza por cifrar y cuantificar el fenómeno delictivo, priorizado por el Instituto, desde una perspectiva objetiva y actual, a partir

de la tipología legal del delito y sus indicadores más destacados, localizándolo territorialmente (la Gran Caracas y a nivel nacional), ubicándolo en el tiempo, concretamente durante el año 2008 y primer semestre del 2009, efectuando el estudio comparativo de lo sucedido entre ellos, valorando su incidencia y efectos, estableciendo sus eventuales cambios favorables a la luz de los factores asociados que positiva y racionalmente sean vinculables al fenómeno delictivo globalmente cuantificado y calificado, y por último, con basamento en todos los elementos indicados y en su naturaleza sistémica, generar Políticas Públicas para erradicar el delito como máximo agente perturbador de la convivencia y seguridad ciudadana.

(Barveito Da Silva s.f.), en el estudio realizado sobre "*Inseguridad Pública en Río de Janeiro*", presenta los siguientes resultados: estudió una muestra de 1,250 elementos de la muestra, con método descriptivo, diseño comparativo-casual, utilizó la Encuesta como instrumento de medición. El 53% de la población percibe que el combate a la delincuencia está gravemente estancado, el 58% afirma que las autoridades están mostrando cierta timidez a hechos de violencia; los Comités de Seguridad ciudadana en sólo 31% están activas, el 25% relativamente activas y el 44% inactivas o inoperantes, 2,520 hogares fueron victimizados en el período 2005-2006 con más de un delito; siendo el 21.7% a 31.3% de hogares re victimizados.

(Patiño Mayer 1999), en su artículo "*Crisis sistémica de la seguridad ciudadana*". El autor realiza un profundo análisis de la crisis de seguridad que atraviesa la Argentina, en especial la región metropolitana de Buenos Aires, abordando la problemática desde la situación de las fuerzas policiales, el sistema penitenciario y el poder judicial hasta la marginalidad y el debilitamiento de la convivencia social. Advierte sobre la necesidad de evitar los planteos oportunistas y de responder con realismo y seriedad a una crisis sistémica de raíces profundas y complejas.

A nivel nacional

(Chuquitarco 2009), en su tesis "*Técnicas y tecnologías aplicadas en fibra óptica*" en su estudio nos menciona que los métodos ópticos y eléctricos basados en multiplexación en el dominio del tiempo (TDM) y en el dominio de la longitud de onda o frecuencia (WDM/FDM), han sido extensamente empleados y desarrollados. Están ampliamente difundidos, sin embargo los elevados requerimientos de TDM en velocidad de procesamiento, así como en sincronización de red. Por otro lado, WDM/FDM requiere sistemas caros, precisos y de difícil estabilización. Las redes de acceso que utilizan la técnica de acceso múltiple por división de código (OCDMA) han sido ampliamente investigadas dada su naturaleza de acceso asíncrono y multiusuario, las altas velocidades soportadas, su escalabilidad y seguridad. El presente trabajo analiza las tecnologías de acceso utilizadas en fibra óptica para lo cual se ha organizado de la siguiente forma: El primer capítulo consta de una introducción teórica general de la comunicación por fibra óptica. En el segundo capítulo se presenta el estudio de las técnicas TDMA y WDMA utilizadas en la fibra óptica así como un análisis de las ventajas y limitaciones que cada una de ellas presenta; se realiza una introducción a la técnica OCDMA. El tercer capítulo consta del estudio de la evolución de la técnica de acceso múltiple por división de código óptico, se analiza las técnicas utilizadas en FE-OCDMA que se basan en códigos 1D y WH-TS-OCDMA basadas en códigos 2D. En el cuarto capítulo se calcula y analiza el desempeño de las técnicas basadas en códigos 1D y 2D, estableciendo como parámetros del desempeño la relación señal a ruido (BER en sistemas digitales) en función número de usuario multiplexados; se presenta y analiza sistemas prácticos llevados a experimentación y las posibles oportunidades en las redes de las empresas operadoras del Perú.

(Quezada Bringas 2006), Secretaria Técnico de CONASEC, en su investigación sobre *"Planes de Seguridad"*, sostiene que sólo cuatro comunas de Lima Metropolitana cumplieron con organizar el Comité de Seguridad Ciudadana, Planificar e informan al órgano Superior. La mayoría de funcionarios maneja distintos criterios para elaborar el diagnóstico distrital y provincial, relacionado con

sus principales problemas. La Guía de Seguridad Ciudadana servirá de base para que los distritos del Perú puedan de una forma homogénea, llevar a cabo sus planes y remitirlos oportunamente. Faltan todavía instalar 350 Comités distritales que es un mínimo significativo.

(Álvarez 2006), en su estudio sobre *"criminalidad en Lima"*, propone, que para reducir la incidencia delictiva en el Perú, se debe establecer las siguientes proyecciones en el área de prevención para los tres próximos años: Reducir en un 90% la micro-comercialización y consumo de drogas, a través de programas culturales y deportivos que impliquen participación y colaboración de los jóvenes. Reducir en un 80% el robo a domicilio, de vehículos así como de autopartes, a través de la participación ciudadana con la organización de las Juntas Vecinales de Seguridad Ciudadana. Reducir en 70% el problema de la violencia familiar, incidiendo en la revalorización del rol de la mujer en el seno familiar y la decidida participación en las Instituciones Educativas. Reducir en 70% el pandillaje juvenil, con la participación de jóvenes, mediante la escuela de valores, difundiendo el deporte y la cultura, basado en valores, la ética y moral

(Salazar y Ruiz 2004), En su investigación sobre: *"La seguridad ciudadana forma parte de las preocupaciones cotidianas y del debate público en los países de la región"*. En el Perú, la percepción de inseguridad está creciendo y requiere de políticas que den respuestas adecuadas. En este contexto, los problemas de seguridad ciudadana, hoy en día, forman parte de la agenda pública peruana y por lo tanto de las políticas de Estado del Acuerdo Nacional y de la Agenda Priorizada Parlamentaria. Seguridad ciudadana está relacionado con los derechos humanos vinculados a la vida, la integridad física, psíquica y moral de las personas y su patrimonio; responde a la necesidad de estar libres de temor y amenazas y está consignado en Constituciones y leyes, así como en el Pacto Internacional de Derechos Civiles y Políticos de las Naciones Unidas, y, en el caso de América Latina, en la Declaración de la OEA en Montrouis.

(Dávila Altamirano 2010), en su tesis "*Las juntas vecinales en el fortalecimiento de la seguridad ciudadana del distrito de San Juan de Lurigancho, del 2006 hasta el 2009*". El presente estudio tiene por objetivo analizar cómo impacta la participación de las juntas vecinales en las acciones de seguridad ciudadana iniciadas por la Municipalidad y las comisarías del distrito de San Juan de Lurigancho entre el 2006 hasta el 2009. La seguridad ciudadana es un concepto novedoso en América Latina. Esta noción nace cuando se agota la Doctrina de Seguridad Nacional (DNS) que llevaron a la práctica los gobiernos militares de la década de 1970. La DSN entendía la seguridad como protección de los "intereses nacionales" frente a los "enemigos" del Estado, quienes, en la práctica, eran los opositores a la dictadura militar. En medio de las transiciones democráticas, la seguridad ciudadana aparece como un derecho de todas las personas a desarrollarse y cuyas políticas deberán garantizar la convivencia entre los ciudadanos. Así, los objetivos de la seguridad nacional se agotan y se establecen nuevos puntos de debate respecto de la seguridad en y para la democracia.

(Chávez Hidalgo 2012), en su tesis "*La estructura y funciones de la Policía Nacional del Perú bajo un enfoque moderno*". El problema principal en el proyecto de investigación está dado por el proceso de globalización mundial, que acarrea una mayor integración económica, política, social y cultural de la sociedad peruana en el concierto mundial de las naciones, con un incremento de la movilización de los personas, de las transacciones comerciales y del intercambio de bienes y dinero, procesos que tienen un fuerte impacto en la sociedad peruana, la misma que aún no logra adecuar sus estructuras sociales al proceso mundial de globalización y modernización mundiales La Policía Nacional a su vez, en el marco de la ley orgánica N° 27238, no ha logrado renovar e innovar sus estructuras organizativas y no ha definido sus funciones y su operatividad técnica y profesional para atender las nuevas demandas de la sociedad respecto a garantizar el orden público y la seguridad ciudadana.

A nivel local

(Alvarado Cáceres 2014), en su proyecto de ingeniería *"Mejoramiento e instalación de video cámaras para el servicio de seguridad ciudadana de la ciudad de Huaraz"*. El presente estudio nos plantea una opción y oportunidad de cambio para Huaraz en lo que se refiere a la seguridad ciudadana dado por el aumento acelerado, dado a este crecimiento ha aumentado la delincuencia, inseguridad, violencia familiar, pandillaje, alcoholismo, etc. Concluyendo que es necesario un equipamiento de un sistema de video vigilancia para así salvaguardar la tranquilidad de los ciudadanos.

(Peréz 2012), en su tesis *"La inoperancia de los agentes de seguridad ciudadana como factor de inseguridad incide en el incremento delincuencial en la ciudad de Huaraz durante el período 2006-2010"* en su estudio hace referencia al incremento de la delincuencia y la criminalidad que son hechos sociales a nivel internaciones, nacional y regional que no solo son un problema policial y judicial sino también del contexto económico, social y cultural tanto de la Provincia de Huaraz como así mismo del País.

2.2 Teorías que sustentan el trabajo

2.2.1 Teoría general de sistemas

De acuerdo a (Murillo Alfaro 1999) Jefe del Instituto Nacional de Estadística e informática nos hace referencia sobre la "*Teoría general de sistemas*", viene a ser el resultado de gran parte del movimiento de investigación general de los sistemas, constituyendo un conglomerado de principios e ideas que han establecido un grado superior de orden y comprensión científicos, en muchos campos del conocimiento. La moderna investigación de los sistemas puede servir de base a un marco más adecuado para hacer justicia a las complejidades y propiedades dinámicas de los sistemas.

Desde hace algún tiempo hemos sido partícipes del surgimiento de "sistemas" como concepto clave en la investigación científica. Los sistemas se estudian desde hace siglos, pero algo más se ha agregado. La inclinación a estudiar sistemas como entidades, más que como conglomerado de partes, es conveniente para analizar fenómenos estrechamente relacionados y examinar segmentos de la naturaleza cada vez mayores. La indagación de sistemas pretende un esfuerzo cooperativo entre las diversas disciplinas científicas y la ingeniería, sin más interés que lograr una mayor comprensión del conocimiento humano.

La Teoría General de Sistemas puede definirse como:

Una forma ordenada y científica de aproximación y representación del mundo real, y simultáneamente, como una orientación hacia una práctica estimulante para formas de trabajo transdisciplinario.

La Teoría General de Sistemas (TGS) se distingue por su perspectiva integradora, donde se considera importante la interacción y los conjuntos que a partir de ella brotan. Gracias a la práctica, la TGS crea un ambiente

ideal para la socialización e intercambio de información entre especialistas y especialidades. De acuerdo a los aspectos consideraciones anteriores, la TGS es un ejemplo de perspectiva científica.

La Teoría General de Sistemas también es vista como una teoría matemática convencional, un tipo de pensamiento, una ordenación de acuerdo a niveles de teorías de sistemas con generalidad creciente.

La Teoría General de Sistemas es la historia de una filosofía, una metodología de análisis, el estudio de la realidad y el desarrollo modelos, a partir de los cuales se puede intentar una aproximación gradual en cuanto a la percepción de una parte de esa globalidad que es el universo, configurando un modelo del mismo no aislado del resto al que llamaremos sistema.

Todos los sistemas comprendidos de esta manera por un individuo dan origen a un modelo del universo, una visión integral cuya clave justifica plenamente cualquier parte de la creación, por pequeña que sea o que podamos considerar, que juega un papel y no puede ser estudiada y captada su realidad última en un contexto aislado.

La ciencia de los sistemas o sistémica es su ejemplo, es decir, su realización práctica, y su puesta en obra es también un ejercicio de humildad, ya que un bien sistémico ha de partir del reconocimiento de su propia limitación y de la necesidad de colaborar con otros, para llegar a captar la realidad en la forma más adecuada para los fines propuestos.

Surgimiento de la Teoría General de Sistemas

La Teoría General de Sistemas, idea desarrollada por L. Von Bertalanffy en 1930, fue un tema nuevo que causó impacto en la comunidad científica, lo que motivó el interés de muchos para su investigación, motivo por el cual un grupo conformado sólo por personas que tenían inquietudes similares

formaron la Sociedad para la Investigación de Sistemas Generales conjuntamente con Anatol Rapoport, Kennet Boulding, Ralph Gerard y otros en 1954.

No pasó mucho tiempo, para que el investigador y estudioso Kennet Boulding realice una clasificación sobre cinco prioridades básicas de la Teoría General de Sistemas. Según la investigación realizada, podemos llamar a estas prioridades: postulados, presuposiciones o juicios de valor.

a. Es preferible que exista una seguridad en el orden, regularidad y carencia de azar, para no encontrarnos en la incertidumbre y esperar un estado fortuito.

b. El orden del mundo empírico hace de éste un buen lugar, que sea motivante, y que origine mucha atracción con respecto a los teóricos de los sistemas.

c. El mundo externo y práctico mantiene un orden en el ordenamiento, es decir un orden en segundo plano: una ley de leyes.

d. El orden se mantiene con la matemática y el análisis cuantitativo, que son herramientas de un valor.

e. El tratar de encontrar la ley y el orden juntos hace que sea necesaria la búsqueda de referencias prácticas.

2.2.2 Teoría de las Telecomunicaciones

De acuerdo a (Sáenz Peña s.f.), en su informe "Teoría de las Telecomunicaciones", Las comunicaciones digitales están desplazando definitivamente a las comunicaciones analógicas. Basta repasar algunos de los sistemas de comunicaciones que nos rodean a diario para ver que quedan muy pocos que sean analógicos.

Podemos nombrar a las transmisiones de radio AM y FM, por algunos pocos años más la televisión (que ya está siendo desplazada por la TV digital de alta definición) y las líneas telefónicas de abonado. Y aun así en este último caso existen los servicios ISDN (en español RDSI, Red Digital de Servicios Integrados) en donde la comunicación que llega al aparato del abonado es íntegramente digital. También la telefonía celular analógica está emigrando definitivamente hacia la tecnología digital. Y la telefonía fija tradicional, analógica, (conocida en la jerga como PSTN, Public Switched Telephone Network, es decir, Red Telefónica Pública Conmutada) poco a poco está comenzando a ser desplazada por la telefonía IP (VoIP, Voice Over IP, es decir, Voz Sobre IP).

El resto de las comunicaciones son digitales. Enlaces satelitales, troncales telefónicas, redes de computadoras, Internet, telefonía celular, videoconferencia, telemetría y hasta los CDs de música que también almacenan la información en forma digital (obviamente, la reproducción del sonido en el parlante es en forma analógica). También los sistemas de señalización en telefonía son digitales, como el SS7 (Sistema de Señalización N° 7).

La característica principal de un sistema de comunicaciones digitales es que, durante un intervalo de tiempo finito transmite una forma de onda preestablecida, tomada de un conjunto finito de formas de onda posibles. Por ejemplo, un conjunto formado por dos formas de onda: un pulso de 5 volts de amplitud y 1 microsegundo de duración y otro pulso de –5 volts de amplitud y 1 microsegundo de duración. Esto contrasta con los sistemas de comunicaciones analógicos que transmiten una señal continua en el tiempo. Es decir, una variedad infinita de formas de onda con una resolución también infinita.

¿Por qué las comunicaciones van emigrando definitivamente hacia los sistemas Digitales? Hay varias razones. Una de ellas es la facilidad con que se regeneran las señales digitales, comparadas con las analógicas. La forma de onda que envía un transmisor se va degradando a lo largo del canal de comunicación (sea éste

de cualquier medio: fibra óptica, aire, cable coaxial, etc.). Esto se debe por un lado a que los medios de comunicación y los circuitos asociados no son lineales, y por otro lado a los efectos del ruido eléctrico indeseado que aparece en cualquier medio. Estos dos mecanismos distorsionan la señal transmitida. Sin embargo, en el caso de las comunicaciones digitales, a pesar de que el ruido y las alinealidades también degradan la señal, es mucho más fácil reconstruir la señal degradada ya que la transmisión parte de un conjunto de señales discreto y finito.

2.2.3 Antecedentes del modelo ISO/OSI

Gracias a la tesis de (Cuaquentzi Cruz, Lechuga Barrientos y Nieto Patlán 2008), podemos ver el antecedente del modelo OSI y hace referencia lo siguiente: En 1979, ISO (Organización Internacional para la Estandarización) definió su modelo de arquitectura de red OSI (Interconexión de sistemas abiertos). Este modelo fue adoptado en 1980 por el CCITT (Comité Consultivo Internacional de Telefonía y Telegrafía) en su recomendación X.200. La comunicación de datos comprende 2 aspectos principales:

- El transporte: involucra todas las funciones relacionadas con la transferencia de datos entre dos usuarios.
- La manipulación de datos: los datos deben ser liberados en una forma inteligible. En algunos casos los datos deben ser convertidos.

Capas del modelo ISO/OSI

Las redes de computadoras, proveen al usuario de una serie de servicios, e internamente poseen funciones. La cuales son realizadas por las capas o niveles de la arquitectura que posee el tipo de red. Las arquitecturas de las redes tienen una serie de capas superpuestas, una encima de otra, en la que cada una desempeña su función.

Las funciones y características de las capas son las siguientes:

- Permiten fraccionar el desarrollo del protocolo que usa.
- Las capas facilitan el entendimiento del funcionamiento global de un protocolo.
- Facilitan las compatibilidades, tanto de software como de hardware de los distintos sistemas conectados.
- La arquitectura o estructuras de capas son flexibles a la hora de modificarlas.

CAPA FÍSICA

Es responsable del transporte de bits. Dependiendo del tipo de enlace físico los bits se representan de una manera en la que puedan ser transportados a través del medio.

Define voltajes, tiempo de duración de los pulsos, el número de patas que tiene el conector de la interface y sus funciones, la forma de establecer la conexión inicial y de interrumpirla, etc.

Generalmente será un cable aunque no se descarta cualquier otro medio de transmisión como ondas o enlaces vía satélite.

CAPA DE ENLACE DE DATOS

- Asegura que la información sea transmitida sin errores entre nodos adyacentes de la red sin importar el medio de transmisión utilizado.
- Maneja tramas de datos como unidad de transmisión de datos.
- Crea los límites de la trama.
- Resuelve problemas de daño, pérdida o duplicidad de tramas.
- Participa en la regulación de flujo de tramas entre los nodos.

CAPA DE RED

Define la forma en que un mensaje se transmite a través de distintos tipos de redes hasta llegar a su destino. El protocolo principal de esta capa es el Protocolo de Internet (IP) aunque también se encuentran a este nivel los protocolos ARP, ICMP e IGMP.

- Se encarga de que los datos sean enviados a su correcto destino, determinando la ruta de transmisión.
- La unidad de transmisión de datos en esta capa es el paquete de datos.
- Participa en el control de congestión de la red.
- Puede llevar la contabilidad del número de paquetes o bits que se enviaron a cada cliente para cuestiones de facturación.
- Puede resolver problemas de interconexión de redes heterogéneas.

CAPA DE TRANSPORTE

La capa de transporte (protocolos TCP y UDP) ya no se preocupa de la ruta que siguen los mensajes hasta llegar a su destino. Sencillamente, considera que la comunicación extremo a extremo está establecida y la utiliza. Además añade la noción de puertos, como se tratará más adelante.

- Acepta los datos de la capa de sesión, los divide, siempre que sea necesario, en unidades más pequeñas (la capa de red generalmente pone un límite en el tamaño de los mensajes que acepta), los pasa a la capa de red y asegura que todos ellos lleguen correctamente a su destino.
- A partir de la capa de red, las 4 capas superiores restantes manejan mensajes como unidad de transmisión de datos.
- Detecta fallas en la red y realiza las acciones correspondientes.

- Solicita el establecimiento de un nuevo enlace, en el caso de que falle un enlace de la red.

CAPA DE SESIÓN

- Es un tipo de sistema operativo para la comunicación de datos.
- Permite que los usuarios de diferentes computadoras puedan establecer sesiones entre ellos.
- Realiza el control del diálogo.
- Lleva a cabo la función de sincronización, es decir, inserta puntos de verificación en el flujo de datos, con objeto de que solamente tengan que retransmitirse los datos que se encuentren en seguida del último punto de verificación cuando se reanuda el servicio después de una caída de la red.

CAPA DE PRESENTACIÓN

- Permite a dispositivos que intercambian información, entenderse o interpretarse entre ellos independientemente de la codificación que utilicen para los caracteres, por ejemplo, código ASCII (American Standard Code for Information Interchange; Código Estadounidense Estándar para el Intercambio de Información) y EBCDIC (Extended Bynary Coded Decimal Interchange Code; Código Extendido de Binario Codificado Decimal).
- Convierte los datos transmitidos a una forma inteligible para el dispositivo terminal.
- Maneja aspectos de representación de la información, por ejemplo: la compresión de datos y la criptografía.

CAPA DE APLICACIÓN

Proporciona los distintos servicios de Internet: correo electrónico, páginas Web, FTP, TELNET.

Contiene una variedad de protocolos que hacen posible ofrecer una serie de aplicaciones al usuario final, por ejemplo:

- Correo electrónico.
- Transferencia de archivos.
- Terminal virtual (telnet).
- Directorio electrónico.

2.2.4 Seguridad Ciudadana

Gracias al aporte de (Wikipedia s.f.) nos dice que La seguridad ciudadana es la acción integrada que desarrolla el Estado, con la colaboración de la ciudadanía y de otras organizaciones de bien público, destinada a asegurar su convivencia pacífica, la erradicación de la violencia, la utilización pacífica y ordenada de vías y de espacios públicos y, en general, evitar la comisión de delitos y faltas contra las personas y sus bienes.

En los países hispanohablantes hay ocasiones en las que se prefiere usar términos como "orden público" o "seguridad de los habitantes" en vez de "seguridad ciudadana" o "seguridad nacional", por motivos históricos que dependen de cada país.

En líneas generales, por "seguridad ciudadana" deben entenderse el conjunto de acciones democráticas en pro de la seguridad de los habitantes y de sus bienes, y ajustadas al derecho de cada país. De hecho, el reto actual es armonizar el ejercicio de los derechos humanos de cada uno con las distintas políticas en materia de seguridad ciudadana de los estados. Por ejemplo, la Organización de los Estados Americanos plantea que en ocasiones se aplican políticas que se han demostrado ineficaces, como por ejemplo el aumento de las penas, la reducción de garantías procesales, o medidas para aplicar el derecho penal a menores de edad; que pueden derivar en movimientos paramilitares o parapoliciales

"milicias de autodefensa" cuando el Estado no es capaz de reaccionar de una forma eficaz ante la violencia y el delito, complicando la situación.

Inoperancia de los agentes de seguridad ciudadana

Conjunto de representantes de las distintas instituciones que no producen efectos positivos en las actividades de seguridad ciudadana que constituyen un problema en la solución del problema delincuencial.

Es un secreto a voces que los destacamentos policiales hace mucho tiempo que no cumplen con la función para la cual fueron creados. En medio de tantos actos delincuenciales, lo mismo que el incremento de casos de riñas, que ya han pasado a ser parte de nuestra cotidianidad, en muchas ocasiones la ciudadanía se siente desprotegida cuando tiene que acudir a uno de esos recintos.

La principal falla de esas dependencias de la Policía Nacional radica en que no disponen, en su inmensa mayoría, del número de efectivos que debieran tener, siempre guardando la proporción con el número de habitantes de los lugares donde operan.

Cuando ocurre un hecho que amerite la presencia de agentes policiales de un destacamento en determinado sector, la excusa es que no hay disponibilidad, o en última instancia que hay que irlos a buscar en un vehículo que nada tiene que ver con la institución llamada a resguardar el orden público.

Tan solo con lo expuesto más arriba se da uno cuenta que los destacamentos de por sí son inoperantes. Estos no solo pueden operar para recibir presos que lleve una patrulla policial, ya sea que los traslade en vehículo, o a pie.

Pero más inoperante aún son esas dependencias cuando uno se entera que hay comandantes y subalternos que se confabulan con lo peor que pueda existir en una determinada comunidad, como son los casos de los cabecillas de puntos de venta de drogas, dueños de bancas de apuestas, de discotecas, de centros de prostitución, etc., etc. La mayor parte de los destacamentos tiene de comandante

a un teniente, o en su defecto un sargento. En menor cantidad los hay que son comandados por un capitán.

Problemas de la seguridad ciudadana

Entre los problemas que más afectan a los vecinos están el hurto, es decir, el robo sin violencia, nos referimos a los arrebatos en las calles, mercados, paraderos de micros. También están el robo a domicilio, el pandillaje, la micro-comercialización de drogas con la consecuencia de la drogadicción y el alcoholismo que fomentan conductas violentas en la calle y en el hogar.

No en todos los barrios los problemas son los mismos, no en todos tienen la misma prioridad. Por ejemplo, en un barrio o distrito el problema más agudo puede ser el pandillaje, en otro, los robos a comerciantes y domicilios, en otro, la micro-comercialización de drogas.

Hay muchos factores sociales que contribuyen a que se produzcan este tipo de faltas y delitos menores. Entre ellos, la desocupación de los jóvenes, la falta de trabajo e ingresos en las familias, la falta de organización p ara la seguridad de la comunidad y la escasa coordinación con la Municipalidad y la PNP así como la ausencia de lazos de solidaridad entre vecinos, la escasa presencia policial, la falta de precaución cuando se sale a la calle.

Hay problemas urbanos que conducen a estimular que se produzcan conductas delictivas: la ausencia de iluminación adecuada en las calles, la escasa regulación del funcionamiento y localización de las discotecas, prostíbulos, del transporte público y del comercio ambulatorio. También existen problemas cuando se dejan terrenos baldíos oscuros y sin cercar.

A nivel de la familia existe falta de comunicación con los adolescentes y jóvenes; muchas horas del día los niños y adolescentes están solos y a que sus p adres trabajan y no hay espacios ni centros de recreación y cuidado. La violencia familiar es un factor que contribuye a expulsar a los niños y adolescentes de sus

hogares. Los jóvenes llegan a reproducir en sús comportamientos la violencia que han experimentado en casa.

Si bien existe preocupación por las violaciones sexuales, los asesinatos y los secuestros, cuando se pregunta en las encuestas, estos aparecen con muy baja incidencia en los distintos distritos del país. Esto lo vemos con toda claridad en el cuadro siguiente.

Delincuencia

El ejemplar de (Marchiori 2005), personalidad del delincuente expone:

Si el delincuente es el sujeto que delinque, o lo que es igual, el sujeto activo o agente del delito, entonces la delincuencia es la calidad del delincuente, la comisión de un delito, o un conjunto de delitos en general, o referidos a un país o época

Delito es la culpa, crimen o quebrantamiento de la ley; dicho de forma más precisa, es la acción u omisión voluntaria, imputada a una persona que infringe el derecho, y que es penada por la ley, según el Diccionario Porrúa de la lengua Española.

El Maestro Eduardo García Maynez señala en su obra Introducción al estudio del Derecho, que se le da el nombre de delito a ciertas acciones antisociales prohibidas por la ley, cuya comisión hace acreedor al delincuente a determinadas sanciones conocidas con el nombre de penas

En cuanto a la delincuencia Jesús Morant Vidal en su libro Delincuencia Juvenil señala que es la conducta resultante del fracaso del individuo en adaptarse a las demandas de la sociedad en que vive.

Un comunicado de prensa emitido por el Consejo Europeo de Tampere, realizado en octubre de 1999, y de la conferencia de alto nivel celebrada en Praia da Tampere, el 4 y 5 de mayo del 2000, relativo a la prevención de la

delincuencia en la Unión Europea, se llegó a la conclusión de que se define la delincuencia como todo acto punible cometido por individuos o asociaciones espontáneas de personas, no obstante indica el mismo documento, esta definición incluye distintas realidades como:

a. La delincuencia en sentido propio.

b. La delincuencia con un nivel de infracción penal menos grave pero más frecuente.

c. La violencia que afecta a los medios más diversos.

d. La falta de Civismo, incluyendo comportamientos asóciales o antisociales, como sería más apropiado decir, que no constituyen una infracción penal.

El delito cometido por el delincuente no es del todo espontáneo, sino que puede ser premeditado y programado. Sin embargo, dependiendo del número de personas que lo cometa y ejecute, de los procedimientos que siga, de los recursos que utilice y de los objetivos que persiga, podrá haber básicamente dos tipos de delincuencia:

- Delincuencia menor.
- Delincuencia organizada.

Tipos de delincuencia

Delincuencia Menor o Delincuencia Común.

La delincuencia menor o delincuencia común, es la más palpable y a la vez temida, pero solamente constituye la punta de iceberg, es cometida por un individuo o cuando mucho por dos, y que tiene por objeto la comisión de un delito que podría ser desde una falta menor hasta una grave y calificada, pero que no trascienden su escala y proporciones, es decir, no son cometidos por bandas, no hay una gran

planeación en los hechos delictivos, y no se pretende operar permanentemente a gran escala.

Es la delincuencia más común, más popular, la que vemos y a la que tenemos miedo, es por esto que los ciudadanos comunes piensan que es un problema grave cuando transitan por determinadas zonas en que pueden ser asaltados y la gente asocia Inseguridad con esto García Maynez, la define como delincuencia callejera: asalto a transeúntes, violación, robo de bienes y artículos menores, robo a casa habitación, robo de vehículos, vandalismo, grafitos y pinta de muros y monumentos.

Estos delitos pueden ser cometidos en grandes proporciones y por muchos individuos, y así se convierte en una delincuencia organizada; cuándo sucede esto, se le llama de modo distinto se convierte en la industria del robo, la industria del secuestro, o la industria del robo de vehículos, etc.

Por supuesto, la delincuencia menor tiene las siguientes características, hablando en términos generales:

1. El asaltante puede apelar o no a dos recursos para lograr sus objetivos:

   - Una precisión técnico-manual elevada y precisa, para cometer el ilícito con rapidez, astucia y disimulo.

   - El uso de la fuerza de apoyo en ventajas físicas e incluso, en el empleo de armas.

2. Normalmente existen compradores de bienes robados, que son los que los adquieren de conformidad con tarifas ya existentes en el mercado negro, mismas que son fijadas por la oferta y la demanda, así como por la situación del entorno local, nacional e internacional.

3. Regularmente los delincuentes operan con apoyo de una red de corrupción entre autoridades intermedias (jueces calificadores, agentes del ministerio público del

fuero común) y corporaciones de seguridad pública desde sus mandos y efectivos elementales hasta sus mandos medios (agentes de policía, jefes de sector, etc.).

Delincuencia Organizada.

En una opinión personal Velasco Gamboa, nos señala las características de la delincuencia organizada, no sin antes citar que es un mecanismo de acumulación, robo y redistribución de capital propio de la economía informal, que también llega a formar parte de la economía formal local, nacional y global.

Evidentemente tiene serias implicaciones del orden económico, constituye una importante derrama de recursos, pues todo el capital generado y distribuido se cubre en efectivo.

La delincuencia colectiva que instrumentaliza racionalmente la violencia institucional de la vida privada y pública, al servicio de ganancias empresariales con rapidez, necesariamente vincula jerarquías en la burocracia política y judicial mediante la corrupción y la impunidad.

Las siguientes son las características concretas de la delincuencia organizada:

1. Opera bajo una disciplina y códigos de comportamiento mafioso.

2. Actúa con la finalidad de obtener, en la forma de prácticas sociales recurrentes, enraizadas en la estructura de trabajo, a nivel local, nacional e internacional, ganancias rápidas sin inversión previa de capital, de origen ilegitimo e ilegal, mediante la apropiación de objetos de uso privado y de propiedad ajena.

3. Se comercializa con bienes, productos y servicios de origen ilegítimo e ilegal, con poca o ninguna inversión de capital.

4. Actúa de manera impune en la clandestinidad, protegida y en ocasiones también dirigida y operada por autoridades corruptas, delincuentes de alto nivel, especialización y jerarquía, y posee capacidad para utilizar la fuerza en aras de lograr sus objetivos.

5. Con respecto a los bienes, productos y servicios ofertados por la misma, una vez que se ponen en circulación, quedan definidos sus precios por las condiciones del mercado regional o mundial, denominado coloquialmente mercado negro, siendo el anterior escenario de esta criminalidad organizada.

Es común referirse a la delincuencia organizada bajo el sinónimos de mafia o mob, como se le conoce en Estados Unidos y Asia; a los delincuentes de gran escala se les llama entonces mafiosos o gángsters.

Los tipos de la delincuencia organizada los encontramos en los siguientes puntos:

- Delincuencia organizada local.
- Delincuencia organizada nacional.
- Delincuencia organizada transnacional.

La primera por deducción se define como la consistente en una banda o varias bandas vinculadas; que opera en una escala territorial menor, ya sea una comunidad, municipio o Estado, y que generalmente opera en esa demarcación y rara vez fuera de ella.

Seguida por la delincuencia organizada nacional, la cual como la anterior puede consistir en una sola banda de grandes proporciones o varias bandas asociadas, que opera dentro de una escala relativamente mayor, y ya se le reconoce como una delincuencia mayor, pues actúa en varias ciudades, provincias o estados y, potencialmente, puede llegar a tener nexos con otras bandas nacionales e internacionales.

Finalmente cuando constituye conexiones con organizaciones similares formando redes en todo el mundo, la Organización de las Naciones Unidas (ONU), la identifica como delincuencia organizada transnacional, también se le denomina delincuencia organizada transfronteriza, las cuales emprenden operaciones ilegales de tipo financiero, mercantil, bancario, bursátil o comercial, acciones de soborno, extorsión, ofrecimiento de servicios de protección, ocultación de servicios

fraudulentos y ganancias ilegales, adquisiciones ilegítimas, control de centros de juego ilegales y centros de prostitución.

Juntas vecinales

Las Juntas Vecinales de Seguridad Ciudadana son agrupaciones comunales y vecinales, de ciudadanos, que se organizan en forma voluntaria y solidaria, que contribuyen al accionar de la Policía para mejorar los niveles de orden y seguridad de sus respectivas jurisdicciones y están integradas por personas honorables que residen o laboran en una misma cuadra, manzana, sector, barrio, conjunto habitacional, edificio, urbanización, localidad, Asentamiento Humano, Pueblo Joven, Comunidad Campesina o Nativa. Constituyen la célula básica de organización de participación de la población para la Seguridad Ciudadana.

Es el ciudadano con altos valores cívicos, que en forma de Seguridad Ciudadana; capacitado por la PNP en las disposiciones elementales y básicas sobre la materia y en los procedimientos preventivos de seguridad y la forma de apoyar y colaborar con la Policía para contribuir a elevar los índices de orden y seguridad de su respectivo domicilio, cuadra, manzana, sector, barrio, conjunto habitacional, edificio, urbanización, localidad, Asentamiento Humano, Pueblo Joven, Comunidad Campesina o Nativa

2.2.5 Constitución política

Según el (Congreso de la Republica del Perú 1993), nos hace referencia lo siguiente:

Art. N° 44.- Estado-Nación-Territorio.- "Son deberes primordiales del Estado, defender la soberanía nacional, garantizar la plena vigencia de los derechos humanos, proteger a la población de las amenazas contra su seguridad; y promover el bienestar general que se fundamenta en la justicia y en el desarrollo integral y equilibrado de la Nación.

Art. N° 166. – "La Policía Nacional tiene por FINALIDAD fundamental garantizar, mantener y restablecer el orden interno.

Art. N° 197. – Estructura del Estado-Descentralización, "Las municipalidades promueven, apoyan y reglamentan la participación vecinal en el desarrollo local; asimismo, brindan servicios de seguridad ciudadana, con la cooperación de la Policía Nacional del Perú, conforme a ley":

Leyes: Ley N° 27972 – Ley Orgánica de Municipalidades (Art. 85°).-Las Municipalidades, en Seguridad Ciudadana, son responsables de promover el establecimiento de Sistemas de Seguridad Ciudadana en su jurisdicción, con la participación de la Policía Nacional y la Sociedad Civil.

2.2.6 Ley N° 27238.-Ley Orgánica de la Policía Nacional del Perú

Artículo 2°.-La Policía Nacional del Perú es la Institución del Estado creada para garantizar el orden interno, el libre ejercicio de los derechos fundamentales de las personas y el normal desarrollo de las actividades de la ciudadanía.

2.2.7 Ley N° 27933 – Ley del Sistema Nacional de Seguridad Ciudadana.

Crea el Sistema Nacional de Seguridad Ciudadana (SINASEC), con el objeto de coordinar eficazmente la acción del Estado y promover la participación ciudadana para garantizar una situación de paz social.

Decretos Supremos:

Decreto Supremo N° 012-2003-IN –de 07 Octubre 2003 que aprueba el Reglamento de la Ley del Sistema Nacional de Seguridad Ciudadana Ley N° 27933. Decreto Supremo N° 008-2000-IN. Reglamento, Ley Orgánica de la Policía Nacional del Perú. Artículo N° 9 Numeral 4 "Tienen entre otras funciones, organiza y capacita a las entidades vecinales".

2.2.8 Sistema de Televigilancia

Según (Daniel 2006) nos dice que el sistema de Televigilancia nació hacia la década de los 80 como complemento visual de la tecnología de audio usada para la verificación de alarmas. Estos sistemas permiten desde una central de control supervisar y controlar una o varias estaciones remotas a través de una conexión alámbrica o inalámbrica y es gracias a esta transmisión que los servicios de tele vigilancia ofrecen todo un abanico de posibilidades, algunas de las más significativas son:

Tele alarma: Alertar automáticamente en caso de ocurrir un evento previamente definido.

Telecontrol: Controlar el funcionamiento de una instalación remota.

Telemando: actuar a distancia sobre los equipos del sistema de tele vigilancia.

Tele gestión: gestionar a distancia el funcionamiento de las instalaciones controladas y registrar la información para analizarla y optimizarla.

Para que un sistema de televigilancia cumpla con el objetivo de vigilar y controlar a distancia, se deben tener en cuenta una gran diversidad de elementos que se integran dependiendo del ambiente en el cuál se está trabajando. A continuación se presentan los tres niveles a tener en cuenta para el desarrollo de un sistema de tele vigilancia.

2.2.9 Niveles de un sistema de televigilancia

Nivel 1: Central de control

En este nivel se ubican los elementos de visualización como monitores, grabadores de video, sistema de activación de alarmas, centros de cómputo y otros dispositivos que permiten el control de cámaras, refrigeración y demás elementos del sitio remoto.

Nivel 2: Red de transmisión de datos

En este nivel se ubica la red de transmisión de datos, la cual establece la comunicación entre la central de monitoreo y la estación remota. Para llevar a cabo dicha comunicación se requiere que en la central de monitoreo como en la estación remota se disponga de un equipo, el cual adecua las señales entre los extremos de red.

Existe gran variedad de tecnologías para establecer la comunicación entre la central de monitoreo y la estación remota; algunas posibilidades son: la red de telefonía pública, Internet, Red Digital de Servicios Integrados

(RDSI), línea Digital Asimétrica de Abonados (ADSL), las redes de radiofrecuencia, redes satelitales, de telefonía móvil y las redes privadas.

Nivel 3: Estación remota

El objetivo de este nivel es recoger información de eventos, para luego transmitirla al puesto de control. Para la recolección de dicha información se utilizan elementos tales como: cámaras de video (analógicas o digitales), sistemas de audio, interruptores, dispensadores, sistemas de identificación (por tarjeta dactilar, óptico, auditivo, entre otros), sensores de movimiento, de temperatura, de presión y demás sensores especiales que son propios de determinados procesos (sensores de nivel de agua, sensores de nivel de radiación, etc.) y en general cualquier dispositivo de entrada que permita obtener información para ejecutar tareas de control.

2.2.10 Fibra óptica

El ejemplar de (Santa Cruz s.f.) hace referencia que la fibra óptica es un medio de transmisión empleado habitualmente en redes de datos; un hilo muy fino de material transparente, vidrio o materiales plásticos, por el que se envían pulsos de luz que representan los datos a transmitir. El haz de luz queda completamente confinado y se propaga por el interior de la fibra con un ángulo de reflexión por

encima del ángulo límite de reflexión total, en función de la ley de Snell. La fuente de luz puede ser láser o un LED.

Las fibras se utilizan ampliamente en telecomunicaciones, ya que permiten enviar gran cantidad de datos a una gran distancia, con velocidades similares a las de radio y superiores a las de cable convencional. Son el medio de transmisión por excelencia al ser inmune a las interferencias electromagnéticas, también se utilizan para redes locales, en donde se necesite aprovechar las ventajas de la fibra óptica sobre otros medios de transmisión.

Características de la fibra óptica

La fibra óptica es una guía de ondas dieléctrica que opera a frecuencias ópticas. Núcleo y revestimiento de la fibra óptica. Cada filamento consta de un núcleo central de plástico o cristal (óxido de silicio y germanio) con un alto índice de refracción, rodeado de una capa de un material similar con un índice de refracción ligeramente menor. Cuando la luz llega a una superficie que limita con un índice de refracción menor, se refleja en gran parte, cuanto mayor sea la diferencia de índices y mayor el ángulo de incidencia, se habla entonces de reflexión interna total.

En el interior de una fibra óptica, la luz se va reflejando contra las paredes en ángulos muy abiertos, de tal forma que prácticamente avanza por su centro. De este modo, se pueden guiar las señales luminosas sin pérdidas por largas distancias.

A lo largo de toda la creación y desarrollo de la fibra óptica, algunas de sus características han ido cambiando para mejorarla. Las características más destacables de la fibra óptica en la actualidad son:

Cobertura más resistente: La cubierta contiene un 25% más material que las cubiertas convencionales.

Uso dual (interior y exterior): La resistencia al agua y emisiones ultravioleta, la cubierta resistente y el funcionamiento ambiental extendido de la fibra óptica contribuyen a una mayor confiabilidad durante el tiempo de vida de la fibra.

Mayor protección en lugares húmedos: Se combate la intrusión de la humedad en el interior de la fibra con múltiples capas de protección alrededor de ésta, lo que proporciona a la fibra, una mayor vida útil y confiabilidad en lugares húmedos.

Empaquetado de alta densidad: Con el máximo número de fibras en el menor diámetro posible se consigue una más rápida y más fácil instalación, donde el cable debe enfrentar dobleces agudos y espacios estrechos. Se ha llegado a conseguir un cable con 72 fibras de construcción súper densa cuyo diámetro es un 50% menor al de los cables convencionales.

Funcionamiento

Los principios básicos de su funcionamiento se justifican aplicando las leyes de la óptica geométrica, principalmente, la ley de la refracción (principio de reflexión interna total) y la ley de Snell. Su funcionamiento se basa en transmitir por el núcleo de la fibra un haz de luz, tal que este no atraviese el revestimiento, sino que se refleje y se siga propagando. Esto se consigue si el índice de refracción del núcleo es mayor al índice de refracción del revestimiento, y también si el ángulo de incidencia es superior al ángulo límite.

Ventajas

Una banda de paso muy ancha, lo que permite flujos muy elevados (del orden del GHz). Pequeño tamaño, por lo tanto ocupa poco espacio. Gran flexibilidad, el radio de curvatura puede ser inferior a 1 cm, lo que facilita la instalación enormemente. Gran ligereza, el peso es del orden de algunos gramos por kilómetro, lo que resulta unas nueve veces menos que el de un cable convencional.

Inmunidad total a las perturbaciones de origen electromagnético, lo que implica una calidad de transmisión muy buena, ya que la señal es inmune a las tormentas, chisporroteo.

Gran seguridad: la intrusión en una fibra óptica es fácilmente detectable por el debilitamiento de la energía lumínica en recepción, además, no radia nada, lo que es particularmente interesante para aplicaciones que requieren alto nivel de confidencialidad. No produce interferencias. Insensibilidad a los parásitos, lo que es una propiedad principalmente utilizada en los medios industriales fuertemente perturbados (por ejemplo, en los túneles del metro). Esta propiedad también permite la coexistencia por los mismos conductos de cables ópticos no metálicos con los cables de energía eléctrica.

Atenuación muy pequeña independiente de la frecuencia, lo que permite salvar distancias importantes sin elementos activos intermedios. Puede proporcionar comunicaciones hasta los 70 km. antes de que sea necesario regenerar la señal, además, puede extenderse a 150 km. utilizando amplificadores láser. Gran resistencia mecánica (resistencia a la tracción, lo que facilita la instalación). Resistencia al calor, frío, corrosión. Facilidad para localizar los cortes gracias a un proceso basado en la telemetría, lo que permite detectar rápidamente el lugar y posterior reparación de la avería, simplificando la labor de mantenimiento. Con un coste menor respecto al cobre. Factores ambientales.

Desventajas

A pesar de las ventajas antes enumeradas, la fibra óptica presenta una serie de desventajas frente a otros medios de transmisión, siendo las más relevantes las siguientes: La alta fragilidad de las fibras. Necesidad de usar transmisores y receptores más costosos. Los empalmes entre fibras son difíciles de realizar, especialmente en el campo, lo que dificulta las reparaciones en caso de ruptura del cable. No puede transmitir electricidad para alimentar repetidores intermedios. La necesidad de efectuar, en muchos casos, procesos de conversión eléctrica-óptica. La fibra óptica convencional no puede transmitir potencias

elevadas. No existen memorias ópticas. La fibra óptica no transmite energía eléctrica, esto limita su aplicación donde el terminal de recepción debe ser energizado desde una línea eléctrica. La energía debe proveerse por conductores separados. Las moléculas de hidrógeno pueden difundirse en las fibras de silicio y producir cambios en la atenuación. El agua corroe la superficie del vidrio y resulta ser el mecanismo más importante para el envejecimiento de la fibra óptica. Incipiente normativa internacional sobre algunos aspectos referentes a los parámetros de los componentes, calidad de la transmisión y pruebas.

Tipos de Fibra óptica

Las diferentes trayectorias que puede seguir un haz de luz en el interior de una fibra se denominan modos de propagación. Y según el modo de propagación tendremos dos tipos de fibra óptica: multimodo y monomodo.

Fibra Multimodo

Una fibra multimodo es aquella en la que los haces de luz pueden circular por más de un modo o camino. Esto supone que no llegan todos a la vez. Una fibra multimodo puede tener más de mil modos de propagación de luz. Las fibras multimodo se usan comúnmente en aplicaciones de corta distancia, menores a 2 km, es simple de diseñar y económico.

El núcleo de una fibra multimodo tiene un índice de refracción superior, pero del mismo orden de magnitud, que el revestimiento. Debido al gran tamaño del núcleo de una fibra multimodo, es más fácil de conectar y tiene una mayor tolerancia a componentes de menor precisión. Dependiendo el tipo de índice de refracción del núcleo, tenemos dos tipos de fibra multimodo: Índice escalonado: en este tipo de fibra, el núcleo tiene un índice de refracción constante en toda la sección cilíndrica, tiene alta dispersión modal. Índice gradual: mientras en este tipo, el índice de refracción no es constante, tiene menor dispersión modal y el núcleo se constituye de distintos materiales. Además, según el sistema ISO 11801 para clasificación de fibras multimodo según su ancho de banda se incluye

el +pichar (multimodo sobre láser) a los ya existentes OM1 y OM2 (multimodo sobre LED).

OM1: Fibra 62.5/125 μm, soporta hasta Gigabit Ethernet (1 Gbit/s), usan LED como emisores.

OM2: Fibra 50/125 μm, soporta hasta Gigabit Ethernet (1 Gbit/s), usan LED como emisores.

OM3: Fibra 50/125 μm, soporta hasta 10 Gigabit Ethernet (300 m), usan láser (VCSEL) como emisores.

Bajo OM3 se han conseguido hasta 2000 MHz km (10 Gbit/s), es decir, una velocidades 10 veces mayores que con OM1.

Fibra Monomodo

Una fibra monomodo es una fibra óptica en la que sólo se propaga un modo de luz. Se logra reduciendo el diámetro del núcleo de la fibra hasta un tamaño (8,3 a 10 micrones) que sólo permite un modo de propagación. Su transmisión es paralela al eje de la fibra. A diferencia de las fibras multimodo, las fibras monomodo permiten alcanzar grandes distancias (hasta 400 km máximo, mediante un láser de alta intensidad) y transmitir elevadas tasas de información (decenas de Gbit/s).

2.3 definición de términos

Tecnología

Conjunto de teorías y de técnicas que permiten el aprovechamiento práctico del conocimiento científico. (Rae[1]2010).

Información

La información es un conjunto organizado de datos procesados, que constituyen un mensaje sobre un determinado ente o fenómeno.
Comunicación o adquisición de conocimientos que permiten ampliar o precisar los que se poseen sobre una materia determinada. (Rae[2] 2010).

Comunicación

Transmisión de la información. (Navarro[3] 2003).
La comunicación consiste en la transmisión de información de un sujeto a otro.
Transmisión de señales mediante un código común al emisor y al receptor.
Acción y efecto de comunicar o comunicarse.

Telecomunicación

Término que se refiere a las comunicaciones (generalmente involucrando computadoras) a través de la red telefónica. (Rae 2010).
Sistema de comunicación telegráfica, telefónica o radiotelegráfica y demás análogos. (Rae 2010).

---

[1]Diccionario de la Real Academia. 2006. http://www.rae.es/rae.html
[2]Diccionario de la Real Academia. 2006. http://www.rae.es/rae.html
[3]Navarro, Ana. 2003. términos de comunicaciones y redes. Madrid: Edit. Pearson Educación.

Protocolo

Conjunto de reglas que se establecen en el proceso de comunicación entre dos sistemas. Plan escrito y detallado de un experimento científico, un ensayo clínico o una actuación médica. (Rae 2010).

Terminal

Dispositivo simple donde se pueden introducir o recuperar datos de una red. En general, los terminales tienen un monitor y un teclado, pero no tienen procesador ni unidad de disco local. (Navarro[4], 2003).

[4]Navarro, Ana. 2003. términos de comunicaciones y redes. Madrid: Edit. Pearson Educación.

CAPÍTULO III: MATERIALES Y MÉTODOS

3.1 Materiales

3.1.1 Instrumental usado

Laboratorios

Se utilizó como laboratorio el área urbana del distrito de Huaraz.

Software

Para el diseño del sistema de televigilancia utilizando fibra óptica, se hizo uso del siguiente software:

Tabla 3.1

Software y herramientas

ÍTEM	SOFTWARE	DESCRIPCIÓN
1	Windows 7	Sistema operativo
2	MS Word 2010	Procesador de texto
3	MS Excel 2010	Para cálculo de presupuesto
4	Autocad 2013	Diseño de planos
5	Adobe Dreamweaver CS6	Diseño grafico

Fuente: elaboración propia

Recursos computacionales

Se hizo uso de los recursos computacionales.

Tabla 3.2

Recursos computacionales

ÍTEM	DESCRIPCIÓN	CARACTERÍSTICAS TÉCNICAS
1	Computadora de escritorio	i7, RAM 4 Gb
2	Computadora portátil	i7, RAM 4 GB
3	Impresora HP	Laser Jet, multifuncional
4	GPS	GPS marca GARMIN

Fuente: elaboración propia

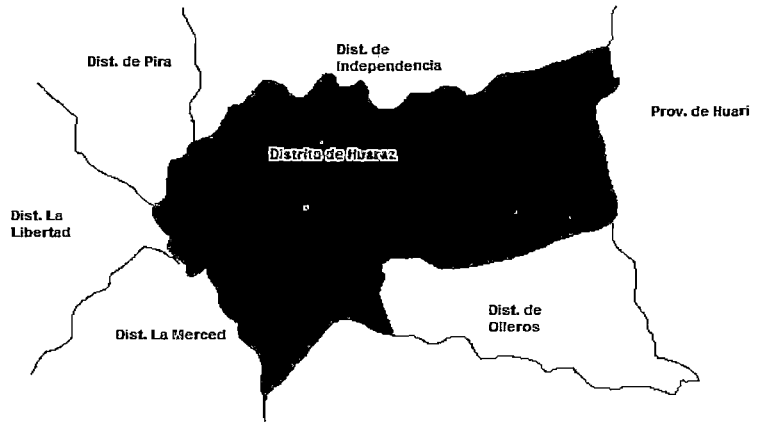
3.1.2 Población y Muestra

Unidad de análisis

Está determinada por el área total de zona urbana y urbana marginal del Distrito de Huaraz, donde se percibe inseguridad y se demanda la acción de las autoridades para que presten un mejor servicio de seguridad ciudadana.

Figura 3.1

Área total de zona urbana y urbana marginal del distrito de Huaraz



Fuente: Municipalidad Provincial de Huaraz

Población

Pobladores del distrito de Huaraz, urbano y urbano marginal.

Tabla 3.3

Pobladores del distrito de Huaraz, urbano y urbano marginal

POBLACIÓN	PROV. **HUARAZ**	DISTRITO **HUARAZ**
Población total, 2012	**161.003**	**61.736**
Hombres	**79.866**	**30.647**
Mujeres	**81.137**	**31.089**

Fuente: Censo de Población y Vivienda del 2007 – INEI

Muestra

El presente trabajo de investigación es descriptivo simple por lo tanto no se utiliza muestra alguna ya que no se realizó encuestas.

3.2 Métodos

3.2.1 Tipo de investigación

De acuerdo a la orientación es tipificada como una investigación aplicada, pues tiene el propósito de desarrollar una solución tecnológica destinada a la solución del problema de inseguridad ciudadana en el área urbana de Huaraz.

De acuerdo a la contrastación se tipifica como descriptiva debido a que los datos han sido obtenidos directamente de la realidad, sin que éstos hayan sido modificados o alterados, sino tal como se presentaron en el levantamiento de información de campo que se realizó en el área urbana de Huaraz.

3.2.2 Definición de variables

Objetivo general

Diseñar sistema de televigilancia utilizando fibra óptica con fines de seguridad ciudadana en el área urbana del distrito de Huaraz en el 2014.

Tabla 3.5

Definición de variables

OBJETIVOS ESPECÍFICOS	VARIABLE	DEFINICIÓN CONCEPTUAL
Levantar información sobre los sucesos de inseguridad existente en el área urbana del distrito de Huaraz, obteniendo el mapa del delito.	V1: Situación actual	Son los hechos de inseguridad presentes en el área urbana del distrito de Huaraz.
Determinar los requerimientos de las tecnologías de banda ancha a ser utilizados para el diseño del sistema de televigilancia, que sirva para minimizar la inseguridad en el área urbana del distrito de Huaraz	V2: Recursos Tecnológicos	Se refiere a los equipos de hardware y software necesarios para desarrollar el sistema de tele vigilancia.
Realizar la evaluación económica de las alternativas estudiadas, a fin de ofrecer la mejor solución técnica económica.	V3: Inversión necesaria para la realización del proyecto	Son los gastos necesarios para la realización del proyecto, donde se describen detalladamente el costo de los equipos que se van a utilizar.

Fuente: elaboración propia

3.2.3 Operacionalización de variables

Objetivo general

Diseñar sistema de televigilancia utilizando fibra óptica con fines de seguridad ciudadana en el área urbana del distrito de Huaraz en el 2014

Tabla 3.6

Operacionalización de variables

OBJETIVOS ESPECÍFICOS	VARIABLE	DIMENSIÓN	INDICADOR
Levantar información sobre los sucesos de inseguridad existente en el área urbana del distrito de Huaraz.	V1: Situación actual	Cantidad de sucesos	Índice de seguridad
Determinar los requerimientos de las tecnologías de banda ancha a ser utilizados para el diseño del sistema de televigilancia.	V2: Recursos tecnológicos	Espacio que ocupa el hardware y software necesario	Cobertura
Realizar la evaluación económica de las alternativas estudiadas.	V3: Evaluación económica	Costo de los equipos necesarios	Nuevos Soles

Fuente: elaboración propia

3.2.4 Diseño de la investigación

Para el diseño de la investigación se tomó en cuenta lo siguiente:

- Población demandante de un servicio de seguridad en óptimas condiciones:

Tabla 3.7

Población demandante de un servicio de seguridad en óptimas condiciones

DESCRIPCIÓN	POBLACIÓN
Número de viviendas	8,252
Número de Pobladores Residentes	41,258
Número de Población Flotante	4,126
DEMANDA TOTAL	45,384

Fuente: elaboración propia

- Se elaboró el siguiente cuadro donde se muestra los puntos álgidos de la delincuencia en el área urbana de Huaraz.

Tabla 3.8

Puntos álgidos de la delincuencia en el área urbana de Huaraz

N°	UBICACIÓN
1	AV. LUZURIAGA
2	AV. RAIMONDI
3	AV. SAN MARTIN
4	AV. SUCRE
5	AV. 13 DICIEMBRE
6	JR. CARAZ
7	JR. COMERCIO
8	MLC. PUENTE QUILCAY
9	ZO. CHAIWUA
10	JR. BOLOGNESI
11	MCDO. CENTRAL DE HUARAZ
12	MCDO. POPULAR DE HUARAZ
13	CISEA HUARAUPAMPA
14	AV. GAMARRA
15	PRQ. LOS INCAS
16	PRQ. GINEBRA
17	AV. BOLIVAR
18	AV. 28 JULIO
19	AV. CIRCUNVALACION
20	AV. 27 NOVIEMBRE

Fuente: elaboración propia

- Información obtenida según los reportes de la policía nacional 2012 al 2013, obteniéndose como resultado el consolidado de video cámaras de vigilancia necesarias.

- Se tuvo en cuenta los siguientes actos delictivos que motivan la inseguridad ciudadana, en el área urbana del distrito de Huaraz:

Tabla 3.9

Actos delictivos que motivan la inseguridad ciudadana

ÍTEM	DESCRIPCIÓN
1	Consumo de bebidas alcohólicas
2	Pandillaje pernicioso
3	Prostitución
4	Accidentes de transito
5	Consumo de drogas
6	Comercialización de drogas
7	Comercio ambulatorio

Fuente: elaboración propia

- Se tuvo en cuenta los siguientes delitos que motivan la inseguridad ciudadana, en el área urbana del distrito de Huaraz:

Tabla 3.10

Delitos que motivan la inseguridad ciudadana

ÍTEM	DESCRIPCIÓN
1	Delitos contra el patrimonio
2	Delitos contra el cuerpo y la salud
3	Delitos contra la salud pública
4	Delitos contra la salud sexual
5	Delitos contra la libertad
6	Delitos contra la familia
7	Inconductas sociales

Fuente: elaboración propia

3.3 Técnicas

3.3.1 Instrumentos de recolección de datos

Se emplearon fuentes primarias la entrevista y observación directa.

Se obtuvo también información de fuentes secundarias, realizada a través de búsqueda de información documental (citas de autores de renombre, revistas, internet, etc.); y se utilizaron fichas técnicas.

Tabla 3.11

Instrumentos de recolección de datos

ÍTEM	TÉCNICAS	INSTRUMENTOS
1	Entrevista	Se aplicaron entrevistas estructuradas al personal de serenazgo y seguridad ciudadana.
2	Observación directa	Guía de observación para realizar observación directa en las zonas de inseguridad ciudadana.
3	Información documental	Plan de seguridad ciudadana, internet, Policía Nacional del Perú.
4	Ficha técnica	Especificaciones técnicas.

Fuente: elaboración propia

3.3.2 Técnicas de procesamiento de la información

Para el procesamiento de la información se elaboró una Matriz de distribución de resultados en una hoja Excel cuyos detalles se presentan en el capítulo de resultados.

3.4 Procedimiento

El procedimiento seguido para cumplir con los objetivos planteados en la investigación, fue el siguiente:

1. Se realizó una inspección de campo del área urbana del distrito de Huaraz, enfocando las áreas de inseguridad ciudadana.

2. Se realizaron entrevistas en el área se seguridad ciudadana de la Municipalidad Provincial de Huaraz.

3. Se buscó información en el serenazgo y PNP de Huaraz, respecto a las incidencias y cantidad de sucesos de delitos y actos perniciosos.

4. Se revisó bibliografía secundaria para determinar los recursos tecnológicos de sistema de televigilancia utilizando fibra óptica y determinar su cobertura.

5. Se buscó información de costos del hardware y software para realizar la evaluación técnica económica.

6. Se realizó el diseño del sistema de televigilancia utilizando fibra óptica con fines de seguridad ciudadana en el área urbano y urbano marginal del distrito de Huaraz. Teniendo en cuenta los estándares internacionales y nacionales para redes de datos y redes eléctricas, y utilizando el modelo ISO/OSI para redes de computadoras.

7. Se elaboró el plan de pruebas para validar el diseño del sistema de televigilancia.

CAPÍTULO IV: ANÁLISIS

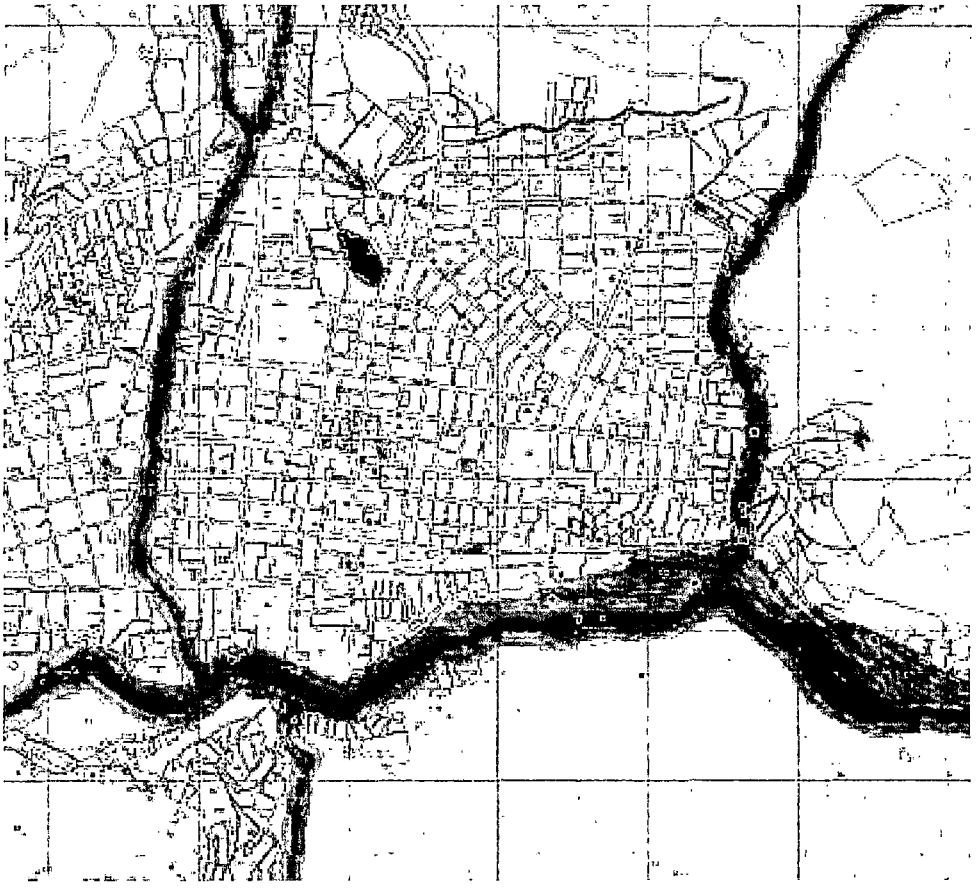
4.1 Análisis de la situación actual

4.1.1 Área de influencia

El área de influencia del proyecto se tomará en cuenta en función al radio de acción del estudio, considerando como la Ciudad de Huaraz – Urbano. Es así que el área de influencia tendrá el siguiente esquema:

Ilustración 4.1

Plano urbano del Distrito de Huaraz



Fuente: Municipalidad Provincial de Huaraz

4.1.2 Características Generales del Área de Influencia

Tipo de Zona

La Zona de influencia del proyecto corresponde a una zona Urbana y Urbana marginal, perteneciente a poblaciones netas de la ciudad de Huaraz y a procesos urbanizadores de la migración de las comunidades.

Características socioeconómicas

Principales Actividades que se realiza en el ámbito de Huaraz:

Entre las principales actividades económicas, predomina el turismo y la minería, seguido del comercio, agricultura e industria ligera como alimentarias, textiles y manufacturas.

Sector Primario

La minería actualmente la principal actividad económica, desde la fundación de la mina Pierina en 1996, concesionada a la empresa peruano canadiense Barrick Misquichilca, Pierina es una mina a tajo abierto, que opera con camiones y cargadores. El mineral es chancado y luego es transportado por fajas sobre tierra a la zona de la cancha de lixiviación. El mineral run-of-mine es llevado directamente por camiones a una operación de lixiviación en valle tradicional. En 2011, Pierina produjo 152,000 onzas de oro a un costo de caja total de $825 la onza. Las reservas mineras probadas y probables al 31 de diciembre de 2011 eran 771,000 onzas de oro. El período de vida de la mina de Pierina se extiende a 2018.

Sector secundario

En Huaraz la actividad industrial, ocupa el 13% de la población económicamente activa, principalmente conformada por micro y medianas empresas dedicadas al rubro de las industrias alimentarias, como la elaboración de lácteos, bebidas gaseosas, cerveza, carne procesada y demás productos de origen de la actividad agropecuaria. También existen empresas dedicadas al rubro de la construcción como ladrilleras, cementeras, madereras. Asimismo, se destaca la fabricación de textiles, artesanías, manufacturas, etc. Sin embargo por el momento la actividad industrial se encuentra dispersa por toda la ciudad.

El 12 de julio del 2011 mediante el Decreto Legislativo 29751, se crea el Parque Industrial de Huaraz, donde se realizarán actividades productivas de la micro, pequeña y mediana empresa, y se generará empleo sostenible, asociatividad, desarrollo económico y social.

Sector Terciario

La ciudad de Huaraz presenta una imagen en la que predomina el comercio y los servicios. El 50% de la población económicamente activa se dedica a estas actividades. Se ha incrementado el comercio y la microempresa como alternativas de supervivencia para enfrentar el desempleo. Sin embargo, la ciudad de Huaraz cuenta con fortalezas, como la importante fuerza laboral de los microempresarios, que impulsa el comercio, el turismo y la artesanía. Asimismo, la ciudad de Huaraz es la principal abastecedora de productos del Callejón de Huaylas, y desde años atrás ha sido el centro de encuentro e intercambio de la región. Así tenemos que en la distribución de la población económicamente activa, por sector de actividad, la población que se dedica al sector primario corresponde al 19%, 13% al secundario y 50 % al sector terciario.

El turismo es una actividad importante en la economía de la ciudad, y lo sigue siendo, ya que Huaraz y sobre todo el Callejón de Huaylas y sus alrededores, son uno de los destinos turísticos más importantes del país, recibiendo anualmente 156.830 visitantes entre nacionales y extranjeros. Huaraz como mayor centro urbano, recepciona la mayor parte de turistas, que están interesados en conocer atractivos como el Callejón de Huaylas, el Parque Nacional Huascarán, Chavín de Huantar, etc. A la vez que la ciudad ofrece diversos servicios turísticos como agencias de viajes, hoteles de primera categoría, así como restaurantes, centros de diversión nocturna, peñas, discotecas, por lo cual constituye un centro de operaciones para el turismo en esta zona del país.

4.1.3 Población afectada

La población referente está constituida por la población general del distrito de Huaraz la cual considera el número de 52,000 habitantes para el año 2007 considerándose en zona rural y urbana identificando la tasa de crecimiento respectivo.

4.1.4 Crecimiento Poblacional

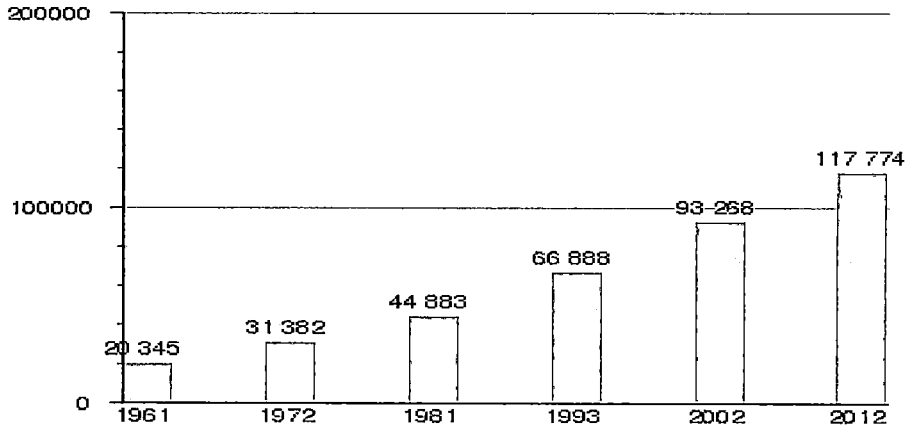
Según proyecciones del INEI hasta julio de 2012, el área metropolitana de Huaraz albergaba 117.774 habitantes. Luego del terremoto de 1970, donde la mitad de la población huaracina murió; se inicia una etapa de reacomodo poblacional que genera grandes oleadas de migración provenientes de otras provincias de la región y posteriormente a finales de la década de 1990, con el inicio de operaciones de las minas Antamina y Pierina, familias de otros departamentos como Huánuco y Lima deciden asentarse definitivamente.

El idioma predominante es el castellano en sus variantes de español andino y español estándar peruano y una minoría utiliza como dialecto

coloquial el quechua ancashino, esta, en zonas rurales aún mantiene predominancia.

Gráfico 4.1

Gráfica de evolución demográfica de Huaraz Metropolitana entre 1961 y 2012



Fuente: Según los censos de población del INEI y de la municipalidad de Huaraz.

4.1.5 Unidad Productora de Servicios en los que intervendrá el estudio

El servicio de seguridad ciudadana se brinda en forma inadecuada produciendo ante la población una sensación de malestar, pues tienen un personal que no tiene capacitación constante, los uniformes están en desuso, la movilidad sufre desperfectos constantes, no tienen un adecuado equipamiento y logística para hacerle frente a la delincuencia que crece a pasos agigantados, existe coordinación con la policía pero esta solo es en el papel, no existe una comunicación radial constante y eficiente pues al no contar con una infraestructura propia es difícil articular esfuerzos, y haber un crecimiento exponencial de la población y de la ciudad es difícil observar y monitorear en tiempo real la ciudad.

Infraestructura Actual

El serenazgo de la Municipalidad de Huaraz no cuenta con un local propio para poder realizar una eficiente tarea de monitoreo del delito en la ciudad de Huaraz, actualmente ocupa un ambiente en el Centro Cultural que les es insuficiente en logística para realizar adecuadamente su servicio de resguardar la seguridad de la población necesidad de este servicios.

Telecomunicación

El serenazgo de la Municipalidad de Huaraz cuenta con un sistema de comunicación obsoleta:

- 2 líneas fijas.
  - Una línea simple.
  - Una línea con rpm e internet.
- 8 radios portátil VHF alcance urbano.
- Una antena inadecuada (Casera).

Una central de operaciones inadecuada para poder monitorear constantemente los incidentes delictivos en la ciudad de Huaraz.

Cuentan con una oficina de 3x4 m, con una sola computadora y un escritorio.

Ilustración 4.2

Local actual del servicio de seguridad ciudadana

Fuente: Municipalidad Provincia de Huaraz

Están prácticamente hacinados en un área, pues no cuenta con un local propio, no tienen un lugar adecuado de descanso del personal.

Equipamiento

Actualmente el serenazgo cuenta con 4 camionetas Nisan (Prontier), de las cuales 2 fueron donadas por Antamina en el 2011 y las otras 2 restantes son vienen de la gestión anterior 2009; cuentan también con un equipamiento deteriorado e Insuficiente, en sus uniformes, armas de disuasión (Huachiporra), vehículos deteriorados (motocicleta, camioneta), las motos con las que cuentan esta malogrados y en el almacén (desusos).

La municipalidad hace esfuerzos para mantener sus unidades operativas:

Ilustración 4.3

Unidades Operativas del Serenazgo

Fuente: Municipalidad Provincia de Huaraz

Con toda esta limitación el personal de serenazgo trata de cumplir cabal mente sus obligaciones con la ciudadanía.

Ilustración 4.4

Unidad operativa del serenzago

Fuente: Municipalidad Provincia de Huaraz

Ilustración 4.5

Unidad operativa de serenazo

Fuente: Municipalidad Provincia de Huaraz

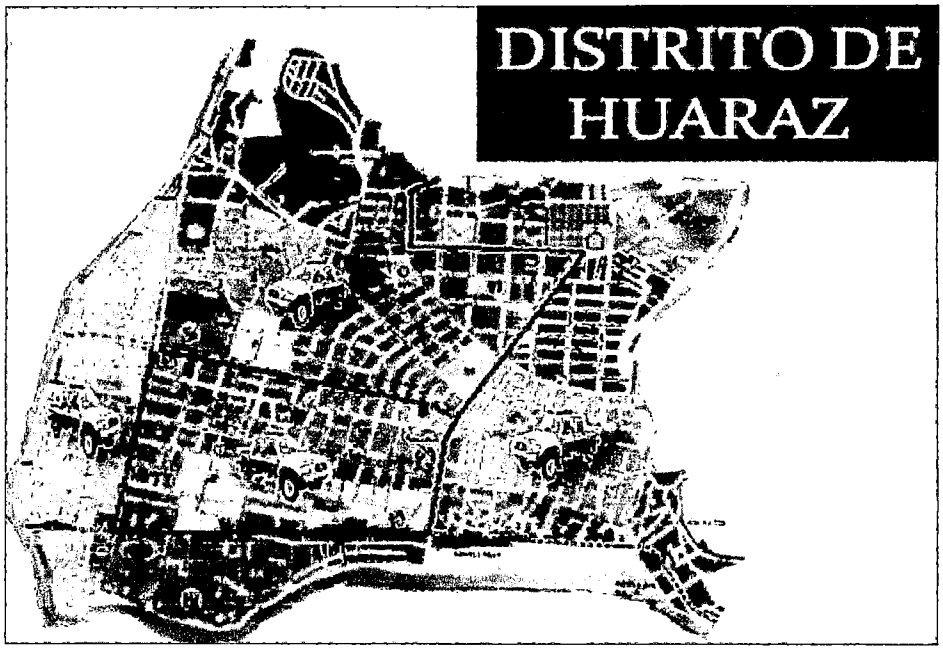
Actualmente la municipalidad de Huaraz no cuenta con ningún convenio institucional, se está coordinando con algunas instituciones (Policía Nacional, fiscalía, etc.), algunos convenios, solo se actúa de oficio ante cualquier hecho delictivo producido es decir se interviene y se comunica a las entidades encargadas de proceder ante el delito (policía, la fiscalía, etc.).

La Población conoce de la situación del servicio de seguridad ciudadana, de sus limitaciones, de los esfuerzos que hacen para poder hacerle frente a la delincuencia, de ahí la exigencia por mejorar el servicio, ya que con el personal que cuenta no cubren todas las necesidades de seguridad

El Serenazgo cuenta actualmente con 45 efectivos distribuidos en los diferentes puntos de la cuidad de Huaraz, con 4 camionetas que están distribuidos en la ciudad de Huaraz, para los centros poblados, barrios emprendedores y anexos que le es insuficiente poder cubrir toda la población de Huaraz, en el mapa, se detalla como es el recorrido de las unidades en la cuidad, para los cuales le es insuficiente.

Ilustración 4.6

Mapa del recorrido de las unidades en la ciudad



Fuente: Foto proporcionada por Serenazgo

El Serenazgo no cuenta con las herramientas de apoyo para hacerle frente a la delincuencia.

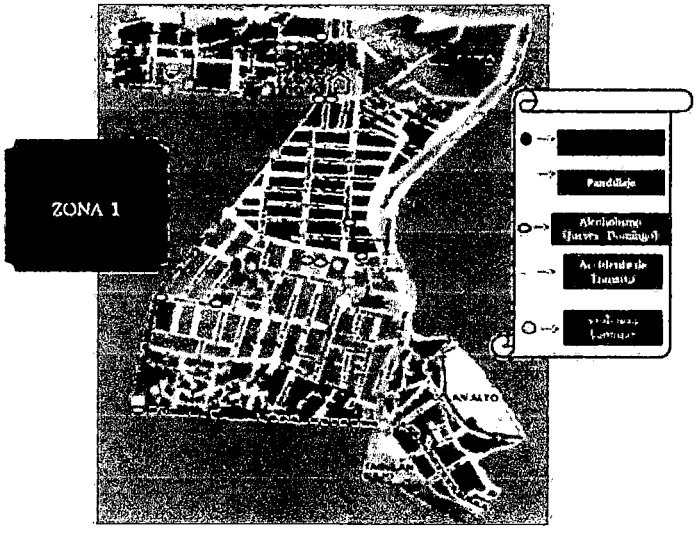
4.1.6 Mapas de peligrosidad

Se ha elaborado mapas de peligrosidad en cuatro zonas donde se muestra los puntos álgidos de la delincuencia en la ciudad:

Zona 1:

Ilustración 4.7

Zona 1 de peligrosidad en la ciudad

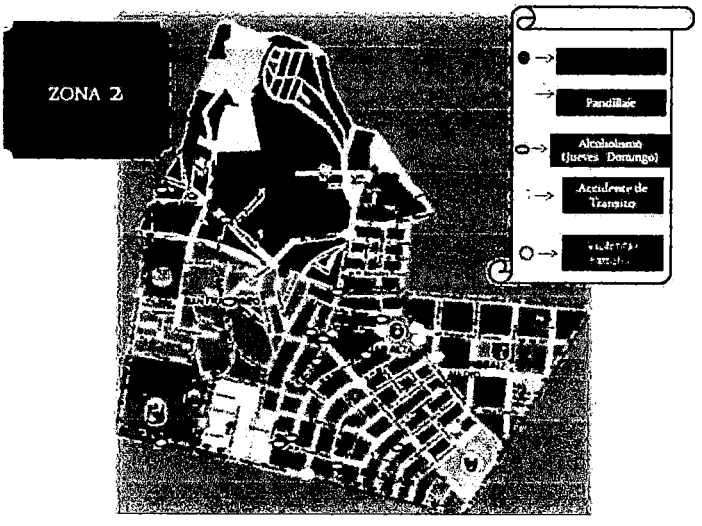


Fuente: Foto proporcionada por Serenazgo

Zona 2:

Ilustración 4.8

Zona 2 de peligrosidad en la ciudad

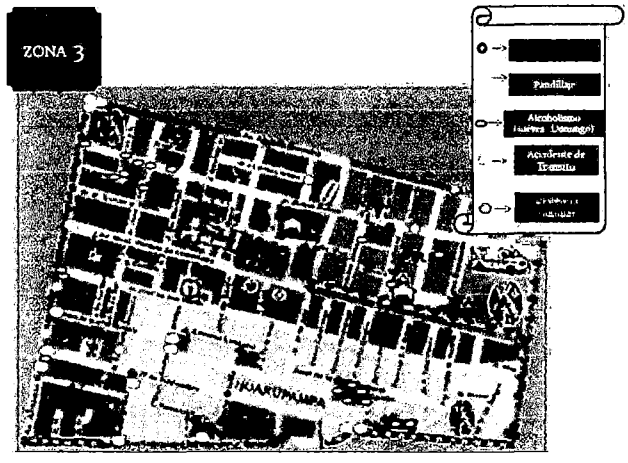


Fuente: Foto proporcionada por Serenazgo

Zona 3:

Ilustración 4.9

Zona 3 de peligrosidad en la ciudad

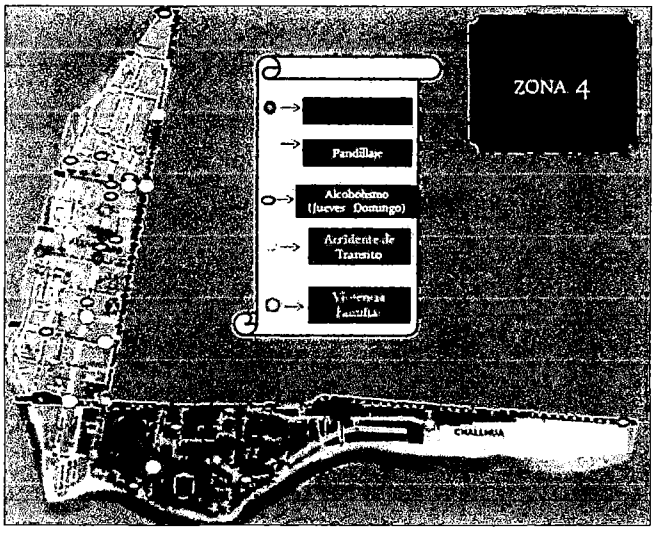


Fuente: Foto proporcionada por Serenazgo

Zona 4:

Ilustración 4.10

Zona 4 de peligrosidad en la ciudad



Fuente: Foto proporcionada por Serenazgo

La Información obtenida según los reportes del 2012 al 2013 de la seguridad ciudadana es:

Bebidas alcohólicas

Las siguientes direcciones presentan una incidencia delictiva de consumo de bebidas alcohólicas: JIRON COMERCIO, AVENIDAD 27 DE NOVIEMBRE, JR. JOSE DE LA MAR, AVENIDAD SIMON BOLIVAR, JIRON BOLOGNESI, AV. CONFRATERNIDAD INTERNACIONAL OESTE, JR. 13 DE DICIEMBRE, JR. CARAZ, AV. GAMARRA, JOSE OLAYA, VILLON ALTO, SOLEDAD, PEDREGAL información obtenida según los reportes de la policía nacional 2012 al 2013.

Ilustración 4.11

Incidencia delictiva de consumo de bebidas alcohólicas

Fuente: Foto proporcionada por serenazgo

Pandillaje pernicioso

Las siguientes direcciones presentan una incidencia delictiva de pandillaje pernicioso: EL ESTADIO ROSASPAMPA, AV. RAIMONDI – AV. CONFRATERNIDAD INTERNACIONAL OESTA, CHAIWUA, VILLON BAJO, ETC. información obtenida según los reportes analizados de la policía nacional – Huaraz; 2012 al 2013.

Ilustración 4.12

Incidencia delictiva de pandillaje pernicioso

Fuente: Foto proporcionada por serenazgo

Prostitución

Las siguientes direcciones presentan una incidencia delictiva de Prostitución: Av. Raimondi, VILLON BAJO, ETC. Información obtenida según los reportes analizados de la policía nacional – Huaraz; 2012 al 2013, obteniéndose como resultado el consolidado "Ubicación de cámaras en el distrito de Huaraz".

Ilustración 4.13

Incidencia delictiva de Prostitución

Fuente: Foto proporcionada por serenazgo

Ilustración 4.14

Incidencia delictiva de Prostitución

Fuente: Foto proporcionada por serenazgo

Accidentes de transito

Las siguientes direcciones presentan una incidencia de accidentes de tránsito: OVALO DEL TAMBO EN EL ESTADIO NACIONAL, PUENTE QUILCAY, AV. GAMARRA - RAIMONDI, VILLON ALTO, JIRON CARAZ, ETC. Información obtenida según los reportes de la policía nacional 2012 al 2013.

Ilustración 4.15

Incidencia de accidentes de tránsito

Fuente: Foto proporcionada por serenazgo

Ilustración 4.16

Incidencia de accidentes de tránsito

Fuente: Foto proporcionada por serenazgo

Consumo de drogas

Las siguientes direcciones presentan una incidencia delictiva de consumo de drogas: SOLEDAD ALTA, PEDREGAL, VILLON ALTO, CONFRATERNIDAD INTERNACIONAL ESTE, AVENIDAD GAMARRA INTERSECCION CON JOSE DE LA MAR Y AVENIDAD BOLIVAR, AV. SAN MARTIN; consolidado obtenido de la PNP de Huaraz entre el 2012 al 2013.

Ilustración 4.17

Incidencia delictiva de consumo de drogas

Fuente: Foto proporcionada por serenazgo

Comercialización de drogas

Las siguientes direcciones presentan una incidencia delictiva de comercialización de drogas: INTERMEDIACIONES DE TACLLAN Y VILLON BAJO, JIRON 13 DE DICIEMBRE, ETC. consolidado obtenido de la PNP de Huaraz entre el 2012 al 2013.

Comercio ambulatorio

Las siguientes direcciones presentan una incidencia de comercio ambulatorio: JIRON CARAZ, JIRON 13 DE DICIEMBRE, JIRON HUASCARAN, JIRON SAN CRISTOBAL, AVENDIDA GAMARRA ALTURA DEL MINISTERIO DE TRABAJO, VILLON ALTO ALTURA DE LA FACULTADA DE DERECHO. Consolidado obtenido de la PNP de Huaraz entre el 2012 al 2013.

Análisis FODA

Tabla 4.1

Análisis FODA con sus debilidades y fortalezas

ANÁLISIS FODA DEL SISTEMA DE TELEVIGILANCIA UTILIZANDO FIBRA ÓPTICA CON FINES DE SEGURIDAD CIUDADANA PARA EL DISTRITO DE HUARAZ, 2014	
DEBILIDADES	FORTALEZAS
a. El servicio de seguridad ciudadana se brinda en forma inadecuada produciendo ante la población una sensación de malestar. b. El serenazgo de la Municipalidad de Huaraz cuenta con un sistema de comunicación obsoleta. c. El serenazgo de la Municipalidad de Huaraz no cuenta con un local propio para poder realizar una eficiente tarea de monitoreo del delito en la ciudad de Huaraz. d. Existe coordinación con la policía pero esta solo es en el papel, no existe una comunicación radial constante y eficiente.	a. Excelente ciudad para actividad turística. b. Existencia del canon minero que ayudará a la viabilidad del proyecto y se ponga en ejecución para el bien de la ciudadanía.

Fuente: Elaboración propia

Tabla 4.2

Análisis FODA con sus amenazas y oportunidades

ANÁLISIS FODA DEL SISTEMA DE TELEVIGILANCIA UTILIZANDO FIBRA ÓPTICA CON FINES DE SEGURIDAD CIUDADANA PARA EL DISTRITO DE HUARAZ, 2014	
AMENAZAS	OPORTUNIDADES
a. Incremento de la violencia y del delito. b. Crecimiento de los conflictos vulnerables de los organismos del Estado relacionados al orden público. c. Sociedad individualista e indiferente, aprehensiva. d. Aparición del crimen organizado. e. Presencia de los organismos del Estado cada vez menos eficaces.	a. Hay interés de la población en la implementación de un sistema de televigilancia, con su respectivo sistema de atención de emergencias. b. Disponibilidad de la administración actual de la municipalidad para la ejecución del proyecto. c. Posibilidad de que otras entidades (minas, empresas, etc.) apoyen al proyecto.

Fuente: Elaboración propia

4.2. Identificación y descripción de requerimientos

4.2.1. Medios fundamentales y planteamiento de acciones

En el presente trabajo se identificaron 4 medios fundamentales como requerimiento para plantear el sistema de televigilancia:

Medio Fundamental 1

- Adecuada infraestructura física.

Acción 1.A

- Construcción de edificación para el servicio de seguridad ciudadana.

Medio Fundamental 2

- Maquinarias y equipos suficientes:
  - Sistema de televigilancia.
  - Equipamiento de comunicación.
  - Vehículos para el patrullaje del Distrito.

Acción 2.B

- Implementación de un sistema de televigilancia, con su respectivo sistema de atención de emergencias.

Acción 2.C

- Implementación de un sistema de radio comunicaciones.

Acción 2.D

- Adquisición de vehículo terrestre.

Medio Fundamental 3

- Fuerte sistema de organización y gestión en Seguridad Ciudadana de la Municipalidad Distrital de Huaraz.

Acción 3.E

- Desarrollar y fortalecer las capacidades en organización y gestión del personal de la Municipalidad que se encargará del servicio de Seguridad Ciudadana, así como de la Policía Nacional y de las Juntas Vecinales, involucrados en el servicio, mediante una empresa especializada en seguridad ciudadana.

Medio Fundamental 4

- Existe integración efectiva entre la Municipalidad, la PNP y a las Juntas Vecinales.

Acción 4.F

- Desarrollar y fortalecer las capacidades en organización y gestión del personal de la Municipalidad que se encargará del servicio de Seguridad Ciudadana, así como de la Policía Nacional y de las Juntas Vecinales, involucrados en el servicio, mediante una empresa especializada en seguridad ciudadana.

Acción 4.G

- Implementación de un Sistema de Radio Comunicaciones.

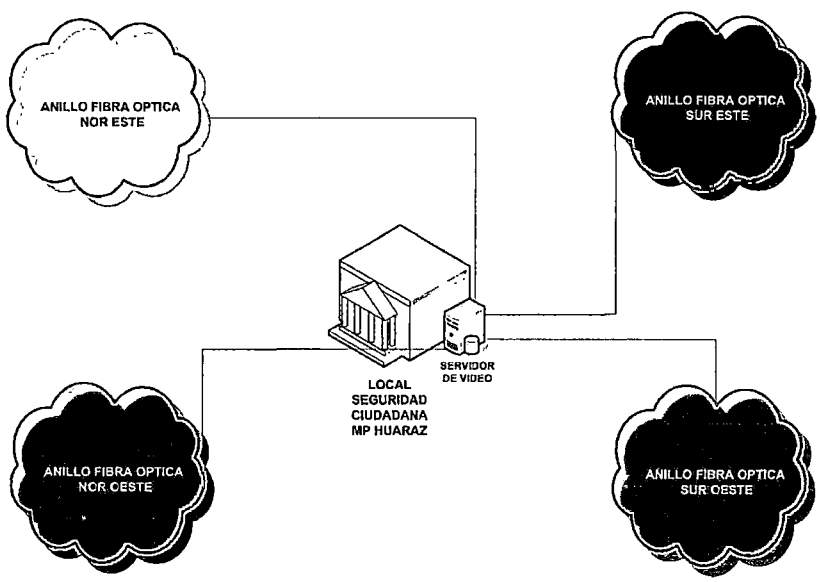
4.2.2 Topología del sistema de televigilancia

Se considera para los nodos de concentración el uso de switch que soporten stream video y para el nodo principal un switch gigabit que soporte igual stream video y este último se utilizará para la conexión de equipos de televigilancia y backbone de fibra óptica y en los nodos de concentración secundarios para conexión al backbone fibra óptica y cámaras IP.

Topología de la red anillo de fibra óptica:

Ilustración 4.18

topología de la red anillo de fibra óptica



Fuente: Elaboración propia

4.3 Diagnóstico de la situación actual

4.3.1 Involucrados

Para el planteamiento del problema y en la formulación de las alternativas de solución, participaran los intereses, problemas, conflictos y potencialidades recogidas a través de entrevistas a los siguientes involucrados:

Municipalidad Distrital de Huaraz, a través de las diferentes dependencias. Las oficinas involucradas directamente son:

La Oficina de Participación Vecinal, Juventudes y Proyectos Productivos en enlace con la Oficina de Seguridad Ciudadana, y Oficina de Informática.

Policía Nacional del Perú, Es una institución del Estado que tiene por misión garantizar, mantener y restablecer el orden interno, prestar protección y ayuda a las personas ya la comunidad, garantizar el cumplimiento de las leyes y la seguridad del patrimonio público y privado, prevenir, investigar y combatirla delincuencia ;vigilar y controlar las fronteras; con el propósito de defender a la sociedad y a las personas, a fin de permitir su pleno desarrollo, en el marco de una cultura de paz y de respeto a los derechos humanos. Esta institución forma parte importante de la alianza estratégica en la seguridad ciudadana del distrito, la misma se encuentra fortalecida por los planes interinstitucionales y está representada a través de las comisarías en el distrito de Huaraz.

Vecinos Residente, participan en su calidad de beneficiarios directos del proyecto y como principales interesados en la ejecución.

Población Flotante participan en su calidad de beneficiarios, ya que instalando el Sistema de televigilancia, mejorara la percepción de seguridad de los visitantes del distrito.

4.3.2 análisis causa

El problema central se define como, insuficiente capacidad de monitoreo, supervisión y control de la seguridad del ciudadano en el distrito de Huaraz.

Análisis de las Causas:

4.3.2.1 Escasa capacidad resolutiva del servicio de Seguridad Ciudadana de la Municipalidad de Huaraz.

Se ha observado que esto se debe a los siguientes factores:

1. Falta de una adecuada infraestructura física.
2. Inexistencia de un sistema de video vigilancia.
3. Insuficiente equipamiento de comunicación.
4. No contar con información detallada y actualizada de los delitos/faltas que ocurren en el distrito.
5. Insuficientes de patrullaje tanto de tierra.
6. Débil sistema de organización y gestión en Seguridad Ciudadana.
7. No existe integración efectiva entre la Municipalidad, la PNP y a las Juntas Vecinales.
8. Insuficiente mobiliario de oficina.

Estos no les permiten resolver los procesos institucionales relacionados con Seguridad Ciudadana, con eficacia, rapidez y determinación.

4.3.2.2 Insuficiente participación de la población en seguridad ciudadana.

Se ha observado que esto se debe a:

1. Indiferencia de la población, por falta de liderazgo del Gobierno Local en lo referente a Seguridad Ciudadana.
2. Existe un Plan de Acción en Seguridad Ciudadana 2012 incompleto, que no compromete la creación y participación de la población para el fortalecimiento de las Juntas Vecinales.
3. Inexistencia de un adecuado sistema de comunicación entre las Juntas Vecinales y Serenazgo.

4.3.2.3 Insuficiente servicio de la PNP en las acciones de seguridad ciudadana de la Municipalidad de Huaraz.

Se ha observado que esto se debe a:

1. Limitado sistema de comunicación entre PNP y Serenazgo.
2. Existe un Plan de Seguridad Ciudadana, incompleto. Entre otras falencias, no muestra una sinergia entre la PNP, el Serenazgo y las Juntas Vecinales.
3. La PNP no está capacitando, ni organizando, ni fortaleciendo a las Juntas Vecinales y Serenazgo de la Municipalidad en Seguridad Ciudadana.

4.3.3. Análisis efecto

Efecto Final, Atraso en el desarrollo social, cultural, económico y educativo de la Provincia de Huaraz.

Análisis de los efectos:

1. Incremento de la violencia y del delito.
2. Crecimiento de los conflictos vulnerables de los organismos del Estado relacionados al orden público.
3. Sociedad individualista e indiferente, aprehensiva.
4. Aparición del crimen organizado.
5. Presencia de los organismos del Estado cada vez menos eficaces.

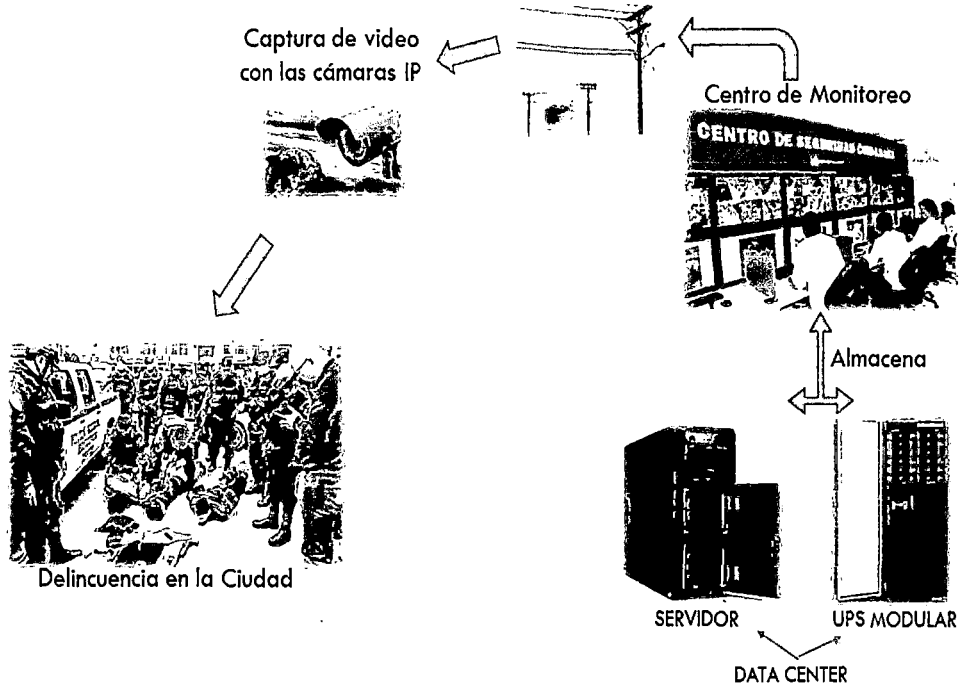
CAPÍTULO V: DISEÑO DE LA SOLUCIÓN

5.1 Arquitectura tecnológica de la solución

5.1.1. Arquitectura del sistema de televigilancia utilizando fibra óptica

Ilustración 5.1

Arquitectura de la red de fibra óptica



Fuente: Elaboración propia

Descripción

Nivel 1: Central de control

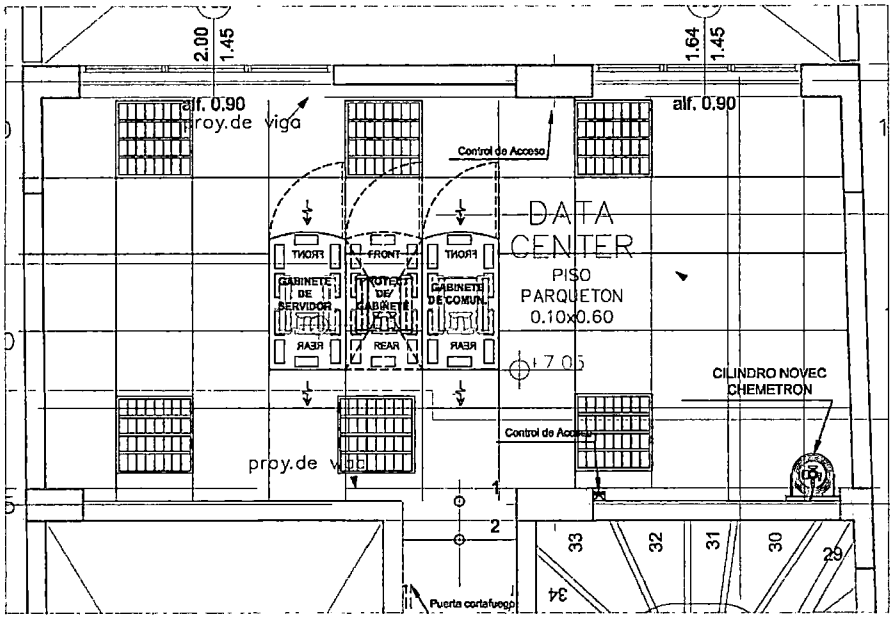
Estará ubicado en el local de seguridad ciudadana de la Municipalidad Provincial de Huaraz.

En este nivel se ubican el Data Center, los elementos de visualización como monitores, grabadores de video, sistema de activación de alarmas, y otros dispositivos que permiten el control de cámaras, refrigeración y demás elementos del sitio remoto.

El servidor de video estará ubicado en el Data Center

Ilustración 5.2

Data Center

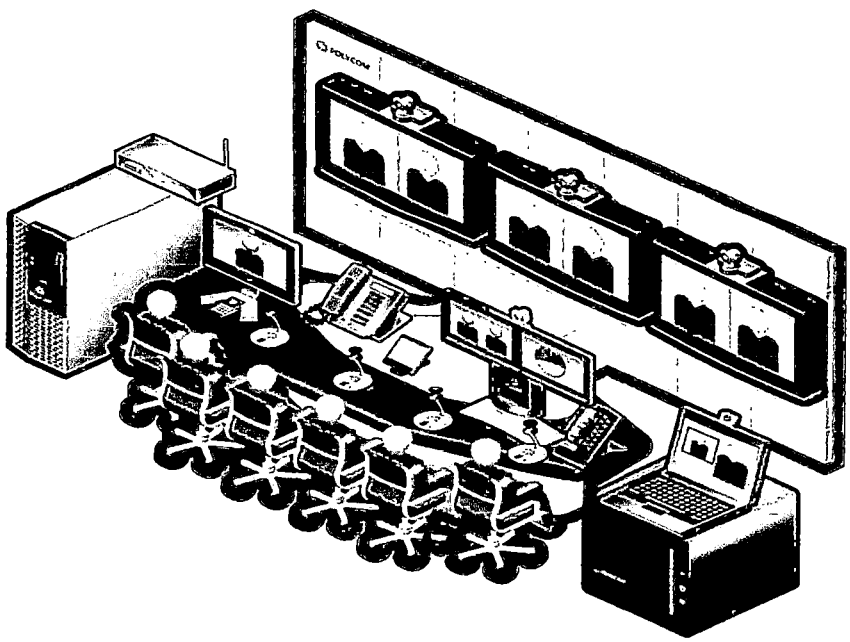


Fuente: Elaboración propia

Central de monitoreo

Ilustración 5.3

Central de emergencia y telefónica



Fuente: Elaboración propia

Nivel 2: Red de transmisión de datos

En este nivel se ubica la red de transmisión de datos, la cual establece la comunicación entre la central de monitoreo y la estación remota. Para llevar a cabo dicha comunicación se requiere que en la central de monitoreo como en la estación remota se disponga de un equipo, el cual adecua las señales entre los extremos de red.

Existe gran variedad de tecnologías para establecer la comunicación entre la central de monitoreo y la estación remota, haciendo uso en este caso de la red dorsal de fibra óptica, para tal fin se ha diseñado 4 anillos para cubrir el área urbana del distrito de Huaraz, como se muestra en la siguiente ilustración:

Ilustración 5.4

Ubicación de video cámaras

Fuente: Elaboración propia

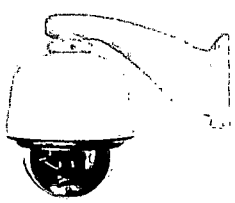
Nivel 3: Estación remota

El objetivo de este nivel es recoger información de eventos, para luego transmitirla a la central de control.

Para la recolección de dicha información se utiliza la cámara IP Domo PTZ.

Ilustración 5.5

Cámara IP Domo PTZ



Fuente: Foto proporcionada por internet

5.2 Diseño de estructura de la solución

5.2.1 Central de control

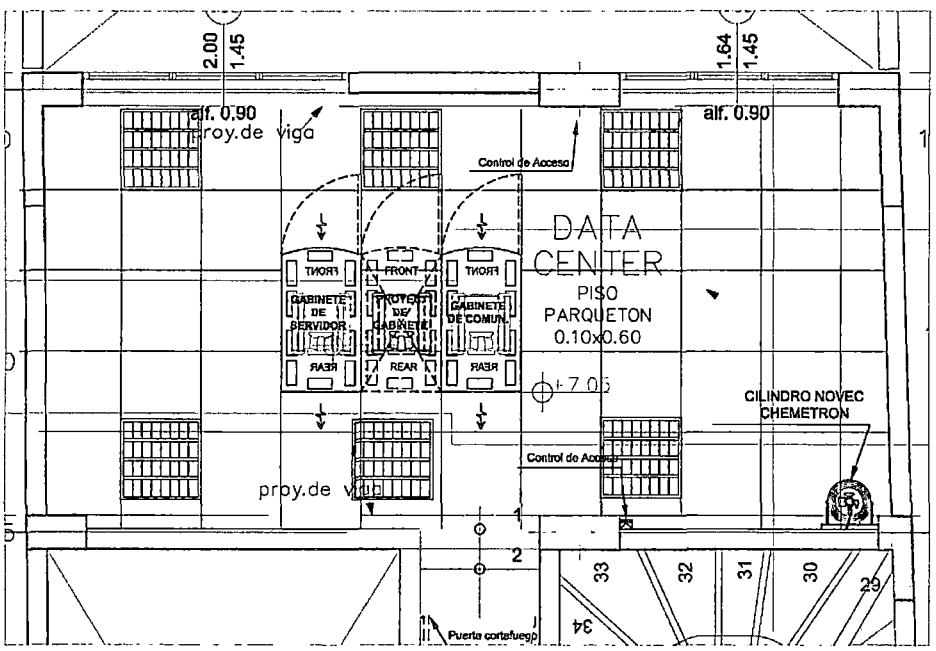
5.2.1.1 Data Center

Implementación del Data Center.

Infraestructura

Ilustración 5.6

Data Center



Fuente: Elaboración propia

En esta estará ubicado los dispositivos, componentes, accesorios, aire acondicionado, gabinetes, switch.

10GBASE-T para 10 Gigabit en el centro de datos

El creciente uso de la virtualización en los centros de datos para hacer frente a la necesidad de reducir los costos de TI ha hecho que muchos administradores tomen una mirada seria a 10Gb Ethernet (10 GbE) como una manera de reducir las complejidades que enfrentan cuando se utilizan los 1Gb Ethernet (1 GbE) las infraestructuras existentes. La consolidación de servidores asociados con la virtualización ha tenido un impacto significativo en la red de E / S, ya que combinan las necesidades de red de varios equipos físicas y el resto de servicios de fondo, como la migración en vivo.

Junto con tendencias como las redes unificada, la capacidad de utilizar una sola red Ethernet tanto para los datos y el tráfico de almacenamiento, están aumentando las demandas de E / S hasta el punto en una red 1 GbE puede ser un cuello de botella y un fuente de complejidad del centro de datos. La decisión de implementar redes unificadas requiere replanteamiento de centros datos de redes. Mientras que las conexiones de 1 GbE podrían ser capaces de manejar los requisitos de ancho de banda de un sola tipo de tráfico, que no tiene suficiente ancho de banda para múltiples tipos de tráfico durante los períodos pico. Esto crea una necesidad para múltiples conexiones de 1 GbE.

Utilizar 10 Gigabit Ethernet (10 GbE) soluciona estos problemas de red, proporcionando más ancho de banda y simplifica la infraestructura de red mediante la consolidación de múltiples puertos Gigabit en una sola conexión de 10 gigabits.

El Centro de Datos Administrados tienen una serie de interfaces de 10 GbE para elegir, incluyendo CX4, SFP + fibra, SFP +. Conexión directa de cobre (DAC) y 10GBASE-T. Hoy en día, la mayoría están eligiendo ya sea óptica o 10GbE SFP + DAC.

Sin embargo, las limitaciones con cada una de estas interfaces les han impedido desplegar ampliamente en todo centro de datos.

Despliegue generalizado requiere una solución rentable que es compatible hacia atrás y tiene la flexibilidad capaz de llegar a la mayoría de los switches y servidores del centro de datos.

La necesidad de 10 Gigabit Ethernet

Una variedad de avances tecnológicos y las tendencias están impulsando la creciente necesidad de 10GbE en el centro de datos.

Por ejemplo, la amplia disponibilidad de los procesadores multi-núcleo y plataformas multi-socket para impulsar el rendimiento del servidor. Esto permite a los clientes reciban más aplicaciones en un único servidor que resulta en múltiples aplicaciones que compiten por un número finito de los recursos de E / S en el servidor. Los clientes también están utilizando la virtualización para consolidar múltiples servidores en un único servidor físico, la reducción de sus equipos y de costos. Los servidores que utilizan los últimos procesadores Intel® Xeon® que pueden soportar tasas de consolidación de servidor de hasta quince a uno.

Sin embargo, la consolidación de servidores y virtualización tienen un impacto significativo en el ancho de banda de red, como la E / S de varios servidores ahora se deben cumplir por los recursos de red de un único servidor físico.

La transición a redes unificadas se suma a la creciente demanda de redes de alto ancho de banda. Los departamentos de TI se están moviendo a la creación de redes unificada para ayudar a simplificar la infraestructura de red mediante la convergencia de tráfico de LAN y SAN, incluyendo iSCSI, NAS y FCoE para un solo protocolo de centro de datos Ethernet. Esta convergencia hace simplificar la red pero aumenta significativamente la demanda de la red de E / S al permitir múltiples tipos de tráfico para compartir una única estructura Ethernet.

Compatibilidad con versiones anteriores

Debido a 10GBASE-T es compatible hacia atrás con 1000BASE-T, se puede implementar en infraestructuras de conmutación de 1 GbE existentes en los centros

de datos que están cableados con CAT6, CAT6A o por encima de cableado, lo que le permite mantener los costos bajos al tiempo que ofrece una ruta de migración fácil de 10GbE.

Energía

Los Puertos GbE están ahora bajo 1W / puerto. Lo mismo ha demostrado ser cierto para 10GBASE-T.

Latencia

Dependiendo del tamaño del paquete, la latencia para 1000BASE-T va de sub-microsegundo a más de 12 microsegundos. 10GBASET oscila entre poco más de 2 microsegundos a menos de 4 microsegundos, un rango de latencia mucho más estrecho.

Para Ethernet tamaños de paquetes de 512B o más grande, 10GBASE-T de general a lo largo ofrece una ventaja sobre 1000BASE-T.

Costo

Como los indicadores de energía han disminuido significativamente en las últimas tres generaciones, el costo ha seguido una similar a la baja de curva. Adaptadores 10GBASE-T de primera generación cuestan $ 1000 por puerto. Hoy adaptadores de dos puertos de tercera generación 10GBASE-T son menos de $ 400 por puerto.

Opciones de arquitectura de centros de datos de red 10 Gigabit Ethernet

El gráfico siguiente muestra las arquitecturas de redes de centros de datos típicos aplicables a las diversas tecnologías de 10GbE.

El cuadro muestra claramente la tecnología 10GBASE-T proporciona una mayor flexibilidad en el diseño de sus dos homólogos de cobre.

Tabla 5.1

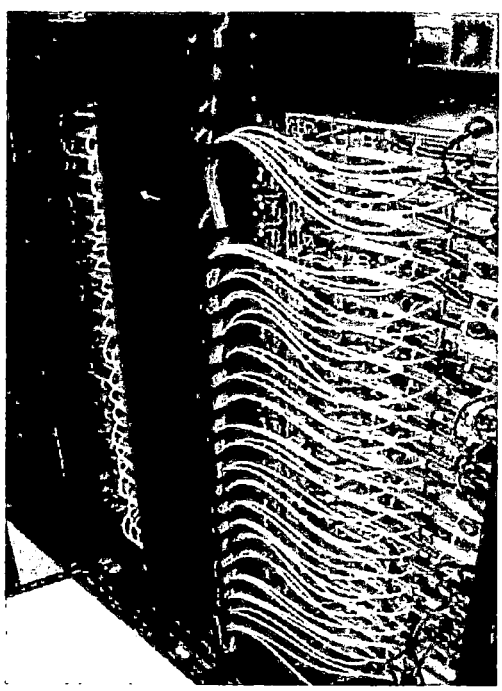
Tecnología 10GBASE-T

Technology	Data Center Network Architectures	Connectivity
10GBASE-SR SFP+ Fiber	• Top of Rack (ToR)	Uplinks from ToR switches to aggregation layer switches
	• Middle of Row (MoR)	Inter-cabinet connectivity from servers to MoR switches
	• End of Row (EoR)	Inter-cabinet connectivity from servers to EoR switches
	• Core network	Backbone
10GBASE-SFP+ DAC	• Top of Rack	Intra-cabinet connectivity from servers to ToR switches
10GBASE-CX4	• Top of Rack	Intra-cabinet connectivity from servers to ToR switches
	• Top of Rack (ToR)	Intra-cabinet connectivity from servers to ToR switches
10GBASE-T	• Middle of Row (MoR)	Inter-cabinet connectivity from servers to MoR switches
	• End of Row (EoR)	Inter-cabinet connectivity from servers to EoR switches

Fuente: Foto proporcionada por internet

Ilustración 5.7

Canales verticales de parcheo



Fuente: Foto proporcionada por internet

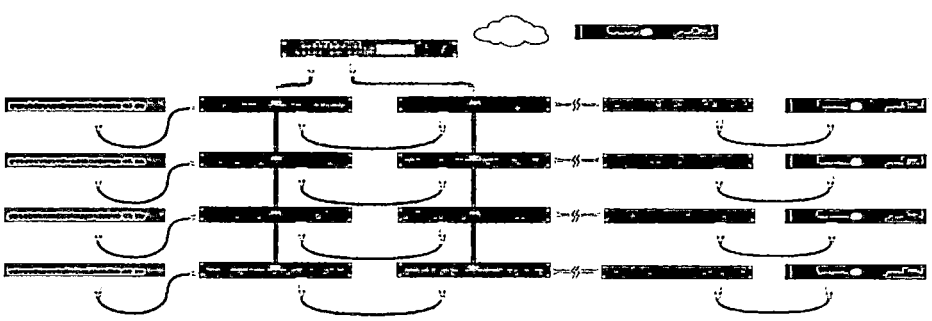
Administración inteligente de infraestructura IIM

Mediante el uso de una zona central de parches o zonas de áreas de parches, la administración inteligente de infraestructura, se puede implementar en manera rentable. Se entiende que el equipo que se mueve dentro y fuera de armarios variará con el tiempo.

Las conexiones en la zona central de parches se supervisan de forma dinámica y en tiempo real por los analizadores que monitorean continuamente a través de los cables de conexión y puentes de fibra. Debido a que el software se puede ver el equipo al final de cada canal a través de SNMP, lo que realmente importa Indiferente lo que el equipo está o si cambia.

Ilustración 5.8

IIM en configuración conexión cruzada



Fuente: Foto proporcionada por internet

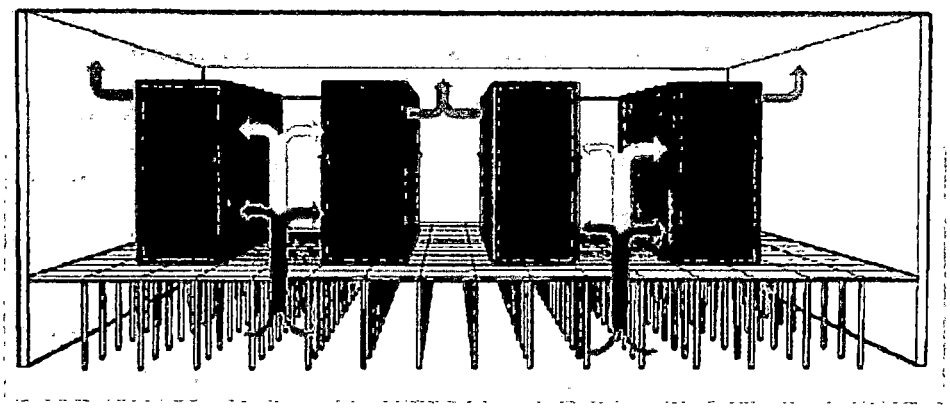
La planificación de refrigeración

Pasillo caliente, arreglos de pasillo frío se hizo popular después de la ASHRAE estudió cuestiones de refrigeración dentro de los centros de datos. Comité Técnico ASHRAE 9,9 caracteriza y estandarizada de las recomendaciones. Se recomienda esta práctica, ya sea para el enfriamiento pasivo o activo o una combinación de los dos.

La disposición en la ilustración 1 muestra cuatro filas de armarios con las baldosas centro entre las filas exteriores representan un pasillo frío (aire frío representado por las flechas azules). Y las caras posteriores de los gabinetes están dirigidas hacia los pasillos calientes (aire calentado representado por las flechas rojas).

Ilustración 5.9

Refrigeración pasiva, utilizando el flujo de aire en la habitación y perforaciones de las puertas.

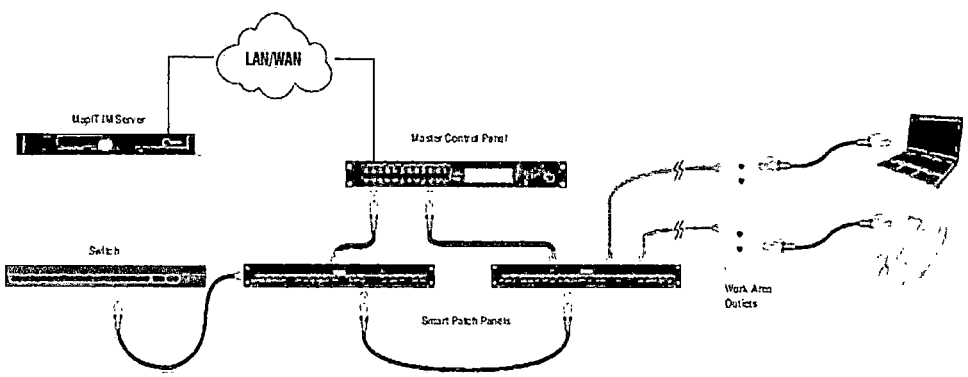


Fuente: Foto proporcionada por internet

Arquitectura del Data Center

Ilustración 5.10

Arquitectura del data center



Fuente: Foto proporcionada por internet

Una vez definido el local adecuado en donde se implementará el Data Center, es necesario algún despliegue de infraestructura en su interior:

- Falsos suelos y/o Falsos techos.
- Cableado de red.
- Generadores y cuadros de distribución eléctrica.
- Acondicionamiento de salas.
- Instalación de alarmas, control de temperaturas y humedad con avisos vía SNMP o SMTP.
- Aire acondicionado, teniendo en cuenta que se usará para la refrigeración del equipamiento de comunicaciones e informático.
- Facilidades de acceso (Debido a que habrá que meter en él, aire acondicionado pesado, gabinetes de piso de 42RU, etc.).

Por otro lado, se tiene que considerar una parte importante al tema de la seguridad física de la instalación. Esta incluye:

- Cerraduras electromagnéticas.
- Cámaras de seguridad.
- Detectores de movimiento y/o Alarmas.
- Tarjetas de identificación o Control de Acceso.

Gabinete de servidores

Los gabinetes deberán ser metálicos, con puertas frontales y traseras perforadas y brindar altos niveles de ventilación a los equipos informáticos que se instalarán en su interior. Deberán tener un bastidor de 19" estándar. Deben ser de altura completa

que permitirán albergar a los equipos de almacenamiento de datos y servidores, cumpliendo las siguientes características:

- Los gabinetes a proporcionar deben ser de un tamaño de 42 unidades de rack de altura, de 800 milímetros de ancho y 1200 milímetros de profundidad, fabricados para soportar equipos de almacenamiento y servidores en los centros de datos o salas de cómputo refrigeradas. Deben tener las puertas laterales sólidas desmontables y la puerta frontal y posterior microperforada al 79% de perforación para optimizar un mayor rendimiento en el ingreso de flujo de aire frío al gabinete en forma pasiva, refrigerando adecuadamente los servidores.

- El bastidor del gabinete debe ser rectangular, con cuatro postes en las esquinas fabricado en acero y aluminio, la construcción debe ser soldada. Los elementos horizontales del bastidor serán de extrusión de aluminio con ranuras que permita la fijación de los rieles de montaje de los equipos y los accesorios de gestión de cables. De tal manera que los rieles pueden ser ajustados en la profundidad del gabinete.

- El gabinete debe soportar un mínimo de 907 Kg de equipamiento instalado en los bastidores.

- El gabinete deberá estar homologado UL como Tecnologías de la Información y el Gabinete Equipo de comunicaciones, cajas y sistemas de bastidores estándar UL 60950 en la categoría NWIN. UL se indica en la documentación del producto del fabricante.

- Cada gabinete debe incluir una barra de tierra vertical para ser instalado en un solo lado en la parte posterior de los gabinetes, el cual debe considerar un tamaño mínimo de 72" de longitud.

Gabinete de Comunicaciones

Los gabinetes deberán ser metálicos, con puertas frontales y traseras perforadas y brindar altos niveles de ventilación a los equipos de integración de red. Deberán tener un bastidor de 19" estándar. Deben ser de altura completa que permitirán albergar a los equipos de cableado estructurado y comunicaciones, cumpliendo las siguientes características:

- Los gabinetes a proporcionar deben tener el tamaño de 42 UR de altura, de 800 mm de ancho y 1200 mm de profundidad, fabricados para ser adecuados en soportar equipos de red y cableado estructurado en los centros de datos o salas de cómputo refrigeradas. Deben tener las puertas laterales sólidas desmontables y la puerta frontal y posterior micro perforada al 79% de perforación para optimizar un mayor rendimiento en el ingreso de flujo de aire frío al gabinete en forma pasiva, refrigerando adecuadamente los equipos de red.

- El bastidor del gabinete debe ser rectangular, con cuatro postes en las esquinas fabricado en acero, la construcción debe ser soldada. Los lados del marco debe ser perforado en la parte superior e inferior con un patrón de agujeros que permita la fijación de rieles de montaje de los equipos y accesorios de gestión de cableado. De tal manera que los rieles pueden ser ajustados en la profundidad del gabinete.

- El gabinete debe soportar 2500 libras o 1134 Kg de equipamiento instalado en los bastidores.

- Los rieles de montaje deberá tener perforaciones cuadradas de acuerdo con el patrón de agujeros EIA-310-D. Estos agujeros perforados de forma cuadrada aceptará tornillos con tuercas enjauladas M6.

- El bastidor de montaje debe utilizar una altura de RU de 1-3/4" (44,45 mm) de altura y deberán ser marcados y numerados en los rieles de montaje. La numeración de comenzar en la parte inferior del riel.

- Cada gabinete debe incluir una barra de tierra vertical para ser instalado a un solo lado en la parte posterior de los gabinetes, el cual debe considerar un tamaño mínimo de 72" de longitud.

Sistema de Control de Acceso al Gabinete

El sistema debe proporcionar control de acceso, pista de auditoría, y la capacidad para el monitoreo tanto del medio ambiente como del status de las puertas de los gabinetes. El sistema puede incluir una combinación de dispositivos de interconexión, interfaces, manijas de cierre electrónico y/o cerraduras electrónicas, sensores y software de gestión. El sistema deberá proporcionar una autorización temporizada para múltiples puertas de gabinetes con la capacidad para abrir una o varias puertas y también debe proporcionar el estado de cada puerta desde una única ubicación. Si es necesario, se deberá incluir una interfaz gráfica de usuario que se pueda utilizar en una red de área local (LAN) o en una red de área amplia (WAN) para administrar el sistema.

Consideraciones:

- El hardware de cierre electrónico no debe utilizar ningún solenoide.

- El hardware de cierre electrónico debe ser compatible con más de 10 fabricantes de gabinetes. El postor debe presentar documento del fabricante donde acredite dicha compatibilidad.

- Las cerraduras deben contar con una llave para desbloqueo manual. No debe utilizar fuente externa para mantener el cierre de seguridad activo. El sistema debe registrar cualquier accionamiento manual con la llave mientras el sistema esté energizado.

- El sistema debe tener un tiempo límite definido después de la autorización que retorne al sistema a modo seguro si ninguna acción fue tomada.

- El sistema debe ser compatible con los estándares de cableado estructurado para distancias de 100 metros.

Dispositivos de Interconexión

El dispositivo de interconexión es un Gateway Ethernet que brinda acceso a los sensores y dispositivos de bloqueo a través de una conexión a red. Soporta una conexión serial "daisy chain" vía RS-485 hasta máximo 32 dispositivos. Las cerraduras, lectoras RFID y sensores pueden ser configuradas, monitoreadas y controladas a través de la interface web embebida en el dispositivo de interconexión sin necesidad de un software adicional. El dispositivo de interconexión puede ser instalado en una unidad de rack o en pared.

- Debe ser compatible con los estándares de cableado estructurado para distancias de 100 metros.

- Debe ser capaz de monitorear y control un total de 16 usuarios, 32 dispositivos, 500 tarjetas RFID.

- Debe operar con 9-32VDC, 2.0A Max. Debe incluir un adaptador de voltaje (entrada: 100-240VAC, 1.2A, 50-60Hz y salida: 24VDC, 1.4A).

- Debe tener 8 puertos RJ 45 para conexión de los dispositivos, 1 puerto RJ45 para conexión a red, 4 terminales de tornillo (2 entradas digitales y 2 salidas de contacto seco) y 1 slot para tarjeta SD (Secure Digital) que pueda soportar hasta 2GB de memoria.

- Debe soportar SNMP para interconexión con sistemas de monitoreo en red.

Lectora RFID con traductor Wiegan, añade la capacidad de sensado RFID y la habilidad de conectar dispositivos que usan comunicación Wiegan tales como

lectoras RFID, scanners biométricos, entre otros. Puede operar como dispositivo stand-alone que controla un pequeño grupo de dispositivos, o como un dispositivo de red que transmite información, como intentos de acceso, al resto de la red.

- Debe contener un Puerto RJ45 para conexión RS-485, 1 terminal analógico con 2 entradas y 2 salidas. Y dos botones tipo "pushbuttons" para almacenar y borrar.
- Debe ser compatible con las tarjetas de 125KHz, 64 bit.
- Debe tener 3 LEDs. 1 que indica el status, 1 que indica modo de red y 1 que indica lectura.

Software de Gestión: Interface Web: Permite control completo y administración sobre un dispositivo de interconexión de 8 puertos y los dispositivos conectados a él.

- Debe conectarse al dispositivo de interconexión a través de la dirección IP del dispositivo de interconexión.
- Debe ser accesible usando cualquier navegador de Internet estándar.
- Debe proveer la capacidad de configurar y administrar los dispositivos que conforman el sistema.
- Debe proveer administración de cuenta de usuarios. La información de cuenta de usuario debe incluir la administración de las tarjetas RFID.
- Debe proveer registro y administración de alarmas.

UPS modular

El SAI deberá ser dimensionado para una carga de 48 kVA y 48 Kw. El banco de baterías del SAI deberá estar dimensionado para una autonomía de un mínimo de 10 minutos a al 100 % de carga con un factor de potencia unitario.

El Sistema UPS deberá soportar una corriente de corto circuito CC de 30kA simétrica con fusibles de tipo gL/gG frente al sistema.

Se debe proveer 1 solo módulo de 16 KW y un transformador de aislamiento para el total de la capacidad del UPS. Asimismo, se debe considerar un tablero bypass para asegurar el funcionamiento continuo de los equipos de comunicaciones ante alguna posible falla del UPS o durante el mantenimiento de este último.

Características del Sistema

Capacidad del Sistema: El SAI deberá estar preparado para entregar la totalidad de la carga en los siguientes tamaños de bastidor:

- 48 KVA/KW con posibilidad de montaje de hasta diez (3) módulos de potencia de 16 kW para configuraciones de tipo N+0.Se proveerá un solo módulo de 16 KW.

Entrada:

- Tensión Alterna de Entrada Nominal trifásica de 3x380V/220V, 3x400V/230V, o 3x415V/240V, 4 conductores L1/R, L2/S, L3/T, N y puesta a tierra GND.

- Rango de Tensión Alterna: 340V a 477V (a un 100% de carga) un rango de 200V-477V (a un 50% de carga) proporcionando suficiente energía para cargar el banco de baterías, dependiendo de la carga el sistema podrá comenzar a cargar las baterías a partir de una tensión de suministro de 200V.

- Máximo rango tolerable de frecuencia: 40-70Hz (autosensante).

- Factor de potencia a la entrada: > 0.99 a más del 25% de carga.

- Arranque Suave: debe ser lineal de 0-100% sin exhibir picos de corriente de arranque tomando un tiempo de 10 segundos.

Salida del SAI:

- Tensión Alterna de Salida Nominal trifásica de 3x380V/220V, 3x400V/230V, o 3x415V/240V, 4 conductores L1/R, L2/S, L3/T, N y puesta a tierra GND.
- Regulación de Frecuencia: La frecuencia de salida deberá estar sincronizada a la entrada de bypass disponible de un rango de 47hz a 53hz Opcional +/- 0,1 Hz y +/- 10Hz configurable desde el panel frontal.
- Tiempo de recuperación para el transitorio de Tensión debe ser menor a los 50ms.
- Distorsión Armónica de Tensión a la Salida < 2% THD para un 100% de carga Lineal < 5% para un 100% de carga no-lineal tal como se defina en la norma EN50091-3/IEC 62040-3.
- Sobrecarga en Operación Normal: 150% durante 60 segundos en operación normal y batería. 125% durante 10 minutos en operación norma y batería.
- Eficiencia del Sistema: > 95% entre el 35% y 100% de Carga.
- Factor de Potencia a la Salida: Para cargas con factor de potencia a la entrada de 0.5 en retraso no será necesario considerar una reducción en la potencia del SAI.

Recarga de Baterías:

- 10% de la potencia de salida con bajos niveles de tensión a plena carga.
- 20% de la potencia de salida con tensiones de entrada nominales (como opcional).

Parámetros ambientales:

- Almacenamiento a Temperatura Ambiente: -15°C a 40°C.

- Temperatura de Operación: 0°C a 40°C (25°C es la temperatura de operación ideal para la mayoría de las baterías).
- Humedad relativa 0 a 95% Sin que exista condensación.
- Altitud: La máxima altitud de instalación manteniendo la potencia máxima de Salida del UPS deberá ser de 1000m. Para Otras alturas se deberá considerar una reducción en la potencia de salida de:
    a) 1500m Carga máxima 95%.
    b) 2000m Carga máxima 91%.
    c) 2500m Carga máxima 86%.

Aire Acondicionado

El control ambiental debe estar específicamente diseñado para aplicaciones de control de temperatura. Monitoreará y controlará en forma automática el enfriamiento filtrado en el espacio que acondicionará. El sistema estará construido con los más altos estándares de calidad e ingeniería siguiendo normas y estándares de fabricación. Será de montaje en piso y de enfriamiento por desplazamiento de aire horizontal. El aire atravesará cada unidad de manera tal de generar un flujo uniforme que cubra la totalidad de la serpentina.

La unidad de refrigeración debe ser de aproximadamente 10 KW y debe controlar la temperatura.

Construcción de Gabinete

- Paneles traseros y delanteros deberán ser de acero 18 perforados con una superficie de apertura total en 69,5% equipado con cerraduras para prevenir el acceso no autorizado a los componentes internos de la unidad.

- La estructura debe estar construida en acero conformado 16 soldado para máxima resistencia. Todas las unidades deben poder ser mantenidas por el frente y por la parte trasera, permitiendo que las partes sean reemplazadas sin remover la unidad de la fila.

- Todos los paneles exteriores deberán estar pintados con pintura en polvo para mayor durabilidad.

- Las unidades deberán incluir ruedas y patas niveladoras para nivelar los equipos en la fila de gabinetes IT.

Forzadores

Forzadores CC de velocidad variable y accionamiento directo:

- La unidad debe estar configurada para un flujo que atraviese la misma proporcionando un patrón de aire uniforme en toda la cara de la serpentina. Cada unidad deberá incluir unos 6 (seis) forzadores de 200mm de CC velocidad variable y accionamiento directo. Cada forzador deberá proporcionar 180,1 L/s (381,7 CFM) para alcanzar un flujo total de 1080,76 L/s (2290 CFM).

- Los forzadores podrán modular su capacidad entre un 30% y 100%. Deberán poder realizar un arranque suave para evitar picos de arranque.

- Cada conjunto de forzador estará compuesto por un marco inyectado en plástico moldeado con protección para los dedos.

- En caso de falla de un forzador la unidad deberá seguir operando pudiéndose reemplazar el elemento en falla por otro sin necesidad de apagar el equipo mientras se encuentra en operación.

Tarjeta de Red WEB/SNMP

La unidad debe incluir una tarjeta de Management WEB-SNMP para poder administrar, controlar y operar la unidad desde una computadora a través del protocolo TCP-IP. Se deberán poder visualizar alarmas y modificar temperaturas de trabajo.

Serpentina de enfriamiento y bandeja de condensado

La unidad deberá utilizar venturis de aluminio corrugado y tuberías de cobre en sus serpentinas. La cabecera de la serpentina estará equipada con un colector para gotas de condensado.

Compresor

Compresor Scroll

Alto nivel EER (hasta 20.0) pocas partes móviles deberán proporcionar una operación eficiente y confiable.

Filtros

Los filtros estándar deberán ser un 20% eficientes de acuerdo a ASHRAE 52.1 MERV Clase 1 ½" malla lavable.

Sensores de Temperatura

Sensores de Temperatura Internos: La unidad deberá contar con sensores tipo termistores montados en la parte frontal y posterior del equipo de modo de poder medir la temperatura de inyección y retorno.

Sensores de Temperatura Remotos:

La unidad deberá contar con un sensor de temperatura remoto que deberá ubicarse en un gabinete IT cercano para medir la temperatura de ingreso del aire refrigerado.

Monitoreo Ambiental

La solución de monitoreo debe permitir conocer las variables críticas más importantes del cuarto de cómputos de manera tal que sean detectables en forma automática niveles de temperatura, humedad, presencia de líquidos y demás condiciones que puedan afectar la operación de la carga crítica.

La solución de monitoreo ambiental deberá registrar en todo momento los siguientes datos:

- 3 sensores por cada gabinete, dos de temperatura y uno de temperatura más humedad al centro.
- Se instalarán en la puerta frontal de los gabinetes.
- Se debe considerar un sensor de aniego.

Todos los sensores deberán conectarse a un dispositivo concentrador de montaje en gabinete con una altura que no supere 1U. Además del dispositivo concentrador podrán utilizarse en caso que sea posible los canales de tensión con conectores para sensores de temperatura.

Acerca del dispositivo central de monitoreo

- Debe poseer indicadores tipo LED que indiquen la existencia de un estado de alerta, funcionamiento correcto del vínculo de conexión a la red, y luz de encendido.
- Debe soportar sensores de: Temperatura, Humedad, Temperatura y Humedad, Apertura de Puertas, Humo, Presencia de líquidos, Vibraciones, Contactos secos, señales de 0-5V y 4 a 20mA.
- Capacidad de ampliar la cantidad de sensores hasta alcanzar los 72.

- Puertos de Conexión disponibles: Conexión Ethernet: (1) 10/100 Base-T, (6) Puertos para Sensores, (1) Puerto USB para Configuración Tipo B, (2) Puertos USB – Tipo A, (1) Puerto A-Link, (1) Salida de Voltaje, (2) Salidas de Relé, (4) Puertos de Entrada de 4-20 mA, (1) Puerto de Alarma, (1) Puerto para cuerda para detección de fluídos.

- Protocolos Soportados: TCP/IP, HTTP, HTTPS, SMTP, SNMP v1, v2c, y v3, DHCP, DNS, Socks v4 or V5 Proxy Server, A-Link.

- Temperatura de operación: 0 -45°C; Humedad Relativa: 10-90% (sin condensación).

Instalación Servicios

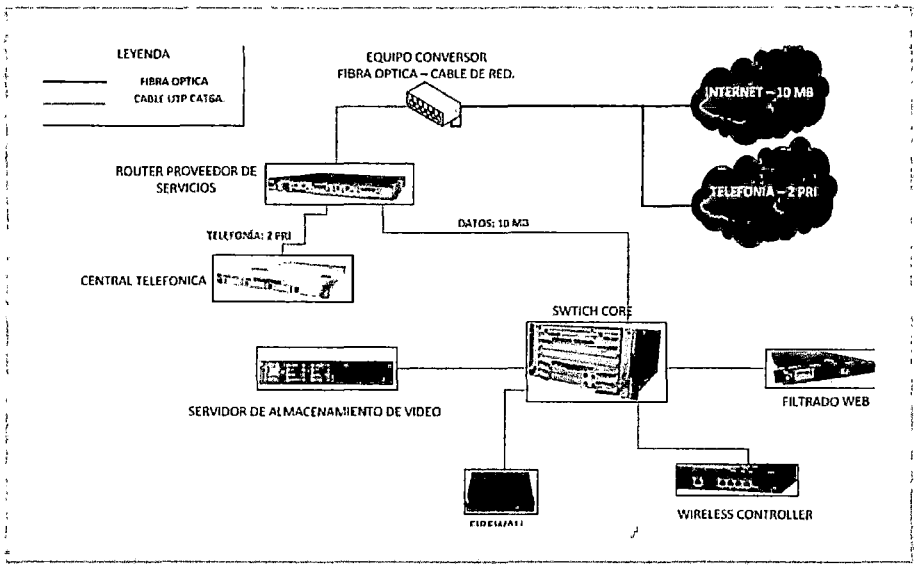
Se deberá realizar la instalación montaje y configuración de la solución de monitoreo incluyendo todo el cableado necesario para la misma.

Se debe incluir la parametrización y configuración de alarmas de acuerdo a las recomendaciones de ASHRAE y los límites que se disponen para el adecuado funcionamiento de los entornos de IT.

En la siguiente ilustración, se muestra el diagrama de conexión de los equipos de comunicaciones dentro del Data Center, así como también el medio de transporte.

Ilustración 5.11

Interconexión de equipos de comunicaciones en el data center



Fuente: Elaboración propia

Sistemas de comunicaciones

Se utiliza para conectar varios dispositivos a través de la misma red dentro de un edificio u oficina. Por ejemplo, puede conectar computadoras, impresoras y servidores, creando una red de recursos compartidos. La plataforma actúa como controlador, permitiendo a los diferentes dispositivos compartir información y comunicarse entre sí. Mediante el uso compartido de información y la asignación de recursos, también permite ahorrar dinero y aumentar la productividad. La plataforma de switching admite voz, video, datos y acceso sumamente seguro. También brinda administración escalable para adaptarse a diferentes escenarios de gestión de red. También tiene la funcionalidad de brindar alimentación eléctrica por Ethernet (PoE, Power over Ethernet) opcional para teléfonos IP, Access Point, Cámaras IP, entre otros.

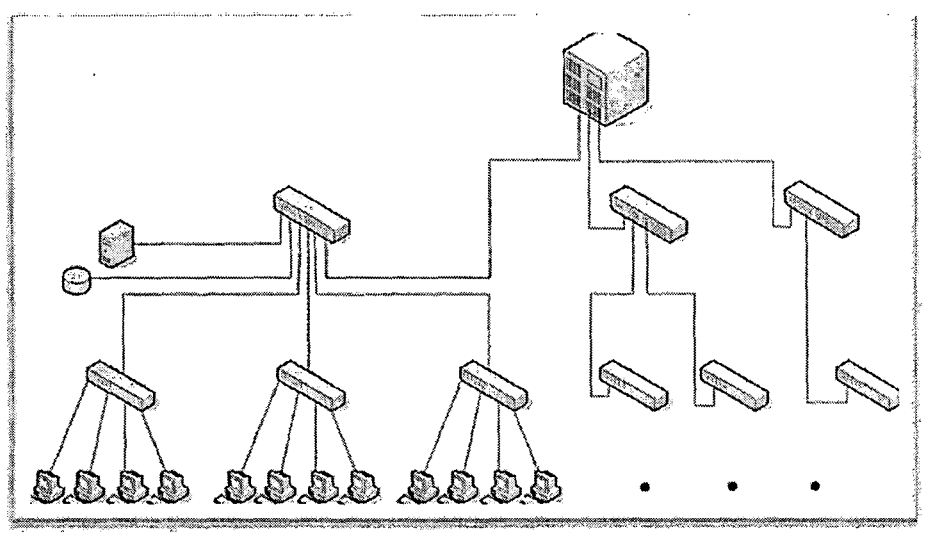
En la siguiente figura, se puede apreciar los equipos más importantes que se implementarán en el Data Center:

Esta plataforma esta subdividida por jerarquía en 3 tipos de switches:

- Switch Core.
- Switch de Distribución.
- Switch de Acceso.

Ilustración 5.12

Jerarquia de swtich



Fuente: Elaboración propia

Switch Core

- Switch multicapa con arquitectura basada en chasis.
- Capacidad de Operación en capas 2, 3 y 4 del Modelo OSI.
- El equipo debe soportar los estándares relacionados: IEEE 802.3, 10BaseT, IEEE 802.3u, 100BaseTX, IEEE 802.3z, 802.3ab, 1000BaseT, 10 Gigabit Ethernet IEEE 802.3ae.
- Switch fabric instalado y operativo de 848 Gbps mínimo.

- Tasa de envío de 250 Mpps instalados y operativos, tanto en Capa 2 como en Capa 3.
- Incluir redundancia en:
    - Módulo de procesamiento o Supervisor.
    - Switch Fabric.
    - La redundancia de estos elementos debe operar de manera que ante la falla de uno, el redundante garantice que el equipo continuará operando al 100%, tanto en su capacidad como en sus funcionalidades en capa 2 y 3.
- El equipo debe soportar interfaces 10Gbps. Las interfaces deben estar disponibles en el mercado al momento de presentar la oferta y deben soportar mínimo 2 puertos de 10Gbps por módulo de procesamiento o supervisor.
- Soporte de tarjetas externas USB y SD para opciones flexibles de almacenamiento.
- Flexibilidad para operar en 6, 24 or 48 Gbps por slot line card sin degrader la performance.
- Debe incluir 12 puertos SFP de 1Gbps como mínimo.
- Los módulos de procesamiento o Supervisor deben ser Hot-Swap.
- Soporte de 4,000 VLAN's mínimo. VLAN trunk IEEE 802.1Q.
- Soporte de 45,000 direcciones MAC mínimo.
- Soporte de Spanning Tree IEEE 802.1d así como las últimas mejoras tales como RST 802.1w y MST 802.1s.

- Ruteo IP. Enrutamiento entre VLANs. Enrutamiento IPv4 estático y dinámico RIPV1 y RIPV2 con capacidad de ampliación a otros protocolos como OSPF y BGPv4 sin cambio de hardware.
- Multicast IGMPv1, v2 y v3 y PIMv1 y v2.
- Soporte de Calidad de Servicio.
    - IEEE 802.1p CoS.
    - Cuatro colas de salida por puerto.
    - Clasificación de tráfico basada en direcciones IP de origen y destino y puertos TCP/UDP.
    - DSCP.
    - Limitación de ancho de banda basada en direcciones IP de origen y destino y puertos TCP/UDP.
- Mecanismos de Seguridad:
    - Seguridad por puerto en base a la dirección MAC.
    - Filtros aplicables por puerto y por VLAN.
    - Filtros basados en direcciones MAC de origen y destino, direcciones IP de origen y destino y puertos TCP/UDP.
    - Soporte de autentificación 802.1x, con asignación dinámica de VLAN.
    - Control de acceso centralizado por RADIUS, ya sea para los administradores del switch como para los usuarios de la red que se autentifican vía 802.1x.
    - Al menos 6 niveles de privilegios de acceso para administración por consola o por Telnet.

- Administración vía protocolos seguros como SNMPv3 encriptado y SSHv2.
- Soporte de mecanismos para evitar ataques tipo DoS y MITM, basados en STP, ARP, DHCP e IP, tales como "MAC Address Flooding", "VLAN Hopping", "DHCP Rogue Server", "ARP Poisoning" y "IP Spoofing".
- Asignación dinámica de VLANs vía 802.1x.
- MAB (MAC Authentication Bypass) via 802.1x.

- Mecanismos de gestión:
  - Puerto de consola para gestión local.
  - Soporte de Telnet, http y SSHv2 para gestión remota.
  - Registro de eventos vía Syslog.
  - Soporte de SNMP v2 y v3.
  - Soporte de RMON.
  - Soporte de protocolos de transferencia de archivos TFTP, FTP, RCP.
  - Soporte de protocolos NTP, DHCP, DNS.
  - El equipo debe tener capacidad de comportarse como servidor DHCP.
  - Soporte de "port mirroring" por puerto o grupo de puertos y por VLAN.
  - Soporte de múltiples sesiones de "port mirroring" así como "port mirroring" remoto.
  - Los switches propuestos deberán poseer un mecanismo que permiten diagnosticar problemas de cableado, sin necesidad de tener este tipo de

herramientas y así acelerar la resolución de problemas atribuibles al cableado y fibra óptica.

- Stack de protocolos IPv6 para administración con funciones mínimas: ping, HTTPS, SSH.
- El equipo debe poder comportarse como servidor DHCP.

- Agregación de puertos, LACP, IEEE 802.3ad, de modo que se pueda usar cualquier puerto del switch del mismo tipo y velocidad.
- Fuente de poder con alimentación a 220Vac 60Hz.
- Montable en rack 19".
- Software actualizable. Incluir la última versión disponible.

Switch de Acceso de 24 puertos PoE

- Switches Capa 2 (L2).
- 24 puertos 10/100/1000 PoE Autosensing.
- 04 puertos SFP y/o 10/100/1000BaseT.
- Herramienta embebida para diagnosticar y resolver problemas con el cableado en los puertos de cobre. (TDR: Time-domain reflectometer).
- Velocidad Stacking 20 Gbps.
- Permitir hasta 4 participantes en el Stack.
- Switch Fabric mínimo de 176 Gbps.
- Tasa de envío mínima de 41.7 Mpps en Capa 2 (basado en paquetes de 64 bytes).

- Memoria Flash 64Mb.
- Memoria DRAM 128 Mb.
- 250 VLANs minima. VLAN trunk IEEE 802.1Q.
- 4000 VLAN IDs.
- 8,000 direcciones MAC mínimo.
- Mean Time between Failures (MTBF) 245,604 horas.
- La solución debe soportar los estándares relacionados: IEEE 802.3, 10BaseT, IEEE 802.3u, 100BaseTX, IEEE 802.3z, 802.3ab, 1000BaseT.
- Soporte de Spanning Tree IEEE 802.1d así como las últimas mejoras tales como RST 802.1w y MST 802.1s.
- Soporte de Spanning Tree como mínimo.
- Soporte de Per-VLAN Spanning Tree Plus (PVST+) para acelerar la reconvergencia de spanning tree por VLAN.
- Soporte de Multicast IGMPv1, v2 y v3 Snooping.
- 250 grupos de IGMP mínimo.
- Soporte de Calidad de Servicio.
    - IEEE 802.1p CoS.
    - Cuatro colas de salida por puerto.
    - Clasificación de tráfico basada en direcciones MAC de origen y destino, direcciones IP de origen y destino y puertos TCP/UDP.
    - DSCP.

- Limitación de ancho de banda basada en direcciones MAC de origen y destino, direcciones IP de origen y destino y puertos TCP/UDP.
- Configuración automática de QoS.
- Los switches deben incluir la capacidad de supresión de broadcast, multicast y unicast.

- Mecanismos de Seguridad:
  - Seguridad por puerto en base a la dirección MAC.
  - Filtros aplicables por puerto.
  - Filtros basados en direcciones MAC de origen y destino, direcciones IP de origen y destino y puertos TCP/UDP.
  - Soporte de autentificación 802.1x, con asignación dinámica de VLAN.
  - Control de acceso centralizado por RADIUS, ya sea para los administradores del switch como para los usuarios de la red que se autentifican vía 802.1x.
  - Al menos 6 niveles de privilegios de acceso para administración por consola o por Telnet.
  - Administración vía protocolos seguros como SNMPv3 encriptado, SSHv2 y SSL.
  - Soporte de mecanismos para evitar ataques tipo DoS y MITM, basados en STP y DHCP, así como "MAC Address Flooding", "DHCP Rogue Server".

- Mecanismos de gestión:
  - Puerto de consola para gestión local.

- Soporte de Telnet, http, https y SSHv2 para gestión remota.
- Stack de protocolos IPv6 para administración con funciones mínimas: ping, HTTPS, SSH.
- Soporte del estándar IEEE 802.1AB (LLDP: Link Layer Discovery Protocol) para intercambio de información de dispositivos en redes multivendor.
- Registro de eventos vía Syslog.
- Soporte de SNMP v1, v2c y v3.
- Soporte de RMON.
- Soporte de protocolos de transferencia de archivos TFTP, FTP, RCP, SCP.
- Soporte de protocolos NTP, DHCP.
- Soporte de "port mirroring" por puerto o grupo de puertos y por VLAN.
- Soporte de múltiples sesiones de "port mirroring" así como "port mirroring" remoto.
- Los switches propuestos deben incluir un mecanismo que permiten diagnosticar problemas de cableado, sin necesidad de tener este tipo de herramientas por separado.
- El puerto de monitoreo debe permitir colocar un dispositivo de detección de intrusos, de modo que este pueda enviar paquetes de reseteo de sesiones TCP a través del mismo puerto (puerto bidireccional).

- Agregación de puertos, LACP, IEEE 802.3ad, de modo que se pueda usar cualquier puerto del mismo tipo y velocidad.

- Fuente de poder con alimentación a 220Vac 60Hz, con capacidad de soportar fuente de poder redundante.
- Soporte de Energiwise.
- Montable en rack 19".
- Software actualizable. Incluir la última versión disponible.

Switches de Acceso de 24 puertos

- Switches Capa 2 (L2).
- 24 puertos 10/100/1000 Autosensing.
- 04 puertos SFP y/o 10/100/1000BaseT.
- Herramienta embebida para diagnosticar y resolver problemas con el cableado en los puertos de cobre. (TDR: Time-domain reflectometer).
- Velocidad Stacking 20 Gbps.
- Switch Fabric mínimo de 176 Gbps.
- Tasa de envío mínima de 41.7 Mpps en Capa 2 (basado en paquetes de 64 bytes).
- Memoria Flash 64Mb.
- Memoria DRAM 128 Mb.
- 250 VLANs minima. VLAN trunk IEEE 802.1Q.
- 4000 VLAN IDs.
- 8,000 direcciones MAC mínimo.

- Mean Time between Failures (MTBF) 349,824 horas.
- La solución debe soportar los estándares relacionados: IEEE 802.3, 10BaseT, IEEE 802.3u, 100BaseTX, IEEE 802.3z, 802.3ab, 1000BaseT.
- Soporte de Spanning Tree IEEE 802.1d así como las últimas mejoras tales como RST 802.1w y MST 802.1s.
- Soporte de Spanning Tree como mínimo.
- Soporte de Per-VLAN Spanning Tree Plus (PVST+) para acelerar la reconvergencia de spanning tree por VLAN.
- Soporte de Multicast IGMPv1, v2 y v3 Snooping.
- 250 grupos de IGMP mínimo.
- Soporte de Calidad de Servicio.
    - IEEE 802.1p CoS.
    - Cuatro colas de salida por puerto.
    - Clasificación de tráfico basada en direcciones MAC de origen y destino, direcciones IP de origen y destino y puertos TCP/UDP.
    - DSCP.
    - Limitación de ancho de banda basada en direcciones MAC de origen y destino, direcciones IP de origen y destino y puertos TCP/UDP.
    - Configuración automática de QoS.
    - Los switches deben incluir la capacidad de supresion de broadcast, multicast y unicast.

- Mecanismos de Seguridad:
  - Seguridad por puerto en base a la dirección MAC.
  - Filtros aplicables por puerto.
  - Filtros basados en direcciones MAC de origen y destino, direcciones IP de origen y destino y puertos TCP/UDP.
  - Soporte de autentificación 802.1x, con asignación dinámica de VLAN.
  - Control de acceso centralizado por RADIUS, ya sea para los administradores del switch como para los usuarios de la red que se autentifican vía 802.1x.
  - Al menos 6 niveles de privilegios de acceso para administración por consola o por Telnet.
  - Administración vía protocolos seguros como SNMPv3 encriptado, SSHv2 y SSL.
  - Soporte de mecanismos para evitar ataques tipo DoS y MITM, basados en STP y DHCP, así como "MAC Address Flooding", "DHCP Rogue Server".
- Mecanismos de gestión:
  - Puerto de consola para gestión local.
  - Soporte de Telnet, http, https y SSHv2 para gestión remota.
  - Stack de protocolos IPv6 para administración con funciones mínimas: ping, HTTPS, SSH.

- Soporte del estándar IEEE 802.1AB (LLDP: Link Layer Discovery Protocol) para intercambio de información de dispositivos en redes multivendor.
- Registro de eventos vía Syslog.
- Soporte de SNMP v1, v2c y v3.
- Soporte de RMON.
- Soporte de protocolos de transferencia de archivos TFTP, FTP, RCP, SCP.
- Soporte de protocolos NTP, DHCP.
- Soporte de "port mirroring" por puerto o grupo de puertos y por VLAN.
- Soporte de múltiples sesiones de "port mirroring" así como "port mirroring" remoto.
- Los switches propuestos deben incluir un mecanismo que permiten diagnosticar problemas de cableado, sin necesidad de tener este tipo de herramientas por separado.
- El puerto de monitoreo debe permitir colocar un dispositivo de detección de intrusos, de modo que este pueda enviar paquetes de reseteo de sesiones TCP a través del mismo puerto (puerto bidireccional).

- Agregación de puertos, LACP, IEEE 802.3ad, de modo que se pueda usar cualquier puerto del mismo tipo y velocidad.
- Fuente de poder con alimentación a 220Vac 60Hz, con capacidad de soportar fuente de poder redundante.
- Soporte de Energiwise.

- Montable en rack 19".
- Software actualizable. Incluir la última versión disponible.

Comunicaciones Unificadas

Requiere contar con un sistema de comunicaciones unificadas que permita comunicar a todas las oficinas y funcionarios en una sola red escalable y convergente. Esta comprende básicamente tres subcomponentes:

Telefonía IP: La aplicación virtualizable de procesamiento de llamadas, video-llamadas y audio-conferencias entre diferentes end-points como Teléfonos IP, Video-Teléfonos IP y Computadoras en tiempo real, proporciona una plataforma de Telefonía IP escalable y de alta disponibilidad, permitiendo conectar a usuarios fijos y móviles. Ofrece enrutamiento de llamadas y video-llamadas, gestión de colas, funciones de conferencia, localización. Las llamadas y video-llamadas dentro de la red interna de la MP Huaraz serán gratuitas e ilimitadas, ya que el procesamiento y establecimiento de cada llamada o video-llamada se lleva a cabo en esta aplicación, es decir en la misma red de la MP Hz por tanto no genera ningún costo con el ISP. Asimismo, esta aplicación deberá conectarse a la Red de Telefonía Fija PSTN a través de líneas telefónicas o Primarios de voz, los cuales enlazarán a todos los anexos o terminales de Telefonía IP con la PSTN y de esta manera puedan comunicarse no solo entre anexos o terminales sino también con cualquier número fijo o móvil local, nacional o internacional, cabe mencionar que esto último si genera un costo con el ISP.

Mensajería Unificada: La aplicación virtualizable de mensajería unificada comprende un potente sistema de mensajería de voz, la cual permite a los usuarios escuchar sus mensajes de voz por teléfono, controlar los mensajes de voz por internet, así como enviar, recibir o reenviar faxes a cualquier parte donde se encuentren. Las opciones de buzón de voz, mensajería integrada forman parte de esta aplicación con altos índices de escalabilidad. Cada end-point de la MP Hz podrá acceder a esta aplicación de manera ilimitada, así como también podrá

gestionar toda su mensajería de manera rápida y sencilla. Cabe mencionar, que esta aplicación no genera ningún cargo o costo con el ISP.

Presencia: La aplicación virtualizable de presencia suma otra capa de funciones a la plataforma de comunicaciones unificadas, mediante la información de presencia dinámica, los usuarios pueden comprobar la disponibilidad de sus colegas en tiempo real, además esta aplicación comprende la instalación de un software licenciado que integra comunicaciones de datos, mensajería instantánea, voz sobre IP, telefonía IP, mensajería unificada, video-llamada y movilidad, todo sobre la misma plataforma IP del sistema de comunicaciones unificadas montada en el servidor virtualizado. Cabe agregar, que esta aplicación permitirá establecer su anexo telefónico para llamadas y video-llamadas, perfil de mensajería instantánea, buzón de voz, etc. en múltiples dispositivos fijos y móviles como smartphones, tablets, laptops, etc. Estas comunicaciones no generarán ningún costo con el ISP, pero si requiere estar conectado a la red interna de la MP Huaraz ya sea vía cableada o inalámbrica, si el usuario se encuentra fuera de la red interna, una buena conexión a internet, donde se establecerá una VPN.

Servidor de Comunicaciones

- Solución que permita manejar soluciones de colaboración en entorno virtualizado.
- Soporte de sistemas de tele presencia.
- Soporte de protocolo BFCP (Binary Floor Control Protocol).
- Encriptación de video.
- DSCP para llamadas de telepresencia.
- Procesamiento de hasta 1000 usuarios (considerar inicialmente 100 usuarios).
- Capacidad de configuración de modos de ahorro de energía en los teléfonos.

- Mejoras en el servicio de directorio a través de los servicios compartidos de data unificada.
- Soporte de video en HD en clientes de telepresencia y teléfonos IP.
- Soporte de códec H.264.
- Soporte de negociación de payload del códec H.264 para mejor resolución.
- Soporte de cambios y consolidación de códec de video en la llamada iniciada.
- Debe contar con una página amigable para añadir teléfonos, consistente en check box por defecto, oculto y de sólo lectura.
- Soporte de protocolo de reserva de recursos (RSVP).
- Movilidad de extensión, cambio de PIN en el teléfono.
- HTTPS para funciones del teléfono.
- Encendido/Apagado de movilidad con interface SIP.
- Servicio de control externo de llamadas.
- Integración Teléfono Computador (CTI) con lista para búsquedas y captura de llamadas.
- Soporte de CTI para reenvío de llamadas.
- Grabación y monitoreo de llamadas de forma segura.
- Soporte de protocolos SIP y SCCP.
- Indicador de audio mensaje de espera.
- Selección de ruta de forma automática.

- Soporta Control de admisión de llamadas.
- Soporte de grabación de llamadas para llamadas encriptadas o no encriptadas.
- Análisis de dígito y tratamiento de llamadas.
- Particionamiento del Dial-Plan.
- Control de llamadas externas, que permita hacer uso de API para permitir tomar las decisiones de enrutamiento de llamadas fuera del servidor de procesamiento de llamadas.
- Fax sobre IP.
- Soporte de H323.
- Debe proporcionar utilidades de monitoreo y depuración:
    - Reportes históricos, vistas de monitoreo y alertas pre configuradas.
    - Monitoreo de performance de aplicaciones (histórico y de tiempo real) a través de herramientas de monitoreo y SNMP.
    - Servicio de colección de data monitoreada.
    - Servicios de terminal remoto para monitoreo y alertas Off-net.
    - Monitoreo de eventos en tiempo real y presentación en Syslog.
- Bloqueo de llamadas salientes.
- Soporte de QSIG.
    - Llamada básica.
    - Servicios de identificación.
    - Devolución de llamadas (Call Back).

- Transferencia de llamadas.
- Prevención de loops.

- Debe ser capaz de realizar conferencias seguras.
- Debe ser capaz de configurar modos de operación seguro y no seguro.
- Debe permitir la autenticación del usuario.
- Debe contar con mecanismos para asegurar la integridad de los datos (cifrado TLS, SHA1 hash, encriptación de la señalización y el medio).
- Administración del servidor mediante HTTPS.
- Soporte de SSL para el directorio de llamadas.
- Detección de la actividad de la voz y supresión del silencio.
- Enrutamiento de llamadas y configuración de restricciones basados en horas del día, días de la semana y días del año.
- Soporte de códec de video.
- Soporte de video telefonía.
- Rastreo e identificación de origen de llamada maliciosa.
- Capacidad de integrar un cliente VPN en el teléfono IP.
- Debe permitir la movilidad del usuario (llevar su número de anexo a dispositivos como smartphones, tablets, softphones, etc.).
- Debe incluirse la solución de mensajería de voz (considerar 100 buzones).

Terminal Video-Telefónico IP

- Display LCD a color basado en pixeles preparado para recibir aplicaciones, con dimensiones mínimas de 640x480 pixeles, debe incluir y una calidad de imagen no menor a 24-bit.
- Debe soportar video llamada de por lo menos 30 frames por segundo e incluir una pantalla a color de 5 pulgadas.
- Debe soportar 5 líneas como mínimo (Cada línea con llamada en espera) expansible a 77 líneas con la adición de un módulo de expansión.
- Debe soportar un máximo de hasta 200 llamadas por dispositivo.
- Debe contar con 4 teclas dinámicas, como mínimo, para guiar al usuario a través de las funciones.
- Soporte de 802.3af (Power over Ethernet).
- Debe incluir interfaz Bluetooth y un puerto RJ-9 para Headset y 02 puertos USB para headseat y cámara.
- Debe permitir al usuario ajustar el contraste de la pantalla y seleccionar el tono del timbre y los parámetros de volumen para todo el audio.
- Posibilidad de establecer preferencias de configuración de la red. La configuración puede definirse de forma automática o manual para DHCP (Dynamic Host Control Protocol), TFTP (Trivial File Transfer Protocol).
- Soporte XML.
- Debe poder mostrar información histórica de llamadas perdidas, llamadas hechas y llamadas recibidas. Así también permitir mostrar el estado de presencia de los usuarios de la institución mediante las opciones mencionadas.

- Indicación visual y/o audible si el teléfono tiene una llamada en espera.
- Indicación visual si el usuario tiene un mensaje de voz.
- Switch interno Ethernet de dos puertos que permita realizar conexiones directas con redes Ethernet 10/100/1000 BaseTx (como mínimo) a través de una interfaz RJ-45 con conexión LAN tanto para el teléfono como para un PC en la misma ubicación.
- Capacidad para designar LAN virtuales independientes (VLAN) (802.1Q) para el PC y los teléfonos IP.
- Soporte de elementos de Calidad de Servicio: DSCP (differentiated services code point) y estandares 802.1Q/p.
- Puerto dedicado de auriculares.
- Compresión de sonido G.711 y G.729a.
- Soporte de protocolo SIP.
- Una asignación de dirección IP: configurado por cliente DHCP o de modo estático.
- Programación de la generación de ruido de apaciguamiento y detección de actividad de voz por cada sistema.
- Puerto EIA/TIA RS-232 para poder añadir en el futuro opciones como la expansión de líneas, el acceso a la seguridad y muchas más.
- Contraste de la pantalla.
- Configuración del Tipo de timbre.
- Configuración de la red.

- Estado de las llamadas.
- Descarga de cambios del firmware desde el servidor central.
- Debe soportar el empleo de una fuente externa de 48 VCC, que se suministran a nivel local en el escritorio mediante una fuente de alimentación.
- Soporte de movilidad del Teléfono. Los usuarios pueden registrarse a cualquier teléfono de este tipo de tal forma que todas las características personales (Voicemail, perfiles de la línea, número de líneas, etc.) pasen al mismo.
- Soporte de códec de audio G.722 para sus diferentes opciones de comunicación (manos libres, auricular, etc.).
- Soporte de códec de audio iLBC para escenarios hostiles de conexión.
- Manejo de h.264 para el funcionamiento de videollamadas en alta definición con la cámara USB.
- Soporte de SRTP para la encriptación de los paquetes de voz que viajan sobre la red.
- Soporte de mecanismos de calidad de servicio para garantizar la mejor experiencia de usuario.

Seguridad de la Información

La información es el bien más preciado de todas las instituciones y por esta razón debe ser protegida de manera adecuada. Partiendo de este hecho, las instituciones deben encaminar sus esfuerzos e inversiones en soluciones tecnológicas que permitan alcanzar niveles adecuados en el campo de la seguridad de la información, establecer los límites de un adecuado uso de la misma y garantizar el cumplimiento de las políticas y normativas de seguridad definidas.

Esta plataforma permitirá asegurar la seguridad de los datos y sistemas informáticos que se transmitan tanto por la red interna como por internet, reduciendo notablemente la posibilidad de hackeo informático, fuga de información desde locaciones internas, prevención de fallas, entre otros.

Seguridad Perimetral

- Solución de seguridad de IPS, Firewall y VPN dentro de hardware de propósito específico que deberá contar con sistema operativo propietario, el mismo que deben ser desarrollados íntegramente por el mismo fabricante.

- El sistema de seguridad deberá poseer licenciamiento ilimitado de usuarios y host, tanto a nivel de Firewall, de IPS y de VPN.

- El Firewall podrá operar en un esquema de alta disponibilidad, redundancia y tolerancia a fallas y en la eventualidad que uno de ellos falle el otro asuma la carga de trabajo.

- El Troughput solicitado para cada una de las características de seguridad deben de ser como mínimo de:

    - FW: 1 Gbps

    - IPS: 250Mbps

    - VPN: 200 Mbps

- Debe soportar esquemas de virtualización, que permitan definir entornos de análisis distintos. Este esquema de virtualización debe de permitir separar recursos dedicados por cada esquema de virtualización de manera configurable e independiente.

- Debe soportar los siguientes protocolos y servicios de comunicación: TCP/IP, HTTP, HTTPS, FTP, POP3, SMTP, TELNET, RPC, DNS, SQL-Net,

Servicios de Multimedia como video-conferencia, servicios de broadcast y soporte de actualización de servicios.

- Debe permitir bloquear código Java, Active X y otros scripts y applets que puedan ser maliciosos.

- Capacidad de poder hacer filtraje dentro de puertos TCP conocidos (por ejemplo el puerto 80 de http), aplicaciones potencialmente peligrosas como P2P (KaZaA, Gnutella, BitTorrent) o Messengers (Yahoo!, MSN, ICQ).

- Debe permitir bloquear comandos HTTP no deseados y cadena de caracteres que indiquen la posibilidad de ser un gusano/troyano en general. Además de poder crear patrones de caracteres en el análisis del tráfico http para filtrado.

- Capacidad incluida e integrada para detección y rechazo de ataques conocidos y desconocidos, protegiendo al menos de los siguientes ataques conocidos: Suplantación de IP (IP Spoofing), Inundación de paquetes con SYN (SYN Flooding), Rastreo de puertos abiertos (Port Scanning), Ping de la muerte, Inundación de ICMP (ICMP Flood), Cross-Side Scripting.

- Debe permitir exportar los archivos LOG de los eventos detectados por el Sistema.

- Los componentes de la solución deberán poseer las configuraciones localmente, no dependiendo su funcionamiento de las consolas de administración, una falla en la consola no debe dejar fuera de servicio a los equipos remotos.

- La configuración de equipos de la solución deberá almacenarse además de centralmente, localmente de manera redundante.

- Los administradores que accedan a los firewalls deberán poder autenticarse mediante algún medio seguro que permita tener doble autenticación.

- El mecanismo de control utilizado por el motor del equipo deberá estar basado en técnicas "statefull inspection" que crean conexiones virtuales, incluso para los protocolos connection-less como UDP y RPC.

- Deberá incluir técnicas de anti-spoofing sobre cada zona de seguridad teniendo la capacidad de activación y desactivación de dicha funcionalidad.

- Deberá poseer capacidad de manejo de apertura de puertos dinámicos en base a protocolos de uso común (FTP, H323, H239, SIP, SCCP) y posibilidad de crear sesiones personalizadas que manejen dicho comportamiento.

- El equipo deberá permitir la configuración de políticas de Calidad de Servicio bajo todas o a cada una de las siguientes:

    - Configuración por protocolo y por regla.

    - Configuración de Ancho de banda garantizado.

    - Configuración de Ancho de banda mínimo tanto para tráfico de entrada como de salida.

- Deberá de soportar mecanismos de alta disponibilidad: Activo/pasivo o Activo/Activo. Este mecanismo, ante tráfico asimétrico, deberá de conservar las sesiones entre los equipos que participan en el esquema.

- Soporte de IPv6.

- Modos de operación transparente y gateway. En los dos modos debe de soportar IPv6 para futuras implementaciones.

- El firewall debe de tener la capacidad de soportar el protocolo Netflow o similares para poder tener información del estado de las sesiones de manera granular.

- Debe de soportar la capacidad de detección de "zombies" en la red. Esta capacidad, permitirá detectar máquinas infectadas con gusanos, los dominios que usan para enviar información, así como también los puertos de comunicación.

- Certificación FIPS 140-2.

- El sistema deberá proveer una consola de administración independiente de los firewalls basado en GUI permitiendo la administración y monitoreo centralizado de políticas de firewall, en una consola de administración central, donde los cambios son aplicados al componente de la solución de manera simple.

- El acceso al GUI debe de soportar OTP usando tokens.

- El sistema deberá tener acceso mediante una línea de comando segura CLI (SSH) con la finalidad realizar configuraciones mediante este medio.

- La comunicación entre la consola de administración y los demás componente de la solución debe estar encriptada y autenticada.

Filtrado Web

- Debe permitir reportes globales que permitan identificar y solucionar los problemas de malware, infecciones potenciales y actividades de botnet.

- Debe permitir la evaluación de todos los puertos de la capa 4 a velocidad de cable, bloqueando actividad spyware y deteniendo malware que intentan sobre pasar el puerto 80.

- Debe comparar el tráfico web solicitado por el usuario contra las políticas asignadas por el administrador.

- Debe proveer visibilidad y protección de las violaciones de uso web por medio de la combinación de un filtrado URL basado en listas y una categorización dinámica en tiempo real.
- Debe contener un sistema de filtros por reputación web.
- Debe soportar un sistema anti-malware.
- Debe poder identificar tráfico malware sobre el puerto 80.
- Debe soportar firmas de múltiples malware en una sola plataforma.
- Debe permitir el control avanzado de las aplicaciones.
- El procesador de ser un Quad Core.
- Debe tener 4GB de memoria RAM.
- Debe tener capacidad de discos duros de 1.8TB.
- Debe tener RAID 1 por Software.
- Debe tener 5 interfaces 10/100/1000 Base TX (RJ-45).
- Debe tener un puerto serial RS-232 (RJ-45).
- Se debe poder gestionar mediante interfaz web con protocolo seguro.
- Se debe poder gestionar por medio de conexiones remotas Telnet y/o SSH.
- Debe poder soportar transferencias de archivos por SCP y FTP.
- Debe soportar el monitoreo por medio de SNMPv1-3 y tener la capacidad de alertas por correo.
- Debe ser de 2RU.

Video Vigilancia

Se debe considerar la instalación y cableado estructurado para el sistema de video vigilancia en los puntos que se requieran.

El presente proyecto define la implementación del sistema de video vigilancia, el cual debe ofrecer escalabilidad, alto performance y una arquitectura basada en plataforma IP.

Las cámaras que se propongan deberán cumplir las siguientes especificaciones como mínimo:

- Cámara IP nativa de Alta Definición (mínimo 720p).
- Función Día/Noche.
- Compresión de video digital: H.264, MPEG-4 y M-JPEG.
- Frecuencia de imágenes: Hasta 30 fps a 1280x720p.
- Sensibilidad lumínica: .5 lux a colores y 0.3 a blanco y negro a F1.2.
- Entrada para transmisión bidireccional de audio.
- Alimentación a través de PoE.
- Debe incluir una carcasa del mismo fabricante si se trata de cámaras fijas.

El servidor deberá cumplir las siguientes especificaciones como mínimo:

- Soporte para 4 cámaras como mínimo.
- Comprensión de video H.264, MPEG -4 Y JPEG.
- Compresión de audio G.711 y G.726.
- Plataforma abierta capacidad para utilizar con cámaras de diferentes marcas.

- Registro automático de cámaras sin necesidad de verificar las direcciones IP.
- Configuración de grabación simple, el software debe calcular automáticamente según el espacio en el disco duro a qué velocidad debe grabar según la duración de grabación establecida por el usuario.
- Interfaz gráfica de usuario (GUI) principal.
- Operación por función "arrastrar y soltar" (cambio de cámara).
- Compatibilidad con monitoreo de puntos clave/monitor dual.
- Control de giro/inclinación/zoom (PTZ) de la cámara.
- Monitoreo de audio.
- Búsqueda y reproducción rápida durante el monitoreo.
- Reproducción de lista de alarmas.
- Control de reproducción y exportación de datos a CD, DVD y Memoria Flash.
- Vistas personalizadas según necesidad del usuario.
- Menú de búsqueda exclusivo.
- Dos funciones de búsqueda, uno utilizando condiciones como fecha, hora, nombre de cámara y tipo de grabación (manual/programada/alarma/evento) y otro mediante la búsqueda de imágenes específicas en el video grabado utilizando funciones inteligentes.
- Búsqueda de resultados por línea de tiempo o por lista.
- Grabación manual.
- Grabación programada.

- Grabación de alarmas/eventos.
- Grabación programada con marcación de alarmas.
- Escalable para cumplir con requerimientos futuros.
- Acepta transmisiones múltiples desde cámaras de múltiples códecs.

En cuanto al software de gestión deberá cumplir las siguientes características:

- Soporte para 4 cámaras como mínimo.
- Compresión de video H.264, MPEG-4 y JPEG.
- Velocidad de grabación máxima 60fps.
- Disco duro de 1TB.
- Capacidad de expansión de almacenamiento mediante e-sata (máx. 4tb).
- 01 Salida de monitor análogo RGB (D-sub 15-pin).
- 01 Salida de audio.
- 04 entradas para sensores.
- 01 salida de alarma.
- 02 Interfaces Ethernet 1000BASE-T/100BASE-TX/10BASE-T.
- 01 Interfaz USB2.0 (Adelante) y 02 USB2.0 (atrás).
- Característica eléctrica DC 12V (AC adaptador: 100V a 240V AC, 50/60Hz).
- Consumo de energía aproximada 36W.
- Temperatura de funcionamiento 5 a 40°C.

- Operación con humedad 20% a 80%.
- Control remoto IR.
- Soporte multilingüe inglés, francés, italiano, alemán, español, ruso y chino simplificado.

Plataforma de Gestión de Red

Es un sistema de monitoreo de redes, el cual sirve para configurar, monitorear, administrar y detección de alarmas de todos los elementos de red de suministrados en la presente licitación y con capacidad de crecimiento de hasta 100% en el total de elementos de red. Para lo cual solo se debe agregar las licencias sin necesidad de actualizar el hardware y software, el sistema de monitoreo debe contar con las siguientes características:

- Debe ser centralizado con autodescubrimiento de la red de por lo menos 100 dispositivos, y crear un inventario de tal forma que el administrador de la red tenga un panorama general de la conformación de la red.
- Debe poder tener acceso por medio de un navegador.
- Debe contar con detección, análisis y reportes del rendimiento de los dispositivos, fallas, reglas, etc.
- Debe tener la capacidad de proveer una visión de dominios VLAN, LAN etc.
- Debe poder configurarse, crear y borrar VLAN en los equipos de red.
- Debe poder relacionar la dirección MAC e IP con el puerto del switch.
- Debe poder realizar un trace route y presentar la información en forma gráfica en un mapa.
- Debe identificar rápidamente discrepancias en el puerto permitiendo reparar el problema.

- Debe contar con detección de fallas en la red, debiendo usar las políticas definidas por el administrador, traps SNMP o poleo de los dispositivos para detectarlas.

- Debe permitir actualizar el sistema operativo de distintos dispositivos reduciendo tiempo y dinero.

- Debe poder acceder a los mapas a través de un navegador web, dibujando de diferentes colores los estados de operación de los dispositivos.

- Debe poder gestionar los dispositivos de la red inalámbrica (controlador, Access Points).

- Debe permitir cargar planos del campus donde se indique de forma gráfica la ubicación de los Access Points y la forma como irradia la señal inalámbrica.

- Debe permitir la solución de problemas y mostrar la información de la red basado en el usuario.

Sistema de Protección Eléctrica

El proyecto incluye la implementación de UPS (sistemas de alimentación ininterrumpida) en cada nodo concentrador donde se instale un equipo de comunicaciones o switch. Este es un dispositivo que gracias a sus baterías, puede proporcionar energía eléctrica tras un corte intempestivo de fluido eléctrico a todos los dispositivos que estén conectados. Otra de las funciones de los UPS es la de mejorar la calidad de la energía eléctrica que llega a las cargas, filtrando subidas y bajadas de tensión y eliminando armónicos de la red en el caso de usar corriente alterna. Este UPS debe cumplir las siguientes especificaciones:

- Garantizar la autonomía por 20 minutos de los que se instalen en los gabinetes de pared.

- Tecnología ONLINE.

- Entrada 220 a 240 V.
- Factor de cresta: 3 a 1.
- Eficiencia con carga completa: Mínimo 85%.
- Tiempo típico de recarga: 03 horas.
- Tipo rackeable.

5.2.1. Central de Monitoreo

El sistema debe contemplar accesos a cualquier stream de cada cámara, en forma rápida dentro de la red, sin que esto signifique tener licencia o estar autorizado en algún servidor, lo único que debe reportar son los datos de autenticación dentro de la red de video distribuida Incluso cuando el sistema no esté grabando, la visualización deberá ser independiente a través de un browser o navegador web.

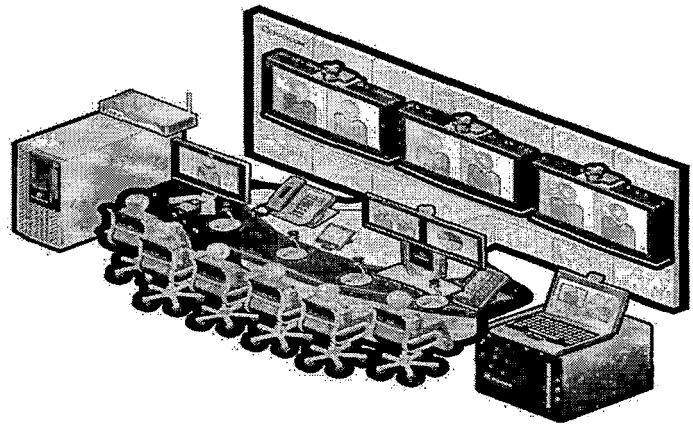
El Sistema de gestión y monitoreo de Video deberá ser una solución distribuida, diseñado para instalaciones que requieren vigilancia 24x7x365.

El sistema de administración y monitoreo debe ofrecer administración centralizada de todas las cámaras, grabadores y usuarios

Centro de atención de emergencias:

Ilustración 5.13

Central de emergencia y telefónica



Fuente: Elaboración propia

Sala de Operadores

En la sala de operadores se contará con cuatro (04) puestos de operador y un (01) puesto de supervisor. Se compondrá de una PC de sobremesa, dos monitores (uno para despacho y otro para la aplicación de cartografía), un teclado, ratón, micrófono de sobremesa, micro cascos y PPT de pedal.

Se deberán utilizar PCs estándar de primeras marcas teniendo en cuenta la continua evolución del mercado.

Como estándar para las aplicaciones de despacho y cartografía, se utilizan monitores LCD TFT de 21".

El tipo de interfaz que gestione el audio del operador permitirá mantener dos conversaciones simultáneamente.

Estación de trabajo para monitoreo

Cantidad:

03 computadores para operador.

- Procesador Quad Core, Core i7 o mejor.
- Memoria RAM de 4GB o mejor.
- Disco duro de 1 TB, de estado sólido.
- Tarjeta gráfica NVIDIA de alto procesamiento (2000 MB) o similar.
- Tarjeta de red Gigabit Ethernet.
- Tarjeta de red inalámbrica.
- Monitor LED de 21" o mejor, para cada estación de trabajo con conexión DVI o HDMI.
- Quemador DVD.
- Puertos USB.
- Windows 7 profesional.
- Teclado y mouse con interfaz USB.

03 módulos de melamine para operador (diseñado por el contratista).

01 Access Point 802.11 de hasta 300 Mbps, o mejor.

01 Switch 24 port, administrable, o mejor.

02 Impresor laser (Características ofertadas por contratista).

01 Escáner (Características ofertadas por contratista).

01 Fotocopiador tipo oficina (Características ofertadas por contratista).

TV LCD de alta definición 42 pulgadas (incluye rack)

Cantidad: 01 unidad

- Tipo de panel : LCD.
- Área visible : 42" LCD Widescreen.
- Ratio contraste dinámico : 4500 :1.
- Resolución mínima : 1,920 x 1080 o superior.
- Aspecto : 16:9.
- Tiempo de respuesta : 8 ms o menor.
- Puertos entradas : HDMI, DVI, VGA PC, RS232C.
- Salidas : HDMI, DVI, VGA PC, RS232C.
- Ángulo de visión : Mínimo 178° Horizontal y Vertical.
- Brillo : 450 cd/m2.
- Voltaje de alimentación : 220 Voltios 60 Hz o auto voltaje.

Video Wall, incluye PC controlador de video

Cantidad: 01 unidad

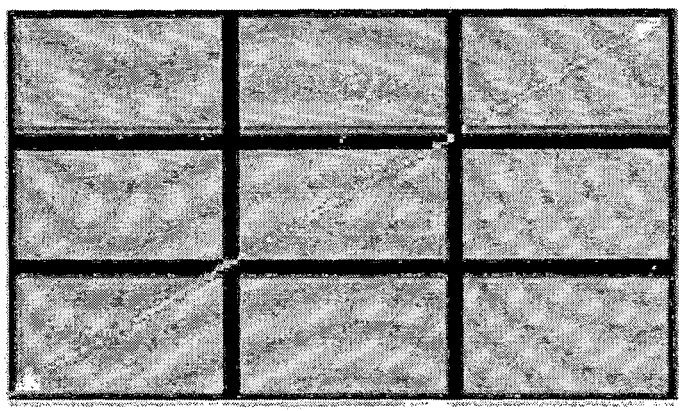
Video Wall, con matriz 3x3, 42" LCD o mejor, borde 3 cm o mejor. Incluye PC controlador de video o mejor.

- Distancia de la pantalla y la pantalla entre dos pantallas ultra-estrecho bisel de 7,3 mm, o mejor.
- Panel LCD.
- Resolución nativa 1360 x 768 WXGA en verdadera relación de aspecto 16:9, brillo máximo de 700 cd / m^2 Relación de contraste de 3000:1 y típico, o mejor.
- Software calibrador Display Wall.
- Control y comunicación Ethernet.
- Función SNMP.

- Tecnología Rapid Response.
- Diversos conectores de entrada.
- Montaje en pared.

Ilustración 5.14

Video wall 3x3



Fuente: Elaboración propia

Teclado de controlador de movimiento (Joystick)

Cantidad: 05 unidades

- 38 teclas de goma retro iluminados.
- Zumbador.
- suministra con manual de instrucciones, el conductor de la instalación, las hojas pre-cortadas, la capa de plástico que protege.
- alimentado a través del puerto USB.
- Consumo: 350 MA máx.
- Comunicación USB 2,0.
- dedicada puerto COM virtual protocolo.
- Joystick HID de 4 ejes 32 emulación clave.
- medio ambiente.
- Uso interior.

- temperatura de funcionamiento: 0 ° C / +45 ° C (+32 ° F / +113 ° F).
- Certificaciones: EN55022 Clase B, EN50130-4, EN61000-6-3, EN60950-1, FCC parte 15 Clase B.
- OPACDCZ: Hojas sueltas para la impresión de los formularios personalizados y láminas de plástico transparente de protección.

Aire Acondicionado

Cantidad: 01 unidad

- Tipo paquete enfriado por aire, especial para renovación 100% aire exterior.
- Capacidad total de 90,000 BTU/Hr.
- Gabinete fabricado en acero galvanizado, pintado con base anticorrosiva y acabada con pintura al horno.
- Características eléctricas: 220v - trifásico – 60HZ.
- Unidad condensadora integrada.
- Gabinete fabricado de plancha de acero galvanizado con protección anticorrosivo y acabado con pintura al horno.
- Serpentín de condensación compuesto de tubos de cobre sin costura, con aletas de aluminio mecánicamente aseguradas en el interior.
- Reóstato de protección para alta y baja presión.
- Circuito de refrigeración con válvulas de servicio en las líneas de alta y baja presión, para: cargar, evacuar y medir presión de refrigerante, para cualquier servicio de mantenimiento o reparación.
- Ventiladores de tipo axial con acople directo al motor.
- Motor-compresor hermético, con refrigerante r-22 o ecológico. Circuito de refrigeración con filtro secador.
- Panel eléctrico con lo siguiente :
    - Contactor eléctrico trifásico para el compresor.
    - Relé de fuerza para el moto ventilador.
    - Temporizador anti-short cycling regulable, para el moto compresor.

- Protección regulable de mínima y máxima tensión y protección de inversión de fases de la moto compresora.

5.2.2 Red de transmisión de datos

5.2.2.1 Fibra Óptica

La fibra óptica es el núcleo de las redes de comunicaciones en la actualidad. Es el tipo de medio predominante para los enlaces en los centros de datos de importancia crítica, redes troncales dentro de los edificios y distancias más largas en redes de campus, teniendo en cuenta la conexión entre los diversos locales de la universidad. A medida que las velocidades de las redes y la demanda de ancho de banda aumentan, las limitaciones de la distancia y de pérdida han disminuido, de forma que la comprobación de fibra óptica es más importante que nunca.

Por ello, se cableará una red troncal o backbone, desde el gabinete central ubicado en el Data Center, hasta cada uno de los nodos secundarios, ubicado en los distintos postes donde se encuentran los videos cámaras IP Domo PTZ.

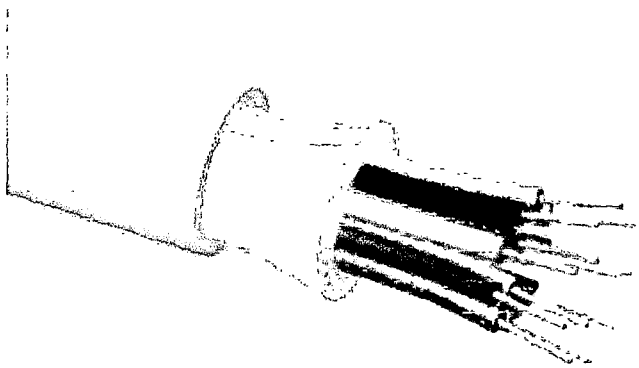
Cable de fibra óptica multimodo

El backbone deberá ser implementado con cable de fibra óptica LOMMF OM3 de 50 micrones multimodo, para exteriores, tipo LSZH de 6 hilos con conectores LC. El cable de fibra óptica que se proponga, deberá ser con chaqueta LSZH y cumplir mínimo con los estándares internacionales IEC 60332-3 (no propagación de Incendio), IEC 61034 parte 2 (baja emisión de humos opacos) e IEC 60754 parte 2 (libre de halógenos y baja emisión de gases corrosivos), (de acuerdo al cumplimiento de la adenda al nuevo código nacional eléctrico) según la RM N° 175-2008 MEM-DM.

Esta solución deberá incluir la fibra óptica, conectores LC, acopladores LC, bandejas metálicas de 1UR en cada extremo de los tendidos, y patch cords LC-LC. Todos estos componentes deberán ser de una misma marca.

Ilustración 5.15

Fibra Óptica OM3 – Blindado



Fuente: Foto proporcionada por internet

La bandeja de fibra debe ser inteligente y debe tener la capacidad de integrarse a una herramienta en software que permita una gestión gráfica de la infraestructura física de red instalada.

A su vez, la fibra óptica ofertada deberá cumplir con el estándar TIA-492AAAC-A (IEC-60793-2-10ed2) para fibras de 50 micrones multimodo índice gradual. Se deberá incluir certificado UL o ETL que lo acredite.

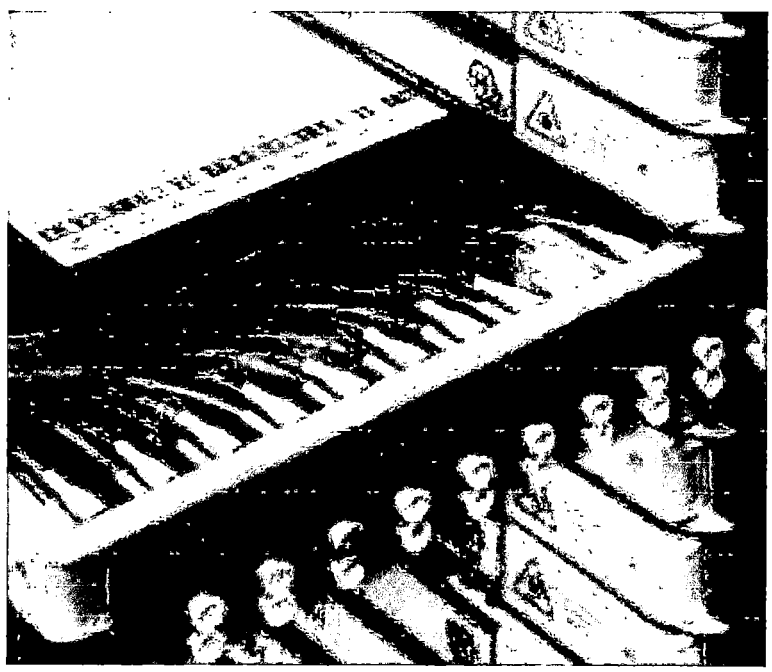
Bandeja Inteligente de Fibra Óptica de 1RU

Es el dispositivo que se encuentra en los gabinetes de comunicaciones y se conecta directamente con el cable de fibra óptica del cableado vertical o troncal. Sirve para realizar las conexiones entre los switches principales de cada poste donde se ubica el video cámara IP Domo PTZ. Debe cumplir las siguientes características:

- Debe poseer anchura de 19" y altura de 1U; identificación del fabricante en el cuerpo del producto.
- Permitirá colocar 4 módulos, cada uno con 12 puertos LC (6 LC dúplex) en el frente.
- La bandeja deberá incluir una tapa acrílica superior para proteger el cableado dentro de la misma.
- La bandeja deberá ser deslizante.
- La bandeja inteligente deberá contar en cada puerto dúplex de la bandeja un sensor, un botón y una luz LED indicadora.
- La bandeja deberá tener entradas de cables posteriores y laterales, y cada entrada contar con una tapa en caso de no ser utilizada o un sistema "boquilla prensa-cable" para la correcta sujeción de los mismos.
- Las bandejas en el centro de cómputos deberán tener una identificación sobre cada módulo que permita identificar hacia qué rack de qué piso de qué edificio corresponden.

Ilustración 5.16

Bandeja Deslizante de Fibra Óptica



Fuente: Foto proporcionada por internet

5.2.2.2 Instalación de fibra óptica

Gabinete Outdoor Nema 4X para poste

Cantidad: 30 unidades

- Gabinetes metálicos 50x60x20cm aprox. para montaje en exteriores.
- Herméticos anti – impacto y anti – ganzúa.
- Doble paleta.
- Sellado contra agua y resistente a la corrosión.
- Debe contar con abrazaderas y ferrería galvanizada para montaje en poste.
- Con certificación NEMA 4x, IP 66 o Superior.

Gabinete de comunicación 8ru (24 RU proyección ups)

Cantidad: 04 unidades

- Puerta frontal desmontable, con centro de acrílico.
- 2 rieles de montaje ajustable.
- Marco de montaje trasero con 6 ranuras, especiales para entrada de cables (3 en la parte superior y 3 en la parte inferior).
- Las rejillas de ventilación en el panel superior listas para la instalación del Kit de ventiladores.
- Puerta frontal y marco trasero, ambos con chapas y llaves.
- Proyección a 24 RU.
- Kit de tornillos.

UPS 2 KVA/220 AC, monofásico, para video cámara en poste

Cantidad: 30 unidades

- Voltaje Nominal de Entrada 230 VAC. Voltaje Nominal de salida soportado 230 VAC.

- Potencia de salida 2000W.
- Frecuencia 50 - 60 Hz nominal.
- Eficiencia al menos del 95%.
- Forma de onda sinusoidal.
- Tipos de Tomacorrientes C-13.
- Corriente Max. De entrada 7 A.
- Ambiente operativo 0 - 40 °C.
- Humedad relativa de operación 10 - 90%.

Kit de montaje eléctrico para radio y video cámara en poste

Cantidad: 30 unidades

Mástil para cámara

- Herméticos anti – impacto y anti – ganzúa.
- Tubo galvanizado de 1.5" x 2.5 mm de espesor.
- Tres (3) abrazaderas para poste.
- Pintado con base anticorrosivo y acabado de esmalte sintético color blanco.

Postes de cemento x 13 metros

Cantidad: 30 unidades

Postes de concreto armado del tipo 13/300/150/300.

- Longitud: 13 m.
- Carga de trabajo 300 (esfuerzo en punta).
- Diámetro en punta 150 mm.
- Diámetro de base 300 mm.
- Cada poste debe incluir la instalación, fijación, anclaje de la misma. Incluir cables y demás accesorios.

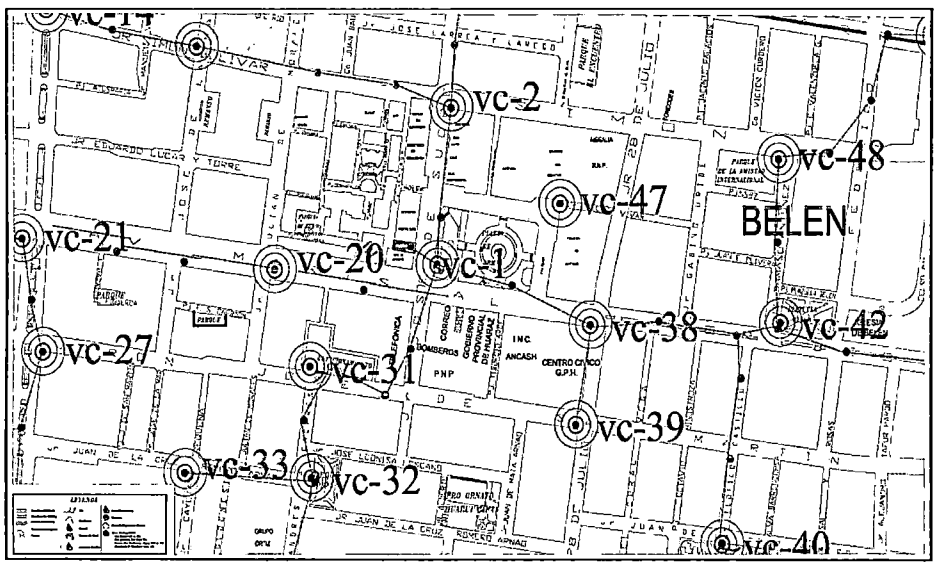
Conexión eléctrica BT5B

Se adquirirá de la compañía proveedora de los servicios de distribución de energía eléctrica (Hidrandina). Esta gestión lo realiza la Municipalidad Provincial de Huaraz.

Inicio Red dorsal fibra óptica

Ilustración 5.17

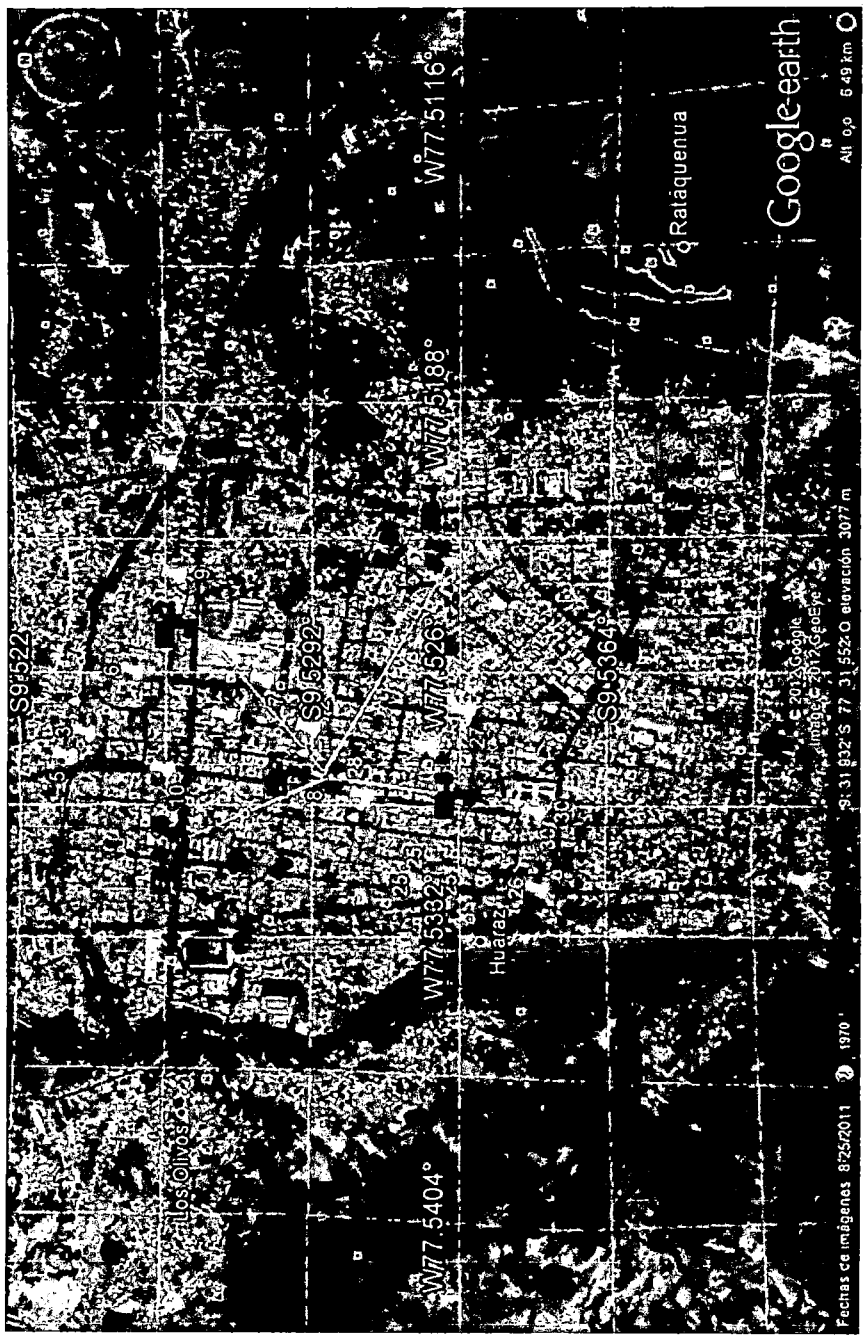
Red dorsal de fibra óptica del distrito de Huaraz



Fuente: Elaboración propia

Ilustración 5.18

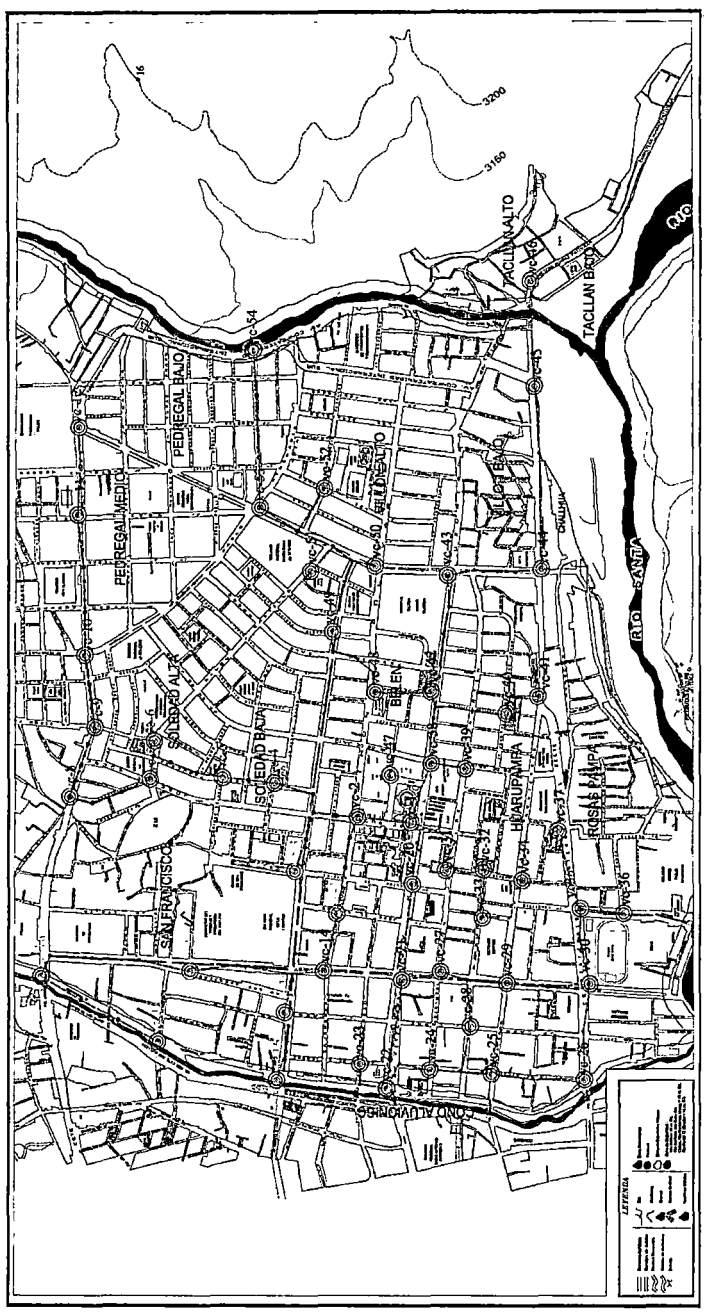
Ubicación de video cámaras en el distrito de Huaraz



Fuente: Elaboración propia

Ilustración 5.19

Mapa general de la red dorsal de fibra óptica del distrito de Huaraz



Fuente: Elaboración propia

5.2.2.3 Sistema de pararrayos

La función específica de los pararrayos es la de acumular y producir una ionización que es dirigida hacia la nube, proporcionando un camino de baja impedancia de la descarga atmosférica. Este tipo de punta cuenta con dos aditamentos, el primero es un elemento llamado electrodos o puntas superiores destinados a recuperar la energía ambiental, ya que se encuentran situadas en el carrusel que se encuentra aislado de la punta que está conectada a tierra y el carrusel se encuentra en el mismo potencial que el aire generando una diferencia de potencial entre ambos elementos resultando en el intercambio de protones un trazador ascendente para la captura de un trazador descendente (rayo), para capturarlo y drenarlo

El proyecto contempla la instalación de puesta a tierra para la descarga de cada sistema de pararrayos. Su ohmiaje debe de ser igual o menor a 10 Ohms.

Características

NORMAS: NFC17-102.

- Captor Ionizante No Radioactivo.
- Pararrayos Tetrapuntal tipo Franklin.
- Radio de Protección radio mínimo 50mts a 15 m de altura.
- Mástil de fijación estándar de Fe 1".
- Abrazaderas aislantes.
- Soporte separador Universal.
- Pernos de ½" x 2".
- Mástil galvanizado en caliente.
- Varilla de cobre Cooper Well.
- Cable de Cobre desnudo de 25 milímetros.

- Brazos Aisladores cerámicos.
- Dosis Química tipo Thorgel.
- Conector de cobre tipo Anderson.
- Material de relleno: tierra de cultivo (tierra negra de alta conductividad).
- Cavado de Pozo y Varilla Aisladora de Pararrayos a la Torre.

5.2.2.5 Sistema de puesta a tierra

En toda instalación eléctrica se pueden producir fallas que pongan en peligro la integridad física de las personas así como dañar los equipos eléctricos y electrónicos, para evitar estos problemas, se han desarrollado sistema de puesta a tierra, consistentes en una serie de conductores y electrodos que conducen la falla eléctrica hacia el suelo, basándose en el principio de que la corriente eléctrica fluye al punto de menor resistencia. En la actualidad los sistemas de puesta a tierra tienen que garantizar que las inducciones de corriente eléctrica (provenientes de rayos, interferencias de radiofrecuencia y electromagnéticas), que se inducen por las estructuras metálicas de las instalaciones, tuberías de agua y tierras físicas convencionales (varillas, mallas, electrodos químicos) etc., no dañen los equipos eléctricos y electrónicos.

Pozo a tierra de cemento conductivo libre de mantenimiento con sus accesorios de instalación, caja de registro que permita verificar la lectura, grapa de conexión entre disipador y cable de cobre desnudo. Se deberá asegurar un ohmiaje menor o igual a 05 ohmios.

Todos los sistemas incluyen lo siguiente:

- Varilla de cobre Cooper Well.
- Dosis Química tipo Thorgel.
- Conector de cobre tipo Anderson.

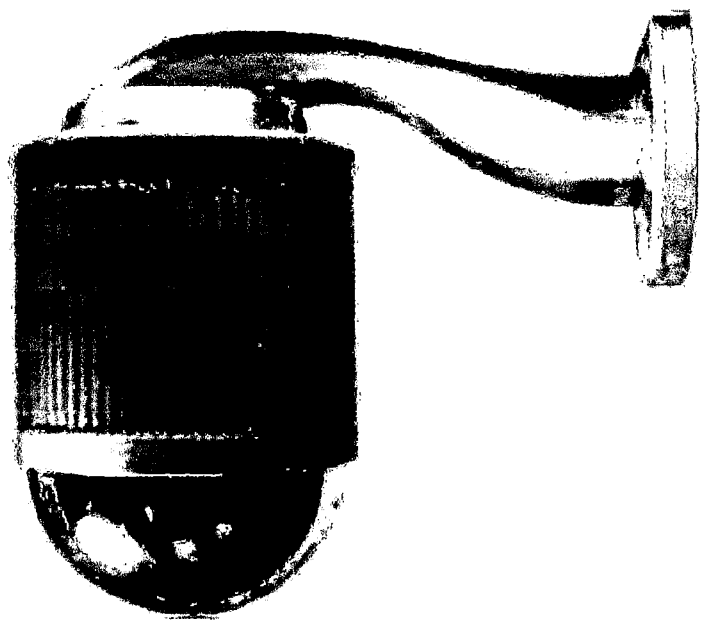
- Material de relleno: tierra de cultivo (tierra negra de alta conductividad).
- Cavado de Pozo y Varilla Aisladora de Pararrayos a la Torre.

5.2.3 Estación remota

Cámara Domo Alta Velocidad Exterior 22x

Ilustración 5.20

Cámara domo alta velocidad

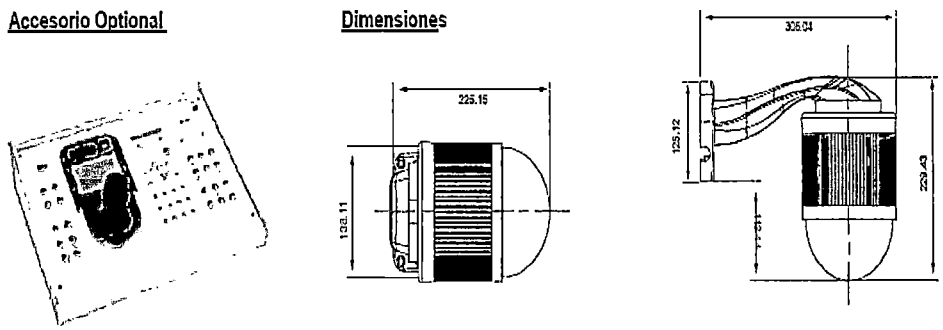


Fuente: Foto proporcionada por internet

Domo exterior de alta velocidad viene equipado con un PAN de 360° y un TILT de 90°, lente zoom de 22X ópticos y con auto focus. Además de tener otras funciones incluyendo AUTO TRACKING INTELIGENTE, ALTA CONFIABILIDAD, Menú gráfico en Pantalla amigable OSD y Control por teclado. Con todas estas potentes características, satisface la mayor parte de aplicaciones de seguridad y vigilancia del mercado.

Ilustración 5.21

Características y accesorio de la cámara domo alta definición



Fuente: Foto proporcionada por internet

Características

- Mecanismo Pan/Tilt de Alta Velocidad y Lente Zoom Auto-Focus
- Brinda 360◦de paneo horizontal, 90◦ (tilt) movimiento vertical y lente zoom óptico de 22X.
- Función Auto Tracking (auto rastreo) para Seguimiento de Intrusos.
- Movimiento pan/tilt y cálculo de coeficiente de zoom muy precisos, este domo hace movimiento horizontal - vertical y zoom muy veloces, para rastreo continuo de intrusos.
- La cámara irá al objetivo automáticamente y seguirá el movimiento del objeto de mayor movimiento en su campo de visión, con enfoque de pan, tilt y zoom a fin de mantener el objetivo en su centro de visión: (1) Predefine el área de vigilancia de las cámaras / (2) pre-define el tiempo de RASTREO. Cuando el objetivo marcado esté fuera del área de vigilancia pre-definida o se mueva menos tiempo del pre-definido en el tiempo de rastreo, la cámara retornará a su punto original de visión. Una excelente función para brindar grabación de evidencias.
- Fiabilidad de uso comprobado.

- La duración patentada de la velocidad de la cámara ha sido comprobada pasando sus componentes por rígidas pruebas de más de 2, 000,000 revoluciones.
- Visualización Gráfica en Pantalla OSD.
- Fácil Operación a través del Teclado Controlador.
- El teclado controlador opcional brinda un joystick muy conveniente de 3D y pantalla touch screen diseñada para una fácil operación.
- Soporta Función Hot Point PTZ.
- Soporta 8 grupos pre-definidos y hasta 256 pre-sets programables.
- Avanzada Función de Balance Blanco AWB.
- De acuerdo a los diferentes colores de temperatura y el lugar de instalación, fije la función de Balance de blancos en un modo diferente.
- Muestra el Título de las Cámaras en su pantalla.
- Muestra e identifica el nombre de cada cámara en el monitor, de hasta 10 caracteres y/o símbolos.

5.3 Diseño del sistema

Televigilancia

Meta

Optimizar la capacidad de monitoreo en áreas públicas determinadas, racionalizando la intervención de los recursos humanos.

Descripción

El sistema deberá estar constituido por una infraestructura tecnológica colocada estratégicamente en el medio urbano con posibilidad de renviar las comunicaciones de video hacia una estación de comando y control.

El sistema de televigilancia será implementado con cámaras tipo DOMO, interconexión mediante fibra óptica, estaciones de monitoreo, centro de grabación,

central telefónica, y respaldo de UPS, en el Centro de Control del Sistema de Telecomunicaciones (CCST).

El sistema de televigilancia está compuesto por:

- Anillo de fibra óptica.
- Centro de datos (Data Center).

Consiste en implementar una red de video vigilancia conformado por treinta (30) cámaras IP tipo DOMO PTZ, estas cámaras deberán ser implementadas en los denominados puntos críticos de la jurisdicción, lugares donde se han detectado mayor incidencia delictiva.

Descripción del sistema

El sistema de video vigilancia debe estar soportado por un canal de comunicaciones de banda ancha de video cámara hacia su enlace receptor.

A través de esa plataforma de comunicación se llega al sistema de video inteligente NVR (Network Video Recorder) para la grabación digital y gestión de la señal de vídeo mediante software analítico, control PTZ y manejo de alarmas de cada una de las cámaras, lo que hará posible que las imágenes sean controladas y visualizadas en tiempo real en el CCST.

El sistema deberá permitir la inclusión de las cámaras en forma de íconos en un mapa de la ciudad, con lo cual se posibilitará la ubicación de la zona del incidente, facilitando así el envío del personal y generando una base de datos que brinde estadísticas de las ocurrencias suscitadas.

El sistema, deberá operar a una velocidad efectiva de mínimo 4000 Mbps, con una tasa de efectividad no menos a 99,99999.

Se considera para los nodos de concentración el uso de switch que soporten administración de stream video y para el nodo principal un switch multicapa 10/100/1000 que gestione igual stream video y este último se utilizará para la

conexión de equipos de video vigilancia y backbone y en los nodos de concentración secundarios para conexión al backbone y cámaras IP.

La ubicación de estos puntos se logró gracias a la información brindada por las comisarías de la PNP y del servicio de serenazgo de la jurisdicción de la provincia del Huaraz.

Componentes:

Cámaras Ip Domo Ptz

- Cámaras color IP DOMO PTZ, Zoom 36X Óptico y 12X Digital, incluye instalación.

Sistema de video inteligente - NVR

- Servidores de grabación.
- Software de video analítico.

Interconexión

- Anillo de fibra óptica.

Software

- Software de Gestión (Administración y grabación).
- Software de exportación de Videos.

Centro de monitoreo y grabación

- Solución de almacenamiento de video 12 TB o superior.
- Estación de trabajo para monitoreo.
- TV LCD de alta definición 50 pulgadas (incluye rack).

- Video Wall incluye PC Controlador de video.
- Teclado/joystick de control de cámaras.
- Switch 48 puertos capa 3.
- Gabinete 42 RU para sala de enlace principal.
- UPS 3 KVA/220 AC, monofásico, para cada nodo de concentración, incluye instalación.

Accesorios de instalación

- Gabinete Out door Nema 4X para poste.
- Gabinete de comunicación 8ru (24 RU proyección ups).
- UPS 2 KVA/220 AC, monofásico, para cámara en poste, incluye instalación.
- Kit de montaje eléctrico para radio y cámara en poste.
- Torre de telecomunicaciones x 30 metros, pintado en rojo y blanco, incluye instalación.
- Postes de cemento x 5 metros.
- Postes de cemento x 13 metros.

Tabla 5.2

Ubicación de video cámaras

CAMARA N°	Av - Jr - Ca - Mlc	UBICACIÓN	Av - Jr - Ca - Mlc	UBICACIÓN
1	Plz.	PLAZA DE ARMAS		
2	Jr.	BOLIVAR	Jr.	SUCRE
3	Av.	LUZURIAGA	Av.	28 DE JULIO
4	Jr.	BOLIVAR	Jr.	LA MAR
5	Av.	CONFRT. INTER. ESTE	Mlc.	MALECON SUR
6	Av.	GAMARRA	Jr.	CARAZ
7	Av.	GAMARRA	Alm.	GRAU
8	Av.	RAIMONDI	Av.	AMERICAS
9	Jr.	CARAZ	Jr.	HUALCAN
10	Jr.	COMERCIO	Jr.	13 DE DICIEMBRE
11	Av.	CONFRT. INTER. OESTE	Jr.	13 DE DICIEMBRE
12	Av.	CONFRT. INTER. OESTE	Jr.	BOLOGNESI
13	Av.	CONFRT. INTER. OESTE	Av.	RAIMONDI
14	Av.	FITZCARRALD	Mlc.	MALECON SUR
15	Jr.	JUAN DL CRUZ ROMERO	Call.	REQUENA
16	Av.	RAIMONDI	A	SAN MARTIN
17	Av.	RAIMONDI	Av.	FITZCARRALD
18	Av.	RAIMONDI	Av.	TARAPACA (27 NOV.)
19	Av.	TARAPACA (27 NOV.)	Jr.	MARISCAL CACERES
20	Av.	CONFRT. INTER. ESTE	Psj.	AGUSTIN LOLI
21	Av.	CONFRT. INTER. ESTE	Av.	VILLON
22	Pzla	LA SOLEDAD	Jr.	RAMON CASTILLA
23	Jr.	SUCRE	Jr.	RAMON CASTILLA
24	Av.	VILLON	Av.	ATUSPARIA
25	Jr.	BOLIVAR	Prq.	AMISTAD INTERNAC.
26	Av.	CONFRT. INTER. OESTE	Av.	TARAPACA (27 NOV.)
27	Av.	CONFRT. INTER. OESTE	Av.	VILLON
28	Av.	GAMARRA	Jr.	FEDERICO SAL Y ROSAS
29	Av.	LUZURIAGA	Av.	VILLON
30	Av.	TARAPACA (27 NOV.)	Pte.	TACLLAN

Fuente: Elaboración propia

Ilustración 5.22

Ubicación de video cámaras

Fuente: Elaboración propia

Central de emergencia

Meta

Optimizar la capacidad de respuesta a las emergencias que se puedan presentar, racionalizando la intervención de los recursos humanos. Para ello será necesario contratar una Línea troncal telefónica, a un proveedor de servicios de Telefonía, que de acuerdo a LEY esta será gratuita para el usuario llamante. Esta Línea se configurará de manera digital y se usara conectividad inalámbrica.

Generalidades

Estará compuesto por la infraestructura tecnológica que le permita a la ciudadanía a través de un número telefónico abreviado y/o de fácil recordación, con la finalidad de solicitar una atención ante una emergencia o un hecho que atente o ponga en peligro su integridad física o moral.

Con la finalidad de dar rápida y oportuna solución a la demanda de la población ante un hecho en contra de la seguridad ciudadana, se deberá estar tecnológicamente equipada y preparada con Mapa Geo referencial de la ciudad de Huaraz, que le permitirá ubicar rápida y efectivamente las emergencias que se desarrollan y poder decidir el tipo de acción a tomar.

Sistema de Ubicación mediante el sistema de localización (GPS) que estará integrado al sistema de comunicación radial. Sistema de comunicaciones que permitirá desplegar fácil y rápidamente a las fuerzas que permitan dar solución a la problemática planteada. Además, el sistema podrá realizar integración de diferentes tecnologías, lo que permitirá una gestión más rápida y eficaz de las incidencias.

Sistema informático que apoye el registro, seguimiento y gestión de incidencias.

El registro de incidencias permite el ingreso de incidentes desde de múltiples canales de comunicación (Central Telefónica, partes diarios, correo electrónico, etc.), clasificación y geo referenciación.

El seguimiento de incidentes permite complementar la información registrada incorporando detalles del incidente como personal operativo que intervino, registro de denunciantes, denunciados, testigos, etc. Registro de bienes en el incidente. Escucha de audio asociado al incidente, el cierre y baja del incidente.

La gestión de incidencias permite a la entidad obtener información geo referenciada del incidente, clasificación de sectores de acuerdo al nivel de incidencias (alto, medio, bajo), reportes estadísticos y listados de incidentes.

El sistema debe estar constituido por una infraestructura tecnológica diseñada para cumplir con los requerimientos de atención de llamadas de emergencias así como también brindar los medios de comunicación adecuados a fin de poder ejecutar las órdenes de desplazamientos de las unidades encargadas de dar atención a las emergencias.

La Central de Atención de llamadas de orientación, consulta, apoyo y emergencia, está compuesto por la integración de sistemas independientes para formar un solo centro de atención con herramientas que ayudan a mantener los niveles de operatividad; mediante los siguientes procesos:

1. Despacho y Gestión.
2. Información Geográfica.
3. Video Vigilancia.
4. Comunicación Radial.

Esta central de llamadas con cuatro (4) operadores/despachadores, será equipada con:

- Servidor para gestión administrativa de emergencias, sistema operativo, base de datos, software para gestión de las emergencias, Central Telefónica IP con 16terminales.
- PRI (Interfaz de Acceso Primario) para uso de telefonía local.

- 16 puertos telefónicos digitales.
- 4 módulos de madera para operadores.
- 4 computadores para operadores.
- 1 módulo de madera para supervisor.
- 1 computador portátil (Laptop) para supervisor del sistema.
- Router y otros accesorios de seguridad eléctrica.

Descripción del sistema

El Sistema contará con un centro de atención de emergencias, de cuatro puestos de operador y un puesto de supervisor, con la siguiente topología:

- Un Servidor de comunicación
    - El número de interface.
    - 1 línea telefónica analógica.
    - 1 módulo GSM.
    - 1 equipos de radio base.

El sistema deberá ofrecer disponibilidad del 99.99999 % por año.

La adquisición de servicio telefónico al proveedor de Telecomunicaciones de la localidad, estará a cargo del usuario final.

El sistema operativo debe ser robusto, de alta disponibilidad.

La Central Telefónica IP deberá soportar la conectividad con proveedores de servicios públicos y/o privados:

- Troncales analógicas.
- Troncales Digitales PRI (Interfaz de Acceso Primario) y BRI (Interfaz de Acceso Básico).
- Troncales IP.

La central telefónica deberá ser de arquitectura abierta SIP (Protocolo de Inicio de Sesión), SOA (Arquitectura Orientado a Servicios) y servicios en Web. Debe soportar Teléfonos IP de la misma marca, así como también teléfonos IP de otros fabricantes siempre que sea de tipo SIP. Esto asegurará un crecimiento en anexos con las mejores prestaciones que exista en el mercado. Debe permitir también la inclusión de aplicaciones de terceros (SOA).

Componentes

Equipamiento y cableado, del centro de control del sistema de telecomunicaciones - CCST

- Implementación del Data Center. (Infraestructura, dispositivos, componentes, accesorios, aire acondicionado, gabinetes, switches, etc).
- Cableado eléctrico para estaciones y equipamiento.
- Servidor para Usuarios de Red Administrativa.
- Implementación de Red LAN (cableado Cat 6, para voz y datos).
- Implementación y funcionamiento de Telefonía IP, con 16 terminales.

Complementos de red

Meta

Optimizar la capacidad operativa y logística mediante el uso de una infraestructura adecuada al desarrollo de la función de seguridad ciudadana y como centro de operaciones ante emergencias del Gobierno Provincial de Huaraz.

Componentes

Dispositivos, equipos y accesorios, complementarios

- Sistema de puesta a tierra para telecomunicaciones.
- Sistema de puesta a tierra para sistema eléctrico.
- Fuente de energía ininterruptible UPS de 20 KW/220 AC, trifásico, incluye instalación.
- Grupo electrógeno 10 KVA.
- Tablero de transferencia automático.

5.4 Diseño de la interfaz de la solución

5.4.1 Plataforma de gestión

Software licenciado de gestión centralizada. Visualización de parámetros IPSLA.

Software de Gestión (Administración y grabación).

Cantidad: 01 unidad.

Software de grabación y monitoreo

- Con arquitectura distribuida **cliente servidor** que permite que los cambios en la configuración del sistema realizados por un administrador sean automáticamente compartidos por todos los operadores. De este modo se elimina cualquier posible punto de fallo único y se ofrece un sistema de gestión de la seguridad con gran capacidad de ampliación que puede abarcar varias sedes al mismo tiempo.

- Rondas de vigilancia y secuencias para admitir todas las características tradicionales de los CCTV, incluida las rondas de vigilancia y las secuencias, así como combinaciones de ellos. El vídeo puede visualizarse en paneles de vídeo en las pantallas del PC.

- En el software se podrá insertar mapas interactivos de un lugar para ayudarles a localizar y gestionar las cámaras y alarmas. Utilizando dos monitores de PC, es posible ver el mapa completo en una pantalla y los paneles de vídeo en la otra.

- Soporte de hasta 03 pantallas como mínimo, cada una con 16 cámaras de video como mínimo.

Software de exportación de Videos

Cantidad: 01 unidad

- La mejor opción para el proceso de exportación de vídeo en la etapa final del proceso de edición.

CAPÍTULO VI: CONSTRUCCIÓN DE LA SOLUCIÓN

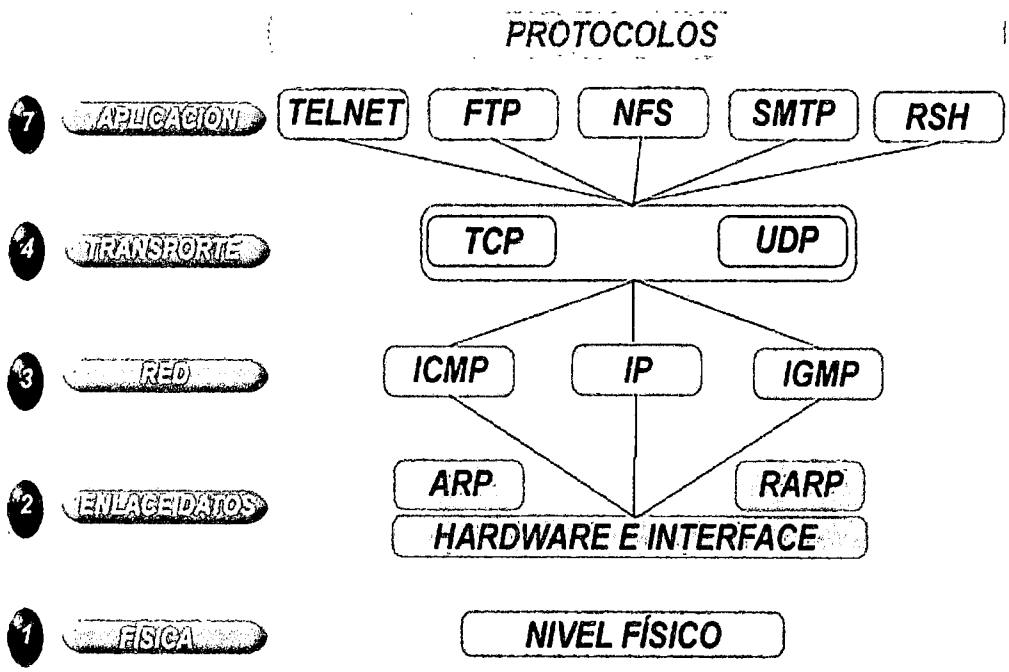
6.1 Construcción

6.1.1. Modelado

Para el diseño del sistema de televigilancia se utilizó el Modelo de referencia TCP/IP, representada en la ilustración siguiente:

Ilustración 6.1

Modelo TCP/IP, estructura de protocolos



Fuente: Foto proporcionada por internet

Este modelo permite construir metodológicamente el sistema de televigilancia utilizando fibra óptica, siguiendo los siguientes procesos:

En la capa física se realizara el tendido de la fibra óptica, instalación de las videocámaras, instalación del data center, e instalaciones eléctricas.

En la capa enlace de datos, se define la tecnología de Bus para la el tendido de la fibra óptica y la tecnología Fast Ethernet para las instalaciones del Data Center.

En la capa de red se define el uso del protocolo de internet IP, para la configuración del sistema de televigilancia.

En la capa de transporte se define el protocolo control de transporte TCP, para la configuración del sistema de televigilancia.

En la capa de aplicación se define el uso del sistema NVR para el control de cámaras a distancia.

6.1.2. Especificación de construcción

6.1.2.1. Especificaciones del sistema de televigilancia

CAMARAS Y ACCESORIOS

- Cobertura de exteriores.
- Cámara domo PTZ Q6035-E, exterior HDTV 1080p, día/noche, H.264, zoom óptico 20x, incluye Hi PoE Midspan.
- Brazo para poste, incluye cinta de acero, requiere herramienta de instalación 21776.
- Midspan T8124 exterior High PoE 60W. 802.3. at y PoE 802.3af.

ENLACES DE FIBRA OPTICA 10G Y 01G

- Cableado de FO 10G Desde Nodo Central a Cámaras de videovigilancia / Nodos.

- Cable FO Multimodo ADSS 24 Fibras - G.652D - 1-Chaqueta c/kevlar 6 kN.
- Bandeja FO Rackeable 1-RU 3 Paneles (No incluye paneles) Deslizable 6/72 Puertos.
- Bandeja para empalme FO (Incluye Prensa Estopa y Clips Guías para reserva de FO).
- Panel FO con 6 Acopladores SC Duplex Multimodo Azul (Para Bandeja S13).
- Pigtail FO SC Multimodo Simplex 0.9 mm 2 mt. Blanco Facil Pelado
- Panel FO Ciego (Para Bandeja S13).
- Manga Termo contraíble para Empalmes de Fibra Óptica 60 mm.
- Patch Cord FO LC/SC Multimodo Duplex 1 Mt.
- Cierre de Empalme Óptico 72 Fusiones.
- Organizador de 12 Empalmes de Fusión para DOME 02-03-04.
- Caja de Pared Int/Ext IP65, soporta 06 acopladores SC Duplex/LC Quad.
- Acoplador FO SC Duplex Multimodo Azul.

CABLEADO ESTRUCTURADO Y NETWORKING

- Networking en SALA DE MONITOREO.
- Catalyst 3750X 24 Port GE SFP IP Services.
- SMARTNET 8X5XNBD Catalyst 3750X 24 Port GE SFP IP Service.
- 1000BASE-LX/LH SFP transceiver module, MMF/SMF, 1310nm, DOM.
- Catalyst 3750X 48 Port Full PoE IP Services.
- SMARTNET 8X5XNBD Catalyst 3750X 48 Port Full PoE IP Servi.
- Cisco 50CM Stacking Cable.
- Catalyst 3K-X 715W AC Power Supply.

- Catalyst 3K-X 1100W AC Power Supply.
- Networking en POSTES.
- 1000BASE-LX/LH SFP transceiver module, MMF/SMF, 1310nm, DOM.
- Cisco IE 3000 Switch, 8 10/100 + 2 T/SFP.
- SMARTNET 8X5XNBD Cisco IE3000 Switch, 8 10/100 + 2 T/SFP.
- Spare, IE 3000 Right Panel.
- Spare Din Rail Clip Pack, IE 3000.
- IE 3000 Power transformer.
- UPS DE 2 KVA.
- Cableado de datos y protección eléctrica en SALA DE MONITOREO.
- Cable F/UTP Sólido 4P Cat 6A 23AWG LSZH, IEC 60332-1 Violeta (Rx305mt).
- Jack RJ-45 Cat6A Apantallado Z-MAX Plano/Angular Negro.
- Patch Panel 24 Puertos Modular TERA Z-MAX Negro.
- Ordenador de Cables Horizontal Frontal 2-RU (85mm x 80mm).
- Jack RJ-45 Cat6A Apantallado Z-MAX Plano/Angular Blanco.
- UPS SmartOnline 20 KVA Monofásico - Monofásico Rack/Tower 200/208/220/230/240V (seleccionable).
- SNMPWEBCARD Tarjeta Interna de Comunicaciones SNMP/Web.
- AIRE ACONDICIONADO.
- Gabinete de Piso 45-RU 2,190 x 710 x 990mm Negro (Puerta Frontal Curva y Posterior Doble, ambas con Malla).
- Unidad de Ventilación Incluye 4 Ventiladores.
- Bandeja 1-RU 19"x 660mm Regulable para GF-2392 o GF-2398 130Kgs. Negra.
- Bandeja 2-RU 19"x 15" Simple 19 Kgs. Negra.

- PDU Monofásico Monitoreable, 20A 200-240V, Instalación Horizontal 1U en Rack, 8 Tomacorrientes C13, Alimentación C20 con adaptador L6-20P.
- Placa de pared 1 Puerto MAX Blanca.
- Caja de Montaje Universal Simple Blanco.
- Patch Cord F/UTP RJ-45, 4 Pares, Cat.6A, LSOH Z-MAX 0.90m. Rojo.
- Patch Cord F/UTP RJ-45, 4 Pares, Cat.6A, LSOH Z-MAX 3.0m. Blanco.
- Cableado de datos y protección eléctrica en POSTE.
- Patch Cord F/UTP RJ-45, 4 Pares, Cat.6A, LSOH Z-MAX 3.0m. Blanco.

SERVIDOR DE GRABACIÓN, TERMINALES DE MONITOREO Y SOFTWARE NVR

- PowerEdge R520 Intel Xeon E5-2407 2.20GHz, 10M Cache, 6.4GT/s QPI, No Turbo, 4C, 80W.
- Consola 1U para montar en rack con LCD de 17".
- PC_MONITOREO i7 20" Full HD.
- LED SAMSUNG de 55" Full HD.
- Licencia INTELLECT Server administra hasta 64 cámaras por Servidor.
- Licencia de full administración remota para INTELLECT server.
- Licencia cliente para INTELLECT Server.
- Licencia por cámara para INTELLECT ENTERPRISE Server.
- Licencia APLR FREEFLOW Server para INTELLECT ENTERPRISE; reconoce placas a 250 Km/h.

INSTALACIÓN DE POSTES

- Servicios de implementación y adecuación eléctrica.
- Postes videocámaras 13 metros – instalados.
- Postes tendido cable FO de 9 metros – instalados.

CENTRO DE MONITOREO Y GRABACION

- Estaciones de trabajo para monitoreo doble monitor.
- TV LCD de alta definición 40 pulgadas (incluye rack).
- Video Wall incluye PC Controlador de video.
- Teclado/joystick de control de cámaras.
- Switch 48 puertos capa 3.
- Gabinete 42 RU para sala de enlace principal.
- UPS 2000 VAC para cada nodo de concentración.

ACCESORIOS DE INSTALACION

- Gabinete Outdoor Nema 4X para poste.
- Gabinete de comunicación 8ru (24 RU proyección ups).
- UPS de 10 KVAC para Centro de Control.

VARIOS

- Muebles de melamine.
- Sillas giratorias con 5 ruedas.
- Cableado estructurado data, eléctrico y telefonía en centro de control.

EQUIPAMIENTO Y CABLEADO DE LA CENTRAL COMUNICACIONES

- Sub sistema de Telefonía IP.
- Cableado estructurado para voz y datos.
- Cableado eléctrico para estaciones.

- Sub Sistema de Red LAN (equipamiento Activo de Red).
- Sub Sistema de Servidores para Usuarios de Red Administrativa.

DISPOSITIVOS, EQUIPOS Y ACCESORIOS, COMPLEMENTARIOS

- Data center. (Aire Acondicionado, gabinetes, switches, etc).
- Sub Sistema de UPS y Pozos a tierra.

6.2 Pruebas

Este ítem será realizado cuando se viabilice por la Municipalidad Provincial de Huaraz el presente trabajo de investigación.

CAPÍTULO VII: IMPLEMENTACIÓN

7.1 Monitoreo y evaluación de la solución

7.1.1. Elementos del Monitoreo y Evaluación

El monitoreo será desarrollado con el enfoque basado en procesos, uno de los fundamentos de la norma ISO 9001 (Gonzales 2011,24), que consiste en la identificación y gestión sistemática de los procesos desarrollados en la organización y, en particular, las interacciones entre los mismos.

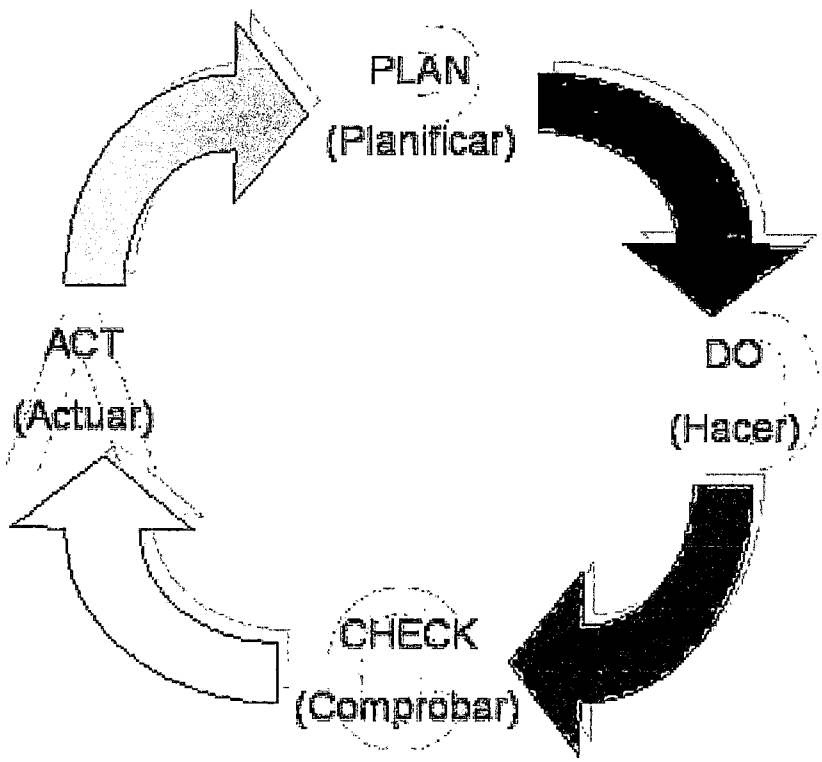
Las acciones de monitoreo se realizarán más eficientemente cuando las actividades y los recursos relacionados se gestionen como un proceso, y para ello, se tiene identificado para su gestión la interacción de los procesos.

El control de los procesos se establecerá a través del ciclo de mejora continua de Deming PDCA (Plan, Do, Check, Act) o Planificar, Hacer, Verificar y Actuar, esquematizado en el Gráfico 7.1.; los elementos del ciclo de monitoreo tienen por función:

1. Toma de datos y registro en las tablas respectivas.
2. Contrastación de los datos contra el nivel esperado de cumplimiento.
3. Decisión respecto de las acciones correctivas o de retroalimentación necesarias de acuerdo a la información obtenida.
4. Implementación de las acciones correctivas o de retroalimentación.

Ilustración 7.1

Ciclo de monitoreo y evaluación



Fuente: Foto proporcionada por internet

7.2 Bitácora y puesta a punto

Este ítem será realizado cuando se viabilice por la Municipalidad Provincial de Huaraz el presente trabajo de investigación.

CAPÍTULO VIII: RESULTADOS

Tabla 8.1

Demanda efectiva del servicio de seguridad ciudadana de Huaraz

PROMEDIO	AÑO 0	AÑO 1	AÑO 2	AÑO 3	AÑO 4	AÑO 5
Número de viviendas	8,252	8367	8484	8603	8723	8846
Número de Pobladores Residentes	41,258	41836	42421	43015	43617	44228
Número de Población Flotante	4,126	4200	4276	4353	4431	4511
DEMANDA TOTAL	45,384	46036	46697	47368	48048	48739

Fuente: Elaboración propia

Esta es la población estimada por un servicio eficiente de seguridad ciudadana la cual está acompañada de la población Flotante que ingresa constante mente a la ciudad por uno y otro motivo (turístico, familiar, comercio, etc.).

Tabla 8.2

Incidencias en el distrito de Huaraz

INCIDENCIAS	2010	2011	2012	2013	2014
Delitos contra el patrimonio	219	224	227	224	224
Delitos contra el cuerpo y la salud	54	55	56	68	64
Delitos contra la salud pública	26	26	30	34	32
Delitos contra la salud sexual	10	10	10	15	16
Delitos contra la libertad	6	6	6	6	6
Delitos contra la familia	48	49	49	53	54
Inconductas sociales	143	147	147	140	139
Total	506	517	525	540	535

Fuente: Elaboración propia

De los resultados se puede observar que mayor cantidad de incidencias son delitos contra el patrimonio en un promedio de 220 incidencias.

Asimismo se observa que las incidencias por inconductas sociales es del orden de 144 incidencias en promedio.

Tabla 8.3

Demanda efectiva de infraestructura de edificación para la seguridad ciudadana

INFRAESTRUCTURA	AÑO 2014
EDIFICACION	I (Demanda)
1. Arquitectura	
2. Estructura	
3. Instalaciones eléctricas	
4. Instalaciones sanitarias	
5. Mobiliario	

Fuente: Elaboración propia

En la actualidad no cuentan con local propio, están ocupando una oficina en el centro cultural que le es insuficiente para poder realizar sus actividades de planes estratégicos de seguridad, entrenamiento, registro, motivación, reunión, etc. Por ende se considera una demanda por infraestructura de edificación y todos sus componentes.

Tabla 8.4

Demanda de requerimientos tecnológicos de telecomunicación para seguridad ciudadana

SEGURIDAD CIUDADANA	AÑ0 2014
TELECOMUNICACIONES	1 (demanda)
1. Televigilancia (ciudad de Hz)	
2. Central de emergencia	
3. Radiocomunicación VHF	
4. Complementos de red	

Fuente: Elaboración propia

En la actualidad la ciudad de Huaraz no cuenta con un servicio de Televigilancia para hacerle frente a la delincuencia en tiempo real, para servir de apoyo a la policía nacional y brindar una sensación de seguridad a la población local y foránea; en su accionar contra la delincuencia. Por ende se considera una demanda para infraestructura de televigilancia y sus respectivos componentes.

Tabla 8.5

Presupuesto estimado para edificación

PRESUPUESTO EDIFICACION

1	ESTRUCTURAS	256,296.78
2	ARQUITECTURA	163,710.00
3	INSTALACIONES ELECTRICAS	108,450.29
4	INSTALACIONES SANITARIAS	30,821.90
5	MOBILIARIO	46,690.00
	TOTAL S/.	**605,968.97**

Fuente: Elaboración propia

Como se observa en la tabla 8.5, el total de los costos para construir el edificio de seguridad ciudadana para la Municipalidad Provincial de Huaraz es de aproximadamente de S/. 605,968.97 nuevos soles.

Tabla 8.6

Presupuesto estimado para telecomunicaciones

PRESUPUESTO
TELECOMUNICACIONES

1	SISTEMA DE TELEVIGILANCIA	2,364,120.00
2	CENTRAL DE EMERGENCIA	297,502.75
3	SISTEMA DE RADIOCOMUNICACION	441,740.00
COSTO DIRECTO TOTAL		3,103,362.75

Fuente: Elaboración propia

Como se observa en la tabla 8.6, el total de los costos para construir la infraestructura de telecomunicaciones que incluye el sistema de televigilancia para seguridad ciudadana para la Municipalidad Provincial de Huaraz es de aproximadamente de S/. 3'103,362.75 nuevos soles, de los cuales el mayor costo es el del sistema de televigilancia por el monto aproximado de S/. 2'364,120.00.

La descripción de este presupuesto se observa en la siguiente tabla:

Tabla 8.7

Presupuesto del sistema de televigilancia

Sub Item	Descripción	UM	Cant.	Unitario S/.	SubTotal	Total S/.
SISTEMA DE TELEVIGILANCIA	CAMARAS IP DOMO					561000,00
	Cámaras color IP DOMO Zoom 36X OPTICO Y 12X Digital	Und.	30	18700,00	561000,00	
	SISTEMA DE VIDEO INTELIGENTE					72000,00
	Equipos de grabación DLS	Und.	3	4000,00	12000,00	
	Software de video analitico IVA	Und.	1	60000,00	60000,00	
	INTERCONEXION					990600,00
	Anillo de fibra óptica multimodo tendido aéreo, incluye instalación	Mt.	5600	45,00	252000,00	
	Nodos de fibra óptica multimodo, con sus respectivos componentes (video cámara), incluye instalación	Und.	30	15000,00	450000,00	
	Terminadores de FO, instalaciones en el video cámara	Und.	30	100,00	3000,00	
	Construcción e instalación de postes de 5mtrs., para tendido de FO	Mt.	5600	18,00	100800,00	
	Gestión de ingeniería	Mt.	5600	15,00	84000,00	
	Verificación de red de fibra óptica	Mt.	5600	18,00	100800,00	
	SOFTWARE					26500,00
	Software de gestión (Administración y gestión)	Und.	1	24500,00	24500,00	
	Software de exportación de videos	Und.	1	2000,00	2000,00	
	CENTRO DE MONITOREO Y GRABACION					226100,00
	Solución de almacenamiento de video 12 TB	Und.	1	81000,00	81000,00	
	Estaciones de trabajo para monitoreo doble monitor	Und.	3	15000,00	45000,00	
	TV LCD de alta defición 50" (incluye rack)	Und.	6	5600,00	33600,00	
	Video wall incluye PC Controlador de video	Und.	1	25000,00	25000,00	
	teclado/joystick de control de cámaras	Und.	2	5500,00	11000,00	
	switch 48 puertos de capa 3	Und.	3	6500,00	19500,00	
	Gabinete 42 RU para sala de enlace principal	Und.	1	3500,00	3500,00	
	UPS 2000 VAC para cada nodo de concentración	Und.	3	2500,00	7500,00	
	ACCESORIOS DE INSTALACION					469000,00
	Gabinete outdoor nema 4X para poste	Und.	30	2000,00	60000,00	
	Gabinete de communicación 8 RU (24 RU proyección ups)	Und.	4	2500,00	10000,00	
	UPS 800 VAC para cámara en poste	Und.	30	500,00	15000,00	
	UPS de 6000 VAC para centro de control	Und.	1	9000,00	9000,00	
	Kit de montaje eléctrico para radio y cámara en poste	Und.	30	500,00	15000,00	
	Postes de cemento x 13 metros, incluye instalación	Und.	30	12000,00	360000,00	
	VARIOS					18920,00
	Aire acondicionado para centro de control	Und.	1	8000,00	8000,00	
	Muebles de melamine	Und.	4	980,00	3920,00	
	Sillas giratorias con 5 ruedas	Und.	4	500,00	2000,00	
	Cableado estructurado data, eléctrico y telefonía en el centro de control	Und.	5	1000,00	5000,00	
	SUB TOTAL					2364120,00
CENTAL DE EMERGENCIA	EQUPAMIENTO Y CABLEADO DE LA CENTRAL DE COMUNICACIONES					297502,75
	Data center (Aire acondicionado, gabinete, switches, etc)	GLB	1	138520,20	138520,20	
	Cableado estructurado para voz y datos	GLB	1	26576,55	26576,55	
	Cableado eléctrico para estaciones	GLB	1	9500,00	9500,00	
	Sub sistema de UPS y pozos a tierra	GLB	1	21000,00	21000,00	
	Sub sistema de servidores para usuarios de red administrativa	GLB	1	26000,00	26000,00	
	Sub sistema de red LAN (equipamiento activo de red)	GLB	1	27456,00	27456,00	
	Sub sistema de telefonía IP	GLB	1	48450,00	48450,00	
	SUB TOTAL					297502,75
SISTEMA DE RADIOCOMUNICACIONES	SISTEMA DE RADIO TRONCALIZADO					441740,00
	Sub sistema de radios remotas (45 radios portátiles)	Und.	45	5560,00	250200,00	
	Sub sistema de radios remotas (10 radios móviles)	Und.	10	6234,00	62340,00	
	Sub sistema de red de communicaciones (1 radio base, 1 repetidor)	Und.	1	56400,00	56400,00	
	Sub sistema de central de communicaciones	Und.	1	72800,00	72800,00	
	SUB TOTAL					441740,00
					TOTAL	3103362,75

Fuente: Elaboración propia

CAPÍTULO IX: DISCUSIÓN DE LOS RESULTADOS

- La demanda efectiva del servicio de seguridad ciudadana de Huaraz, según la tabla 8.1, en el año 0, es decir en el año 2014, es de 45,384 pobladores, de los cuales número de Pobladores Residentes 41,258 y número de Población Flotante 4,126
  - Los beneficios sociales que se generan con la implementación del proyecto son en su mayoría de naturaleza cualitativa y se encuentran orientados a mejorar la calidad y cobertura del servicio de seguridad ciudadana, originando de esta manera que la población beneficiaria puedan ser capaces de mejorar sus condiciones de seguridad.
- De acuerdo a la tabla 8.2, las incidencias en el distrito de Huaraz respecto a los delitos cometidos en años anteriores y actuales como son: Delitos contra el patrimonio, Delitos contra el cuerpo y la salud, Delitos contra la salud pública, Delitos contra la salud sexual, Delitos contra la libertad, Delitos contra la familia, Inconductas sociales.
  - De los resultados se puede observar que mayor cantidad de incidencias son delitos contra el patrimonio en un promedio de 220 incidencias.
  - Asimismo se observa que las incidencias por inconductas sociales es del orden de 144 incidencias en promedio.
- Según la tabla 8.3, la demanda efectiva de infraestructura para la seguridad ciudadana en lo que respecta a: Arquitectura, Estructura, Instalaciones eléctricas, Instalaciones sanitarias. Mobiliario, es positiva. Es decir que se requiere infraestructura necesaria para el mejor servicio de seguridad ciudadana.

- En lo que respecta a la demanda de telecomunicación para la seguridad ciudadana, de acuerdo a la tabla 8.4, se puede observar que es necesario el uso de

televigilancia en la ciudad de Huaraz, así como Central de emergencia, Radiocomunicación VHF y Complementos de red.

- Como se observa en la tabla 8.7, el costo implementar el sistema de televigilancia es por el monto aproximado de S/. 3'103,362.75, con tecnología de fibra óptica multimodo para 10G Ethernet de alta velocidad y video cámara PTZ tipo Domo de última generación,

- Podemos mencionar los principales beneficios cualitativos asociados al proyecto:

    - Disminución del riesgo de ocurrencia delictiva
    - Al existir mayor capacidad tecnológica de monitoreo mediante cámaras de video vigilancia, disminuirá el riesgo de ocurrencia ya que funcionara el sistema como un método disuasivo para cometer actos delictivos.
    - Disminución de gastos en seguridad, personal, domiciliaria y comercial
    - La población residente con la mayor inversión de la municipalidad de Huaraz disminuirá sus gastos en seguridad.
    - Disminución del porcentaje de sensación de inseguridad
    - La población con la mayor inversión en capacidad tecnológica de monitoreo mediante cámaras de video vigilancia, disminuirá la sensación de seguridad ya que se sentirá mayor protegida.
    - Aumenta el valor del predio
    - Al existir seguridad y tranquilad en todos los sectores del Distrito el valor del predio crece sustancialmente en el mercado.
    - Aumenta la inversión privada
    - El empresario o microempresario, dada las condiciones de seguridad busca invertir su capital en el Distrito.
    - Incrementa el Turismo.

Gracias a la seguridad que brinda eficientemente el sereno reduciendo las amenazas delictivas y pandillaje en algunos sectores, provoca el acercamiento de los turistas o visitantes al Distrito.

CONCLUSIONES

1. Un eficiente servicio de Seguridad Ciudadana, trae como consecuencia progreso, tranquilidad y bienestar hacia los vecinos del distrito de Huaraz.

2. Cubrir las atenciones de los servicio de seguridad ciudadana en el distrito de Huaraz en los lugares de intervención mediante el sistema de monitoreo mediante cámaras de video vigilancia.

3. El diseño del sistema de televigilancia utilizando fibra óptica con fines de seguridad ciudadana, permitirá contar con tecnología de última generación teniendo como resultado un eficiente servicio en las telecomunicaciones.

RECOMENDACIONES

- Realizar las gestiones para presentar el presente proyecto para su ejecución por la Municipalidad Provincial de Huaraz.
- Es recomendable el uso de tecnologías de telecomunicación de banda ancha como es el uso de la fibra óptica que optimiza la transmisión de datos, por lo que es recomendable su utilización.
- Debido al incremento poblacional se recomienda aumentar las video cámaras de vigilancia de 30 a 60, ubicados en lugares estratégicos, teniendo en cuenta los índices de peligrosidad.

REFERENCIAS BIBLIOGRÁFICAS

Alcino, Wilder. *Responsabilidad de la familia y la escuela frente al problema del pandillaje.* Argentina: Universidad de Buenos Aires, 2005.

Alvarado Cáceres, Luis. *Mejoramiento e instalación de video cámaras para el servicio de seguridad ciudadana de la ciudad de Huaraz.* Proyecto de ingeniería, Huaraz: MP Huaraz, 2014.

Álvarez, Fernando Antonio. *Criminalidad en Lima.* Técnico, Lima: Ministerio de Justicia, 2006, 123-124.

Barveito Da Silva, Marcelo. «Inseguridad Pública en Rio de Janeiro.» *Seguridad Ciudadana*, s.f.: 14-15.

Carpaneto, Gino. *Adolescencia y juventud en américa latina y el caribe: problemas, oportunidades y desafios en el comienzo de un nuevo siglo.* Chile, 2000.

Chávez. «El ABC de la seguridad ciudadana.» *Seguridad Ciudadana* (Instituto de defensa legal), 2003: 6-7.

Chávez Hidalgo, Ángel Joel. *La estructura y funciones de la Policia Nacional del Perú bajo un enfoque moderno.* Lima: Universidad Nacional Mayor de San Marcos, 2012.

Chipix Notz, Edwin Nathanael. *Participación de actores sociales en espacios de seguridad ciudadana y prevención del delito.* Guatemala: Universidad de San Carlos, 2009.

Chuquitarco, Victor. *Técnicas y tecnologías aplicadas en fibra óptica.* Lima: Universidad Nacional Mayor de San Marcos, 2009.

Congreso de la Republica del Perú. *Constitución Política del Perú.* Lima, 1993.

Cuaquentzi Cruz, Vera Aurora, Edson Eduardo Lechuga Barrientos, y Miguel Angel Nieto Patlán. *Implementación de un sistema de seguridad vía internet.* México D.F.: Instituto Politécnico Nacional de México, 2008.

Daniel, García Murillo. *Telecomunicas y domotica.* Buenos Aires: soluciones domoticas Imagium, 2006.

Dávila Altamirano, Deici Marilú. *Las juntas vecinales en el fortalecimiento de la seguridad ciudadana del distrito de San Juan de Lurigancho, del 2006 hasta el 2009.* Lima: Universidad Nacional Mayor de San Marcos, 2010.

Garcia, Manglyo. *Sistema de comunicaciones por medio de fibre óptica.* Guatemala, 1999.

Guaycha, Mercedes. *Inseguridad Ciudadana.* México D.F.: Mc - Graw Hill Interamericana, 2005.

Hernández Sampieri, Roberto. *Metodología de la investigación.* Colombia: Panamericana e impresos S.A., 1997.

Herrera, Herly. *Diseño de una red de tele vigilancia inalámbrica para los equipos que conforman el sistema de ayuda a la navegación aérea en el aeropuerto palonegro de bucamanga.* Colombia: Universidad Industrial de Santander, 2012.

Lledo Real, Pilar. *La seguridad ciudadana como condición de la democracia.* España: Universidad Autónoma de Madrid, 2003.

Marchiori, Hilda. *Personalidad del delincuente.* México D.F.: Porrúa, 2005.

Murillo Alfaro, Félix. «Teoria General de Sistemas.» *Instituto Nacional de Estadística e informática*, 1999: 8-16.

Patiño Mayer, Hernán. «Crisis sistémica de la seguridad ciudadana.» *Resvista latinoamericana de temas internacionales*, 1999: 61-75.

Peréz, Maria. *La inoperancia de los agentes de seguridad ciudadana como factor de inseguridad incide en el incremento delincuencial en la ciudad de Huaraz durante el período 2006-2010.* Huaraz: Universidad Católica ULADECH, 2012.

Prince, Alejandro. *Las TIC y su relación con la seguridad ciudadana: un marco de análisis a la problemática.* Argentina: Universidad de Buenos Aires, 2010.

Quezada Bringas, Rolando. *Planes de seguridad.* Lima: Universidad Inca Garcilaso de la Vega, 2006.

Rangel, Pedro. *El delito como factor de inseguridad ciudadana.* Caracas Venezuela, 2009.

Sáenz Peña, Roque. *Teoria de las telecomunicaciones.* Buenos Aires: Universidad Nacional de Quilmes, s.f.

Salazar, Antonio, y Juan Carlos Ruiz. «Semana de la Justicia en San Martín: Entre el calor y la búsqueda de justicia.» *Consorcio Justicia Viva*, 2004: 39-41.

Santa Cruz, Oscar. «Principios generales del sistema de fibra óptica.» 2010, Madrid, s.f.

Wikipedia. *Seguridad ciudadana.* s.f. http://es.wikipedia.org/wiki/Seguridad_ciudadana.