UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO

CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

TEMA:

“Propuesta de plataforma crítica de monitoreo para la migración hacia una ciudad inteligente, orientada al aumento de la seguridad y optimización de recursos en el Ecu-911 Ecuador”

AUTOR:

Rodríguez Zambrano, Avelinda Kerench

Trabajo de Titulación previo a la obtención del grado de

INGENIERO EN TELECOMUNICACIONES

TUTOR:

M. Sc. Córdova Rivadeneira, Luis Silvio

Guayaquil, Ecuador

12 de septiembre del 2019

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO

CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

CERTIFICACIÓN

Certificamos que el presente trabajo fue realizado en su totalidad por la Srta. **Rodríguez Zambrano, Avelinda Kerench** como requerimiento para la obtención del título de **INGENIERO EN TELECOMUNICACIONES**.

TUTOR

_____

M. Sc. Córdova Rivadeneira, Luis Silvio

DIRECTOR DE CARRERA

_____

M. Sc. Heras Sánchez, Miguel Armando

Guayaquil, 12 de septiembre del 2019

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO

CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

DECLARACIÓN DE RESPONSABILIDAD

Yo, **Rodríguez Zambrano, Avelinda Kerench**

DECLARO QUE:

El trabajo de titulación: **"Propuesta de plataforma crítica de monitoreo para la migración hacia una ciudad inteligente, orientada al aumento de la seguridad y optimización de recursos en el Ecu-911 Ecuador",** previo a la obtención del Título de **Ingeniero en Telecomunicaciones**, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance del Trabajo de Titulación referido.

Guayaquil, 12 de septiembre del 2019

LA AUTORA

_____

Rodríguez Zambrano, Avelinda Kerench

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO
CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

AUTORIZACIÓN

Yo, **Rodríguez Zambrano, Avelinda Kerench**

Autorizo a la Universidad Católica de Santiago de Guayaquil, la publicación, en la biblioteca de la institución del Trabajo de Titulación: "**"Propuesta de plataforma crítica de monitoreo para la migración hacia una ciudad inteligente, orientada al aumento de la seguridad y optimización de recursos en el Ecu-911 Ecuador"**", cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y total autoría.

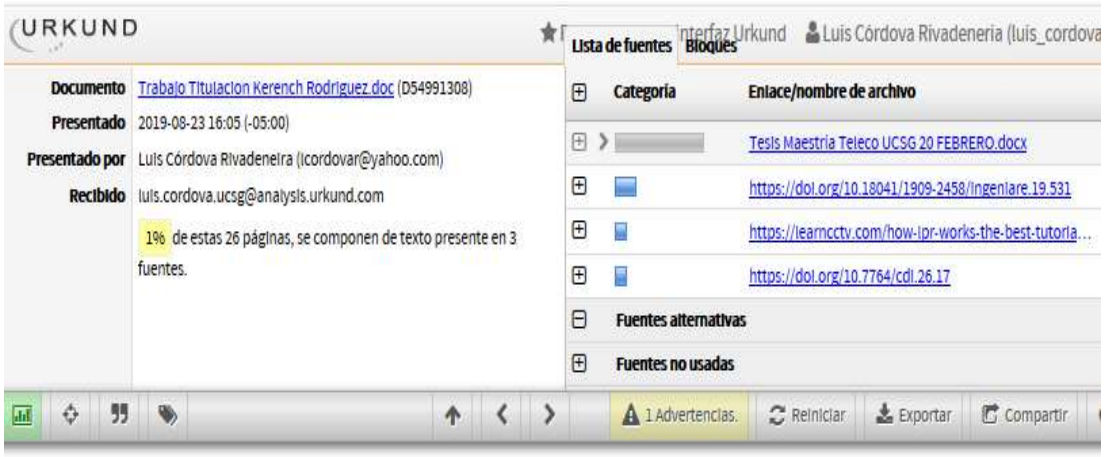
Guayaquil, 12 de septiembre del 2019

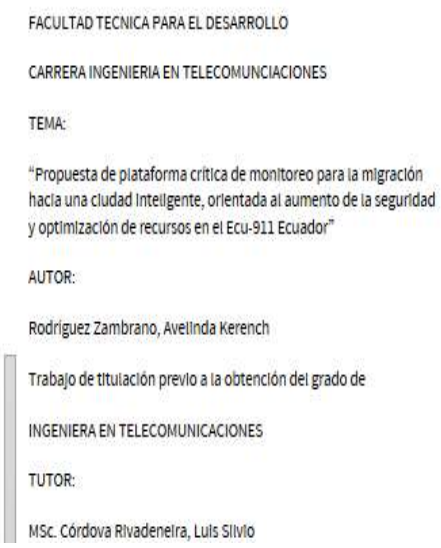
LA AUTORA

_____

Rodríguez Zambrano, Avelinda Kerench

REPORTE DE URKUND





FACULTAD TECNICA PARA EL DESARROLLO

CARRERA INGENIERIA EN TELECOMUNCIACIONES

TEMA:

"Propuesta de plataforma crítica de monitoreo para la migración hacia una ciudad inteligente, orientada al aumento de la seguridad y optimización de recursos en el Ecu-911 Ecuador"

AUTOR:

Rodríguez Zambrano, Avelinda Kerench

Trabajo de titulación previo a la obtención del grado de

INGENIERA EN TELECOMUNICACIONES

TUTOR:

MSc. Córdova Rivadeneira, Luis Silvio

Se ha revisado el trabajo de titulación de la alumna **Rodríguez Zambrano, Avelinda Kerench** en la plataforma **URKUND,** y se ha aprobado con un porcentaje de plagio del 1%.

TUTOR

f. _____

M. Sc. CORDOVA RIVADENEIRA, LUIS SILVIO

DEDICATORIA

Este trabajo de titulación se lo dedico a mis queridos padres: doña Bélgica Zambrano Solórzano y don Rafael Rodríguez Delgado quienes siempre han velado por mi bienestar, me han brindado su amor, así como apoyo incondicional, les honro hoy, ustedes son mi inspiración para ser una mejor persona cada día.

A mis hermanos y familia que todo el tiempo me han apoyado y han sido mi ejemplo para alcanzar mis metas propuestas durante el trayecto de mi vida.

LA AUTORA

Rodríguez Zambrano, Avelinda Kerench

AGRADECIMIENTO

A Dios Todopoderoso, Padre querido, quien me ha dado de su gracia y guiado mis pasos, por sacarme de mi zona de confort y darme de su aliento para aspirar a más. ¡Agradezco su amor inagotable y su gran fidelidad!

A mi familia y amigos por todas las concesiones que hicieron para apoyarme en el desarrollo de esta etapa profesional.

A todo el personal de la Facultad Técnica que me acogió en este período de estudios, agradezco el aprendizaje y el hacerme sentir como en casa, en verdad disfruté este tiempo.

Al Ing. Luis Córdova Rivadeneira por afirmar y enriquecer mis conocimientos con su valiosa experiencia, y complementarlo con su valiosa amistad.

.

LA AUTORA

Rodríguez Zambrano, Avelinda Kerench

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE EDUCACIÓN TÉCNICA PARA EL DESARROLLO

CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

TRIBUNAL DE SUSTENTACIÓN

f. _____

M. Sc. ROMERO PAZ, MANUEL DE JESUS

DECANO

f. _____

M. Sc. PALACIOS MELÉNDEZ, EDWIN FERNANDO

COORDINADOR DEL ÁREA

f. _____

M. Sc. BASTIDAS CABRERA, TOMAS GASPAR

OPONENTE

ÍNDICE GENERAL

Índice de Figuras

Capítulo 2

Capítulo 3

Índice de Tablas

Capítulo 2

Resumen

En el presente trabajo se realiza un análisis técnico a fin de presentar una propuesta de plataforma crítica de monitoreo que pueda operar como base tecnológica de un centro de seguridad ciudadana y que brinde las condiciones para la migración hacia ciudades inteligentes, incrementando la seguridad y la optimización de recursos de personal, financieros y tiempos de respuesta de un centro de atención ciudadana como lo es el Ecu-911. En el Capítulo 1, se presentan algunos de los criterios que rigen los modelos de ciudades inteligentes y de gestión de control de la infraestructura critica, se emplea una investigación de tipo descriptiva y exploratoria y se establecen los objetivos del presente trabajo. El Capítulo 2, comprende la fundamentación teórica del tema de evaluación, abordando nociones de video vigilancia base, hasta la cobertura de conceptos específicos relacionados con la inteligencia de video a implementar. El Capítulo 3 se enfoca en la aportación realizada por quien suscribe a nivel del diseño, en cuanto a la selección de la plataforma a usar, implementación de los servicios específicos seleccionados. El Capítulo 4, finaliza con las conclusiones y recomendaciones resultantes de las pruebas realizadas en el presente trabajo en miras de adoptar una infraestructura de gestión crítica su contribuir de esta manera con el establecimiento de ciudades inteligentes en miras de la mejora de la calidad de vida de la población.

PALABRAS CLAVE: CIUDAD INTELIGENTE, MONITOREO, RECONOCIMIENTO, GESTIÓN, CONTROL, VIDEO ANALITICA.

ABSTRACT

In this work, a technical analysis is presented before recommending the implementation of a system for monitoring the critical infrastructure for cities where the ECU911 is present. The ECU911 is the Ecuadorian government entity created to integrate and coordinate security services, integrating the police, firefighting group, risk management minister, etc. In the future, this system could be linked to other platforms allowing the cities to be considered as smart cities. In chapter 1, smart cities models, and how they manage the critical infrastructure monitoring are discussed. Based on this, the general and specific objectives for this work are defined. In chapter 2, the video-surveillance fundamentals, including specific issues such as intelligence of video are evaluated respect to the objectives defined in the chapter 1. In chapter 3, the proposed platform design is presented. The criteria used by the author for designing and implementing the system is discussed. The conclusions and recommendations are showed in chapter 4, based on the testing results carried out during the execution of the present work. Recommendations are focused on a potential implementation of this system, allowing the cities to be considered as a smart city.

KEY WORDS: SMART CITY, MONITORING, RECOGNITION, VIDEO GESTION, CONTROL VIDEO ANALYTICS.

CAPÍTULO 1: INTRODUCCIÓN

1.1. Introducción.

El crecimiento exponencial de las ciudades a nivel mundial ha llevado al desarrollo del concepto de las Ciudades Inteligentes o Smart Cities, entendiéndose como ciudades inteligentes un área geográfica o territorio que se caracteriza por el uso intensivo de las tecnologías con el objetivo, de manera general, de mejorar la calidad de vida de los ciudadanos y el desarrollo sostenible de las ciudades bajo los supuestos de la colaboración y la innovación (Góngora, 2015).

En las ciudades inteligentes a nivel mundial, los servicios de seguridad suelen implementarse por medio de los centros de atención ciudadana por ser ciudades en desarrollo y cuyo dinamismo hace que el requerimiento de seguridad sea uno de los factores primordiales para una atención activa al público que impulsa el turismo y a la vez combate el crimen.

Dado a que las grandes ciudades requieren más recursos para manejar amenazas tales como asaltos, robo de vehículos, agresiones, tráfico de drogas, violencia de pandillas, etc… teniendo como finalidad acabar con la delincuencia y puntos ciegos de la ciudad, como también reducir el tiempo administrativo mejorando la eficiencia del recurso humano, los funcionarios Municipales y de Centros de atención de Seguridad Ciudadana 911 han implementado una revisión integral de sus soluciones de seguridad, requiriendo para ello de sistemas confiables y eficientes para proteger mejor a sus comunidades.

1.2. Antecedentes.

El término “Infraestructura Crítica” en una ciudad fue definido por los autores Luiijf, Burger y Klaver, en su paper *Critical Insfraestructure Protection in the Nehterlands: A Quick –Scan (2003)*, definen “infraestructura crítica” a partir de servicios o productos que tienen ciertos atributos: aquellos que realizan una contribución esencial en la sociedad, en el sentido de mantener

niveles mínimos definidos de estado de derecho y orden público local e internacional, seguridad pública, economía, salud y medioambiente. Cuando su pérdida o interrupción impacta a los ciudadanos y a la administración (gobierno) a escala nacional o pone en riesgo los niveles mínimos de calidad de servicio (Barros, 2010).

Dicho concepto abarca una amplia gama de locaciones de control como lo son carreteras, autopistas, servicios públicos, edificios gubernamentales, plantas de tratamiento de agua, etc. A ello se le suma los controles de tránsito vehicular y detección de incidentes que se presenten en la ciudad, por lo que monitorear todas estas áreas requiere de una vigilancia permanente por parte de los operarios de los centros de monitoreo de la ciudad y el ser asistidos por tecnologías soporte como lo son sensores, cámaras de video vigilancia, drones, etc.

La importancia de monitorear la infraestructura crítica no es sólo para efectos de seguridad, sino también para garantizar que la población disponga de suministros ininterrumpidos de los servicios proporcionados por el gobierno, que incluyen el servicio de agua, electricidad, acceso a carreteras, etc…todo ello en vías de una mejor calidad de vida de los residentes de dicha ciudad (Barros, 2010).

Las cámaras de vigilancia cumplen dos grandes roles en su operación: la disuasión del delito y pruebas forenses para documentar incidente; sin embargo, además de las cámaras de vigilancia y los sensores, los niveles de interés en la utilización de aviones no tripulados (drones) para inspecciones y monitoreo están creciendo rápidamente en ciudades que buscan traducir mayores beneficios a sus habitantes y que asimismo deben incluirse en la gestión de control.

Por lo que el monitoreo de infraestructura crítica es una prioridad esencial que una ciudad debe emprender para aumentar la seguridad, mantener servicios continuos en toda la ciudad, cumplir con las regulaciones gubernamentales y potencialmente aumentar los ingresos para la ciudad, para

lo cual el presente trabajo hace el planteamiento de uso de una de las plataformas de gestión de infraestructura critica más conocidas y versátiles a nivel mundial, realizar un diseño de una demo para efectos de validar su compatibilidad con la infraestructura actual del ECU-911 y validar la operación de los módulos de inteligencia seleccionados por la institución para efectos de estas gestión.

Ello con miras a contribuir con la implementación de ciudades inteligentes o Smart Cities las cuales tienen un enfoque de gobernabilidad y seguridad, así como brindar las condiciones para una convivencia pacífica de sus habitantes, por lo que se propone al ECU-911 el uso de una plataforma crítica de monitoreo que brinde herramientas analíticas inteligentes útiles para una mejor operación interna, que generen iniciativas pro activas mediante el uso de módulos avanzados de procesamiento de video en vivo o grabado, entre ellos como Face Recognition (Reconocimiento Facial), Lectura de placas de automóviles (LPR) en regiones y puntos estratégicos de la ciudad para identificar posibles infractores, evitar la circulación de vehículos robados en la ciudad, analíticas varias como objetos abandonados, removidos, seguimiento de personas, y aglomeración en áreas específicas de control, entre otros, brindando asimismo informes o reportes forénsicos con búsquedas avanzadas en cuestión de segundos.

1.3. Justificación del Problema.

Debido al volumen de cámaras de video vigilancia instaladas en todo el país, día a día se almacena una densidad cada vez mayor de información de video, cuyo análisis o búsqueda de un evento figura una compleja labor dada la significativa información disponible. Esta realidad experimentada de igual forma a nivel mundial, ha conllevado al desarrollo de sistemas de video inteligente que permiten gestionar de forma ágil la información captada por las cámaras, como lo son matrículas de vehículos, conteo de personas, entre otros.

Dichos datos al ser contrastados por el sistema inteligente contra una base de datos facilita la identificación de diversos eventos en fracciones de

segundos, traduciéndose en una reducción del trabajo del personal y una mayor eficiencia en el control de la seguridad, por ello este proyecto propone realizar las pruebas de compatibilidad y funcionamiento de una plataforma crítica de gestión, complementando la infraestructura tecnológica ya existente en el ECU-911 permitiéndole incrementar su eficiencia y elevando su capacidad en tiempos de respuesta ante los eventos que requieren su atención.

1.4. Definición del Problema.

La idea nace por la gran convergencia de cámaras instaladas en el centro de atención ciudadana que requieren ser controladas a diario por parte del ECU-911 por lo que se busca brindar una alternativa al ECU-911 de un sistema de video inteligente que sea compatible con la actual plataforma que cuenta la institución y que permita el ágil proceso de imágenes de video, incrementando los niveles de respuesta a eventos y así contribuir con el incremento de seguridad en la población.

1.5. Objetivos del Problema de Investigación.

1.5.1. Objetivo General.

Proponer una plataforma crítica de monitoreo para la migración hacia una ciudad inteligente, orientada al aumento de la seguridad y optimización de recursos en el Ecu-911 Ecuador, por medio de la activación y pruebas de las principales funcionalidades de seguridad en video vigilancia disponibles en la plataforma.

1.5.2. Objetivos Específicos.

- Configurar y probar la operación de la plataforma propuesta con las cámaras pre-existentes en la institución.
- Realizar la configuración de lectura multinacional de placas en las cámaras con las que opera la institución.
- Activar la funcionalidad de reconocimiento facial en las cámaras disponibles en el ECU-911.
- Efectuar la activación y pruebas de la funcionalidad de Analítica de video en las cámaras que determine la institución.

1.6. Hipótesis.

Con el debido diseño, dimensionamiento y configuración de la plataforma crítica de monitoreo propuesta, se brindará las condiciones para la migración hacia una ciudad inteligente, orientada al aumento de la seguridad y optimización de los recursos en el Ecu-911 Ecuador.

1.7. Metodología de Investigación.

La metodología utilizada en este trabajo de titulación es de tipo investigativo-analítico ello debido a que la propuesta requiere la adquisición de conocimientos para poder actuar y diseñar la solución, así como de tipo analítico, dado a que se requiere efectuar cálculos para obtener datos que permitan un diseño eficaz.

CAPÍTULO 2: FUNDAMENTACIÓN TEÓRICA

2.1. Introducción.

En el presente capítulo se revisan conceptos principales relacionados con la propuesta del presente trabajo de titulación que brindan las bases para realizar el planteamiento en mención, por lo que se inicia con una revisión de la evolución de la gestión de Video Vigilancia, se revisan asimismo algunos criterios de la inteligencia artificial y se complementa con la indicación de las cámaras de red, su definición, características y tipos existentes.

2.2. Evolución de la Gestión de Video Vigilancia.

2.2.1. DVR.

Un equipo DVR (Digital Video Recorder) es considerado la evolución de una video casetera de grabación de video vigilancia. Se trata de una solución orientada a cámaras de video analógicas, en la cual se concentra la conexión de todos los cables coaxiales que caracterizan las conexiones de las cámaras de esta tecnología.

Aunque los DVR están orientados a gestionar cámaras análogas, existen modelos con versión Híbrida, que permiten la conexión de cámaras IP de forma paralela. Por esta razón este equipo también es conocido como “codificador de video”, ya que permite tomar la información de la cámara (análoga y/o IP), digitalizarla y enviarla a través de una red basada en IP (LAN, WAN y/o internet).

Esta solución de grabación suele contar con una capacidad limitada de cámaras a gestionar, asociadas al modelo de equipo que se escoja, el mismo que tiene un número máximo de cámaras que puede procesar según la capacidad del equipo.

Ventajas:

- Es una solución muy sencilla de instalar.
- Requiere de conocimientos mínimos de configuración IP.

- Es una opción muy económica.

Desventajas:

- Límite de cámaras a gestionar: determinado por el modelo de hardware a usar.
- Los costos por adquisición de hardware no requerido: en esta gestión de video indistintamente de la cantidad de cámaras a instalarse, el DVR debe adquirirse en función de los modelos disponibles por el fabricante.
- La densidad de cables: dado a que integra conexiones con cable coaxial, el espacio y peso que requiere este tipo de cableado representa un tema de consideración en el diseño de un cuarto de seguridad.

En la Figura 2.1 indicada a continuación se puede observar el diagrama estándar de conexión de un equipo DVR.

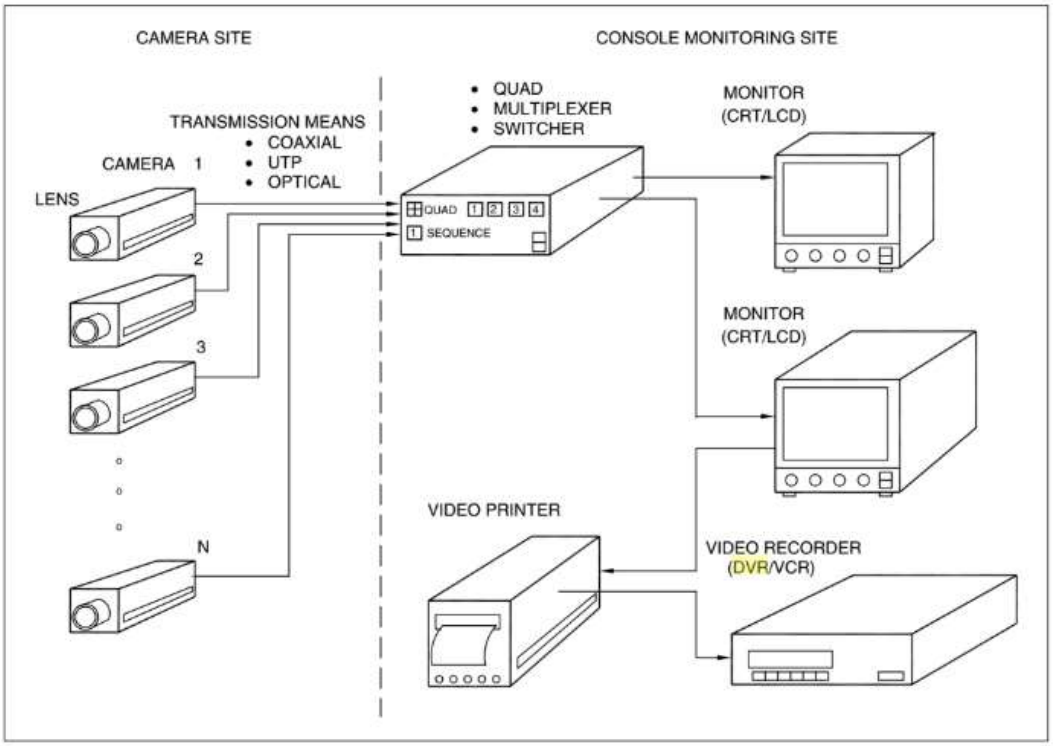


Figura 2. 1: DVR - Diagrama de conexión.
Fuente: (Kruegle, 2011)

2.2.2. NVR.

Una solución de grabación más sofisticada la constituye el grabador de red conocido como NVR (Network Video Recorder), el cual permite la

grabación digital de cámaras de red (cámaras IP) y cuya gestión y visualización se efectúa a través de un PC ubicado en la red.

Los NVR iniciaron el gerenciamiento de las imágenes, como lo son búsqueda de videos por medio de filtros más avanzados, acceso remoto a cámaras a través de una red IP, gestión de eventos, alimentación a través de Ethernet y medidas avanzadas de seguridad. En la Figura 2.2 se indica el diagrama de conexión de una red con gestión de video vía NVR.

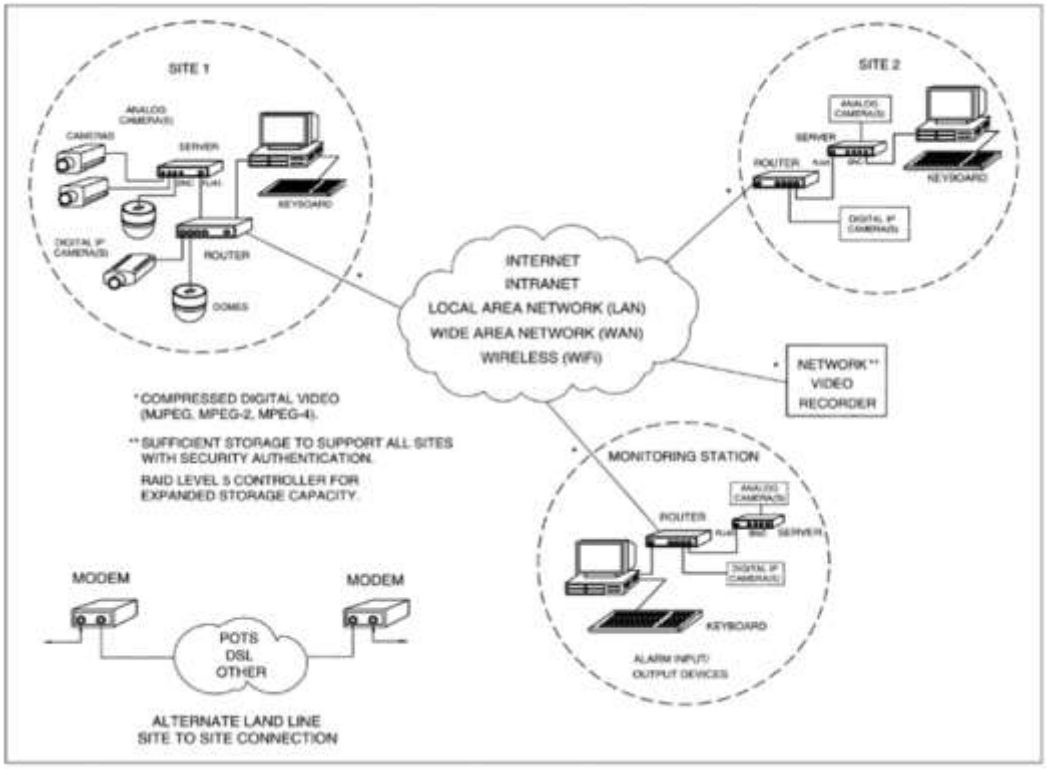


Figura 2. 2: NVR - Diagrama de conexión.
Fuente:(Kruegle, 2011)

2.2.3. VMS.

La evolución de la gestión de video dio un gran paso con la aplicación de la solución de plataforma de servidor de PC, donde se obtiene un marcado incremento del rendimiento del procesamiento de la información de video, basado en el diseño especifico de los componentes del sistema (computador) a usar en función del requerimiento.

El VMS (Video Management Software) es como sus siglas lo indican, un software que se ejecuta en un computador con sistema operativo Windows.

La plataforma de gestión de video VMS brinda la flexibilidad de escoger los fabricantes de nuestra preferencia y la última tecnología disponible para sus diferentes componentes.

El software de administración de video (VMS) es responsable de ubicar y agregar todas las cámaras IP que se encuentran en la red, proporcionar una conexión segura a las cámaras y grabar todo el video especificado de todas las cámaras. Es conocido que si una persona mira fijamente un pantalla durante varios minutos, escenas importantes no son percibidos, por lo que el software VMS también proporciona alertas especificas a la persona de seguridad, optimizando actividades que antes dependían de un operador (Addati, 2014)

Para esta solución, se enlistan a continuación las principales ventajas y desventajas**:**

Ventajas:

- Al estar cimentado en una estructura robusta de hardware, el sistema VMS amplía el concepto de gestión del sistema de seguridad, por lo que la información de cámaras de video se constituye ahora en uno de los componentes de seguridad, agregándose a la gestión dispositivos de grabación digital, control de acceso, sistemas de alarmas, biométricos, etc…
- Brinda la opción de gestión de las cámaras a través de la nube.
- Otorga servicios de video avanzados como lo son lectura de placas, reconocimiento facial, analítica de video, etc...
- Interacción con tecnología de cámaras análogas e IP.
- Gestión de un número ilimitado de cámaras
- Opción de contar sistemas de redundancia y Fail Over.
- Integración multimarcas de cámaras y NVRs (depende del VMS a elegir).
- Mapas dinámicos interactivos
- Control de activos
- Código abierto que permite integrar otro tipo de dispositivos a la plataforma de gestión.

Desventajas:

- La computadora utilizada para ejecutar el software VMS debe tener suficiente rendimiento y almacenamiento para admitir la cantidad de cámaras IP a conectarse.

- Cuantas más cámaras y cuanto mayor sea la resolución de las cámaras a usar, mayor será el rendimiento requerido. El período de tiempo del video grabado determinará la cantidad de almacenamiento requerido en el disco duro.
- Alto nivel de conocimientos requeridos. Dependiendo del software VMS utilizado es necesario un nivel de capacitación o certificación especializado para efectuar las configuraciones de la plataforma (software de gestión).
- Alto costo en hardware, dado el diseño personalizado de componentes a usar.
- Orientado principalmente a requerimientos de alto nivel, por lo que no suele aplicar a soluciones tipo hogar o pequeñas empresas.

Se puede observar en la Figura 2.3 el diagrama de conexión del sistema VMS

Figura 2. 3: Diagrama de conexión VMS.
Fuente: (Marshall Electronics, 2019)

2.3. Comparativo entre sistemas de Gestión de Video Vigilancia

En la siguiente Tabla 2.1 se efectúa un comparativo de las principales funcionalidades de los sistemas de gestión de video vigilancia en relación con su complejidad, alcance y servicios.

Tabla 2. 1: Comparativo entre soluciones de gestión de video vigilancia**.**

Caracteristicas	DVR	NVR	VMS
Numero de camaras	Limitado*	Limitado*	Ilimitado
Integracion de Camaras Analogas	Sí*	No	Sí
Integracion de Camaras IPs	Sí*	Sí	Sí
Lectura de placas	No	No	Sí
Video Analitico	No	No	Sí
Reconocimiento facial	No	No	Sí
Deteccion de Intrusion Perimetral	No	No	Sí
Control de Acceso	No	No	Sí
Intercomunicadores	No	No	Sí
Mapas dinamicos e interactivos	No	No	Sí
Servicios en la nube	No	No	Sí
Control de Activos	No	No	Sí
Nivel conocimientos para configuracion	Bajo	Intermedio	Alto
Distancias de gestion	Corta	Media	Alta
Enfoque de aplicación	Hogar/Pyme	PYME	Corporativo
* Asociado al modelo de hardware escogido			

Elaborado por: Autor

2.4. Procesamiento de información.

Dado a que el software de gestión de video VMS realiza el procesamiento de la información, se revisa brevemente a continuación las opciones de procesamiento de la información.

2.4.1. Procesamiento centralizado. -

Escenario donde una sola computadora o “host”, a menudo una unidad central, maneja todo el procesamiento; es decir: entrada, salida y almacenamiento de datos. Este tipo de procesamiento de información caracterizó los inicios de los sistemas de computación.

Su principal ventaja es que se tiene un solo punto de control por lo que pueden reforzarse los controles de seguridad, así como son fáciles de

mantener dado a que el soporte es en un solo punto. En la Figura 2.4 se grafica la interacción de este tipo de procesamiento

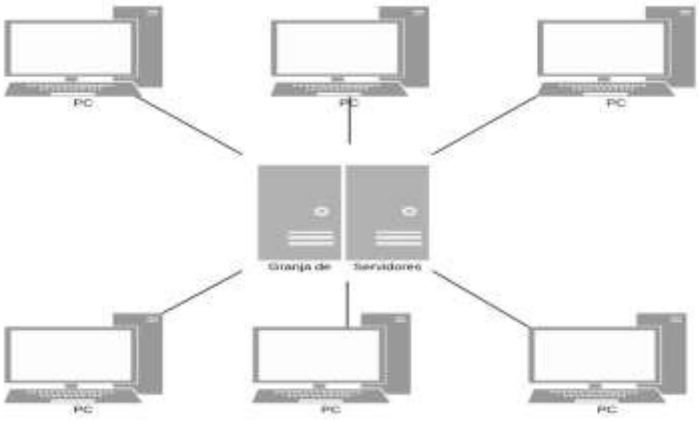


Figura 2. 4: Procesamiento Centralizado.
Elaborado por: Autor

2.4.2. Procesamiento distribuido. –

Corresponde al sistema de procesamiento de información utilizado en la actualidad en el que todo el procesamiento es manejado por un número determinado de computadoras o "host" como lo son estaciones de trabajo, PC, servidores, etc…Los diferentes hosts, se distribuyen físicamente y se interconectan a través de las comunicaciones de red. Cada máquina posee sus propios componentes (hardware y software) pero que el usuario los percibe como un solo sistema, accediendo a recursos remotos como locales con la misma facilidad.

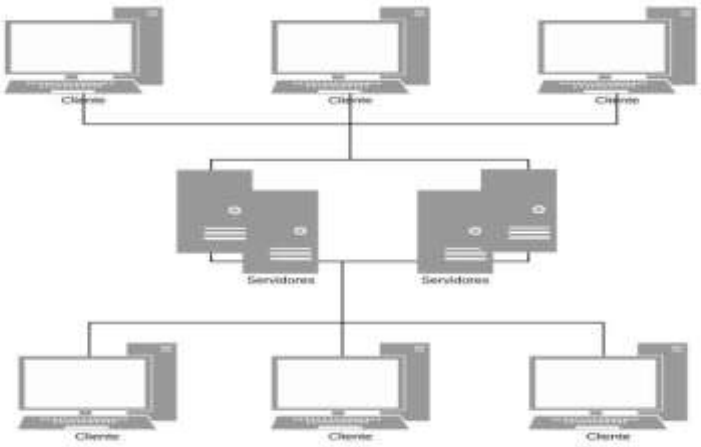


Figura 2. 5: Procesamiento Distribuído
Elaborado por: Autor

Los sistemas distribuidos deben ser diseñados de forma muy estable dado que, si un sistema falla, otro elemento debe tener la capacidad de cubrirlo, lo cual se denomina “Tolerancia a fallas”. En la Figura 2.5 se visualiza el procesamiento de información distribuído.

2.4.3. Procesamiento cooperativo. –

El desarrollo y requerimientos de la tecnología visualiza un procesamiento cooperativo, indicado en la Figura 2.6, como el futuro de la tecnología en procesamiento de información, donde aunque muy similar al caso anterior, una serie de computadoras (estaciones de trabajo, servidores, etc.…) manejen todo el procesamiento, estén distribuídas físicamente y se conecten a través de la red, su diferencia y optimización radique en que el procesamiento sea a través del intercambio de recursos y que ello sea transparente para el usuario.

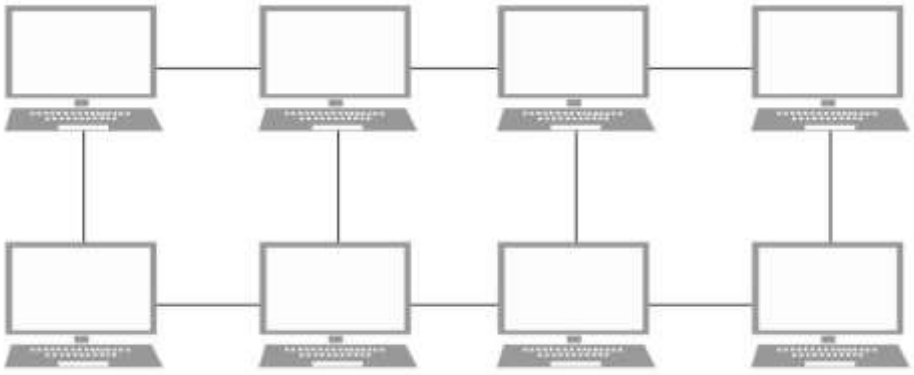


Figura 2. 6: Procesamiento Cooperativo
Elaborado por: Autor

En este punto se definen dos agentes presentes en estos escenarios de procesamiento de información:

a. Servidor:

Es una máquina cuyo propósito es proveer de un servicio que otras máquinas puedan le hayan solicitado proveer. En estricto rigor un servidor es un tipo de software que provee un servicio que ha sido requerido por sus usuarios; sin embargo, actualmente, el término servidor se utiliza generalmente para referirse al conjunto de hardware (máquina) y el software de servicio que se ejecuta en el mismo. Un servidor le permite a un cliente

accesar a los servicios que este brinde (programas, archivos, datos, etc…), brinda sus servicios a través de una interfaz verdadera o mediante una línea telefónica o digital y almacenan información en forma de páginas web por medio del uso del protocolo HTTP y lo entregan a petición de los clientes (navegadores web) en formato HTML.

b. Cliente. -

Es un tipo de software que demanda información de un servidor. De igual manera que en el caso del servidor, el software cliente puede estar instalado en una máquina desde donde se realizan las peticiones al servidor de interés. Un punto a destacar es que un cliente puede operar como servidor y un servidor puede operar como cliente. A continuación, en la Tabla 2.2 se establece un comparativo entre las principales diferencias entre los sistemas de procesamiento de información centralizado y distribuído.

Tabla 2. 2: Sistemas de procesamiento de información

Area	Centralizado	Distribuído
Punto de control	Uno	Soporta Tolerancia a fallos
Mantenimiento	Fácil	Complejo
Toma de decisiones	Locales	En cada lugar, de forma independiente de otras localidades
Interfaz de usuario	Poco llamativa	Llamativa y amigable
Ancho de banda	Requiere control	Solo consume el de una red local
Velocidad de respuestas	Lenta	Rápida
Respaldo, contingencia	Es critico dado a que si falla el punto principal no hay servicio alguno	Es recomendable, pero aisla los puntos de falla
Crecimiento	Depende del hardware	Se adapta a los requerimientos
Distribucion de datos	Centralizada	Permite escoger de acuerdo a la logica del negocio
Costo y complejidad del software	Económico	Alto
Soporte de tecnología	Local	En cada lugar se debe tener personal de soporte

Elaborado por: Autor

2.4.4. Arquitectura cliente-servidor. -

Cliente/servidor es una arquitectura de red en la que cada ordenador o proceso en la red es cliente o servidor. Normalmente, los servidores son ordenadores potentes dedicados a gestionar unidades de disco (servidor de ficheros), impresoras (servidor de impresoras), tráfico de red (servidor de red),

datos (servidor de bases de datos) o incluso aplicaciones (servidor de aplicaciones), mientras que los clientes son máquinas menos potentes y usan los recursos que ofrecen los servidores. Esta arquitectura implica la existencia de una relación entre procesos que solicitan servicios (clientes) y procesos que responden a estos servicios (servidores). Estos dos tipos de procesos pueden ejecutarse en el mismo procesador o en distintos (Luján-Mora, 2001). La arquitectura cliente/servidor implica la realización de aplicaciones distribuidas. La principal ventaja de esta arquitectura es que permite separar las funciones según su servicio, permitiendo situar cada función en la plataforma más adecuada para su ejecución (Luján-Mora, 2001).

Esta arquitectura cuenta asimismo con los sistemas multicapas que consiste en que el servidor de divide en diferentes programas que pueden ser ejecutados por diversas computadoras incrementando de esta manera el grado de distribución del sistema.

2.4.5. Arquitecturas de dos y tres niveles. -

La diferencia entre las aplicaciones de dos y tres niveles estriba en la forma de distribución de la aplicación entre el cliente y el servidor. Una arquitectura de dos niveles está basada en un sistema gestor de bases de datos donde las aplicaciones supeditan la lógica de los procesos cliente al gestor de base de datos que se está usando.

En las arquitecturas de tres niveles, la lógica de presentación, la lógica de negocio y la lógica de datos pueden estar repartidas entre distintos procesadores. El objetivo de aumentar el número de niveles en una aplicación distribuida es lograr una mayor independencia entre un nivel y otro, lo que facilita la portabilidad en entornos heterogéneos(Luján-Mora, 2001) .

2.5. Cámaras IP

A diferencia de una cámara análoga, una cámara IP es un sistema completo que cuenta con computador embebido (CPU) incorporada y un servidor web que transmite imágenes de video de alta calidad generalmente utilizada en propósitos de video vigilancia y seguridad.

El disponer de estos elementos internos, permite que el procesamiento de las imágenes sea digital desde el momento de recibir la información externa por medio del lente, así como su transmisión posterior a través de la red de comunicaciones, por medio del protocolo IP (Internet Protocol) con el que opera. En la Figura 2.7 se visualiza en diagrama de bloques, la secuencia interna de procesamiento de información en una cámara IP.

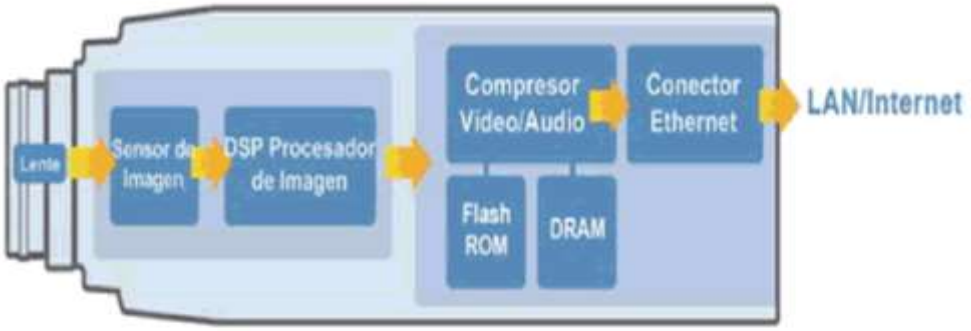


Figura 2. 7: Diagrama de bloques de operación cámara IP
Fuente: (Mata, 2010)

La concepción de un CPU interno en la cámara IP le permite operar en cualquier punto donde exista una conexión de red, de forma independiente de un computador,

Asimismo, al contar con una interfaz de red (ya sea cableada o inalámbrica), a este tipo de cámara se le asigna un direccionamiento IP como otro equipo en la red, dado los protocolos de IP con los que cuenta, lo cual le permite operar dentro de la red interna del cliente o, si fuese necesario y con los permisos respectivos, puede ser accesada desde afuera de la red local, vía internet.

Tipos de cámaras IP

Las cámaras IPs se clasifican por el tipo de construcción con el que fueron diseñadas y por el tipo de enfoque que brindan sus lentes.

2.5.1. Por el tipo de construcción

Se clasifican en cámaras de interiores y exteriores. Las cámaras de interiores (indoor) son cámaras que están contruídas para trabajar en ambientes controlados de luz y temperatura.

En el caso de las cámaras para exteriores (outdoor), los elementos con los que están contruídas han sido pensados para soportar condiciones atmosféricas adversas como altas o bajas temperaturas, agua, polvo, vandalismo o incluso explosiones.

Para identificar el grado de protección con el que está diseñada una cámara se creó el estándar estadounidense ANSI/IEC 60529-2004, el cual consiste en un par de dígitos que se agregan a las siglas IP (International Protection), cada uno de ellos con un significado específico, según se detalla a continuación en la Figura 2.8.

Figura 2. 8: Grado de protección IP
Fuente: (NUO by Techdesign, 2015)

A continuación, se detallan en la Tabla 2.3 las referencias de protección asociadas al primer dígito

Tabla 2. 3: Significado del primer dígito de protección IP-_ X

NIVEL	DESCRIPCIÓN
0	Sin protección
1	Protegido contra la entrada de elementos sólidos de hasta 50mm.
2	Protegido contra la entrada de elementos sólidos de hasta 12,5mm.
3	Protegido contra la entrada de elementos sólidos de hasta 2,5mm.
4	Protegido contra la entrada de elementos sólidos de hasta 1mm.
5	Protegido contra la entrada de polvo (la cantidad que entra no intefiere con el funcionamiento del dispositivo).
6	Totalmente protegido contra la entrada de polvo.

Fuente: (NUO by Techdesign, 2015)

De la misma manera, se indica el enfoque de protección del segundo dígito según se puede observar en la Tabla 2.4:

Tabla 2. 4: Significado del segundo dígito de protección IP-_ X

NIVEL	DESCRIPCIÓN
0	Sin protección
1	No debe entrar el agua cuando se la deja caer, desde 200mm de altura respecto del equipo, durante 10 minutos (a razón de 3-5mm³ por minuto).
2	No debe entrar el agua cuando se la deja caer, durante 10 minutos (a razón de 3-5mm³ por minuto). Dicha prueba se realizará 4 veces a razón de una por cada giro de 15° tanto en sentido vertical como horizontal, partiendo cada vez de la posición normal de trabajo.
3	No debe entrar el agua nebulizada en un ángulo de hasta 60° a derecha e izquierda de la vertical a un promedio de 11 litros por minuto y a una presión de 800-100 kN/m² durante un tiempo que no sea menor a 5 minutos.
4	No debe entrar el agua arrojada desde cualquier ángulo a un promedio de 10 litros por minuto y a una presión de 800-100 kN/m² durante un tiempo que no sea menor a 5 minutos.
5	No debe entrar el agua arrojada a chorro (desde cualquier ángulo) por medio de una boquilla de 6,3 mm de diámetro, a un promedio de 12,5 litros por minuto y a una presión 30 kN/m² durante un tiempo que no sea menor a 3 minutos y a una distancia que no sea menor de 3 metros.
6	No debe entrar el agua arrojada a chorros (desde cualquier ángulo) por medio de una boquilla de 12,5 mm de diámetro, a un promedio de 100 litros por minuto y a una presión 100 kN/m² durante un tiempo que no sea menor a 3 minutos y a una distancia que no sea menor de 3 metros.
7	El equipo debe soportar sin filtración alguna la inmersión completa a 1 metro durante 30 minutos.
8	El equipo debe soportar sin filtración alguna la inmersión completa y continua a la profundidad y durante el tiempo que especifique el fabricante del producto con el acuerdo del cliente, pero siempre que resulten condiciones más severas que las especificadas para el valor 7.

Fuente: (NUO by Techdesign, 2015)

Por lo que, si en la descripción de una cámara IP para exteriores se indica que esta cuenta con la protección IP67, de acuerdo a la referencia de los cuadros previos, por su primer dígito (6) se determina que la cámara IP está protegida contra el ingreso de polvo bajo toda circunstancia, mientras que el segundo dígito (7) hace referencia a su protección al ingreso de líquidos en una inmersión durante 30 minutos, con hasta 1 metro de profundidad.

2.5.2. Por el tipo de enfoque

Las cámaras pueden clasificarse a su vez por el enfoque de una imagen que brindan a través de sus lentes en cámaras de toma fija y movimiento o PTZ.

Cámaras Fijas. -

Se denominan así las cámaras que tienen una toma de vista fija. Este tipo de cámaras son fácilmente identificables dado a que la ubicación de la cámara y su lente determinan la dirección de la toma que está realizando.

Este tipo de cámaras son muy usadas en video vigilancia como elementos disuasivos y sus presentaciones varían según el área de instalación disponible.

El modelo de cámara fija tipo Caja (Box) es uno de los primeros modelos de cámaras de video vigilancia y se visualiza en la Figura 2.9. Se dispone de carcasa de protección para instalaciones en exteriores.

Figura 2. 9: Cámara Fija Tipo Caja (Box)
Fuente: (Mata, 2010)

Otro modelo de cámara fija es conocida como Bala (Bullet) con iguales funciones que el modelo Box, pero con forma cilíndrica y de menor dimensión, indicada en la Figura 2.10.

Figura 2. 10: Cámara Fija Tipo Bala
Fuente: (Uniview Technologies Co., Ltd, 2011)

La presentación tipo Domo indicada en la Figura 2.11 indicada a continuación, es otro caso de cámaras con toma fija, siendo su principal uso en techos,

Figura 2. 11: Cámara Fija Tipo Domo
Fuente: (Mata, 2010)

Mientras que el modelo tipo Cubo, indicado en la Figura 2.12, es la versión más compacta de su tipo, pensada para ser lo más discreta posible, contribuyendo con la estética del lugar.

Figura 2. 12: Cámara Fija Tipo Cubo
Fuente: (Bosch Security, 2019)

Cámaras panorámicas 360 grados. -

Siempre ha existido la necesidad de visualizar “todo alrededor”, como lo es una habitación entera, ello es posible usando una cámara panorámica, también conocida como FishEye (ojo de pez).

Los lentes panorámicos de este tipo de cámaras (Figura 2.13) reciben la luz desde los 360 grados de la escena panorámica que llegan a su vez al sensor de la cámara y los procesa como si fuesen los componentes de una imagen de cámara Domo, los algoritmos matemáticos convierten esa imagen panorámica en una imagen tipo rectangular para poder ser vista en un monitor convencional.

Figura 2. 13: Cámara panorámica FishEye.
Fuente: (Kruegle, 2011)

Cámaras con Movimiento. -

Las cámaras con movimiento, son las que pueden cubrir un amplia área al permitir una mayor flexibilidad en la funciones de movimiento horizontal continuo de 360 grados y un movimiento vertical de 180 grados (Mata, 2010)ya sea por decisión de quien las opera o por medio de rutas de recorrido que les hayan sido pre establecidas.

Las cámaras con movimiento (Figura 2.14) también llamadas PTZ, siglas que abrevian las funciones de movimiento horizontal (Pan) y vertical (Tilt), así como el acercamiento o alejamiento de imagen (Zoom) que realiza este tipo de cámaras.

Figura 2. 14: Cámara con movimiento PTZ
Fuente: (Mata, 2010)

Las instrucciones de movimiento en las cámaras PTZ se envían a través del cable de red a la cámara evitando así cableados adicionales (energía, control de rotor, audio etc…) y tiempos de instalación. En el rastreo en vivo, a menudo a una persona rastrea y examina de cerca un objeto, aunque también pueden realizarse operaciones no tripuladas, en función de los criterios de seguimiento que se configuran en el programa de gestión de la cámara.

La facilidad de mover el área de visión de la cámara PTZ es un punto a considerar en términos de diseño, dado a que, si bien es cierto por su facilidad de movimiento la cámara que enfocar diferentes zonas, puede

enfocar una a la vez, lo cual significa que se deja de captar los eventos que ocurren en las otras áreas. Por lo que se recomienda usar este tipo de cámaras como complemento de cámaras con toma fija, de modo que se garantice la total cobertura del área.

Cámaras multidireccionales con PTZ. -

Las cámaras multidireccionales permiten visualizar varias direcciones al mismo tiempo dado a que cuentan en su parte superior con 4 cabezales de cámara que brindan una cobertura de 360° en cuatro secuencias independientes con sus respectivas configuraciones de ángulo de visión y nivel de zoom de cada cabezal de cámara, proporcionado la flexibilidad de elegir entre las vistas completas y las imágenes con un excelente nivel de detalle.

Como se puede observar en la Fig. 2.15 en este tipo de cámaras los cabezales se complementan con la funcionalidad PTZ que permite realizar un acercamiento a un área de interés sin perder la información de video del área. Las cámaras multidireccionales son adecuadas para áreas amplias, tanto de interior como de exterior. Resultan particularmente idóneas para instalarlas en las esquinas externas de los edificios y en los cruces de vestíbulos y carreteras (AXIS Communications, 2019).

Figura 2. 15: Cámara multidireccional con movimiento PTZ
Fuente: (Axis Communications, 2019)

Parámetros de cámaras de red.

Aunque las cámaras de red IP cuentan con muchos parámetros, se revisarán a continuación algunos destacados al momento de seleccionar una cámara:

Resolución

La gran demanda de resoluciones más altas llevó a proponer muchas técnicas nuevas y mejoras de compresión en la codificación de video. (A. Mazhar, 2016). La resolución es uno de los factores que influyen en la calidad de la imagen, a mayor resolución, mayores detalles pueden identificarse en la imagen, lo cual por otra parte incide en el bajo rendimiento.

La resolución corresponde al número de pixeles en al sensor de imagen medidos vertical y horizontalmente, dichos pixeles están determinados para cada estándar de video, de los cuales se brinda una referencia rápida en la Figura 2.16 indicada a continuación.

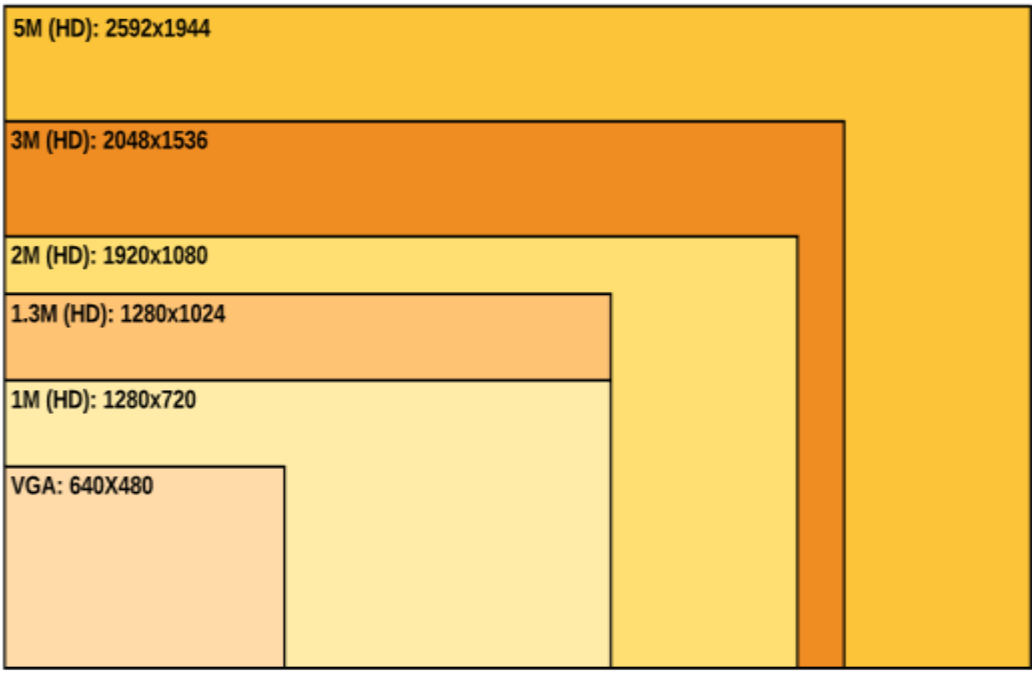


Figura 2. 16: Resolución de pixeles
Elaborado por: Autor

El incremento de resolución es cada vez mayor por lo que actualmente algunos fabricantes ofrecen ya cámaras con arreglos de lentes que permiten llegar de 24 y 32 Mega pixeles de resolución.

Luminancia. -

La luminancia es un parámetro que se utiliza para medir la cantidad de luz que reposa en los objetos, expresada en unidades de Lux. En términos de cámaras IP entre más bajo sea el valor de Lúmenes (Lux), mayor será la sensibilidad del sensor de la cámara.

Cuadros por segundo. -

El número de imágenes que son capturadas en un segundo es lo que se conoce como cuadros por segundo o sus siglas FPS (Frames per second), en castellano se les llama también fotogramas por segundo. El número mayor de cuadros por segundos permitirá hacer más fluido el vídeo, evitándose así el efecto robotizado en las imágenes. En la Figura 2.17 se visualiza una referencia de las imágenes capturadas en tres tasas diferentes durante una misma fracción de segundo.

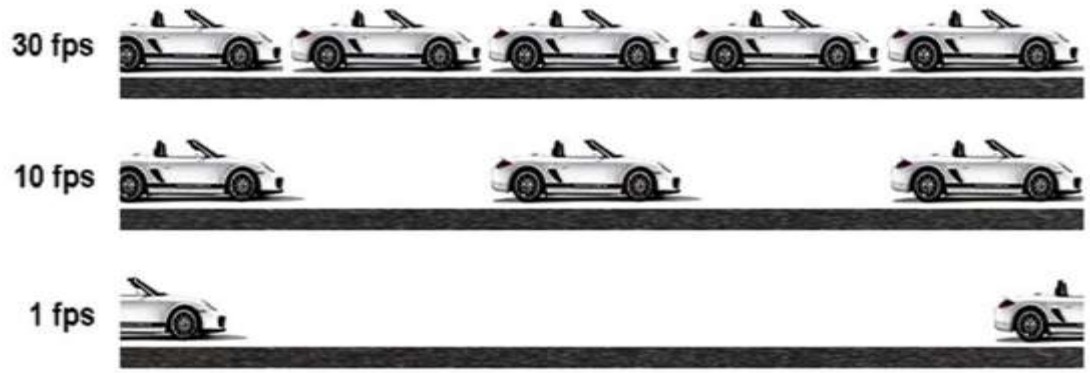


Figura 2. 17: Resolución 15 vs.30 pixeles
Fuente: (Dicsan Technology, 2019)

Existen dos usos de los FPS uno con el que se graba el vídeo y otro a usarse en la reproducción ello para optimizar el recurso de grabación a usar.

Para video vigilancia los cuadros por segundos pueden escogerse desde 1 hasta 30 FPS. Aunque el número de frames por segundo (1 a 30 FPS) pueden ser escogidos a criterio de quien configure los parámetros de la cámara, es importante indicar que entre más alto sea el número de FPS escogido, mayor será el consumo de ancho de banda, por esta razón 15 FPS es un promedio muy usado, para nivelar el consumo de ancho de banda y obtener un buen número de imágenes por segundo.

Compresión. -

Es forma con la que se comprime o reduce el tamaño de un vídeo usando para ello el códec adecuado para el caso requerido. La palabra códec es un acrónimo de codificador y decodificador; es decir, un códec toma la información de video (y audio) provenientes de la cámara IP y los convierte en un flujo de bits (codificación), un archivo digital que puede ser leído por un computador.

En el extremo en el que se recibe el flujo de bits codificado, opera la función del decodificador que lee el flujo, lo interpreta y reproduce de la misma manera en que era originalmente. En términos generales, el códec optimiza la tasa de información a enviar ya que elimina las redundancias de los fotogramas y sólo en el flujo de bits codificado binario las diferencias encontradas en la información. A continuación, en la Tabla 2.5 se listan los códecs más conocidos con su relación de formato y resolución.

Tabla 2. 5: Listado de Códecs

<table>
<tr><th colspan="4">Tipo de formato: *.mov, *.avi, *.mpeg, *.3gp, *.mkv, *.vro, *.divx</th></tr>
<tr><th colspan="4">Contenedor: MOV, AVI, MP4, FLV, MKV, ASF, 3GP, VRO, VOB, SVAF</th></tr>
<tr><th>Codecs de Video</th><th>Resolución:</th><th>Velocidad (fps):</th><th>Velocidad bits (Mbps):</th></tr>
<tr><td>HEVC (H.265)</td><td rowspan="2">4096 x 2160</td><td>4096 x 2160
3840 x 2160</td><td>60</td></tr>
<tr><td>H.264</td><td>60</td><td>80</td></tr>
<tr><td>Motion (JPEG)</td><td>3840 x 2160</td><td>30</td><td>80</td></tr>
<tr><td>MVC</td><td rowspan="8">1920 X 1080</td><td rowspan="6">60</td><td rowspan="8">20</td></tr>
<tr><td>DivX 3.11/4/5/6</td></tr>
<tr><td>MPEG4</td></tr>
<tr><td>Window Media Video v.9</td></tr>
<tr><td>MPEG2</td></tr>
<tr><td>MPEG1</td></tr>
<tr><td>H.263</td><td rowspan="2">30</td></tr>
<tr><td>VP.6</td></tr>
</table>

Elaborado por: Autor

La codificación de video H.262 / MPEG-2 y la codificación avanzada de video (AVC) H.264 / MPEG-4 fueron los pilares conocidos en la evolución de los estándares de codificación de video (Jyothirmai, Mounika, Bhavana, Supriya, & Viharika, 2018).

Al día de hoy, uno de los códecs más usados es el AVC (Codec Avanzado de video, Advanced Video Codec) también conocido como H.264 para el ITU-T o MPEG-4 versión 10, para la ISO/IEC, dado a que es reconocido como un estándar de alta compresión de video, el cual opera muy bien la transmisión de video en alta definición (HD).

Sin embargo, para mayores resoluciones de video como 4K se requiere un mejor formato de codificación, como el HEVC (High Efficiency Video Codec) también conocido como H.265, el cual es un método complejo de compresión de videos en vivo, que permite asimismo visualizar videos en línea, por lo que se postula como uno de los códecs con mayor eficiencia en la compresión de video, dado a que brinda una mejor calidad de vídeo por la técnica avanzada que utiliza para realizar la compresión, a la vez de un menor uso de ancho de banda para la transmisión del vídeo (A. Mazhar, 2016).

2.6. Lectura de placas LPR

El sistema inteligente de lectura de placas o LPR (License plate recognition) reconocimiento óptico de caracteres, se basa en la tecnología OCR (reconocimiento óptico de caracteres) que permite leer y grabar el video asociado a la placa de un vehículo, para compararlo en tiempo real, con una base de datos pre determinada Figura 2.18.

Figura 2. 18: Lectura de placa vehicular
Fuente:: (Wen et al., 2011)

La tecnología de reconocimiento de matrículas (LPR) ha sido extremadamente efectiva, tanto usando información histórica como en tiempo real, además porque los datos recopilados con esta tecnología no incluyen información de identificación personal y, por lo tanto, por definición son considerados datos anónimos. Existen dos maneras de realizar esta función: ejecutada directamente en la cámara y/o activación de la función LPR vía software de gestión de cámaras.

La primera opción generalmente permite una sencilla configuración e instalación (dado a que son cámaras preparadas especialmente para esta función); sin embargo, involucra costos considerablemente más altos. La activación de este servicio vía software, contribuye con el presupuesto dado a que sus costos son radicalmente menores, empero implica una mayor complejidad en su instalación y configuración.

Siendo que la orientación del presente trabajo es la recomendación de una plataforma de gestión de cámaras, se realiza el enfoque a la segunda opción a implementar, por lo que en la imagen a continuación se grafica en la Figura 2.19 el diagrama de operación de un sistema de lectura de placas activado vía software.

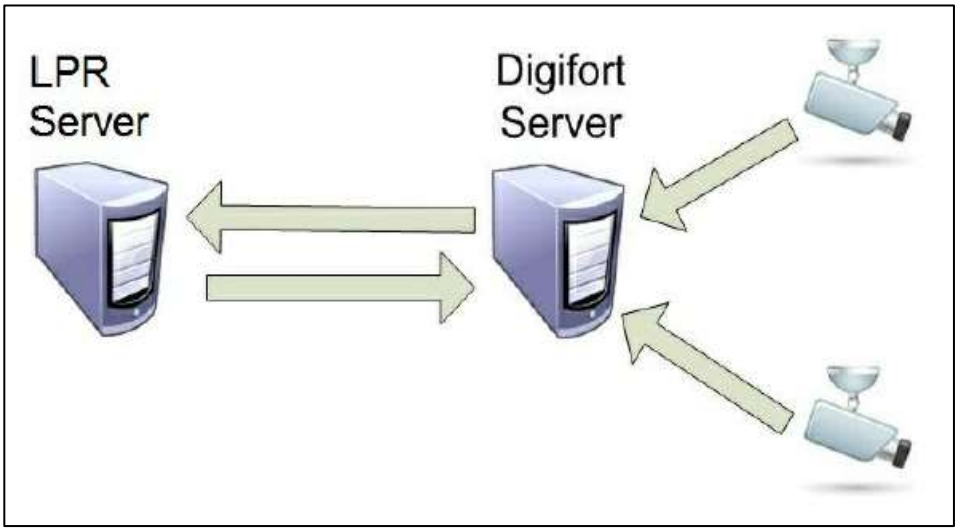


Figura 2. 19: Diagrama de conexión servicio LPR
Fuente:: (Digifort, 2018)

Las cámaras IP deben contar con suficiente resolución y calidad de imagen a fin de que el servidor LPR pueda realizar el reconocimiento óptico

de caracteres (OCR), almacenar la información en una base de datos y obtener los resultados del reconocimiento de matrículas. Indistintamente del fabricante, una cámara IP convencional puede ser parte del sistema LPR, si cumple con las siguientes características técnicas.

Resolución de imagen

El uso de cámaras IP 4K es altamente recomendado; sin embargo, modelos con Full HD; es decir, con resolución de imagen superiores a 2MP (Mega Pixel) ó 1080p son válidas para esta función.

Lente varifocal

Es necesario el uso de lentes vari focales para ajuste correcto de la apertura, el zoom y el ángulo de la imagen, con corrección de infrarrojos y una distancia focal de 5 a 50 mm.

Velocidad de obturación

Con el control de velocidad del obturador (también conocido como shutter), es posible "congelar" imágenes que están en movimiento, característica muy útil para los vehículos en movimiento y poder así realizar la correcta lectura de caracteres.

Compensación de Luz

Siendo que el sistema requiere visualizar la información de la placa vehicular se requiere proporcionar al sistema esta información de forma clara; sin embargo, en ambientes externos esto es un desafío debido a los constantes cambios de luz natural, así como la integración de luz artificiales como son los faros de luz pública y de los vehículos en sí. Por lo que las cámaras IP a considerar para operar en el sistema LPR deben contar con funciones de compensación de luz como lo son:

- **HLC** (compensación de saturación de luz) orientada específicamente a detectar luces intensas en el video (como las producidas por faros de los vehículos) y reducir la exposición en estos puntos para mejorar la calidad de las imágenes.

- **WDR - True WDR** (Wide Dynamic Range o Rango Dinámico Amplio) equilibra la luz de la parte posterior de una imagen a través del procesador de señal digital (DSP) y los sensores con los que cuenta (CCD y COMS).

Existen dos tipos de tecnologías de amplio rango dinámico (WDR) utilizadas en cámaras IP: Digital WDR y True WDR.

Las cámaras de vigilancia con la función WDR utilizan algoritmos de software para iluminar las áreas oscuras y atenuar las áreas excesivamente iluminadas en las imágenes, mientras que el WDR verdadero (True WDR) implementan sensores sensibles a la luz (CCD / CMOS) y tecnología DSP para equilibrar la iluminación.

- **BLC** (Compensación de Luz de Fondo o Back Light Compensation)

Su función es la de iluminar toda la escena en un cuadro de video o imagen en lugar de equilibrar las luces en áreas sobreexpuestas y subexpuestas como lo hace WDR, que, en algunos casos, elimina algunas áreas demasiado iluminadas en una imagen o video.

En la Figura 2.20 se pude observar la calidad de imagen de una toma normal y con usos de los parámetros BLC y WDR

Figura 2. 20: Uso de parámetros BLC Y WDR
Fuente:: (Montavue, 2017)

Con la observación de soporte de estas especificaciones técnicas en las cámaras IP a utilizar, es posible mejorar la calidad de la imagen a analizar para efectos de realizar la función de lectura de placas.

2.5.1. Reconocimiento Facial

El reconocimiento automático de caras humanas es uno de los problemas que ha supuesto (y sigue siendo) un desafío en informática. Los seres humanos estamos muy acostumbrados a reconocernos entre nosotros usando rasgos faciales. Además, las medidas faciales han sido usadas en medicina legal y forense durante muchos años para identificar individuos, y por lo tanto han dado origen a una gran cantidad de estudios (Cabello Pardos, 2004).

Desde 1960 se registra el esfuerzo de investigadores y científicos por crear sistemas basados en computadora que puedan homologar la función neuronal humana de reconocimiento facial usando imágenes digitales o un cuadro de video (frame) como fuente de análisis.

El reconocimiento facial es uno de los parámetros biométricos de identificación cada vez más utilizado como identificador digital. A continuación, en la Figura 2.21 se indica una referencia de los parámetros que componen el identificador biométrico ideal, el cual combina los diferentes parámetros de un individuo, se espera en un futuro próximo actúe de forma paralela y en tiempo real al momento de identificar a un individuo.

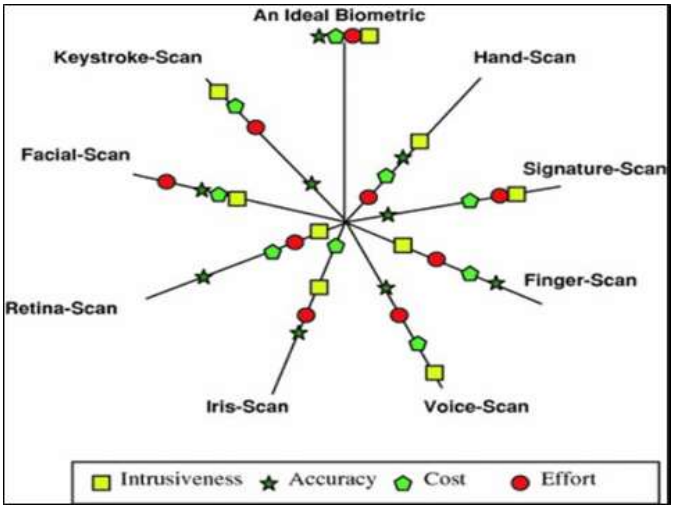


Figura 2. 21: Parámetros Identificador ideal
Fuente: (Lu, 2015)

Siendo que la identificación facial de personas ha tomado gran importancia por la agilidad que otorga a diferentes procesos, optimización del

acceso bancario o por su contribución en la demanda de seguridad, esta tecnología ha experimentado un vertiginoso desarrollo, apoyada por la disponibilidad de cámaras digitales y el cada vez más accesible desarrollo de computadoras con notable procesamiento de información.

En pocas décadas se han desarrollado diferentes algoritmos con los que el computador obtiene la mejor referencia de las características de una imagen facial para su evaluación.

Este procedimiento se basa principalmente en las características únicas de cada rostro; es decir, las medidas de distribución (distancia y profundidad) particular y única de los elementos de su rostro (ojos, nariz, mentón, etc…) según se observa en la Figura 2.22.

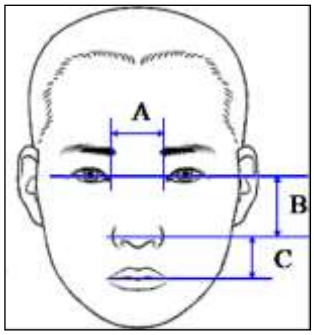


Figura 2. 22: Valor de posición estructural de puntos faciales
Fuente: (Yoon, Park, Oh, Cho, & Jang, 2019)

Hoy en día más de 130 medidas del rostro son tomadas y convertidas en texto simple que la computadora analiza en microsegundos (Figura 2.23).

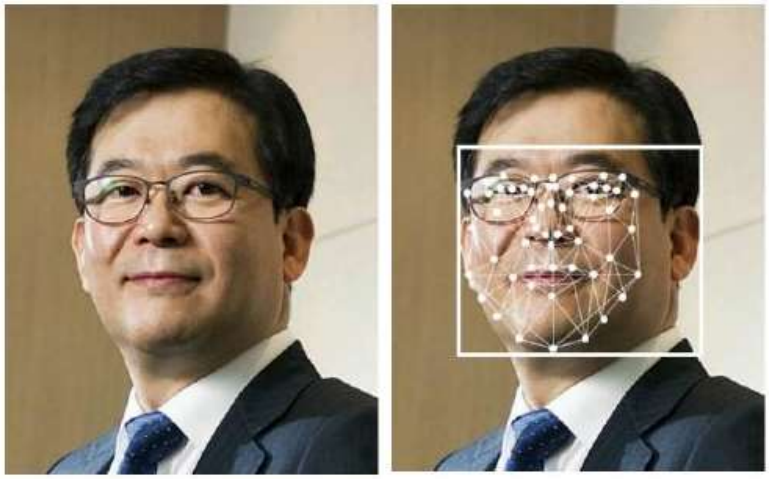


Figura 2. 23: Precisión de medidas de rostro
Fuente: (Yoon et al., 2019)

Los diferentes algoritmos que han sido creados para el análisis de la información, se clasifican según su enfoque en esquemas basados en: apariencia y modelos. Por otra parte, el reconocimiento facial puede efectuarse en cualquiera de las dos áreas que lo componen: la detección o verificación y el reconocimiento o identificación facial.

Detección/Verificación facial. –

Corresponde a la comparativa uno a uno que realiza el sistema contra una base de información previamente provista, como pueden ser rostros (fotografías) para validar que una persona es quien dice ser.

Reconocimiento o Identificación facial. –

El objetivo es, como su nombre lo dice, identificar a quién corresponden las características del rostro que ingresa al sistema, por lo que es un proceso comparativo de uno a muchos datos, que suelen estar en una base de datos.

Las características del rostro son comparadas en la base de datos del sistema, el cual provee los resultados similares renqueados con su calificación de probabilidad en orden descendente. El porcentaje más alto de similitud es identificado como “Top Score” para verificación del operador.

Un gran desafío que tienen los sistemas de reconocimiento facial está relacionado a las variaciones en la imagen de un mismo sujeto como lo son:

- Posicionamiento de cabeza 3D
- Iluminación (interiores y exteriores)
- Expresión facial
- Uso de accesorios Ejemplo: sombreros o gafas de sol
- Edad
- Vello facial

La detección de rostros tiene muchas dificultades debido a que la información a analizarse puede variar, como se observa en la Figura 2.24, según el tamaño de la cara, la rotación izquierda y derecha, así como si tiene

rotación hacia arriba o hacia abajo, si se cuenta con una cara lateral y cara frontal, si la imagen muestra expresión facial y asimismo influye el estado de la luz.

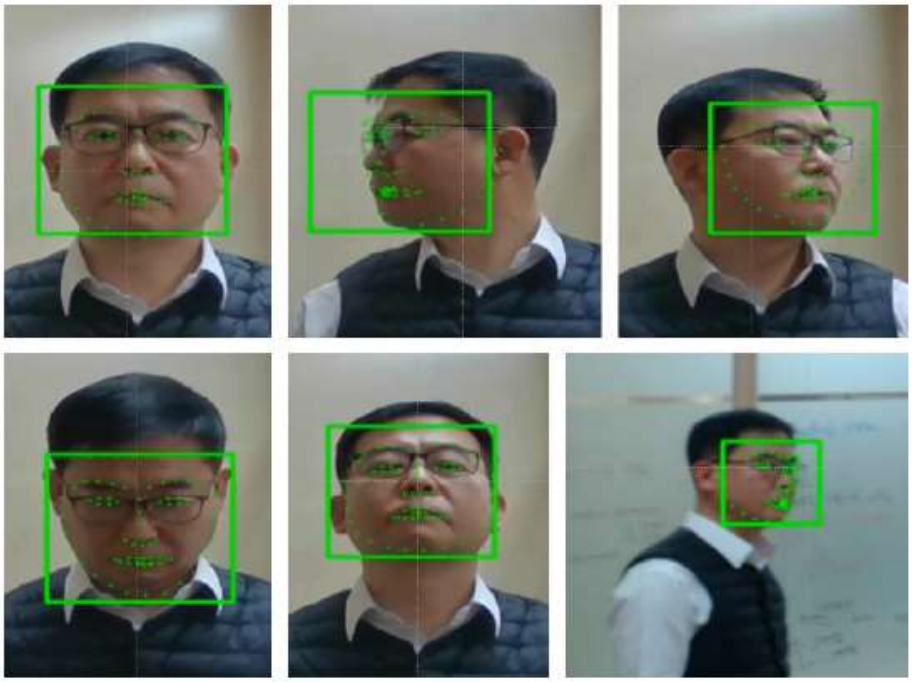


Figura 2. 24: Variación de imagen de un mismo sujeto
Fuente: (Yoon et al., 2019)

En base a ello, se extraen los rasgos faciales y los rasgos extraídos se reconstruyen geométricamente para mejorar la tasa de reconocimiento facial en la región facial extraída.

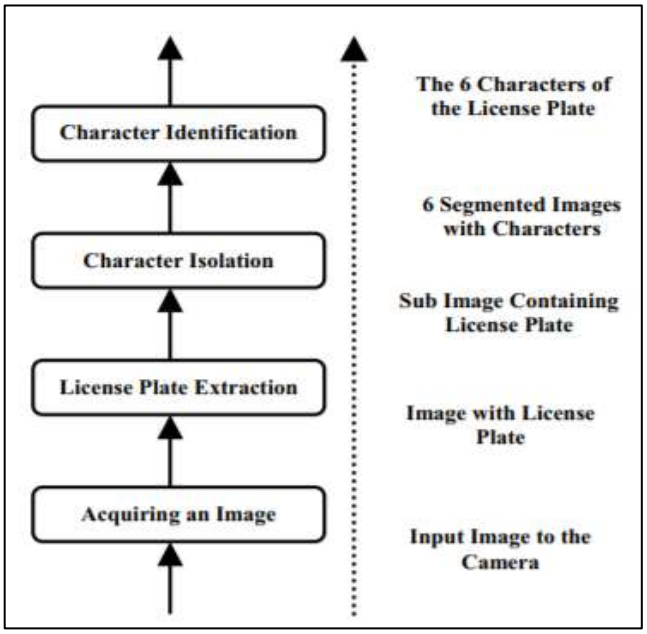


Figura 2. 25: Proceso de reconocimiento facial
Fuente: (Sarfraz & Jameel, 2005)

El sistema entonces ajusta el ángulo de la cara utilizando el vector de rasgos faciales reconstruido y mejora la tasa de reconocimiento para cada ángulo de la cara. En el intento de reconocimiento que usa el resultado después de la reconstrucción geométrica, tanto el ángulo facial arriba como abajo y el ángulo izquierdo y derecho han mejorado el rendimiento del reconocimiento. Brevemente se bosqueja a continuación en la Figura 2.25, el proceso estándar del reconocimiento facial:

Aprendizaje Profundo. -

El aprendizaje profundo (Deep Learning) corresponde a una sub-rama de aprendizaje automático la cual identifica rostros humanos en imágenes digitales, para lo cual el sistema emplea una red neuronal artificial de nueve capas con más de ciento veinte millones de interconexiones entre ellas.

Ello permite al sistema no sólo manejar una alta densidad de imágenes, sino procesarlas por medio de este sistema de neuronas que tienen enlaces entre sí, como el graficado en la Figura 2.26, el resultado de una neurona tiene un peso, que es resultado del valor de la salida de la misma multiplicado por un valor de peso, este valor resultante activa las neuronas adyacentes realizando análisis más detallados, en menor cantidad de tiempo y con muy alta precisión.

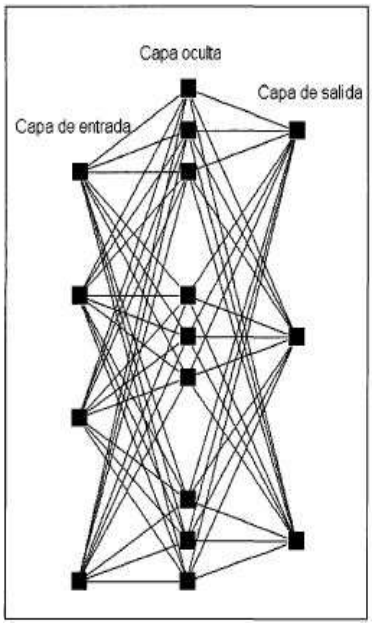


Figura 2. 26: Red neuronal
Fuente: (Cabello Pardos, 2004)

El sistema de reconocimiento facial con aprendizaje profundo (Deep Learning), permite realizar el reconocimiento de identidad y expresión en humanos, y sus aspectos de desarrollo y neurofisiológicos (Bülthoff, Cunningham, & Wallraven, 2011), permitiendo manejar más información de una imagen por lo que en este tipo de tecnología se puede obtener una cierta cantidad de información sobre la profundidad de la cara analizando el patrón de reflexión de acuerdo con el brillo y la relación de contraste de la fotografía.

Cuando se adquiere la información de profundidad de la cara, como se indica en la Figura 2.27, se convierte en datos básicos para hacer una forma de cara 3D. La forma de la cara 3D obtenida oscurece la forma de la cara de la nube de puntos. Además, es posible compensar poses libremente, lo que puede compensar las desventajas del reconocimiento facial 2D. Dado que la cara 3D generada es una cara imperfecta, la forma de la cara se reconstruye realizando la compensación de pose mediante el paso de pre procesamiento.

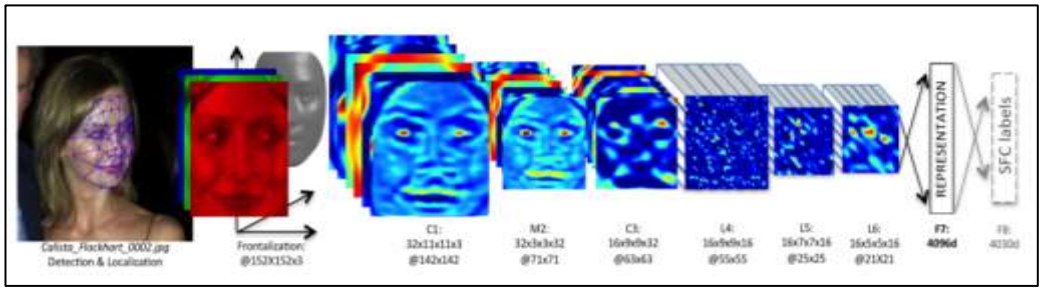


Figura 2. 27: Esquema de la arquitectura DeepFace
Fuente: (Taigman, Yang, Ranzato, & Wolf, 2014)

Para realizar el reconocimiento facial, es necesario normalizar las coordenadas de la forma del rostro generado por medio del punto de base. Las caras 2D difieren en tamaño y posición de las características faciales adquiridas de acuerdo con los factores ambientales en el momento del disparo y las características faciales personales. Por lo tanto, es difícil extraer ciertos datos de características faciales si no se realiza el proceso de normalización y una compensación de pose se realiza al frente para extraer datos precisos de las características. Hoy en día es posible encontrar sistemas con índices de precisión del 99% que identifica un individuo entre millones de personas, en tan sólo segundos, permitiendo distinguir el género, grupo étnico, edad y tono de piel, por lo que se considera a este método como casi perfecto.

CAPÍTULO 3: SIMULACION Y RESULTADOS OBTENIDOS

3.1. Introducción

En el presente apartado se detallan las necesidades de la solución requerida, el seleccionamiento de la plataforma a usar, se describen las consideraciones de diseño, así como se establecen los resultados obtenidos de las pruebas realizadas con la plataforma propuesta.

3.2. Requerimientos de servicios

Los siguientes servicios fueron identificados como puntos de interés prioritario de evaluación por parte de la institución de seguridad ciudadana, para activación en las cámaras pre-existentes, los cuales se indican a continuación:

- Soporte de gestión de marcas y modelos de cámaras pre-existentes.
- Activación del sistema lectura de placas multinacional.
- Levantar la funcionalidad de reconocimiento facial.
- Activación de la funcionalidad de Analítica de video.

3.3. Selección de la plataforma a usar

Se procedió a evaluar el soporte de los requerimientos arriba indicados en diferentes y reconocidas plataformas VMS del mercado que cumplen con la operación cliente-servidor descrita en el capítulo previo y con el soporte de las funciones arriba descritas, en base a lo cual la plataforma DIGIFORT fue seleccionada por el cumplimiento de lo antes indicado, más las características distintivas orientadas a la gestión de un Centro de Seguridad Ciudadana, que se detallan a continuación:

3.3.1. Independencia

Se considera la mejor administración y gestión video IP a los sistemas VMS que son independientes del hardware (servidores, equipos de almacenamiento, etc..) dado a que dan libertad al usuario de seleccionar el

mejor elemento disponible en su clase. Digifort hace eco de este punto en su sistema, favoreciendo no solamente la apertura de seleccionar la última tecnología del momento con el fabricante de hardware de preferencia del usuario, sino también a la optimización de costos y tiempos de entrega en el desarrollo de un proyecto.

3.3.2. Avances tecnológicos

Por medio de alianzas estratégicas, Digifort ha incorporado a sus soluciones y trasladado el servicio de sus usuarios los beneficios de los avances y nuevas tecnologías de los mejores “players” del momento, Briefcam para Video Analítica y Forence.

El módulo de reconocimiento facial Digifort es una asociación mundial entre Digifort y la empresa estadounidense RealNetworks, con el módulo SAFR (TM) Este módulo permite el reconocimiento facial con excelente precisión y alta confiabilidad (actualmente medido y certificado por el NIT de la Universidad de Massachusetts) con una calificación de 98.86% (Digifort, 2018).

3.3.3. Costos.

Un tema de consideración es la inversión que todo sistema de seguridad requiere, por lo que en este sentido el licenciamiento para operación de cámaras en esta plataforma es vitalicio, de forma que libera el presupuesto del usuario de renovaciones de licencias anuales, sin perder las actualizaciones del sistema que se encuentran incluídas.

3.3.4. Plataforma abierta.

Dado a que Digifort es una plataforma abierta, brinda la libertad de elección dentro un amplio espectro fabricantes, marcas y equipos: de más de 6000 dispositivos y 247 fabricantes diferentes de cámaras IP, NVRs, Control de Accesos, Sistema de Incendios forestales, Point of Sales (Puntos de venta), Protección Perimetral, Sistema PSIM, Integración RFID, etc…) ya homologados con la plataforma. Adicionalmente permite integrar otros equipos de interés de un proyecto.

3.3.5. Mapa.

Admite la creación de mapas de varios niveles, así como la inclusión de mapas de Google para situar la cámara en la zona geográfica donde se encuentra instalada, como se observa en la Figura 3.1. Con un doble click es posible visualizar la imagen en tiempo real de dicha cámara.

Figura 3.1:Herramienta Insight
Fuente: (Digifort, 2018)

3.3.6. Matriz virtual.

Con la opción Matriz virtual, Digifort Surveillance Client puede conectarse a cualquier monitor de cualquier computadora en la red que tenga el cliente de vigilancia en funcionamiento, Figura 3.2. De esta manera, es posible enviar objetos entre los clientes, como cámaras, mapas y estilos de pantalla.

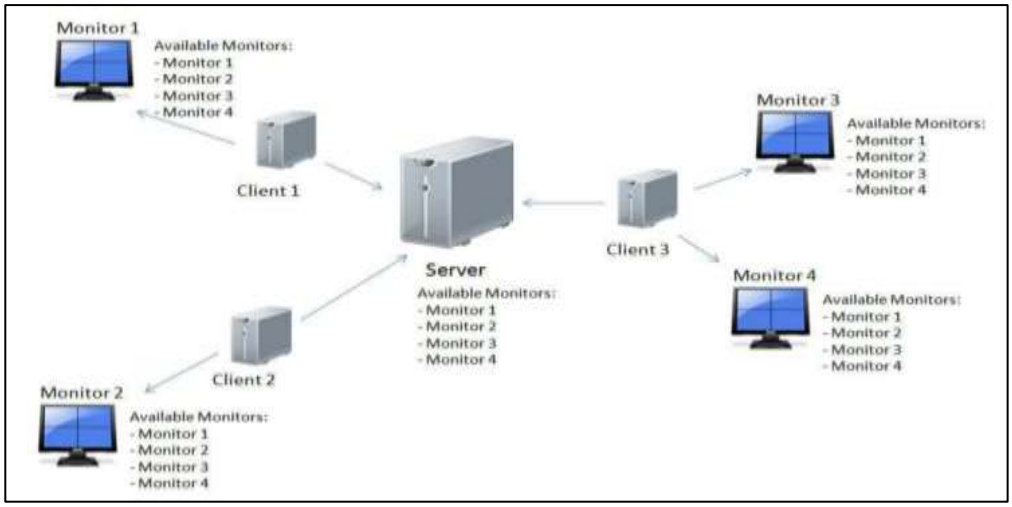


Figura 3.2:Herramienta Insight
Fuente:: (Digifort, 2018)

3.3.7. Sincronización rápida de Intel.

Soporta la decodificación de video (H.264 y H.265) usando Quick Sync a través de la tarjeta de video con procesador Intel.

3.3.8. Insight de Digifort. –

Esta es una herramienta de software versátil y gratuita proporcionada por Digifort que se observa en la Figura 3.3, que permite capturar y gestionar el software de terceros que se ejecutan en un PC local o remoto, permitiendo hacer integraciones con cualquier sistema sin requerir la interacción de un SDK o API.

Figura 3.3:Herramienta Insight
Fuente:: (Digifort, 2018)

3.3.9. Failover.

La protección contra fallas está contenida en esta plataforma, de forma que protege datos críticos, dado a que proporciona acceso continuo y puede tolerar las fallas que pudiera presentar el hardware sin interrupción del sistema, logrando así una conectividad ininterrumpida y garantizando el máximo tiempo de actividad, como se grafica en la Figura 3.4

La activación de esta opción reactivará en el servidor de respaldo el comportamiento anterior del sistema, en caso de falla de comunicación con el servidor original (generalmente debido a una falla de hardware), el sistema elimina los objetos de este servidor del cliente para que pueda cargar los objetos correlacionados del servidor de conmutación por error, asegurando un buen funcionamiento transición al nuevo servidor en caso de falla del sistema.

La plataforma Digifort extiende la cobertura de esta función a los servicios de LPR, VCA y dispositivos de E/S (Entrada y Salidas)

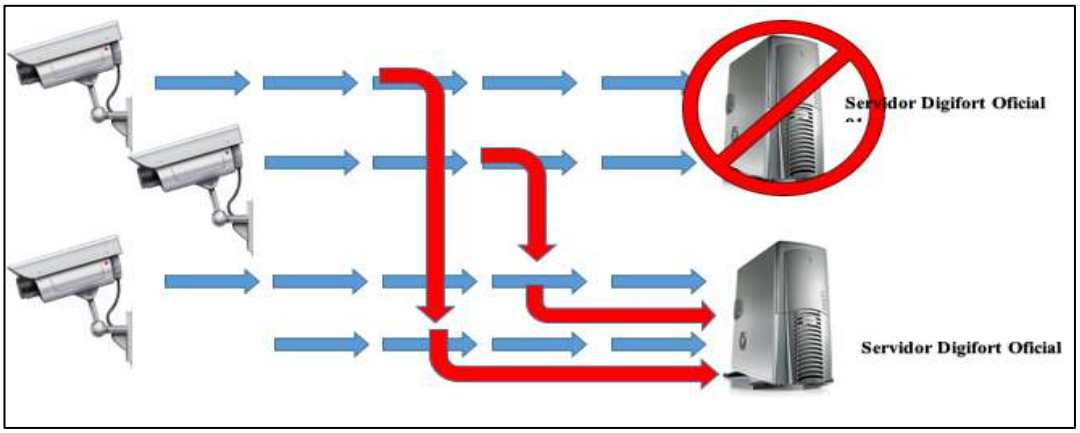


Figura 3.4:Diagrama operación Failover
Elaborado por: Autor

3.3.10. Digifort Mobile.

Digifort Mobile es un software desarrollado en la plataforma Java para dispositivos móviles como Smartphones, PDA, etc. Lo cual hace posible la visualización de cámaras IP y codificadores de video (Figura 3.5) así como activar eventos, desde dispositivos móviles, de forma que permite a los directores de monitoreo mantenerse al tanto de lo que ocurre si requieren cambiar su ubicación física.

Figura 3.5:Digifort Mobile
Fuente:: (Digifort, 2018)

3.3.11. Grabación de borde.

Las grabaciones de borde efectuadas directamente en la memoria de las cámaras son viables de realizar en esta plataforma, por lo que es posible grabar en la tarjeta SD de la cámara a fin de que cuando haya una desconexión de red, se pueda recuperar la información de la misma, esta función permite que una vez se restablezca el enlace, el video de esta cámara será transferido al servidor central. La reproducción Edge puede efectuarse directamente tanto desde dispositivos como cámaras con tarjeta SD o DVR/NVRs para dispositivos compatibles,

3.3.12. Mobile Camera. –

El sistema permite la grabación y visualización en vivo de imágenes desde cámaras de dispositivos móviles inteligentes (Android o iOS), donde no hay cámaras de seguridad. Como se observa en la Figura 3.6 los elementos de seguridad como lo son policías, Inspectores de carga, Patrulla / Guardias de seguridad, etc…pueden recibir la activación en sus teléfonos inteligentes de esta función e inmediatamente integrar a la plataforma central la información de las cámaras de dichos agentes.

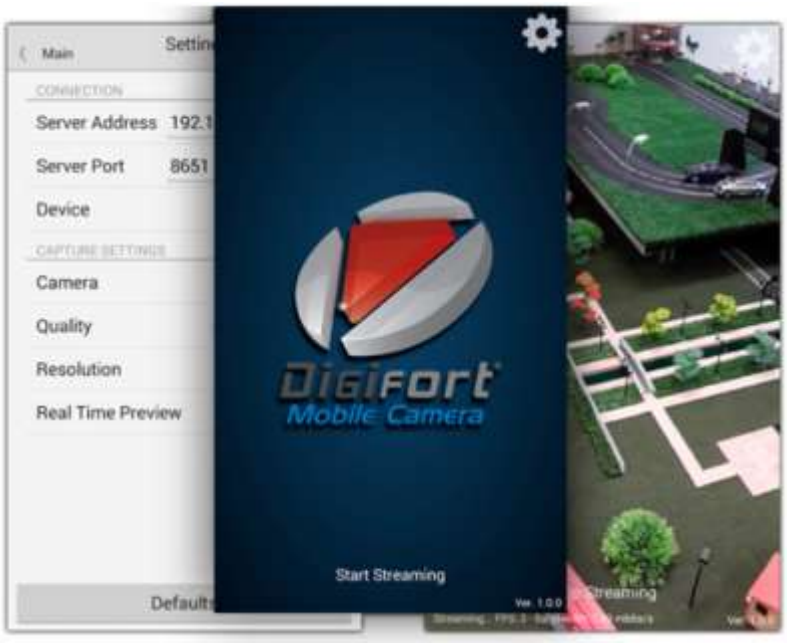


Figura 3.6: Mobile Camera
Fuente:: (Digifort, 2018)

Vale indicar que servicios como lectura de placas (LPR) y reconocimiento facial son viables de asignar a estas cámaras y de esta

manera extender la cobertura de seguridad a áreas donde no existan cámaras IP convencionales de la institución, como podrían ser accidentes, revueltas, coberturas de eventos masivos, etc…

3.3.13. Cyber Security.

La seguridad cibernética, disponible desde la versión más sencilla de la plataforma, a diferencia de algunos VMS que usan tecnología de cifrado obsoleta (DES-56), en el caso de Digifort, se encuentran disponibles mayores niveles de seguridad como Túnel inverso, cifrado TLS 1.2 y enmascaramiento dinámico, utilizando diferentes capas de autenticación y protecciones, la plataforma requiere un número limitado de puertos para abrir, lo cual limita aún más el riesgo de ataques cibernéticos.

A nivel de uso interno, la plataforma brinda esquemas de contraseña segura para los operadores (con tiempos de inicio, creación de horarios y filtros específicos por usuario etc..), detección de la dirección IP determinada a fin de que no se pueda accesar desde ninguna computadora, así como bloqueo de usuario si la contraseña es incorrecta luego de un determinado número de intentos.

También permite la deshabilitación de protocolos y servicios no utilizados (por ejemplo, servidor RTSP, HTTP). Uso de VLANs y acceso a encriptación.

3.3.14. Evidence. -

La amplia disponibilidad de herramientas para el procesamiento de señales multimedia ha llevado a la preocupación que las imágenes y los videos no puedan considerarse una evidencia confiable, por la facilidad con la que pueden modificarse (Milani et al., 2012)

Esta posibilidad plantea la necesidad de verificar si un contenido multimedia es original o no en base a que las alteraciones no son reversibles y dejan en la señal reconstruida algunas "huellas", que pueden analizarse para

identificar los pasos de procesamiento (Simão, Firmino, Simão, & Firmino, 2019).

En virtud de ello, la plataforma dispone de la función “Evidence” la cual abre un registro cuando ocurre un evento identificado en la grabación como robo, robo, incendio, vandalismo, etc… e integra información de fecha, hora, evento, operador, cámara relacionada y un código de barras, como se observa en la Figura 3.7 que permite validar la legitimidad del video generado a fin de que pueda establecer la veracidad de la evidencia entregada (Digifort, 2009).

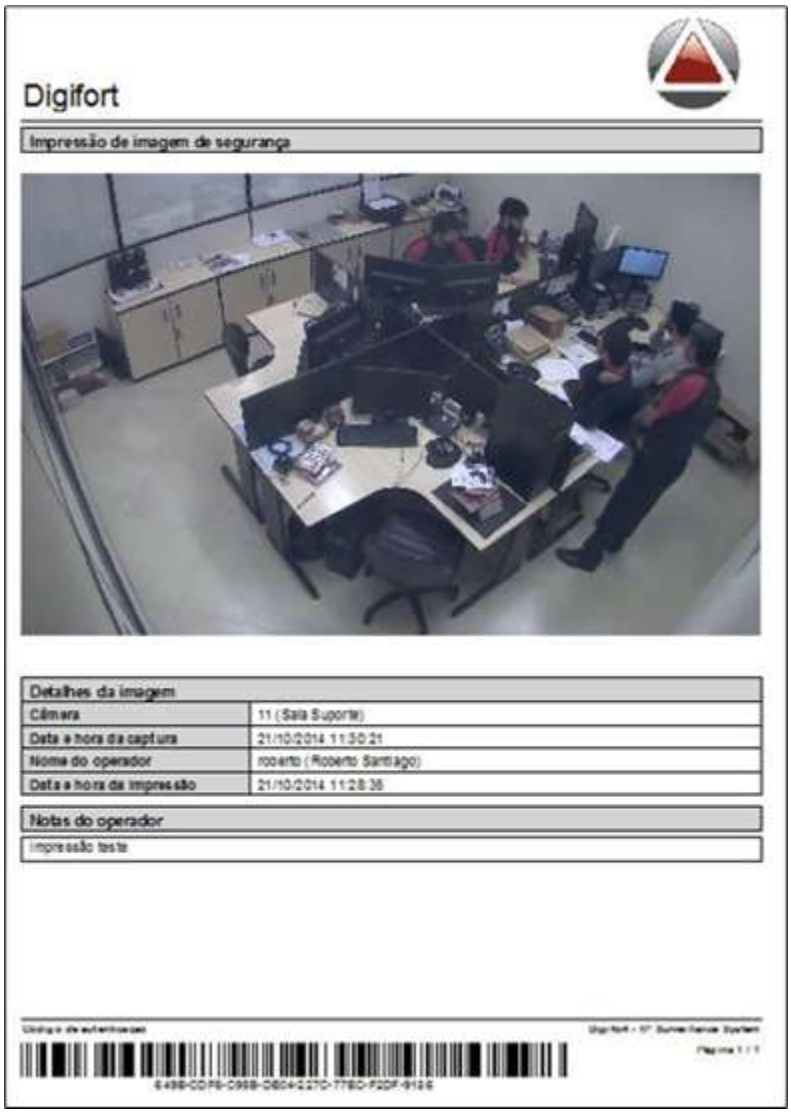


Figura 3.7:Reporte Evidence
Fuente:: (Digifort, 2002)

Al realizarse en la plataforma la identificación diaria de los diferentes eventos ocurridos (robos, incendios, vandalismo, etc…), la función Evidence

permite asimismo realizar búsquedas específicas de dichos eventos de forma de realizar estadísticas, organización y gestión de eventos rápidamente.

3.4. Video Managment System – VMS.

Para la activación de este y los demás requerimientos de servicio fue requerido por el fabricante la toma de una certificación especializada, de una semana intensiva en sus instalaciones (Sao Paulo-Brasil), debido a los procedimientos necesarios por cada servicio a levantar, por lo que en el presente trabajo no se detallan dichos procedimientos; sin embargo, se comparten las consideraciones de diseño y resultados obtenidos.

La primera tarea que se realizó en esta fase fue la integración de las cámaras de video vigilancia con las que cuenta el ECU-911, de diferentes tipos (fijas y PTZ), marcas y modelos, lo cual es posible levantando la plataforma base (Video Managment System, VMS) y realizando el proceso de activación de cámaras descrito por el fabricante.

Para efectos de las pruebas a realizar se integran seis (06) cámaras de las marcas Tiandy y Huawei y Hikvision.

3.4.1. VMS Consideraciones de diseño

A continuación, se indica en la Figura 3.8 la arquitectura de la plataforma Digifort

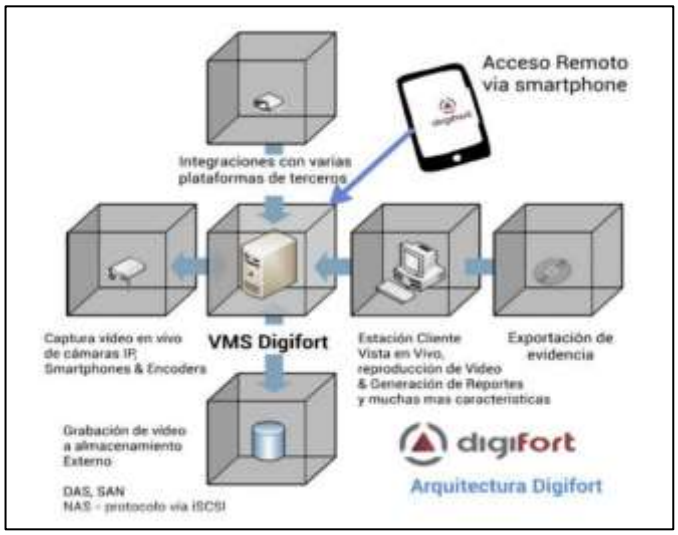


Figura 3.8:Diagrama arquitectura Digifort
Fuente:: (Digifort, 2002)

Para efectos de determinar el hardware a requerirse la plataforma Digifort dispone de una herramienta (Figura 3.9) disponible en su página web, que permite dimensionar las características del hardware a requerirse. Esta herramienta de fácil uso, brinda casilleros para ingreso de los principales parámetros de la solución a implementar, por lo que deben establecerse el número de cámaras, resolución a usar, compresión, tiempo de grabación, FPS, así como el tipo de video a monitorear, etc…en base a lo cual entrega la sugerencia de hardware a usar.

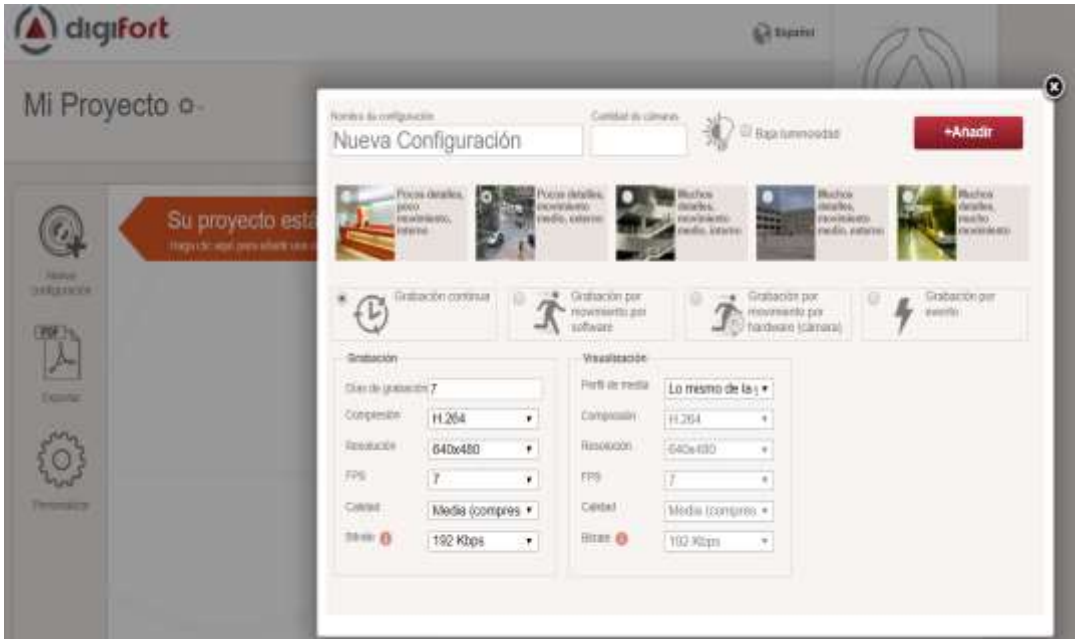


Figura 3.9: Herramienta de cálculo Digifort
Fuente:: (Digifort, 2019)

Debido a que son seis unidades de cámaras a usar para efectos de la demostración a realizar, para las cuales se requiere activar los siguientes servicios:

01 Plataforma base VMS
06 Licencias de cámaras IP
01 Licenciamiento de lectura de placas vehiculares LPR
01 Licencia para reconocimiento facial
01 Analítica vídeo Synopsis

En base a lo cual, usando la herramienta provista por el fabricante, obtenemos las características de hardware sugerido que se detalla a

continuación en la Figura 3.10, en la cual se considera un sólo servidor para gestionar las funciones de VMS, Lectura de Placas, Synopsis y Analítica. Dejando la activación de reconocimiento facial para una unidad de servidor adicional.

Digifort VMS + Modulo Analítico + Modulo LPR + Modulo Sinopsis

1x Processor Intel Core i7-7700 4.2 GHz
Memoria de 16 GB DDR4-3200 Memory
Disco duro secundario 10 TB (7200RPM Internal Hard Drive)
1x Tarjetas de Red 1GB

Digifort Modulo Reconocimiento facial

1x Processor Intel Core i7-7700 4.2 GHz
Memoria de 16 GB DDR4-3200 Memory
Disco duro secundario 3 TB (7200RPM Internal Hard Drive)
1x Video Card --> EVGA - GeForce GTX 1080 Ti 11GB Founder Edition Video Card **(2-Way SLI)**
1x Tarjetas de Red 1GB

Figura 3.10: Resultado cálculo de hardware
Elaborado por: Autor

3.4.2. VMS Activación de plataforma

Se realiza la instalación de la plataforma en su versión Enterprise, en su versión 7.2 con la activación de las seis cámaras requeridas, como se muestra en la Figura 3.11.

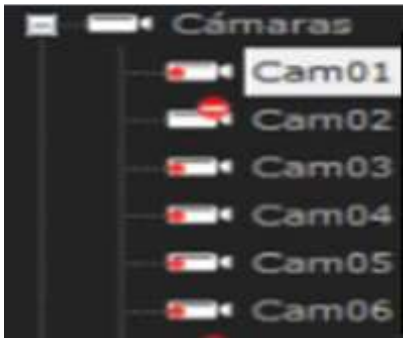


Figura 3.11: Activación de cámaras
Elaborado por: Autor

En la Figura 3.12 se visualiza la interfaz de activación de cámaras junto con el video obtenido de una las cámaras en el centro de la imagen. A mano izquierda de la imagen se encuentran los controles de parámetros de grabación de la cámara.

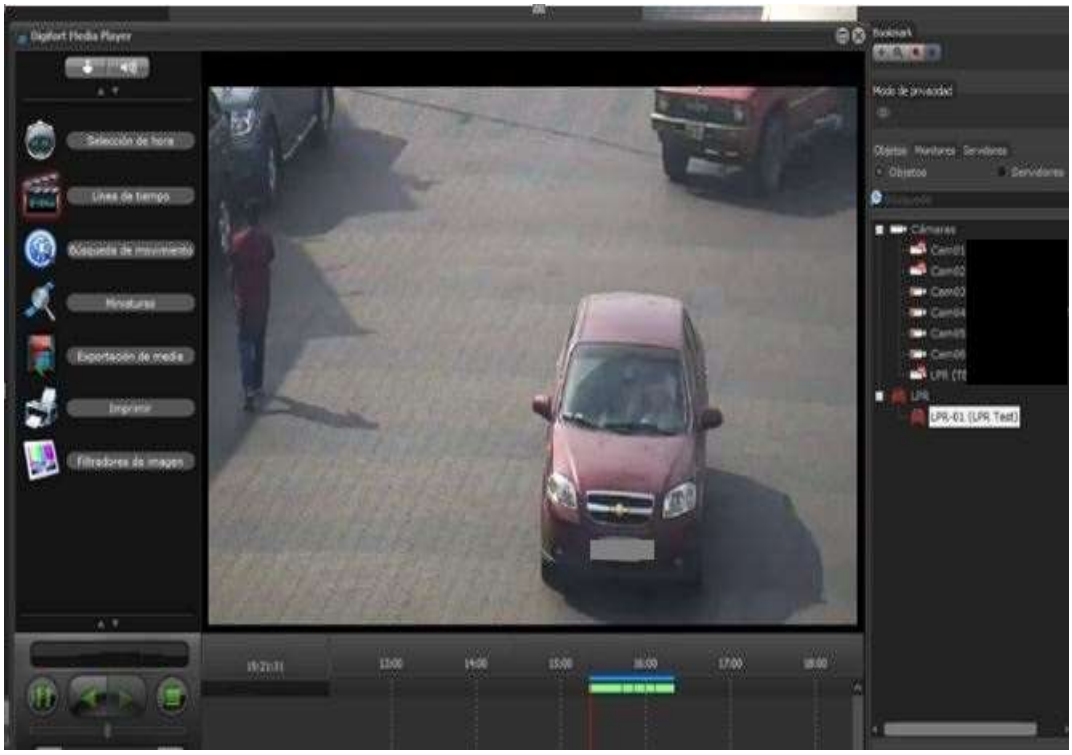


Figura 3.12: Interfaz configuración cámaras
Elaborado por: Autor

3.5. LPR - Consideraciones de diseño.

Como se ha indicado anteriormente la integración de sistemas de lectura de placas LPR aumenta la seguridad vehicular de las ciudades inteligentes ofreciendo la posibilidad de forma preventiva detectando anomalías en el desempeño del tránsito (exceso de velocidades) disminuyendo la tasa de accidentes, o de forma reactiva identificando placas de vehículos sospechosos en tiempo real colaborando así con un mejor desenvolvimiento de la fuerza de seguridad a nivel nacional.

Para efectos de realizar un correcto dimensionamiento de la solución de lectura de placas vehiculares, existen algunas consideraciones de diseño, que deben tenerse presente para su debida captura y correcta identificación que brinda este servicio, consideraciones que deben ser tenerse presente al momento de realizar el diseño, las mismas que se indican a continuación:

3.5.1. Mínimo de resolución. –

Para el caso de la plataforma Digifort el tamaño del carácter de la cámara que realiza la función de LPR debe ser de 16 pixeles de alto, pero la resolución podría ser incluso de 320x240 con 3FPS siempre y cuando la imagen que se obtenga tenga resolución espacial, brillo, contraste y condiciones de luz, junto con un correcto ángulo de vista.

3.5.2. El ángulo visualización. –

El objetivo principal es facilitar a la cámara que va a cumplir la función LPR de una vista completa del vehículo y de la placa que contiene el registro del vehículo.

3.5.3. Ubicación de cámara: Frontal al vehículo

Las mejores prácticas indican a la posición de vehicula de la siguiente imagen, Figura 3.13, como el ángulo ideal para el funcionamiento de LPR con el vehículo en forma perpendicular al suelo y de frente a la cámara.

Figura 3.13: Ubicación frontal de cámara
Elaborado por: Autor

3.5.4. Ubicación de cámara superior al vehículo

Aunque la ubicación anterior es considerada la más ideal para efectos de captura de placas de vehículos, en la realidad suele requerirse la cámara en ubicaciones diferentes, por lo que es posible la activación del servicio de lectura de placas cuando la cámara está situada en una posición por encima del vehículo (Figura 3.14), en ese caso la recomendación que debe considerarse es la ubicación de la cámara un ángulo máximo de 40 grados

desde el eje horizontal de la altura del objeto de nuestro interés, para garantizar que el servicio LPR opere sin inconvenientes.

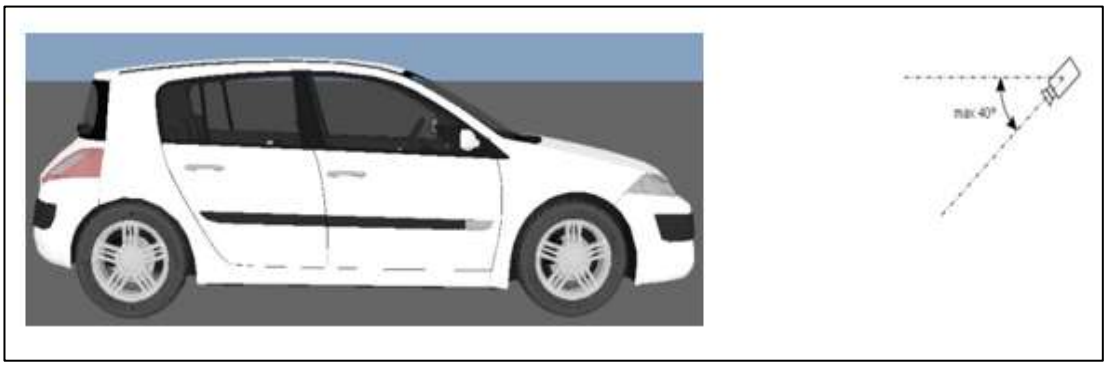


Figura 3.14: Ubicación cámara – Superior al vehículo
Elaborado por: Autor

3.5.5. Ubicación de cámara lateral al vehículo

Si la cámara debe estar ubicada en un ángulo lateral del paso del vehículo, como se muestra en la Figura 3.15, el ángulo máximo que debe usarse es de 30 grados.

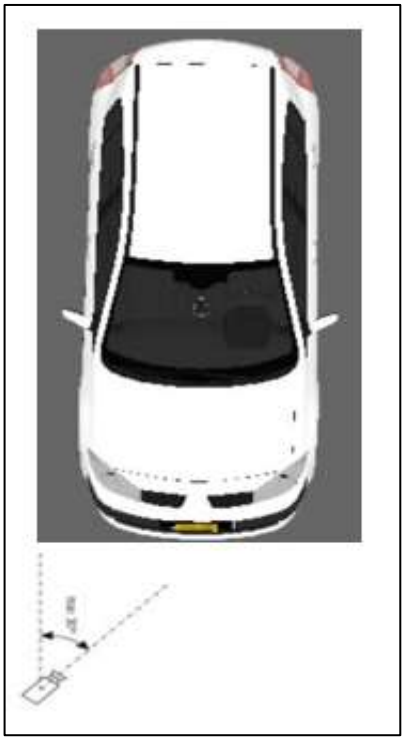


Figura 3.15: Ubicación cámara – Lateral al vehículo
Elaborado por: Autor

Estos son lineamientos base con los cuales se rige la distribución global de las cámaras; sin embargo, existen más herramientas que permiten diseñar un detallado y afinado sistema a fin de evitar puntos ciegos en la

monitorización del video o errores al escoger el lente adecuado para una solución. Este es caso de la herramienta “IP Video System Design” disponible para compra en www.jvsg.com, la cual provee de diferentes funcionalidades para realizar el cálculo de la cobertura visual de las cámaras, almacenamiento y demás parámetros a requerir, etc…El uso de esta herramienta es una práctica manera de visualizar el resultado de la ubicación de las cámaras, así como una referencia de lo que sería la visualización del video con el cambio de diferentes parámetros.

En la siguiente ilustración Figura 3.16, se realiza la graficación de la incidencia que tiene la ubicación de la cámara (altura), ya que si está instalada demasiado alta no podrá verse la placa vehicular. Como se puede observar, la ubicación de la cámara a una altura de 10 metros, para un objetivo de visualización de 3.5 metros de genera un rango de visión efectivo de la cámara entre los 18 metros y 32 metros, distancias menores a este rango, corresponden a puntos ciegos de visibilidad. En la toma superior se observa que a una distancia de 20 metros el ancho de cobertura visual es de 5.17 metros.

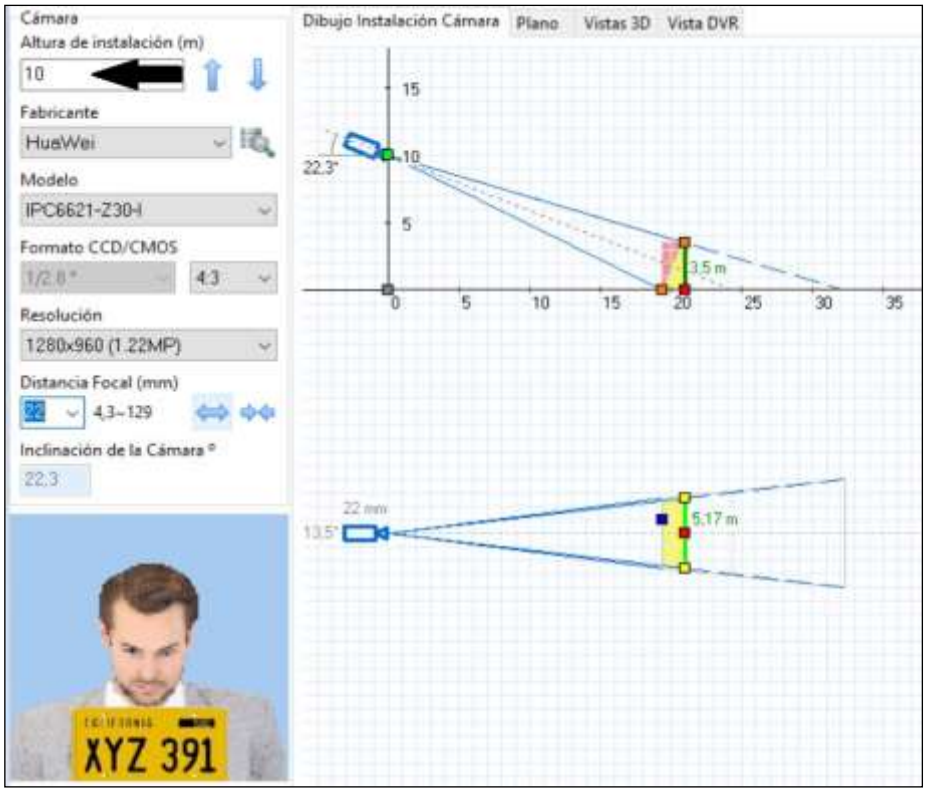


Figura 3.16: Campo de visión - Altura:10 metros
Elaborado por: Autor

Vale indicar que, para reducir los puntos ciegos, existen tres opciones:

1. Ampliar el campo de visión FOV
2. Ubicar las cámaras en una altura inferior
3. Reducir la altura del FOV

Para efectos de validar la incidencia de la altura de la cámara, con los mismos parámetros de distancia y objetivo a visualizar, se grafica a continuación en la Figura 3.17 el campo de visión de la cámara, con una altura de 6 metros. En la imagen el rango del campo visual de amplía entre 20 a 50 metros. En ambas imágenes se observan zonas de color, dado a que el software de diseño realiza automáticamente cálculos de la densidad de pixeles que la cámara tendrá en cada una de esas zonas a fin de brindar una rápida referencia de los servicios que pueden aplicarse en dichas áreas

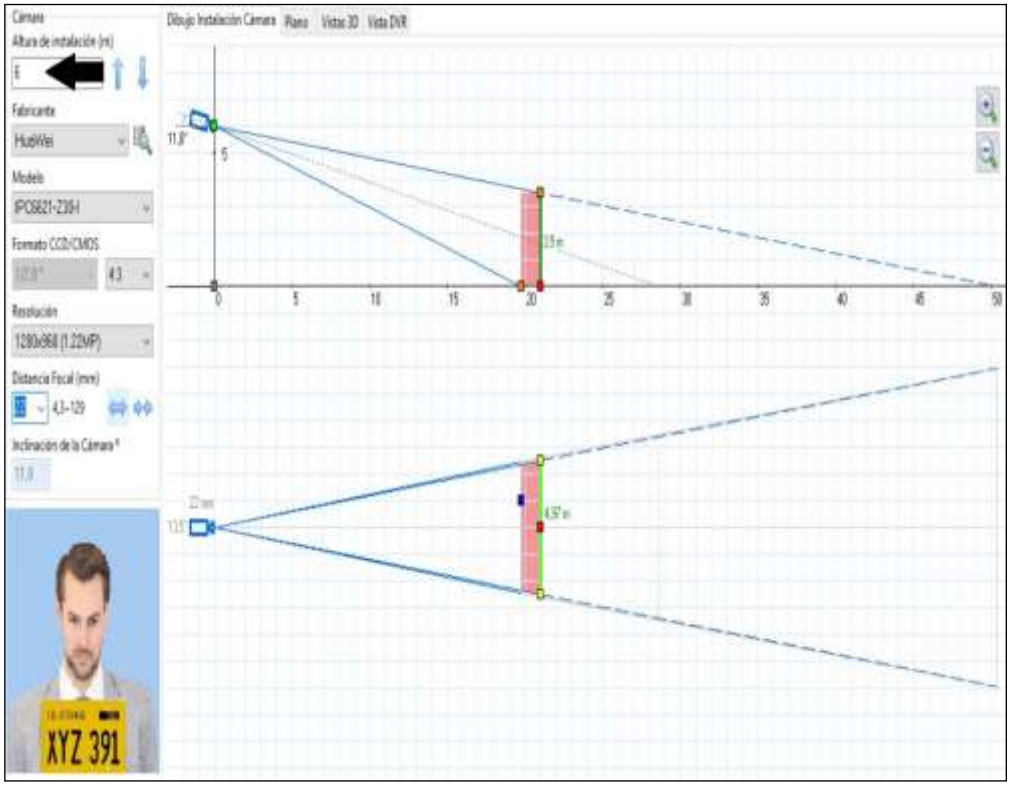


Figura 3.17: Campo de visión - Altura:6 metros
Elaborado por: Autor

Vale indicar que la densidad de pixeles es un parámetro importante al momento de cubrir un objetivo como lo sería la identificación facial, el reconocimiento o si de monitorear una multitud se trata. Este valor resulta de

la relación entre la resolución de la cámara y del ancho que se requiera tenga el campo de visión FOV (Field of Vision), indicado a continuación:

$$\text{Densidad de Pixeles} = \frac{\text{resolución horizontal}}{\text{campo de visión (FOV)}}$$

Dependiendo de la unidad en que se hayan establecido las métricas el resultado puede ser expresado en: Pixeles por pies (PPF) o Pixeles por metros (PPM). Por lo que en la Figura 3.18 indicada a continuación se indica el tipo de servicios a aplicarse en función los pixeles de cada zona del campo de visualización.

			Pixeles por metro	Pixeles por pies
Tono	**Color**	**Aplicación**	**(PPM)**	**(PPF)**
	Rojo	Identificación	250	76
	Amarillo	Reconocimiento	125	38
	Verde	Observación	62	19
	Verde Claro	Presencia	25	08
	Azul	Monitoreo Masas	12	04

Figura 3.18: Relación servicios - pixeles
Elaborado por: Autor

Para efectos de la activación del servicio de Lectura de Placas LPR debe acotarse la altura del objeto foco de visualización a fin de evitar falsos positivos en la lectura de información.

En base a ello, la graficación del ángulo de visión indicado se visualiza en la Figura 3.19. Realizando el ajuste de la altura del objeto foco a 0,5 metros, la herramienta nos indica visualmente el área en que la cámara podría efectuar identificación señalizada en color rojo, en el rango de distancia entre 15 y 18 metros y de 19 a 20 se considera válido para reconocimiento. Los valores de cálculo de los pixeles por metro PPM se indican en cifras en la

parte posterior de la imagen, siendo el ícono femenino con 303 mx/m el punto del FOV más cercano a la cámara y 228 px/m con el masculino como el más distante.

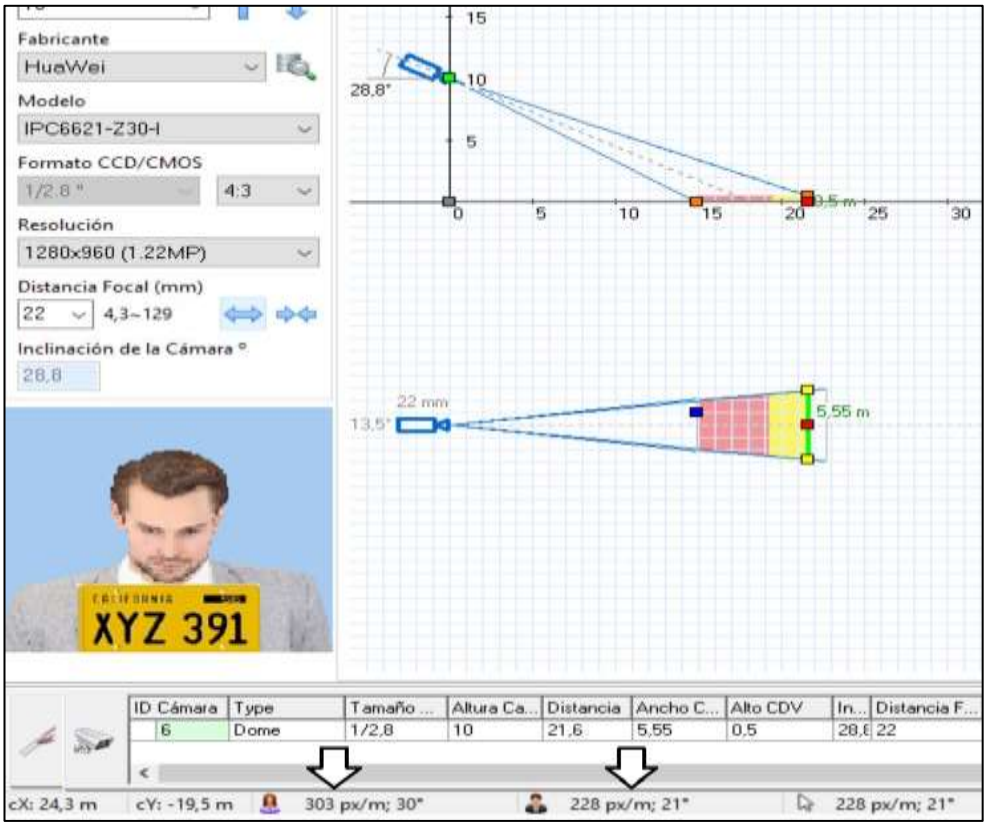


Figura 3.19: Ajuste altura objeto foco
Elaborado por: Autor

3.5.6. Ancho de banda

En la viñeta contigua al campo de Vision, se encuentra el cálculo que asimismo efectúa el software en términos del ancho de banda estimado y el espacio de disco duro de almacenamiento a requerirse.

A continuación, en la Figura. 3.20 se hace referencia al cálculo que, para los parámetros establecidos en el gráfico, sugiere la herramienta como consumo de ancho de banda en Mbits/s y almacenamiento expresados en Gigabits.

Figura 3.20: Cálculo de ancho de banda
Elaborado por: Autor

3.6. Activación del servicio LPR

Se procedió a activar el servicio de acuerdo con el procedimiento paso a paso de la plataforma Digifort, utilizando para ello una licencia provisional que fue facilitada por el fabricante para las pruebas, lo cual permitió la activación de la función de Lectura de placas LPR en una (01) de las cámaras indicadas por el ECU-911 Machala. Una vez activada la función se seleccionó la lectura de diferentes diseños de placa vehicular con la que cuenta la plataforma Digifort, activando para ello, la capacidad de lectura de formatos de placas de los siguientes países:

- Ecuador
- Colombia
- Perú
- Bolivia
- Brasil

En base a los cálculos previos efetuados, se realiza la ubicación de la câmara para lectura de placas y se observa el registro en la plataforma de las distintas placas vehiculares identificadas por la plataforma.

Figura 3.21: Lectura de placas vehiculares
Elaborado por: Autor

En la Figura 3.21 se observa el registro de lectura de placas, mientras que en la Figura 3.22 se valida la correcta la identificación de caracteres de la placa vehicular.

Figura 3.22: Validación lectura placas vehiculares
Elaborado por: Autor

3.6.1. Sumario de la activación del servicio LPR

Corresponde indicar que la demostración fue solicitada en el escenario actual de las cámaras; es decir:

- Las unidades disponibles al momento por la institución (tipo, marca, modelo)
- En la ubicación en que estas se encontraban operando, es decir instaladas en postes a 10 metros de altitud.

Por lo que siendo cámaras PTZ fue necesario fijar la toma a un área específica, así como realizar acercamientos de toma para obtener el enfoque de placas requerido.

- Pese a ello, se corroboró la integración y activación del servicio LPR en cámaras de diferentes fabricantes
- Se valida que para la mayoría de los casos resoluciones mayores a 2MP son válidas para efectuar esta función
- Se requiere las características de compensación de luz en las cámaras a usar para obtener mejor imagen
- Es muy importante usar el ángulo correcto en la cámara y que su toma sea fija

3.7. Video Synopsis

El manejo de la alta densidad de información de video recolectada a diario, por un centro de atención ciudadana como lo es el ECU-911 hace que un servicio como el resumen de información, conocido también como Video Synopsis, sea una herramienta indispensable para su operación del día a día., ello para efectos de liberar el uso de recursos humanos asignados en la búsqueda de grabaciones de video y optimizar la eficiencia (tiempos de respuesta) de dicha búsqueda.

El servicio activado de Video Synopsis superpone objetos sobre un fondo estacionario, de forma que muestra eventos que han ocurrido en diferentes momentos de forma simultánea, de esta manera es posible efectuar búsquedas de eventos almacenados en extensas horas de grabación y reducirlas a escasos minutos o incluso segundos de búsqueda. Entre los principales beneficios de este servicio son:

- Descubrir con facilidad eventos no reportados / no buscados
- Maximizar las inversiones de Cameras / VMS
- Tener la evidencia, en el menor tiempo posible
- Reducir el costo y el tiempo de funcionamiento
- Sincronizar vídeos off-lines con la base de la central de datos
- Integrar la experiencia del usuario con inteligencia e intuición
- Exportar y compartir la información investigada

Aunque no es objeto de este estudio, la plataforma brinda otras funcionalidades de análisis del vídeo como lo son conteo de personas, detección de objetos olvidados, análisis de ruta. etc…

3.7.1. Consideraciones de diseño Video Synopsis

El módulo de Video Synopsis de Digifort opera con una licencia de base que debe instalarse en el servidor para efectos de levantar el servicio, luego de lo cual se procese a activar las licencias para las cámaras, para las cuales se hayan adquiridos las licencias de soporte de esta funcionalidad. Vale indicar que las licencias no se fijan en una cámara determinada lo que permite

cambiar la configuración o asignación de dicha licencia, cuando necesite realizar el análisis en otras cámaras.

3.7.2. Activación del servicio Video Synopsis, filtro: vehículo-color

Durante esta fase se implementó el prototipo demostrativo de la tecnología mejorada de Video Synopsis, asimismo con el licenciamiento provisional proporcionado por el fabricante y se procede a realizar las pruebas .de sus funcionalidades, según se observa en la Figura 3.23.

Luego de haberse definidos los filtros de búsqueda (carro, rojo) el sistema encontró 34 unidades que coinciden con dicho criterio (indicados en ángulo superior derecho) de un total de 8706 objetos que identificó el sistema en este análisis.

Figura 3.23: Aplicación filtro tipo vehículo-color
Elaborado por: Autor

.

Se puede observar en un segundo plano los elementos –presentes en el video- pero que no son objetos de búsqueda, quedando en primer plano los que coinciden con el criterio deseado.

Asimismo, se observa que el sistema resume en un total de 03:21 segundos (ángulo inferior derecho), las apariciones de vídeo de las unidades de carros rojos que identificó en la búsqueda.

3.7.3. Aplicación de filtros: Género Masculino

Sobre el mismo video analizado se establece un nuevo criterio de búsqueda, en esta ocasión se realizará la búsqueda del género masculino.

Como resultado de la aplicación de este filtro se visualiza en la Figura 3.24 la identificación de 3.549 hombres en las horas de video analizado. Se observa que asimismo el sistema asigna sobre los individuos de la imagen la hora del vídeo donde ha ubicado a cada individuo en la grabación.

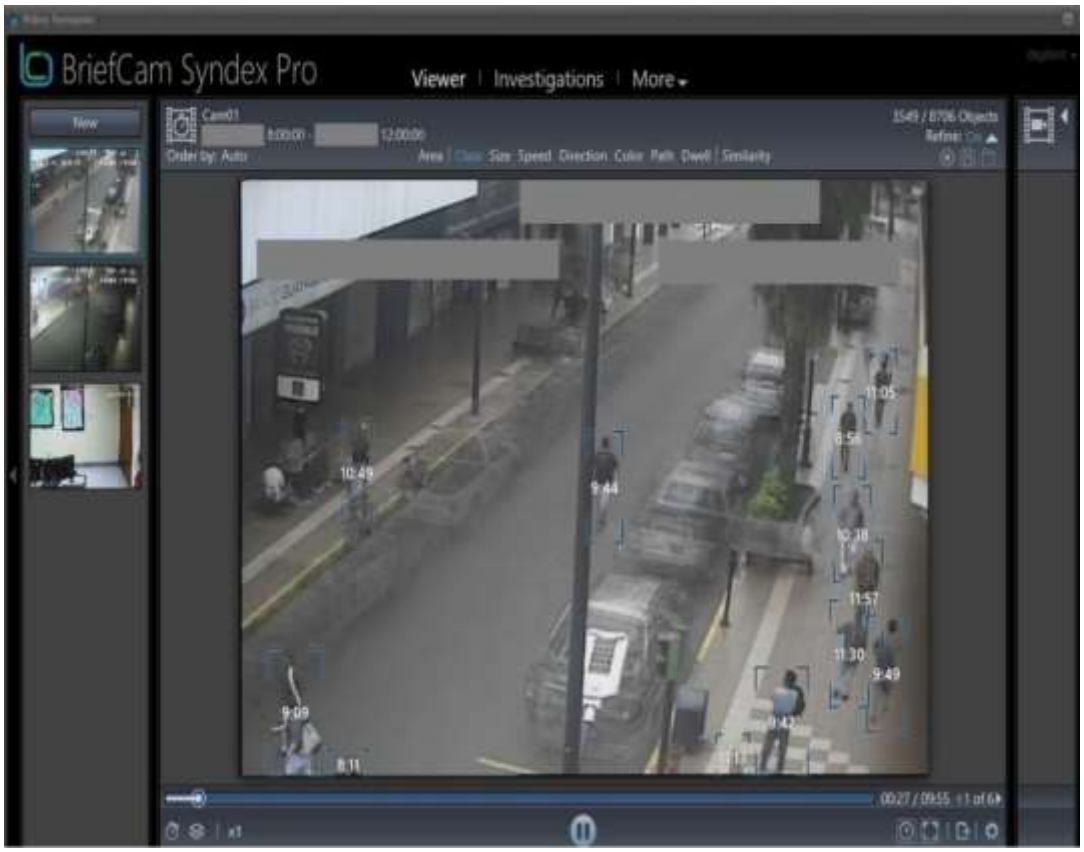


Figura 3.24: Aplicación filtro género-masculino
Elaborado por: Autor

3.7.4. Combinación de filtros: Género y ruta de circulación

En el video analizado, aplicando los nuevos criterios de búsqueda de género masculino y ruta definida, la herramienta en su búsqueda identificó 36 resultados, según se observa en la Figura 3.25.

Esta combinación de filtros (Género Hombre y ruta) fue efectuada para mostrar la versatilidad de la herramienta dado a que, si es de interés el análisis de circulación por una ruta específica, es posible hacerlo por medio de la graficación de una línea en el área de interés de búsqueda, esto lo permite la herramienta por medio de un cursor con el que se dibuja la línea sobre el video, en el ejemplo en mención corresponde a línea blanca en la imagen.

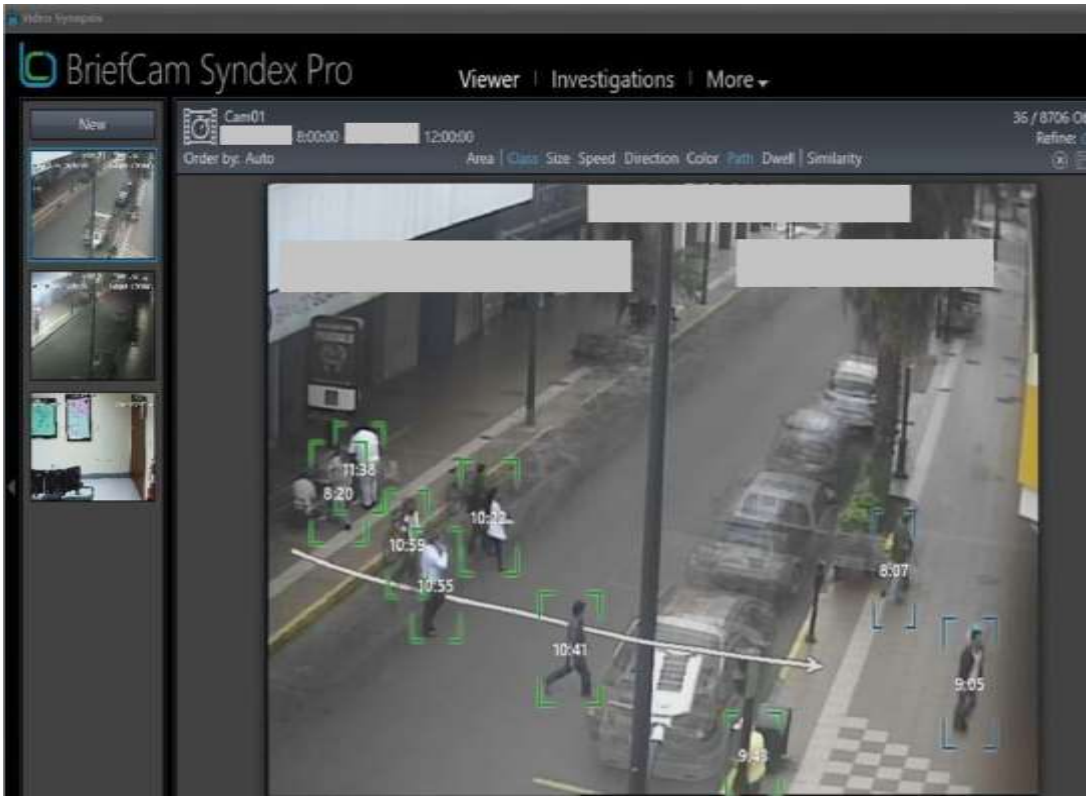


Figura 3.25: Aplicación filtros género-ruta
Elaborado por: Autor

3.7.5. Mapa de calor

En los filtros anteriores se inicia con el operador definiendo el área de la búsqueda, pero también se validó el filtro Mapa de Calor, indicado en la Figura 3.26, donde es el sistema ahora que analiza la mayor cantidad de movimiento, por medio de colores a fin de crear un mapa de calor que gráficamente permita visualizar las áreas de mayor circulación.

Esta información es muy importante no sólo para asignar medidas de seguridad o atención a los pasajeros de una terminal terrestre –por ejemplo- para asignar mayor personal de mantenimiento al identificar visualmente las áreas de mayor circulación de la población.

Esta información también en muy valiosa en términos de marketing dado a que se puede demostrar qué locales cuentan con mayor afluencia de clientes y tomar acciones comerciales en base a ello.

Figura 3.26: Aplicación filtro Mapa de calor
Elaborado por: Autor

3.8. Reconocimiento facial

Se procede con la activación del módulo de reconocimiento de rostros por medio de la licencia temporal provista por el fabricante y que habilita el servicio del experto mundial en tecnología de reconocimiento facial Sentinel, este servicio es activado en una de las cámaras existentes.

3.8.1. Aprendizaje de rostros

En esta fase la cámara a la que se le ha activado la función de reconocimiento facial provee video continuo a la plataforma de monitoreo, la cual captura diferentes ángulos del rostro de una misma persona como parte de su proceso Deep Learning, según se observa en la Figura 3.27 de forma de tener precisión al momento de identificar al individuo la próxima vez que registra su paso por la cámara. Los diferentes ángulos son expuestos para consideración del operador, de forma que pueda seleccionar los ángulos que identifican mejor a una persona, para su posterior identificación.

Estos pasos corresponden al aprendizaje automático de la plataforma de nuevos rostros y es óptimo para un determinado personal

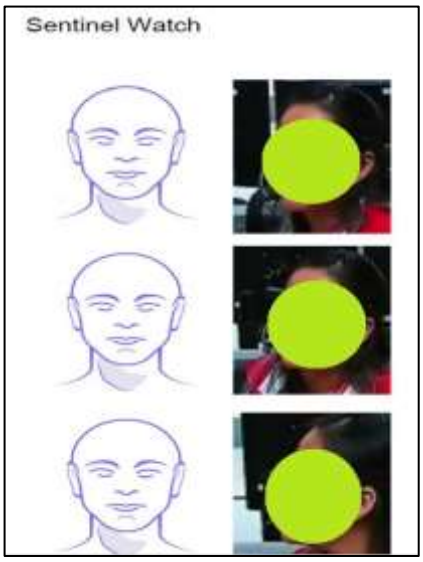


Figura 3.27: Captura automática ángulos de rostro
Elaborado por: Autor

3.8.2. Registro de nuevos rostros receptados

El sistema ofrece la opción de hacer un comparativo con una base de datos previa para realizar la comparación o proveer un listado de rostros capturados por medio de las cámaras para un operador realice la identificación inicial sobre la que efectuará las identificaciones en adelante que realice el sistema.

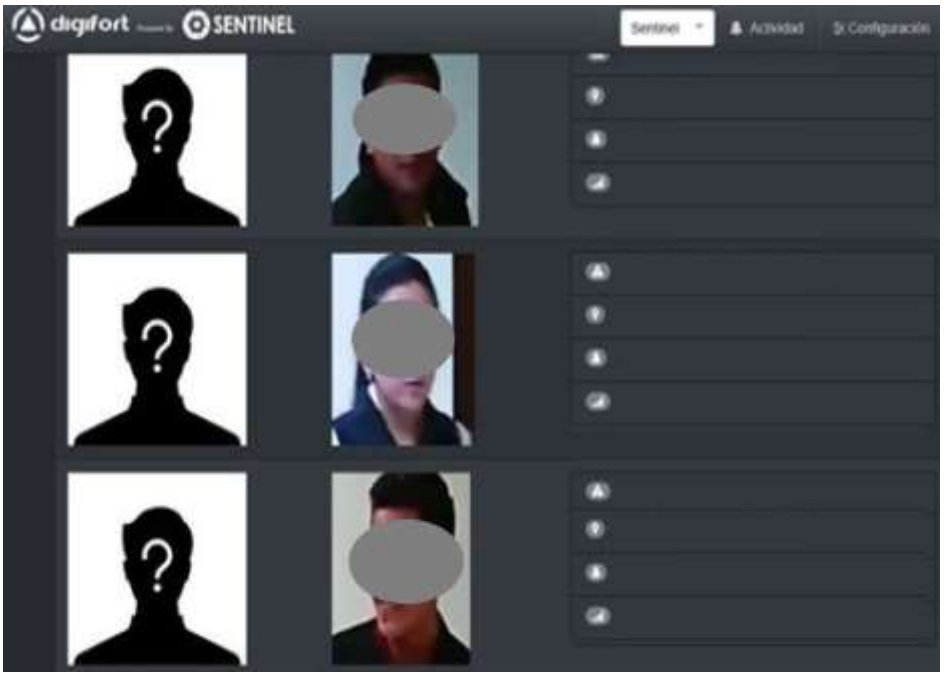


Figura 3.28: Captura facial para identificación
Elaborado por: Autor

En el caso de la presente demostración la segunda opción es la adoptada, es decir, el registro manual de cada nuevo rostro detectado por las cámaras, según se puede visualizar en la Figura 3.28, esta opción crea su propia base de registros y requiere la intervención de personal para realizar la debida identificación de rostros captados por la plataforma.

3.8.3. Identificación facial (Face recognition)

Con los datos de registros ingresados del punto anterior, se realiza la identificación facial de las personas que transitan en el área visual de cobertura de la cámara.

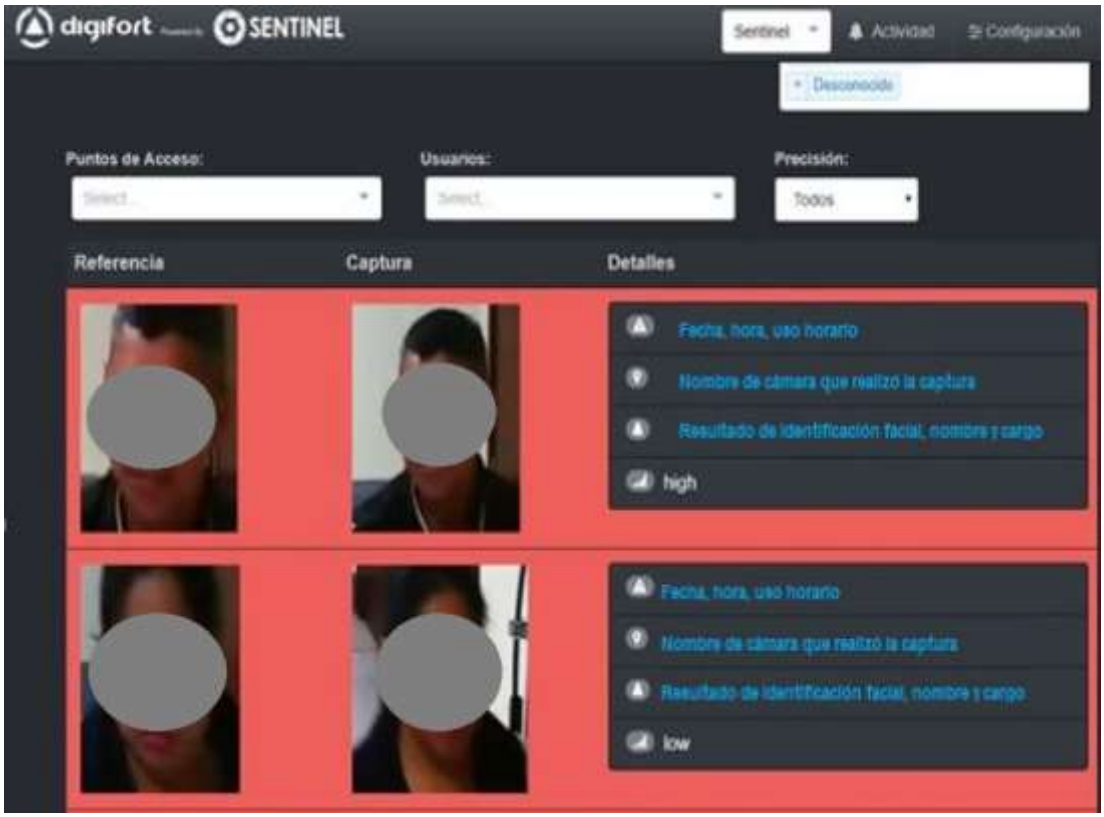


Figura 3.29: Ejecución de reconocimiento
Elaborado por: Autor

Además de la identificación facial la herramienta brinda opción de activación de listas blancas o negras, para efectos de toma de decisión en base a la identificación realizada. Las blancas hacen referencias a los rostros cuyo registro está permitido para el acceso a un área en particular, mientras que las negras son rostros que están denegados de circular o ingresar a determinadas áreas. Estas listas (blancas o negras) pueden activar alarmas a través de la plataforma, por medio de alertas emails, o, previa la debida

instalación, la activación de alarmas sonoras, cerramiento de puertas, activación de luces, comunicaciones en línea con las autoridades policiales, etc…

El fondo en color rojo de la Figura 3.29 corresponde una referencia visual que el sistema ya efectuó el reconocimiento facial de las imágenes proporcionadas, entregando en los casilleros ubicados en el área derecha los resultados asociados a cada una de ellas, en base a las identificaciones de identidad realizadas en el punto anterior. Nota: Por temas de seguridad, ha sido cubierta la información entregada por el sistema; sin embargo, los resultados originales han sido entregados a la institución.

CAPÍTULO 4: CONCLUSIONES Y RECOMENDACIONES.

4.1. Conclusiones.

- Mediante la demostración realizada en el ECU-911 Machala se concluye que la propuesta plataforma crítica de monitoreo DIGIFORT contribuye al establecimiento de las condiciones para la migración hacia una ciudad inteligente, orientada al aumento de la seguridad y optimización de recursos en el ECU-911 Ecuador.

- Por medio de la integración efectuada, se determina que la plataforma propuesta DIGIFORT es compatible con el hardware (marcas y modelos) de cámaras que actualmente disponible la entidad a nivel nacional, lo cual permite una migración sencilla, de forma paralela y por fases hacia la plataforma, para una transición transparente del servicio brindado.

- Con la demostración realizada se concluye que es factible activar, de forma inmediata, el servicio de lectura de placas en las actuales cámaras de monitoreo ciudadano a nivel nacional, con la facilidad que brinda la plataforma del traslado de dicho servicio a las cámaras que se desee asignar, según sea el requerimiento de búsqueda de la institución de un evento en particular, brindando de esta manera optimización de costos, versatilidad y como resultado, el incremento del nivel de seguridad en favor de la ciudadanía.

- Asimismo, se concluye que la funcionalidad de reconocimiento facial es viable de activar en las cámaras que dispone la institución, según sea el evento o requerimiento del momento, lo cual además del servicio de seguridad que brinda, optimiza recursos económicos dado a que no se requiere adquirir cámaras con esta función específica, sino que libera el servicio a la cámara de interés de evaluación.

- Se valida de igual forma la optimización de tiempos de respuesta y recursos humanos necesarios en la búsqueda de eventos grabados,

por medio de la activación de la funcionalidad de Analítica de video evaluada, la cual reduce a minutos de revisión extensas horas de grabación de video, en base a criterios de búsqueda determinados.

4.2. Recomendaciones.

- Dada la evolución de tecnología en video vigilancia y el tiempo de operación de las cámaras que cuenta la institución, se recomienda su renovación por modelos de cámaras IP que integren los adelantos de tecnología disponibles en el mercado abordados en el presente documento, de forma que se brinden niveles superiores de calidad y definición del video en el que se basan los servicios de video vigilancia que brinda la plataforma.

- Debido al tipo de servicio que brinda el centro de seguridad ciudadana, en lugar del modelo del modelo PTZ tradicional, se sugiere la adopción del tipo de cámara multisensor con integración de PTZ, de forma que, en todo momento, se cuente con la grabación del video de todos los ángulos de visualización de la cámara, de forma paralela al movimiento PTZ que se requiera efectuar en un momento dado, evitando así la pérdida de cobertura por rotación de la cámara.

- Para efectos de optimización de los anchos de banda requeridos por las cámaras y los rubros asociados a ello, se recomienda la adquisición de cámaras con soporte del códec de compresión H.265, de forma de reducir entre un 70% y 90% el consumo de ancho de banda, sin pérdida de calidad de la imagen del video.

- Para efectos de un mayor nivel de seguridad, se aconseja asimismo el uso de VPN (Virtual Private Network) con cada unidad de cámara IP, en el paso de información de video sobre los hilos de fibra óptica.

- Se recomienda el uso de la versión 7.3 de la plataforma, recientemente liberada, a fin de integrar las nuevas funcionalidades de analítica que incorpora a este servicio más granular de búsqueda.

- Siendo que la demostración de los servicios de la plataforma Digifort propuesta, se centró en la activación y pruebas de las principales funcionalidades de seguridad en video vigilancia, se recomienda la activación de otros servicios de esta línea como lo son cámara Móvil, integración de NVRs existentes y de funcionalidades adicionales de monitoreo de infraestructura crítica como lo son Protección Perimetral, Sistema de Incendios forestales, etc…

  .

REFERENCIAS BIBLIOGRÁFICAS

A. Mazhar, A. (2016). Performance Evaluation of h.265/mpeg-hevc, vp9 and h.264/mpeg-avc Video Coding. *The International Journal of Multimedia & Its Applications*, *8*(1), 35–44. https://doi.org/10.5121/ijma.2016.8103

Addati, G. A. (2014). *Sistemas VMS y PSIM* (Working Paper Núm. 539). Recuperado de Serie Documentos de Trabajo website: https://www.econstor.eu/handle/10419/110055

Axis Communications. (2019). AXIS Q6000-E Mk II PTZ Network Camera. Recuperado el 19 de septiembre de 2019, de Axis Communications website: https://www.axis.com/products/axis-q6000-e

Barros, A. (2010). El comportamiento de la infraestructura tecnológica y de comunicaciones / The response of the communications technological infrastructure. *Cuadernos.info*, *0*(26), 123-137–137. https://doi.org/10.7764/cdi.26.17

Bosch Security. (2019). TINYON IP 2000 WI. Recuperado el 19 de septiembre de 2019, de https://la.boschsecurity.com/es/productos/videosystems_1/ipcameras_1/hdmpfixedcameras_1/tinyonip2000wi_1/tinyonip2000wi_1_18997

Bülthoff, H. H., Cunningham, D. W., & Wallraven, C. (2011). Dynamic Aspects of Face Processing in Humans. En S. Z. Li & A. K. Jain (Eds.), *Handbook of Face Recognition* (pp. 575–596). https://doi.org/10.1007/978-0-85729-932-1_22

Cabello Pardos, E. (2004). *Técnicas de reconocimiento facial mediante redes neuronales* (Phd, Facultad de Informática (UPM)). Recuperado de http://oa.upm.es/215/

Dicsan Technology, D. (2019). How many frames per second is good for a security camera? | Dicsan Technology. Recuperado el 19 de

septiembre de 2019, de https://dicsan.com/Security_Cameras/security_cameras_frame_rate

Digifort. (2002). *Administration Client—Version 6.4.0.0*. 315.

Digifort. (2018). Video Management. Recuperado el 19 de septiembre de 2019, de https://www.digifort.com/gerenciamento-de-video.php#insight

Digifort. (2019). Design Tool. Recuperado el 19 de septiembre de 2019, de http://designtool.digifort.com.br/calc/Engine?extranet=yes;cmd=open

Góngora, G. P. M. (2015). Revisión de literatura sobre ciudades inteligentes: Una perspectiva centrada en las TIC. *Ingeniare*, (19), 137–149. https://doi.org/10.18041/1909-2458/ingeniare.19.531

Jyothirmai, M., Mounika, A., Bhavana, C., Supriya, T. S., & Viharika, D. (2018). Comparing H.264/M PEG-AVC, H.265/MPEG-HEVC and VP9 Encoders. *International Journal of Electronics*, *7*(4), 5.

Kruegle, H. (2011). *CCTV Surveillance: Video Practices and Technology*. Elsevier.

Lu, X. (2015). *Image Analysis for Face Recognition*. 37

.

Luján-Mora, S. (2001). *Programación en Internet: Clientes web*. Recuperado de http://rua.ua.es/dspace/handle/10045/16994

Marshall Electronics. (2019). Network Video Management Software—VMS-16, VMS-36, VMS-64 and VMS-128 Network Video Management Software. Recuperado el 19 de septiembre de 2019, de http://www.marshall-usa.com/software/VMS-16.php

Mata, F. J. G. (2010). *Videovigilancia: CCTV usando vídeos IP*. Editorial Vértice.

Milani, S., Fontani, M., Bestagini, P., Barni, M., Piva, A., Tagliasacchi, M., & Tubaro, S. (2012). An overview on video forensics. *APSIPA*

Transactions on Signal and Information Processing, *1*. https://doi.org/10.1017/ATSIP.2012.2

Montavue. (2017, marzo 8). Understanding why Wide Dynamic Range (WDR), Highlight Compensation (HLC), and Backlight Compensation (BLC) are crucial to a clear image. Recuperado el 19 de septiembre de 2019, de Montavue website: https://montavue.com/2017/03/08/understanding-wide-dynamic-range-wdr-highlight-compensation-hlc-backlight-compensation-blc-crucial-clear-image/

NUO by Techdesign. (2015, diciembre 9). ¿Qué son los grados de protección IP? Recuperado el 19 de septiembre de 2019, de NÜO Planet: Sistemas de Control de Accesos y Control de Puertas website: https://nuoplanet.com/blog/grados-de-proteccion-ip/

Sarfraz, M., & Jameel, M. (2005). License Plate Recognition System: Saudi Arabian Case. En M. Sarfraz (Ed.), *Computer-Aided Intelligent Recognition Techniques and Applications* (pp. 19–32). https://doi.org/10.1002/0470094168.ch2

Simão, M. de M. B., Firmino, R. J., Simão, M. de M. B., & Firmino, R. J. (2019). A construção social de um sistema de mobilidade inteligente: Mapeando controvérsias no caso do Swisspass. *Cadernos Metrópole*, *21*(44), 331–354. https://doi.org/10.1590/2236-9996.2019-4414

Taigman, Y., Yang, M., Ranzato, M., & Wolf, L. (2014). DeepFace: Closing the Gap to Human-Level Performance in Face Verification. *2014 IEEE Conference on Computer Vision and Pattern Recognition*, 1701–1708. https://doi.org/10.1109/CVPR.2014.220

Uniview Technologies Co., Ltd. (2011, 2019). IPC2128SR3-DPF40(60) 4K Mini Fixed Bullet Network Camera—Zhejiang Uniview Technologies Co., Ltd. Recuperado el 19 de septiembre de 2019, de http://www.uniview.com/Products/Cameras/Prime/IPC2128SR3-DPF40(60)/

Wen, Y., Lu, Y., Yan, J., Zhou, Z., von Deneen, K. M., & Shi, P. (2011). An Algorithm for License Plate Recognition Applied to Intelligent Transportation System. *IEEE Transactions on Intelligent Transportation Systems*, *12*(3), 830–845. https://doi.org/10.1109/TITS.2011.2114346

Yoon, A. K., Park, K., Oh, D., Cho, H., & Jang, J. (2019). Analogical Face Generation based on Feature Points. https://doi.org/10.33851/JMIS.2019.6.1.15

DECLARACIÓN Y AUTORIZACIÓN

Yo, **Rodríguez Zambrano, Avelinda Kerench** con C.C: # 080172515-1 autor del Trabajo de Titulación: **"PROPUESTA DE PLATAFORMA CRÍTICA DE MONITOREO PARA LA MIGRACIÓN HACIA UNA CIUDAD INTELIGENTE, ORIENTADA AL AUMENTO DE LA SEGURIDAD Y OPTIMIZACIÓN DE RECURSOS EN EL ECU-911 ECUADOR",** previo a la obtención del título de **INGENIERO EN TELECOMUNICACIONES** en la Universidad Católica de Santiago de Guayaquil.

1.- Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

2.- Autorizo a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de propiedad intelectual vigentes.

Guayaquil, 12 de septiembre del 2019

f. _____

Nombre: Rodríguez Zambrano Avelinda Kerench

C.C: 080172515-1

REPOSITORIO NACIONAL EN CIENCIA Y TECNOLOGÍA

FICHA DE REGISTRO DE TESIS/TRABAJO DE TITULACIÓN

TÍTULO Y SUBTÍTULO:	"PROPUESTA DE PLATAFORMA CRÍTICA DE MONITOREO PARA LA MIGRACIÓN HACIA UNA CIUDAD INTELIGENTE, ORIENTADA AL AUMENTO DE LA SEGURIDAD Y OPTIMIZACIÓN DE RECURSOS EN EL ECU-911 ECUADOR".		
AUTOR(ES)	Rodríguez Zambrano, Avelinda Kerench		
REVISOR(ES)/TUTOR(ES)	M. Sc. LUIS SILVIO CORDOVA RIVADENEIRA		
INSTITUCIÓN:	Universidad Católica de Santiago de Guayaquil		
FACULTAD:	Facultad de Educación Técnica para el Desarrollo		
CARRERA:	Ingeniería en Telecomunicaciones		
TITULO OBTENIDO:	Ingeniero en Telecomunicaciones		
FECHA DE PUBLICACIÓN:	12 de septiembre del 2019	**No. DE PÁGINAS:**	76
ÁREAS TEMÁTICAS:	Telecomunicaciones, Nueva Tecnología		
PALABRAS CLAVES/ KEYWORDS:	CIUDAD INTELIGENTE, MONITOREO, RECONOCIMIENTO, GESTIÓN, CONTROL, VIDEO ANALITICA		

RESUMEN/ABSTRACT:

En el presente trabajo se realiza un análisis técnico a fin de presentar una propuesta de plataforma crítica de monitoreo que pueda operar como base tecnológica de un centro de seguridad ciudadana y que brinde las condiciones para la migración hacia ciudades inteligentes, incrementando la seguridad y la optimización de recursos de personal, financieros y tiempos de respuesta de un centro de atención ciudadana como lo es el Ecu-911. En el Capítulo 1, se presentan algunos de los criterios que rigen los modelos de ciudades inteligentes y de gestión de control de la infraestructura critica, se emplea una investigación de tipo descriptiva y exploratoria y se establecen los objetivos del presente trabajo. El Capítulo 2, comprende la fundamentación teórica del tema de evaluación, abordando nociones de video vigilancia base, hasta la cobertura de conceptos específicos relacionados con la inteligencia de video a implementar. El Capítulo 3 se enfoca en la aportación realizada por quien suscribe a nivel del diseño, en cuanto a la selección de la plataforma a usar, implementación de los servicios específicos seleccionados. El Capítulo 4, finaliza con las conclusiones y recomendaciones resultantes de las pruebas realizadas en el presente trabajo en miras de adoptar una infraestructura de gestión crítica su contribuir de esta manera con el establecimiento de ciudades inteligentes en miras de la mejora de la calidad de vida de la población.

ADJUNTO PDF:	☒ SI	☐ NO
CONTACTO CON AUTOR/ES:	**Teléfono:** +593-9-9818-4118	E-mail: kerenchaaa@gmail.com
CONTACTO CON LA INSTITUCIÓN: COORDINADOR DEL PROCESO DE UTE	**Nombre:** Palacios Meléndez Edwin Fernando	
	Teléfono: +593-9-67608298	
	E-mail: edwin.palacios@cu.ucsg.edu.ec	

SECCIÓN PARA USO DE BIBLIOTECA	
Nº. DE REGISTRO (en base a datos):	
Nº. DE CLASIFICACIÓN:	
DIRECCIÓN URL (tesis en la web):	