UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI

FACULTAD DE INDUSTRIAS AGROPECUARIAS Y CIENCIAS AMBIENTALES

CARRERA DE INGENIERÍA EN INFORMÁTICA

Tema: "Sistema de video vigilancia para la seguridad de los equipos en los laboratorios de la carrera de computación"

Trabajo de titulación previa la obtención del título de Ingeniero en Informática

AUTOR: Arévalo Puetate Jimmy Javier

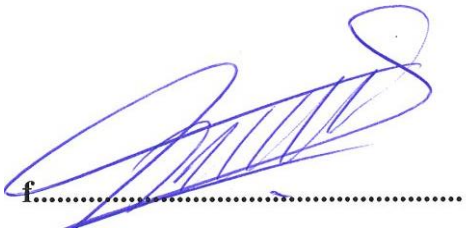
TUTOR: Ing. Milton Gabriel Del Hierro Mosquera MSc.

Tulcán, 2023

CERTIFICADO JURADO EXAMINADOR

Certificamos que el estudiante Arévalo Puetate Jimmy Javier con el número de cédula 0402134613 ha elaborado el trabajo de titulación: "Sistema de video vigilancia para la seguridad de los equipos en los laboratorios de la carrera de computación"

Este trabajo se sujeta a las normas y metodología dispuesta en el Reglamento de Titulación, Sustentación e Incorporación de la UPEC, por lo tanto, autorizamos la presentación de la sustentación para la calificación respectiva



f.....

Ing. Del Hierro Mosquera Milton Gabriel MSc.

TUTOR

f.....

Ing. Hidalgo Guijarro Jairo Vladimir MSc.

LECTOR

Tulcán, octubre de 2023

AUTORÍA DE TRABAJO

El presente trabajo de titulación constituye requisito previo para la obtención del título de **Ingeniero** en la Carrera de ingeniería en informática de la Facultad de Industrias Agropecuarias y Ciencias Ambientales

Yo, Arévalo Puetate Jimmy Javier con cédula de identidad número 0402134613 declaro: que la investigación es absolutamente original, auténtica, personal y los resultados y conclusiones a los que he llegado son de mi absoluta responsabilidad.

f.....

Arévalo Puetate Jimmy Javier
AUTOR

Tulcán, octubre de 2023

ACTA DE CESIÓN DE DERECHOS DEL TRABAJO DE TITULACIÓN

Yo, Arévalo Puetate Jimmy Javier declaro ser autor de los criterios emitidos en el trabajo de investigación: “Sistema de video vigilancia para la seguridad de los equipos en los laboratorios de la carrera de computación” y eximo expresamente a la Universidad Politécnica Estatal del Carchi y a sus representantes legales de posibles reclamos o acciones legales.

f.....

Arévalo Puetate Jimmy Javier
AUTOR

Tulcán, octubre de 2023

AGRADECIMIENTO

Quiero expresar mi profundo agradecimiento a todas las personas que hicieron posible la realización de esta tesis, sin su apoyo y colaboración este proyecto no habría sido posible. En primer lugar, quiero agradecer a mi tutor de tesis el MSc Milton Del Hierro, por su orientación, paciencia y sabiduría a lo largo de este proceso, su experiencia y dedicación fueron fundamentales para dar forma a este trabajo y ayudarme a alcanzar mis objetivos académicos. En segundo lugar, quiero expresar mi gratitud a los docentes de la carrera y personal de TICS quienes amablemente compartieron sus conocimientos conmigo y me brindaron valiosas sugerencias para mejorar mi trabajo, también quiero agradecer a mi familia por su apoyo incondicional a lo largo de mi carrera académica, su amor, aliento y sacrificio son la razón por la que he llegado hasta aquí. No puedo dejar de mencionar a todas las personas que participaron en las entrevistas y encuestas que formaron parte de mi investigación su colaboración fue esencial para recopilar datos significativos y obtener conclusiones sólidas. Finalmente, quiero agradecer a mi Universidad Politécnica Estatal del Carchi por brindarme los recursos necesarios para llevar a cabo este proyecto y por fomentar un ambiente de aprendizaje enriquecedor.

¡Gracias a todos!

DEDICATORIA

Dedico este trabajo a mis padres, Bolívar Arévalo, Piedad Puetate y mi hermana Shirley, quienes han sido mi fuente inagotable de apoyo, amor y sabiduría a lo largo de mi vida y durante este arduo proceso de investigación, su constante aliento y sacrificio han sido la luz que me guio en los momentos difíciles. También dedico esta tesis a mi abuelita Beatriz y mi tía Rosa, cuya inspiración y aliento me han orientado en cada paso de este viaje académico. A mis amigos por compartir risas, alegrías y desafíos a lo largo de estos años, su amistad ha sido un recordatorio constante de la importancia de la comunidad y el compañerismo. A todos ustedes, mi más sincero agradecimiento.

Jimmy Arévalo

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE ANEXOS

RESUMEN

La presente tesis aborda la implementación de un sistema de video vigilancia que se llevó a cabo en la carrera de computación de la Universidad Politécnica Estatal del Carchi con el objetivo de mejorar la seguridad. Ya que el mal uso de los laboratorios por parte de los estudiantes tubo como consecuencia el hurto y daño de equipos, es así como el objetivo del proyecto se basó en el diseño, creación e implementación de un sistema de videovigilancia eficiente con estándares de calidad que sea accesible solo para el personal autorizado aprovechando tecnologías de software libre. Como guía de desarrollo de forma rápida se analizó la metodología ágil Scrum como solución a medida que se la utilizo por su seguridad de éxito al ser aplicada con gran facilidad de adaptabilidad, para lograr esto, se seleccionó estándares de calidad, cámaras y se estableció una topología de red en cableado para garantizar la transmisión de datos en tiempo real, de la misma manera se instaló un servidor NVR equipado con software de análisis de video que permitirá la detección y grabación automática lo que redujo la necesidad de una supervisión constante, igualmente se implementaron medidas de privacidad y seguridad para proteger la información capturada y garantizar el cumplimiento de las regulaciones de protección de datos, los resultados obtenidos demostraron una mejora en la seguridad del campus, con una detección temprana de eventos anómalos y una respuesta rápida a situaciones de riesgo. Este proyecto representa un avance significativo en la aplicación de tecnologías de videovigilancia en entornos educativos, contribuyendo a la creación de ambientes más seguros y protegidos para la comunidad universitaria

Palabras Claves: Video vigilancia, Estándares de Calidad, NVR (grabado de video en red), Software libre

ABSTRACT

This thesis studies the implementation of a video surveillance system that was carried out in the computer career at the State Polytechnic University of Carchi to improve security. Since the misuse of the laboratories by the students resulted in the theft and damage of equipment, that is why the objective of the project was based on the design, creation, and implementation of an efficient video surveillance system with quality standards that is accessible only to authorized personnel taking advantage of free software technologies. As a quick development guide, the agile Scrum methodology was analyzed as a tailored solution that was used for its security of success when applied with great ease of adaptability, to achieve it, quality standards and cameras were selected and a network topology in cabling were established to ensure real-time data transmission, in the same way, an NVR server equipped with video analysis software was installed that will allow automatic detection and recording, which reduced the need for constant monitoring, privacy, and security measures were also implemented to protect the captured information and ensure compliance with data protection regulations, the results showed an improvement in campus security, with early detection of anomalous events and rapid response to risk situations. This project represents a significant advance in the application of video surveillance technologies in educational environments, contributing to the creation of safer and more protected environments for the university community.

Keywords: Video surveillance, Quality Standards, NVR (network video recording), Free software

INTRODUCCIÓN

La inseguridad en la sociedad ha generado una creciente necesidad de implementar sistemas de seguridad eficientes para salvaguardar entornos públicos y privados, es así que para el desarrollo del proyecto de implementación video vigilancia emerge como una herramienta fundamental para monitorear y gestionar la seguridad, de igual manera este trabajo de tesis se sumerge en el ámbito de la informática y la seguridad, focalizándose en la implementación de un sistema de video vigilancia en la carrera de computación de la prestigiosa UPEC. En el capítulo uno el problema nos hace referencia a la comunidad universitaria, al igual que muchas otras instituciones, enfrenta desafíos significativos en términos de seguridad, que son incidentes como intrusiones no autorizadas, vandalismo y situaciones de emergencia que requieren respuestas rápidas y efectivas. De tal manera el planteamiento del problema se centra en la falta de un sistema de video vigilancia específicamente adaptado a las necesidades de la carrera de computación, lo que puede generar inseguridad, por otro lado, el objetivo principal de esta investigación es diseñar, implementar un sistema de video vigilancia que optimice la seguridad y gestión de recursos en el entorno educativo de la carrera de computación es así que se buscó proporcionar una solución integral que no solo garantice la detección y prevención de situaciones indebidas, sino que también facilite el análisis de datos para mejorar la eficiencia y la toma de decisiones en el ámbito académico.

En el capítulo dos aborda los antecedentes que fue información de mucha importancia ya que de estas fuentes se pudo construir el marco teórico y poder obtener datos valiosos de cómo se desarrollaron trabajos similares en diferentes instituciones al implementar el sistema de video vigilancia, es así como se identificaron conceptos de vital importancia a la hora de implementar el sistema

En el capítulo tres se da a conocer la metodología que se utilizó en la investigación para alcanzar los objetivos propuestos, en primer lugar, se realizará un análisis exhaustivo de la literatura científica y técnica relacionada con la videovigilancia en entornos universitarios con el fin de comprender los enfoques y tecnologías más actuales en este campo, después se llevó a cabo un estudio detallado de las necesidades y requisitos de seguridad específicos de la universidad que fue el objeto de estudio.

En el capítulo cuatro se diseñó un sistema de videovigilancia adaptado a las necesidades de la carrera, aprovechando tecnologías avanzadas como software libre, cámaras de alta resolución, análisis de vídeo, almacenamiento en el sistema, es así como la implementación se realizará en fases, considerando la infraestructura de red existente y la capacidad de procesamiento de datos, además de la realización de pruebas en los diferentes ámbitos del sistema de video vigilancia

I. EL PROBLEMA

1.1. PLANTEAMIENTO DEL PROBLEMA

En Latinoamérica la evolución de la tecnología crece a ritmo acelerado y actualmente ha asumido un papel clave en el desarrollo social, al igual que la delincuencia cada vez toma cavidad en las ciudades, las personas en estos tiempos han optado por el uso de sistemas de seguridad para salvaguardar la integridad de los bienes materiales en hogares y oficinas. El aumento de la delincuencia en el Ecuador y a nivel mundial actualmente es motivo de preocupación para la población, por eso se toma medidas preventivas como la video vigilancia puede fortalecer y aumentar la seguridad de los ciudadanos además de los bienes materiales en cualquier ambiente, como es en el caso de bienes inmuebles, estudios, trabajo. La falta o inexistencia de los sistemas de video vigilancia provoca un sin número de problemas (Heredia & Rea, 2022) argumentan que existen personas inescrupulosas que realizan desmanes sea en los sectores público o privados y perjudican a los dueños de los bienes materiales además causan pérdidas económicas muy considerables al no contar con algún sistema de vigilancia, no saben qué persona realizo el delito y tampoco pedir que se haga cargo de sus actos realizados (p.17).

> En el Ecuador han indo incrementando la implementación de los CCTV(circuito cerrado de televisión), así mismo su eficacia ha sido cuestionada debido a la ausencia de supervisión y control de las autoridades, por lo tanto existen preocupaciones sobre la privacidad de los ciudadanos, ya que estos sistemas pueden ser utilizados para vigilar y monitorear a la población sin su consentimiento, en efecto surge la necesidad de investigar la efectividad de los sistemas de videovigilancia en Ecuador, así como su impacto en la privacidad y derechos humanos de los ciudadanos, de igual manera se deben analizar las políticas y regulaciones existentes para determinar si son adecuadas para garantizar una implementación justa y responsable. De acuerdo con la Fiscalía General del Estado por medio del ECU-911 en la provincia del Carchi el reporte de denuncias en el año 2021 al 2022 fueron de 476 ya que él cuenta con CCTV (circuito cerrado de televisión) propio, con esto los militares, policías y aduaneros gracias a su sistema supervisado por personal altamente capacitado identificaron la mayoría de los puntos de conflicto y cruces fronterizos irregulares, pero no pueden vigilar toda la provincia por la falla de cobertura de las telecomunicaciones en varios puntos estratégicos donde son los lugares más importantes en el combate contra la delincuencia

y el narcotráfico para así garantizar la seguridad de la población tulcaneña (CARCHI AL DÍA, 2021) .

En el cantón de Tulcán por el hecho de ser zona fronteriza se cometen muchos delitos los cuales no son percibidos por la inexistencia de cámaras en zonas estratégicas y no se ha podido controlar la delincuencia, el contrabando, ni el narcotráfico ya que este tipo de actividad solo favorece a personas que violan la ley. En la Universidad Politécnica Estatal del Carchi se encuentra implementado un sistema de video vigilancia mas no cubre con la mayoría del campus universitario como resultado según el ingeniero Javier Torres encargado del sistema de vigilancia se produjeron varios robos de equipos en las instalaciones de la universidad es así que existen riesgos de inseguridad en los laboratorios de computación al no contar con la vigilancia de dichas áreas exponiéndolas a robo y vandalismo por parte de los estudiantes, además de las personas que ingresan a los laboratorios sin credenciales y de consecuencia el área educativa sufre de actos delictivos sin poder encontrar a los culpables.

En la UPEC según los encargados del área de tics se han presentado robos y daños a los equipos que se encuentran en las aulas y laboratorios. De la misma manera en la carrera de computación se presentó el robo de dos proyectores, es decir estos actos se presentaron porque no se cuenta con un sistema de video vigilancia lo que hace ineficiente al sistema actualmente instalado por no cubrir todas las áreas del campus sino también al no aplicar normativas y estándares de calidad en el circuito cerrado de televisión, lo cual para el proyecto se planteó el desarrollo de un sistema de video vigilancia con un monitoreo en línea, cámaras IP, equipo NVR y servidor en sus laboratorios así mismo no cuentan con un supervisor el cual lleve un adecuado monitoreo virtual de equipos en los laboratorios.

El mal uso de los laboratorios por parte de los estudiantes tiene como consecuencia el hurto o desaparición de equipos y daños, además de tener en cuenta a las personas que ingresan sin ninguna medida de control da como resultado el mal uso de los equipos, por otro lado, al no tener ningún control de acceso no se puede saber las personas que realizan alguna clase de delito ni evidencias anteriores en los laboratorios de la carrera de computación

1.2. FORMULACIÓN DEL PROBLEMA.

La deficiente aplicación de estándares de calidad en el sistema de video vigilancia de la UPEC en el año 2022 causa inseguridad en los laboratorios de la carrera de computación, que provoca pérdida y daños de los equipos informáticos.

1.3. JUSTIFICACIÓN

En la actualidad la tecnología va avanzado cada vez más, provocando cambios y por esta razón es que se ha visto involucrada en varias áreas para el desarrollo de la humanidad una de ellas es la seguridad de la gente y sus posesiones. Según Morán (2022) el Ecuador necesita un sistema de videovigilancia con detección facial que sea capaz de detectar situaciones anómalas con una inversión de más de 29.5 millones de dólares para instalar cámaras de seguridad en todo el país. Además, se han desarrollado sistemas de reconocimiento facial y de matrículas de vehículos para mejorar la capacidad de monitoreo y seguimiento de personas además de vehículos en tiempo real, los sistemas de videovigilancia han sido ampliamente utilizados en Ecuador para mejorar la seguridad y reducir los índices de criminalidad.

La presente investigación se realizará en las instalaciones del área de TICS y continuaría en los laboratorios de la carrera de computación de la Universidad Politécnica Estatal del Carchi de la ciudad de Tulcán, por los sucesos de inseguridad anteriormente sucedidos por la sustracción de equipos tecnológicos de los laboratorios además de no contar con ninguna persona supervisando de forma física o virtual la seguridad. Se pretende desarrollar una solución informática para que la universidad pueda prevenir el daño además del robo de los equipos, ya que la red del circuito cerrado de televisión cuenta con cámaras IP, cableado, NVR y el servidor HPE que ayudara a la seguridad en los laboratorios de la carrera computación así mismo se puedan vigilar las cámaras de seguridad en tiempo real.

Este proyecto contara con un NVR que está compuesto por las cámaras, el servidor y asimismo contar con cuatro discos duros de 1.2 terabytes de almacenamiento que permita almacenar los videos para la administración y gestión que se encuentran conectados al sistema de seguridad local de los laboratorios de computación para realizar la tarea de obtención de video y a su vez guardarlos, en tal sentido el sistema debe de ir conectado al switch para así poder agregar el número de cámaras IP correspondientes a todos los laboratorios de la carrera de igual manera la utilización de la VLAN que proporciona tics para poder conectarnos al servidor y tener acceso a nuestro sistema, además de emplear el uso de herramientas de software libre en el equipo NVR para poder monitorear el sistema de manera online con este sistema de seguridad se garantizara al administrador un control en los laboratorios de computación para así evitar la sustracción de los equipos y pueda otorgar seguridad a estos mismos con la opción de ser escalable para poder añadir varias cámaras IP a futuro.

Para la Universidad Politécnica Estatal del Carchi en definitiva es importante tener un sistema de video vigilancia con estándares de calidad y normas que respalden cada componente e instalación realizada en los equipos ya que con estos estándares podemos tener un sistema de video vigilancia con mayor seguridad y a la misma ves poder dar un mantenimiento, los principales beneficiarios de este proyecto serán los estudiantes, docentes y personal administrativo de la universidad por otorgar seguridad con el uso de streaming de video además de poder prevenir robos o sustracción de los equipos al tener una mayor calidad en imagen de los entornos donde se encuentren ubicadas las cámaras de vigilancia.

1.4 OBJETIVOS Y PREGUNTAS DE INVESTIGACIÓN

1.4.1. Objetivo General

Diseñar un sistema de video vigilancia con estándares de calidad para la seguridad de los equipos tecnológicos en los laboratorios de la carrera de y computación

1.4.2. Objetivos Específicos

1. Sustentar bibliográficamente el uso de los estándares de calidad además de los componentes tecnológicos que se emplearon en el sistema de video vigilancia para la elaboración del proyecto de investigación.
2. Identificar los estándares de calidad del sistema de video vigilancia para la seguridad de los laboratorios.
3. Determinar los equipos tecnológicos necesarios para el desarrollo del sistema de video vigilancia
4. Implementar un sistema de video vigilancia con sus respectivos componentes para los laboratorios de la carrera de informática

1.4.3. Preguntas de Investigación

- ¿Cómo la fundamentación teórica y bibliográfica apoya a la investigación de los sistemas de video vigilancia con toda su infraestructura?
- ¿Cuáles son las políticas, regulaciones y estándares de calidad que se usan en el sistema de video vigilancia en los laboratorios de la UPEC?
- ¿Cómo influye los sistemas de video vigilancia para la prevención de hurto de los equipos tecnológicos y ayuden a tener más seguridad en los laboratorios?
- ¿Cuáles son las herramientas de hardware, software que se utilizaran para implementar en sistema de video vigilancia?

II. FUNDAMENTACIÓN TEÓRICA

2.1. ANTECEDENTES INVESTIGATIVOS

Para Heredia y Rae (2022) en su tesis "Diseño e implementación de un sistema video vigilancia y detección facial utilizando cámaras IP para el reconocimiento de individuos en la cercanía de residencias familiares",

> En donde el proyecto de tesis citado utilizó numerosos estudios para analizar la problemática del tema con el objetivo de resolver la incertidumbre y aumentar la seguridad, lo que implico desarrollar un prototipo de sistema de reconocimiento facial para personas que viven cerca de residencias familiares, esto se debe a que la seguridad del hogar se ha convertido en un tema importante para tener en cuenta, ya que permite controlar los eventos internos y el comportamiento de las personas. Y como resultado, fue posible ver en base al estudio que se realizó, que el 100% de las nuevas tecnologías implementadas en las áreas de reconocimiento facial de videovigilancia mejoraron la seguridad y monitoreo en la mayoría de los hogares.

Para Pazmiño (2022) en su trabajo de investigación "Implementación de sistema de CCTV con cámaras IP en las sucursales de una empresa farmacéutica a nivel nacional" que tuvo como objetivo implementar un sistema circuito cerrado de televisión en varias sucursales de una empresa farmacéutica a nivel nacional,

> En donde con este trabajo pretenden brindar mayor seguridad a los empleados que colaboran en estas instalaciones y ejercer un mayor control sobre la mercadería contenidas en los cuartos de la empresa, se procedió a establecer los estándares de calidad y normas de cableado estructurado para su correcta instalación del cableado UTP, además de hacer uso de las recomendaciones de los fabricantes de cámaras y sistema de grabación. El resultado es una funcionalidad óptima del sistema y un control de punto ciego, de esta forma se crea un sistema de videovigilancia fiable y seguro. Para Baque (2019) en su proyecto de titulación con tema "Implementación de un sistema de video vigilancia mediante cámaras IP para el fortalecimiento de la seguridad en la parte posterior de la edificación de la carrera ingeniería en computación y redes",
>
> En este proyecto de investigación, el objetivo de investigación es diseñar un sistema de videovigilancia que permita la monitorización continua, así como configurarlo mediante comunicación con enlaces de microondas para la introducción de tecnologías de imagen, diseñado para monitorizar diversos entornos interiores y exteriores de las

> instalaciones. Además de la capacidad de definir el diseño de sistemas, utilizando enfoques cualitativos, descriptivos y bibliográficos para lograr los objetivos establecidos, las pautas de investigación brindan niveles de decisión para la investigación propuesta para el proyecto.

Para Pastuña y Viteri (2021) en su proyecto de investigación "Implementación de un sistema de circuito cerrado mediante IP, para mejorar los procesos de video vigilancia en el bloque b de la Universidad Técnica de Cotopaxi extensión la maná",

> Al momento de implementar el proyecto de sistema de video vigilancia y monitoreo, es conveniente investigar los eventos y sucesos que se desarrollan en el entorno universitario para controlar la seguridad, de modo que los usuarios puedan visualizar de manera segura de las imágenes de vigilancia desde cualquier lugar, en el coso de esta investigación la cual se encuentra en el bloque B de la universidad, con la ayuda de la investigación de campo se cubrirá de manera más efectiva todo el perímetro del bloque B con una configuración precisa de los equipos de red en una arquitectura que permita el control de todas las ubicaciones necesarias y el despliegue de todo el proyecto de red para almacenar todas las imágenes de video generadas en los dispositivos de grabación, que es generada por el sistema de videovigilancia

2.2 MARCO TEÓRICO

La seguridad ayuda a tener orden en la sociedad y llevar una vida tranquila, es así como desde los años ochenta se han desarrollado e implementado los sistemas de video vigilancia que se caracterizan por brindar seguridad en lugares públicos, personas y sus bienes materiales, de manera similar se utiliza para guardar las imágenes y videos capturados por cámaras y software de vigilancia permiten a los usuarios ver imágenes en tiempo real o más tarde.

2.2.1 Estándares de calidad en video vigilancia

IEE es un proyecto que está integrado por estándares de calidad que abarcan distintos medios tecnológicos y puedan trabajar juntos, así es el estándar 802 el cual está encargado de brindar información del cableado físico y transmisión de datos. Es importante tener en cuenta que los estándares de la IEEE son voluntarios y no son obligatorios para la implementación de sistemas de videovigilancia, por lo tanto, cumplir con estos estándares puede mejorar la interoperabilidad y la seguridad de los sistemas

Según el Estándar IEEE (2017) indica que los estándares:

IEEE 802.1X

El estándar aborda la autenticación de dispositivos en la red, lo cual es importante para garantizar que solo los dispositivos autorizados puedan acceder a las redes de CCTV

EEE 802.2

Control de enlace lógico LLC ("Logical Link Control") define la forma en que se transmiten los datos en el medio físico y proporciona servicios a las capas superiores

Según IEEE (2022) afirma que el estándar **IEEE 802.3** o con;

El nombre correcto para esta tecnología es IEEE 802.3 CSMA/CD, pero casi siempre es referido como Ethernet está diseñado de tal manera que no puede enviar mucha información a la vez, el objetivo es que no se pierda información y está controlado por un sistema llamado CSMA/CD Detección de Portadora con Acceso Múltiple y Detección de Colisiones y la cual está diseñada para que una estación emisora pueda enviar su información y receptora debe percibir esa señal para transmitirla en el sistema de video vigilancia

- **IEEE 802.3af-2003:** Este estándar establece las especificaciones para Power over Ethernet (PoE), que permite alimentar dispositivos de red a través de del cable Ethernet
- **IEEE 802.3at-2009:** Esta norma es una extensión de la norma 802.3af y establece especificaciones para el suministro de energía eléctrica a dispositivos de red que requieren una mayor potencia, como cámaras de vídeo de alta definición y sistemas de CCTV

Según Estándar IEEE (2017) afirma que:

IEEE 802.7

Este estándar es diseñado para crear una red de área local conectada cable coaxial además de ser más utilizada por todas las empresas de internet por cable ya que su ancho de banda para transferir datos, imágenes y sonido al servidor el cual procesa toda la información al sistema de vigilancia,

- Proporcionar información en forma analógica
- Establece señales por medio del cable
- Se prepara la señal (AM o FM)

- Envió en banda dividida de diferentes señales para conseguir canales de transmisión

IEEE 802.8

Es un conjunto de normas para trabajar con fibra óptica y dar soporte a esta misma además de tener un diseño diferente a redes con cable de cobre, por su mejor velocidad usando tokens y así aumentando sus capacidades de transmisión de información

Estándar 802.9

Este estándar establece un servicio de flujo multiplexado que lleva canales para voz y datos sobre redes de control de acceso a medios (MAC), incluidos nodos informáticos y códecs de video, el trabajo del grupo (IEEE, 2022) son los sigui3entes:

- Desarrollar un sistema que integre voz y datos con una interfaz que pueda regular el acceso al medio y admitir todos sus muchos límites compatibles con el estándar 802
- Prestar atención al uso de cable como opción principal para la distribución debido a las transferencias de cable en el ancho de banda.

IEEE 802.10

El estándar 802.10 brinda especificaciones para administrar la seguridad junto con el almacenamiento de los videos para que no sean vulnerables. Es un estándar de control de acceso para funciones de seguridad, integridad que podría usarse en redes de área local y redes de área metropolitana amplia.

Según Parsons (2022) asegura que los estándares:

IEEE 802.11

Este estándar especifica las características técnicas de las redes inalámbricas de muchos sistemas de videovigilancia utilizan redes inalámbricas para conectar cámaras y dispositivos, por lo que este estándar es relevante para asegurando la compatibilidad y la interoperabilidad de los dispositivos.

IEEE 1599

Este estándar especifica un formato para transmisión de audio y video basado en IP. Es especialmente importante para la transmisión de video en sistemas de videovigilancia basados en IP.

IEEE P1858

Este estándar se centra en la interoperabilidad entre diferentes sistemas de videovigilancia, lo que es importante para permitir que los usuarios combinen y utilicen diferentes dispositivos y sistemas de diferentes fabricantes.

2.2.1.1. Estándares de calidad en cableado estructurado

Un sistema de cableado estructurado consiste en una serie de elementos de cableado inerte que enlazan dispositivos activos y un sistema de gestión en una ubicación determinada, su finalidad es brindar servicios de audio, datos y video. El sistema de cableado estructurado para la vigilancia por vídeo se sujeta a normas internacionales que recomiendan mejores prácticas de instalación para lograr un sistema eficiente y seguro. (Pazmiño, 2019, pág. 6)

Estándar ANSI-TIA-EIA: 568-B

Esta norma específica los requisitos mínimos para los componentes de fibra óptica utilizados en el cableado de edificios como universidades, como cables, conectores, latiguillos, latiguillos y equipos de prueba. También define los tipos de elementos de fibra óptica, como mono modos y multimodos de 62,5/125 um y 50/125 um. La fibra de 62,5/125 um tiene un ancho de banda de 160/500 MHz/km, mientras que la fibra de 50/125 um tiene un ancho de banda de 500/500 MHz/km y una atenuación de 3,5/1,5 dB/Km para las longitudes de 8050/13050/130500 nm. (Dianca A, 2019).

Estándar ISO/IEC 11801

Pantoja, Pinzón y Roa (2021) afirman que esta norma establece que se la utiliza como requisito en redes de telecomunicaciones y diseño de cableado estructurado con sus componentes, y la topología de la capa física en los sistemas de control además de cumplir con la garantía de los protocolos propuestos en las TICS, este estándar fue diseñado para cubrir 3km de distancia como también trabajar a velocidades de hasta 1000 Mbps en conexiones entre diferentes edificios en un campus (p.20).

ANSI-TIA-EIA: 569-B (Normas de canalizaciones para telecomunicaciones)

Según Pazmiño (2019) el estándar establece las pautas para la dirección en la que se debe colocar un cable, también conocido como enrutamiento o canalización. De acuerdo con este estándar, los dispositivos de enrutamiento como canaletas, tuberías o bandejas pueden ser instalados conforme a la estructura del edificio o la zona, asimismo,

proporciona las instrucciones para la instalación adecuada de tuberías, los ángulos máximos a los que se pueden doblar los cables y otros requisitos esenciales para garantizar una infraestructura bien instalada. Según este estándar, las rutas en los edificios deben ser planificadas de manera que permitan futuros cambios y expansiones, por lo tanto, es crucial verificar la ruta diseñada antes de proceder con la instalación. (p.48)

ANSI-TIA-EIA: 606-A (Normas de administración de infraestructura de telecomunicaciones)

> Las etiquetas, registros, informes, planos, gráficos, órdenes de trabajo y actas de entrega y recepción se elaboran de conformidad con el estándar para asegurar la identificación adecuada del sistema, cada elemento debe contar con su propia etiqueta, ya sea un panel de conexiones, un rack o un punto de usuario final. Los registros contienen detalles sobre los elementos instalados, como el nombre del cable, la ruta o ubicación, el número de serie o modelo de tal manera que los planos representan las distintas etapas de planificación e instalación del sistema, incluyendo la ubicación y dimensiones de las rutas, espacios y equipos finales, como cámaras de red, sistemas biométricos y puntos de red, todos debidamente identificados. Las órdenes de trabajo y actas son documentos que describen las actividades llevadas a cabo durante la instalación del sistema. (Pazmiño, 2019, pág. 48)

Protocolo ONVIF (Foro abierto de interfaz de video en red)

Existen varias contradicciones en la comunicación IP, donde intervienen más dispositivos de diferentes marcas, para esto ONVIF creó un estándar de comunicación entre diferentes dispositivos de diferentes fabricantes, para conectar productos de seguridad física basados en IP además de integración de video de diferentes marcas dispositivos en línea de manera más fácil y automática. (NIVIAN, 2019).

2.2.2 Políticas de seguridad de la información

Las políticas de seguridad de la información se crearon para cumplir con los requisitos legales que se agregaron a los circuitos cerrados de televisión (CCTV) para vigilar el espacio público y aumentar el control social. La norma ISO/IEC 27000 es un marco de gestión de la seguridad proporcionado por un conjunto de estándares de calidad en seguridad que se han desarrollado o están en proceso de desarrollo.

Según Contero (2019) manifiesta que la:

Norma ISO 17799

El estándar ISO/IEC 27000 es un marco para administrar la seguridad proporcionado por una colección de estándares de seguridad que se han desarrollado o están en proceso de desarrollo

Norma ISO 27001:2013

Esta norma usa un modelo para proteger la creación, integridad, mantenimiento y mejora de un sistema de gestión de seguridad de la información de una empresa.

ISO/IEC 27002

Es un código de buenas prácticas para gestionar la seguridad de la información

Norma ISO / IEC 27033-1

Esta norma involucra la orientación de como identificar, analizar la seguridad de la red, el uso la planificación y la implementación de la red

Norma ISO 27005

Gestión de riesgos de seguridad de la información que puedan comprometer a las organizaciones

2.2.3. Sistema de video vigilancia

2.2.3.1. Definición

Durante los últimos diez años, los sistemas de videovigilancia se han vuelto muy populares en empresas y hogares que solicitan este servicio para observar una escena, esto se debe a que pueden instalarse en lugares internos o externos y brindar al usuario un control sobre el área que quiere monitorear. En los últimos años, los sistemas de videovigilancia se han vuelto muy populares en hogares y empresas que solicitan este servicio para observar una escena, estos sistemas tienen un efecto persuasivo porque evitan cualquier acto antisocial. (Pastuña & Viteri, 2021, pág. 16)

Los sistemas de videovigilancia son herramientas de supervisión disponibles las 24 horas del día y los 365 días del año mediante medios tecnológicos como cámaras analógicas o digitales, servidores, medios de transmisión corta y Wifi. Los sistemas de videovigilancia también son sistemas de seguridad que utilizan cámaras de video y otros dispositivos para supervisar y grabar áreas específicas para prevenir el delito y garantizar la seguridad, estos sistemas se utilizan con frecuencia en lugares públicos y privados, como tiendas, centros comerciales,

estacionamientos, edificios de oficinas, hospitales, aeropuertos, estadios deportivos y otras áreas.

Ventajas de las redes de video vigilancia

Hoy en día, las redes IP brindan flexibilidad y rentabilidad para las comunicaciones de tal modo que este es el alcance del video, incluida la facultad de extender la red para un sistema de conexiones de red muy estable, por lo tanto, estas redes tienen las siguientes ventajas según (Echeverría, 2020) que son aceptadas:

- Habilidad para utilizar video cámaras de resolución alta. Consistencia de la imagen independientemente de la distancia.
- Habilidad para usar Power over Ethernet.
- Configuración remota de cámaras vía IP.
- Flexibilidad y escalabilidad generales

2.2.3.2. Topologías de red.

Se representa geométricamente entre enlaces y dispositivos interconectados en sus nodos (Chaglla & Villa, 2021) lo que confirma que las redes tienen la facilidad de detallarse por la ubicación y conectividad de estos nodos se puede clasificar como:

a) **Topología de bus.**

   Esta topología geométrica se aplica a todos los nodos conectados directamente al enlace, si no hay otra conexión entrenada, así todos los dispositivos de la red ahora pueden ver todas las señales gracias a esta tecnología y así recibir esta información. (Chaglla & Villa, 2021)

b) **Topología en estrella.**

   En esta topología, las redes se conectan directamente al servidor y, además, su comunicación necesariamente debe realizarse a través de él, se conectan por separado y está diseñado para facilitar el acompañamiento y la gestión de los datos como se usa en la UPEC (Chaglla & Villa, 2021)

c) **Topología en anillo**

   En esta topología, las redes LAN están conectadas en forma de anillo, porque cada una está conectada con la siguiente, y la del final está conectada con la primera. Cada conexión realizada está diseñada para pasar por un repetidor. comunicación con la siguiente estación en el círculo y proporcione una identificación de testigo que pueda transmitir paquetes de datos. (Chaglla & Villa, 2021)

d) Topología jerárquica.

En esta topología los nodos se localizan de manera distribuida y consta de un nodo denominado nodo maestro. Solo la parte de la red que está directamente debajo del nodo que falla se ve afectada por una falla de nodo.

2.2.3.3. Sistemas

a) CCTV Analógicos

En el mercado actual según Jalca (2019) los circuitos cerrados de televisión analógicos, los grabadores y las cámaras analógicos, entre otros elementos analógicos, se utilizan más comúnmente porque son sistemas tradicionales y funcionan de manera independiente, los elementos analógicos están disponibles de varios fabricantes y en una amplia gama. Las cámaras analógicas tienen salidas de video compuesto que se conectan a través de un cableado únicamente utilizado para visualizar las imágenes de las cámaras conectadas. (p.26)

b) CCTV Híbridos

Es un avance tecnológico en comparación con el circuito cerrado de televisión analógico que utiliza cable las instalaciones existentes para cámaras HD e IP bajo una grabadora y reproductor de video dependiendo de las necesidades específicas y especiales de cada cliente, esta puede ser una buena elección (Jalca, 2019, pág. 27)

c) CCTV IP

indica que el sistema CCTV IP es un sistema moderno ya que los datos y la información de la calidad de video grabación que proporcionan se transfieren a través de un cable FTP del mismo modo también se lo conoce por sistema de direccionamiento porque cada elemento funciona de forma independiente no necesita una grabadora (Jalca, 2019, pág. 27).

2.2.3.4. Protocolos para la transmisión de video IP

Los protocolos de transmisión son un conjunto de normas establecidas entre dispositivos para que los datos puedan ser enviados a través de Internet, permitiendo una comunicación eficiente entre diferentes terminales y utilizando IP, soporta dos protocolos TCP (Transmission Control Protocol) y UDP (User Datagram Protocol) para garantizar que los datos se transmitan

Según Abril y Cuzco (2019) afirman que los protocolos son los siguientes:

FTP (protocolo de transferencia de archivos)

Podemos enviar imágenes o videos desde una cámara IP a un servidor de video para una aplicación usando el protocolo FTP.

SMTP (protocolo simple de transferencia de correo)

El protocolo de transferencia simple de correo utiliza imágenes adjuntas en mensajes de correo electrónico y notifica a los clientes con alertas para enviar mensajes de correo electrónico.

HTTPS (protocolo seguro de transferencia de hipertexto)

El protocolo fue creado para realizar la transmisión segura de información a través de internet mediante encriptación, se utiliza en cámaras IP para transmitir video desde dispositivos, utiliza autenticación para transmitir información desde cámaras certificadas No. X.509

SSL (capa de sockets seguros)

Este protocolo se lo usa para tener blindadas las conexiones que se establecen así mismo es muy importante para tener un sitio seguro ante cualquier ataque ya que el protocolo nos brinda un certificado de seguridad con un cifrado para dar seguridad a los clientes

RTSP (protocolo de transmisión en tiempo real)

Es un protocolo que ayuda a transmitir video o audio sobre UDP o TCP y podemos controlar de forma remota cualquier dispositivo compatible en él, este protocolo es muy utilizado en servidores multimedia y gestión de cámaras IP (p.11).

2.2.4. Equipos tecnológicos del sistema de video vigilancia

2.2.4.1. Cámaras IP

Según Chaglla y Villa (2021) deduce que en los sistemas de video vigilancia las cámaras IP se clasifican dependiendo su función y su ubicación o si serán ubicadas en interiores o exteriores para poder regular su funcionamiento en distintos sectores (p.35)

a) **Cámaras fijas Hikvision**

   Estos son dispositivos de grabación convencionales que ofrecen discreción, poseen un ángulo de visión ajustable y son muy sencillos de instalar. Además, proporcionan una excelente calidad de imagen de 1080 grados con una gran visibilidad además son muy fáciles de ocultar con una fuente de alimentación de 12 voltios.

b) **Cámaras domo fijas**

Es una cámara fija que se puede instalar en cualquier lugar con su carcasa, la cámara enfoca imperceptiblemente en cualquier dirección, además es difícil saber en qué dirección apunta la cámara, por lo que es ideal para vigilancia y monitoreo.

c) Cámaras PTZ

Las cámaras con capacidades PTZ (Pan, Tilt y Zoom) se pueden mover vertical u horizontalmente, y el zoom se puede ajustar de forma automática o manual, las funciones anteriores pueden ser realizadas por cámaras PTZ digitales sin necesidad de conexiones adicionales, y la transmisión de video y la transmisión de comandos se envían a través del cable de red.

2.2.4.1.1 Equipos POE inyector para cámaras IP

FS Community (2022) dice que un equipo de alimentación a través de internet brinda energía y datos simultáneamente compatibles mediante un solo cable CATx por el motivo de que son para dispositivos de baja potencia además de brindar mayor flexibilidad contando con el estándar de IEEE 802.3 que da la adecuada potencia para alimentar la poeticidad de las cámaras de seguridad y reduciendo al mínimo el impacto de la infraestructura así mismo añadirle su fácil instalación (Medium, 2019)

2.2.4.2. Medio de transmisión de video

En la transmisión de datos hay diferentes tipos de cableados las cuales están sujetas a las diversas topologías de red ya que se apoyan en el ancho de banda implantado para obtener la productividad de transmisión, y no tener presencia de pérdida de señal en las instalaciones de cableado en los diferentes entornos en los que se plantee la infraestructura

Cable par trenzado: este tipo de cableado hoy en día es el más utilizado es distintos circuitos por tener conductores eléctricos aislados y entrelazados que son más utilizados en las telecomunicaciones, este está compuesto por ocho cables formando cuatro pares de hilos trenzado, en Ethernet su cobertura máxima es de 100 metros de 10 Mbps que es de cuatro pares de hilos en 1000 Mbps y 10,000 Mbps con su conector RJ45 utilizando la certificación UTP (Unshielded Twisted Pair) de par trenzado que contiene las siguientes categorías 5, 5e, 6, 7 y 8 que son utilizadas en los últimos años según (Bazurto & Jaramillo, 2020, pág. 30)

Categoría 6: se emplea en redes de infraestructura en telecomunicaciones creando una red de área local (LAN), esta cumple con el estándar ANSI/TIA/EIA 568-B.2-1, ISO/IEC 11801 similares a la de la categoría 5e, la norma en la categoría 6 usa 250mhz

además de llevar señales telefónicas también consta con cable LSHF para aumentar el rendimiento del cableado (Bazurto & Jaramillo, 2020).

Fibra Óptica: La Fibra Óptica es el medio de comunicación más utilizado en redes debido a sus propiedades intrínsecas como ser un material transparente y tener una pérdida de señal baja.

Según (Chaglla & Villa, 2021), tiene varias características útiles, por ejemplo,

Mayor longitud. La fibra óptica también mejora la seguridad ya que no induce ningún sellado y es resistente a la radiación externa, por lo que no puede ser captada ni deformada por inducción o contacto superficial. Cualquier cambio a un F.O. da como resultado un aumento significativo en la atenuación, haciéndolo fácilmente identificable.

Aumento de seguridad. La fibra no produce señales y es resistente a la radiación externa, por lo tanto, es imposible capturar o distorsionar los sellos por inducción contacto superficial, etc. Cualquier acción sobre un F.O. da como resultado un aumento notable en la atenuación, lo que hace que la acción sea fácilmente reconocible.

Incremento de la calidad de la imagen. Incluso en lugares expuestos a intensas radiaciones electromagnéticas, tormentas atmosféricas u otros fenómenos similares, la calidad de la imagen permanece en un nivel óptimo.

Mayor duración del cableado. En comparación con el cable coaxial, permite una mayor longitud en cada enlace cámara-monitor sin necesidad de repetidores, además, si se elige el cable de fibra óptica adecuado, el tendido y la conexión de los extremos son relativamente sencillos y tienen un grado de dificultad similar al del cable eléctrico.

Fiabilidad. La fibra óptica ofrece ventajas adicionales, como su prolongada vida útil debido a la ausencia de componentes susceptibles de deteriorarse por la acción del tiempo o la oxidación. Además, su fiabilidad se sustenta en su resistencia a las interferencias electromagnéticas, su constante estabilidad a lo largo del tiempo y su capacidad de ser inaccesible. Incluso en situaciones de incendio, se puede mantener la supervisión en la zona afectada.

Sencillez del cableado. Utilizar un solo cable para controlar el movimiento de la cámara y transmitir la señal de video reduce el número de cables a tender (p.39)

2.2.4.3. Monitores

Los monitores ayudan al personal de vigilancia a monitorear las localidades al visualizar los videos que emiten las cámaras. Con el avance de la tecnología, hoy en día se puede monitorear de forma remota en dispositivos conectados a Internet como smartphones, Tablet, SmarTv, además es importante que los monitores estén conectados a un sistema de grabación de video para poder revisar las grabaciones en caso de ser de uso. También es recomendable usar monitores de respaldo en caso de que alguno de los monitores principales falle, así mismo otro aspecto a considerar en los monitores para sistemas de videovigilancia es la resistencia y durabilidad, especialmente si se van a instalar en áreas exteriores o en lugares donde puedan ser expuestos a factores ambientales adversos como polvo, humedad o cambios de temperatura, por lo tanto es importante seleccionar monitores que estén diseñados para su uso en sistemas de videovigilancia y que tengan una buena garantía (Pazmiño, 2019, pág. 7)

2.2.4.4. Sistema de circuito cerrado de TV

Un sistema de circuito cerrado de TV (CCTV) es también conocido como videovigilancia este sistema se basa en la ubicación estratégica de las cámaras, monitores y grabadoras de vídeo que se comunican a través de cable para tener un enlace y así tener una transmisión de datos al sistema de video vigilancia, en el sistema CCTV envía los datos a los discos de almacenamiento para procesar los vídeos emitidos por las cámaras por lo tanto, un sistema de circuito cerrado de televisión (CCTV, por sus siglas en inglés) es un sistema de vigilancia que utiliza cámaras de video para capturar imágenes y enviarlas a un sistema centralizado de monitoreo o grabación. El sistema se llama "cerrado" porque las imágenes se transmiten solo a un número limitado de monitores o dispositivos de grabación, en lugar de ser transmitidas públicamente como en una transmisión de televisión abierta de la misma manera los sistemas de CCTV suelen utilizarse para la seguridad y la vigilancia en lugares públicos y privados, como tiendas, edificios de oficinas, aeropuertos, estacionamientos, calles y hogares. Los componentes típicos de un sistema de CCTV incluyen cámaras, dispositivos de grabación, monitores, cables y software de gestión de video. (Sivtec, 2019)

2.2.4.5 Switch Catalyst 2960

> Según la empresa CISCO (2021) afirma que los equipos switches 2960X y 2960xr facilitan la integración, configuración de los conmutadores del mismo modo la administración de redes además de mejorar la funcionalidad de la capa 2 y capa 3 con 24 puertos Gigabit Ethernet contando con 4 enlaces ascendentes fijos al mismo tiempo

una administración con interfaz de usuario web simple con visualización de topología de igual manera un protocolo de enrutamiento estático y RIP con estándar 802.1 al mismo modo una asignación de VLAN basada en MAC comprender el tráfico en la red e identificar anomalías en paquetes específicos visibilidad de dominio como fuente autorizada y usando una fuente de alimentación estática y la posibilidad de poner una fuente redundante con un conjunto de funciones cisco IOS IP Lite.

2.2.4.6 Servidor HPE (Hewlett Packard Enterprise) Proliant dl360 gen10

Este hardware según (Hewlett Packard Enterprise, 2023) entrega seguridad y desempeño en cualquier centro de datos, escalando con procesadores Intel Xeon con DDR4 (velocidad de datos doble de 4ta generación) HPE SmartMemory 2933 MT/s (millones de transferencias por segundo), con ganancias de rendimiento de hardware de hasta 192 GB por sistema y la capacidad de albergar hasta 12 NVDIMM (módulos de memoria no volátil) por chasis para aumentar la resistencia de la memoria, así como la capacidad de control, así mismo la comprobación de firmware en tiempo de ejecución para comprobar el firmware del servidor cada 24 horas verificando su actualización y confiabilidad para facilitar el mantenimiento del servidor mediante la automatización de tareas críticas en el ciclo de vida del servidor

2.2.4.7 Router Cisco 4300

El enrutador de servicios integrados Cisco 4300 proporciona un ancho de banda de 100 Mbps a 300 Mbps y cuenta con una ranura de módulo de servicio mejorado (SM-X) que admite módulos de servicio de ancho simple y doble, lo que brinda flexibilidad en las opciones de implementación múltiples niveles de rendimiento de 35 Mbps a 2 Gigabyte por segundo (SENYDA, 2018) del mismo modo este modelo tienen OIR (inserción y extracción en línea) para PTT también aumenta drásticamente la memoria RAM máxima (hasta 16 GB en algunos modelos) así mismo el mismo modelo, conjunto de características de licencias de software IOS que el ISR G2 anterior (Mercado IT, 2020).

2.2.5. DVR, NVR e Híbridos

Servidor de video

Conecta varias cámaras de vigilancia digitales utilizadas en los sistemas de circuito cerrado de TV en un sistema de video vigilancia IP para el almacenamiento y gestión de video del mismo modo el servidor de video puede ser un equipo físico o una aplicación de software instalada en

un ordenador. También puede estar alojado en la nube y ofrecer servicios de almacenamiento y acceso remoto. Además del almacenamiento, el servidor de video también puede realizar otras funciones, como la administración de cámaras, la configuración de alertas y la gestión de usuarios y permisos.

Servidor multimedia

Un DVR (Grabador de Video Digital) es un equipo que posee hardware propietario y software para la gestión de video preinstalado, en donde realiza en proceso de entregar contenido multimedia a través de la red es así que (Cuesta, 2021, pág. 24) dice que le permite la administración del video con su almacenamiento desde el codificador del video o desde las cámaras de video debido a esto es considerado como popular en los sistemas pequeños de 4 a 16 cámaras por su fácil instalación

Según Cuesta (2021) un NVR se conecta a la red de cámaras IP y se utiliza para grabar y almacenar las imágenes de video de las cámaras. El NVR también puede ser utilizado para gestionar y configurar las cámaras, así como para permitir el acceso remoto a las imágenes de video, por lo tanto, el NVR pueden variar en términos de capacidad de almacenamiento, número de canales de video que pueden grabar simultáneamente, resolución máxima de grabación, y otras características como la capacidad de reproducir las grabaciones y videos en tiempo real o de recibir alertas en tiempo real.

2.2.5.3 Disco duro WD Purple 1.2TB

Según Western Digital (2019) los discos duros WD son construidos para el sistema de seguridad HD siempre funcionan las 24 horas, 7 días a la semanas para reducir errores y pixelado también admite tasas de carga de trabajo de hasta 180 TB al año con 64 cámaras que pueden estar en el sistemas de seguridad confiables además de estar optimizadas para el sistema de almacenamiento así también los discos duros WD Purple de 8 TB, 10 TB, 12 TB, 14 TB y 18 TB están diseñados para análisis de aprendizaje profundo para admitir sistemas NVR inteligentes con tasas de carga de trabajo mejoradas de hasta 360 TB al año y hasta 16 canales de IA para análisis en el sistema

2.2.5.4 Fuente de alimentación

Según Mejía, J. (2019) es un circuito que funciona con un valor de tención alterna y convertirla a continua para poder encender cualquier tipo de dispositivo por varias etapas que son transformación, rectificación y regulación para poder dar el correcto amperaje al equipo NVR que se va a encontrar conectado por largos periodos de tiempo (P.2).

2.2.6 Software Libre

El software libre tiene como objetivo adecuar herramientas para su libre uso y ser ejecutadas por los usuarios por su gran compatibilidad en aplicaciones en diferentes sistemas informáticos y representa libertad así mismo presentar grandes beneficios para quien los usan esto representa una gran ayuda de forma económica e intelectual por ser código abierto a las personas, empresas y compañías además de contar con seguridad informática debido a esto tiene un mayor respaldo para trabajar con el de este modo se puede ejecutar programas para cualquier propósito de tal modo que se distribuye, copia y mejora el software que permita el acceso de código fuente es indispensable para poder mejorar los programas

2.2.6.1 Ubuntu

> Este sistema operativo de código abierto se caracteriza por ser robusto y gratuito, ya que está basado en Debian es así como su principal enfoque es en la facilidad de uso para la comunidad, sin generar conflictos en los equipos. Además, se ofrece un sistema actualizado y estable de código abierto, con una mayor cantidad de paquetes de software que soportan arquitecturas Intel, AMD y Apple. Este sistema es adaptable a las necesidades de cada usuario e incluye paquetes GNOME para diversas aplicaciones de escritorio, programación e internet, con el objetivo de que Ubuntu pueda ser utilizado por el mayor número de personas posible. (Jinez & Pantoja, 2020, pág. 23)

2.2.6.2 Motion

> Es uno de los programas más comunes para detectar movimientos, destacando por su velocidad y fiabilidad, algunas de sus funciones incluyen la capacidad de modificar el nivel de sensibilidad y generar imágenes que resalten únicamente los píxeles activados durante la detección de movimiento, del mismo modo también es uno de los softwares de detección de movimiento más populares, con soporte para múltiples eventos de cámara que pueden ocurrir de la misma manera una secuencia de comandos al monitorear las señales de video de todas las cámaras y puede detectar si partes importantes de la imagen han cambiado o no (Abril & Cuzco, 2019, pág. 17)

2.2.6.3 MotionEyesOs

> Según Abril, B., y Cuzco, P., (2019) deducen que es un software libre que usa interfaz de usuario basada en web, móvil es adaptable a la mayoría de las cámaras así mismo detección de movimiento con sus notificaciones tipo de archivos JPEG con una fácil administración para monitorear las cámaras IP y estabilidad del sistema al mismo

tiempo cuenta con distribución de Linux para computadoras de placa reducida como RaspBerry pi que le atribuye en un sistema de videovigilancia así como su sistema operativo se basa en BuildRoot y utiliza Motion como Backend y Motion Eyeos como interfaz de usuario web con funciones editables (p.17).

2.2.6.4 Shinobi CCTV

Este es un software Open Source que funciona como servidor de video vigilancia que contiene código fuente Node.js con una interfaz muy fácil de utilizar obteniendo un gran rendimiento así mismo es un servidor multiplataforma que soporta cualquier tipo de cámara con distintos tipos de formatos de grabación además de regrabar, reproducir audio, video detectar movimiento incluyendo asignar el almacenamiento de cada cámara, así mismo esta plataforma tiene la capacidad de registrar secuencias de audio y video utilizando formatos de grabaciones compatibles con los ajustes de hardware por lo tanto, hay tres opciones de grabación distintas: grabación continua, grabación durante eventos y grabación seguida de eliminación si no se detecta ningún evento. Es así como crea una solución de grabación de video fácil de usar de la misma manera se requiere autenticación de nombre de usuario y contraseña, y hay diferentes niveles de usuarios que restringen los privilegios por otra parte al ingresar a la interfaz de configuración, se puede acceder a las grabaciones de las cámaras así que se puede visualizar las secuencias y grabaciones en un dispositivo móvil a través de un navegador web sin necesidad de instalar una aplicación específica (Echeverría, 2020, pág. 76).

Ventajas de Shinobi CCTV:

- Posibilidad de detección de movimiento y análisis de patrones.
- Admite audio y video.
- Permite visualizar varias cámaras en la interfaz web.
- Ofrece varios formatos de grabación, incluyendo resoluciones 4K.
- Se puede definir el almacenamiento para cada cámara.
- Cuenta con una API potente para integración con otras aplicaciones.
- Permite transmitir flujos de video en múltiples formatos compatibles con protocolos HTTP y Websocket para optimizar el ancho de banda.
- Utiliza tráfico Multicast para mejorar el ancho de banda.
- Admite HTTPS.
- Compatible con el protocolo MQTT.
- Permite controlar cámaras PTZ.

- Incluye un calendario de eventos para cada cámara.
- Se puede acceder mediante interfaz web sin necesidad de una aplicación.
- Compatible con dispositivos móviles.
- Ofrece un servicio de almacenamiento en la nube (Google Drive, Dropbox).
- No tiene límite en cuanto a la cantidad de cámaras que se pueden integrar, ya que Shinobi CCTV ejecuta cada cámara como un proceso independiente. La cantidad de cámaras está limitada por la capacidad del hardware del sistema.

Limitaciones actuales de Shinobi CCTV:

- La línea de tiempo de Shinobi se basa en puntos fijos sin una imagen de vista previa, por lo que para ver lo que sucedió entre dos puntos, es necesario ver el video vinculado.
- La detección de movimiento es más difícil de configurar en comparación con otros softwares de gestión de video.

2.2.6.5 Pfense

En el trabajo de investigación de (Gerra, 2019) deduce que es un producto diseñado para las necesidades del laboratorio ya que está basado en FreeBSD (sistema completamente gratuito), Pfsense usa Linux, que al estar ejecutándose en este sistema operativo brindara más seguridad, es considerado uno de los mejores del mundo ya que tiene características que permiten filtrar el tráfico TCP/IP así mismo tener un adecuado controlar en el tráfico de ancho de banda y gráficos, permite realizar ajustes de VPN, crea interfaces, y puertos fijos en términos de seguridad analiza, detecta y bloquea continuamente a personas no autorizadas además tiene incluida una lista extensa de paquetes extensibles y no poner en riesgo todas las funciones sin comprometer la seguridad de la red o del sistema (p.61).

2.2.6.6 Open VPN (Red privada virtual)

Según Sánchez, E. (2017) es un software libre SSL que está diseñado para la construcción de redes privadas virtuales punto a punto que conecta a los usuarios por medio de validación a un host conectados remotamente dando acceso a una interfaz de red virtual en el servidor VPN y sus clientes además de contemplar la opción de conectarse por túneles a nivel de IP y Ethernet permitiendo abrir redes y firewalls específicos contando con flexibilidad en secuencias de comando para tener un NAT(Traducción de direcciones de red) sin problemas teniendo un mayor rango de seguridad (p.45).

2.2.6.8 Base de datos (MariaDB)

Sistema de vigilancia Shinobi CCTV utiliza MariaDB como su sistema de base de datos, ya que permite administrar, almacenar y recuperar información de una base de datos, así como administrar usuarios y recuperar información en caso de fallas del sistema. MariaDB tiene la capacidad de administrar datos relacionales entre varios usuarios y plataformas de hardware, lo que la convierte en una herramienta comercial muy útil, teniendo en cuenta que MariaDB es una de las mejores opciones para los sistemas de gestión de bases de datos de código abierto (Echeverría, 2020), además de incorporar mejoras de rendimiento y seguridad sobre MySQL, el desarrollador de Shinobi CCTV optó por utilizarlo como sistema de gestión de bases de datos para su proyecto. Por ello, debido a estas características el desarrollador de Shinobi CCTV ha determinado que MariaDB es la mejor opción

III. METODOLOGÍA

3.1. ENFOQUE METODOLÓGICO

La metodología es esencial para el desarrollo de proyectos que usa un conjunto de técnicas, instrumentos y procesos utilizados para investigar y examinar un determinado tema o problema con el fin de responder a una pregunta de investigación de la misma manera es un plan completo que se utiliza para guiar todo el procedimiento de investigación para asegurar la validez y confiabilidad de los resultados obtenidos.

Según Niño (2011) busca profundizar en la metodología de investigación y los tipos de fundamentos, técnicas e instrumentos o solo recolección de información, dicho de otro modo, crea la actividad cognoscitiva para realizar un plan detallado que se utiliza para guiar todo el proceso de investigación como el desarrollo del tema y problema propuesto

3.1.1. Enfoque de investigación

En el presente proyecto de investigación se utilizará el enfoque de carácter cualitativo, de diseño de estudio de caso ya que toma como investigación básica diagnosticar como se llevan los estándares de calidad en el sistema de video vigilancia de los laboratorios de la UPEC, además se realizarán observaciones en diferentes áreas de la universidad para obtener una visión completa de cómo se utilizan los sistemas de videovigilancia en la práctica, luego se llevó a cabo entrevistas y encuestas con diversos miembros de la comunidad universitaria, incluyendo profesores y personal administrativo, para comprender cómo se encuentran los sistemas de videovigilancia y cómo influyen en su sensación de seguridad y privacidad (Niño, 2011)

3.1.2. Tipo de Investigación

3.1.2.1. Investigación Documental bibliográfica

La recolección de datos se la realizará a través de un proceso planeado, organizado de revisión de material académico con documentación de trabajos de tesis que determinará las características de hardware y software del sistema de video vigilancia además de los estándares de calidad de seguridad que se deben implementar al momento de la instalación y ubicación de las cámaras. Se realizo la investigación bibliográfica donde se tomaron en cuenta otros sistemas similares en trabajos de grado para tener un soporte del desarrollo de los sistemas con otras tecnologías (Duran, López, & Prada, 2019, pág. 16)

3.1.2.2 Investigación Descriptiva

Se realizó la investigación descriptiva para recopilar información como especificaciones técnicas video, fotos de las instalaciones sobre el estado actual y funcionamiento del sistema de video vigilancia así mismo sus técnicas para describir el objetivo principal y describir el funcionamiento del sistema además de las características del fenómeno, procesos, funciones, monitoreo con respecto a la condición de la seguridad en los laboratorios de computación de la UPEC que faciliten el diseño de la solución informática.

3.1.2.3 Investigación de campo

Según (Enriquez, Arcos, & Mina, 2019) la investigación de campo "Se caracteriza por tomar los datos directamente de la fuente que los origina y sin ninguna manipulación. Es decir, el investigador recoge la información, pero no altera las condiciones del medio". Por lo tanto, la investigación se llevó a cabo en las oficinas de tics y laboratorios de computación donde se tiene las manifestaciones del problema del sistema de video vigilancia el que se desarrolló en base a una entrevista realizada a el ingeniero Javier Torres encargado del sistema de video vigilancia además de realizar observaciones a la cobertura de las cámaras, iluminación y respuesta en tiempo real de los laboratorios de la UPEC, donde proporcionaron la información requerida.

3.2. IDEA A DEFENDER

El diseño de un sistema de video vigilancia con estándares de calidad permitirá ayudar a mejorar la seguridad de los equipos tecnológicos en los laboratorios y aulas de la carrera de computación en la UPEC

3.3. DEFINICIÓN Y OPERACIONALIZACIÓN DE VARIABLES

3.3.1 Definición de las variables

3.3.1.1 Diseño de un sistema de video vigilancia (Variable independiente)

Son sistemas que están compuestos por hardware y software que permite capturar y guardar grabaciones de video para tener un respaldo de las acciones de las personas que se realicen en empresas hogares o diversos lugares públicos

3.3.1.2 Estándares de calidad para la seguridad (Variable dependiente)

Son normas de calidad que debe de cumplir un sistema para asegurar que su funcionamiento sea seguro y eficiente a la hora de ponerlo en el mercado.

Tabla 1. Operacionalización de variables

Variable	Concepto	Dimensión	Indicadores	Técnica	Instrumento
Independiente: Diseño de un sistema de video vigilancia	Es el conjunto de hardware y software que permite capturar y guardar contenido multimedia para resguardar la seguridad de las personas y sus bienes materiales	Equipos del sistema de video vigilancia	Cámaras IP Servidores Cableado Infraestructura	**Entrevista**	Guion de entrevista
		Software del servidor NVR	Shinobi Motion Eyeos Ubuntu Pfense	**Encuesta**	Cuestionario
Dependiente: Estándares de calidad para la seguridad	Son normas que debe de cumplir un producto o servicio para asegurar que su funcionamiento sea seguro y eficiente	Estándares de calidad	Normas ISO Estándares IEEE Estándares ANSI/TIA/EIA	**Entrevista**	Guion de entrevista
				Encuestas	Cuestionario

3.4. MÉTODOS UTILIZADOS

En el presente proyecto de investigación se aplicaron los siguientes métodos

3.4.1. Inductivo – Deductivo

Debido a esta investigación con el método inductivo se logró analizar situaciones particulares dentro de una observación detallada del sistema de video vigilancia actual, identificando sus fortalezas y debilidades mediante un estudio individual para la generalización de un conocimiento de la situación de los laboratorios, en donde el método deductivo permitió determinar lo general para centrarse en lo específico de cómo se están llevando los estándares de calidad en el sistema de video vigilancia de los laboratorios de la UPEC identificando los recursos necesarios para implementar la propuesta y estableciendo un cronograma para llevar a cabo las acciones.

3.4.2. Analítico-Sintético

Se aplicó el método analítico que conforma la totalidad del caso a estudiar al realizar la descomposición del problema de la video vigilancia en sus elementos más básicos como dispositivos de grabación, cámaras entre otros, además de las características técnicas, almacenamiento, calidad de imagen entre otros factores relevantes con las cuales está compuesto el sistema, para que el método sintético capte de lo abstracto a lo concreto, a través de los métodos para esto, se debe considerar la ubicación de cada cámara, el ángulo de visión requerido, la calidad de imagen necesaria para cada área, la capacidad de almacenamiento necesaria, etc. Así mismo se logar descubrir la esencia del objeto investigado y apoye a los procesos de abstracción, análisis, síntesis

3.4.3. Histórico - Lógico

Este método permite realizar el estudio y establecer los antecedentes de los fenómenos que son objeto de investigación para saber cuáles son los estándares de calidad adecuados en el sistema de video vigilancia en términos de tecnología, diseño y funcionalidad para de esa forma se pueda obtener detalles de la lógica del desarrollo del proceso y elementos primordiales que incidieron en los cambios que surgieron a lo largo de los últimos años para tener en cuenta cómo ha evolucionado un sistema de videovigilancia, qué problemas ha enfrentado y cómo se han abordado. También puede ayudar a identificar patrones y tendencias en el desarrollo de este tipo de sistemas y cómo pueden influir en el futuro.

3.4.4. Técnicas de Investigación

3.4.4.1 Entrevista

La entrevista se realizó en el departamento de tics de la UPEC con el objetivo de conocer los detalles sobre la información de estándares de calidad en video vigilancia que existe en los laboratorios, su aplicación y si en los últimos años se los está usando. De igual forma se utilizará la técnica de entrevista estructurada que se dio al generar una guía de entrevista anteriormente para la evaluación y conclusión de que estándares se utilizan y saber cuáles se deberían implementar.

3.4.4.2. Encuesta

Se aplico mediante el uso de un cuestionario a los docentes de la carrera de computación con el fin de recolectar información sobre diversos temas del sistema de video vigilancia con preguntas puntuales que ayuden a la interpretación de la problemática y si resultase viable implementar un sistema de seguridad de circuito cerrado o video vigilancia para incrementar la seguridad de los laboratorios de la carrera

3.4.4.3. Guía de observación

La guía de observación directa colaboro a tener un conocimiento más específico al sistema de video vigilancia con respecto a los objetivos de investigación para conocer adecuadamente la problemática de inseguridad que se perpetuaba en los laboratorios

3.4.5 Población y muestra

3.4.5.1. Población

Para la elaboración de este proyecto se elimina de aplicar un método estadístico o una fórmula para calcular la muestra ya que está conformado por un grupo pequeño de docentes de toda la carrera de computación que laboran en la Universidad Politécnica Estatal del Carchi a los cuales va dirigido el proyecto

3.4.5.2. Muestra

En este caso seleccionamos una muestra no probabilística por conveniencia que se aplica a los docentes de la carrera por tener una población pequeña para facilitar la investigación ya que se desea tener resultados favorables para el proyecto

3.5. RECURSOS

Tabla 2. Recursos del Proyecto

Humanos	**Institucionales**	**Materiales**	**Económicos**	**Tecnológicos**
Estudiante. Jimmy Arévalo Tutor: MSc. Milton del Hierro Lector el MSc. Jairo Hidalgo.	Aulas Biblioteca de la universidad Laboratorios de informática Departamento de tics	Apuntes Libros Entrevistas Encuesta Guía de observación	Cable UTP Conectores Plug RJ45 Canaletas	Internet Computadora Cámaras IP Monitor Servidor Switch Disco duro

IV RESULTADOS Y PROPUESTA

Para cumplir con los objetivos que se han planteado en esta tesis se necesita información la cual se pudo obtener mediante la entrevista realizada a todos los profesionales del área de tics de manera similar a los docentes de la carrera de computación de la Universidad Politécnica estatal del Carchi para su análisis e interpretación en tal sentido de tener una buena comprensión del tema planteado en esta investigación

4.1 Análisis e interpretación de Resultados del proceso de investigación

4.1.1 Resultados de entrevista

1. **¿Como está compuesto el sistema de video vigilancia?**

   Respuesta: Son 2 sistemas, sistema antiguo con CPU de computadoras y cámaras. Que ya están obsoletas. 2, sistema nuevo con NBR de 256 canales y 40 cámaras activas.

   Análisis: Obtenido la respuesta de los encargados del sistema de video vigilancia se pudo tener en conocimiento que el sistema actual de CCTV que se encuentra implementado en la universidad está compue3sto por un sistema antiguo y que se debe de realizar una actualización del mismo modo un nuevo sistema que no se encuentra implementado en diversas ubicaciones de la universidad

2. **¿De acuerdo con la normativa internacional como se maneja la infraestructura del sistema de video vigilancia?**

   Respuesta: La infraestructura de red para videovigilancia es administrada e instalada por el área de redes y comunicaciones.

   Análisis: con la entrevista realizada se obtuvo la información de que las únicas personas que están capacitadas para manejar la infraestructura del sistema de video vigilancia son los profesionales del área de redes y comunicaciones.

3. **¿Qué tipo de servidor de video NVR, DVR se utiliza y cuantos canales contiene?**

   Respuesta: El NVR principal tiene 256 canales con 40 cámaras y predicciones. Los DVR secundarios son de 8 canales IP activos.

   Análisis: considerando las respuestas de los profesionales entrevistados los NVR que se encuentran instalados en el sistema de video vigilancia antiguo son kits de seguridad de 8 canales y el NVR principal tiene 256 canales de los cuales solo están utilizados 40 y la institución no tienen ningún DVR

4. **¿En la universidad que tipo de cámaras se utiliza para el sistema de video vigilancia?**

Respuesta: Son cámaras IP tipo domo de cuatro megapíxeles.

Análisis: Teniendo en cuenta los datos recolectados se puede decir que las cámaras que se encuentran instaladas en la universidad son de 4 megapíxeles, de igual manera en algunas áreas se encuentra cámaras PTZ que se encuentran en el sistema antiguo y un número estimado de todas las cámaras que se encuentran en funcionamiento son de 106 en total

5. **¿Qué tipo de políticas de seguridad se utiliza en el sistema de video vigilancia?**

Respuesta: Los equipos NVR que posee la UPEC tiene únicamente acceso el personal de seguridad y el encargado de cada área

Análisis: Tomando en cuenta lo dicho por los encargados del sistema de video vigilancia su pudo deducir que se manejan políticas de seguridad responsable de los datos personales en el acceso y monitoreo, del mismo modo los datos recogidos se manejan con la seguridad y protección cumpliendo la normativa de garantía de los derechos digitales ya que para realizar una extracción de video se debe de realizar una solicitud a la autoridad máxima

6. **¿De acuerdo con el estándar internacional que tipo de cableado y topología es la que se encuentra implementada en el sistema de video vigilancia?**

Respuesta: Se utiliza cableado UTP categoría 6 y por medio de una topología en estrella en cada uno de los edificios, incluyendo la NVR principal.

Análisis: después de realizar las entrevistas se pudo deducir que el tipo de cableado que se maneja en la universidad es UTP categoría 6 para todo el sistema de video vigilancia de la misma manera la topología es en estrella por ser que el NVR principal se encuentra en el data center y se interconecta por todos los Switch POE que se encuentran distribuidos en todo el campus de la universidad

7. **¿De acuerdo con la estándar ISO 27001 que tipo de mantenimiento se lleva en el sistema de video vigilancia?**

Respuesta: El sistema principal tiene aproximadamente 2 meses. Y los mantenimientos aún no se encuentran planificados.

Análisis: Con respaldo de la información obtenida no se hacen mantenimientos regularmente por que el sistema del NVR principal se encuentra por muy poco tiempo en

funcionamiento, por otro lado, en los sistemas antiguos se mantiene un plan de mantenimiento a realizar por el motivo de que ya se van quedando obsoletos y se pretende migrar todo el sistema al NVR con más canales

8. **¿Cómo realiza los respaldos de información del contenido multimedia y en que plataforma?**

Respuesta: Las grabaciones se las realiza en el disco interno de cada NVR

Análisis: Las grabaciones de respaldo se generan en el sistema de Hikvision además que el almacenamiento de lo que generan las cámaras de video vigilancia se almacenan en los discos duros del sistema ya que el super NVR puede hacer un arreglo 24 disco de 10 TB cada uno

9. **¿De acuerdo con la normativa cuánto tiempo se considera que se debe de tener guardados los archivos de video?**

Respuesta: Se debe considerar un tiempo mínimo de siete días o máximo un mes

Análisis: De acuerdo con la normativa se debería de tener en cuenta un número máximo de noventa días, pero por cuestiones de tecnología y cantidad de dinero que representaría en gastos es un número más limitado de días, de la misma manera en la universidad los reclamos son casi inmediatos de tal manera que en esos momentos se hace uso de las grabaciones en algún tiempo determinado en menos de una semana

10. **¿Qué tipo de VLAN se utiliza para que todas las cámaras de la institución se interconecten?**

Respuesta: Se utiliza una VLAN 208 de datos.

Análisis: Tomando lo dicho por los profesionales se puede decir que la red de área local VLAN que utilizan administra la red de cada una de las cámaras para tener una mejor administración en él envió de datos por la red

11. **¿Cuánto espacio de almacenamiento considera usted el recomendable para el manejo de los elementos de multimedia del sistema de video vigilancia?**

Respuesta: Se debe considerar al menos 7 días de almacenamiento.

Análisis: Con los datos obtenidos se puede decir que es recomendable tener un almacenamiento externo para poder tener más capacidad de almacenamiento por motivo que los almacenamientos internos de los NVR pueden llegar a ser costosos

4.1.2 Resultados de la encuesta

Análisis de datos de encuestas realizadas a los docentes de la carrera de computación

1.-Conoce usted si se encuentra implementado algún tipo de sistema de video vigilancia en la carrera de computación

Tabla 3. Respuestas si tiene un CCTV la carrera de computación

OPCIONES PREGUNTA 1	RESPUESTA	%
Actualmente si	0	0,0%
No tiene idea	4	40,0%
No cuenta con ninguno	6	60,0%
TOTAL	10	100,0%

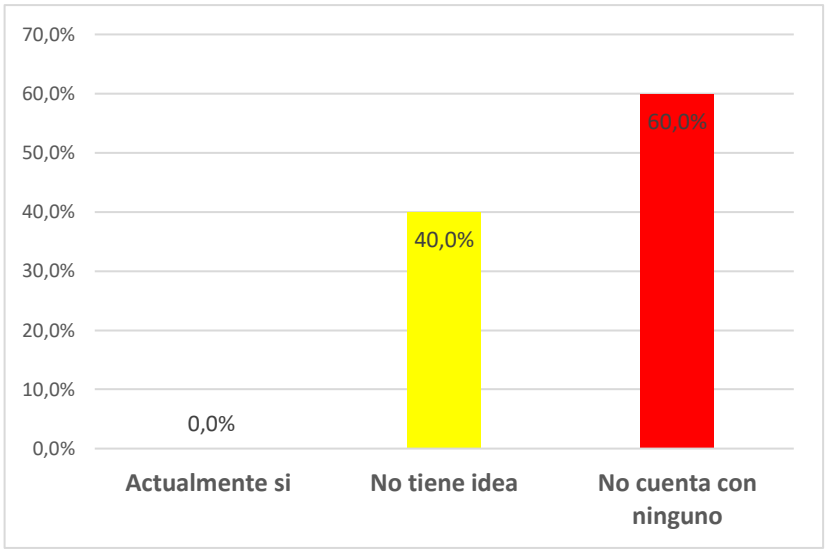


Figura 1: Resultados primera pregunta

Análisis: Tomando los datos obtenidos por las encuestas los docentes en un sesenta por ciento afirman que los laboratorios y aulas de la carrera de computación no cuenta con ningún sistema de video vigilancia, por lo tanto consideraron que al implementar el sistema de video vigilancia se podría prevenir los robos además de daños a los equipos de los laboratorios y de la misma manera a las instalaciones, por otro lado el cuarenta por ciento de los docentes respondieron que no tienen idea si de algún sistema de video vigilancia se tenía en las instalaciones

2.-El sistema de video vigilancia actual que se encuentra en la universidad como lo considera

Tabla 4. Resultados actual sistema de video vigilancia

OPCIONES PREGUNTA 2	RESPUESTAS	%

Satisfactorio	0	0,0%
Poco satisfactorio	7	70,0%
Malo	3	30,0%
TOTAL	10	100,0%

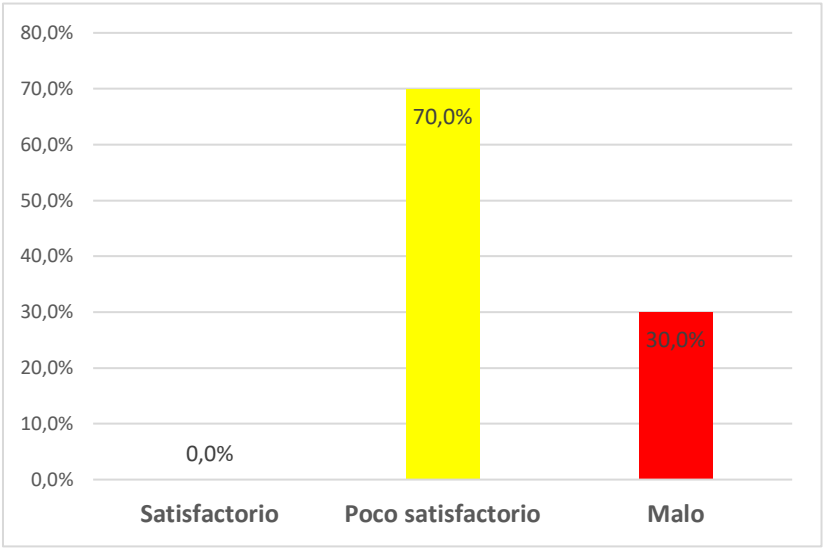


***Figura 2*:** Resultados segunda pregunta

Análisis: En relación al sistema de videovigilancia actual los resultados obtenidos en la encasta realizada a los docentes de la carrera de computación se pudo decir que el setenta por ciento de los encuestados aseguran que el sistema es poco satisfactorio por no cubrir diversos puntos de la carrera lo que genera que se provoque daños y robos en la carrera además consideran que se puede mejorar las medidas de seguridad y protección, por lo contrario el treinta por ciento de los encuestados aseguran que el sistema es malo reconociendo la falta de implementación de un sistema de video vigilancia expresando que se podría dar un cambio con el implemento de este mismo sistema.

3.-Cuál cree que es el encargado de llevar el monitoreo del sistema de video vigilancia

Tabla 5. Resultados del encargado de monitoreo del CCTV

OPCIONES PREGUNTA 3	RESPUESTAS	%
Guardia de seguridad	5	50,0%
Encargado de TICS	3	30,0%
No existe	2	20,0%
TOTAL	10	100,0%

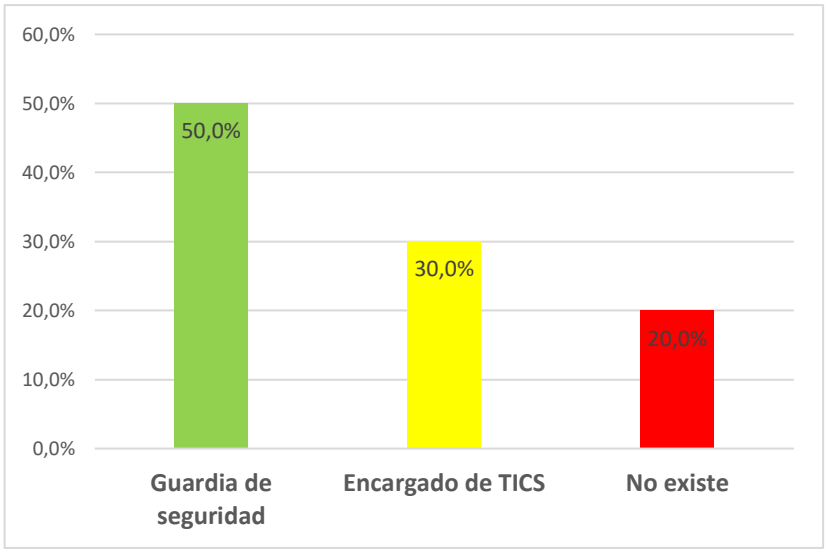


***Figura 3*:** Resultados tercera pregunta

Análisis: En opinión de los encuestados con un cincuenta por ciento el encargado de monitorear el sistema de video vigilancia es el guardia de seguridad porque es el encargado de tomar una medida o realizar una acción para prevenir daños o robos, en cambio el treinta por ciento de los docentes recomiendan que el encargado de monitorear las cámaras es el encargado de TICS sin tener en cuenta que el encargo de tics tienes más tareas por realizar, por otra parte el veinte por ciento deduce que no existe ninguna persona encargada de monitorear y controlar el sistema de video vigilancia.

4.-Se debería aumentar la seguridad en los laboratorios con la implementación de cámaras IP

Tabla 6. Respuesta de seguridad en los laboratorios

OPCIONES PREGUNTA 4	RESPUESTAS	%
Si se debe de aumentar más seguridad	10	100,0%
Poca seguridad	0	0,0%
Nada	0	0,0%
TOTAL	10	100,0%

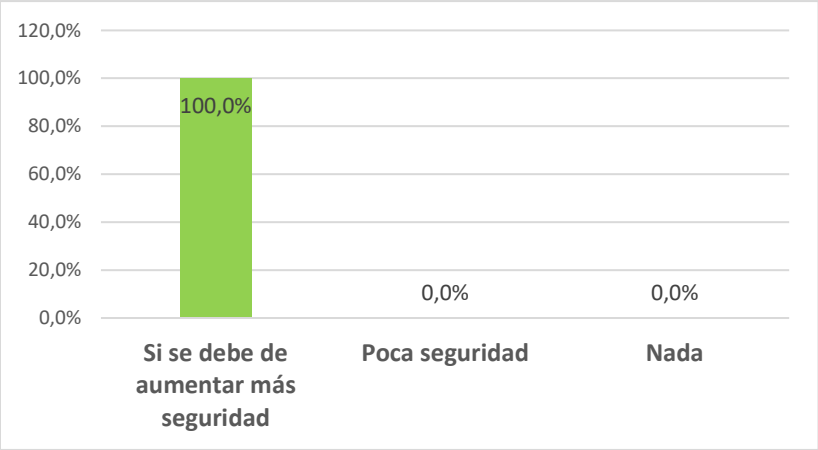


***Figura 4*:** Resultados cuarta pregunta

Análisis: De acuerdo con los datos de los encuestados con un cien por ciento en esta pregunta se reconoce la falta de implementar un sistema de video vigilancia en las instalaciones de la carrera de informática para así aumentar la seguridad de los laboratorios y equipos valiosos que se encuentran en los mimos

5.-Considera usted que contar con una infraestructura de cableado con estándares es lo ideal para fortalecer la seguridad en los laboratorios de informática

Tabla 7. Respuesta de infraestructura de cableado

OPCIONES PREGUNTA 5	RESPUESTAS	%
Si es ideal	7	70,0%
Neutral	3	30,0%
Poco importante	0	0,0%
TOTAL	10	100,0%

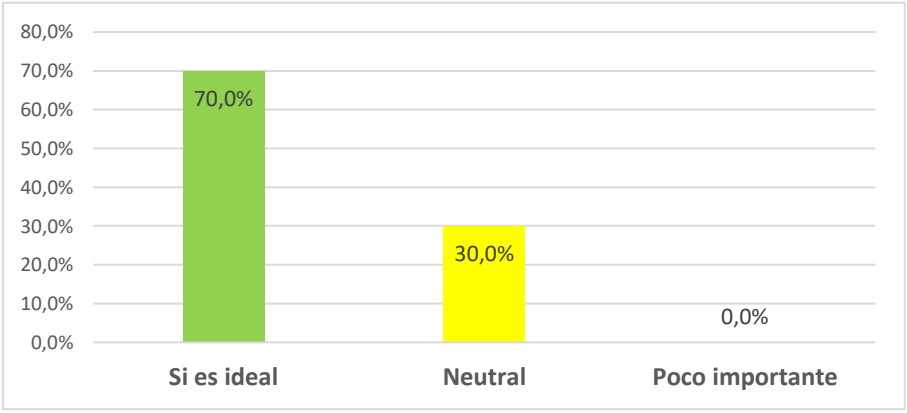


Figura 5:Resultados quinta pregunta

Análisis: Con los resultados de los datos de que se representa en el grafico se puede decir que el setenta por ciento de los encuestados consideran que es ideal contar con una infraestructura de cableado con estándares de calidad tomando en cuenta que en la implementación de este proyecto se acoge a las normas impuestas en la universidad por otro parte el treinta por ciento de los encuestados deducen que es neutral tener una infraestructura con estándares además de que consideran que no fortalecerá la seguridad en los laboratorios.

6.-Tiene idea de algún otro tipo de sistema de vigilancia que se puede implementar en los laboratorios

Tabla 8. Resultados de otro sistema CCTV a implementar

OPCIONES PREGUNTA 6	RESPUESTAS	%
Si	1	10,0%
No	7	70,0%
Cual	2	20,0%
TOTAL	10	100,0%

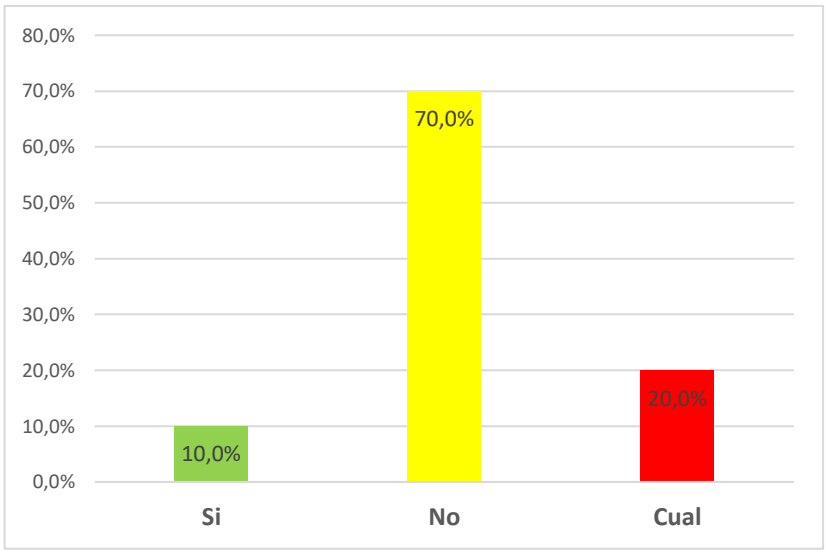


***Figura 6*:** Resultados sexta pregunta

Análisis: Se aprecio los datos de los encuestados con el valor de un diez por ciento que tiene conocimiento el sistema de video vigilancia Hikvision que se encontraba instalado en el campus, no más en la carrera, por otro lado el setenta por ciento de los encuestados no tenían idea de algún sistema a implementar en la carrera, del mismo modo se tuvo un veinte por ciento que manifestó implementar el sistema de video vigilancia con cámara PTZ las cuales son más usadas par exteriores y la otra opción fue la implementación de cámara vía wifi

7.-Está de acuerdo que en el sistema de video vigilancia se lleve políticas de seguridad

Tabla 9. Resultados de políticas de seguridad

OPCIONES PREGUNTA 7	RESPUESTAS	%
Totalmente de acuerdo	6	60,0%
De acuerdo	3	30,0%
En desacuerdo	1	10,0%
TOTAL	10	100,0%

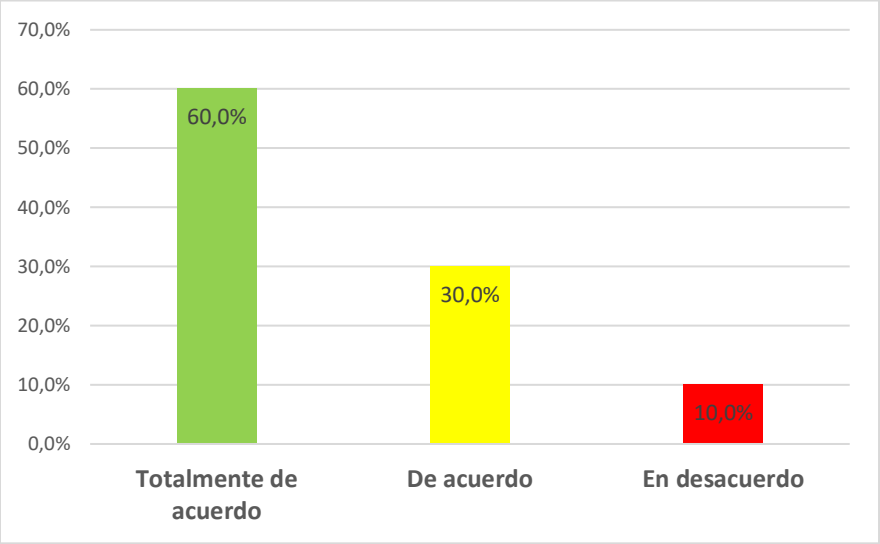


***Figura 7*:** Resultados pregunta siete

Análisis: Según los encuestados al realizar esta pregunta contestaron un sesenta por ciento que se deben de llevar políticas de seguridad para que continuamente se esté evaluando las mejoras o actualizaciones de tal manera que el sistema de video vigilancia se más efectivo para las personas monitorean el sistema así mismo para las personas que se encuentran siendo grabadas, por otra parte el treinta por ciento de los encuestados es tan solo de acuerdo considerando que las políticas de seguridad al momento de implementar el sistema no se ejecutan, así mismo el diez por ciento de los encuestados asegura que se vulneraria la privacidad delas personas de la carrera de la carrera

8.-Está de acuerdo que un sistema de video vigilancia debe monitorear las cámaras de video vigilancia de cualquier lugar

Tabla 10. Respuestas de monitoreo de cámaras desde cualquier sitio

OPCIONES PREGUNTA 8	RESPUESTAS	%

Totalmente de acuerdo	7	70,0%
De acuerdo	2	20,0%
En desacuerdo	1	10,0%
TOTAL	10	100,0%

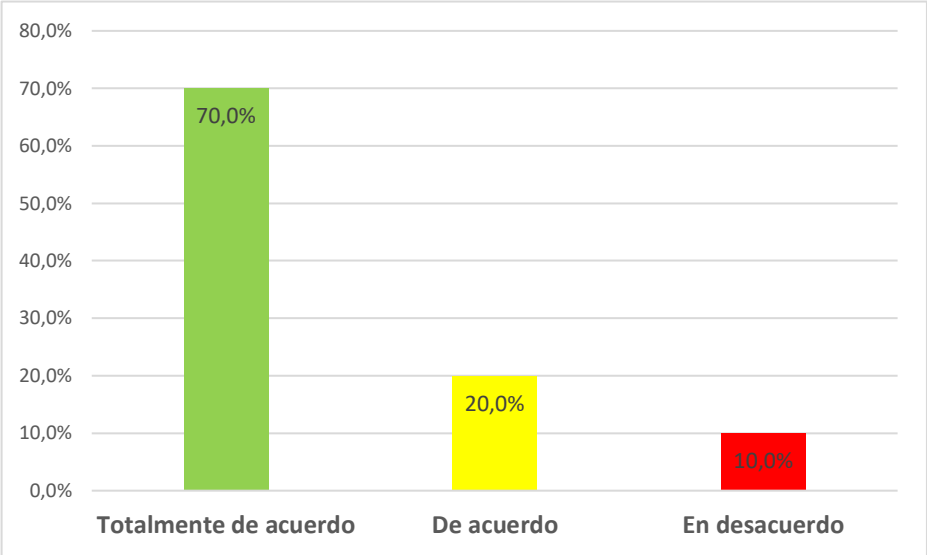


Figura 8: Resultados pregunta ocho

Análisis: Los encuestados en esta pregunta el setenta por ciento supo manifestar que el sistema de videovigilancia se debería monitorear de cualquier sitio en donde se encuentre la persona encargada tomando las medidas de seguridad, por otro lado, el veinte por ciento de los encuestados están de acuerdo considerando que los únicos que puedan tener acceso son el personal de TICS, así mismo el diez por ciento asegura que sería mejor no entregar las credenciales aparte del encargado

9.-Considera usted que se debe de utilizar una VLAN (red de área local virtual) para controlar el tráfico de red del sistema de video vigilancia

Tabla 11. Respuestas de uso de VLAN

OPCIONES PREGUNTA 9	RESPUESTAS	%
Totalmente de acuerdo	10	100,0%
De acuerdo	0	0,0%
En desacuerdo	0	0,0%
TOTAL	10	100,0%

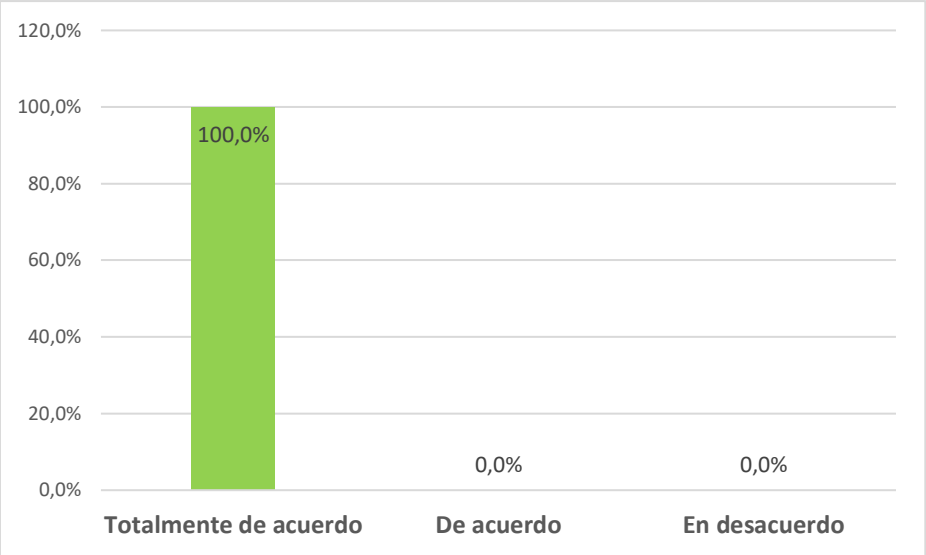


***Figura 9*:** Resultados pregunta nueve

Análisis: Tomando las respuestas de todos los encuestados aseguraron que se debe de tener una VLAN para majar todo el tráfico de datos que genere las cámaras del sistema de video vigilancia así garantiza el uso correcto de datos en toda la universidad sin generar un consumo alto de ancho de banda

10.-Considera que la integridad de los equipos que están en los laboratorios es de importancia para desarrollo de una buena educación

Tabla 12. Resultados de la integridad de los equipos

OPCIONES PREGUNTA 10	RESPUESTAS	%
Son de vital importancia	7	70,0%
Parcialmente tiene importancia	3	30,0%
No tiene importancia	0	0,0%
TOTAL	10	100,0%

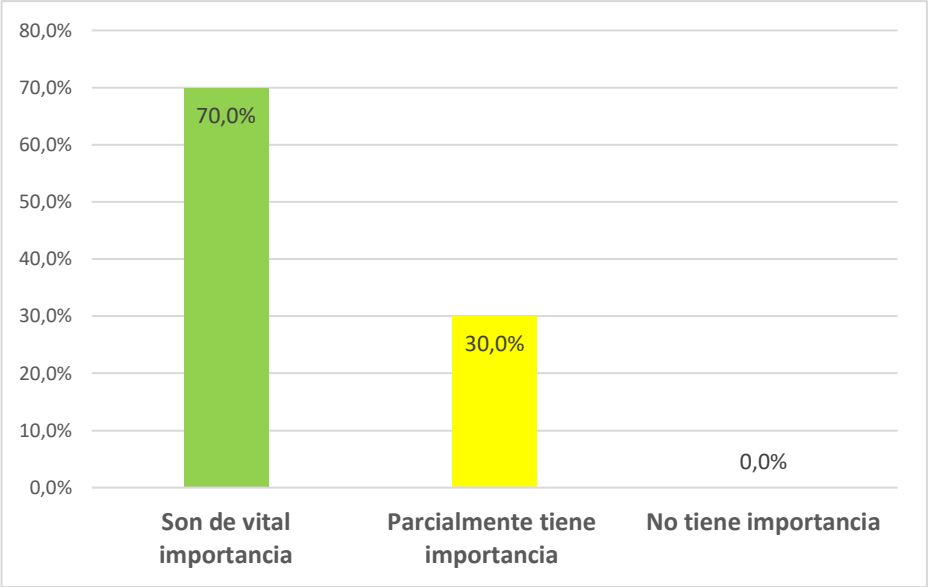


Figura 10: Resultados pregunta 10

Análisis: Los encuestados con un setenta por ciento de aceptación en esta pregunta manifestaron que los equipos tecnológicos que están en los laboratorios ayudan a fomentar una educación integral de tal modo que el sistema de video vigilancia ayuda a prevenir los daños de estos mismo, por otro lado, el treinta por ciento de los encuestados dijeron que realmente los equipos de la carrera no influyen al cien por ciento a generar una buena educación.

4.2 Planificación de la Propuesta

Introducción

De acuerdo con los información que se obtuvo para la implementación de este proyecto con su respectiva investigación de campo la cual fue fundamental para detectar las zonas que se desea cubrir con las necesidades de video vigilancia con la utilización de herramientas de software libre además se ejecuta la siguiente propuesta informática que se implementará en los laboratorios de informática, dando como resultado un sistema el cual será monitoreado en tiempo real así mismo el manejo de las cámaras se las pueda hacer por acceso remoto, el sistema que se pretende implementar se ejecutara en tres partes.

La primera parte consta en crear el equipo NAS con el hardware del servidor HPE Proliant del360 en su placa principal que es el servidor, así mismo configurar el sistema operativo ya que esta se encargara del sistema de video además de todas las cámaras que se encuentran el en sistema, de la misma manera configurar la unidad de almacenamiento que contenga todo el streaming capturado de las cámaras.

En segundo lugar, se configuro el servidor de video vigilancia Shinobi el cual gestionara el monitoreo de las cámaras de seguridad el cual este configurado con el sistema operativo Linux con uso de la base de datos preinstalada, del mismo modo se debe configurar la conexión mediante VPN's para poder comunicarse con los usuarios.

En la tercera parte tenemos que realizar las instalaciones de cableado con su etiquetado, cámaras, switches, router y servidor, del mismo modo debemos de realizar pruebas de streaming y almacenamiento lo que podrá cubrir la necesidad de poder anexar cámaras IP de distintas marcas en un solo sistema

Metodología Scrum

En la propuesta de este proyecto como guía de desarrollo de forma rápida se analizó la metodología ágil Scrum como solución a medida que se la utilizo por su seguridad de éxito al ser aplicada con gran facilidad de adaptabilidad en las etapas que se realizaron en el sistema, dependiendo de todas las características que se ejecutan unas después de otras enfocándose en el proceso de configuración del NVR mediante un proceso riguroso de elección de hardware, software que cubre las necesidades de la video vigilancia que requiere rapidez y flexibilidad para adaptarse en los diferentes cambios del diseño e implementación del sistema de video vigilancia y así mismo gestionar una solución informática de video vigilancia para los laboratorios de la carrera

4.2.1 Selección de Hardware

4.2.1.1. Cámaras Hikvision IR Mini Bullet Network Camera

Las mini cámaras de bala IP modelo DS-2CD2042WD-I son de gran ayuda por tener una precisión, fiabilidad, calidad y durabilidad con excelente resolución aprovechando al máximo sus 4 Megapíxeles además de contar con un lente focal de 4.7-118mm permitiendo una muy buena video vigilancia en interiores como en exteriores incorporando su IR (Luz infrarroja) con un alcance de 30 metros para cubrir completamente los entornos de día y noche de los laboratorios además cuenta con una cubierta con estándar IP66 que le ayuda a soportar el agua así mismo abarca la tecnología 3D para poder reducir el ruido y mejorar las imágenes con poca luz contando con la ventaja de ser alimentado por un Ethernet (POE) para una instalación sencilla (mgTRADING, 2019)

Figura 11.Cámara IR mini bullet network modelo DS-2CD2020F-I

Fuente: (HIKVISION, 2019) Cámaras IP

Especificaciones técnicas de cámara Hikvision IR Mini Bullet Network Camera

- Resolución: video 1080 HD, 4MP; imagen 20 FPS (2688 × 1520); 30 FPS (1920 × 1080), (1280 ×720)
- Lente fija de 4mm, 6mm
- Sensor de imagen: 1/3 CMOS de 2 megapíxeles
- Dia noche: Filtro mecánico de infrarrojos (ICR)
- Reducción de ruido digital 3D
- Rango IR: 30 FPS, hasta 20 metros
- Ajuste de 3 ejes
- Idioma: Ingles
- Salida de video: Conmutable TVI, AHD
- Compresión video: H.264+, H.264 MJPEG
- Consumo de energía: 5W/6.5 W (POE 802.3af)
- Tasa de bits 32 kbps a 16Mbps
- Distancia 30 metros
- Uso interiores y exteriores
- Resistencia estándar IP66

- Angulo de visión 85°
- Obtención de video para monitoreo de forma local y remota (HIKVISION, 2019).

4.2.1.2. Switch CISCO Catalyst 2960-X series

Este equipo es indispensable para poder desarrollar el sistema de video vigilancia y poder interconectar todos los demás componentes en la capa 2 de la red además de poder transmitir 10/100/1000 Mbps Gigabit Ethernet que ofrece en empresas pequeñas, medianas y grandes se conecten a la red de manera segura y confiable así mismo este switch brinda la capacidad de ser una fuente de energía de alta capacidad de 740W que puede cubrir la totalidad de los 24 puertos para POE+ (CISCO, 2021) que permiten poder ingresar las cámaras con una buena visibilidad del mismo modo contando con una interfaz de usuario web y líneas de comandos para poder ejecutar distintas configuraciones que se requieran realizar en el mismo, su seguridad se basa en control de acceso dinámico enfocado en roles en la red de la tecnología Cisco TrustSec mediante 802.1X evitando robo de direcciones IPV6 y ataques maliciosos

Figura 12. Switch Catalyst 2960-X series

Fuente: (CISCO, 2021) Hoja de características switch cisco 2960-X series

Características Switches Cisco Catalyst series 2960-X

Según (CISCO, 2021) afirma que las características del equipo son las siguientes:

- 4 enlaces ascendentes fijos de 1 Gigabit Ethernet de factor de forma pequeño conectable (SFP) o 2 enlaces ascendentes fijos de 10 Gigabit Ethernet SFP+
- Compatibilidad con POE+ con un presupuesto de energía de hasta 740 W y POE perpetuo

- Administración de dispositivos con interfaz de usuario web, acceso inalámbrico a través de Bluetooth, interfaz de línea de comandos (CLI), protocolo simple de administración de red (SNMP) y acceso a la consola RJ-45 o USB
- Visibilidad con el sistema de nombres de dominio como fuente autorizada (DNS-AS) y NetFlow completo (flexible)
- Seguridad con 802.1X, Serial Port Analyzer (SPAN) y Bridge Protocol Data Unit (BPDU) Guard
- Resistencia con fuentes de alimentación dobles opcionales reemplazables en campo

4.2.1.4. Router CISCO 4300 Series

El enrutador ISR (servicios integrados) aporta con su infraestructura WAN con función de ruteador, firewall para poder concretarse de forma segura al llevar por la mejor ruta el tráfico de paquetes incluyendo el cifrado y optimización de las redes WAN por donde transito el contenido del sistema de video vigilancia, así mismo automatiza, simplifica y protege la red además de contener fuentes de alimentación dual capaz de proporcionar alimentación POE con estándar 802.3af/at incrementando una capa adicional tolerante a fallos (CISCO, 2021)

Figura 13. Router Cisco 4300 series - ISR4321-SEC/K9

Fuente*:* (CISCO, 2021) Hoja de datos del enrutador cisco 4300 series

Especificaciones técnicas de Router CISCO 4300 Series

- Rendimiento agregado de 500 Mbps
- 4 puertos WAN o LAN 10/100/1000 integrados
- 4 puertos RJ-45, SFP
- 2 GB de memoria predeterminada DDR3 ECC DRAM y 16 plano de control de servicios

- Memoria flas predeterminada 8 GB y máxima de 32
- Ranuras USB 2.0 externas tipo A
- Fuente de alimentación interna redundante CA, CC, POE
- Frecuencia de entrada de corriente alterna 47-63Hz
- Altura de estante 1 unidad RACK (1RU)
- Normas operativas de telecomunicaciones TIA-968-B CS-03, ANSI T1.101, UIT-T G.823, G.824, IEEE802.3
- Software cisco IOS XE (CISCO, 2021)

4.2.1.5 Servidor HPE (Hewlett Packard Enterprise) Proliant dl360 gen10

Este equipo es muy importante por aportar en poder crear el servicio de gestión de video con el uso de diverso software libre es decir que procesa altas velocidades en rendimiento así mismo abarcar grandes cantidades de trabajo administrando las tareas del ciclo de vida del servidor Silver 4110, este mismo nos ofrece seguridad, agilidad y la capacidad de poder expandirse que adapta diversas cargas de trabajo ayudando a procesar todo el contenido streaming que se genera de las cámaras IP a la placa RaspBerry y así mismo almacenar en el servidor todo lo que se genera de todo el sistema de video vigilancia (Hewlett Packard, 2022)

Figura 14. Servidor HPE (Hewlett Packard Enterprise) Proliant dl360 gen10 Silver 4110

Fuente*:* (Hewlett Packard, 2022) Descripción general del Servidor HPE ProLiant DL360 Gen10

Especificaciones técnicas del Servidor HPE (Hewlett Packard Enterprise) Proliant dl360 gen10

- Capacidad de 2 zócalos, 2S - 2UPI a 9,6 GT/s
- DDR4 de 6 canales a 2400 MT/s, 768GB de capacidad de memoria máx.

- Tecnología Intel Turbo Boost, Intel AVX-512 (FMA 1 x de 512 bits) de la tecnología Hyper-Threading de Intel
- Estándar de video de hasta 1920 x 1200 a 60 Hz (32 b/p), 6MB de memoria de vídeo, Flash de 32MB, 4 Gb de DDR3, con protección ECC
- Tecnología HPE Integrated Lights-Out (iLO5), UEFI, Aprovisionamiento inteligente, iLO5 RESTful API
- Seguridad validación de FIPS 140-2 (certificación de iLO 5)
- Recuperación segura, recupera el firmware crítico al último estado correcto conocido cuando detecta un firmware comprometido
- 1 CPU: incluye 5 ventiladores estándares, 2 CPU: incluye 7 ventiladores estándares
- Conjunto de chips Intel C621
- Compatibilidad de arranque seguro y de inicio seguro de UEFI
- Espacio de una unidad rack (1RU)
- 5 puertos USB 3.0 (Hewlett Packard, 2022).

4.2.1.6 Selección de tipo de NVR (Grabador de video en red)

Tabla 13. Comparación de tipos de NVR

Tipo de NVR	Descripción	Ventajas	Desventajas
NVR autónomo	Es un dispositivo dedicado que se utiliza para grabar y almacenar vídeo.	Mayor fiabilidad y estabilidad debido a la falta de dependencia de un ordenador.	La funcionalidad es limitada en comparación con otros tipos de NVR.
NVR basado en PC	Es un software instalado en un ordenador que permite grabar y almacenar vídeo.	Mayor flexibilidad y capacidad de personalización en comparación con otros tipos de NVR.	Dependencia de un ordenador que puede ser menos fiable que un dispositivo dedicado.
NVR en la nube	Es un servicio en línea que permite grabar y almacenar vídeo en la nube.	Se puede acceder desde cualquier ubicación con conexión a Internet.	Dependencia de una conexión estable a la red para garantizar el acceso.

NVR híbrido	Es un dispositivo que admite tanto cámaras IP como analógicas.	Mayor flexibilidad al permitir la integración de cámaras antiguas con las más modernas.	Puede ser más costoso que otros tipos de NVR debido a su mayor capacidad.

Fuente: Elaborado por Jimmy Arévalo, fuente (Paula, 2019).

El NVR hibrido y basado en PC es el que se encargara de contener el sistema operativo del CCTV que se alojara en el servidor HPE además es la solución de videovigilancia que combina la flexibilidad y la escalabilidad de un sistema IP con la compatibilidad con las cámaras analógicas existentes, así mismo el NVR híbrido puede admitir cámaras IP y analógicas lo que permite aprovechar cámaras heredadas mientras se va actualizando el sistema de videovigilancia, además los NVR híbridos suelen ser más asequibles que los NVR IP completos porque no requieren que todas las cámaras sean compatibles con IP lo que es una ventaja significativa en presupuesto por otro lado es más fácil de instalar y usar que los sistemas de videovigilancia IP completos

4.2.2 Selección de software (equipo de monitoreo)

Los sistemas operativos del miniordenador RaspBerry Pi 4 B se los encuentra en páginas oficiales y no oficiales con el riesgo de descargar algún tipo de archivo malicioso

4.2.2.1 Selección de sistema operativo

Tabla 14. Características de sistemas operativos

Sistemas Operativos			
Características	**Raspbian**	**Ubuntu Desktop**	**Arch Linux ARM**
Logo			
Procesador	Cuatro núcleos a 1.5 GHz	Doble núcleo de 2 GHz o superior	Broadcom BCM2711 1,5 GHz
Memoria	2,4,8GB	4 GB	4GB

Almacenamiento en tarjeta microSD	4 Gb más paquetes de instalar	25 Gb espacio libre	6 Gb más paquetes de instalar
Conectividad inalámbrica	Si	Si	No
Usuario por defecto	Pi	No configurado	No configurado
Rendimiento microSDHC de E/S	Usa una clase 6 o 10 micro SDHC	Clase 10 micro SDHC	Clase 10 micro SDHC

Fuente: Elaborado por Jimmy Arévalo, fuente (Archlinux ARM, 2018), (UBUNTU, 2022).

Con la información recolectada en la tabla anterior el sistema a instalarse en el servidor HPE Proliant dl360 es Ubuntu para poder llevar a cabo el sistema ya que el tamaño para la instalación es adecuado a las necesidades, conteniendo una interfaz de usuario interactiva y fácil de utilizar y contando con la gran opción de usar un sistema gratuito así mismo tiene una conectividad wifi, bluetooth que gana velocidad en la lectura de archivos, de la misma manera optimiza el hardware del del ordenador además de contar con muchas programas que ayudaran a lograr cumplir con los objetivos planteados

4.2.2.2 Software de gestión de video

Tabla 15. Software de gestión de video

Software para el servidor de video			
Características	**Motion**	**Shinobi**	**MotionEyeOs**
Logo			
Formato de video	Mpeg4, msmpeg4, swf, flv, ffvl, mov, ogg, mp4, mkv, heve	Mp4, mpeg4, flv, mov, mkv	Mpeg4, msmpeg4, swf, flv, ffvl, mov, ogg, mp4, mkv, heve

Base de datos	MySQL PostgreSQL	MySQL MariaDB	MySQL PostgreSQL
Presentación automática	Imágenes en tiempo real	Transmisión en tiempo real	Imagen tiempo real
Consumo de recursos	Bajo	Alto	Bajo
Grabación inteligente	Activada automáticamente por su detección de movimiento	No configurada, pero si está disponible	Configurada automáticamente
Mantenimiento	Si tiene soporte	Si tiene soporte	Si tiene soporte
Configuración	Fácil	Mediana	Fácil
Programación	C	JavaScript	Python
Acceso remoto	A configuraciones, cámaras, transmisión por internet y navegadores web	Usando VPN, reenvío de puertos y P2P (punto a punto)	Configuración remota de cámaras y acceder por medio de servidor FTP

Fuente: Elaborado por Jimmy Arevalo, fuente (Motion, 2018), (RANDOM NERD, 2018), (Shinobi, 2020).

El software que se encargara de la gestión del sistema de video vigilancia con sus cámaras de seguridad que nos dará la opción de monitorear todo el video que se genere por parte de las cámaras será el sistema Shinobi el cual obtendrá el video que se genere el tiempo real extrayendo el video en tiempo real y enviárselo al cliente además de contar que Shinobi nos da la opción de instalar un mayor número de cámaras con calidad HD así mismo tiene la ventaja de que el sistema pueda funcionar con un ancho de banda bajo del mismo modo se debe descargar su complemento de instalación que es MotionEyeOs que es una mejor opción que aporta con una interfaz gráfica para la detección de movimiento que generen las cámaras.

Requisitos del sistema Shinobi:

- Sistema operativo: Linux (recomendado) o Windows.
- CPU: Procesador de doble núcleo o superior.
- RAM: 2 GB o más (recomendado 4 GB para un rendimiento óptimo).
- Almacenamiento: Espacio suficiente en disco duro para guardar los vídeos grabados.

Funcionalidades principales:

- **Monitorización en tiempo real:** Shinobi permite la visualización en tiempo real de cámaras de seguridad desde cualquier dispositivo con conexión a internet como ordenadores, teléfonos inteligentes o tabletas
- **Grabación de vídeo:** Puede grabar vídeos de forma continua o programada desde las cámaras conectadas así mismo los archivos de vídeo se guardan en el disco duro del sistema
- **Detección de movimiento:** Shinobi puede detectar automáticamente el movimiento en las imágenes de las cámaras y activar la grabación en consecuencia así ayuda a ahorrar espacio de almacenamiento y facilita la búsqueda de eventos específicos
- **Notificaciones**: El sistema puede enviar notificaciones por correo electrónico, mensajes de texto o por medio de otras plataformas de mensajería cuando se detecta movimiento o se produce algún evento configurado
- **Acceso remoto:** Shinobi permite acceder al sistema y ver las cámaras desde cualquier ubicación utilizando una conexión segura a través de internet

4.2.2.3 Software de creación de redes virtuales privadas

Tabla 16. Elección de software de creación de redes virtuales

Características	OPENVPN	PPTP	IPSec
Logo			
Interfaz	Usuario Web fácil de usar	Interfaz PPTP	Con panel de conexión sencillo
Acceso remoto	Mediante conexiones VPN entre varios servidores de acceso multi acceso	Protocolo punto a punto	Sitio a Sitio Control de acceso

Plataformas	Multiplataformas	Plataformas privadas	Plataformas privadas
Autenticación	Certificados digitales	Certificados digitales	Certificados digitales
Capa OSI	Enlace de datos, Red, Aplicación	Enlace de datos	Red
Confidencialidad	AES 128, 256 bits	DES 64 AES 128, 192 ,256	AES 256 bits
Velocidad	Alta velocidad	Muy baja velocidad y mayor procesamiento	Baja velocidad
Software libre	Si	No	No

Fuente: Elaborado por Jimmy Arévalo, fuente (OPENVPN, 2022), (Redes Zone, 2021)

Se selecciona el programa Open VPN en primer lugar por ser un sistema operativo libre el cual se ejecuta por medio de comandos en nuestro sistema Ubuntu el mismo que estará alojado en nuestro servidor para poder hacer la conexión VPN que nos ayudara a generas las redes privadas virtuales a nuestro centro de procesamiento de datos en donde se debe de configurar el cliente VPN para concluir con la configuración del software libre, además de contar con la ayuda del envió al almacenamiento y monitoreo que se debe de realizar a las cámaras de video de los laboratorios.

4.2.2.4. Detalles de VLAN y direccionamiento

La VLAN 4 actúa como una red independiente con su propio dominio de difusión, lo que proporciona mayor seguridad, eficiencia y flexibilidad en la administración y resulta beneficioso para organizar y controlar el tráfico de video de manera más eficiente de tal modo que la configuración de la VLAN en el sistema de video vigilancia garantiza el aislamiento y la seguridad del tráfico de video, es decir se utilizó una red de área local virtual (VLAN 4) en el switch CISCO Catalyst 2960-X series de capa dos por aportar organización además de seguridad de modo que el TAG con el estándar universal 802.1Q controla los Frames de ingreso y salida de los puertos del switch para no autorizar el acceso a las cámaras, de los dispositivos que se encuentren conectados a la misma red

///// Crear VLAN/////

Switch#

Switch# conf t

Switch(config)# vlan 208

Switch(config-vlan) # video vigilancia

Switch(config-vlan) # exit

///// Asignar puertos/////

Switch#

Switch#config t

Switch(config)# interface gi 1/0/2

Switch(config-if-range) # switchport access vlan 4

Switch#(config)# exit

Direccionamiento IP

La dirección IP es una identificación única que se le asigna a un equipo de red, con ella se puede identificar un dispositivo de red en particular dentro de la red, debido a esto en el sistema se utilizó una IP privada de clase B 172.20.4.1 con mascara 24 se pretende no usar más direcciones de las que el sistema necesita por otra parte, se asigna direcciones IP a las cámaras de seguridad dentro de una red. Cada cámara de videovigilancia necesita una dirección IP única para poder comunicarse en la red y transmitir video, por lo tanto, se asignó los nombres para conocer la ubicación de las cámaras del mismo modo para el piso que está ubicada

Tabla 17. Direccionamiento del sistema de video vigilancia

Direccionamiento IP			
VLAN	4		
IP	172.20.4.1		
Máscara	255.255.255.0 /24		
Broadcast	172.20.4.255		
Dispositivo	**Dirección IP**	**Máscara red**	**Broadcast**
LABORATIORO DE REDES	172.20.4.91/24	255.255.255.0	172.20.4.255
SALA PROFESORES 1	172.20.4.92/24	255.255.255.0	172.20.4.255

SALA PROFESORES2	172.20.4.93/24	255.255.255.0	172.20.4.255
PASILLO CARRERA1	172.20.4.94/24	255.255.255.0	172.20.4.255
PASILLO CARRERA 2	172.20.4.95/24	255.255.255.0	172.20.4.255
FATLAB1	172.20.4.96/24	255.255.255.0	172.20.4.255
FATLAB2	172.20.4.97/24	255.255.255.0	172.20.4.255
Switch	172.20.2.1/24	255.255.255.0	172.20.2.255
Servidor	172.20.4.90	255.255.255.0	172.20.4.255

4.3 Diseño del sistema de video vigilancia

4.3.1 Diagrama de conexiones del sistema de video vigilancia

Con este diagrama de conexiones propuesto en la figura 15, procede a detallar el esquema como está compuesta la red de video vigilancia ubicando el servidor HPE del 360 que tiene la función de ser el centro de procesamiento de video que se genere por medio de las cámaras IP, además estas mismas transmiten todo el streaming que se haya generado al almacenamiento que se encuentra configurado en la placa del servidor.

Las imágenes y videos que se generan pasan por el centro de almacenamiento que se procesan y analizan en los disco duros de 1.2 terabytes ya que el servidor se encuentra conectado por un cable UTP categoría 6 al switch cisco que es poe además de trabajar con mayor velocidad al enviar los datos a la red, la función del switch es permitir que los datos y streaming de las cámaras ingresen al servidor así mismo se procesen los datos del servidor de video para ser enviados al router el cual encapsula los datos para ser enviados a internet y así el streaming que este generando las cámaras se almacenen en el servidor HPE.

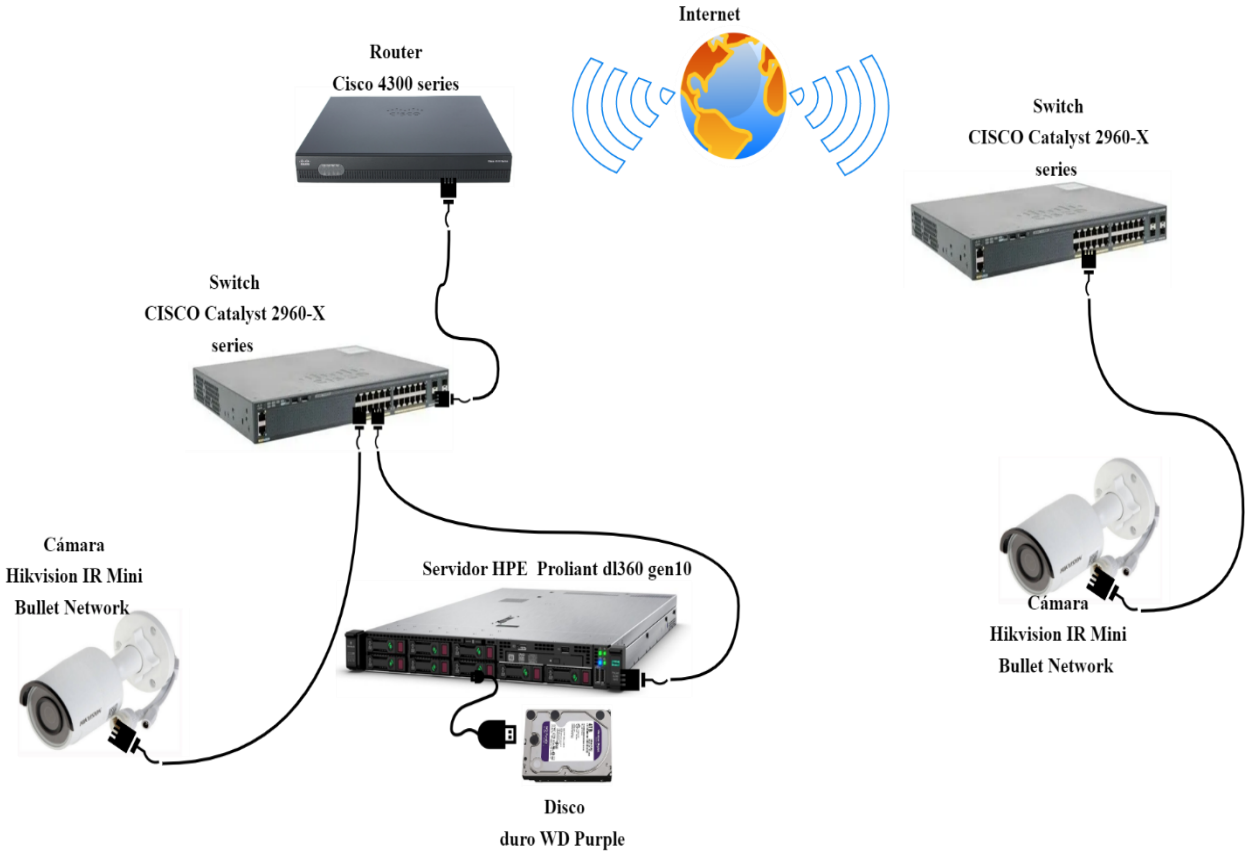


Figura 15. Diagrama del sistema de video vigilancia

4.3.2Cálculo de almacenamiento de disco duro

El almacenamiento que se implementará en el servidor de video se dará para las 7 cámaras que estarán grabando 7 días las 24 horas al día, con una resolución de 1080 con formato H.264, sistema de codificación NTSC (Comité Nacional de Sistemas de Televisión) y resolución de (1920X1080) que nos proporciona las cámaras IP, con la ayuda de la calculadora de Hikvision podemos realizar el cálculo con las especificaciones anteriores y así mismo su cálculo de ancho de banda

Cálculo de almacenamiento en disco duro con su ancho de banda en la herramienta de Storade and Network Calculator hikvision

Según la normativa para que el sistema de video vigilancia grabe en tiempo real se necesita de 25 a 30 FPS, pero de la misma manera las cámaras pueden trabajar habitualmente de 12 a 15 en espacios de poco movimiento con una calidad de video parcialmente aceptable, es así como el cálculo se acopla a las necesidades del sistema a implementar con las especificaciones de la capacidad de la cámara que se usó como se muestra en la figura 16

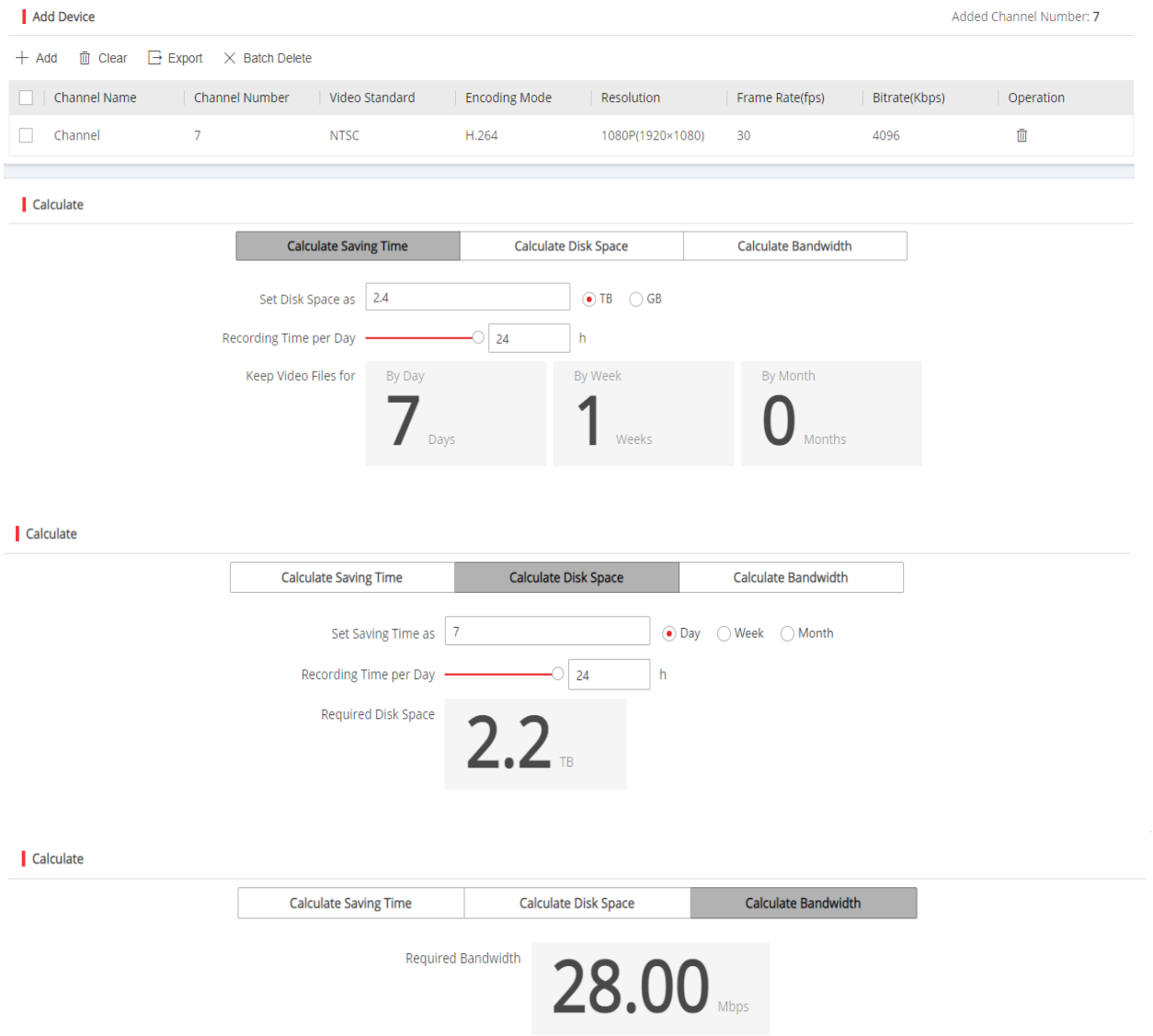


Figura 16 Cálculo de almacenamiento y ancho de banda de las cámaras Ip

Fuente: elaborado en herramienta Storade and Network Calculator hikvision

4.3.3 Diagrama de red

La figura 17 da a conocer cómo se encuentra la distribución del sistema de video vigilancia que se implementó en la universidad politécnica estatal del Carchi, como muestra la imagen se puede observar que la red de la universidad se maneja por medio del core el cual conecta a todos los edificios, es así que el edificio de aulas 4 es donde están situadas las aulas y laboratorios la carrera de computación, de tal manera el servidor con el sistema SHINOBI se encuentra instalado en la planta baja del edificio que conecta por cableado Ethernet a las aulas del primer piso e interconectar las cámaras para obtener las grabaciones en el servidor de video,

de la misma manera en el edificio en donde se encuentra FATLAB se realiza la conexión por medio de VLANS que maneja la universidad e interconectar todas las cámaras del primer piso

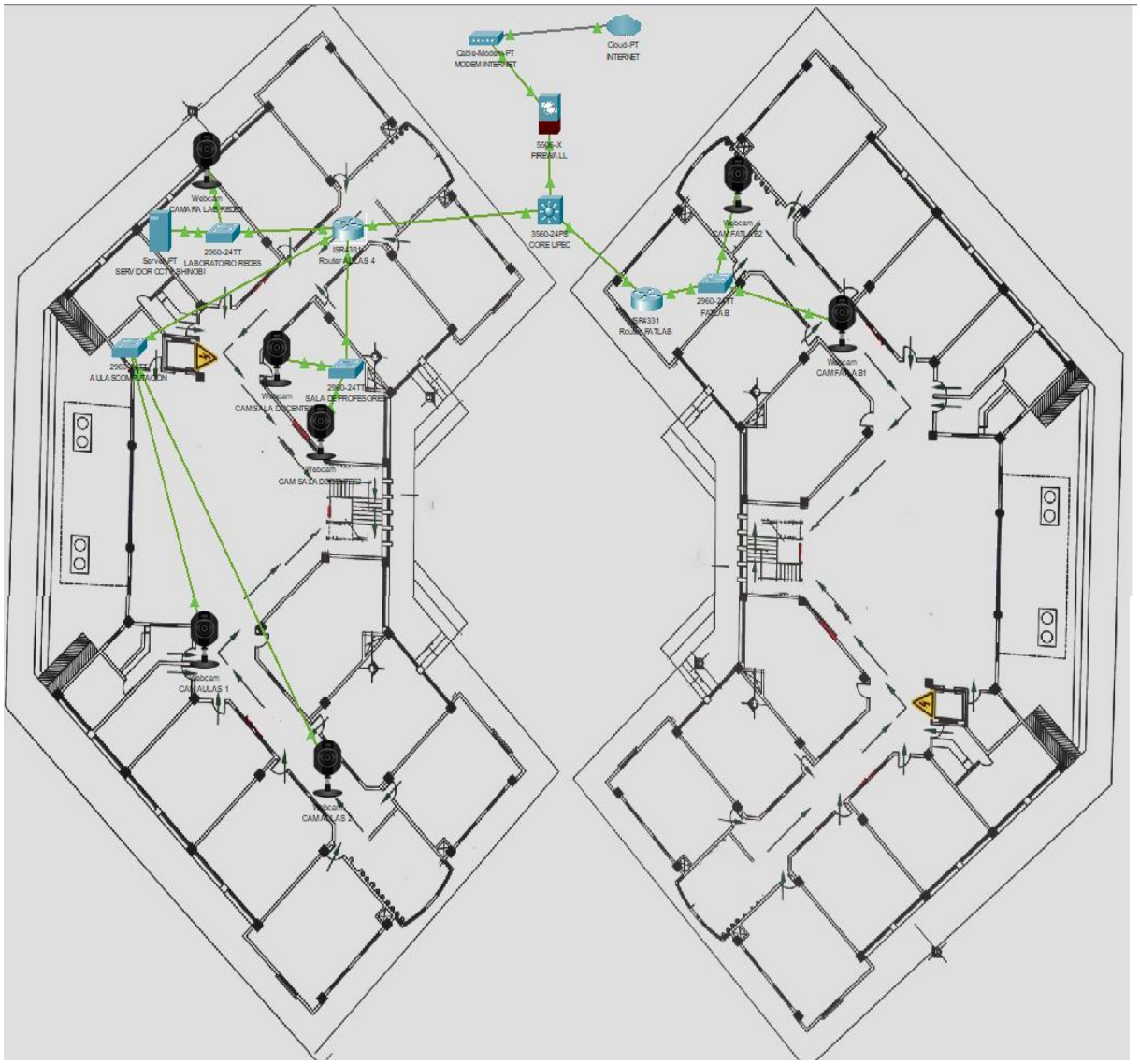


Figura 17:Diagrama de red de CCTV

4.3.3.1 Distribución de cámaras

Para la distribución de las cámaras y red de video vigilancia tomando en cuenta el área para monitorear se ingresó todas las especificaciones exactas de las cámaras como, la marca, el modelo DS-2CD2020F-I, resolución 1080 y distancia focal de 4mm para calcular todos los ángulos al mismo tiempo del tal manera que maximice la cobertura dentro del rango de cobertura y así poder realizar la implementación del sistema de video vigilancia, es así que para la visualización de los laboratorios de la carrera se utilizó las medidas de la infraestructura de la universidad además de cubrir los puntos ciegos así mismo poder cubrir las necesidades

específicas de seguridad de los laboratorios y carrera de computación como se da a apreciar en las figuras en donde se encuentra el sistema.

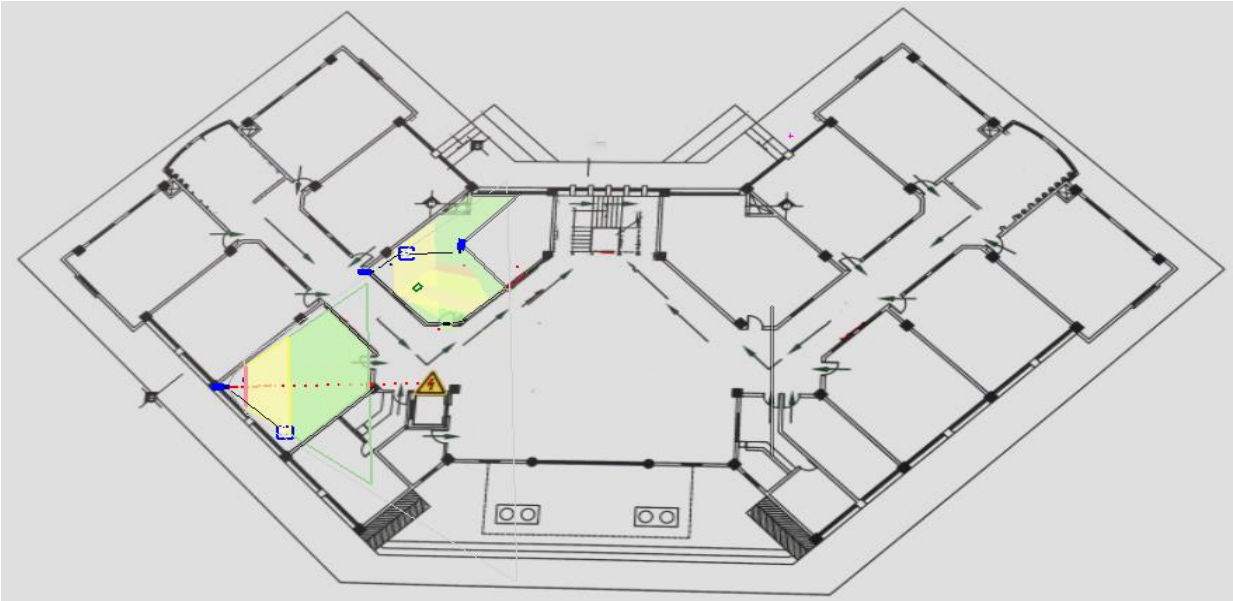
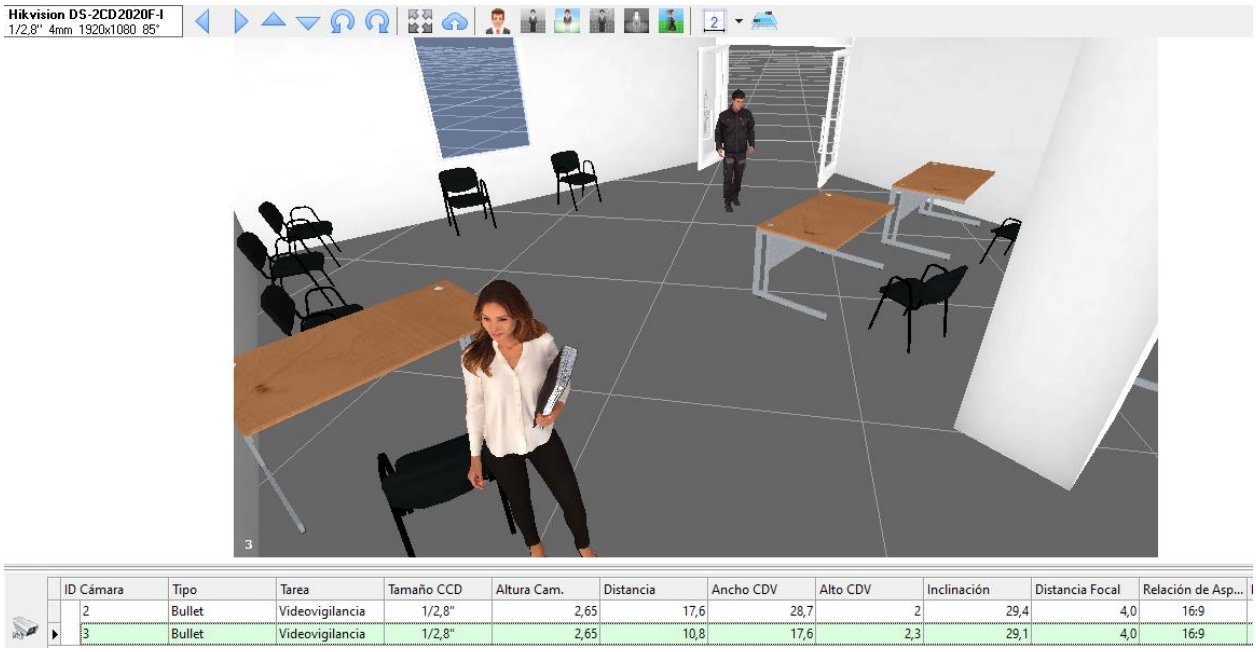


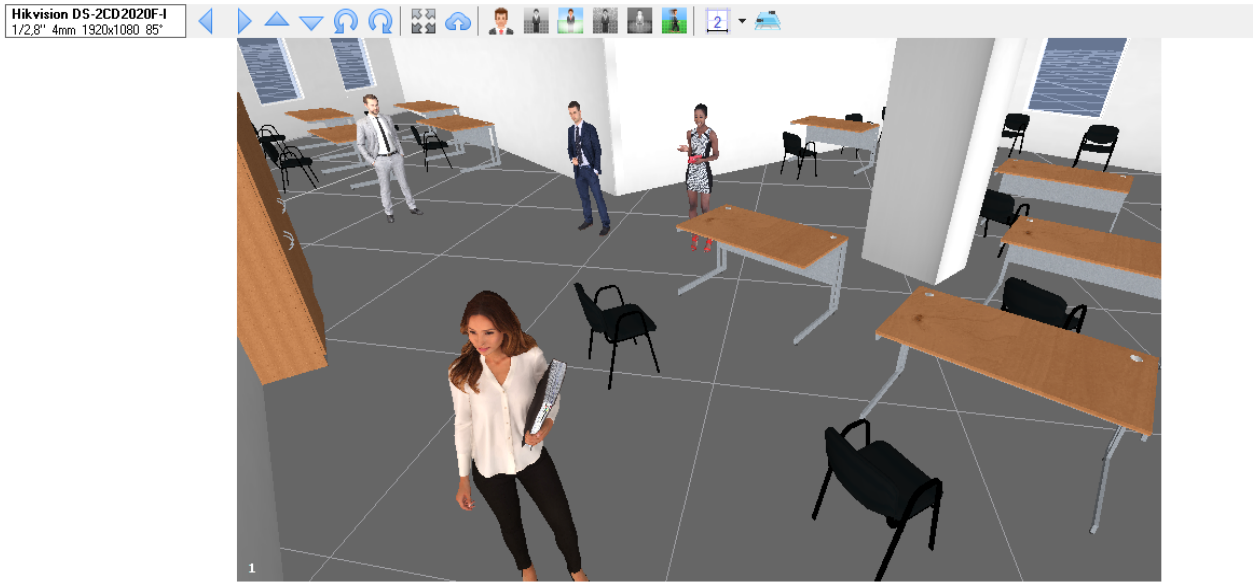
***Figura 18**:* Ubicación de cámaras planta baja de la carrera de computación

La herramienta IP video System Desing Tool da la ventaja de poder hacer una visión en tercera dimensión además de favorecer a la implementación del sistema de video vigilancia en todas las áreas en las cuales se encuentre la infraestructura a vigilar como es en el caso de la planta baja de la carrera de computación del mismo modo planificar ángulos, altura de cámaras y asegurar que se encuentren correctamente ubicadas como muestra la imagen



	ID Cámara	Tipo	Tarea	Tamaño CCD	Altura Cam.	Distancia	Ancho CDV	Alto CDV	Inclinación	Distancia Focal	Relación de Asp...
	2	Bullet	Videovigilancia	1/2,8"	2,65	17,6	28,7	2	29,4	4,0	16:9
▶	3	Bullet	Videovigilancia	1/2,8"	2,65	10,8	17,6	2,3	29,1	4,0	16:9

***Figura 19*:** Visión en 3D sala de profesores cámara 1



ID Cámara	Tipo	Tarea	Tamaño CCD	Altura Cam.	Distancia	Ancho CDV	Alto CDV	Inclinación	Distancia Focal	Relación de Asp...
1	Bullet	Videovigilancia	1/2,8"	2,65	17,2	28,0	2	29,4	4,0	16:9
2	Bullet	Videovigilancia	1/2,8"	2,65	17,6	28,7	2	29,4	4,0	16:9

***Figura 20*:** Visión en 3D sala de profesores cámara 2

En esta imagen se puede observar el laboratorio de redes con la ubicación exacta de la cámara asegurando no tener puntos ciegos y poder tener una calidad de imagen aceptable en el sistema

Figura 21: Visión en 3D laboratorio de redes

Diagrama de ubicación de cámaras en el primer piso con coberturas en los pasillos de la carrera de computación

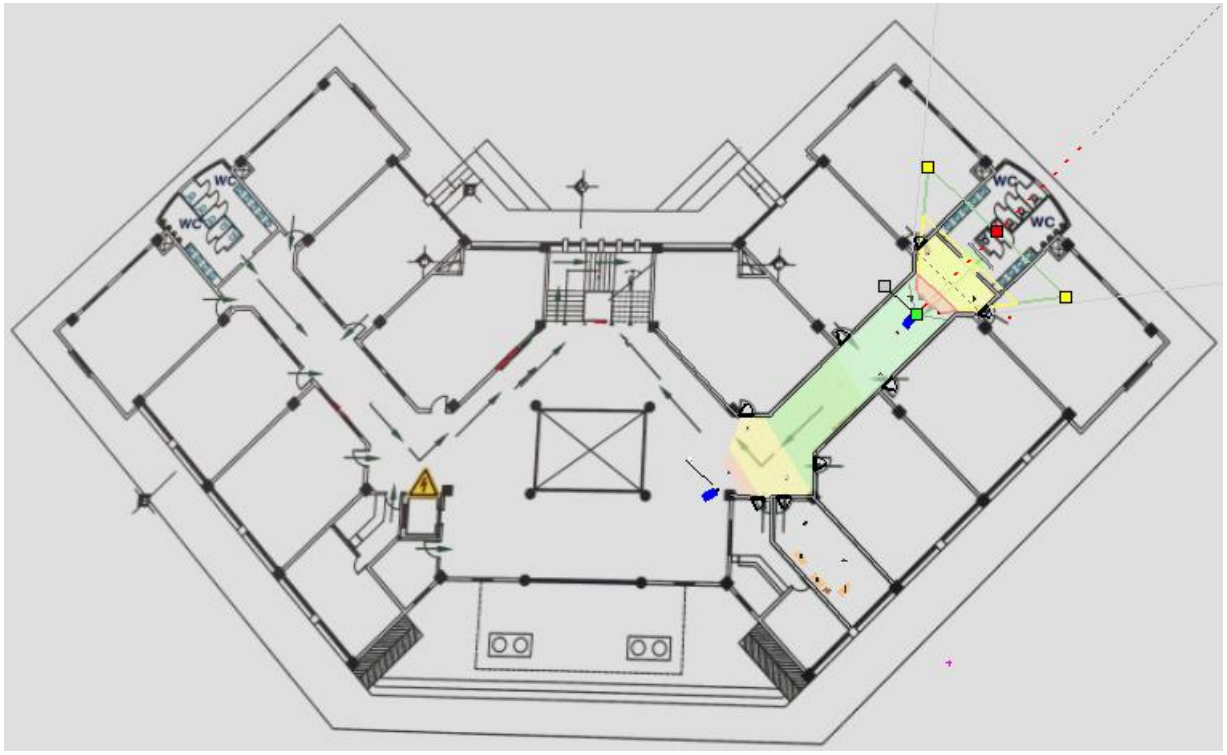


Figura 22: Ubicación cámaras primer piso carrera de computación

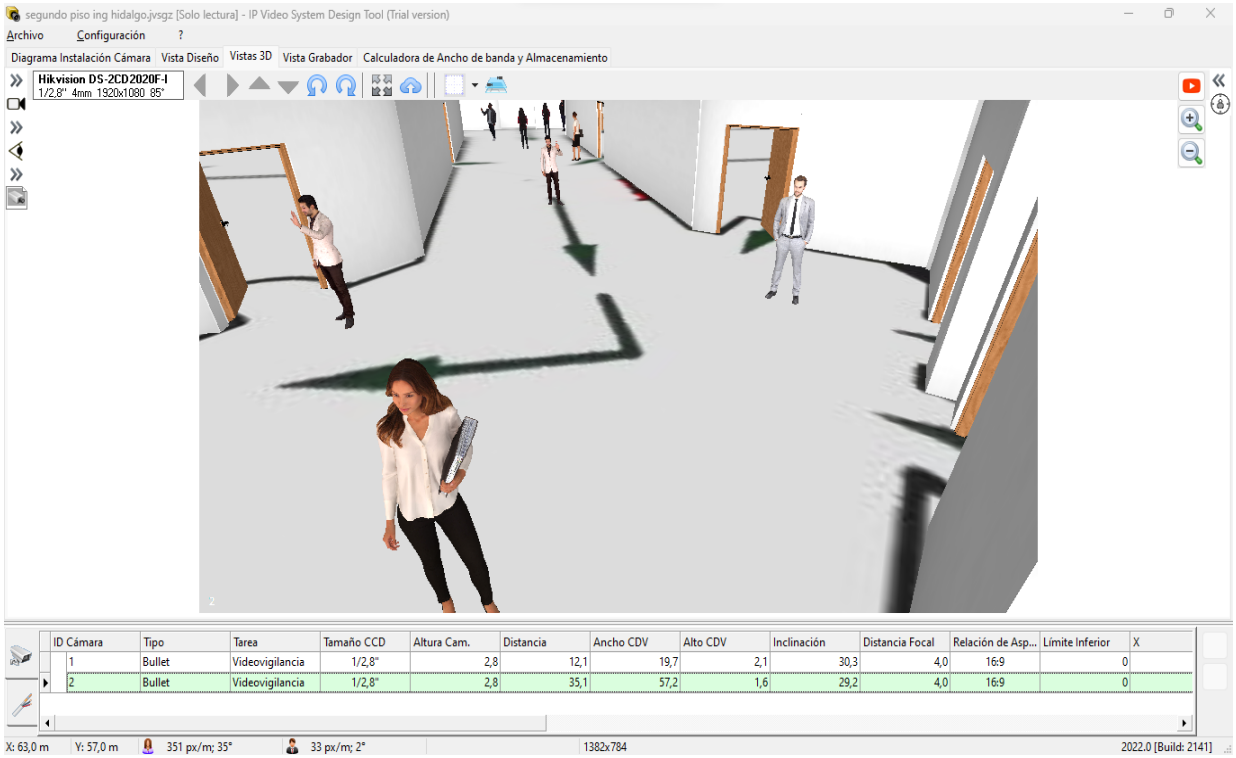


***Figura 23*:** Visión en 3D pasillos de carrera cámara 1

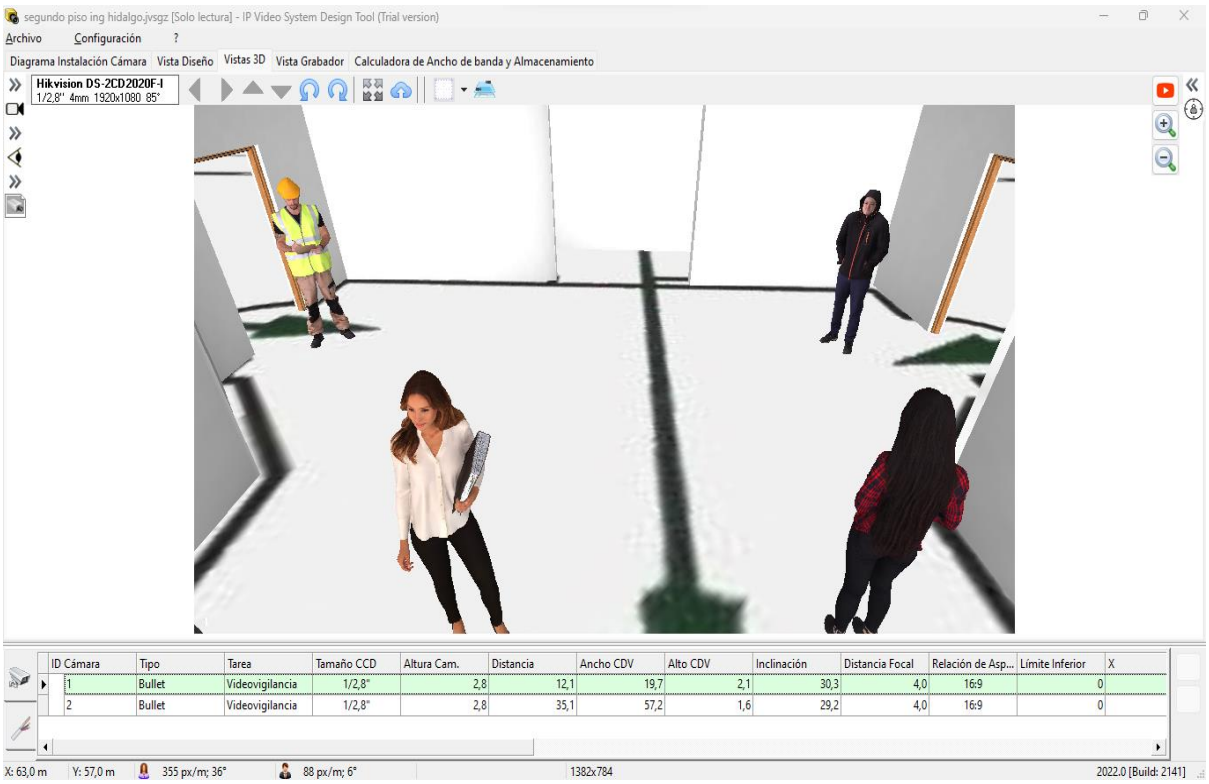


Figura 24: Visión 3D pasillos de carrera cámara 2

Ubicación de cámaras planta baja con cobertura en el área de FATLAB de la carrera de computación

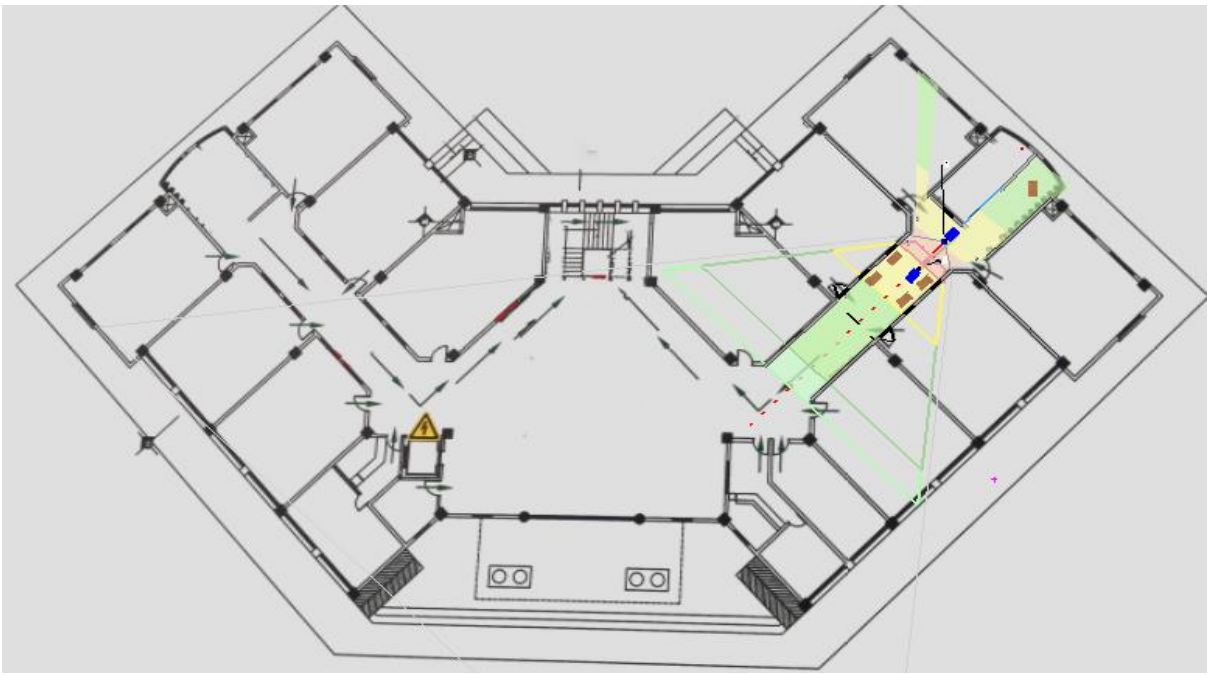
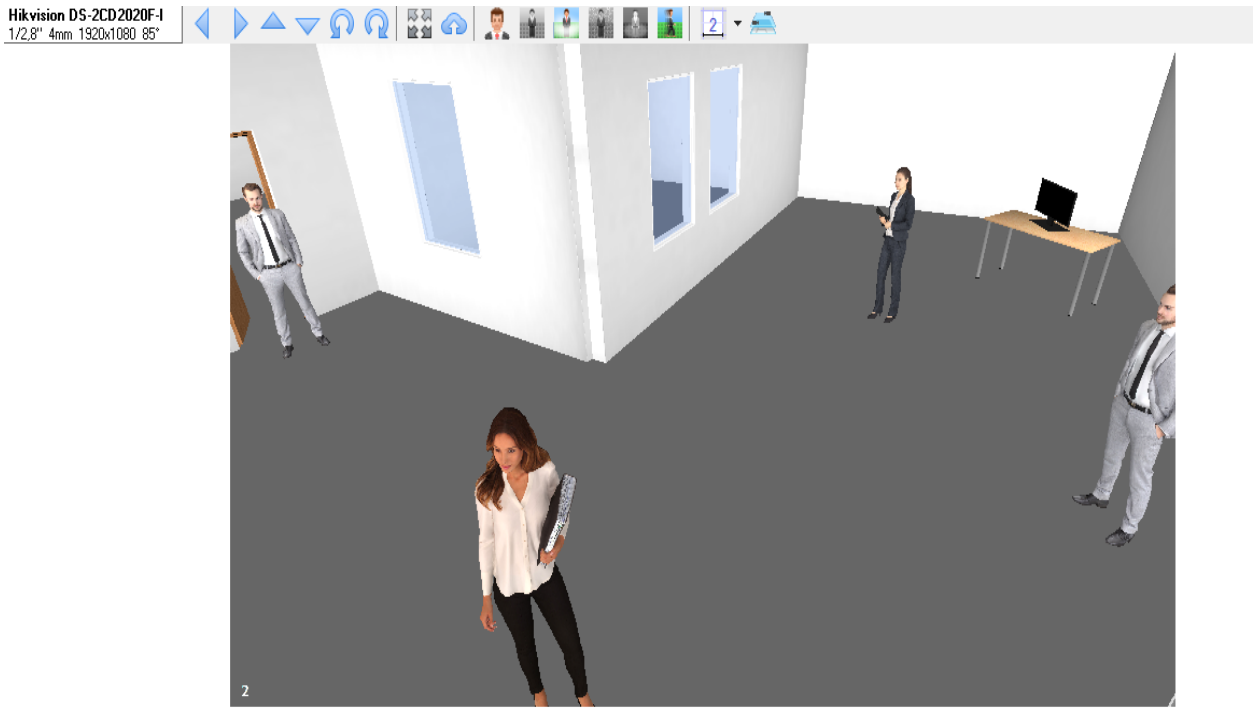


***Figura 25*:** Ubicación cámaras FATLAB

Vista 3D previa al área de FATLAB

ID Cámara	Tipo	Tarea	Tamaño CCD	Altura Cam.	Distancia	Ancho CDV	Alto CDV	Inclinación	Distancia Focal	Relación de Asp...	Límite Inferior
1	Bullet	Videovigilancia	1/2,8"	3	20,2	32,9	2,2	29,6	4,0	16:9	0
2	Bullet	Videovigilancia	1/2,8"	3	15,6	25,4	2,6	28,8	4,0	16:9	0

***Figura 26*:** Visión 3D FATLAB cámara 1



ID Cámara	Tipo	Tarea	Tamaño CCD	Altura Cam.	Distancia	Ancho CDV	Alto CDV	Inclinación	Distancia Focal	Relación de Asp...
1	Bullet	Videovigilancia	1/2,8"	3	12,0	19,6	2,2	31,2	4,0	16:9
2	Bullet	Videovigilancia	1/2,8"	3	15,6	25,4	2,6	28,8	4,0	16:9

Figura 27: Visión 3D FATLAB cámara 2

4.4 Desarrollo

4.4.1 Creación de NAS Y NVR

Para la creación del NAS se necesitaba tener acceso a la red de la universidad por lo cual se debía tener acceso al switch del laboratorio de redes, para la apertura de puerto del switch se usó el cable serial para ingresar por consola en el switch por lo tanto se procedió a configurar los puertos a utilizar dentro del Swicht con la ayuda de la herramienta putty se ingresó al CLI y dar acceso al puerto Gigabit ethernet dos con VLAN 4 del sistema del Switch cisco catalyst el cual se ingresa el comando ena para abrir la configuración de la terminal en el switch y utilizar los siguientes comandos

```
end

Switch#conf term
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#inter gi 1/0/2
Switch(config-if)#sw
Switch(config-if)#switchport ac
Switch(config-if)#switchport access v
Switch(config-if)#switchport access vlan 4
Switch(config-if)#end
Switch#wr
Building configuration...

Jan  8 20:57:44.370: %SYS-5-CONFIG_I: Configured from console by console[OK]
Switch#
```

Figura 28: Ingreso de comandos en Switch

Se conecto los cables de energía y red para poder realizar el primer ingreso al servidor y así mismo realizar el primer arranque utilizando las credenciales que tiene por defecto el servidor en la etiqueta de fabricación para ingresar poe hilo del sistema del servidor

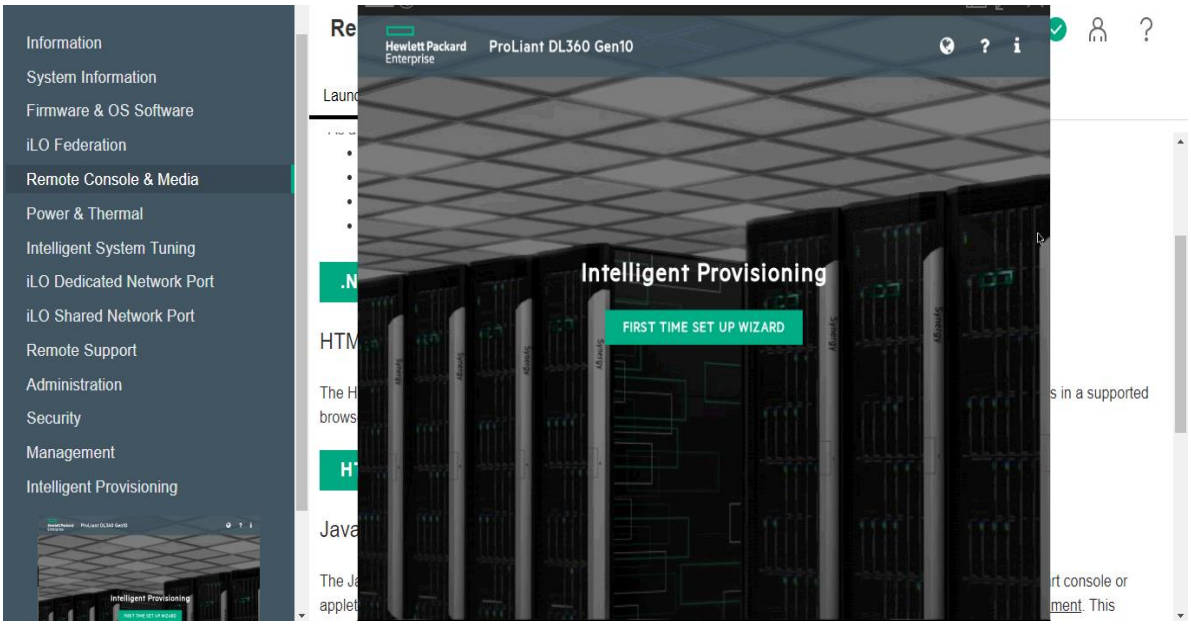


Figura 29: Ingreso a la interfaz del servidor

Configuración de zona horaria, idioma, modo de arranque

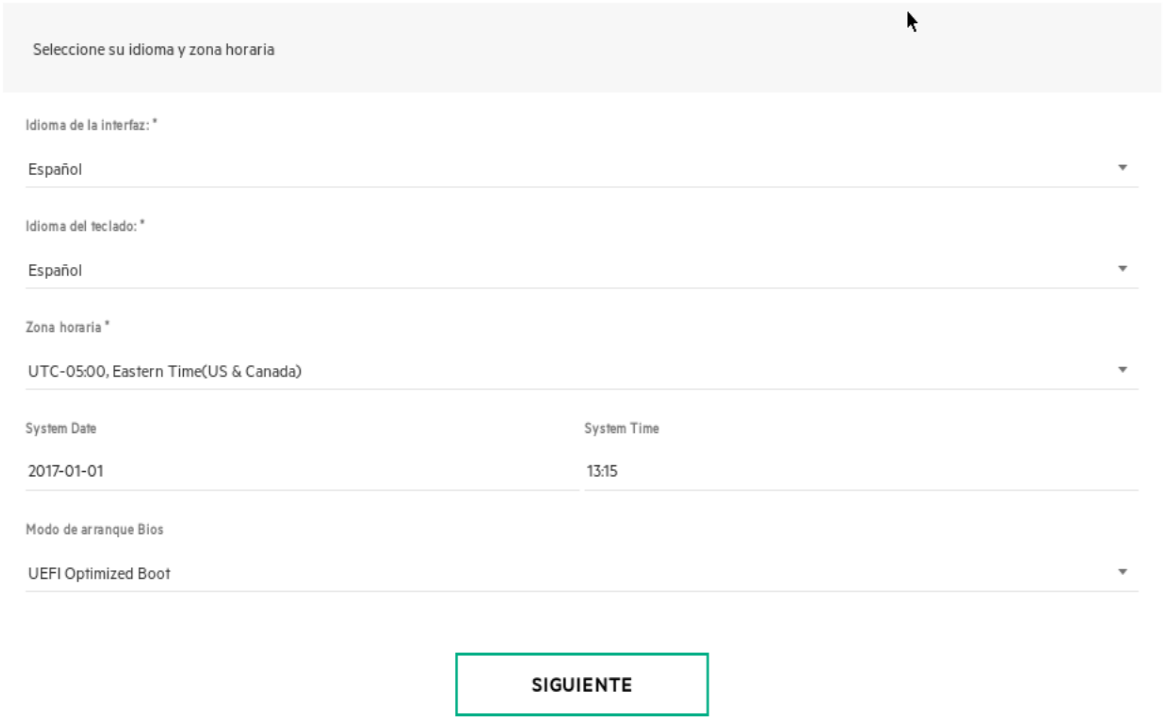


Figura 30: Ingreso de datos en el servidor

Opciones de optimización del servidor habilitando la opción de F10 para el ingreso a la interfaz de configuración del servidor

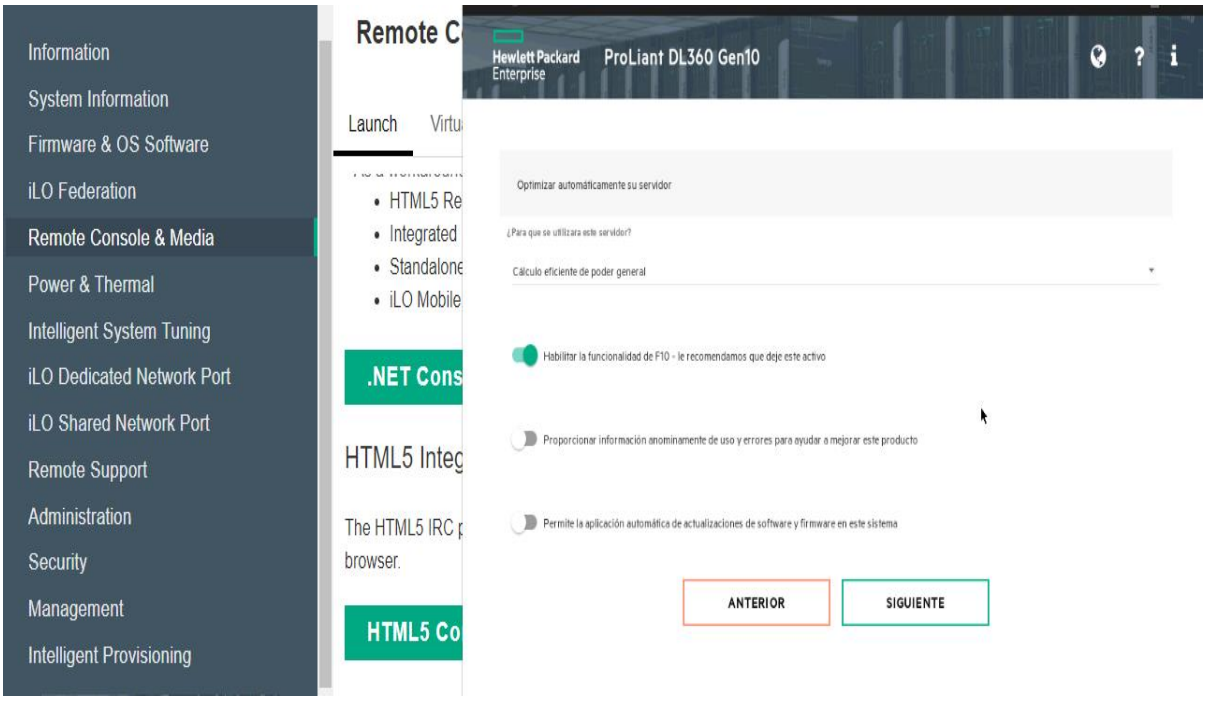


***Figura 31*:** Selección de opciones de optimización

Continuando con el proceso se seleccionó la configuración de red para la asignación de una IP en DHCP de igual manera en la configuración de red del hilo del servidor

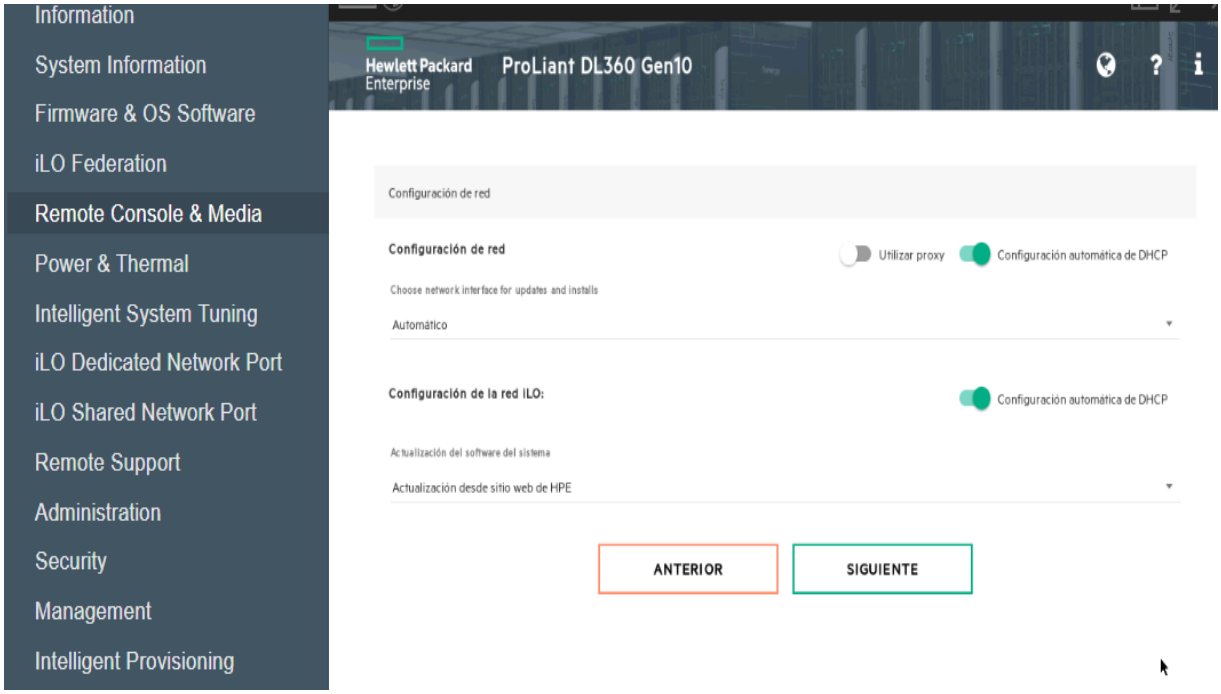


Figura 32: Configuración de red

Página principal del servidor que contiene todas las configuraciones para seguir con la instalación del sistema de video vigilancia

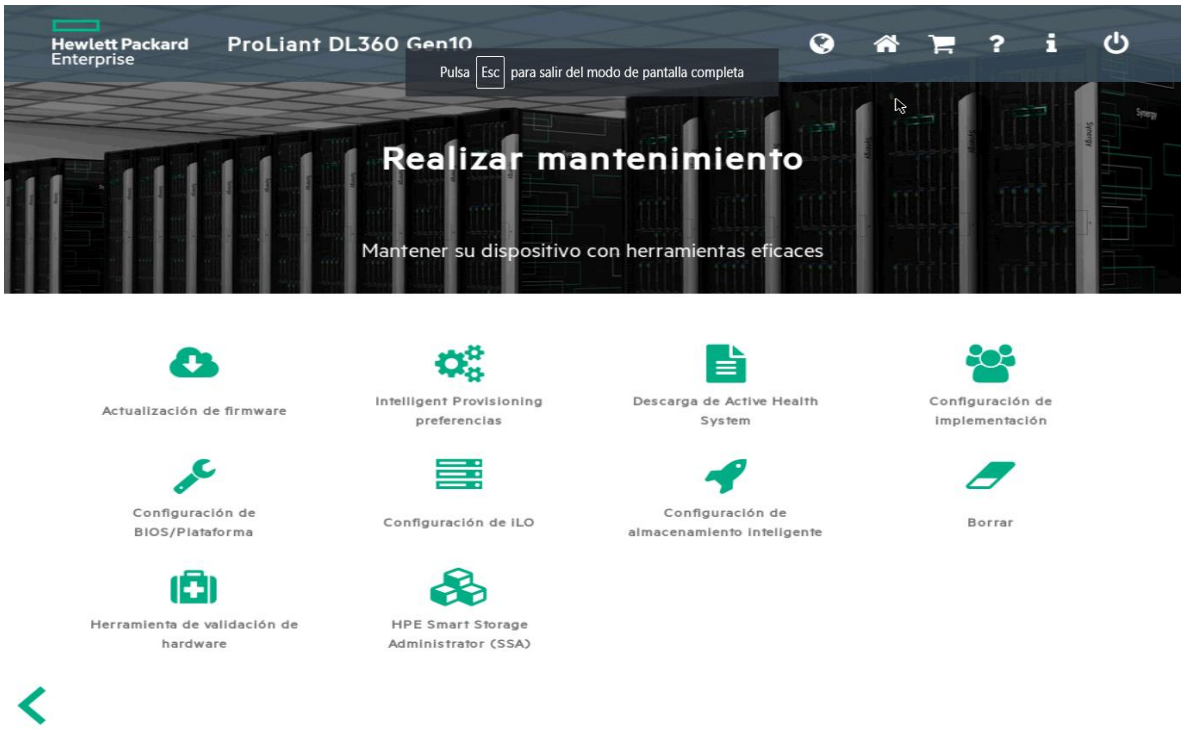


***Figura 33*:** Interfaz principal del servidor

Para seguir con la instalación se debe de crear un RAID por lo que en el botón **HPE Smart Storage Administrador** nos da la opción de crear el mismo a continuación, se presiona el botón **HPE Smart Array** como muestra en la imagen

Figura 34: Creación de RAID

Seguidamente se debe de presionar el botón de configuración, de igual manera en crear array

Figura 35: creación de array

Se procedió a elegir todos los discos que se encontraron en el servidor sumando todos los discos para crear una unidad lógica

Figura 36: Elección de almacenamiento

Se creo el RAID 1+0 por la opción espejo que brinda este por dar la opción de cuando se dañe un disco no se pierda toda la información así mismo se elige el tamaño de duplicación

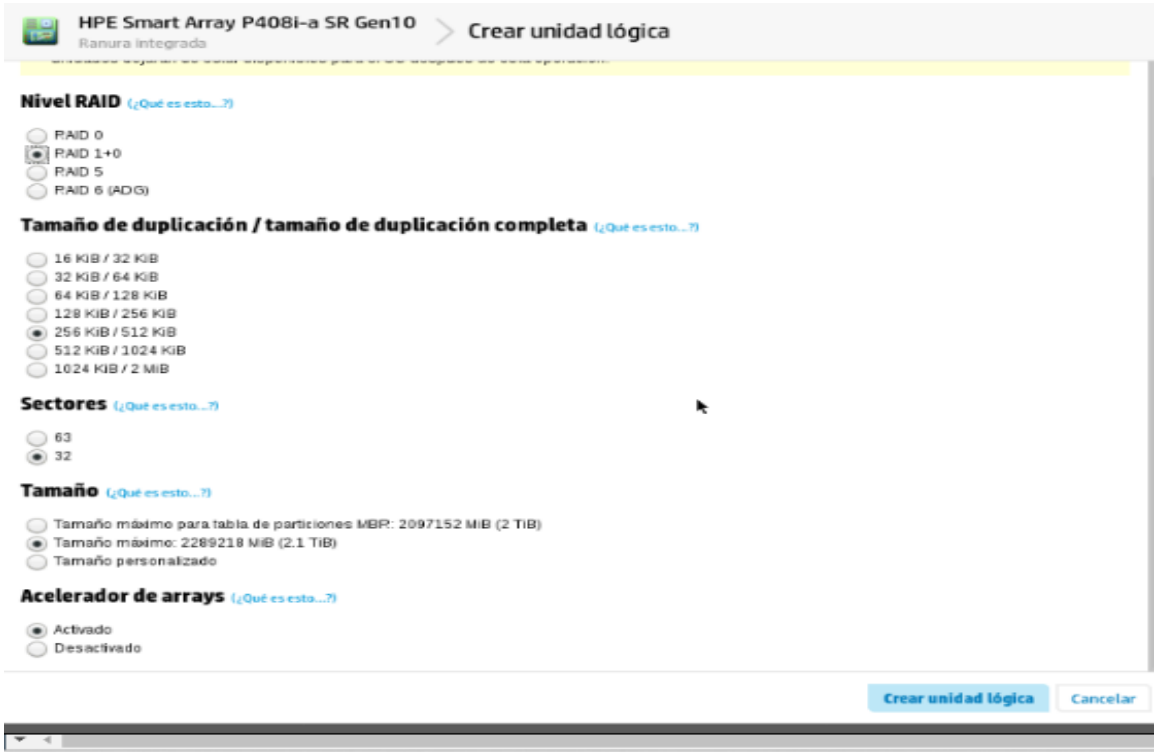


Figura 37: Configuraciones de RAID

Detalles de la unidad lógica creada en el sistema para poder almacenar el sistema CCTV

Figura 38: Detalles de unidad lógica

Para finalizar con la creación de la unida lógica se debe de observar con la siguiente imagen

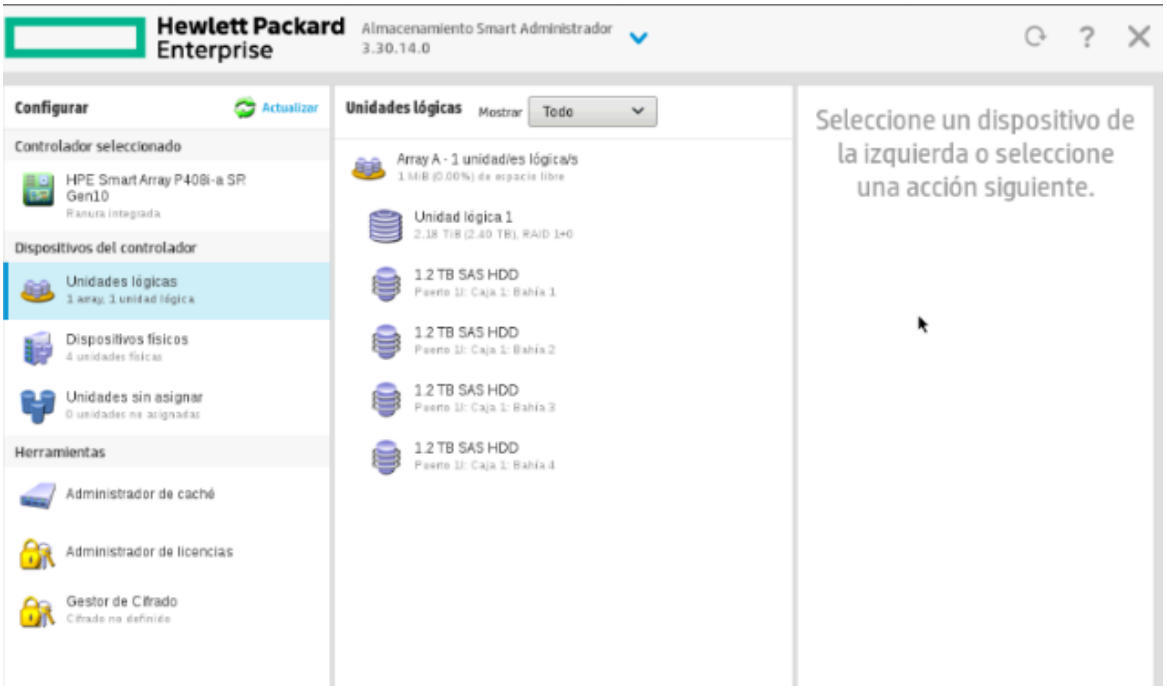


***Figura 39*:** Finalización de creación de unidad lógica

4.4.1.1 Instalación de Ubuntu en servidor

Para la instalación de SHINOBI se debe de reiniciar el sistema y presionar la tecla F9 para ingresar a la configuración de la BIOS la cual nos da la siguiente imagen

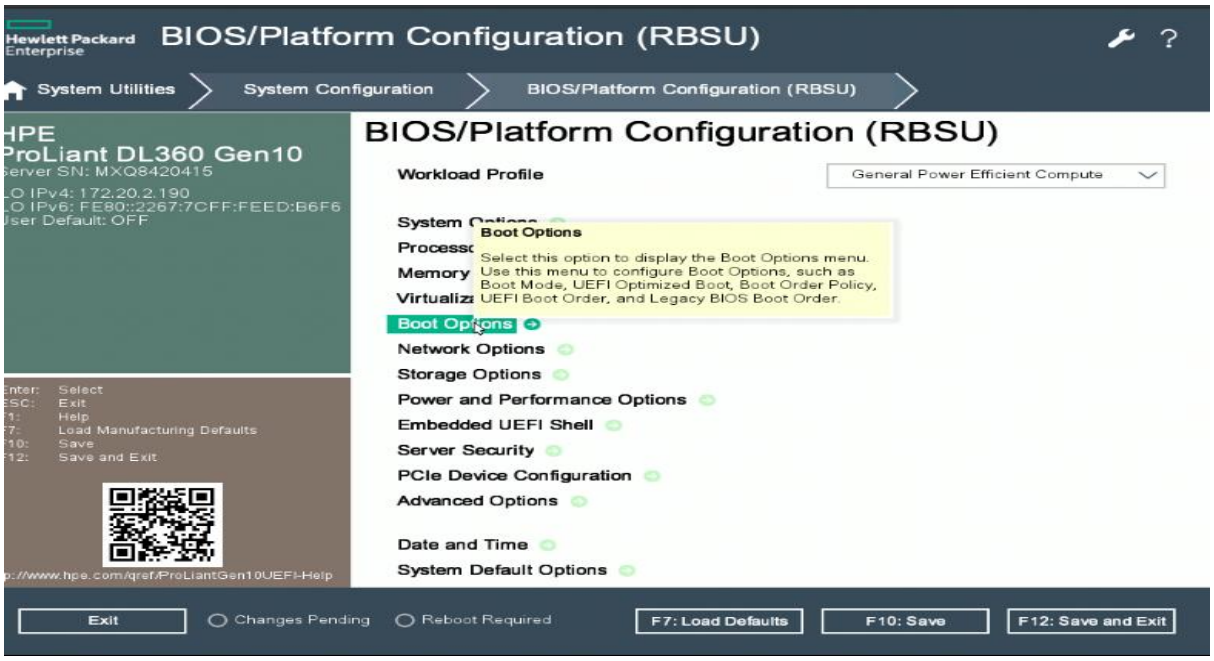


Figura 40: Ingreso a la BIOS

A continuación, se eligió el botón **ONE-TIME BOOT MENU** en este menú nos da escoger la unidad que contiene el sistema operativo

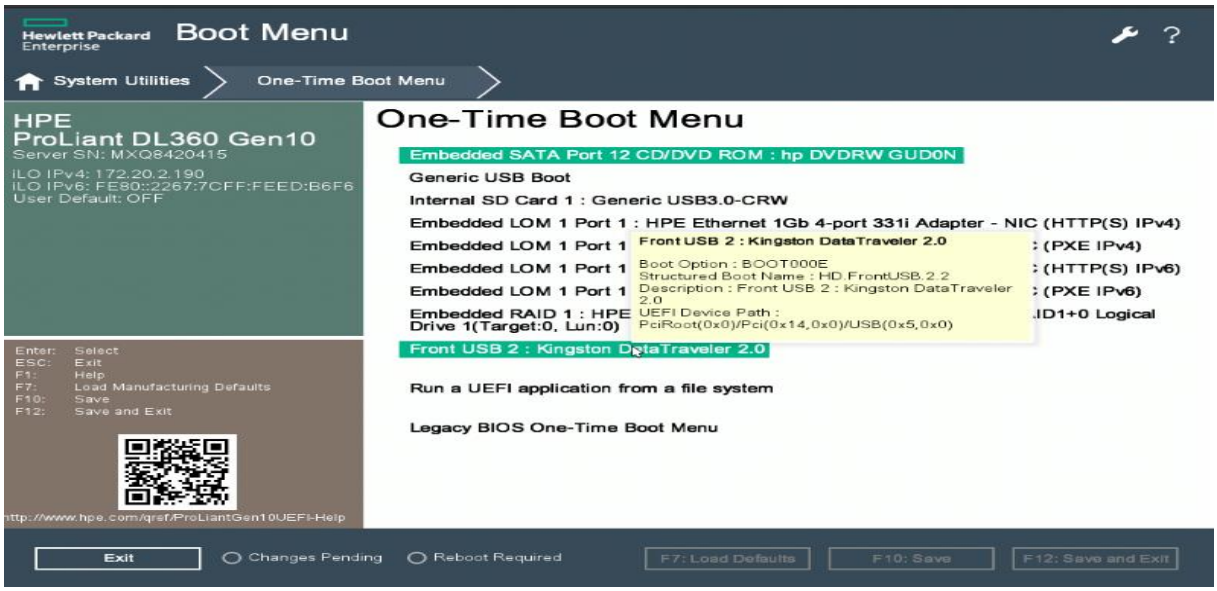


***Figura 41*:** Elección de unidad con sistema operativo

Se eligió la instalación del sistema operativo Ubuntu así mismo el idioma, disposición de teclado red, zona horaria entre otros y finaliza la instalación del sistema que ayudo a contener el CCTV

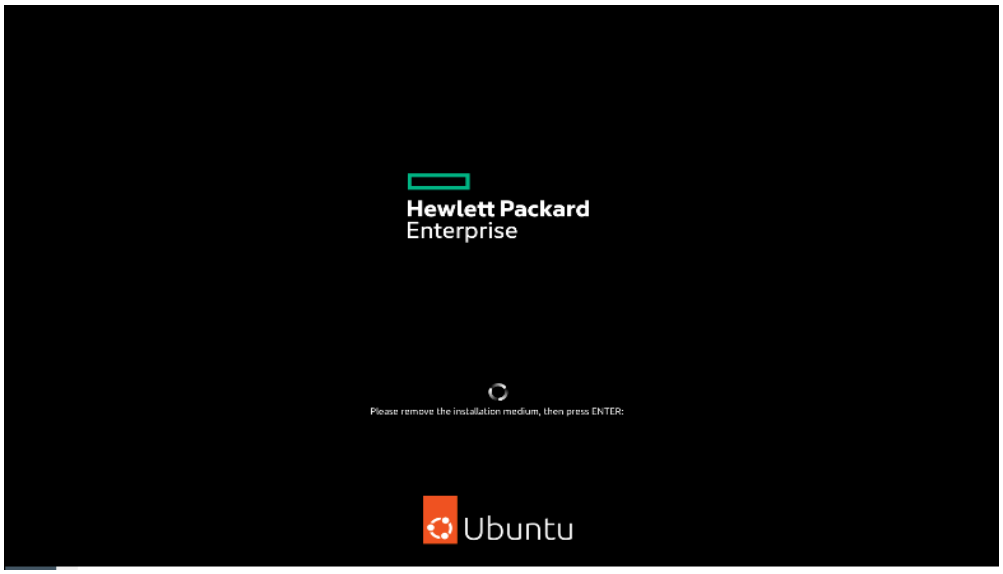


***Figura 42*:** Instalación de Ubuntu en servidor

4.4.2 Cambio a IP estática del servidor

En esta configuración en primer orden se debe de averiguar cuál es la IP de nuestro servidor de video, es así como en la ventana de la terminal se ejecuta el comando *ifconfig* la cual da los datos de la red ipv4 de manera similar da a conocer la puerta de enlace, de igual modo se ingresó

el comando *sudo nano /etc/network/interfaces*, dentro del archivo se debe de ingresar los valores que hemos generado en el direccionamiento de red.

***Figura 43*:** Cambio de IP

De modo que al terminar el ingreso de las configuraciones de red guardamos con control x y salimos del nano a continuación se debe de reiniciar las interfaces de red por lo que se ejecuta el comando *sudo /etc/init. d/networking restart* u ocupar el comando *sudo ifconfig eth0 up* seguidamente comprobamos las configuraciones realizadas de forma gráfica en los detalles de red de nuestro servidor para observar el cambio de ip estática realizado con éxito

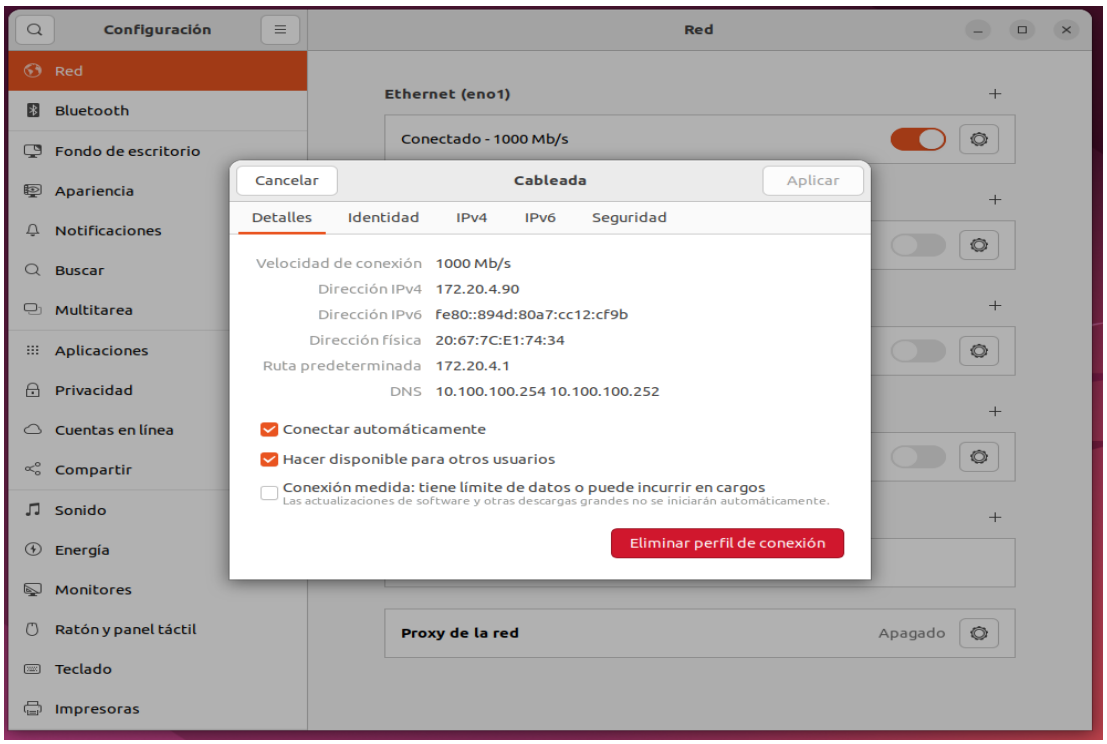


***Figura 44*:** Datos de IP del servidor

4.4.3 Instalación de sistema Shinobi y creación de cuentas super usuario y clientes

Realizado el cambio de IP y reiniciado el servidor se continuo con la instalación del sistema de video Shinobi, abriendo la terminal del sistema se ejecutó los siguientes comandos

#Sudo su

#apt update && apt install curl wget nano net-tools -y

#sh < (curl -s https://cdn.shinobi.video/installers/shinobi-install.sh)

Para finalizar la instalación se selecciona **Ubuntu- Fast Touchless** que al finalizar nos dará los datos de ingreso a la interfaz del sistema Shinobi**,** de igual manera se abrió el navegador del servidor, al mismo tiempo se tipeo la dirección IP de nuestro servidor de video para poder ingresar como super usuario utilizando las credenciales que el sistema dio al momento de la instalación como recalca en la captura de pantalla

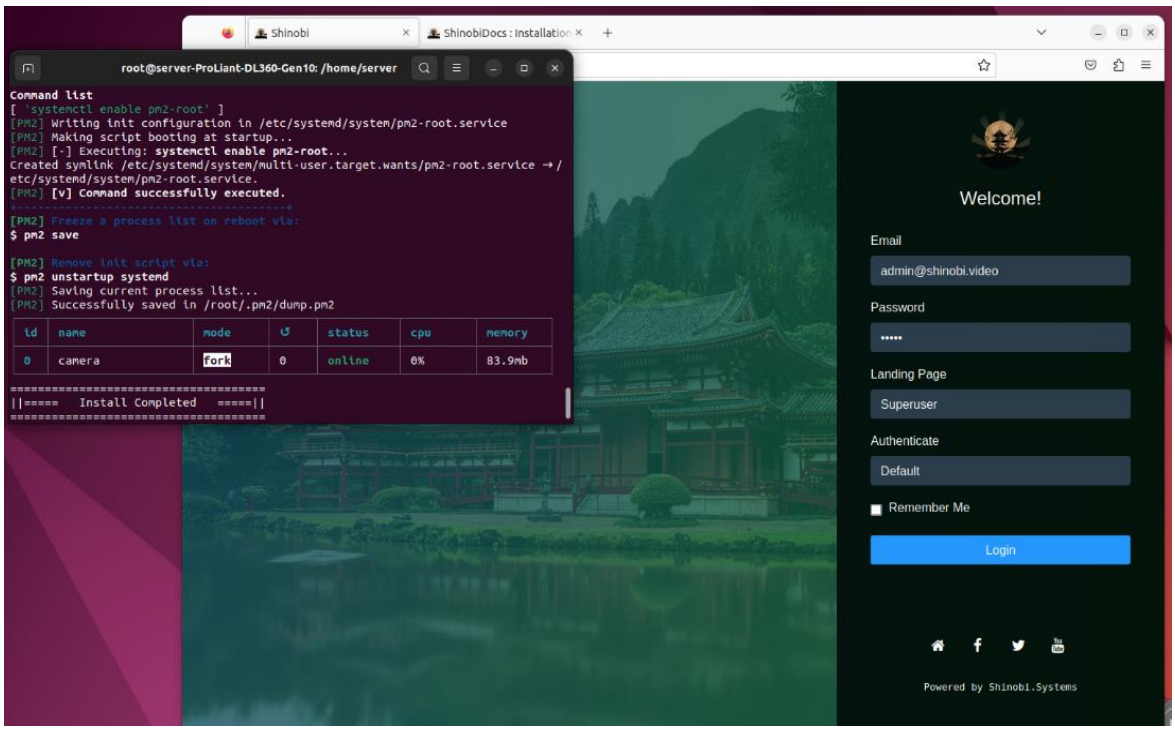


Figura 45: Instalación de Shinobi

Antes de seguir con la configuración del servidor de video se realizó el cambio de credenciales de ingreso al super usuario por lo que dentro de la interfaz en la cinta de opciones se eligió el botón de preferencias, por lo tanto, se procedió al cambio de correo y contraseñas que el sistema da por defecto teniendo muy en cuenta el tipo de contraseña ya que si de alguna manera es olvidada toca realizar cambios en el archivo conf. json

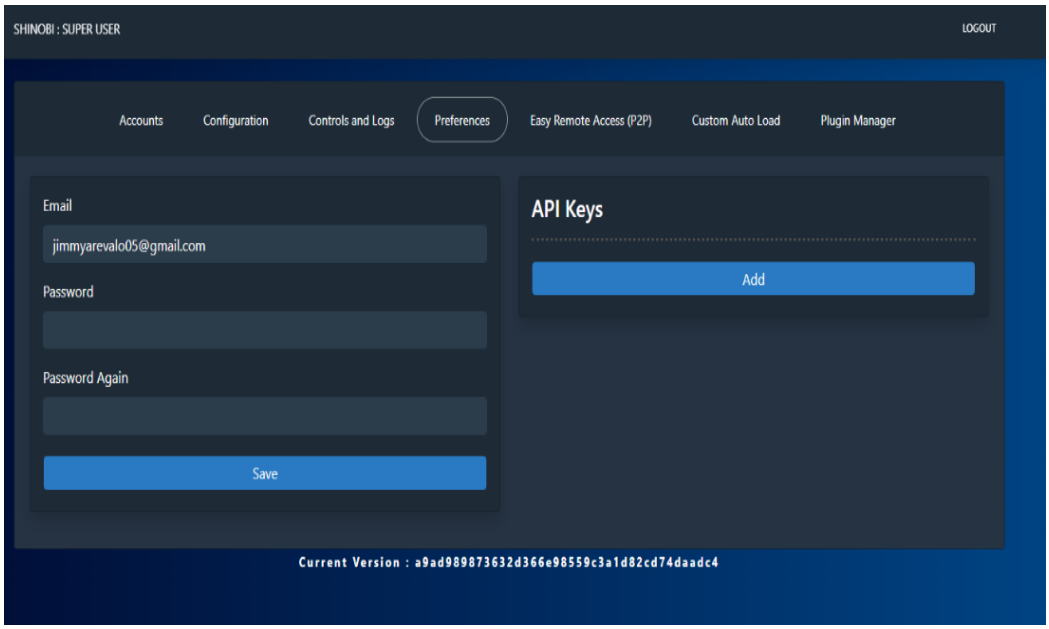


Figura 46: Interfaz de super usuario

Continuando al momento de ingresar al servidor del sistema de video vigilancia se debe de crear el cliente, de esta manera en la cinta de opciones elegimos **accounts** y presionamos en el botón **+add** que mostro un formulario el cual se llenó los datos con información del cliente, en esta parte como super usuario se debe otorgar los privilegios necesarios para dar paso a todos los componentes del sistema, así como muestra la imagen

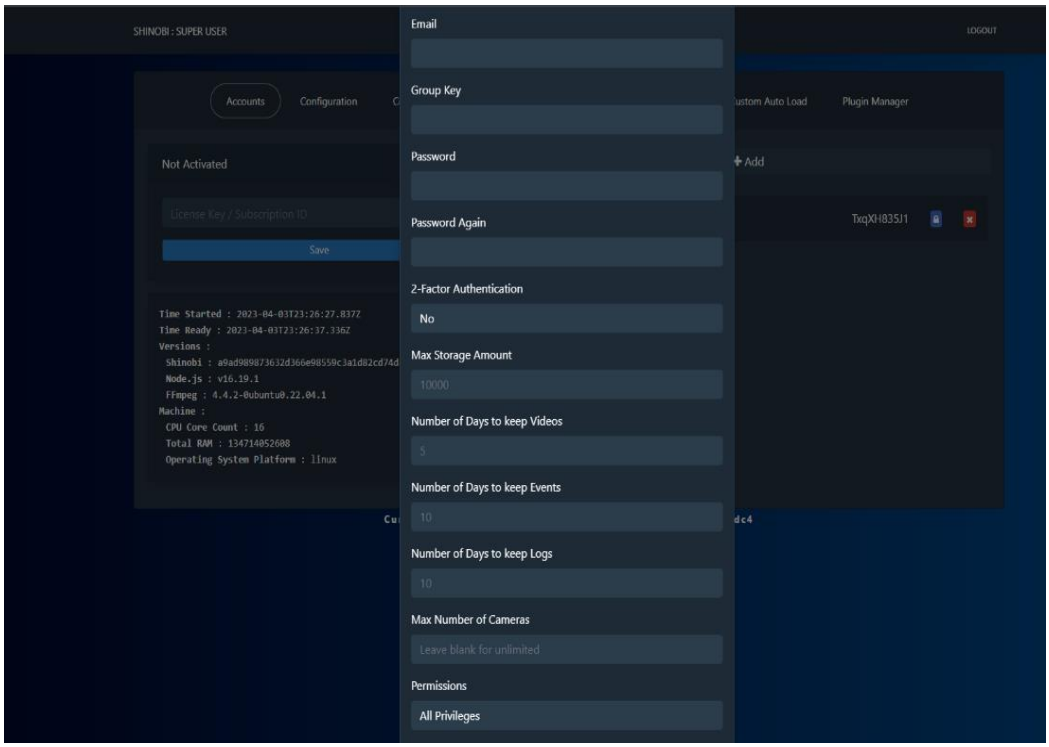


***Figura 47*:** Creación de usuarios

Ingresado todos los datos pertinentes nos muestra toda la interfaz con los datos del servidor además de todas las cuentas creadas en el servidor como super usuario al momento de mirar el estado del servidor esta no activado por lo cual se puede activar mediante la compra de algún servicio del mismo sistema, de tal manera en este proyecto que se realizó ocupamos la versión de software libre las demás configuraciones se activan mediante ingreso de librerías en el sistema sin tener una suscripción, como el sistema resalta no es impedimento para poder utilizarlo con todos los componentes y configuraciones

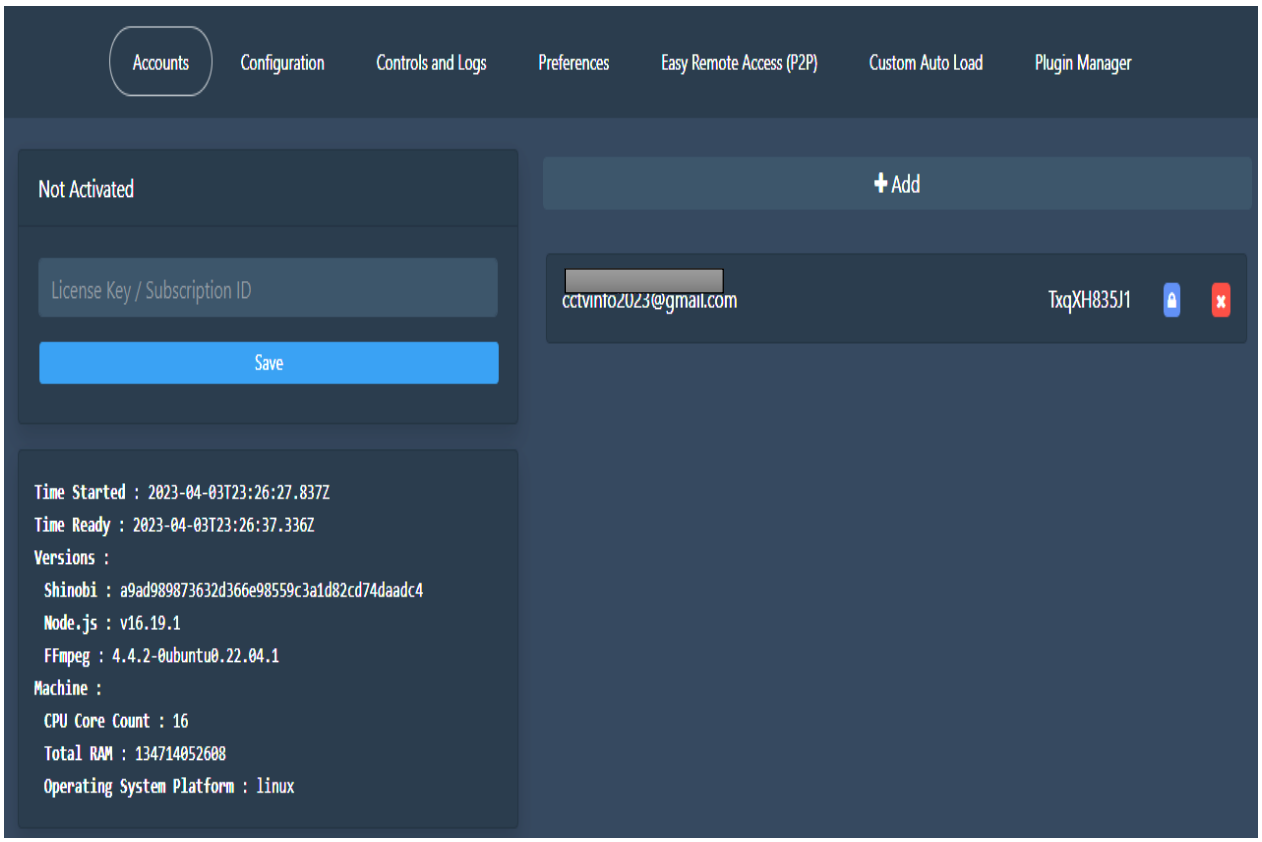


***Figura 48*:** visualización de usuarios

Realizados los cambios se tuvo que reiniciar el servidor para eso en la cinta de opciones en **Controls and Logs** se elige el botón **Restart core** como super usuario para guardar todos los cambios del servidor, así como se puede observar en la imagen el sistema está corriendo para dar ingreso a los clientes y acoger a todas las configuraciones pertinentes que se realice en sistema de video vigilancia

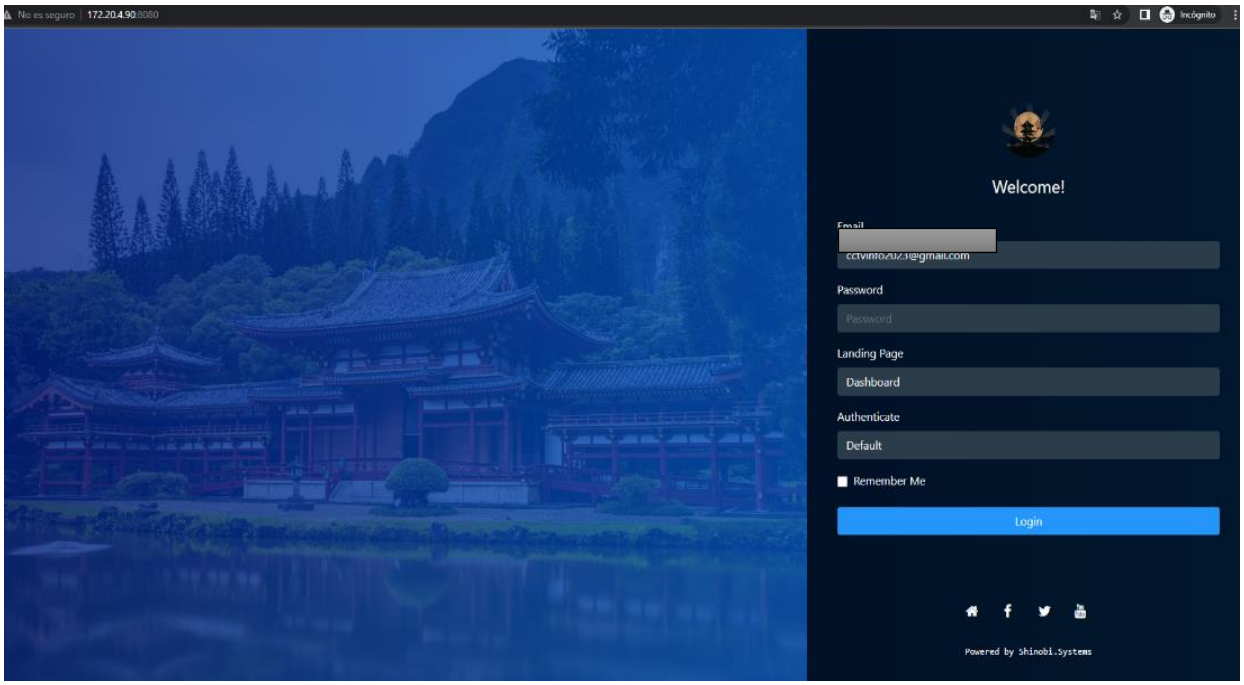


***Figura 49*:** Interfaz de usuario

Una vez ingresado las credenciales ingresa y se puede contemplar la interfaz del cliente con todas las opciones para configurar los monitores de tal modo que ya se puede ingresar todos los monitores o cámaras que se desee usar, teniendo en cuenta que para poder ingresar la cámara se debe de tener en cuenta la tabla de direccionamiento del proyecto para asignar una IP estática a la cámara y pueda hacer conexión con el sistema Shinobi

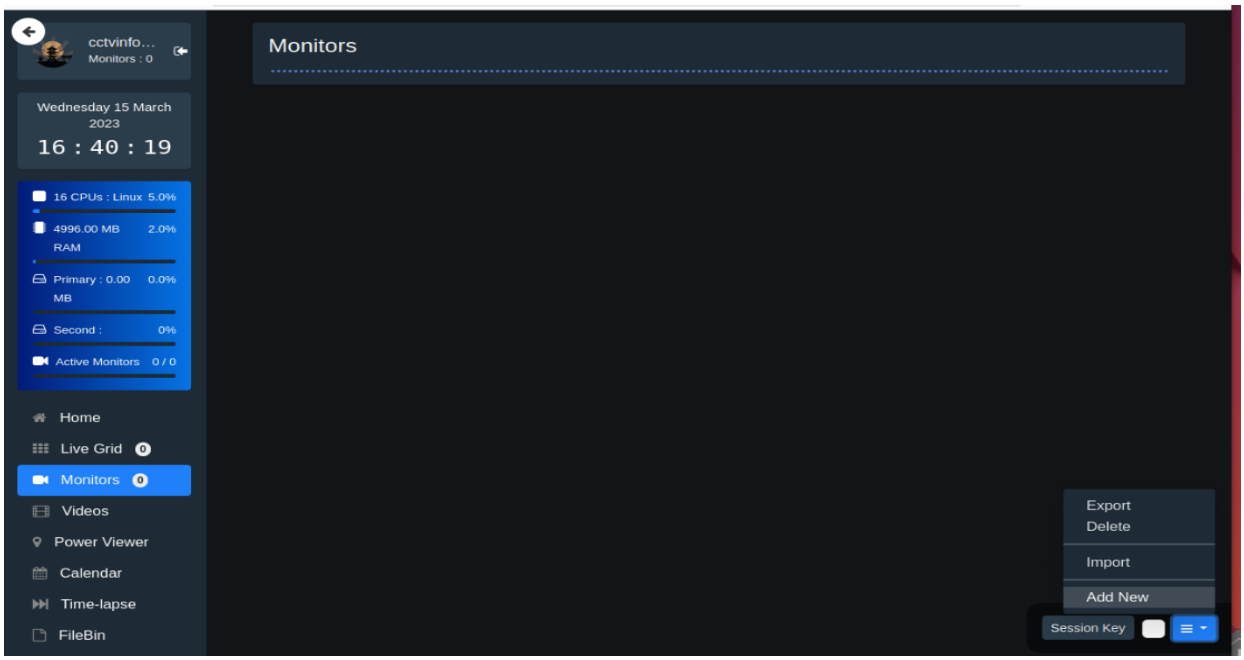


Figura 50: Página principal de usuario

4.5 Implementación

4.5.1 Tendido de cable

El cableado para el sistema de video vigilancia generalmente implica la instalación de cables para conectar las cámaras de seguridad al sistema de grabación y monitoreo. A continuación, se describirá los pasos que se usó para cablear el sistema de CCTV en los laboratorios y pasillos de la carrera de computación.

Con la ayuda de las herramientas IP video System Desing Tool que se usó anteriormente en la investigación se pudo planificar correctamente el tendido del cableado del sistema antes de comenzar, de tal manera que se determinó la ubicación de la cámara y la ruta del cable desde la cámara hasta el sistema de grabación o vigilancia así mismo se consideró la distancia, el tipo de cable que se usó y cualquier obstáculo o restricción que se pueda encontrar en el camino, es así como se eligió el tipo de cable de red (Ethernet) categoría 6 porque son adecuados para distancias largas, los cables de red par trenzados (UTP) cumplen con los requisitos técnicos de longitud grosor y calidad así mismo son más flexibles y fáciles de usar para distancias cortas. Se realizo una preparación del cable para cortar a la longitud deseada teniendo en cuenta el recorrido que se va a realizar, es así como se tomó un extremo del cable y se cableo por el cielo raso de los laboratorios teniendo en cuenta todas las herramientas a utilizar como muestra en la imagen.

Figura 51: Herramientas y Cable UTP

Por otro lado, en el edificio de Aulas 2 en los laboratorios de FATLAB y realidad aumentada se procedió a realizar una conexión eléctrica con un cable numeración 12 además de un tomacorriente ya que los equipos switch de este edificio no cuentan con la tecnología poe es así como para poder hacer el uso de las cámaras era necesario tener los cargadores de las cámaras que usan 1.5A para hacer uso eficiente de las imágenes que capturan las cámaras es así que en un extremo de la cámara ya se utilizarían los dos puertos.

Figura 52: Instalación eléctrica

De manera similar al momento de comenzar con el cableado se recurrió a utilizar una escalera con la cual se pudo tirar del cable a través de los conductos existentes del cable de red además de usar las diferentes aperturas de pared o techo para asegúrese de que los cables estén bien protegidos y no se dañen durante la instalación de la misma manera dejar un óptimo tendido de cable. De igual manera al terminar con el tendido de cableado se ponchó los extremos con los conectores RJ45 de forma 568 B para así tener una conexión establecida en ambos entremos de la cámara de seguridad al switch que tiene conexión con el NVR, por lo tanto, por el cielo raso el cableado se debió mantener en orden ya que los cables no deben de salir del lugar designado ya que al no cumplir con lo maquetado no estaríamos cumpliendo con lo requerido

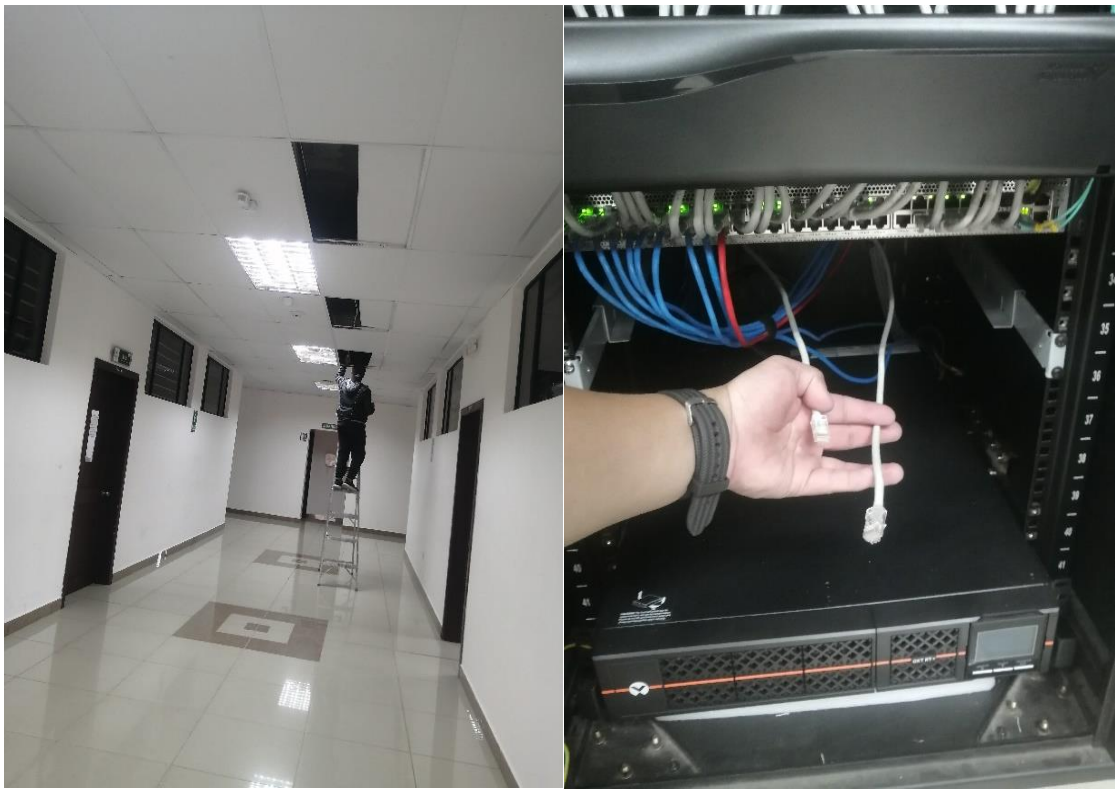


Figura 53: Cableado de red y ponchado

4.5.2 Instalación y configuración de cámaras

Seguidamente se realizó la instalación y conexión de las cámaras una vez que los cables ya estaban en su lugar, se conectó cada extremo del cable a las cámaras de seguridad, del mismo modo se conectaron los conectores RJ45 al a los puertos del switch que se encuentran configurados con la VLAN en donde se encuentra nuestro dispositivo de grabación NVR por lo tanto podremos realizar las pruebas y revisar que nuestras cámaras se encuentren correctamente instaladas, Por otro lado se tuvo en cuenta el código de colores se encuentre muy bien ubicado en cada ranura del conector RJ45 y así generar una conexión optima entre los dos extremos así en la cámara de video vigilancia del mismo modo en el NVR que va a contener todas las grabaciones de las cámaras, de otro modo la imagen que se genere no puede ser vista en el servidor de video

***Figura 54**:* Conexión de cámara

Por otro lado, para verificar si las cámaras están en red desde la computadora en la barra de búsqueda se ingresó la IP que nos muestra en el manual de las cámaras, o así mismo se hizo uso de la herramienta de Hikvision SADP lo cual se conectó con un cable externo a la cámara para poder activarla ya que aquí nos muestra una ventana la cual nos pidió crear una nueva contraseña para el ingreso del menú de configuración como muestra en la imagen.

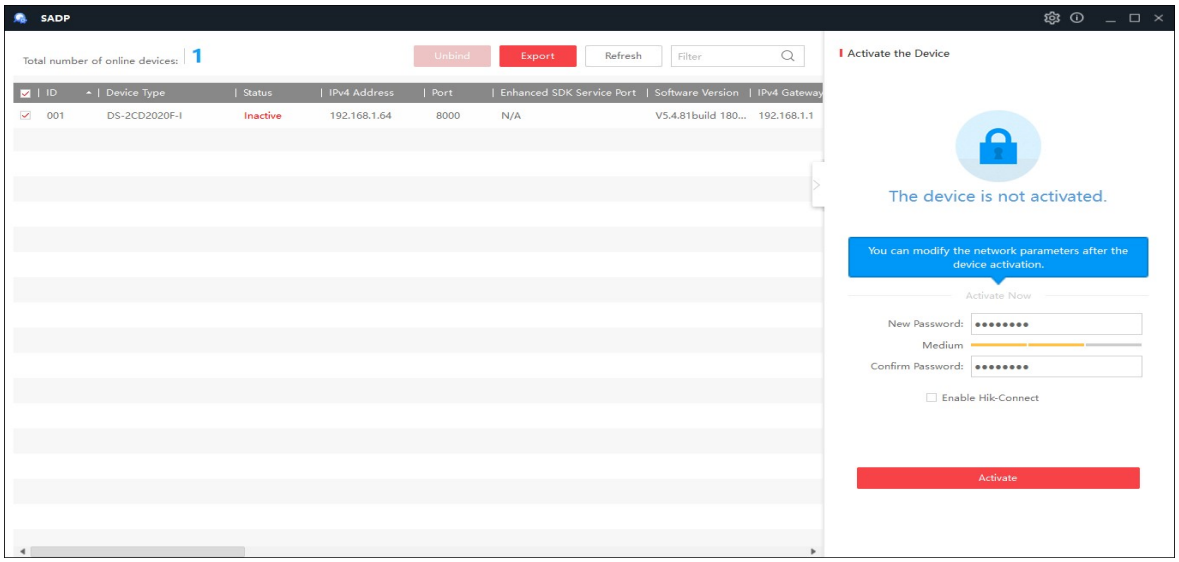


Figura 55: Activación de cámaras con herramienta SDAP

Seguidamente se procedió a ingresar la IP que se asignó en la tabla de enrutamiento que se generó anteriormente y así poder ingresar a la ventana de configuración de la cámara de video vigilancia, del mismo modo en el botón de configuración de la cámara se procedió a ingresar la

configuración de video y audio para ajustar la resolución de 1920*1080P y la velocidad de Frames que vamos a necesitar para que la Cámara capte las imágenes y sean enviadas a la sistema de grabación NVR del mismo modo la codificación de video se encuentre en H.264 por otro lado los ajustes de red muestra la dirección IPv4, mascara de subred y la IPv4 por defecto, por otro lado para la configuración de la hora de las cámaras en la cinta de opciones de configuración del sistema nos muestra el menú de ajuste de hora la cual podemos sincronizar automáticamente con la de la computadora que estamos realizando la configuración, tomando en cuenta la seguridad de cada cámara se usó contraseñas seguras así mismo se podría administrar otras contraseñas para el ingreso de las mismas

Figura 56: Configuración de cámaras

4.5.3 Configuración NVR

Para la configuración del sistema de videovigilancia Shinobi se hace uso de la cuenta que se generó en el servidor por el super usuario para ingresar, para ingresar se debe abrir el navegador de la computadora e ingresar la dirección IP de nuestro servidor de manera siguiente ingresar las credenciales así mismo se abre el panel de control de las herramientas de Shinobi que se encuentra en el lado izquierdo de la pantalla. Después de iniciar sesión se debe de ingresar a la página y seguidamente en **configuración de la cuenta**, aquí podremos personalizar las configuraciones básicas de nuestro sistema como la zona horaria, el idioma y las preferencias de visualización y al finalizar guardar los cambios.

De la misma manera para añadir las cámaras en el lado izquierdo en el menú se encuentra el botón **configuraciones de monitor**, ya en esta ventana en el lado inferior derecho muestra el

botón de añadir nuevo monito el cual al dar clic nos muestra un menú a completar con la dirección IP el puerto, el nombre de usuario y la contraseña y así dar acceso a la nueva cámara que se ha ingresado.

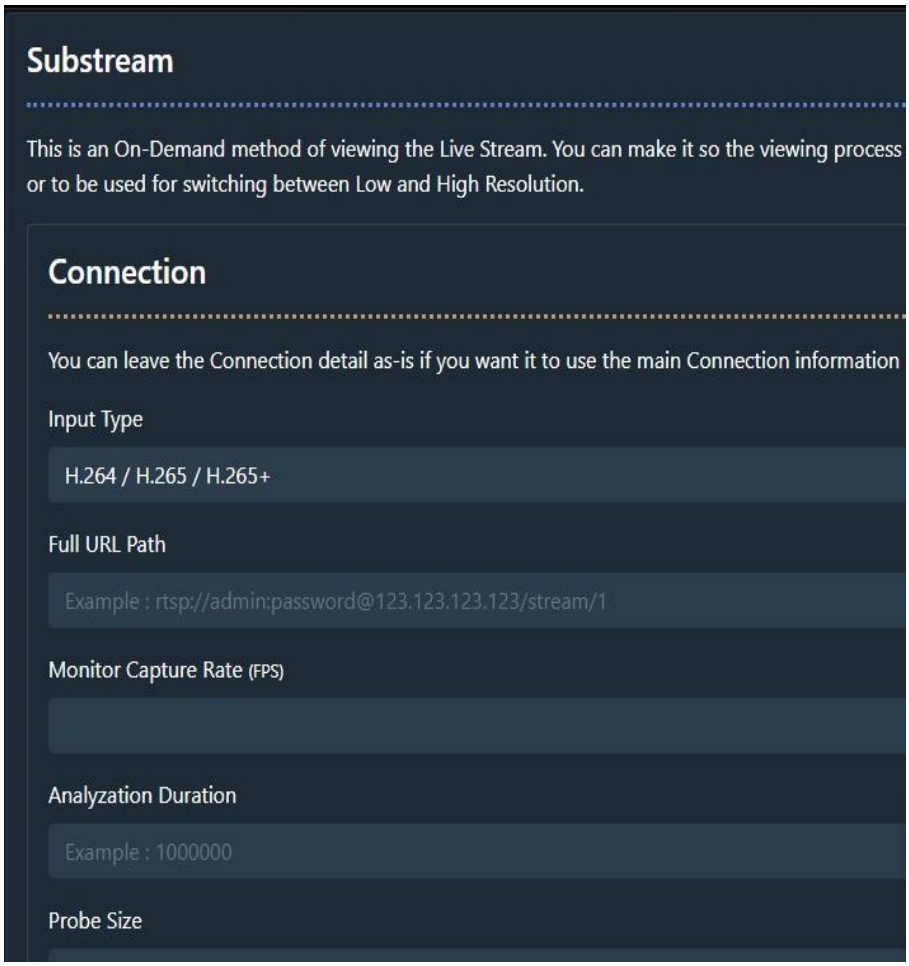


***Figura 57**:* Agregar cámara

Después de realizar el ingreso de la Cámara debemos de hacer la visualización en tiempo real la cual se puede mirar desde el menú de Shinobi, tomando en cuenta que este paso si izo después de configurar las cámaras para ver las transmisiones en tiempo real, desde la sección monitor se seleccionó la cámara deseada y esta apareció en vivo en la pantalla así mismo se puede ver varias vistas en tiempo real al mismo tiempo. De manera similar para activar la grabación de la Cámara se debe de dirigir a la configuración del monitor y en la parte derecha se despliega una ventana con las opciones de configuración de la Cámara, así nos dirigiremos al apartado de grabación para elegir el tipo de grabación, codificación de grabación y el intervalo de minutos a grabar

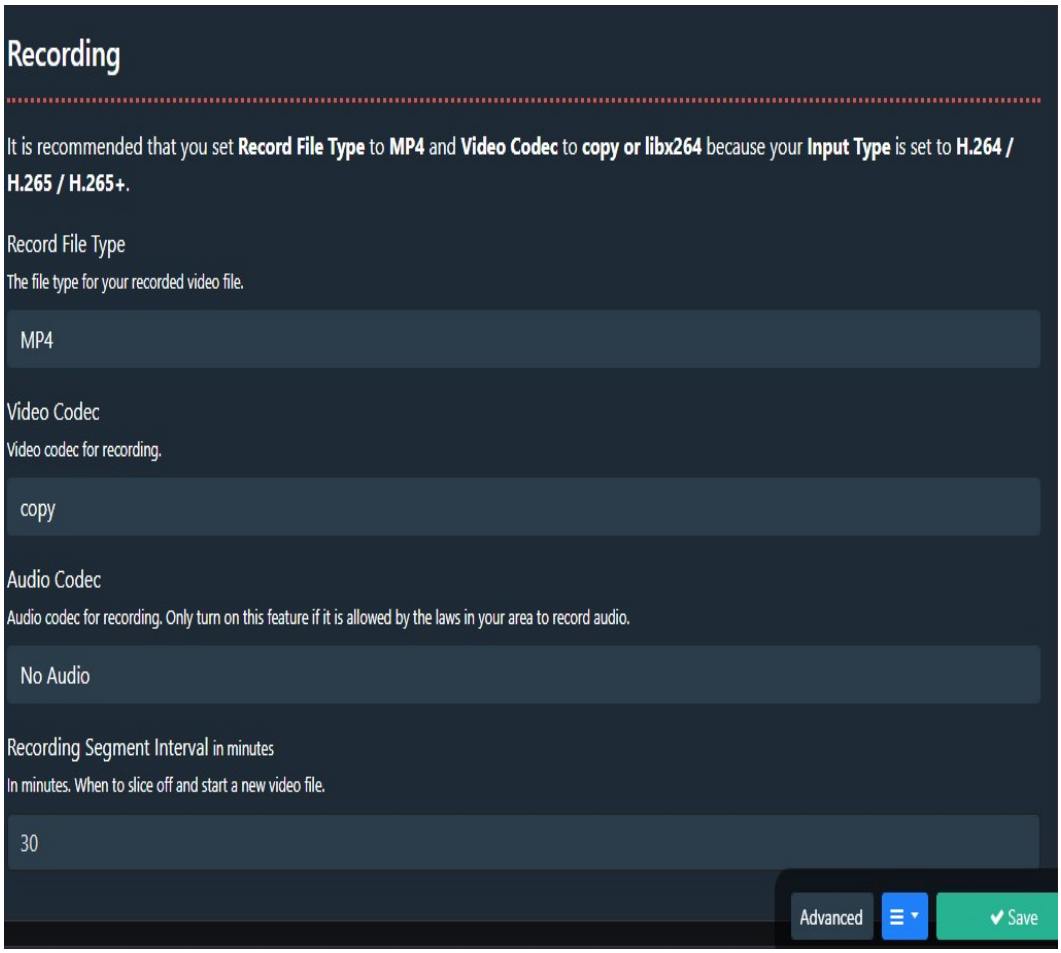


***Figura 58*:** Configuración de grabación

Para acceder a las transmisiones en vivo y las grabaciones se ingresó a la interfaz de Shinobi al lado izquierdo del mismo modo seleccionamos una cámara o el monitor que acabamos de ingresar, así mismo se señaló la pestaña línea tiempo con los vídeos que se generan y allí se encontrarán todas las grabaciones disponibles para reproducirlas, también contaremos con todas las cámaras que se han ingresado para así mismo acceder a las grabaciones y detecciones de movimiento con los parámetros correspondientes. Por otra parte, las configuraciones de detección de movimiento y la creación de eventos para la visualización cuando se genera un evento así mismo con las notificaciones son opcionales ya que se genera un tráfico de datos más grande al generar toda esta información así mismo el CPU del servidor se vuelve más lento, estas configuraciones son recomendables con una tarjeta gráfica más aceptable.

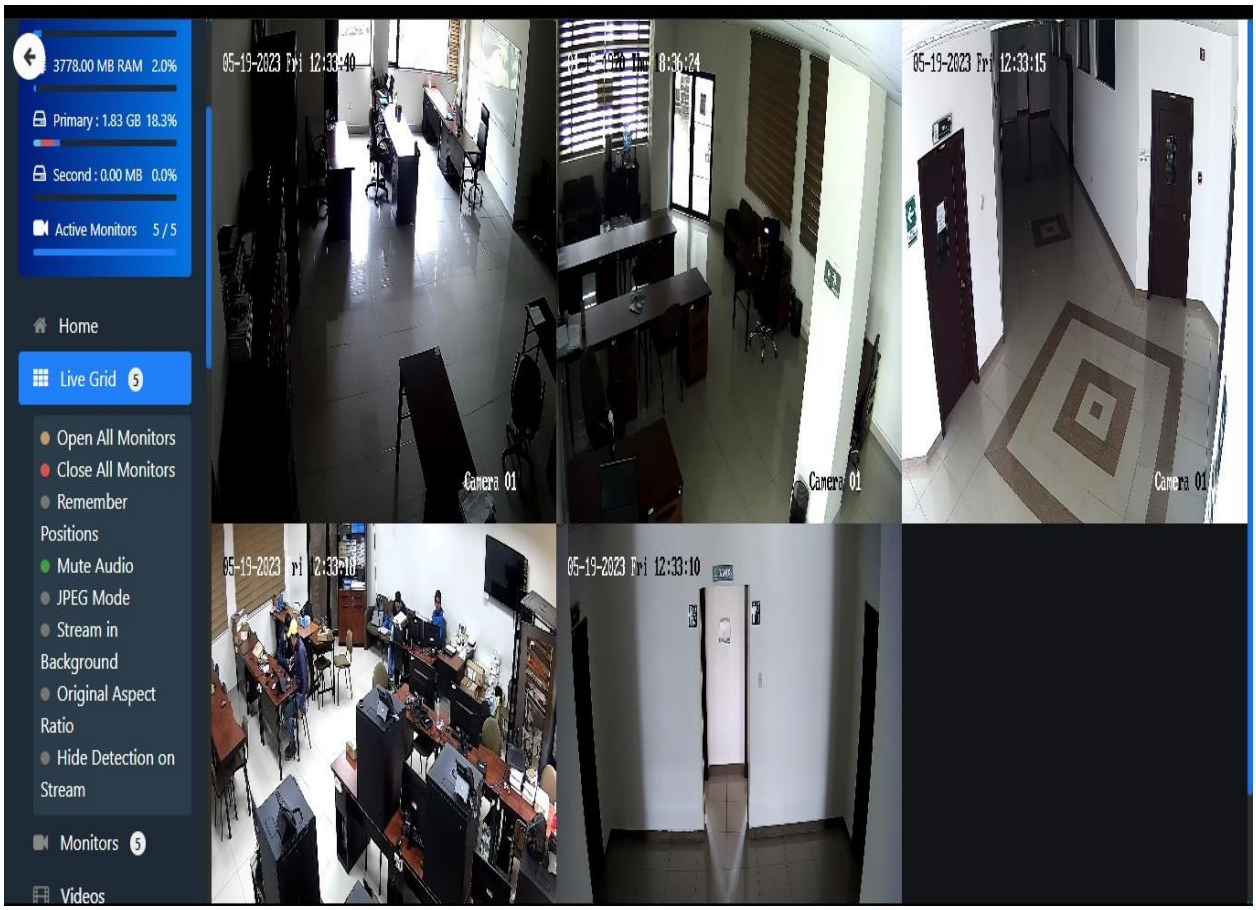


Figura 59: Visualización de monitores

4.6 Pruebas

Ya asegurado el funcionamiento correcto del sistema de video vigilancia con las cámaras correctamente instaladas y grabando, además de capturar los videos en una línea de tiempo de acuerdo con las características de las configuraciones se realizaron las pruebas de conexión, enfoque, cobertura, almacenamiento, monitoreo.

4.6.1 Cobertura

Las pruebas de cobertura que se realizaron en el sistema de video vigilancia implicaron en hacer la verificación, eficiencia de la altura y enfoques de las cámaras de seguridad para así cubrir los puntos ciegos así mismo identificar los posibles obstáculos que puedan afectar la calidad de imagen al instalar las cámaras según las especificaciones de los fabricantes de tal manera que se pudo tener la cobertura deseada como se muestran en algunas de las imágenes que siguen a continuación

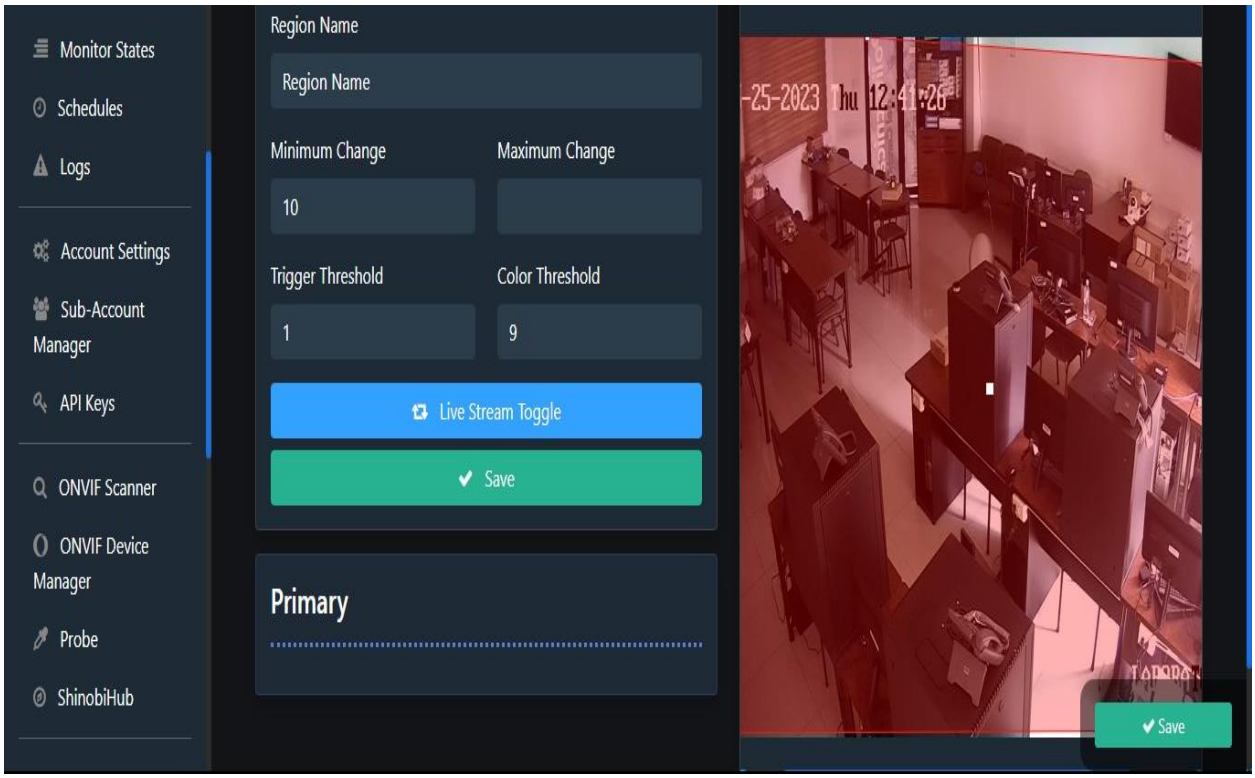


Figura 60: Cobertura laboratorio de redes

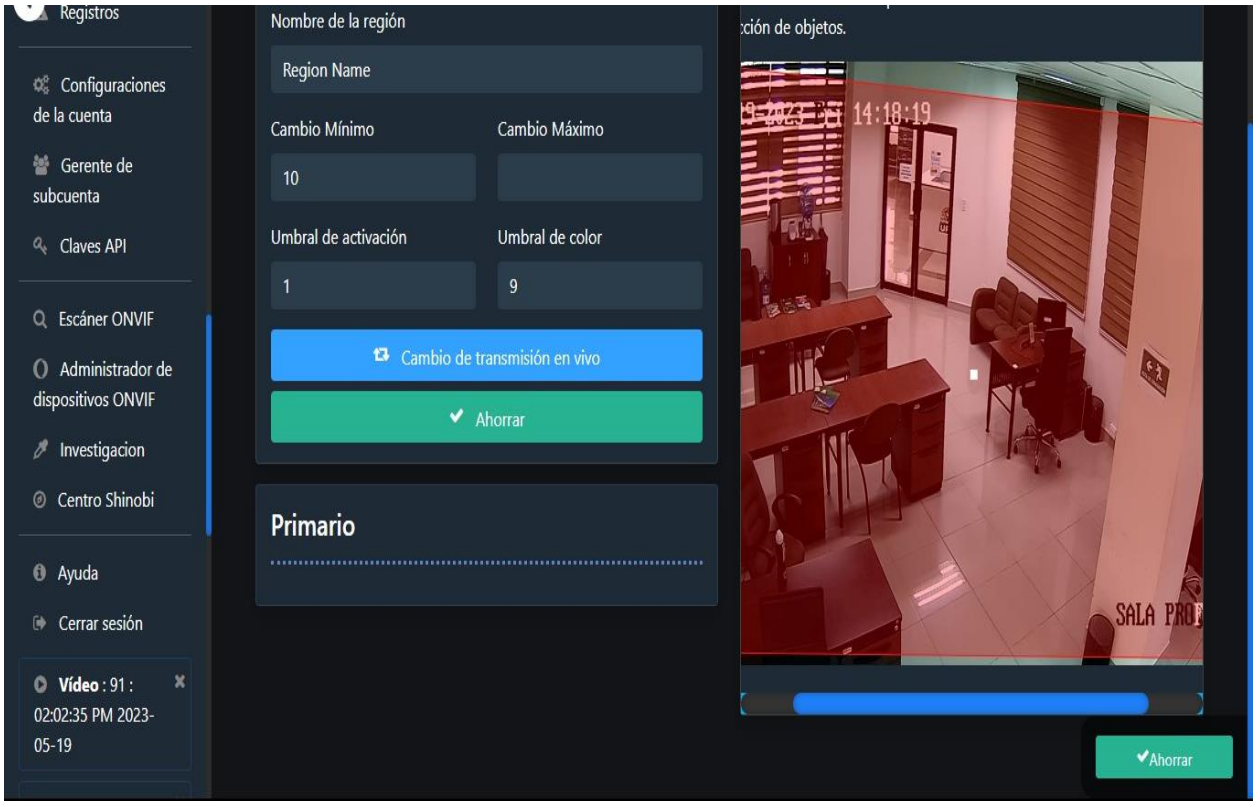


Figura 61: Cobertura sala de profesores

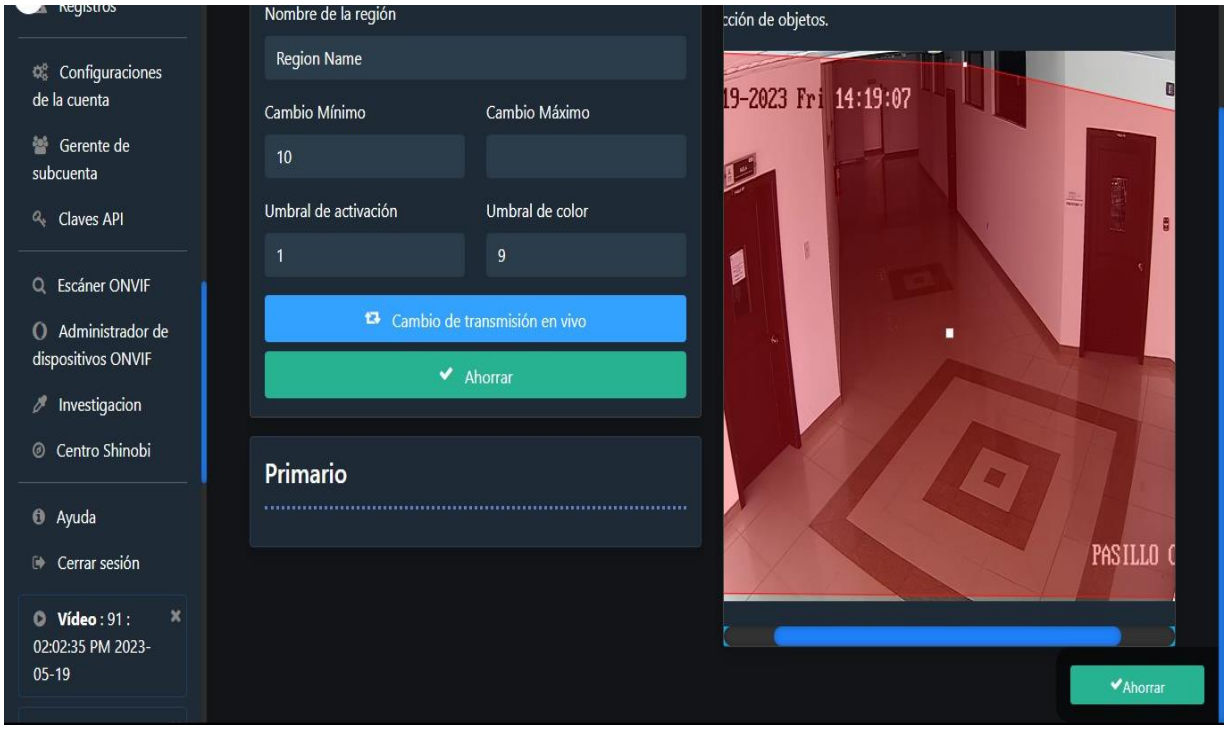


Figura 62: Cobertura a los pasillos de la carrera de computación

Dando solución a los obstáculos además de ángulos que se encontraban enfocadas las cámaras se las pudo calibrar la cobertura y así obtener una mejor imagen editando la región que anteriormente muestre las imágenes obteniendo una visión más aceptable que se ha de grabar en sistema de grabación de Shinobi

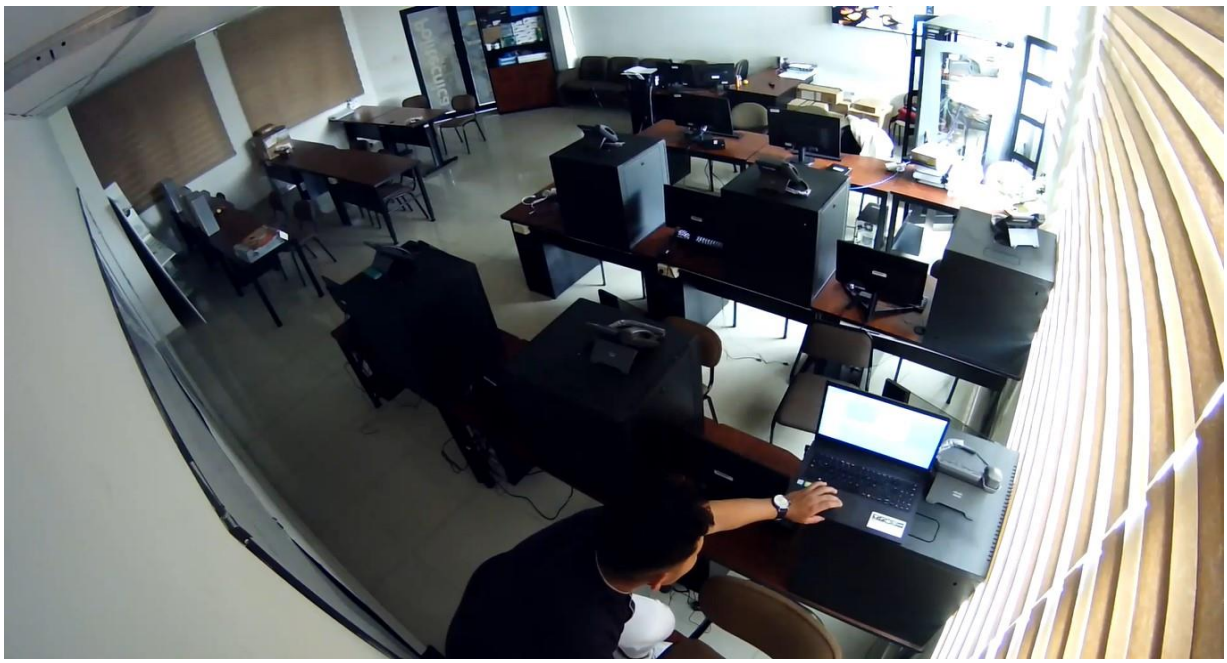


Figura 63: Corrección de región del laboratorio de redes

Figura 64: Corrección de región de sala de profesores

***Figura 65*:** Corrección de región pasillos de carrera

4.6.2 Visualización nocturna

Las pruebas de visualización se las realizo para evaluar la capacidad de las cámaras para capturar imágenes claras en condiciones de poca luz o tengan una iluminación mínima, de tal manera que el infrarrojo de las cámaras mejora la visión nocturna y la imagen tenga calidad así mismo pueda ser observada además que el ruido no haga falta de detalles en las imágenes en

las grabaciones del NVR ya que las cámaras tienen que compensar el efecto en contra luz para detectar objetos y se pueden distinguir entre diferentes distancias

4.6.3 Extracción de información almacenada

La prueba de extracción de información se la realizo para tener datos relevantes de las grabaciones de video con la finalidad de analizar e investigar fechas y horas exactas de las grabaciones de las cámaras ya que se pueden ser identificación de una persona o asegurarse de que únicamente el personal con credenciales tenga acceso a los laboratorios así sea el caso de que se requiera algún tipo de grabación el encargado se la facilite a la autoridad que lo requiera ya que para realizar este proceso se debe realizar por profesionales especializados en video vigilancia

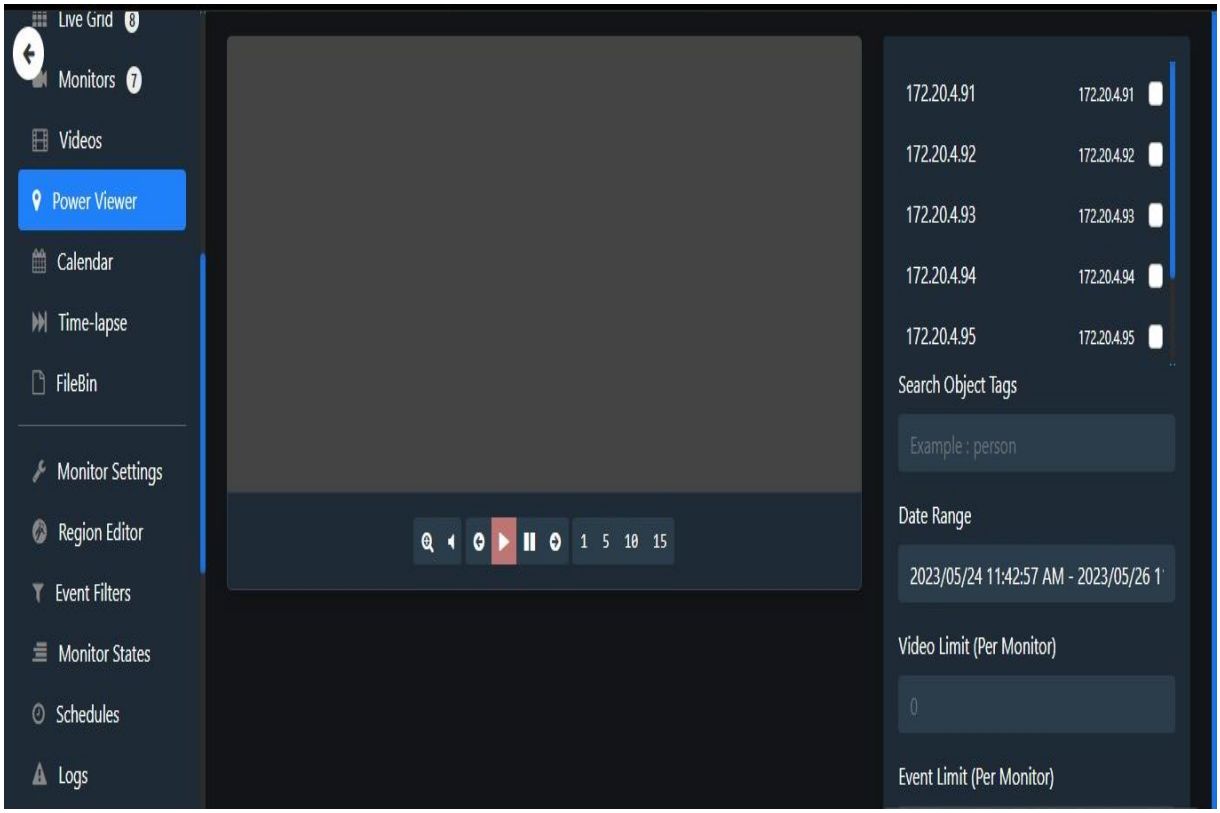


***Figura 66*:** Visualización de videos del sistema

Capacidad de almacenamiento del sistema que constantemente está en cambio y dirección donde se puede hacer la extracción de datos

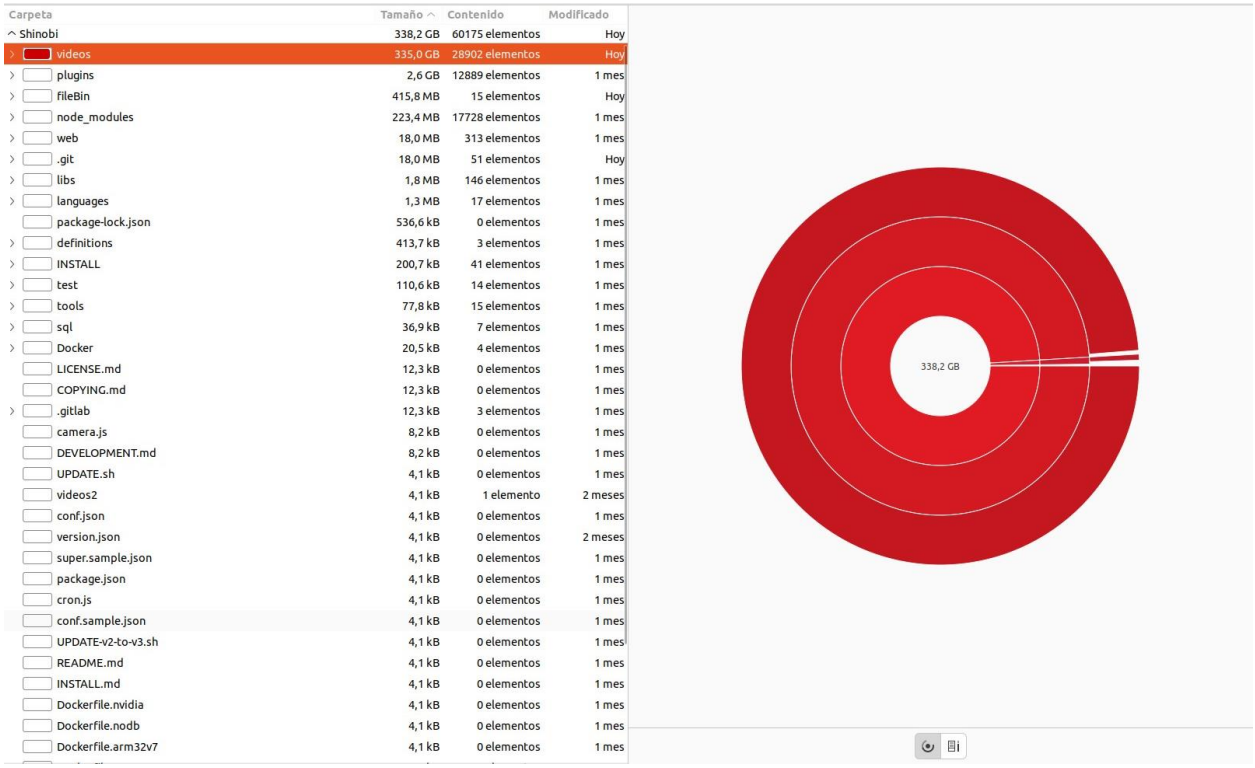


***Figura 67*:** Almacenamiento de videos del sistema

V. CONCLUCIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

- Se determino por medio de la recolección de información a través de las encuestas, entrevistas al personal de tics incluyendo a los docentes de la carrera sobre el sistema de video vigilancia de la universidad para tener una visión precisa sobre el tema investigado del mismo modo se usó revistas, artículos, tesis e internet que contribuyeron al desarrollo y soporte del proyecto
- Se diagnostico los estándares de calidad existentes dentro del sistema de video vigilancia actual de tal manera que se planteó una solución informática con estándares idénticos para que funcione de forma robusta y confiable para la seguridad así mismo también la supervisión de las instalaciones de la carrera de computación.
- Los componentes tecnológicos del sistema de video vigilancia que brindo el laboratorio de redes se examinaron detalladamente para determinar que cumplan con los estándares de calidad y características adecuadas que puedan complementar el diseño e implementación del sistema
- La implementación del sistema es una solución sólida y versátil que cubre las necesidades de seguridad al monitorear los dispositivos tecnológicos y así mismo a las instalaciones de la universidad que contribuyen a la educación de los estudiantes
- Una ventaja del sistema es la compatibilidad con una amplia variedad de cámaras IP, es decir distintas marcas y modelos entre otros dispositivos de video vigilancia lo que permita integrarse con el sistema de video vigilancia de la universidad para actualizar la infraestructura de seguridad sin tener la necesidad de remplazar los dispositivos
- El sistema de video vigilancia Shinobi creado en el servidor HPE por su capacidad de almacenamiento que es un RAID 1+0 en modo espejo tiene la ventaja de hacer un respaldo de información y del mismo modo al fallo de dos discos duros el sistema sigue funcionando normalmente hasta realizar un cambio de los discos duros que ya no sirven.
- Gracias a la capacidad del servidor el sistema de video vigilancia es escalable por tener la capacidad de procesar una gran cantidad de datos que se envían desde las cámaras, de manera similar ya que Shinobi no es un sistema invasivo vale decir que con solo implementar el sistema en la red de la universidad se tuvo acceso a las cámaras instalas sin la necesidad de cablear diversos equipos.

5.2 RECOMENDACIONES

- Hacer el uso de estándares de calidad y normativas similares que fortalezcan las necesidades de grabación, almacenamiento y streaming que sean generadas por el sistema de video vigilancia SHINOBI
- Realizar una buena gestión, administración y control de los equipos en donde se encuentre alojado el sistema de video vigilancia para tener una buena supervisión de las grabaciones de las aulas y laboratorios.
- Al ingresar una cámara nueva al sistema se tenga en cuenta las credenciales de la cámara y del mismo modo si la cámara se encuentra activada o esté en el mismo segmento de red VLAN, de caso contrario no se puede hacer uso de la cámara que se desee ingresar, por lo tanto, las configuraciones que se realicen en las cámaras no necesariamente deben ser similares ya que si se desea se puede activar la detección de movimiento y para activarlo solo se deben de agregar las cámaras al evento
- Se recomienda que el personal que tenga acceso al servidor sea una persona con conocimientos solidos en sistemas de video vigilancia para poder manipular o monitorear las cámaras de la carrera de computación
- Para trabajos futuros se debería instalar una tarjeta gráfica que puede mejorar el sistema con los complementos de control de eventos, detección de movimiento, detección facial aprovechando la escalabilidad que tiene el sistema de este proyecto
- Considerar aumentar el almacenamiento del servidor de video para poder cubrir con los tiempos dispuestos con la normativa ya que el sistema actual cuenta solo con 2.4TB que tiene su respaldo por el RAID y el servidor tiene sócalos restantes vacíos para incrementar discos duros
- Realizar un plan de mantenimiento preventivo al Hardware y software del sistema

VI. REFERENCIAS BIBLIOGRÁFICAS

Abril, B., & Cuzco, P. (2019). *Implementación de un sistema de video vigilancia remoto para hogares, utilizando herramientas de software libre*. *(Tesis de pregrado).* Universidad Politécnica Salesiana sede Cuenca, Cuenca, Ecuador. https://dspace.ups.edu.ec/bitstream/123456789/17311/1/UPS-CT008253.pdf

Archlinux ARM. (2018). *Raspberry Pi 4*. https://archlinuxarm.org/platforms/armv8/broadcom/raspberry-pi-4

Baque, S. (2019). *IMPLEMENTACIÓN DE UN SISTEMA DE VIDEO VIGILANCIA MEDIANTE CÁMARAS IP PARA FORTALECIMIENTO DE LA SEGURIDAD EN LA PARTE POSTERIOR DE LA EDIFICACIÓN DE LA CARRERA INGENIERÍA EN COMPUTACIÓN Y REDES*. *(Tesis de pregrado).* Universidad Estatal del Sur de Manabí, Jipijapa, Manabí, Ecuador. http://repositorio.unesum.edu.ec/bitstream/53000/1958/1/UNESUM-ECU-REDES-2019-67.pdf

Bazurto, R., & Jaramillo, L. (2020). *Diseño e implementación de un módulo didáctico para pruebas físicas y simuladas, utilizando cables tipo coaxial y utp para uso de estudiantes de la carrera Ingeniería en Telecomunicaciones de la Universidad Politécnica Salesiana. (Tesis de pregrado).* Universidad Politécnica Salesiana, Guayaquil, Guayas, Ecuador. https://dspace.ups.edu.ec/bitstream/123456789/20743/1/UPS-GT003338.pdf

Caballero, F., Morales, M., Silva, E., & Caballero, D. (Junio de 2020). *Raspberry Pi, conectividad y programación mediante puertos GPIO*. *Revista de Ingeniería Innovativa, 4*(14), 1-13. doi: 10.35429/JOIE.2020.14.4.1.13

CARCHI AL DÍA. (17 de Noviembre de 2021). *COOPERATIVA PABLO MUÑOZ VEGA Y ECU 911 TULCÁN FIRMAN CONVENIO PARA FORTALECER VIDEO VIGILANCIA*. *Carchi al día*. https://carchialdia.com/2021/11/17/cooperativa-pablo-munoz-vega-y-ecu-911-tulcan-firman-convenio-para-fortalecer-video-vigilancia/

Chaglla, J., & Villa, L. (26 de mayo de 2021). *Estudio técnico de implementación de un sistema de video vigilancia IP para el control de la seguridad de las áreas administrativas, aulas, talleres, laboratorios, etc. En los Campus Centro y Belisario Quevedo de la Universidad De Las Fuerzas Armadas ESPE*. *(Tesis de pregrado).* Universidad De Las Fuerzas Armadas ESPE, Quito, Pichincha, Ecuador. Silo.Tips. https://repositorio.espe.edu.ec/bitstream/21000/25383/1/M-ESPEL-SIT-0110.pdf

CISCO. (05 de Noviembre de 2021). *Hoja de datos de los switches de las series Cisco Catalyst 2960-X y 2960-XR*. https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-2960-x-series-switches/datasheet_c78-728232.html

CISCO. (25 de Agosto de 2021). *Hoja de datos del enrutador de servicios integrados de la familia Cisco 4000*. https://www.cisco.com/c/en/us/products/collateral/routers/4000-series-integrated-services-routers-isr/data_sheet-c78-732542.html

Contero, W. (Marzo de 2019). *DISEÑO DE UNA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN BASADA EN LA NORMA ISO 27002:2013, PARA EL SISTEMA DE BOTONES DE SEGURIDAD DEL MINISTERIO DEL INTERIOR. (tesis de postgrado).* Universidad Internacional SEK, Quito, Pichincha, Ecuador. Seguridad informática. https://repositorio.uisek.edu.ec/bitstream/123456789/3345/1/TESIS%20MC%2026_03_2019.pdf

Cuesta, J. (2021). *GESTIÓN DE VIDEO STREAMING MEDIANTE DISPOSITIVOS IOT*. *(Tesis de pregrado).* Universidad Técnica de Machala, Machala, EL oro, Ecuador. http://repositorio.utmachala.edu.ec/bitstream/48000/16885/1/TTFIC-2021-IS-DE-00004.pdf

Dianca A. (2019). *Estándar ANSI/TIA/EIA-568-B.* ESTANDAR ANSI. http://saber.ucv.ve/bitstream/10872/507/3/APENDICE-dianca%20tesis.pdf

Duran, M., López, Á., & Prada, C. (2019). DISEÑO DE UN SISTEMA DE VIDEO VIGILANCIA POR MEDIO DE ENLACES MICROONDAS PARA LA EMPRESA DISAM SUCURSAL SANTA MARTA. *(Tesis de pregrado).* Universidad Cooperativa de Colombia, Santa Marta, Magdalena, Colombia. Recuperado de: https://repository.ucc.edu.co/bitstream/20.500.12494/6175/1/2018_dise%C3%B1o_sistema_vigilancia.pdf

Echeverría, J. (2020). TESIS DE DIPLOMA EN OPCIÓN AL TÍTULO DE INGENIERO EN TELECOMUNICACIONES Y ELECTRÓNICA. *(Tesis de pregrado).* Universidad Tecnológica de La Habana, La Habana, Cuba. https://www.researchgate.net/profile/Yilian-Castillo-Romero-2/publication/348356105_Raspberry_Pi_como_solucion_de_NVR_y_VMS_para_redes_IP_de_video-vigilancia/links/5ff9d76a45851553a032ed4a/Raspberry-Pi-como-solucion-de-NVR-y-VMS-para-redes-IP-de-video-vig

Enriquez, C., Arcos, G., & Mina, J. (2019). Propuesta de una metodología para la enseñanza de la investigación formativa en educación superior. *SATHIRY*, 15. http://revistasdigitales.upec.edu.ec/index.php/sathiri/article/view/803/868

Estandar IEEE. (27 de Marzo de 2017). *Estandar IEEE 802*. Recuperado de: http://ieee802blognana.blogspot.com/

FS community. (18 de Enero de 2022). *¿Qué es un inyector PoE y cómo utilizarlo? Community*.https://community.fs.com/es/blog/what-is-a-poe-injector-and-how-to-use-it.html

Gerra, V. (2019). Diseño e Implementación de la red de datos del laboratorio centro de desarrollo de software y productos IOT de la facultad de ingeniería de la Universidad Católica de Santiago de Guayaquil. *(Tesis de Pregrado)*. Universidad Católica de Santiago de Guayaquil, Guayaquil, Guayas, Ecuador. http://repositorio.ucsg.edu.ec/bitstream/3317/13883/1/T-UCSG-PRE-ING-CIS-247.pdf

Heredia, C., & Rea, D. (2022). DISEÑO DE UN SISTEMA DE DETECCIÓN FACIAL UTILIZANDO CÁMARAS IP PARA EL RECONOCIMIENTO DE INDIVIDUOS EN LA CERCANÍA DE RESIDENCIAS FAMILIARES. *(Tesis de pregrado)*. Universidad Politécnica Salesiana Sede Quito, Quito, Ecuador. https://dspace.ups.edu.ec/bitstream/123456789/23050/1/UPS%20-%20TTS866.pdf

Hewlett Packard. (2022). *Descripción general del servidor HPE Proliant DL360 Gen10*. https://support.hpe.com/hpesc/public/docDisplay?docId=a00018801es_es&docLocale=es_ES

Hewlett Packard Enterprise. (2023). *Servidor HPE ProLiant DL360 Gen10 Hoja de datos*. HPE PROLIANT DL360 GEN10 SERVER. https://www.hpe.com/psnow/doc/PSN1010007891MXES.pdf

HIKVISION. (2019). *Cámara mini bala fija de 2 MP*. https://www.hikvision.com/es-la/products/Turbo-HD-Products/Turbo-HD-Cameras/Value-Series/ds-2ce16d0t-irpf-c-/

IEEE. (2022). *Programa IEEE GETTM*. Recuperado de: IEEE 802.3™: Ethernet. https://ieeexplore.ieee.org/browse/standards/get-program/page/series?id=68

Jalca, S. (2019). ESTUDIO DE FACTIBILIDAD DE UN SISTEMA DE VIDEO VIGILANCIA CON CÁMARAS IP PARA EL LABORATORIO DE HARDWARE EN LA CARRERA DE INGENIERÍA EN COMPUTACIÓN Y REDES. *(Tesis de pregrado).* Universidad Estatal del Sur de Manabí, Jipijapa, Manabí, Ecuador. http://repositorio.unesum.edu.ec/bitstream/53000/1598/1/UNESUM-ECU-REDES-2019-44.pdf

Jinez, R., & Pantoja, C. (2020). TRABAJO PREVIO A LA OBTENCIÓN DEL TÍTULO DE TECNÓLOGO EN. *(Tesis de pregrado).* ESCUELA POLITÉCNICA NACIONAL, Quito, Pichincha, Ecuador. https://bibdigital.epn.edu.ec/bitstream/15000/21340/1/CD%2010856.pdf

Medium. (04 de Octubre de 2019). *¿Qué es un inyector PoE y cómo utilizarlo?* https://xxxamin1314.medium.com/qu%C3%A9-es-un-inyector-poe-y-c%C3%B3mo-utilizarlo-10247dce4b97

Mejía, J. (2019). *Fuentes, Importancia en la industria.* Logicbus SA. https://www.logicbus.com.mx/pdf/articulos/Fuentes-Importancia-industria.pdf

Mercado IT. (20 de Agosto de 2020). *La serie de routers Cisco 4000 redefine el rol tradicional de los routers*. https://www.mercadoit.com/blog/noticias-it/la-serie-de-routers-cisco-4000-redefine-el-rol-tradicional-de-los-routers/

mgTRADING. (2019). *Cámara Mini Bala para Exteriores 4MP/ IR LED / Model DS-2CD2042WD-I*. https://mg.com.pe/producto/camara-mini-bala-para-exteriores-4mp-ir-led-model-ds-2cd2042wd-i/

Morán, S. (18 de Mayo de 2022). *Plan V Hacemos Periodismo* Guayaquil abre la puerta a la videovigilancia masiva con millonario contrato. https://www.planv.com.ec/historias/derechos-humanos/guayaquil-abre-la-puerta-la-videovigilancia-masiva-con-millonario

Motion. (2018). *Documentación de Motion*. https://motion-project.github.io/motion_guide.html

Niño, V. (2011). *Metodología de la investigación.* (A. Gutiérrez, Ed.) Bogotá, Colombia: Ediciones de la U. https://gc.scalahed.com/recursos/files/r161r/w24802w/Nino-Rojas-Victor-Miguel_Metodologia-de-la-Investigacion_Diseno-y-ejecucion_2011.pdf

NIVIAN. (16 de 08 de 2019). *¿Qué significa el protocolo ONVIF?* https://www.nivianhome.com/es/que-es-onvif/

Openmediavault. (13 de Febrero de 2022). *¿Qué es OpenMediaVault?* https://www.openmediavault.org/

OPENVPN. (2022). *Acceso seguro y conectividad de red reinventados*. https://openvpn.net/#

Pantoja, H., Pinzón, J., & Roa, J. (2021). REDISEÑO DE RED LAN AJUSTADO A LAS NORMAS EIA/TIA-568-B E ISO/IEC 11801 PARA LA COMERCIALIZADORA ARTURO CALLE S.A.S. *(Tesis de pregrado).* Universidad Cooperativa de Colombia, Bogotá, Colombia. https://repository.ucc.edu.co/bitstream/20.500.12494/33644/3/2021_redise%c3%b1o_red_arturo.pdf

Parsons, G. (20 de Diciembre de 2022). *IEEE 802.11*. https://www.ieee802.org/1/files/public/docs2022/liaison-80211-TSNsupport_1222.pdf

Pastuña, E., & Viteri, P. (2021). IMPLEMENTACIÓN DE UN SISTEMA DE CIRCUITO CERRADO MEDIANTE IP, PARA MEJORAR LOS PROCESOS DE VIDEO VIGILANCIA EN EL BLOQUE B DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI EXTENSIÓN LA MANA. *(Tesis de pregrado).* Universidad Técnica de Cotopaxi, Latacunga, Cotopaxi, Ecuador. http://repositorio.utc.edu.ec/bitstream/27000/7285/1/UTC-PIM-000304.pdf

Paula, C. (01 de Septiembre de 2019). *Análisis del ODROID-N2*. https://magazine.odroid.com/es/article/odroid-n2-review/

Pazmiño, P. (2019). IMPLEMENTACIÓN DE SISTEMA DE CCTV CON CÁMARAS IP EN. *(Tesis de licenciatura).* ESCUELA POLITÉCNICA NACIONAL, Quito, Pichincha, Ecuador. https://bibdigital.epn.edu.ec/bitstream/15000/20088/1/CD-9528.pdf

RANDOM NERD. (30 de Enero de 2018). *Instalar MotionEyeOs en Raspberry Pi – Sistema de cámaras de vigilancia*. https://randomnerdtutorials.com/install-motioneyeos-on-raspberry-pi-surveillance-camera-system/

Raspberry Pi. (2020). *Raspberry Pi 4*. https://www.raspberrypi.com/products/raspberry-pi-4-model-b/

RaspBerry PI. (2021). *Instalar Raspbian con Raspberry Pi Imager de forma sencilla*. https://geekland.eu/instalar-raspbian-con-raspberry-pi-imager/

Redes Zona. (10 de Junio de 2021). *Mejora la seguridad de tu VPN con el protocolo IPsec*. https://www.redeszone.net/tutoriales/vpn/ipsec-que-es-como-funciona/

Sánchez, E. (2017). IMPLEMENTACIÓN DE UN SERVIDOR OPENVPN INTEGRADO CON SEGURIDAD LATCH MONTADO EN UNA RASPBERRY PI PARA LA EMPRESA REPORNE S.A. *(Tesis de pregrado).* Universidad de Guayaquil, Guayaquil, Guayas, Ecuador. http://repositorio.ug.edu.ec/bitstream/redug/23727/1/B-CINT-PTG-N.200.S%C3%A1nchez%20Estrada%20Edwin%20Eduardo.pdf

SENYDA. (2018). *RU Cisco router de 4300 series, router ISR4331-VSEC/K9 de la sucursal de Cisco*. http://spanish.gigabitlanswitch.com/sale-10799824-1-ru-cisco-4300-series-router-cisco-branch-office-router-isr4331-vsec-k9.html

Shinobi. (2020). *Documentos Shinobi*. https://shinobi.video/docs/start

Sivtec. (4 de septiembre de 2019). *Cctv Que Es; Circuito Cerrado De Televisión*. https://sivytec.com/cctv-que-es-circuito-cerrado-de-television/

TRENDnet. (Febrero de 2021). *GUÍA DE CÁMARAS POE PARA PRINCIPIANTES*. https://www.trendnet.com/langsp/poe-cameras-guide-beginners

UBUNTU. (2022). *Descargar escritorio de Ubuntu*. https://ubuntu.com/download/desktop

Western Digital. (2019). *DISCOS DUROS PARA VIDEOVIGILANCIA*. https://media.flixcar.com/f360cdn/Western_Digital-3807284878-esn_spec_data_sheet_2879-800012.pdf

VII. ANEXOS

Anexo 1: Acta de sustentación Predefensa del TIC

UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI
FACULTAD DE INDUSTRIAS AGROPECUARIAS Y CIENCIAS AMBIENTALES
CARRERA DE INGENIERIA EN INFORMATICA

ACTA

DE LA SUSTENTACIÓN DE PREDEFENSA DEL INFORME DE INVESTIGACIÓN DE:

NOMBRE: JIMMY JAVIER AREVALO PUETATE
CÉDULA DE IDENTIDAD: 0402134613
NIVEL/PARALELO: 0
PERIODO ACADÉMICO: 2023B

TEMA DE INVESTIGACIÓN: "Sistema de video vigilancia para la seguridad de los equipos en los laboratorios de la carrera de computación"

Tribunal designado por la dirección de esta Carrera, conformado por:
PRESIDENTE: MSC. ARCOS PONCE GEORGINA GUADALUPE
LECTOR: MSC. JIMÉNEZ CÁRDENAS STALIN VANTROY
ASESOR: MSC. DEL HIERRO MOSQUERA MILTON GABRIEL

De acuerdo al artículo 21: Una vez entregados los requisitos para la realización de la pre-defensa el Director de Carrera integrará el Tribunal de Pre-defensa del informe de investigación, fijando lugar, fecha y hora para la realización de este acto:

EDIFICIO DE AULAS: 4 **AULA:** 107
FECHA: martes, 26 de septiembre de 2023
HORA: 16H30
Obteniendo las siguientes notas:
1) Sustentación de la predefensa: 6,00
2) Trabajo escrito 2,40
Nota final de PRE DEFENSA **8,40**
Por lo tanto: **APRUEBA CON OBSERVACIONES** ; debiendo acatar el siguiente artículo:

Art. 24.- De los estudiantes que aprueban el Plan de Investigación con observaciones. - El estudiante tendrá el plazo de 10 días laborables para proceder a corregir su informe de investigación de conformidad a las observaciones y recomendaciones realizadas por los miembros Tribunal de sustentación de la pre-defensa.

Para constancia del presente, firman en la ciudad de Tulcán el martes, 26 de septiembre de 2023

MSC. ARCOS PONCE GEORGINA GUADALUPE
PRESIDENTE

MSC. DEL HIERRO MOSQUERA MILTON GABRIEL
TUTOR

MSC. JIMÉNEZ CÁRDENAS STALIN VANTROY
LECTOR

Adj.: Observaciones y recomendaciones

Anexo 2: Certificado de ABSTRACT por parte de idiomas

UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI
FOREIGN AND NATIVE LANGUAGE CENTER

ABSTRACT- EVALUATION SHEET

NAME: Jimmy Javier Arévalo Puetate
DATE: 5 de octubre de 2023

TOPIC: "Sistema de video vigilancia para la seguridad de los equipos en los laboratorios de la carrera de computación"

MARKS AWARDED — QUANTITATIVE AND QUALITATIVE

VOCABULARY AND WORD USE	Use new learnt vocabulary and precise words related to the topic	Use a little new vocabulary and some appropriate words related to the topic	Use basic vocabulary and simplistic words related to the topic	Limited vocabulary and inadequate words related to the topic
	EXCELLENT: 2 ☐	GOOD: 1Vera Jativa Edwin Andrés,5 ☐	AVERAGE: 1 ☐	LIMITED: 0,5 ☐
WRITING COHESION	Clear and logical progression of ideas and supporting paragraphs.	Adequate progression of ideas and supporting paragraphs.	Some progression of ideas and supporting paragraphs.	Inadequate ideas and supporting paragraphs.
	EXCELLENT: 2 ☐	GOOD: 1,5 ☐	AVERAGE: 1 ☐	LIMITED: 0,5 ☐
ARGUMENT	The message has been communicated very well and identify the type of text	The message has been communicated appropriately and identify the type of text	Some of the message has been communicated and the type of text is little confusing	The message hasn't been communicated and the type of text is inadequate
	EXCELLENT: 2 ☐	GOOD: 1,5 ☐	AVERAGE: 1 ☐	LIMITED: 0,5 ☐
CREATIVITY	Outstanding flow of ideas and events	Good flow of ideas and events	Average flow of ideas and events	Poor flow of ideas and events
	EXCELLENT: 2 ☐	GOOD: 1,5 ☐	AVERAGE: 1 ☐	LIMITED: 0,5 ☐
SCIENTIFIC SUSTAINABILITY	Reasonable, specific and supportable opinion or thesis statement	Minor errors when supporting the thesis statement	Some errors when supporting the thesis statement	Lots of errors when supporting the thesis statement
	EXCELLENT: 2 ☐	GOOD: 1,5 ☐	AVERAGE: 1 ☐	LIMITED: 0,5 ☐
TOTAL/AVERAGE	9 - 10: EXCELLENT 7 - 8,9: GOOD 5 - 6,9: AVERAGE 0 - 4,9: LIMITED	TOTAL 9		

UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI FOREIGN AND NATIVE LANGUAGE CENTER

Informe sobre el Abstract de Artículo Científico o Investigación.

Autor: Jimmy Javier Arévalo Puetate
Fecha de recepción del abstract: 5 de octubre de 2023
Fecha de entrega del informe: 5 de octubre de 2023

El presente informe validará la traducción del idioma español al inglés si alcanza un porcentaje de: 9 – 10 Excelente.

Si la traducción no está dentro de los parámetros de 9 – 10, el autor deberá realizar las observaciones presentadas en el ABSTRACT, para su posterior presentación y aprobación.

Observaciones:

Después de realizar la revisión del presente abstract, éste presenta una apropiada traducción sobre el tema planteado en el idioma Inglés. Según los rubrics de evaluación de la traducción en Inglés, ésta alcanza un valor de 9, por lo cual se validad dicho trabajo.

Atentamente

EDISON BOANERGES PEÑAFIEL ARCOS

Ing. Edison Peñafiel Arcos MSc
Coordinador del CIDEN

Anexo 3:Entrevistas realizadas al personal de tics

UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI

FACULTAD DE INDUSTRIAS AGROPECUARIAS Y CIENCIAS AMBIENTALES

CARRERA DE COMPUTACIÓN

NOMBRE: Jimmy Arévalo

Tema: Sistema de video vigilancia para la seguridad de los equipos en los laboratorios de la carrera de computación

Enfoque cualitativo

Dirigida a los encargados del área de tics de la UPEC

Datos del entrevistado

Fecha: 22/02/2023.

Hora: 11:30 de la mañana.

Nombre: Andrea Guevara.

Profesión: Maestra de ingeniería de software.

Cargo que ocupa en la institución: directora de tics.

GUIÓN DE ENTREVISTA

1. **¿Como está compuesto el sistema de video vigilancia?**

Son 2 sistemas, sistema antiguo con CPU de computadoras y cámaras. Que ya están obsoletas. 2, sistema nuevo con NBR de 256 canales y 40 cámaras activas.

2. **¿De acuerdo con la normativa internacional como se maneja la infraestructura del sistema de video vigilancia?**

La infraestructura de red para videovigilancia es ministrada e instalada por el área de redes y comunicaciones.

3. **¿Qué tipo de servidor de video NVR, DVR se utiliza y cuantos canales contiene?**

El NVR principal tiene 256 canales con 40 cámaras y predicciones. Los DVR secundarios son de 8 canales IP activos.

4. **¿En la universidad que tipo de cámaras se utiliza para el sistema de video vigilancia?**

Son cámaras IP tipo domo de cuatro megapíxeles.

5. **¿Qué tipo de políticas de seguridad se utiliza en el sistema de video vigilancia?**

Los equipos NVR que posee la UPEC tiene únicamente acceso el personal de seguridad y el encargado de cada área

6. **¿De acuerdo con el estándar internacional que tipo de cableado y topología es la que se encuentra implementada en el sistema de video vigilancia?**

Se utiliza cableado UTP categoría 6 y por medio de una topología en estrella en cada uno de los edificios, incluyendo la NVR principal.

7. **¿De acuerdo con la estándar ISO 27001 que tipo de mantenimiento se lleva en el sistema de video vigilancia?**

El sistema principal tiene aproximadamente 2 meses. Y los mantenimientos aún no se encuentran planificados.

8. **¿Cómo realiza los respaldos de información del contenido multimedia y en que plataforma?**

Más grabaciones en las realiza en el disco interno de cada NVR

9. **¿De acuerdo con la normativa cuánto tiempo se considera que se debe de tener guardados los archivos de video?**

Se debe considerar un tiempo mínimo de 30 días.

10. **¿Qué tipo de VLAN se utiliza para que todas las cámaras de la institución se interconecten?**

Se utiliza una VLAN de datos.

11. **¿Cuánto espacio de almacenamiento considera usted el recomendable para el manejo de los elementos de multimedia del sistema de video vigilancia?**

Se debe considerar al menos 7 días de almacenamiento.

Entrevista número 2

UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI

FACULTAD DE INDUSTRIAS AGROPECUARIAS Y CIENCIAS AMBIENTALES

CARRERA DE COMPUTACIÓN

NOMBRE: Jimmy Arévalo

Tema: Sistema de video vigilancia para la seguridad de los equipos en los laboratorios de la carrera de computación

Enfoque cualitativo

Dirigida a los encargados del área de tics de la UPEC

Datos del entrevistado

Fecha: 22/02/2023.

Hora: 14:00 de la tarde.

Nombre: Javier Torres.

Profesión: Ingeniero en Sistemas.

Cargo que ocupa en la institución: Encargado del sistema de video vigilancia de TICS.

GUIÓN DE ENTREVISTA

1. **¿Como está compuesto el sistema de video vigilancia?**
   El sistema de video vigilancia este compuesto por varios servidores algunos se encuentran obsoletos por el motivo de estar instalados en computadores de escritorio de igual manera se encuentran con cámaras muy antiguas desde cuando se inició la construcción de los edificios del campus cuenta con kits de seguridad que cuenta con 8 cámaras
2. **¿De acuerdo con la normativa internacional como se maneja la infraestructura del sistema de video vigilancia?**
   La infraestructura de red para videovigilancia es administrada e instalada por el área de redes y comunicaciones.
3. **¿Qué tipo de servidor de video NVR, DVR se utiliza y cuantos canales contiene?**

El principal NVR es de 256 canales de los cuales solo están utilizados 40 en el área de biblioteca además se tiene 7 kits de seguridad instalados cada kit cuenta con 8 canales y no se cuenta con ningún DVR

4. **¿En la universidad que tipo de cámaras se utiliza para el sistema de video vigilancia?**

   Se utiliza cámaras tipo domo en algunos sectores de 4 megapíxeles cada una de igual manera se tiene cámaras PTZ en el sistema video vigilancia antiguo y están quedando un poco obsoletas en total son 106 cámaras que se utilizan

5. **¿Qué tipo de políticas de seguridad se utiliza en el sistema de video vigilancia?**

   Políticas de seguridad solo en accesos y monitoreo en la parte de seguridad, además el encargado del área así mismo el área de seguridad de la universidad son los único que tiene acceso a las cámaras de igual manera para la extracción de videos se hace mediante solicitudes dirigidas a la máxima autoridad

6. **¿De acuerdo con el estándar internacional que tipo de cableado y topología es la que se encuentra implementada en el sistema de video vigilancia?**

   El tipo de cableado que se maneja para las cámaras de seguridad es cableado categoría 6 UTP para las cámaras interiores, la topología es tipo estrella ya que el NVR principal se encuentra en el Data Center y desde ahí se interconectan a todos los switches POE orientado solamente ara las cámaras de cada edificio para hacer el control de todo el sistema de video vigilancia

7. **¿De acuerdo con la estándar ISO 27001 que tipo de mantenimiento se lleva en el sistema de video vigilancia?**

   Hoy en día no se encuentran haciendo ningún mantenimiento debido a que las cámaras se encuentran obsoletas en el sistema de video vigilancia antiguo y en el sistema de vigilancia nuevo aún no se realizan mantenimientos dentro del plan por que recientemente se tiene 3 meses desde su instalación

8. **¿Cómo realiza los respaldos de información del contenido multimedia y en que plataforma?**

   El respaldo de toda la información de todo el contenido que se genera en la plataforma del sistema hikvision y el almacenamiento simplemente se almacenan dentro de los NVR ya que los kits pequeños cuentan cada con un disco duro de 4 TB y en el super NVR se puede hacer un arreglo 24 disco de 10 TB cada uno

9. **¿De acuerdo con la normativa cuánto tiempo se considera que se debe de tener guardados los archivos de video?**

En los kits pequeños se tiene un estimado de 40 días y solo poseen 8 cámaras así mismo en el super NVR está calculado para 3 semanas con las cámaras existentes y no cuentan Storage para sobre escribirse, la razón es por espacio, tecnología y la cantidad de dinero que representaría en gastos, ya que en la universidad los reclamos de algún percance son inmediatos y se hace uso de un video o grabación de algún tiempo determinado del contenido multimedia de los NVR en menos de una semana

10. **¿Qué tipo de VLAN se utiliza para que todas las cámaras de la institución se interconecten?**

    Nosotros manejamos únicamente una VLAN que administra la red de todas las cámaras de video vigilancia que es la VLAN 208 y en esa VLAN toda la red de las cámaras

11. **¿Cuánto espacio de almacenamiento considera usted el recomendable para el manejo de los elementos de multimedia del sistema de video vigilancia?**

    Hay que tomar en cuenta análisis, control de personas de tal manera que sería recomendable al no tener almacenamiento externo serian 15 días ya que el almacenamiento interno de los NVRS puede ser costosos

A**nexo 4**:Encuestas realizadas a los docentes de la carrera

ENCUESTA

1.-Conoce usted si se encuentra implementado algún tipo de sistema de video vigilancia en la carrera de computación

a) Actualmente si
b) No tiene idea
c) No cuenta con ninguno

2.-El sistema de video vigilancia actual que se encuentra en la universidad como lo considera

a) Satisfactorio
b) Poco satisfactorio
c) Malo

3.-Cuál cree que es el encargado de llevar el monitoreo del sistema de video vigilancia

a) Guardia de seguridad
b) Encargado de TICS
c) No existe

4.-Se debería aumentar la seguridad en los laboratorios con la implementación de cámaras IP

a) Si se debe de aumentar más seguridad
b) Poca seguridad
c) Nada

5.-Considera usted que contar con una infraestructura de cableado con estándares es lo ideal para fortalecer la seguridad en los laboratorios de informática

a) Si es ideal
b) Neutral
c) Poco importante

6.-Tiene idea de algún otro tipo de sistema de vigilancia que se puede implementar en los laboratorios

a) Si
b) No
c) Cual _____

7.-Está de acuerdo que en el sistema de video vigilancia se lleve políticas de seguridad

a) Totalmente de acuerdo
b) De acuerdo
c) En desacuerdo

8.-Está de acuerdo que un sistema de video vigilancia debe monitorear las cámaras de video vigilancia de cualquier lugar

d) Totalmente de acuerdo
e) De acuerdo
f) En desacuerdo

9.-Considera usted que se debe de utilizar una VLAN (red de área local virtual) para controlar el tráfico de red del sistema de video vigilancia

a) Totalmente de acuerdo
b) De acuerdo
c) En desacuerdo

10.-Considera que la integridad de los equipos que están en los laboratorios es de importancia para desarrollo de una buena educación

a) Son de vital importancia
b) Parcialmente tienen importancia
c) No tiene importancia

Anexo 5:Manual de cámaras

Manual de cámaras

Para poder activar las cámaras como primer paso es usar el software SADP y conecta la cámara a la computadora para asignarle una contraseña además de la IP que se usara en el sistema

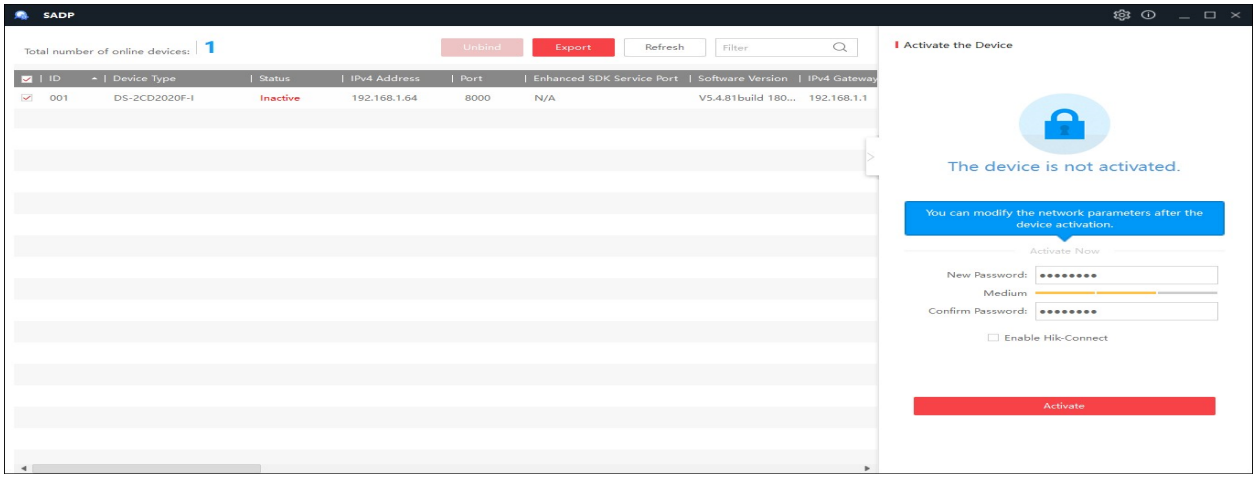


Figura 68: Página principal configuración de las cámaras

Ingresar a la interfaz de las cámaras desde un explorador web Ingresando la IP de la Cámara y las credenciales asignadas en el momento de la configuración de manera similar al ingresar las credenciales deben ser correctas para su ingreso exitoso.

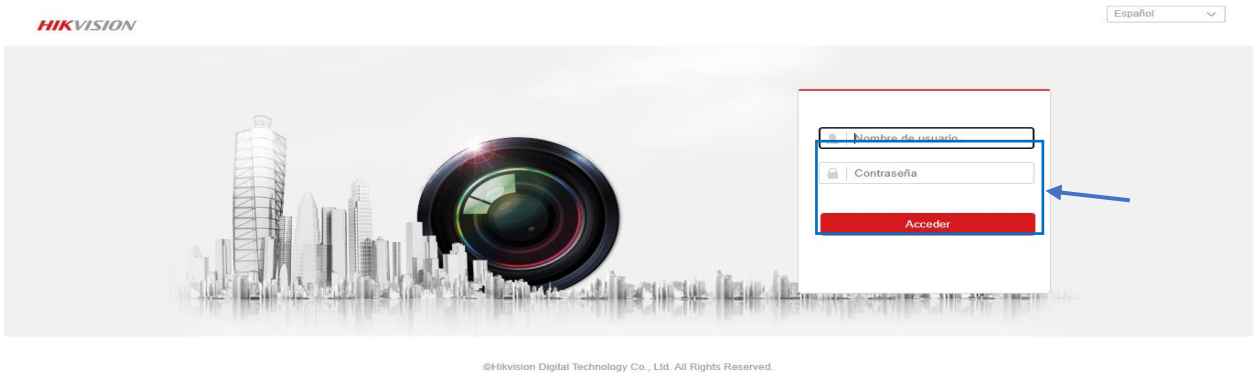


Figura 69: Ingreso de credenciales para el ingreso

Al ingresar a la interfaz de la Cámara en la cinta de opciones podemos realizar cualquier configuración. En este caso se puede ingresar en el botón de leve View para poder mirar en tiempo real lo que está grabando la Cámara

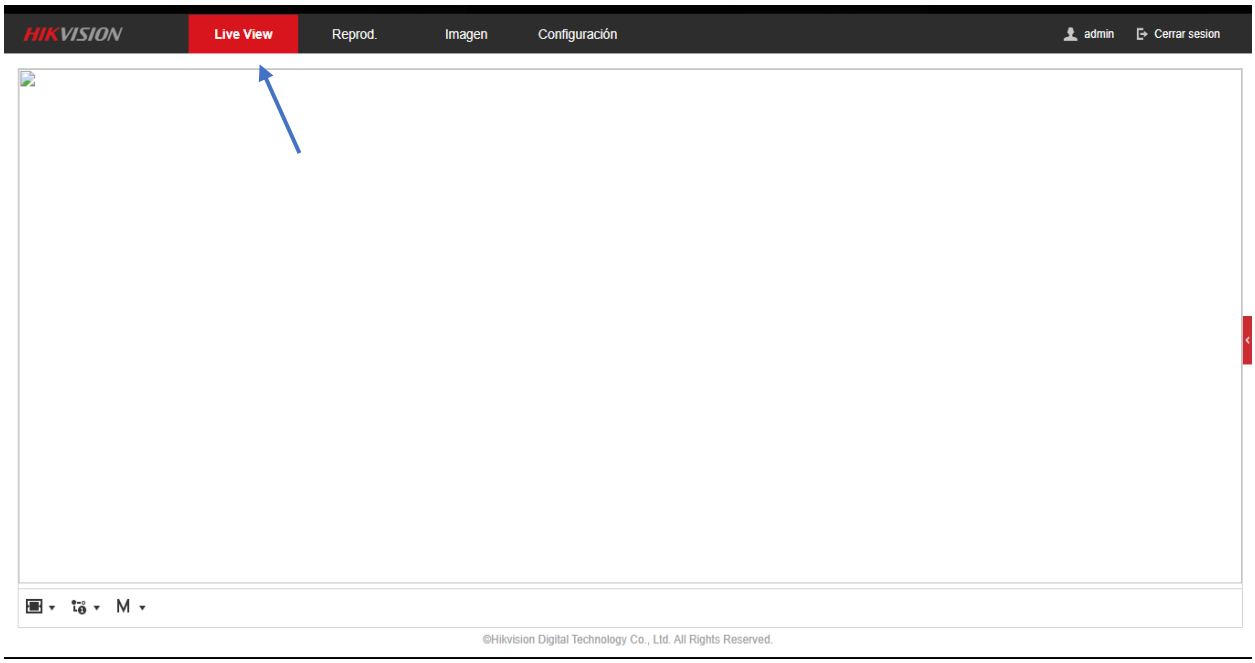


Figura 70: Pestaña vista en vivo

Para poder reproducir las grabaciones de las cámaras en la cinta de opciones presionamos el botón de reproducción y podemos elegir las fechas que se desee obtener los videos

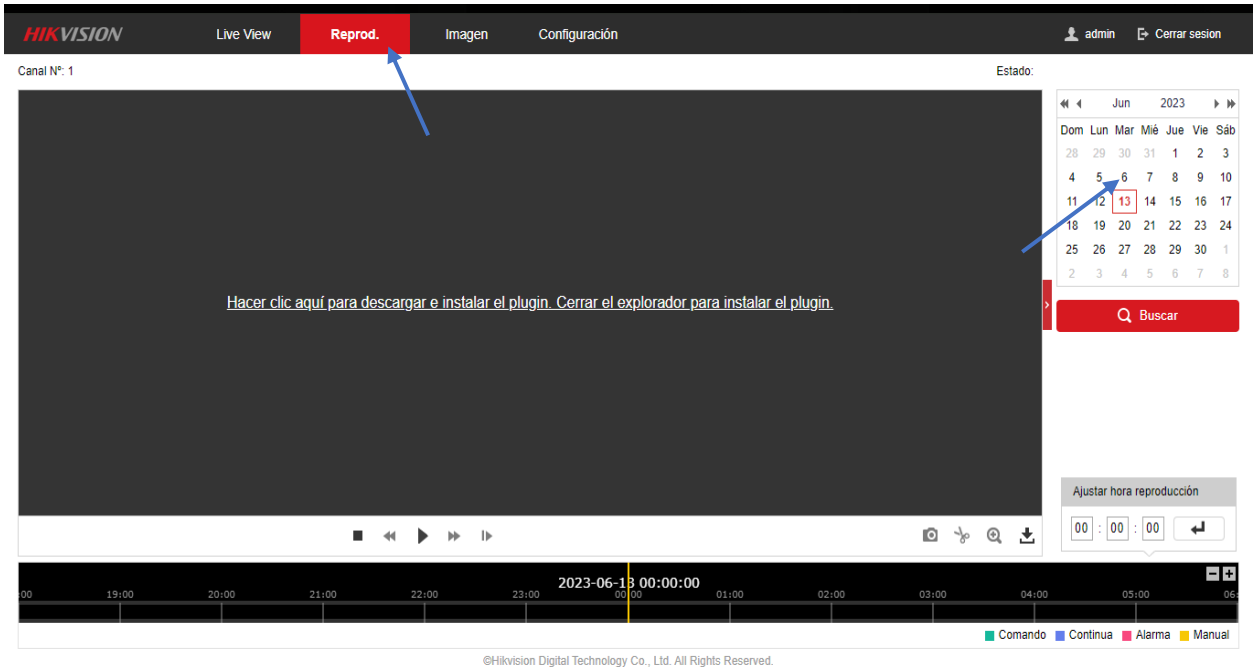


Figura 71: Ventana línea de tiempo de la cámara

De igual forma si se desea obtener los videos de los distintos eventos que genera el sistema se escoge el tipo de evento y el almacenamiento de la cámara

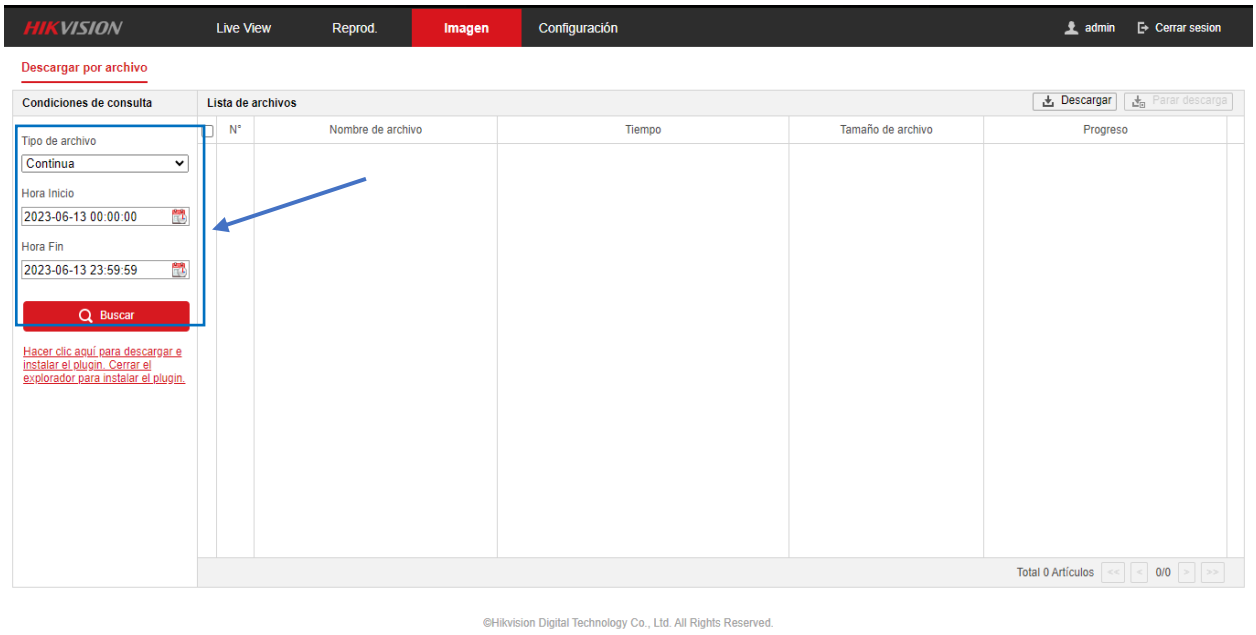


Figura 72: Tipos de grabación de las cámaras

En el botón de configuración se realizó los cambios que se necesitó en el sistema de video vigilancia

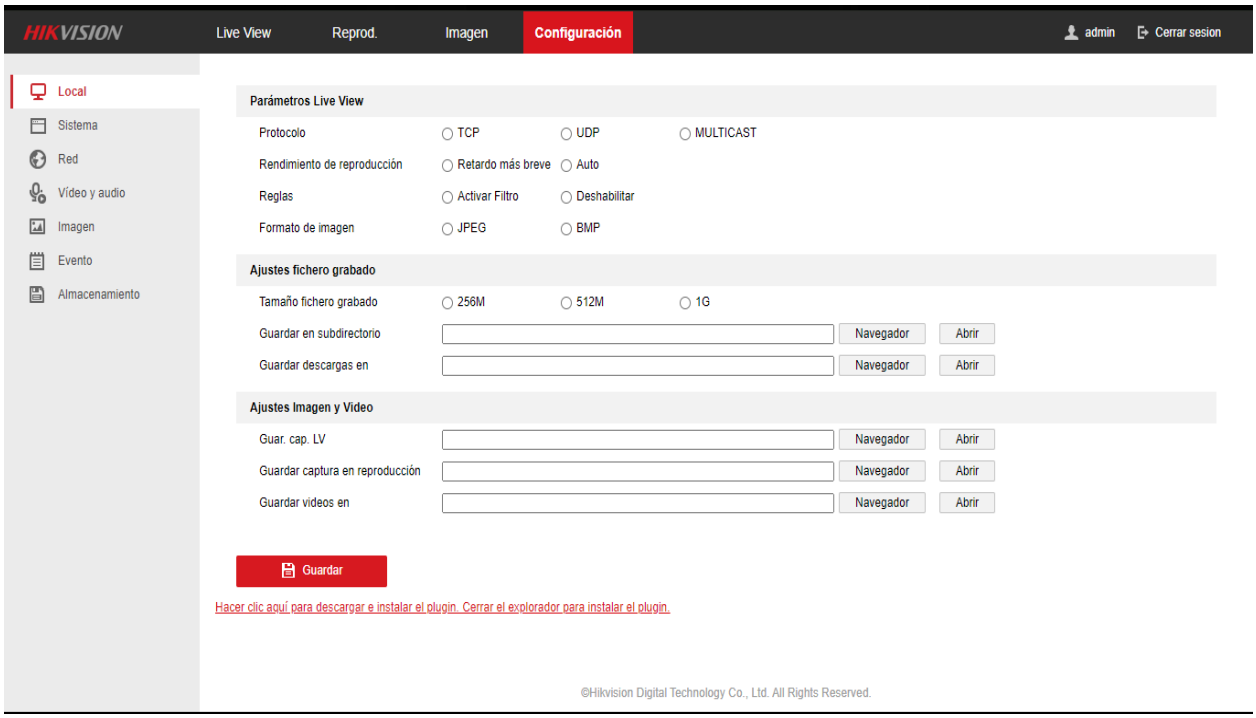


Figura 73: Ventana de configuración principal

En la configuración del sistema podremos obtener la información básica de la cámara

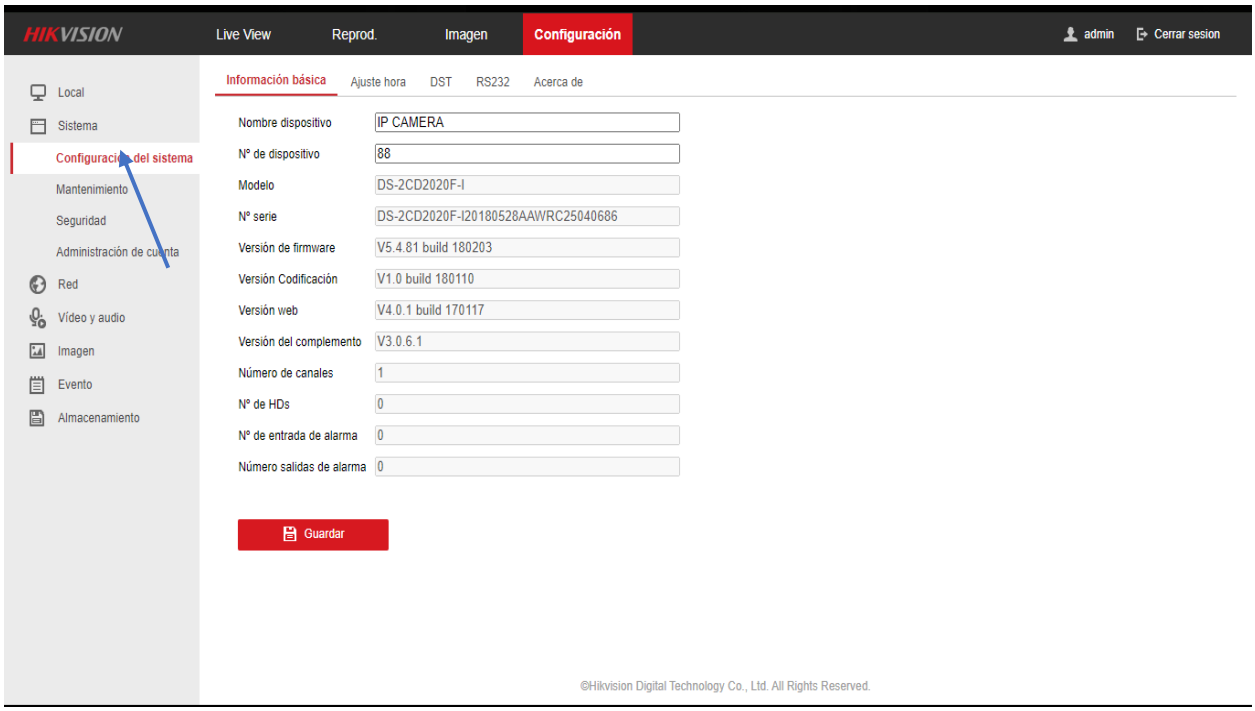


***Figura 74**:* Menú configuración del sistema

De la misma manera para poder configurar la hora de la cámara de forma manual o automática

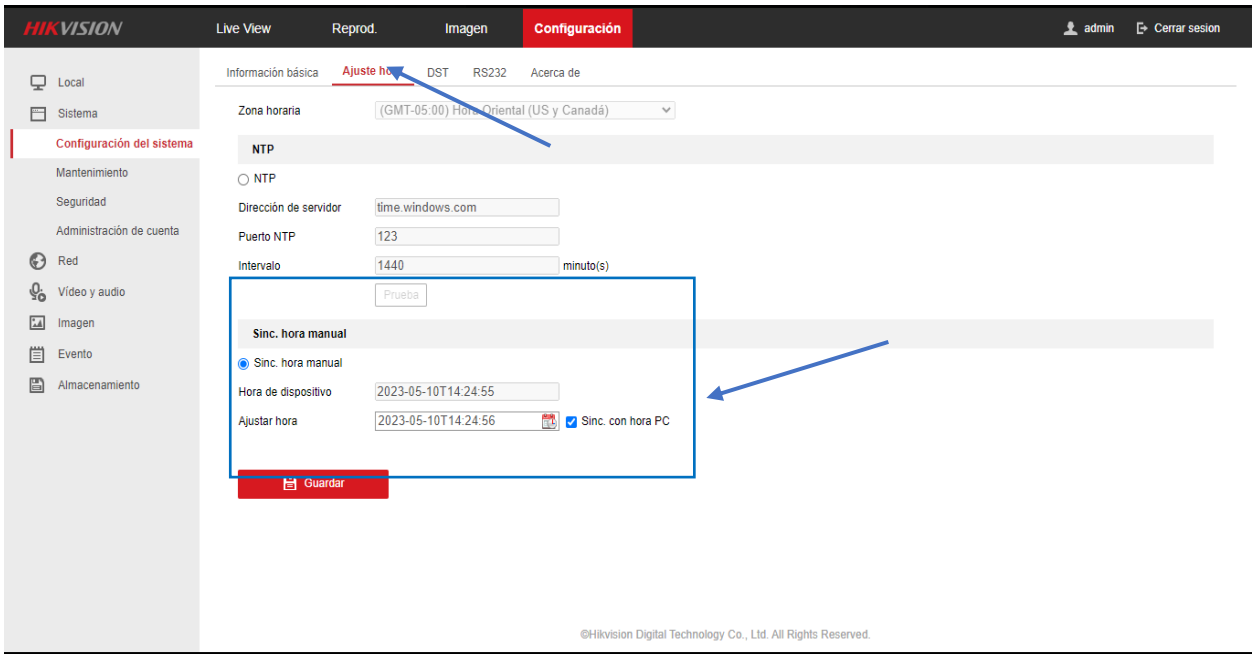


***Figura 75**:* Menú ajustes de hora

En el menú del sistema en el botón administrar la cuenta se obtiene información de todos los usuarios que tienen acceso a la cámara

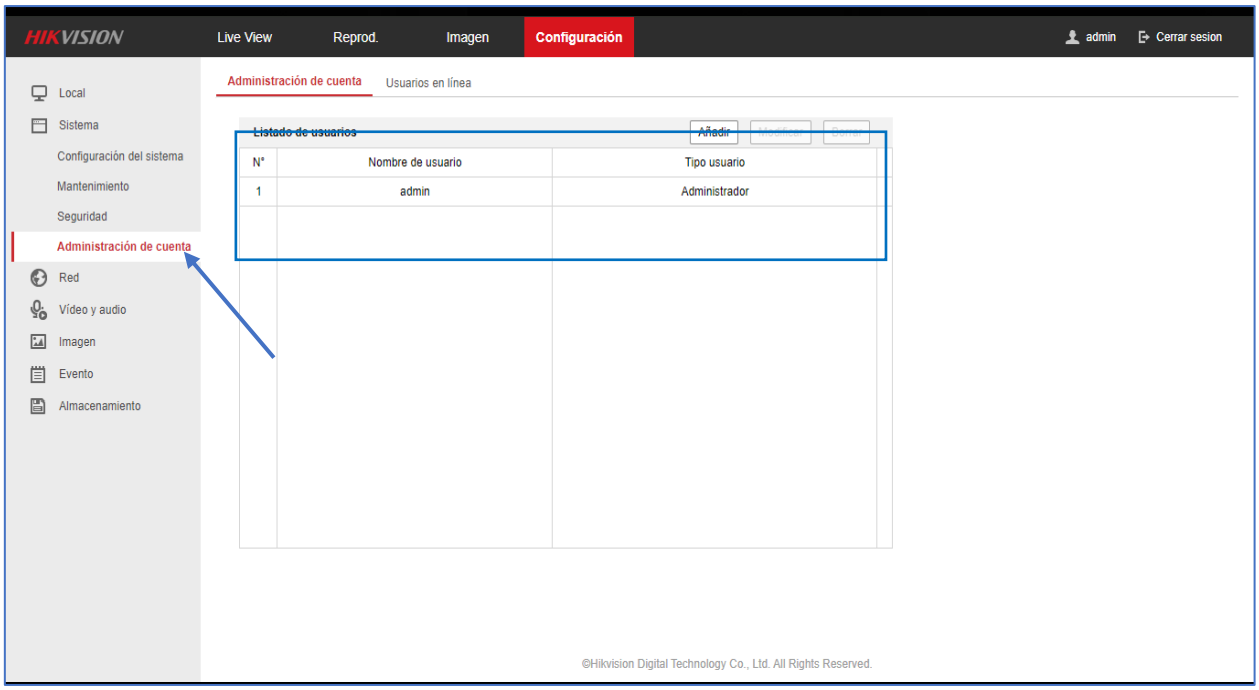


Figura 76: Lista de cuentas de acceso a la cámara

En el menú de RED se debe de cambiar las IP que va a utilizar el sistema para que todos se encuentren en el mismo segmento de red

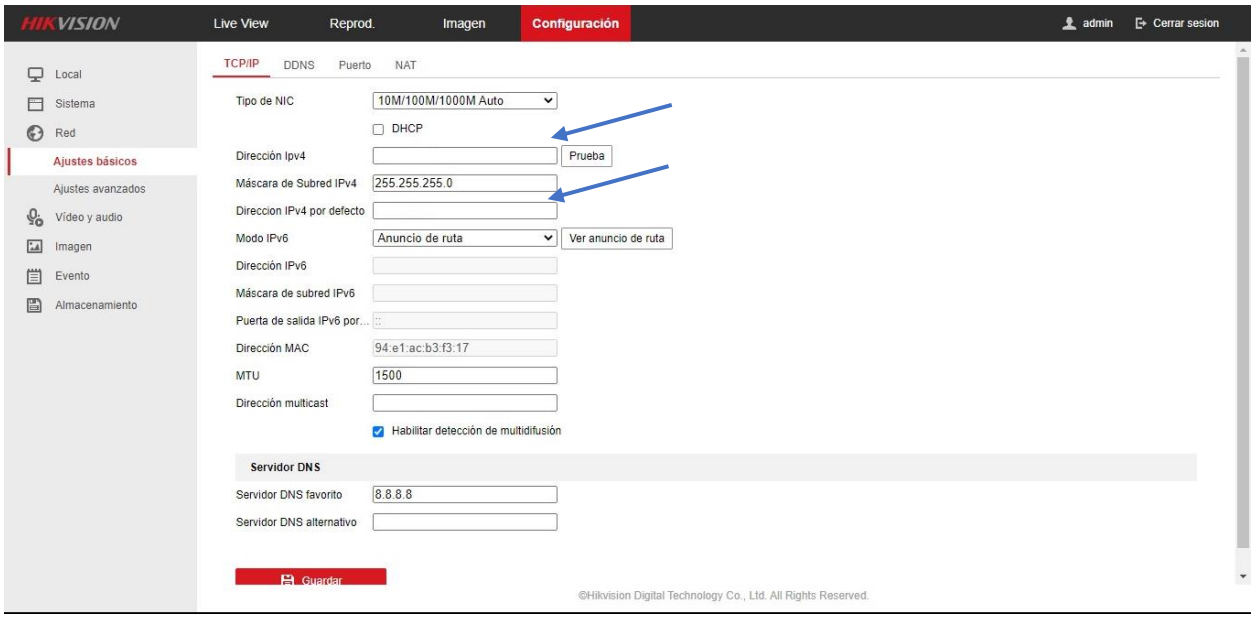


Figura 77: Interfaz de ajustes de red

Si se desea usar otro puerto por el cual conectar al sistema se debe de cambiar si no es el caso mantener el por defecto

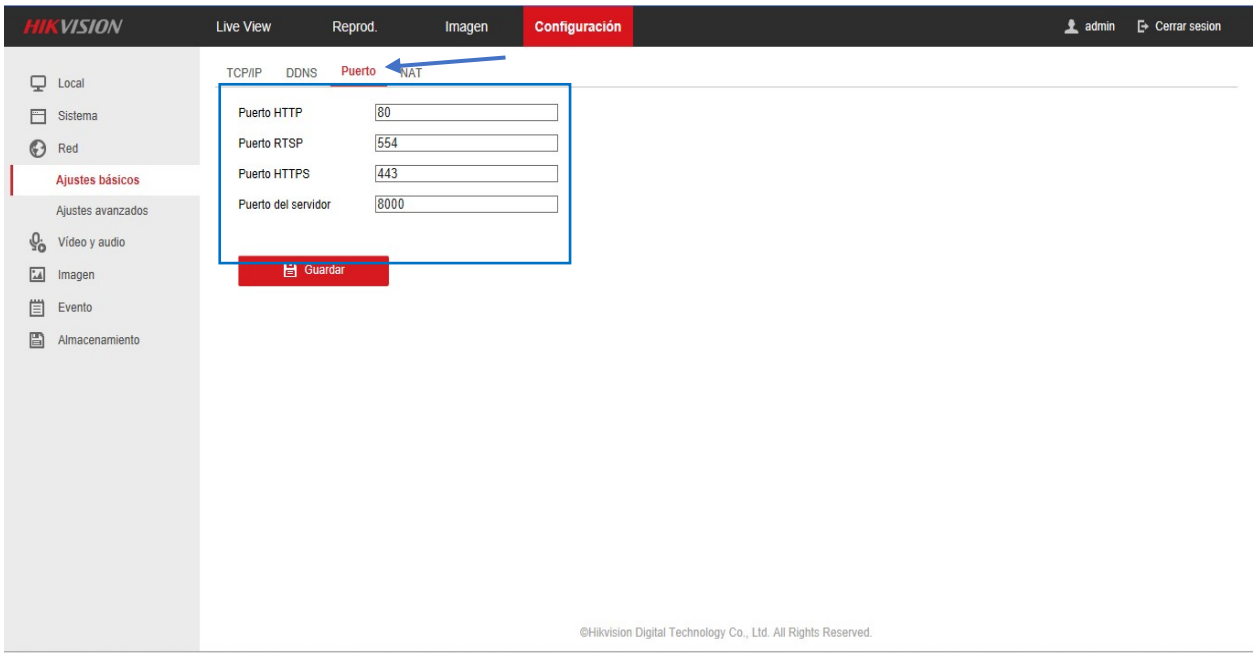


Figura 78: Puertos de la cámara

Para poder conectar la cámara con el sistema de grabación se debe tomar en cuenta el puerto FTP que este encendido al momento de ingresar en Shinobi

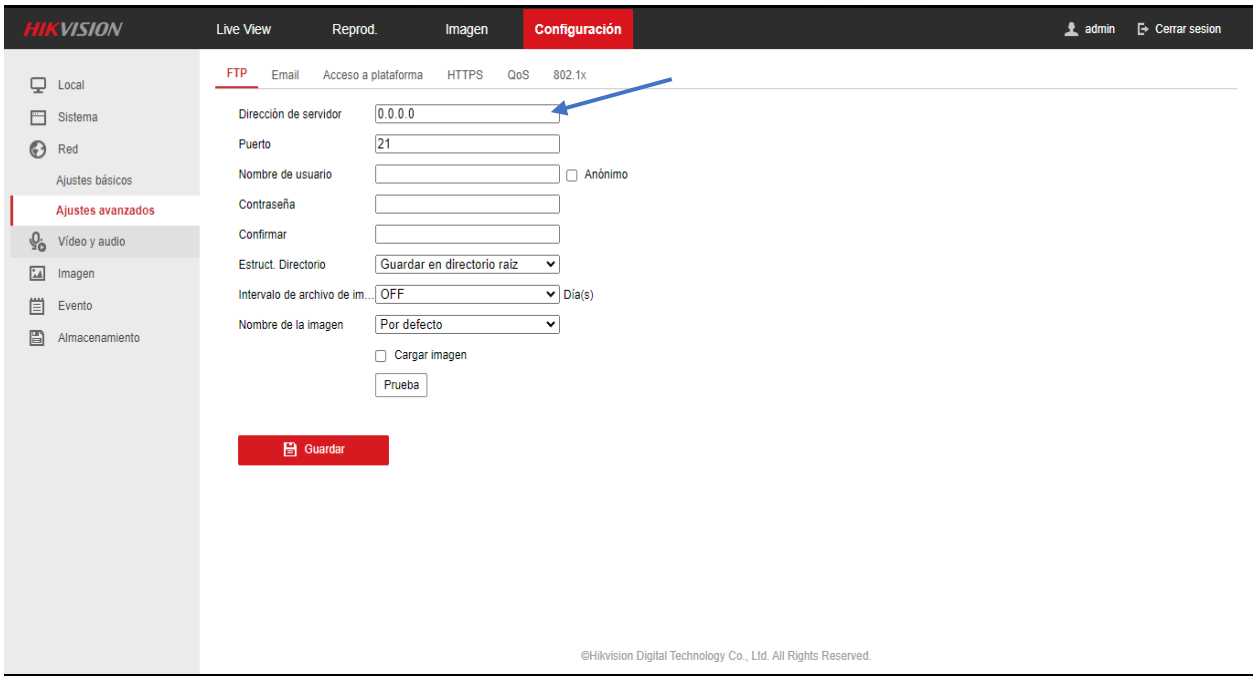


***Figura 79*:** Interfaz de ajustes avanzados

En el menú se encuentra el botón de Video y Audio en el cual se puede configurar la resolución, frames, velocidad, codificación entre otros

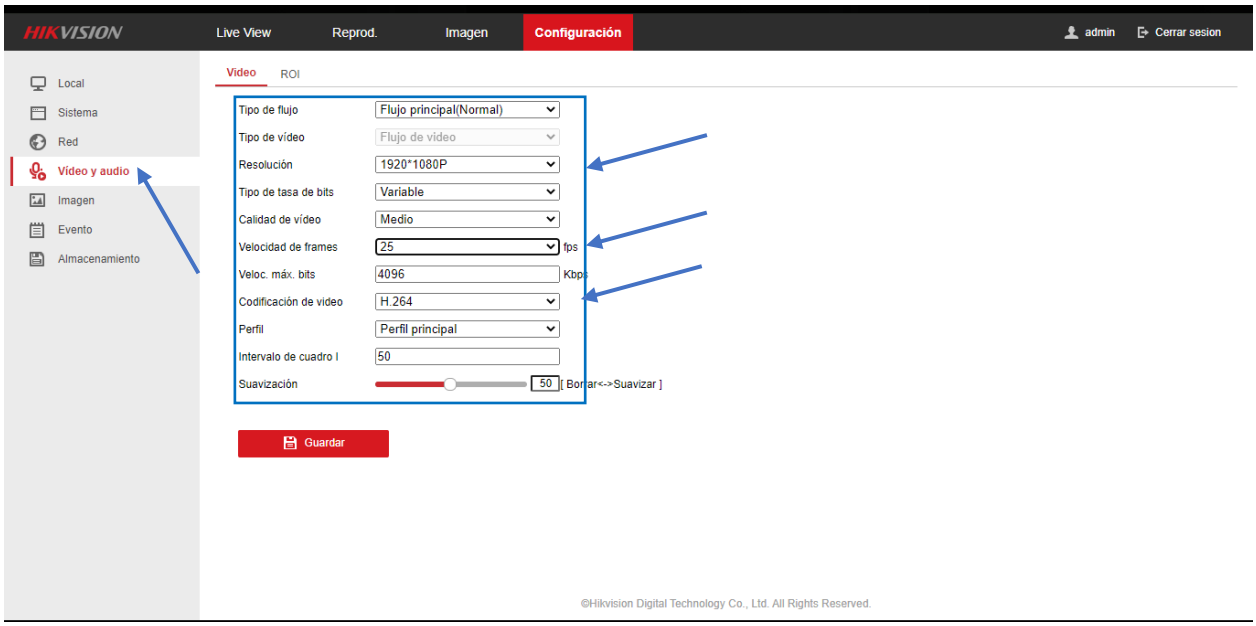


***Figura 80*:** Interfaz video y audio de la cámara

En la opción de Imagen se debe de dar el nombre como se va a visualizar la cámara además del formato de hora, formato de fecha

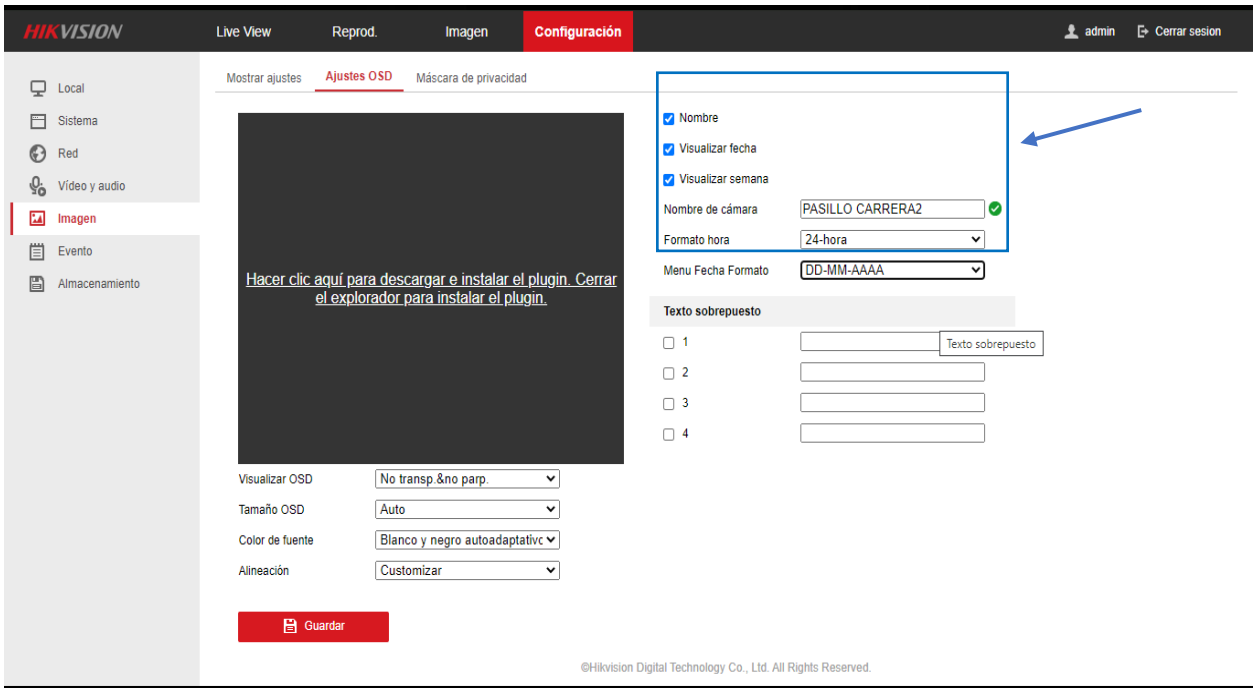


***Figura 81*:** Ajustes de OSD

En el menú de almacenamiento se pueden crear los eventos a almacenar es decir los tiempos a almacenar

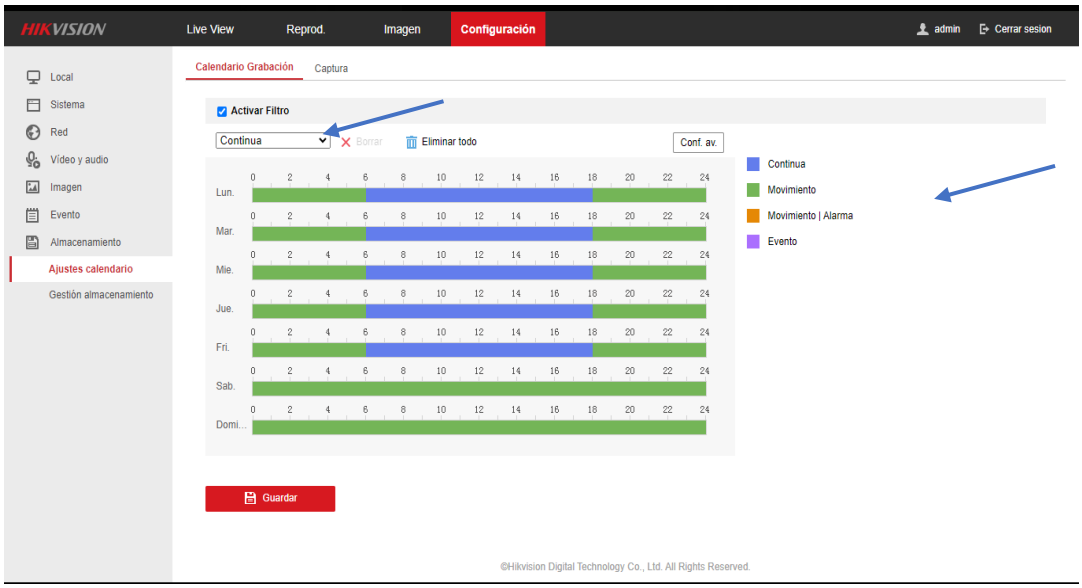


Figura 82: Ajustes de tipo de grabación

Anexo 6:Manual de Servidor

MANUAL DE SERVIDOR

Para arrancar el servidor se usó un cable serial que se conectó en el puerto de hilo del servidor el cual podemos ingresar las credenciales del servidor e ingresar a realizar la configuración deseada presionando en el botón por primera vez como muestra en la imagen

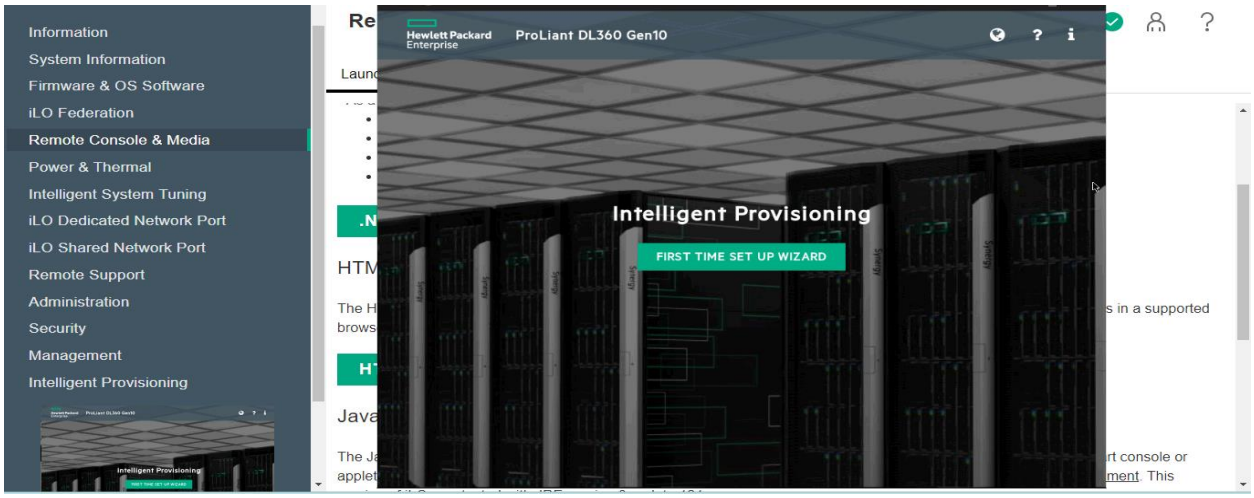


***Figura 83*:** Ventana de inicio de servidor

Seguidamente se debe de seleccionar el idioma, zona horaria, y el modo de arranque de la BIOS la cual se debe de mantener en UEFI

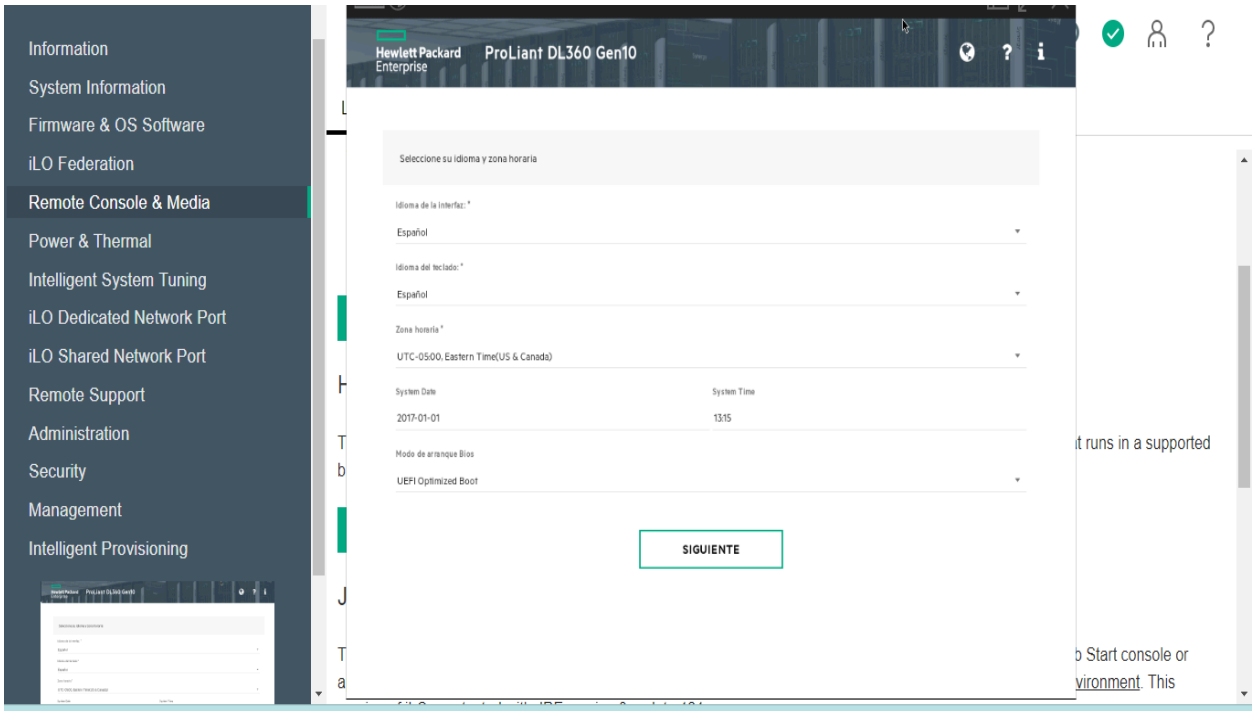


Figura 84: Configuración inicial del servidor

Se debe de aceptar las condiciones de EULA

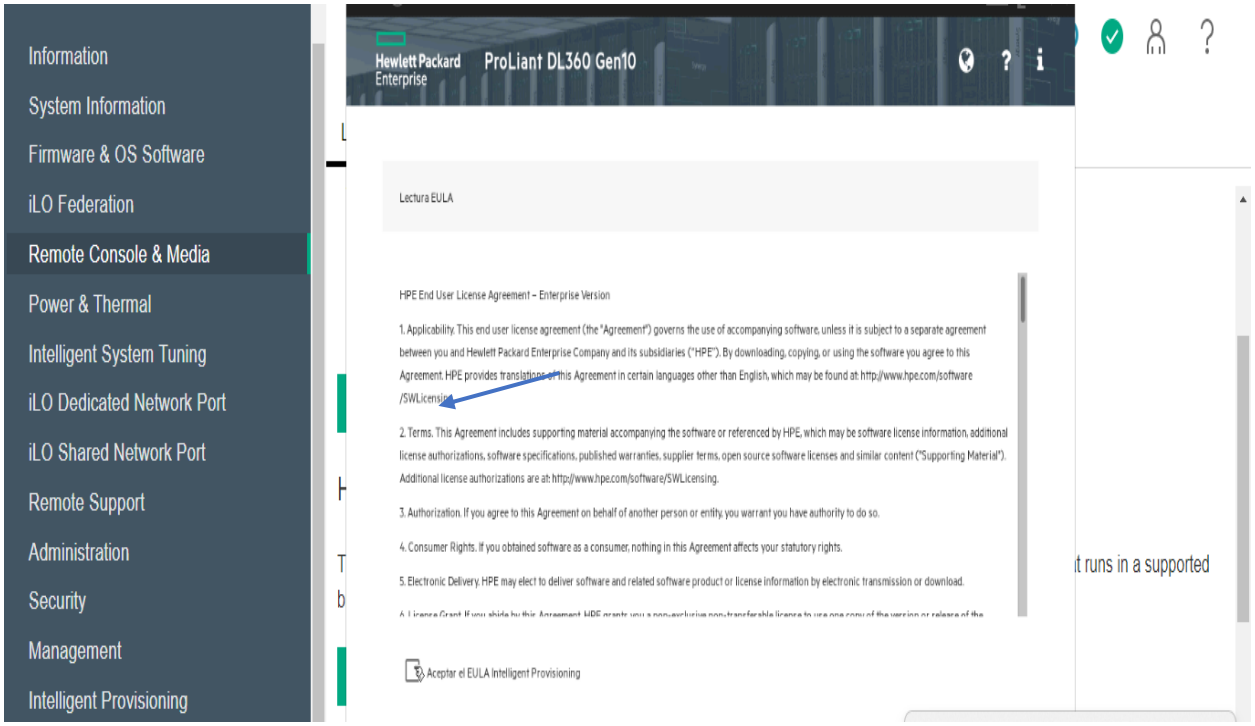


Figura 85: Aceptar términos y condiciones

Se debe de escoger las opciones que vamos a utilizar en el servidor y presionar siguiente

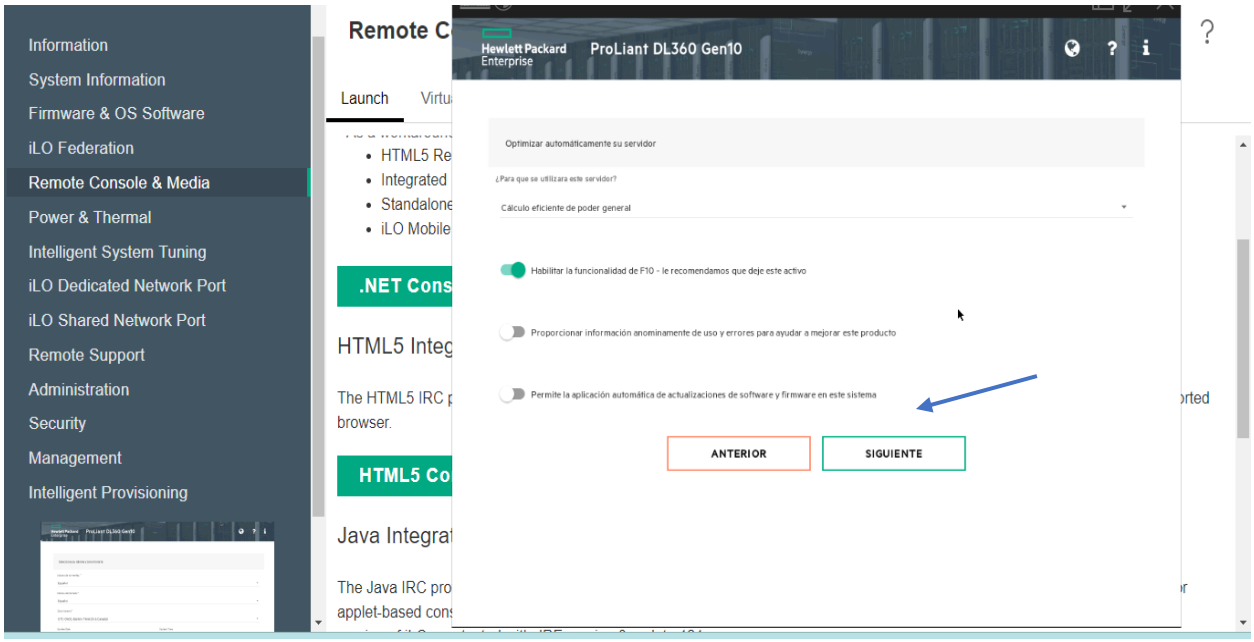


Figura 86: Optimización de servidor

A continuación, nos muestra las configuraciones de red las cuales por primer arranque se deben dejar en DHCP para después ingresar una IP en el segmento de red que se ocupe en sistema

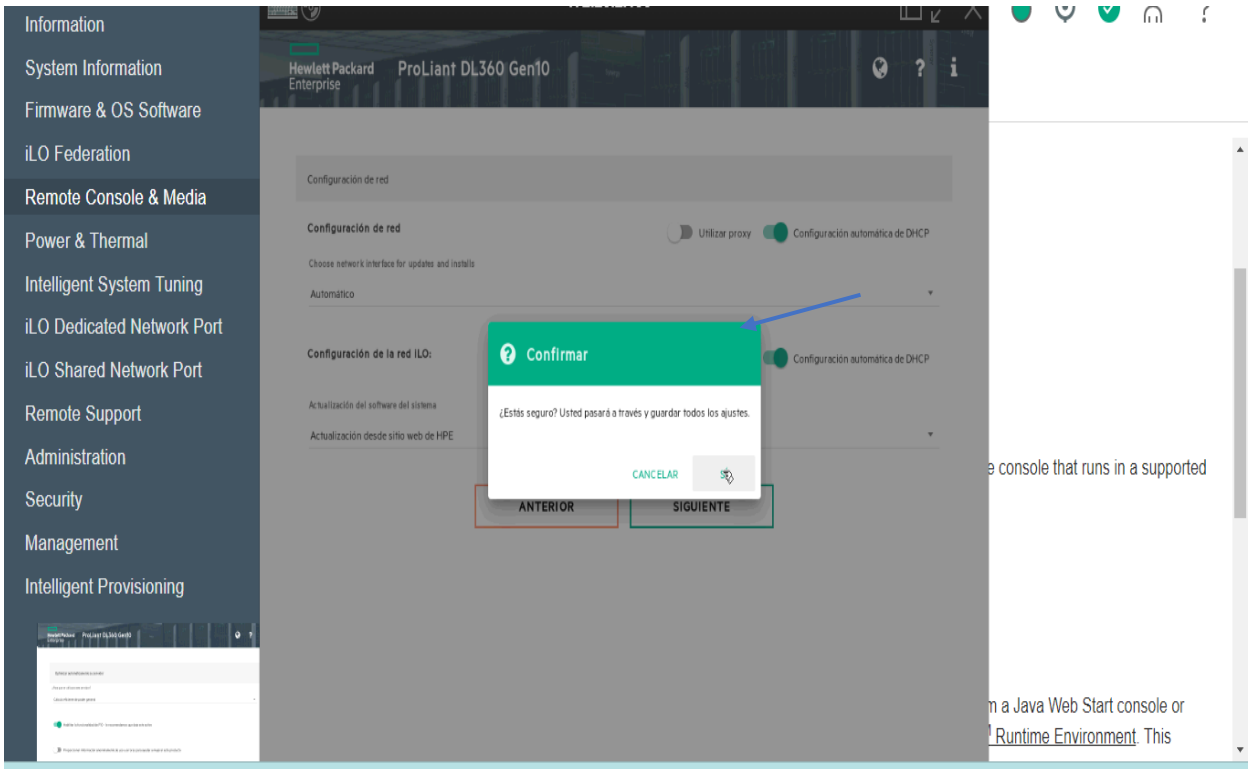


Figura 87: Confirmación de ajustes de red

Realizado todos los ajustes previos nos mostrara el menú principal de nuestro servidor

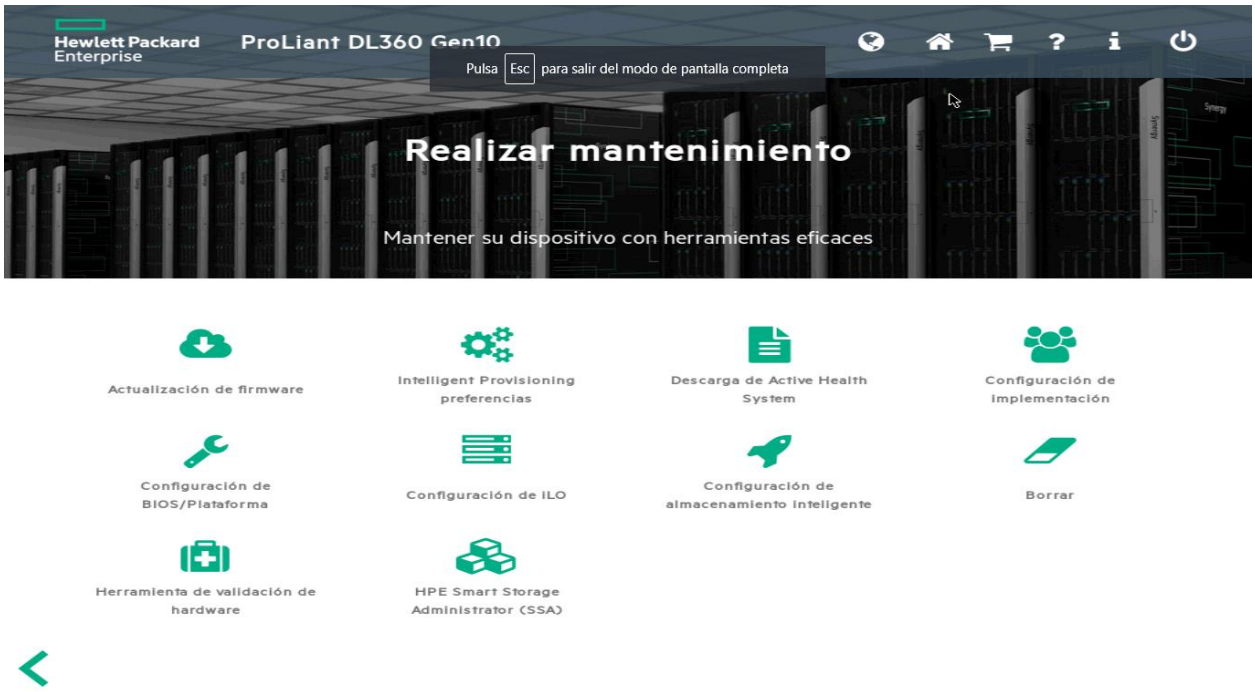


Figura 88: Interfaz de herramientas del servidor

Creación de RAID

Para la creación de nuestro RAID 1+0 se debe de ingresar al HPE Smart Storage Administrador

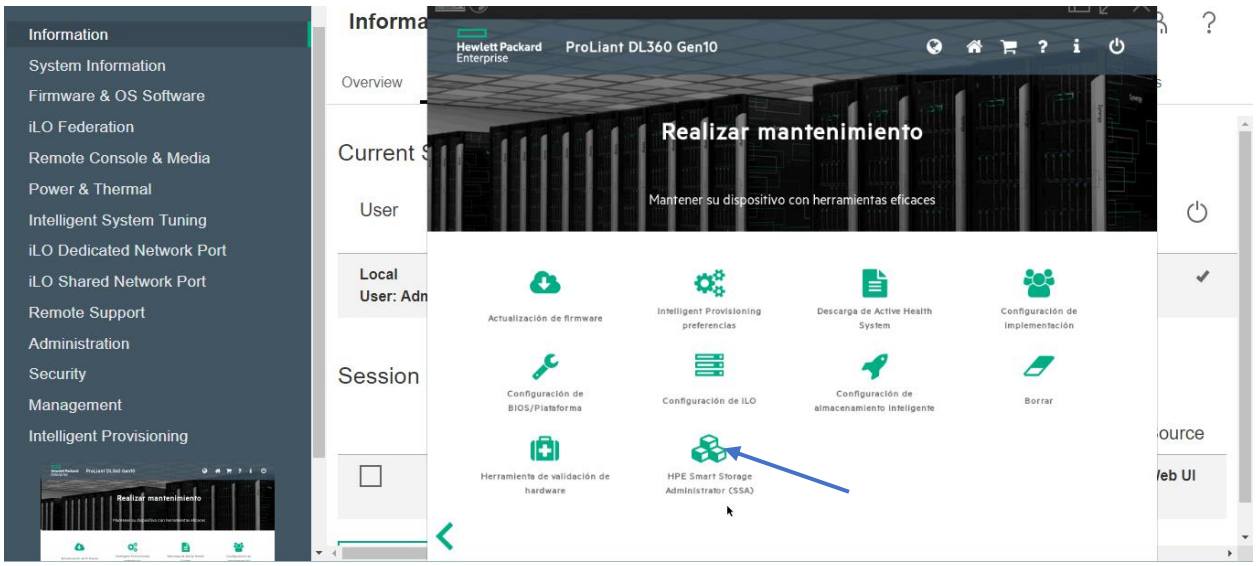


Figura 89*:* Almacenamiento inteligente

En la ventana que muestra se debe de elegir HPE Smart

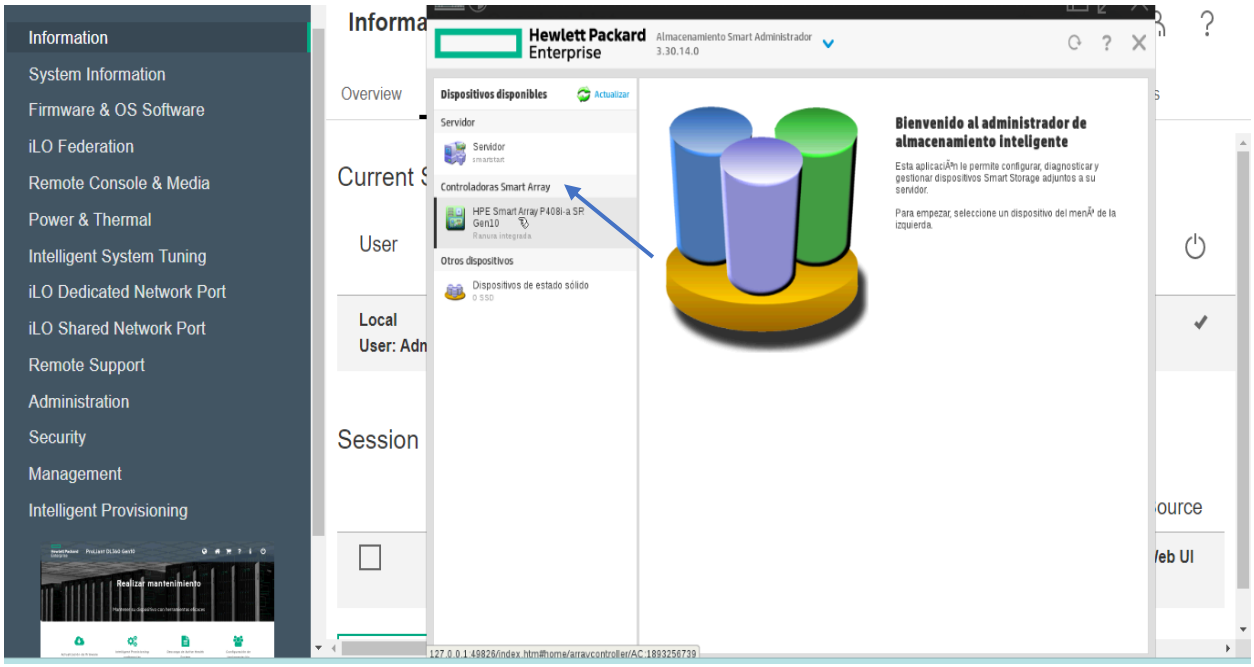


Figura 90: Ventana administrador de almacenamiento

En la ventana siguiente se debe de elegir acciones y presionar en configurar

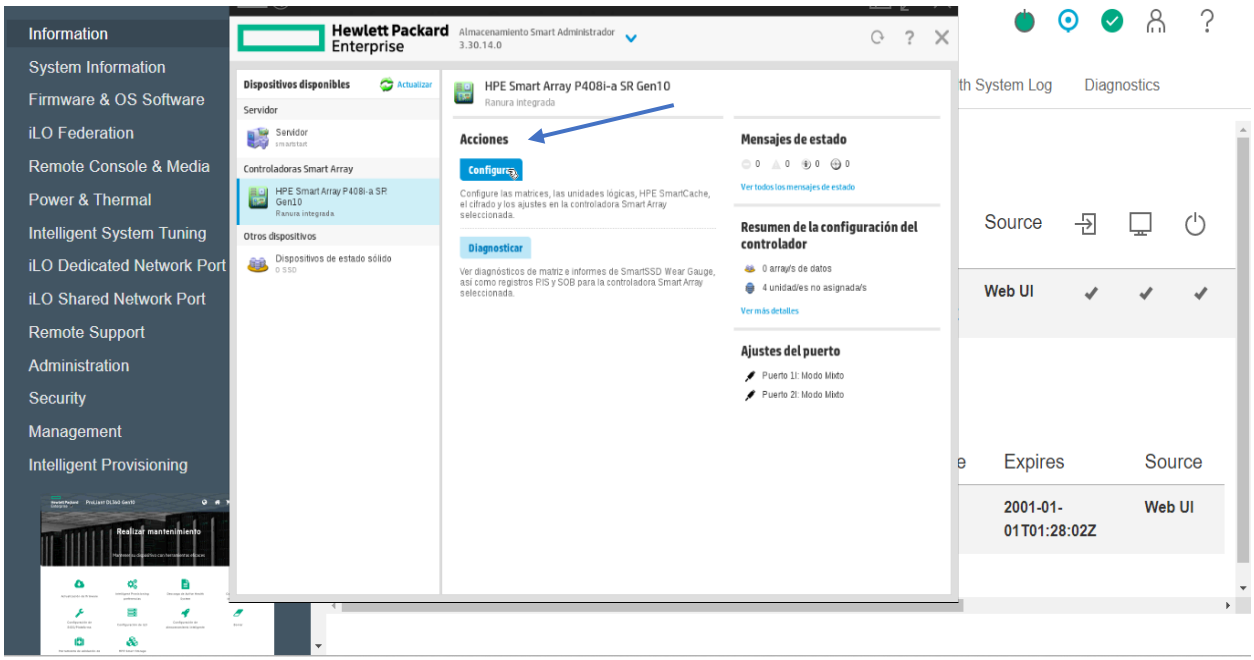


Figura 91: Configuración de RAID

Antes de crear el array se debe de revisar si se encuentran unidades lógicas en uso, y si ese es el caso se procede a borrar las que se encuentren creadas

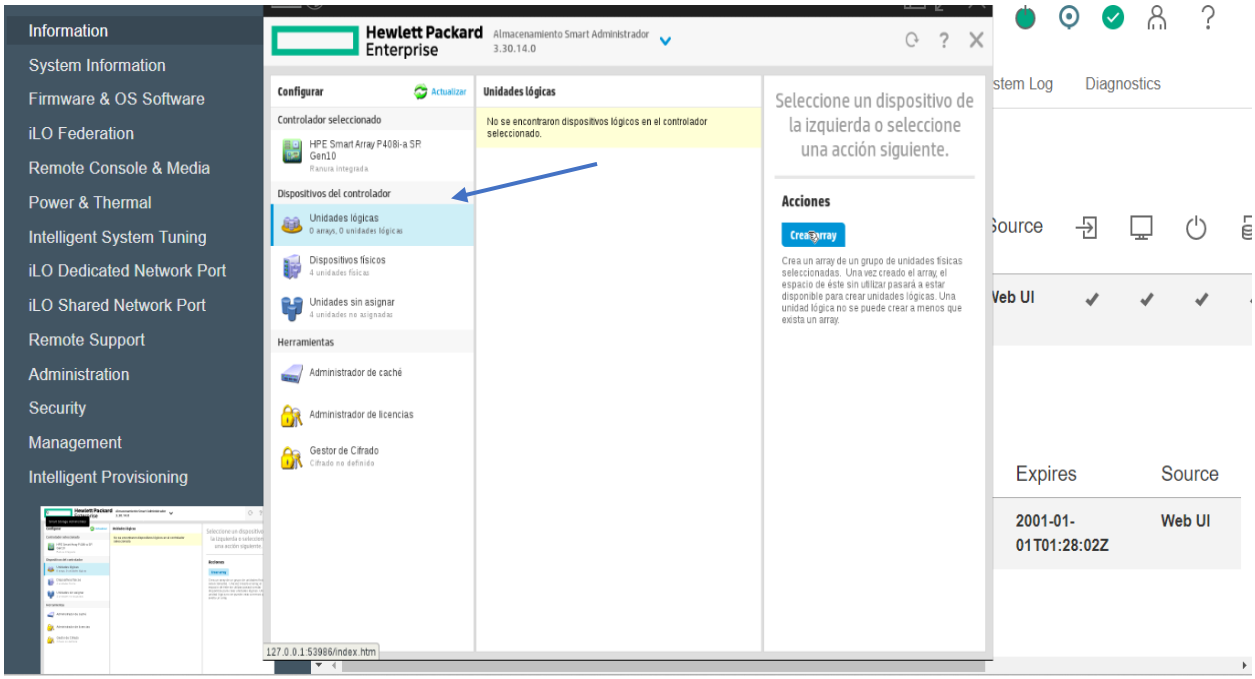


Figura 92: Creación de unidades lógicas

Después en la ventana que nos muestra se debe de elegir crear ARRAY

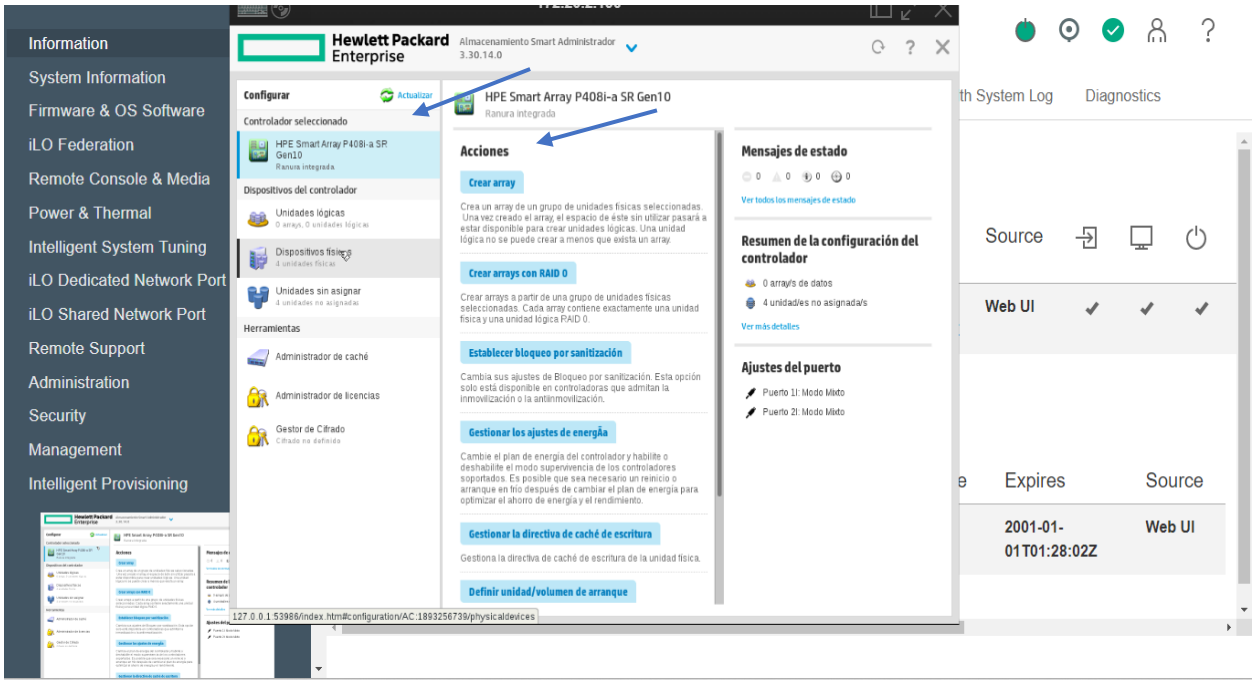


***Figura 93*:** Creación de array

En la ventana siguiente muestra los discos que contine el servidor además de su respectivo tamaño, del mismo modo se deben de escoger los discos referentes al tipo de RAID que se va a crear, pero como en este caso es un 1+0 se seleccionó los 4 discos y se presiona crear array

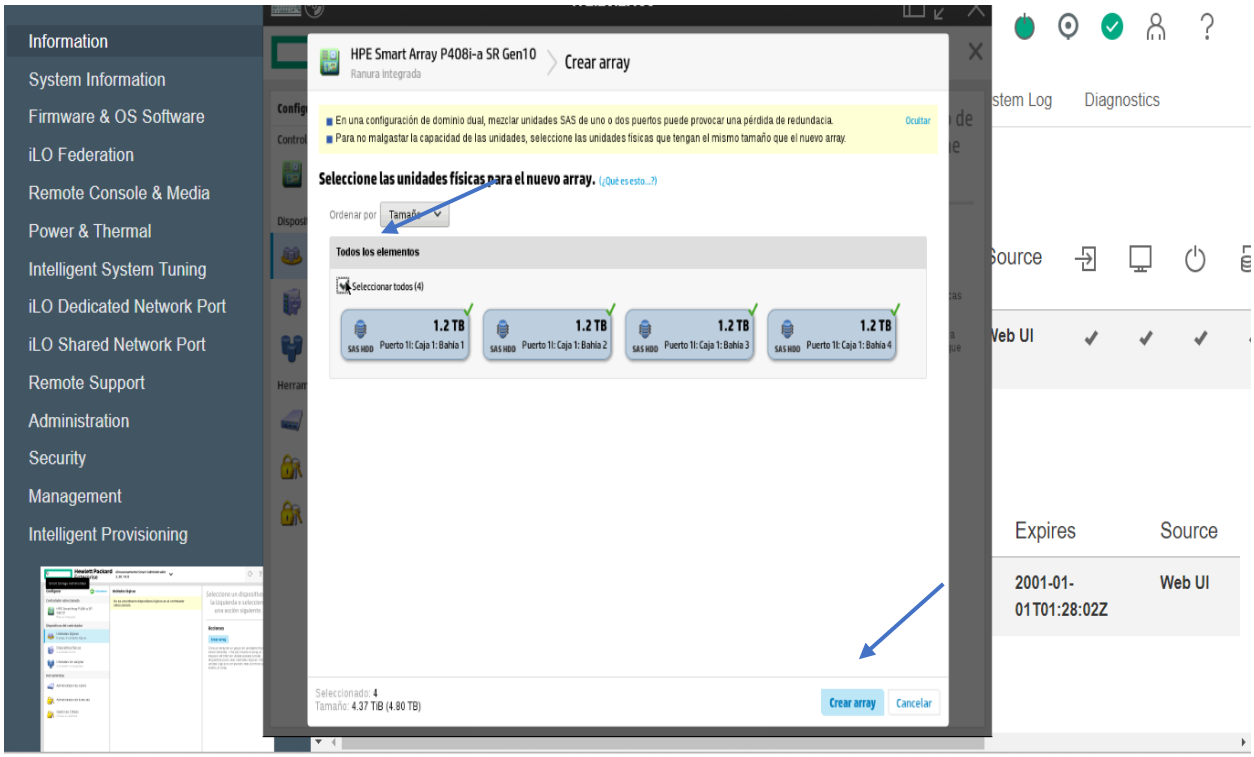


Figura 94: Selección de discos duros

Antes de crear el Raid debemos de confirmar los datos ingresados

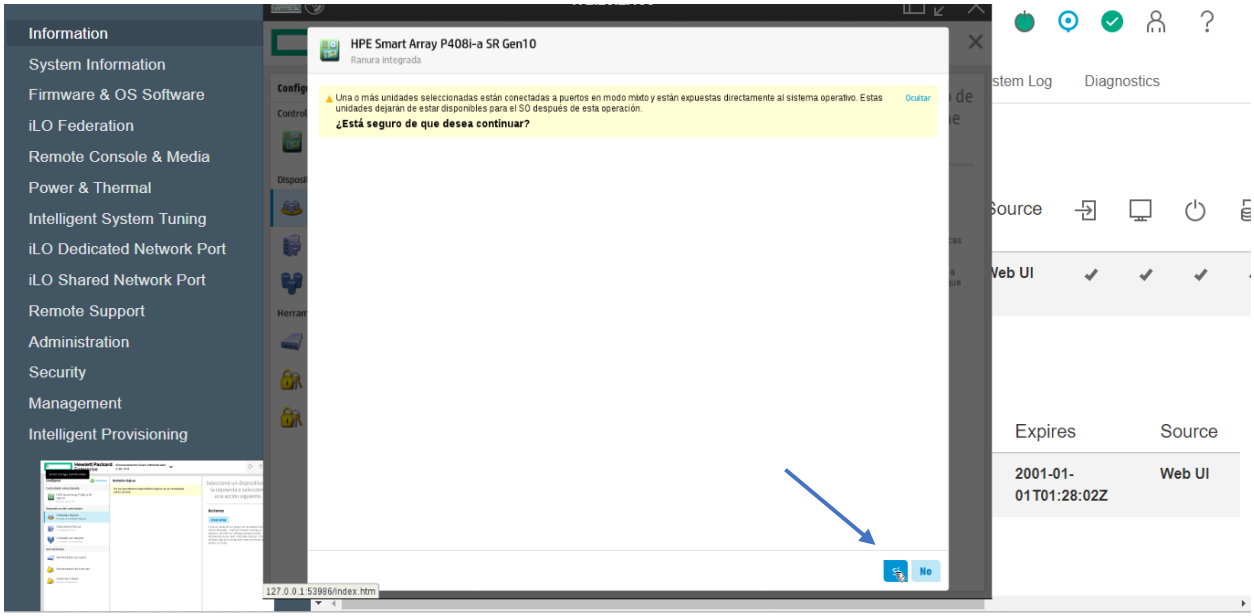


Figura 95: Aceptar crear el array

En esta ventana se debe de elegir el tipo de raid a crear en este caso estas son las elecciones que se escogió y presionamos la unidad lógica

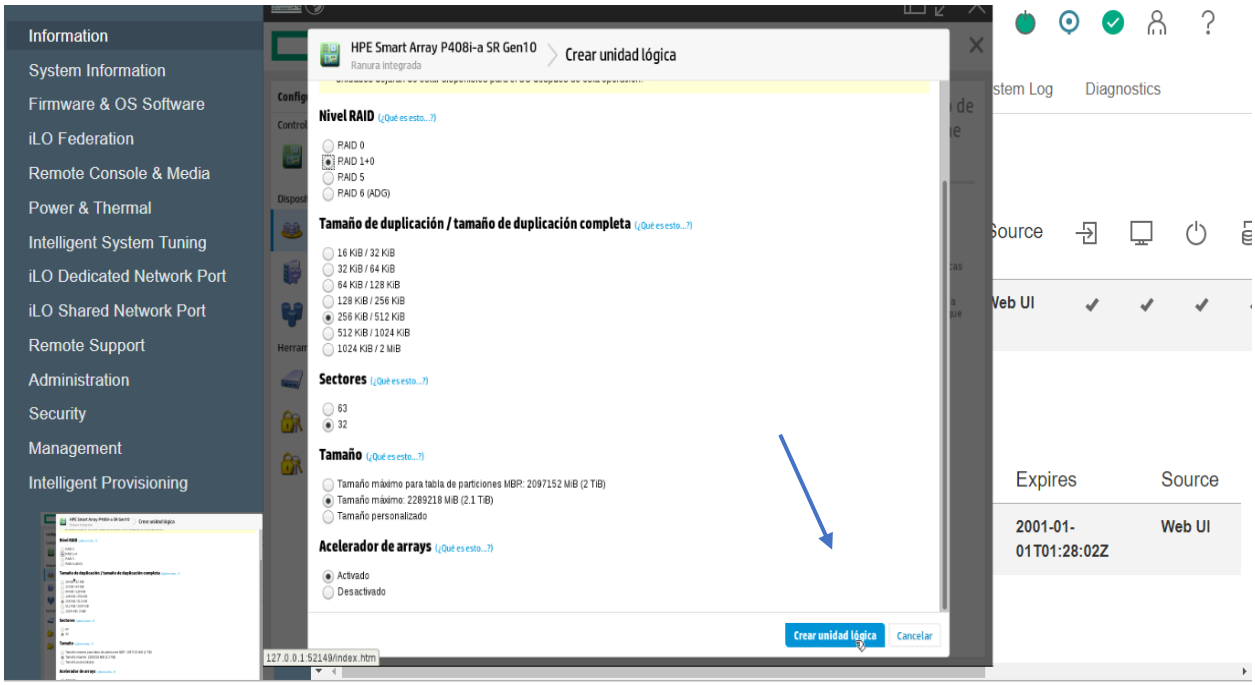


Figura 96: Ajustes de RAID

En la ventana que se muestra a continuación se muestra todas las especificaciones de nuestro raid creado y para seguir se presiona el boto finalizar

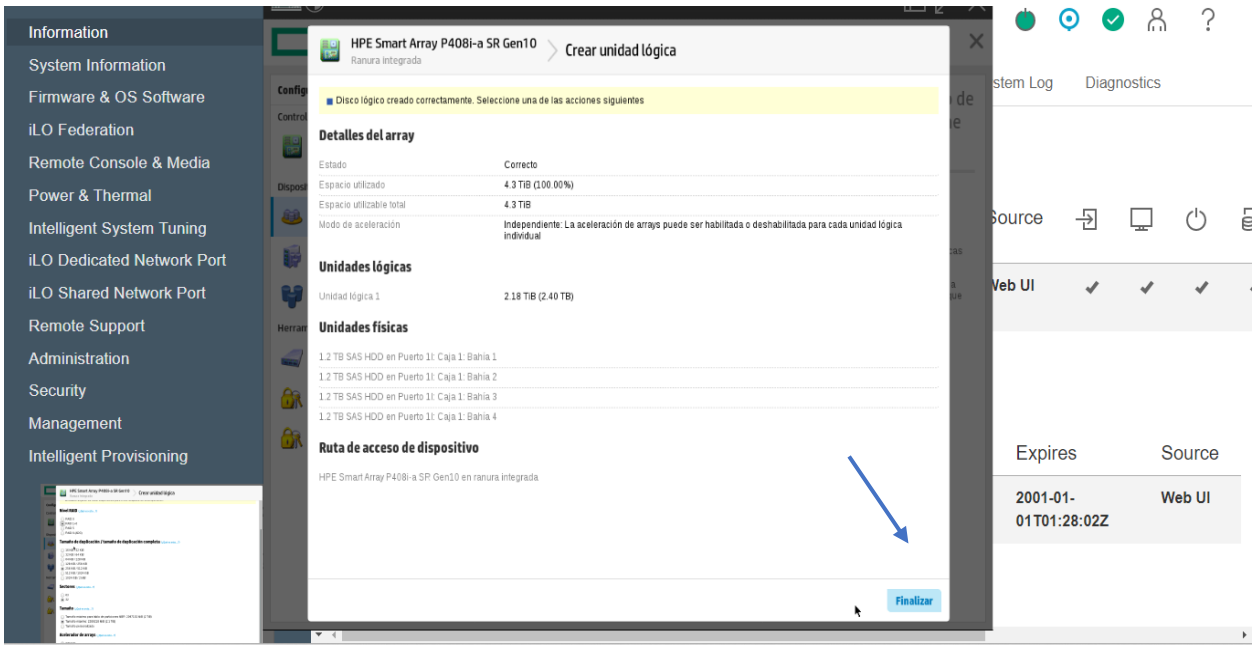


Figura 97: Detalles de RAID

Para verificar si nuestras unidades lógicas están montadas se debe de revisar en unidades lógicas y para finalizar se debe de reiniciar el servidor

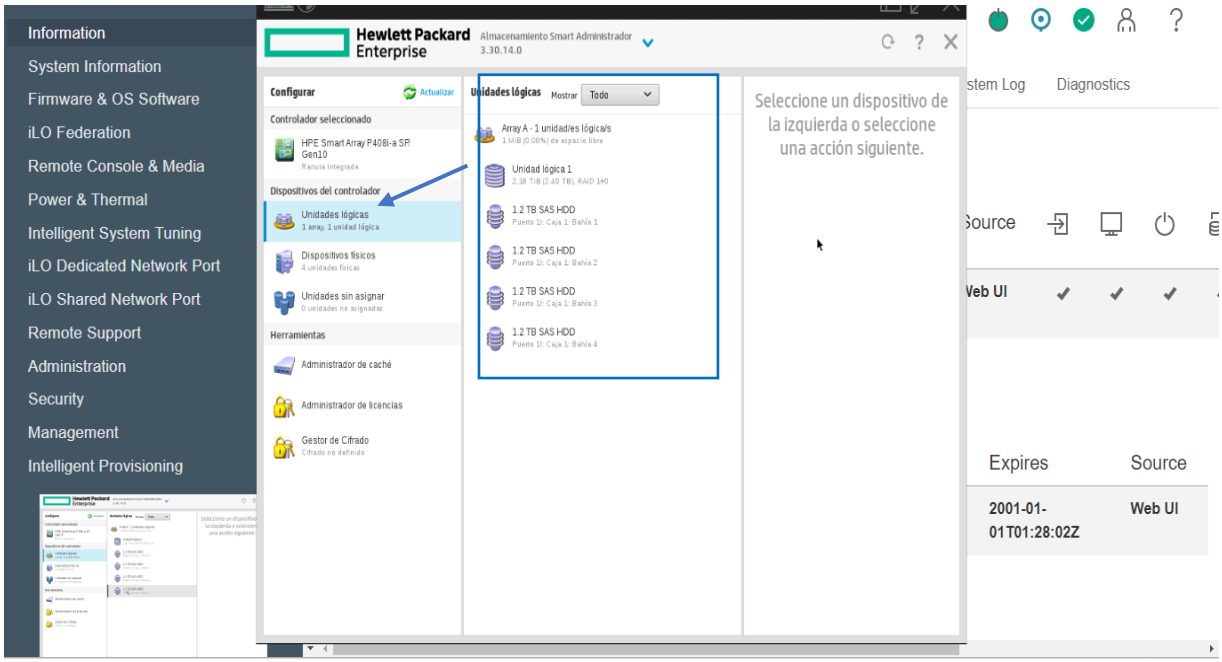


***Figura 98**:* Detalles de unidades lógicas

Habilitar la opción de virtualización del servidor

Esta opción se debe de habilitar para ejecutar más de un sistema operativo ya que nuestro grabador de video se va a alojar en Ubuntu, para activar la virtualización se ingresa a la BIOS del servidor por medio del hilo, seguidamente se selecciona configuración del sistema

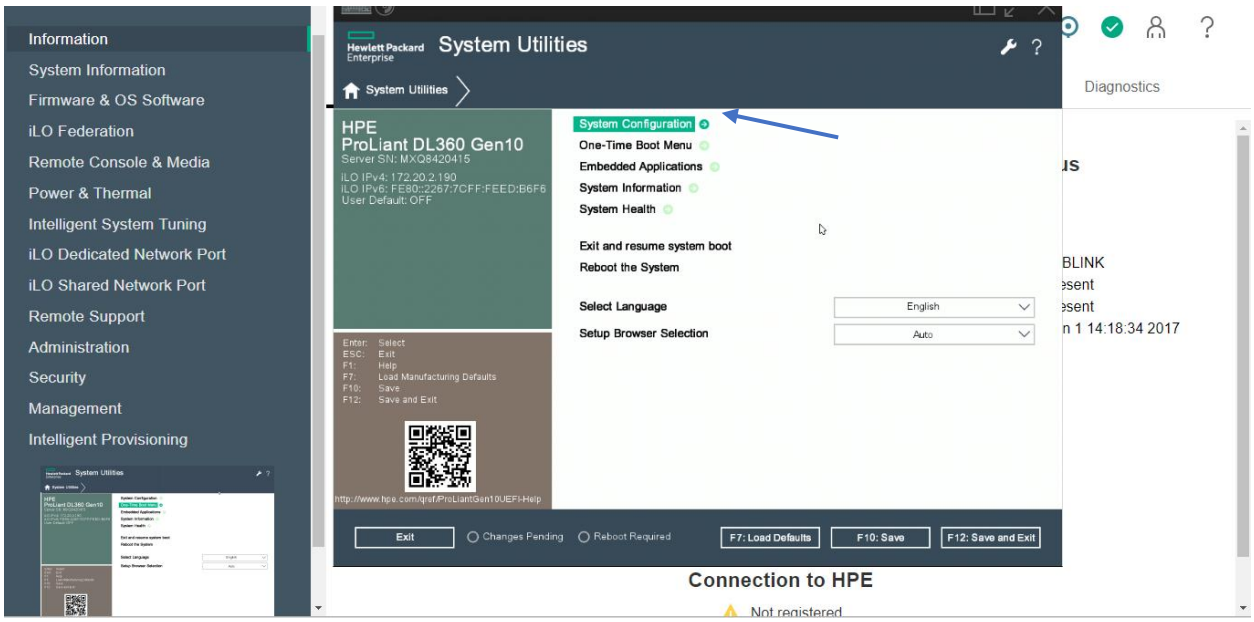


Figura 99: Boot del servidor

A continuación, se presiona BIOS

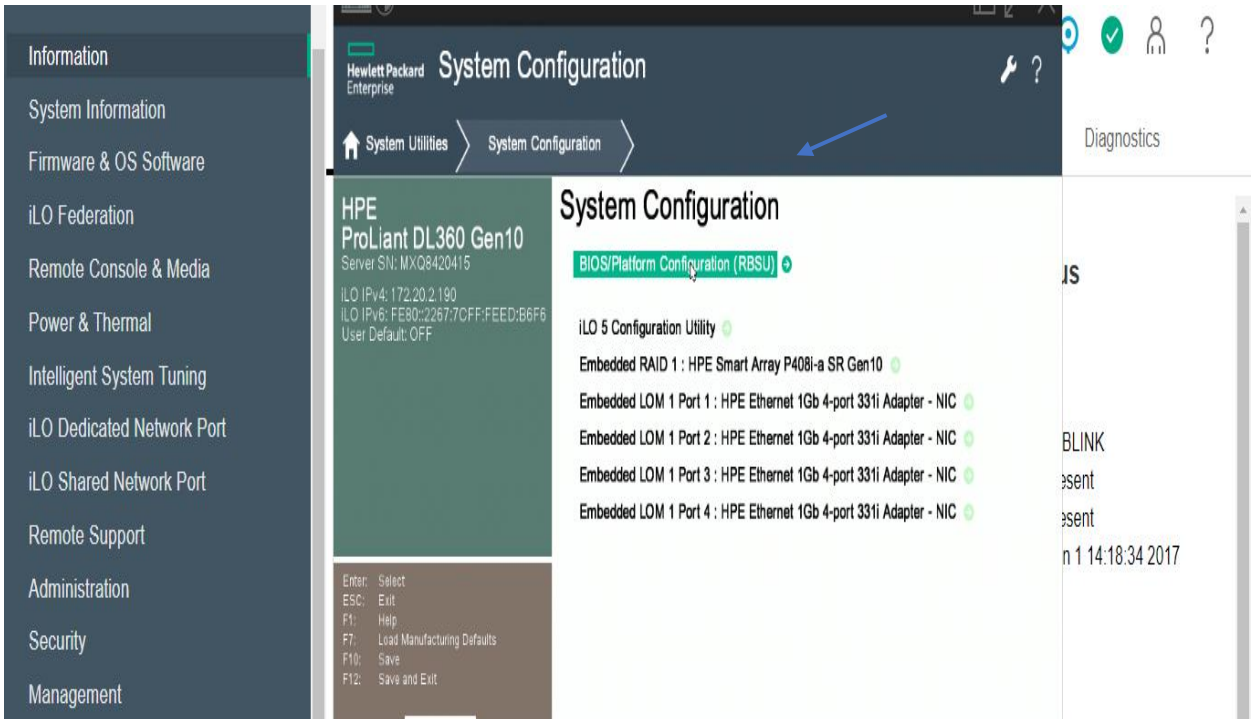


Figura 100: Configuración del sistema

Se elige el botón opciones del sistema

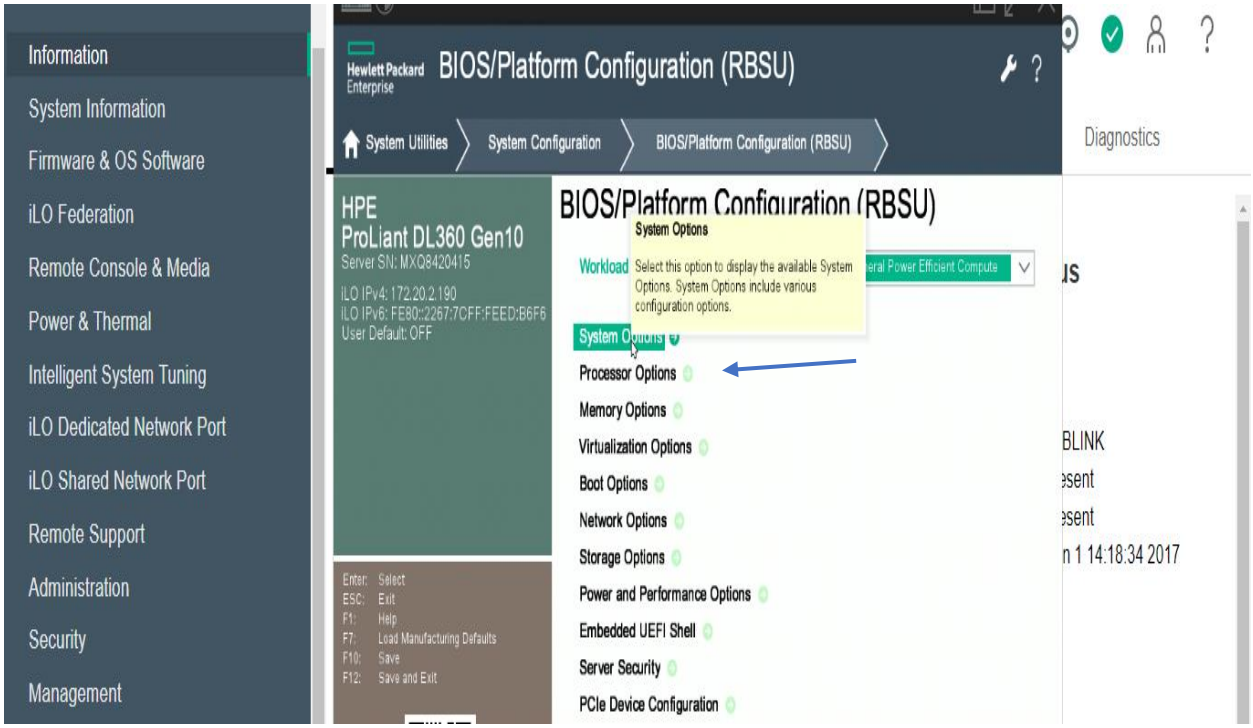


***Figura 101*:** Opciones del sistema del servidor

En esta ventana habilitamos la visualización del servidor y se guarda presionando F10

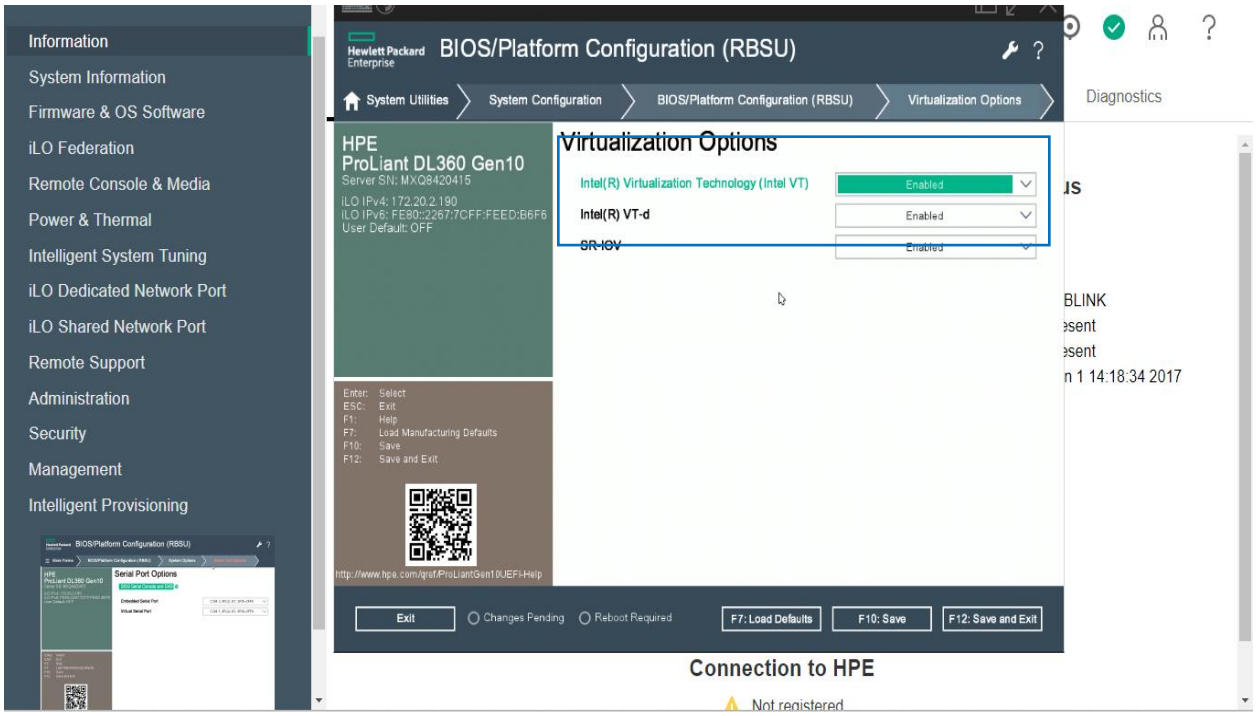


Figura 102: habilitar virtualización

De la misma manera revisamos las opciones del procesador

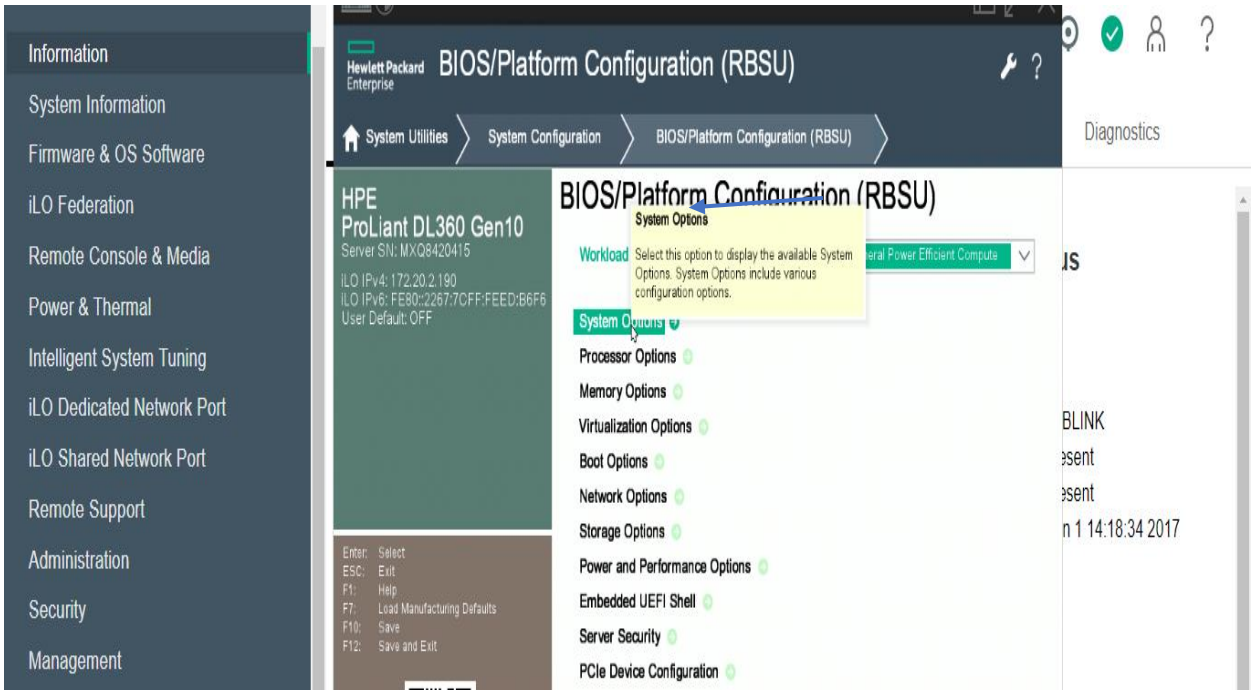


Figura 103: Opciones del procesador

De manera similar se debe de habilitar esta opción y se presiona la tecla F10

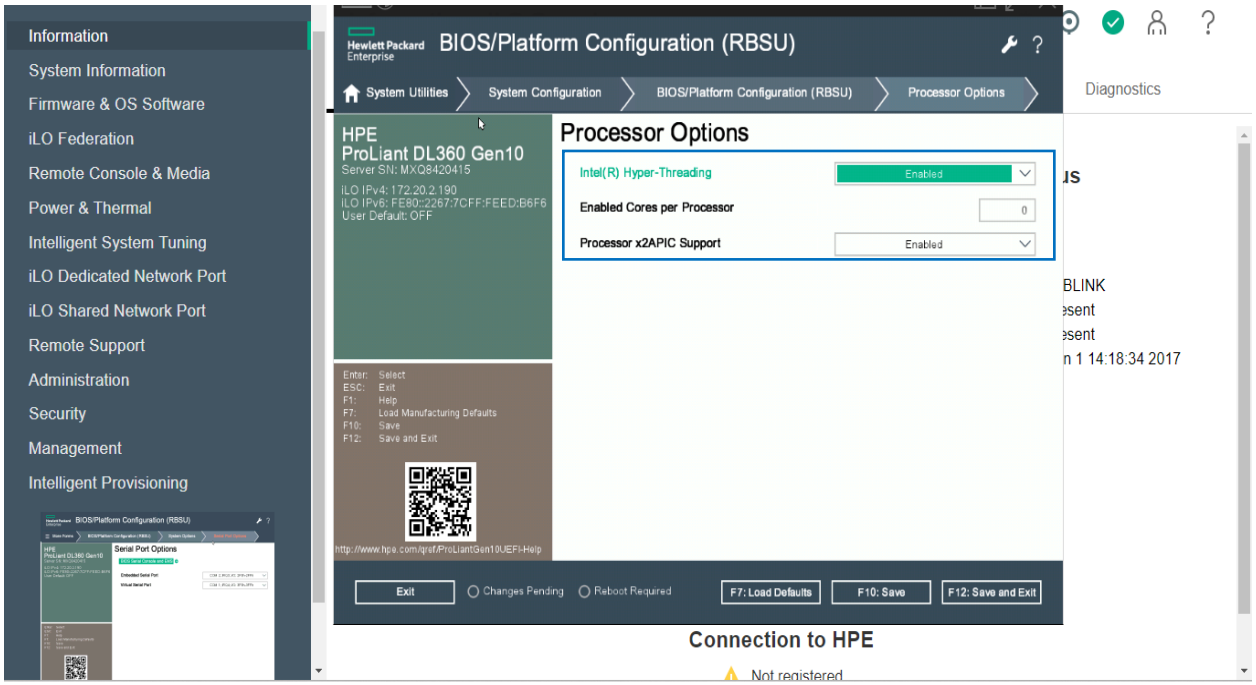


Figura 104: Habilitar opciones del procesador

Para finalizar las configuraciones se presiona en el botón que muestra la imagen

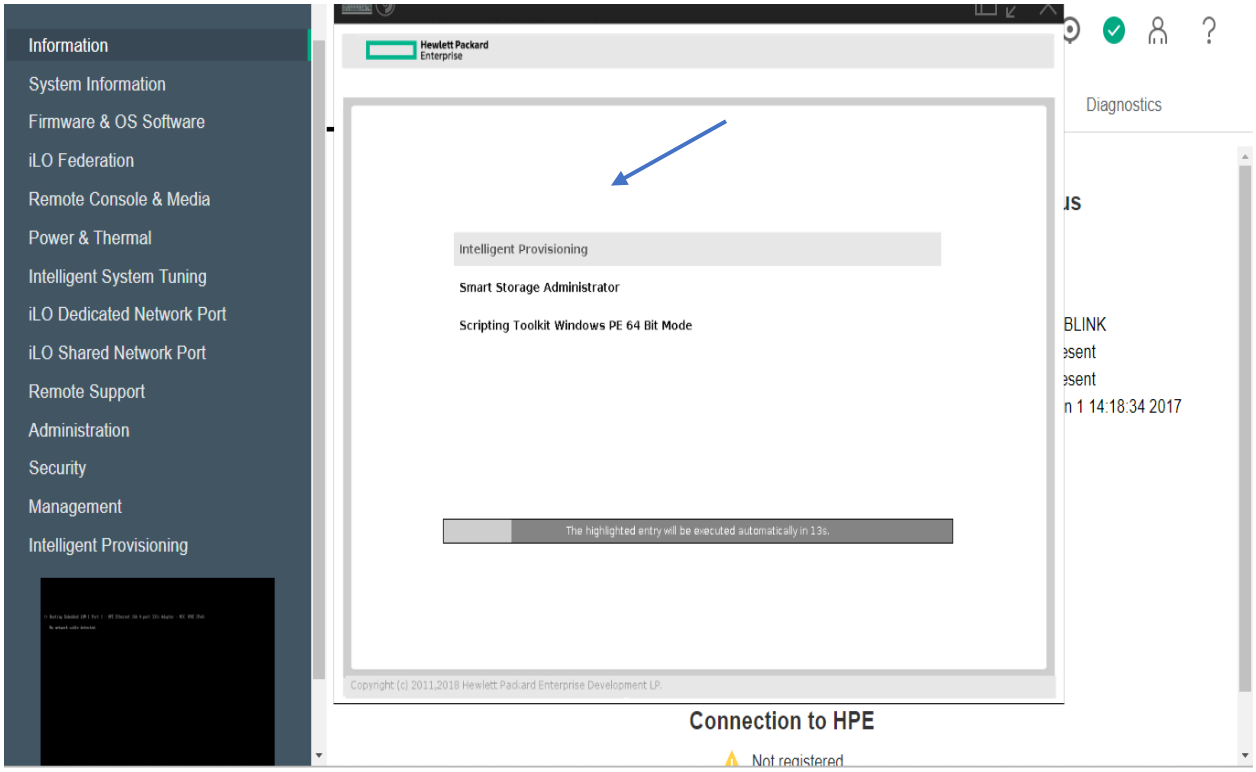


Figura 105: Aplicación de cambios al servidor

A continuación, el servidor se reiniciará y estará listo para instalar el sistema de video vigilancia

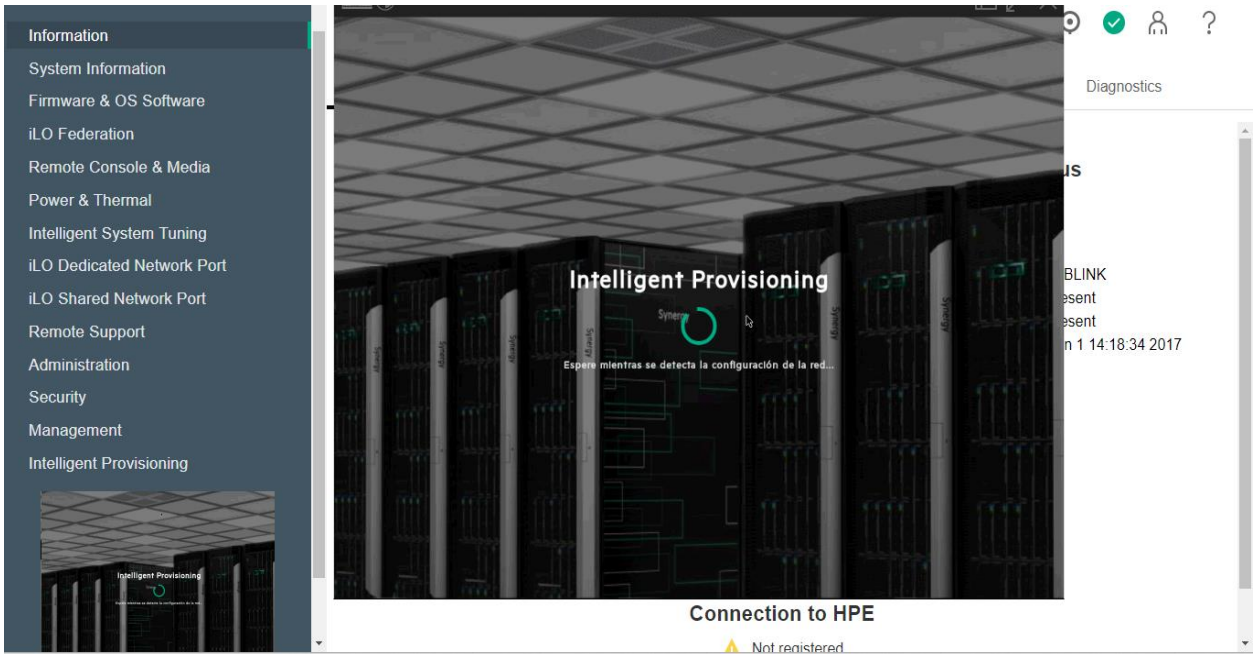


Figura 106: Interfaz de reinicio del boot

Por otro lado, para obtener la información del servidor gracias al puerto del hilo se tiene directamente la información del procesador

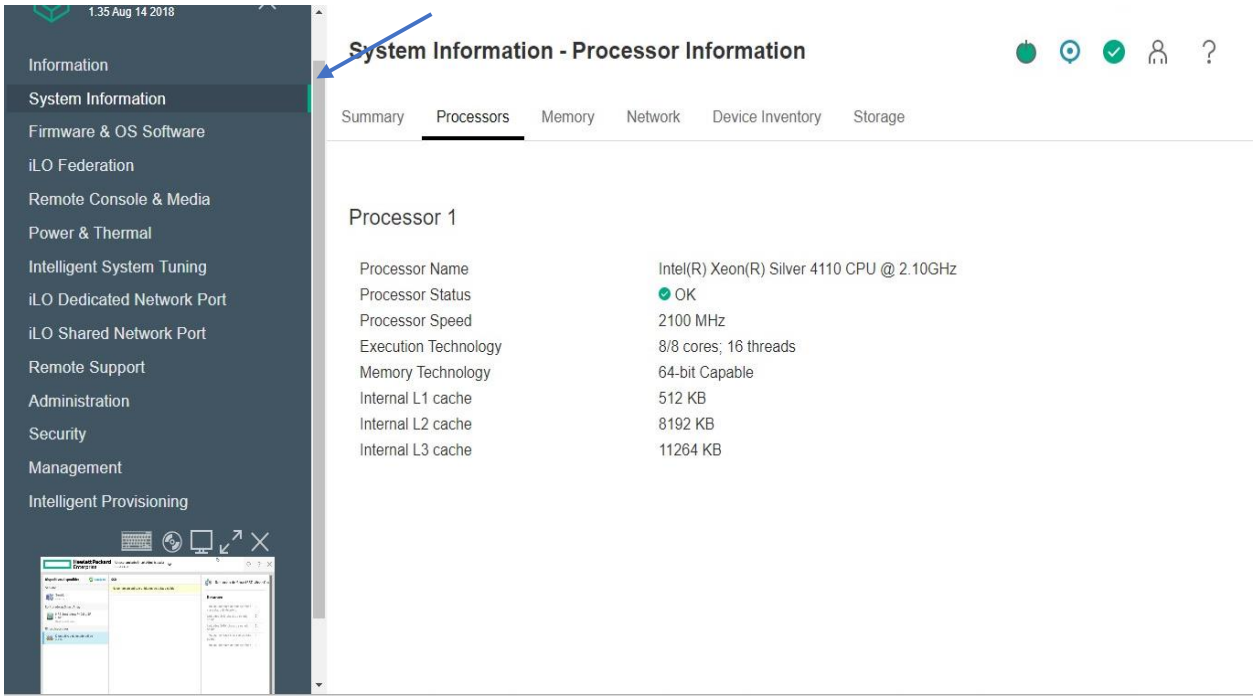


Figura 107: Ventana de información del sistema

En el botón de información de memoria se puede observar la utilizada

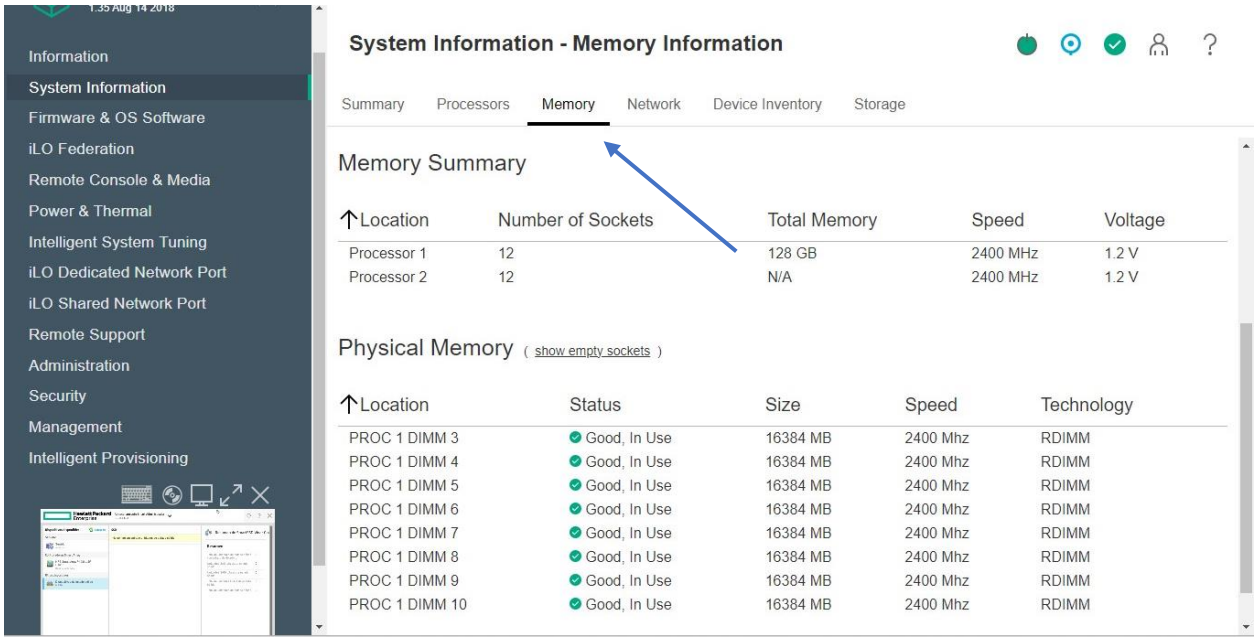


Figura 108: Memoria del servidor

Instalación de Ubuntu

Para iniciar con la instalación de Ubuntu al reiniciar el servidor se presiona la tecla F9 para ingresar a la BIOS

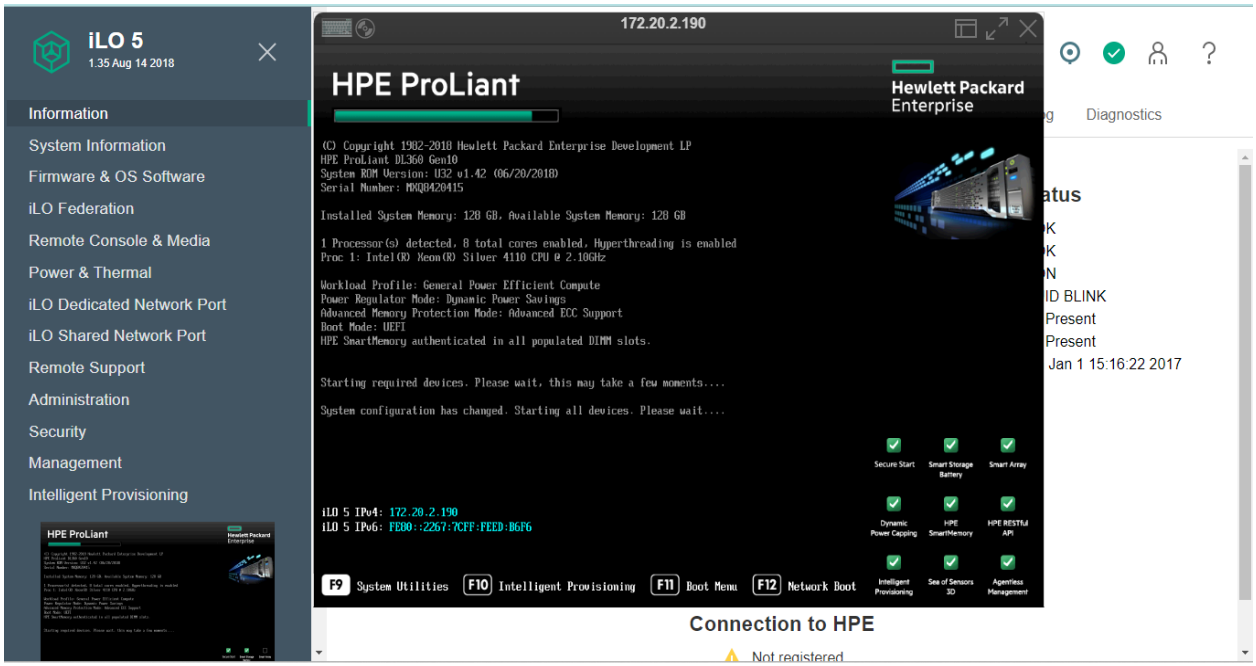


Figura 109: Ventana de inicio del servidor

Ingresamos al menú Bot

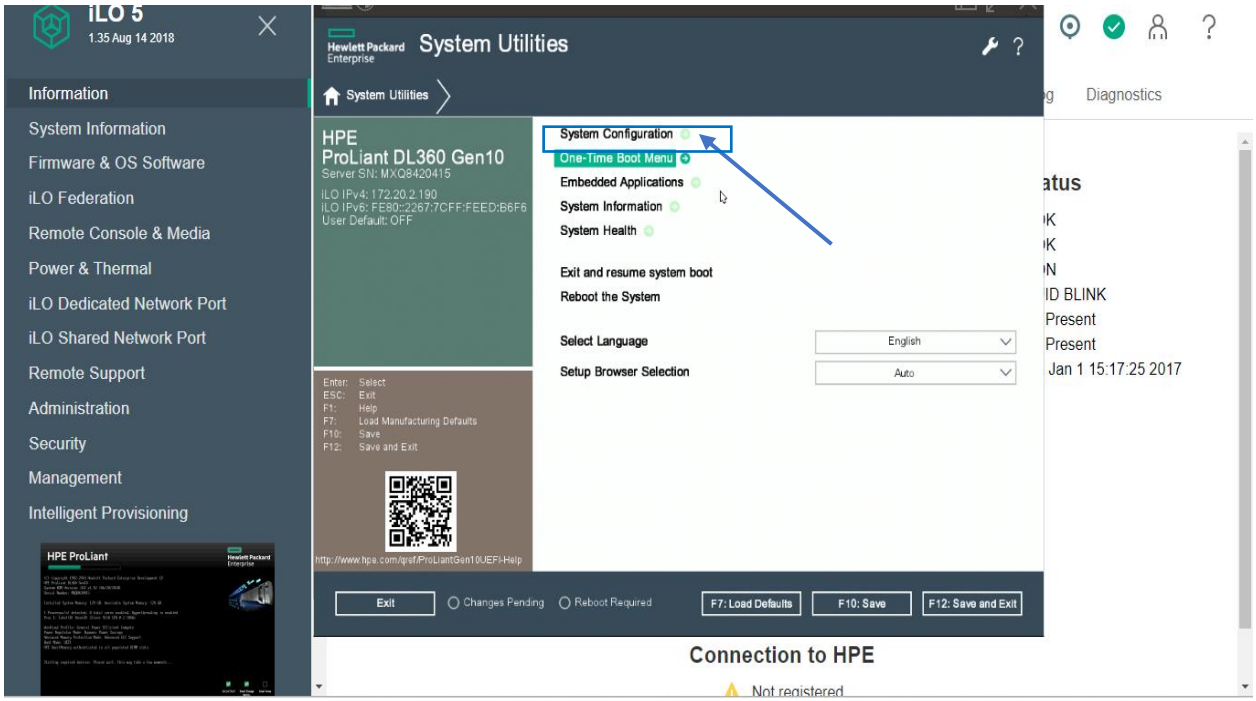


Figura 110: Menú de boot

Seleccionamos nuestra USB boteada para iniciar con la instalación de Ubuntu

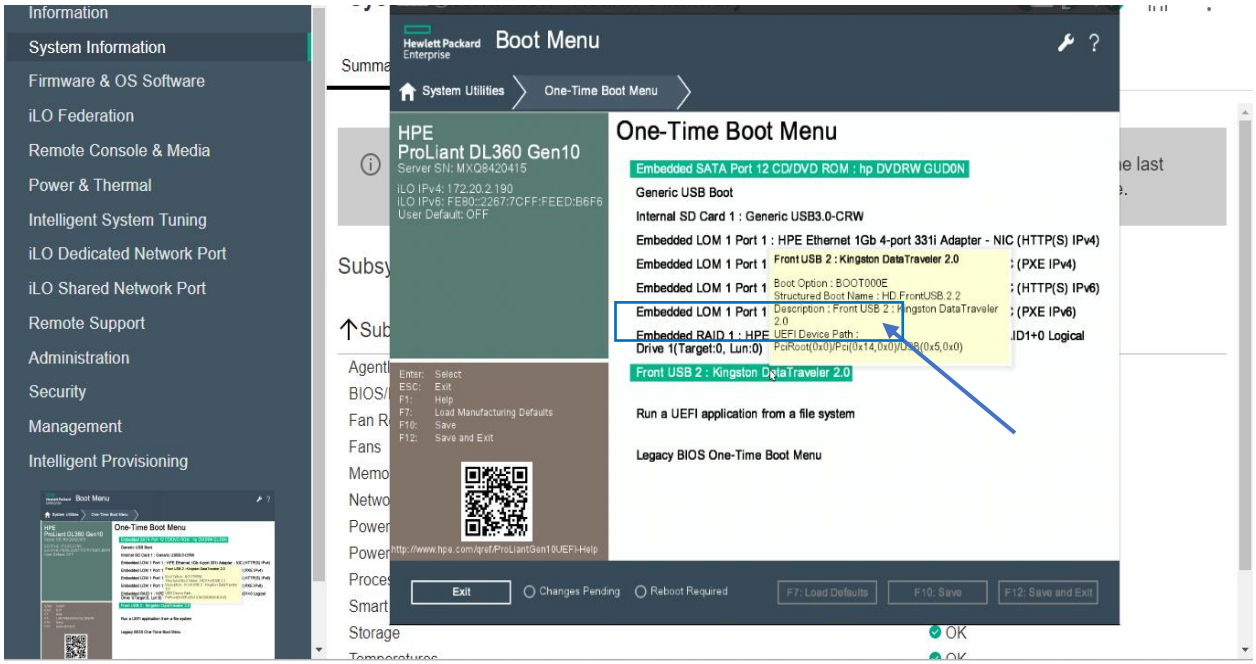


Figura 111: Elección del dispositivo con el sistema a instalar

Seguidamente seleccionamos la instalación de Ubuntu

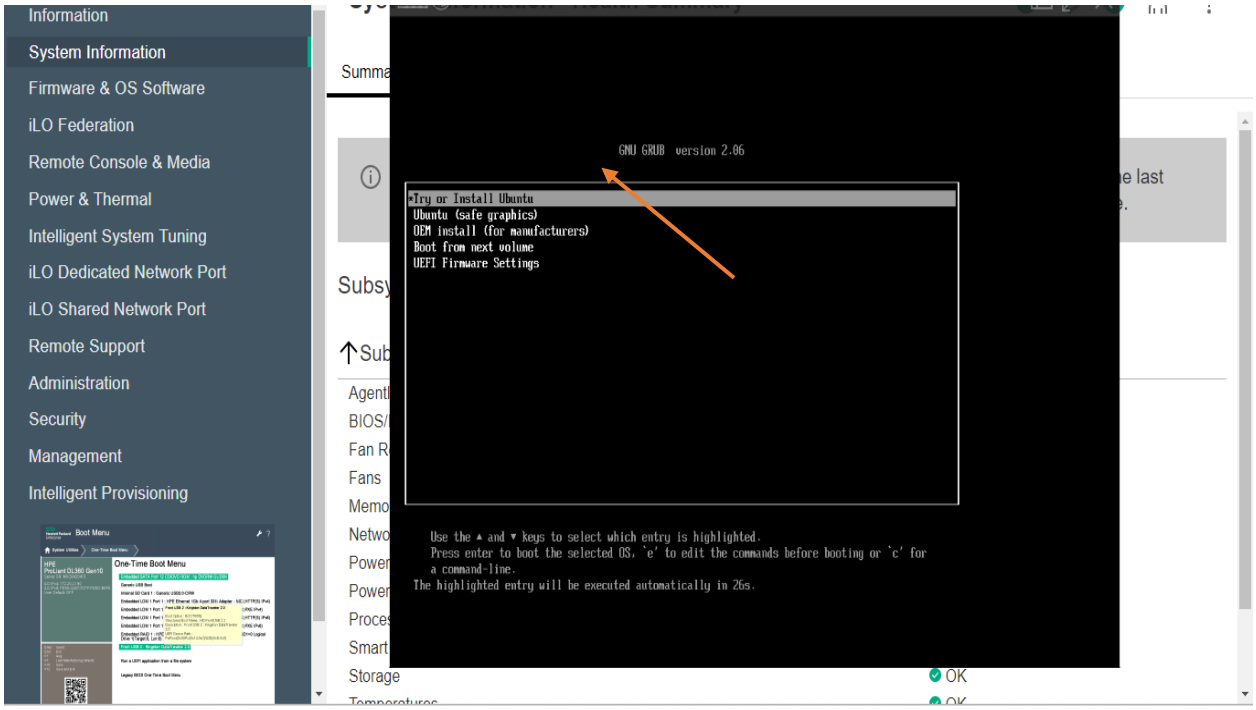


Figura 112: Interfaz instalación

El sistema empieza a cargar para empezar con la configuración

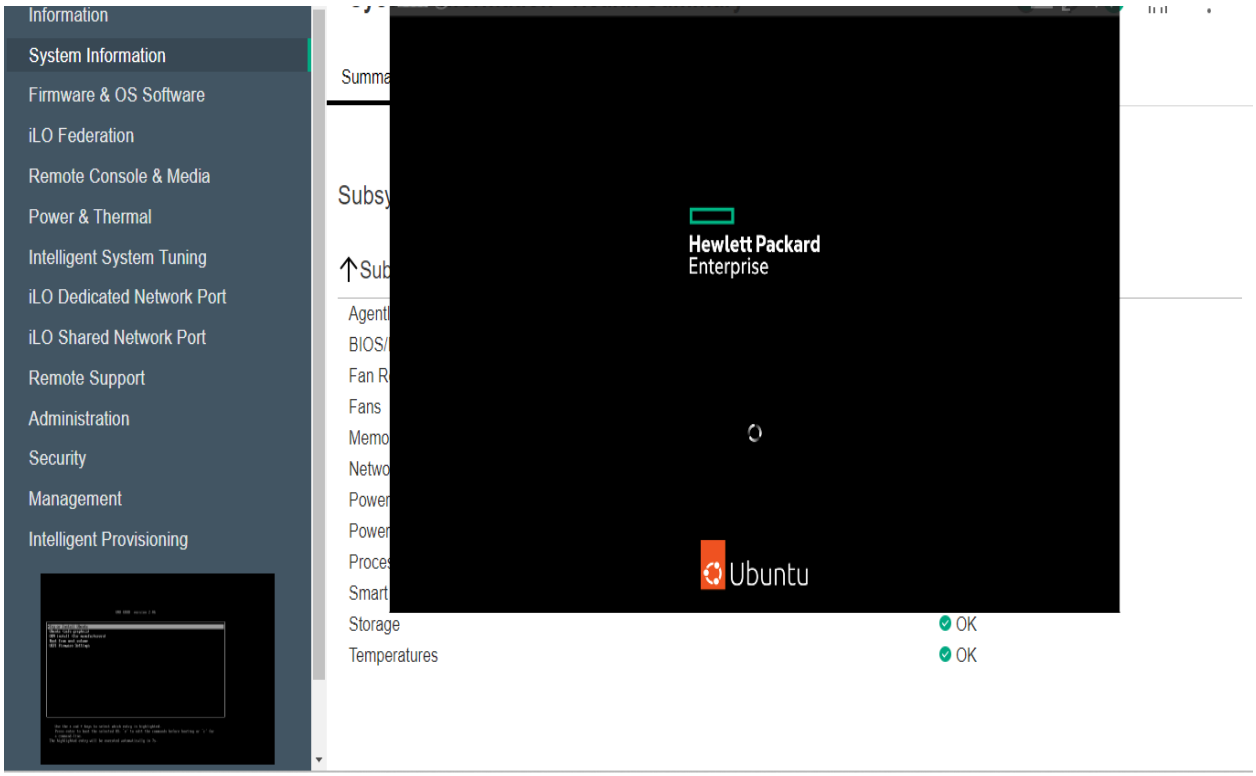


Figura 113: Instalación de Ubuntu

Elección de idioma e instalación de Ubuntu

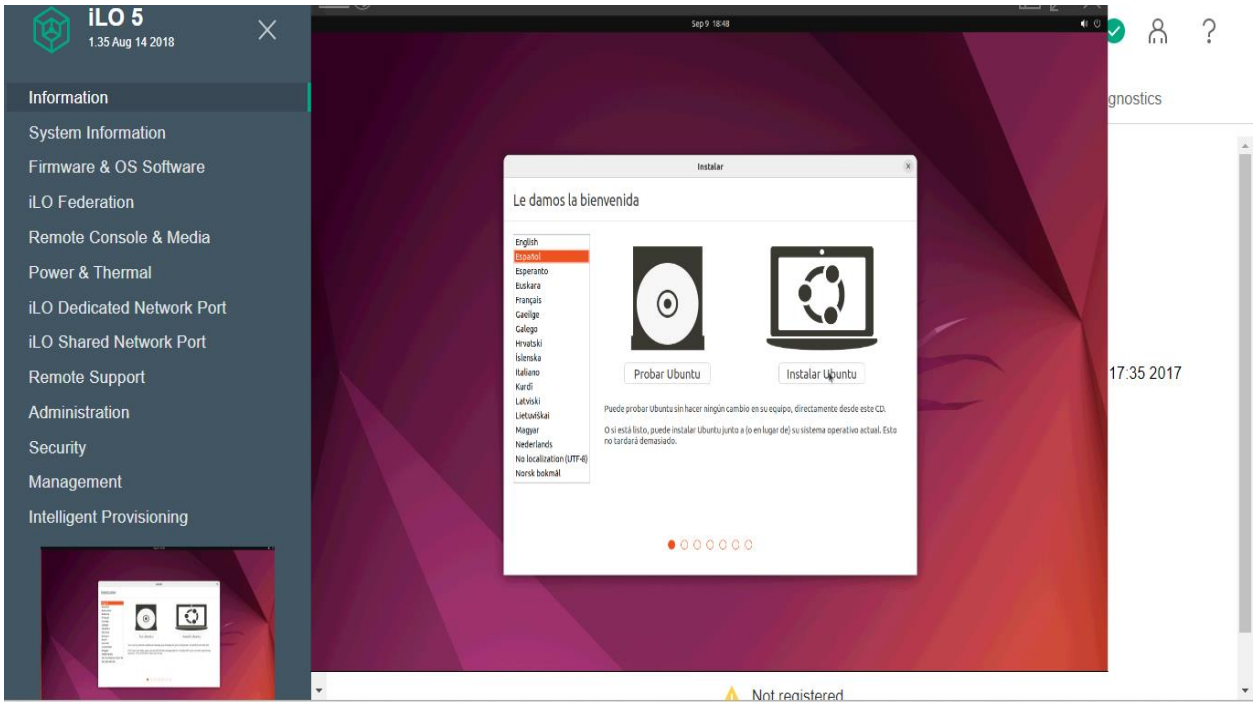


Figura 114: Instalación de Ubuntu

Elección de disposición del teclado

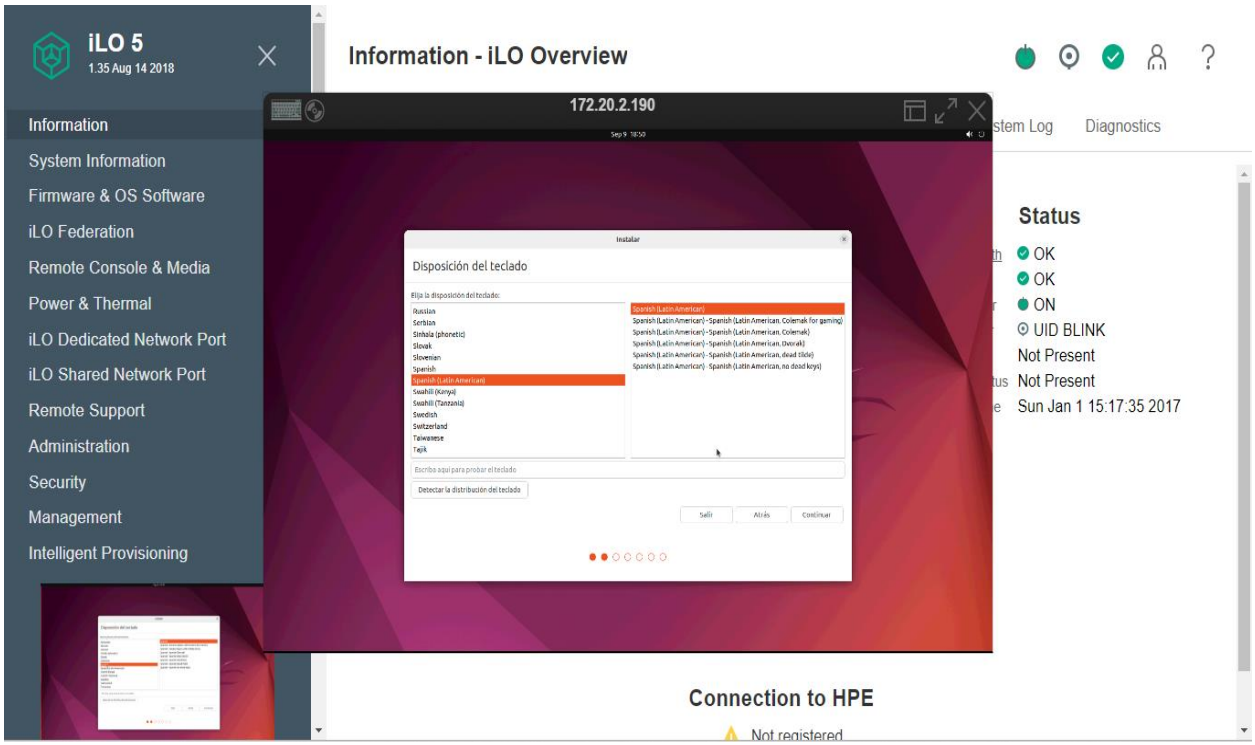


Figura 115: Disposición de teclado

Elección de actualizaciones y elección de aplicaciones de terceros

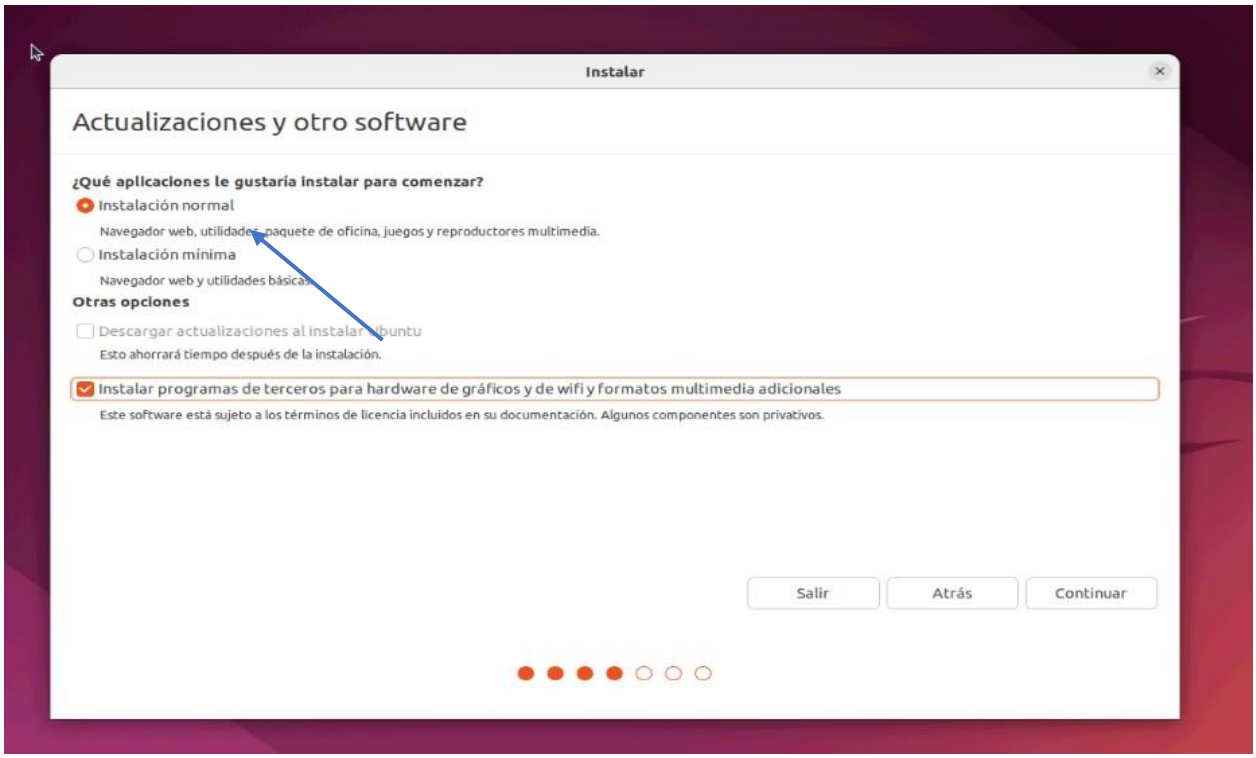


Figura 116: Tipo de instalación

Elecciones tipo de instalación recomendada del mismo modo de red

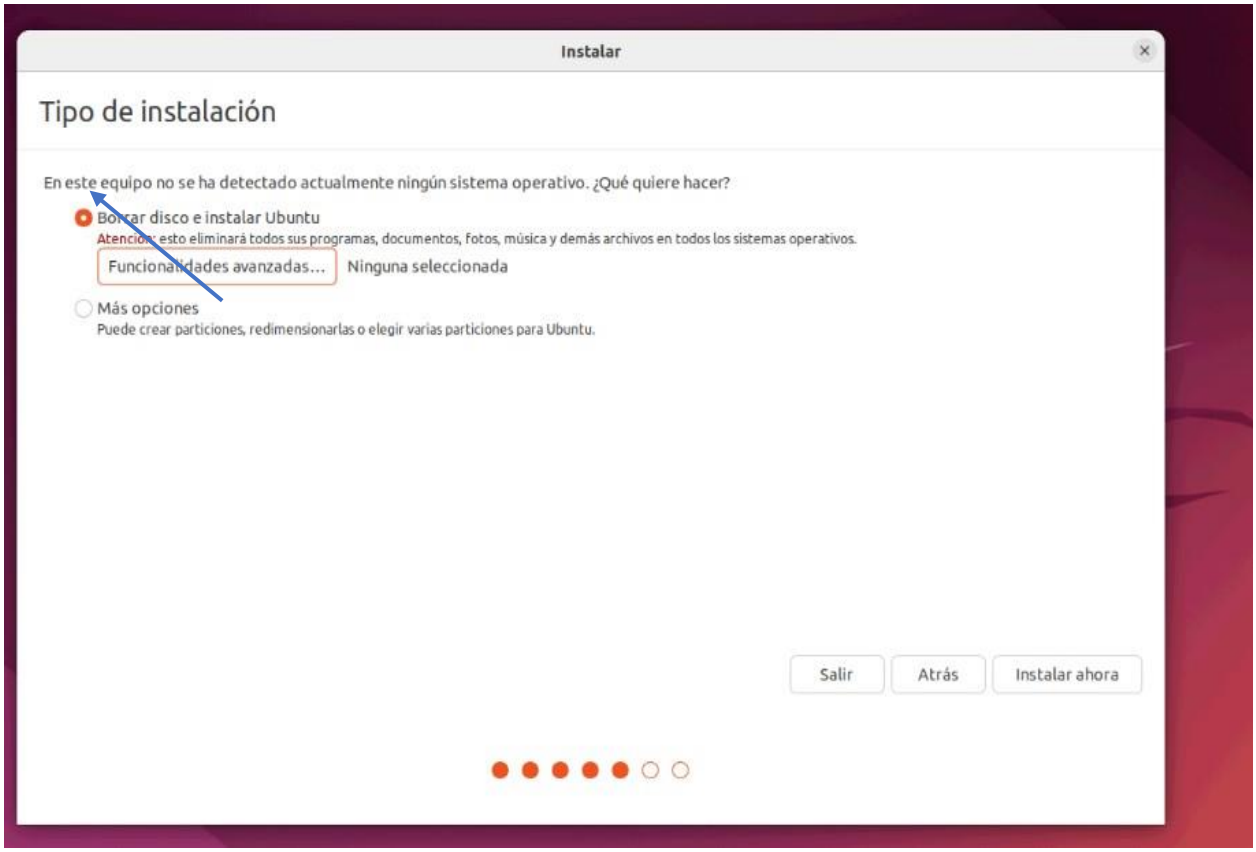


Figura 117: Formateo de discos

Creación de credenciales para el usuario para ingresar al escritorio de Ubuntu

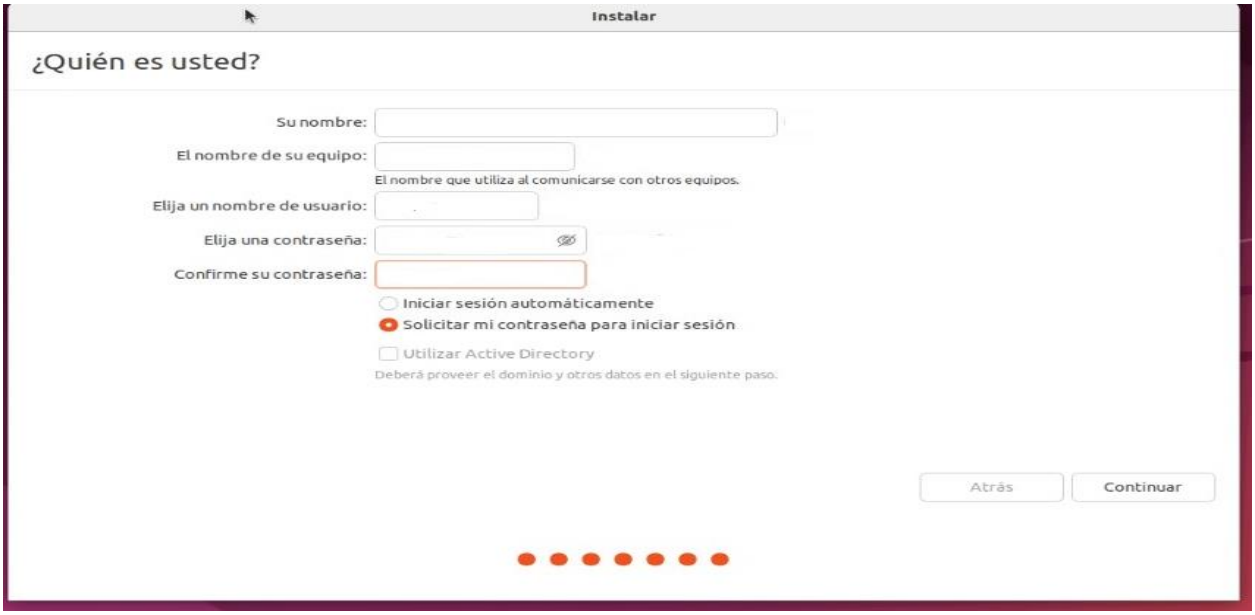


Figura 118: Ingreso de credenciales

Anexo 7:Manual de monitoreo del sistema

MANUAL DE MONITOREO DEL SISTEMA

Interfaz de inicio del sistema de video vigilancia la cual nos da la línea de tiempo de grabación

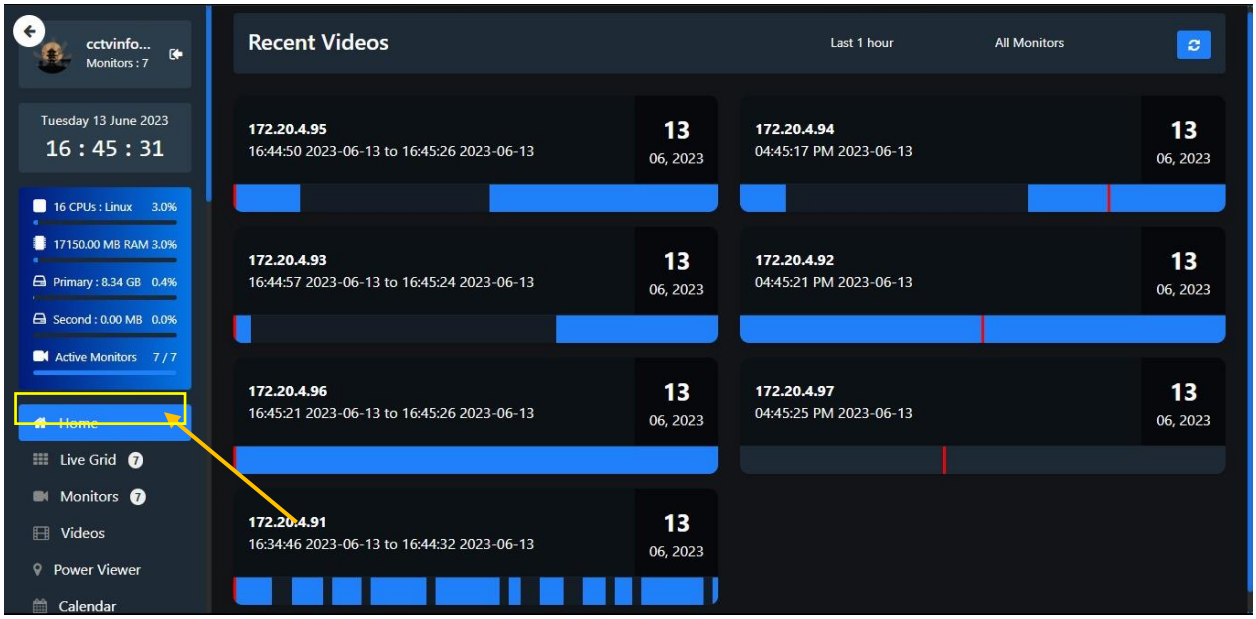


Figura 119: Interfaz de inicio del sistema SHINOBI

En el botón de live grid indica las cámaras que se encuentran conectadas al sistema así mismo los accesos a configuraciones, videos.

Figura 120: Grabaciones en tiempo real

En el menú de monitores se puede ingresar nuevas cámaras o revisar las configuraciones de las que se encuentran enlazadas

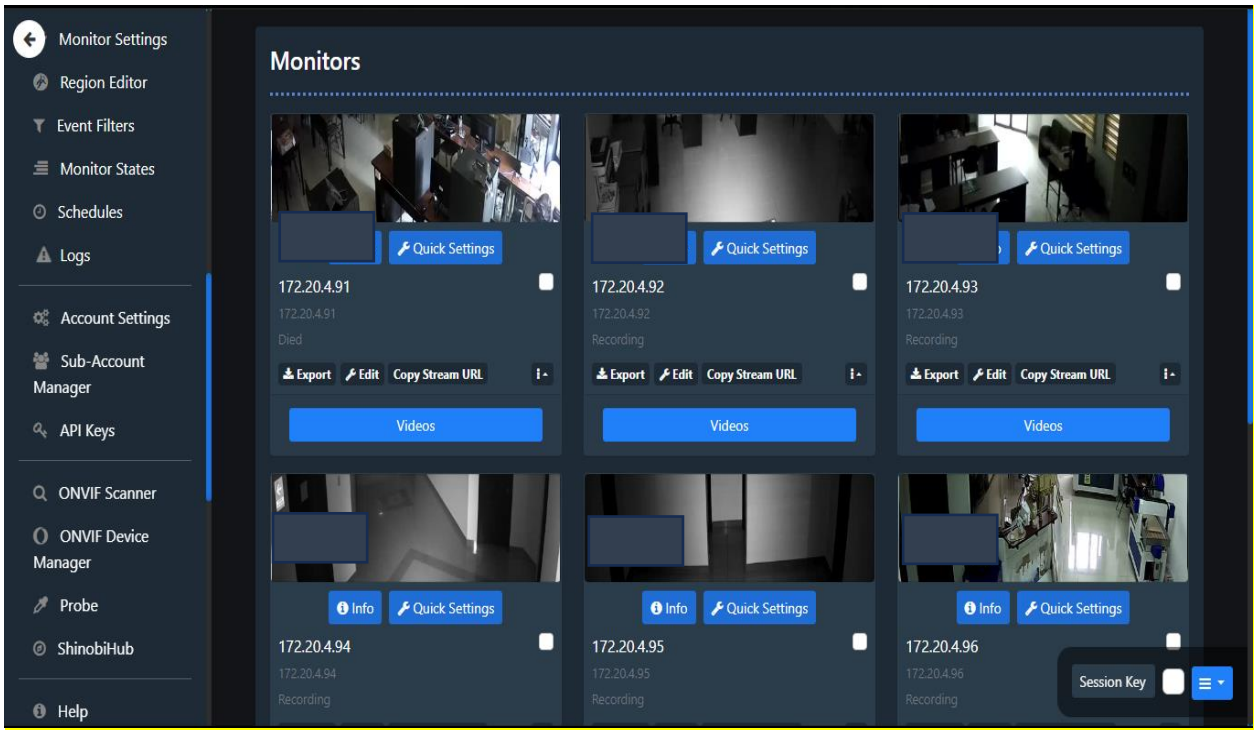


***Figura 121*:** Configuración de monitores

En menú de video podremos observar todos los videos que son capturados por las cámaras que se encuentran en la carrera de computación

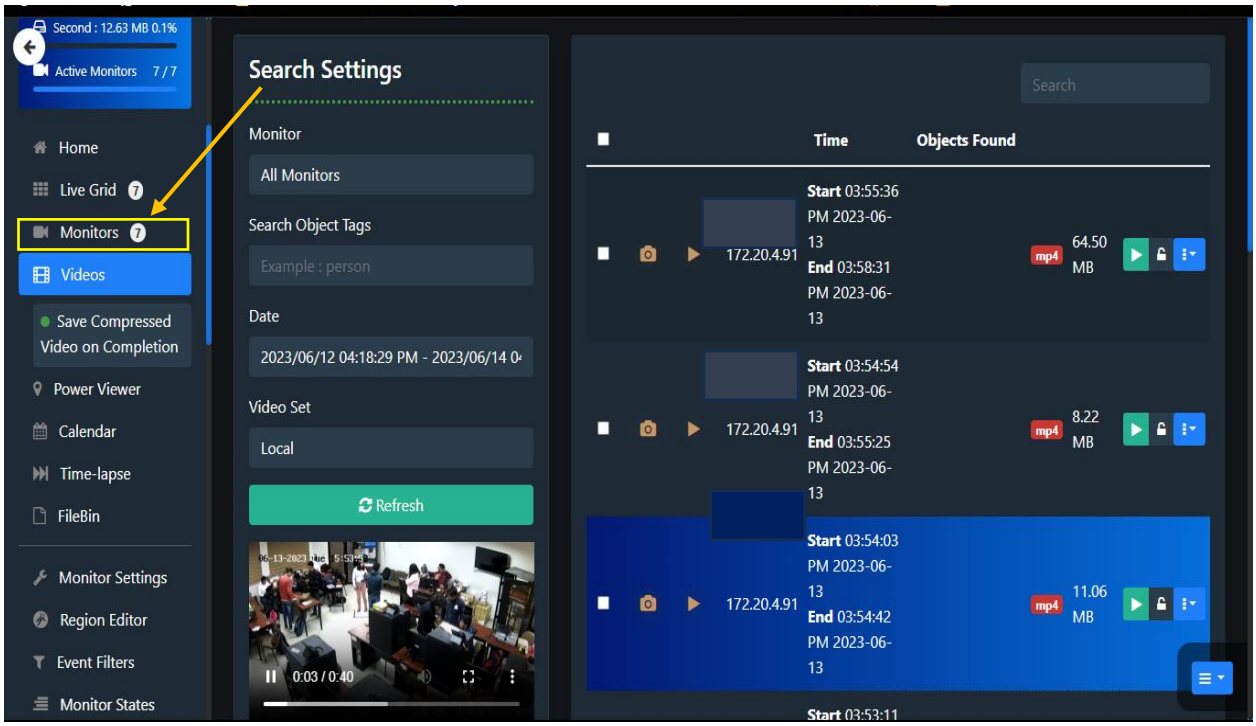


***Figura 122**:* Videos grabados

Visualización de videos por fechas especificas en el calendario

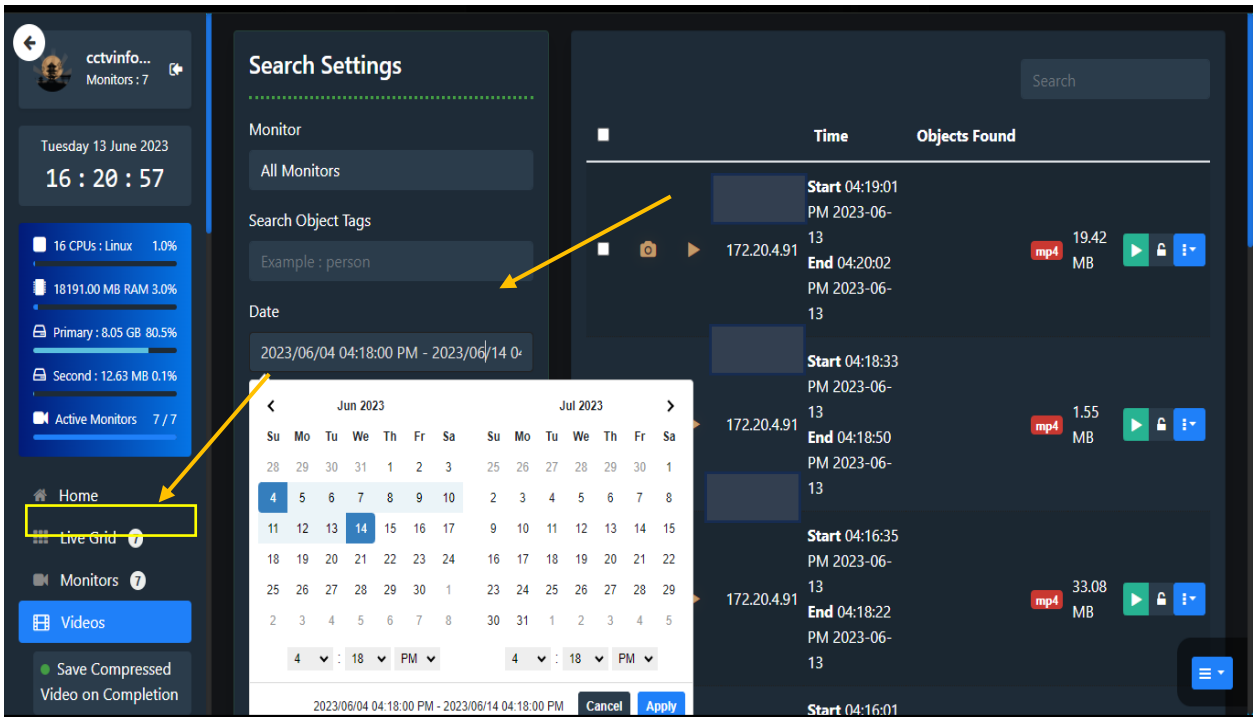


Figura 123: Vista de videos por intervalos de tiempos

En el botón de vista se puede elegir la cámara y revisar la línea de tiempo de grabación

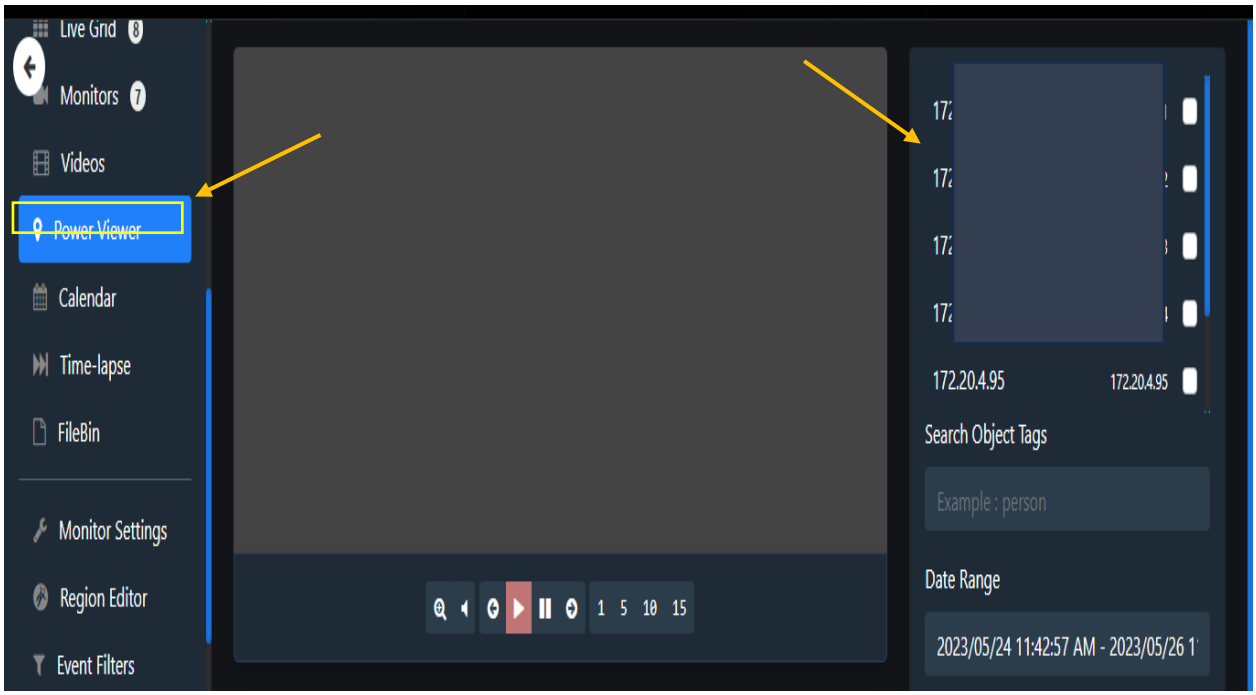


Figura 124: Grabaciones de cámaras

En la línea de tiempo se puede divisar el rango de fecha que desea visualizar son los videos, así como los eventos.

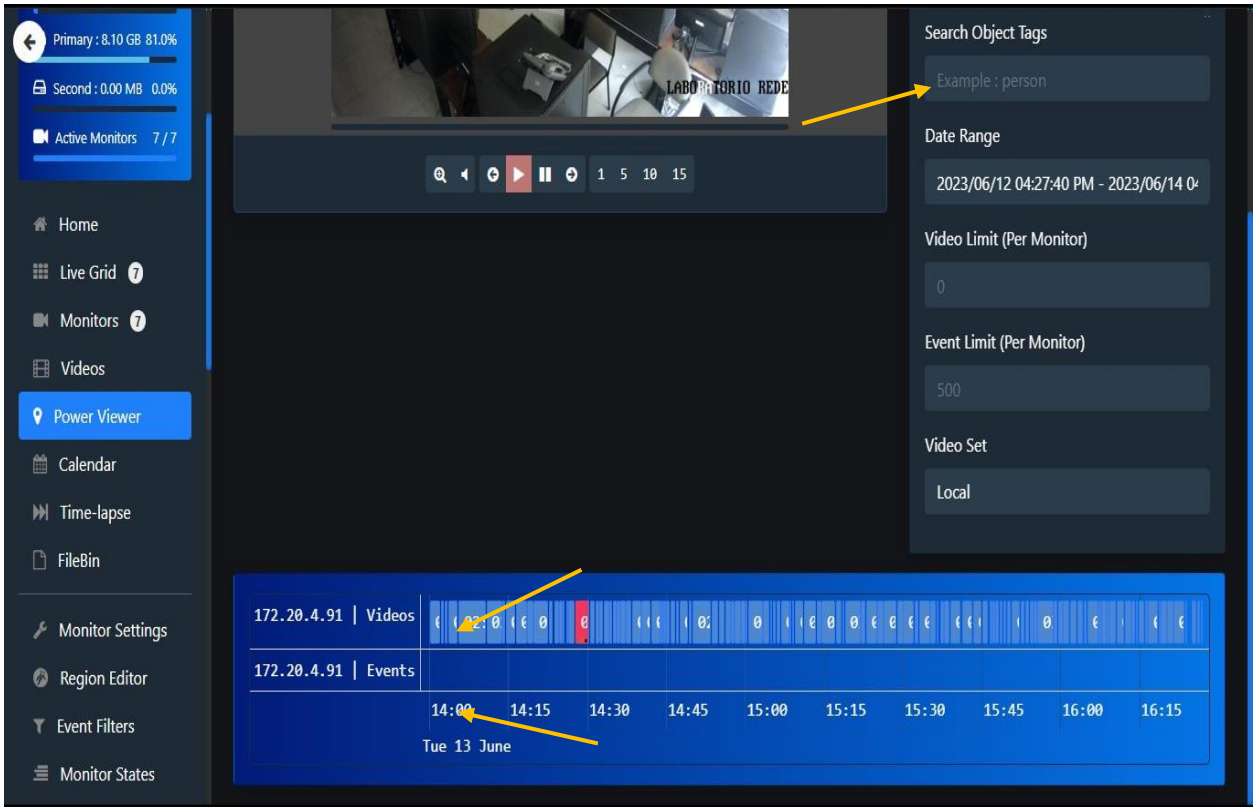


Figura 125: Línea de tiempo de las cámaras

En el calendario podemos elegir la cámara y nos muestra los días de grabación

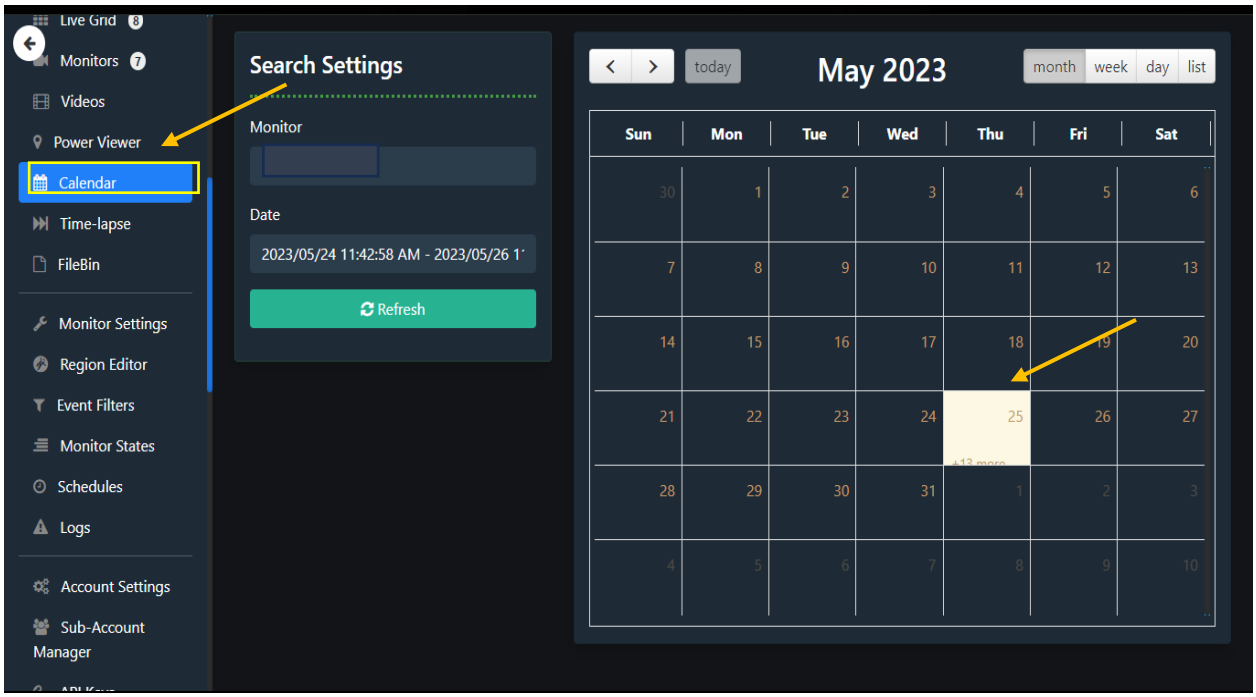


Figura 126: Vista de grabaciones en el calendario

En el editor de región se puede dibujar la zona a grabar o detectar movimiento

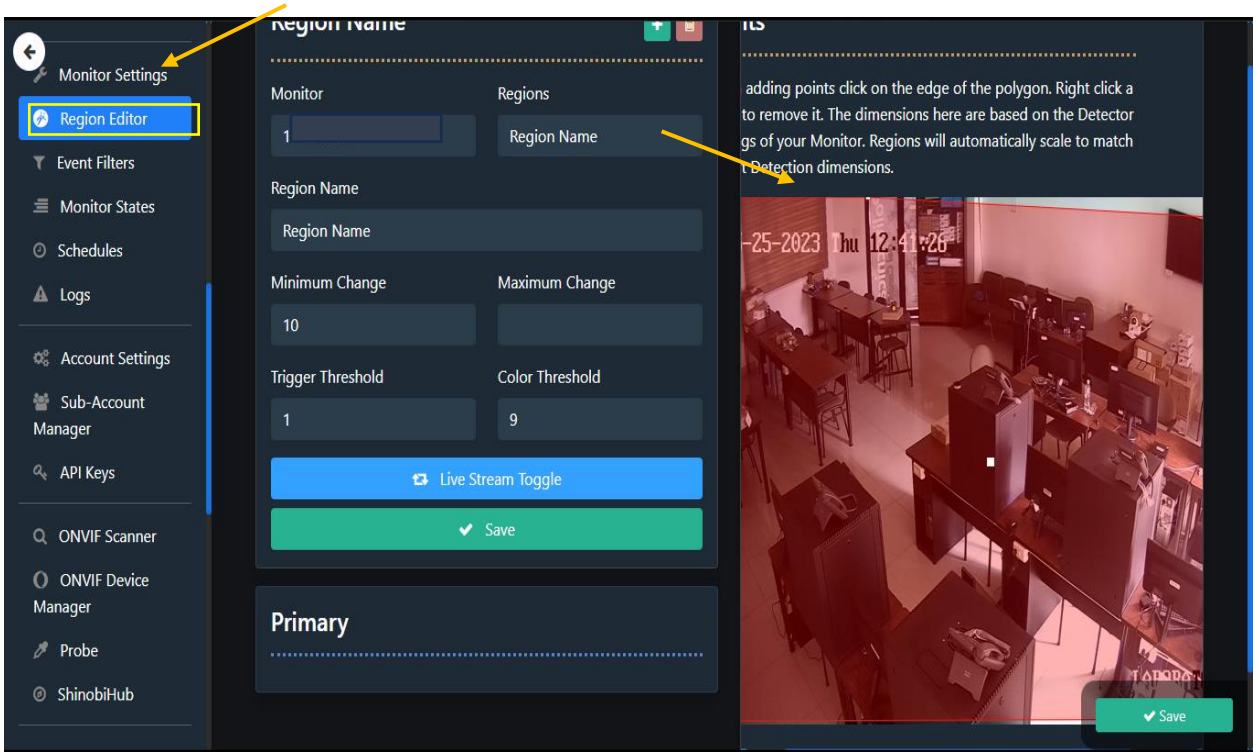


Figura 127: Editor de región de la cámara

El filtro de eventos se encarga de configurar la detección de movimiento en diferentes horarios

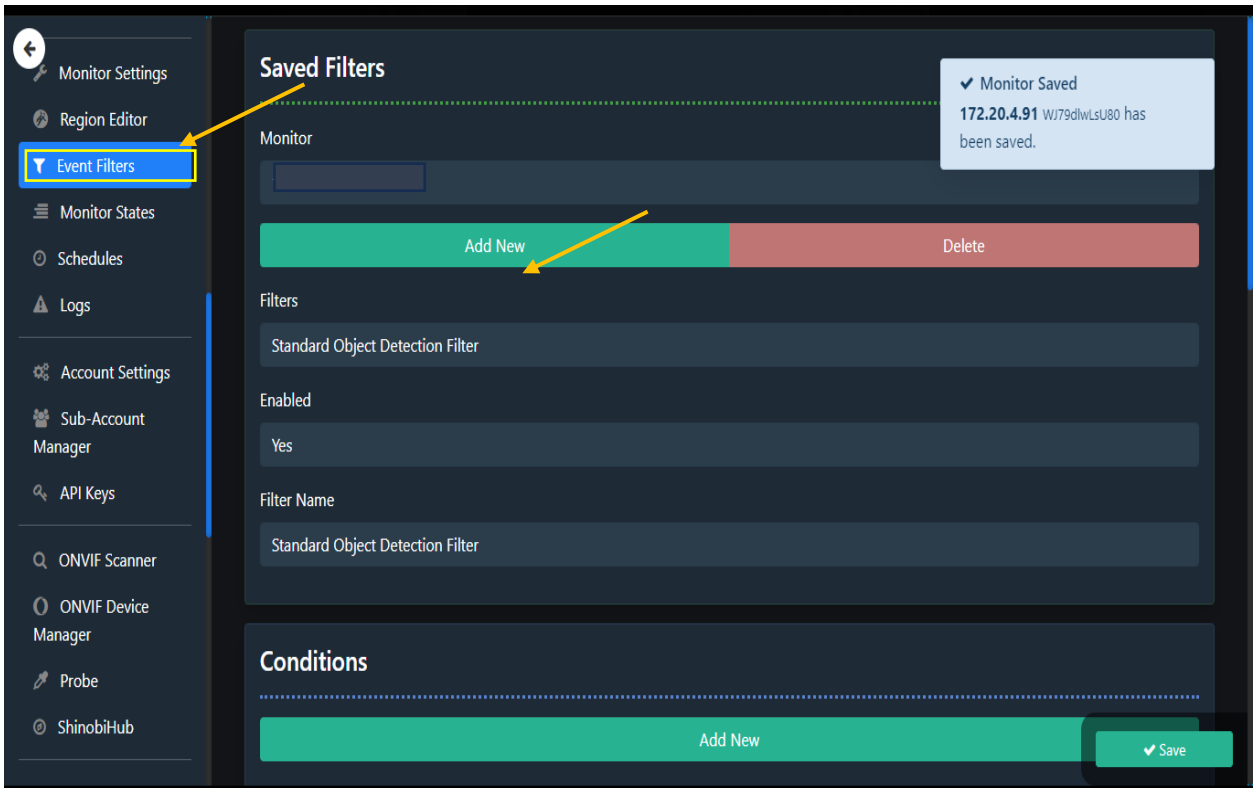


Figura 128: Filtro de eventos

Objeto de detección de eventos

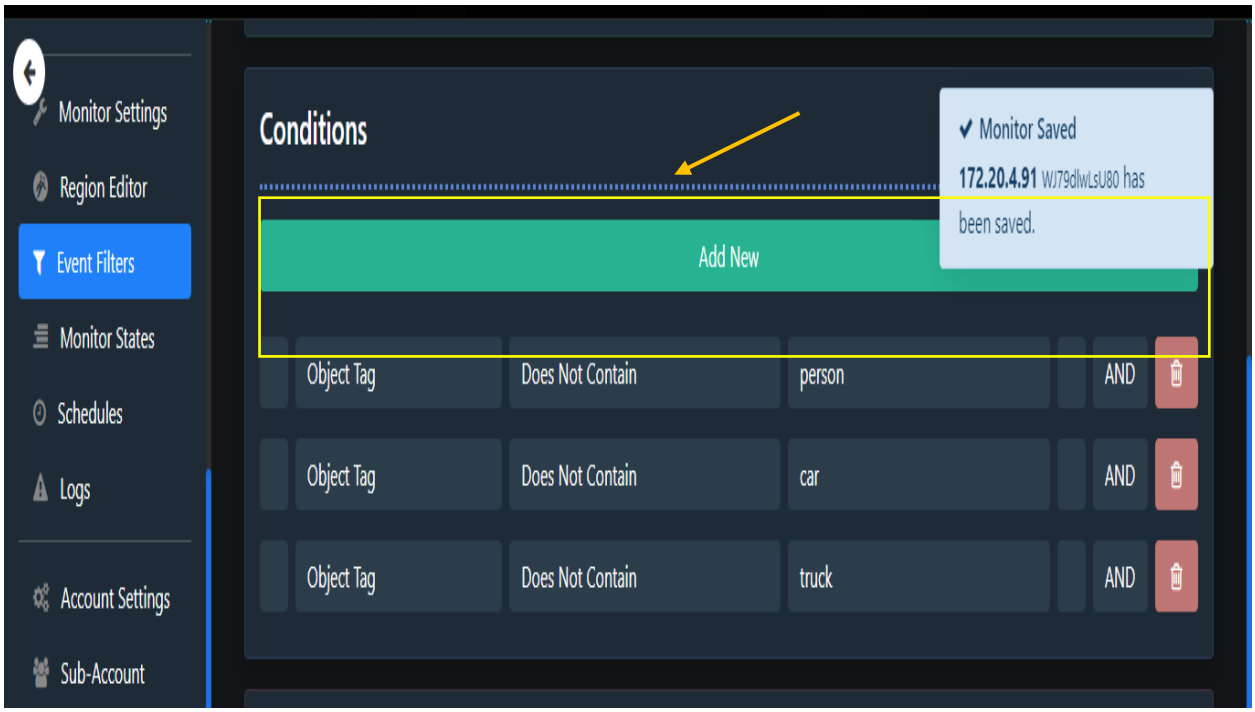


Figura 129: Objetos a visualizar

Configuración de acciones a realizar en la detección de objetos

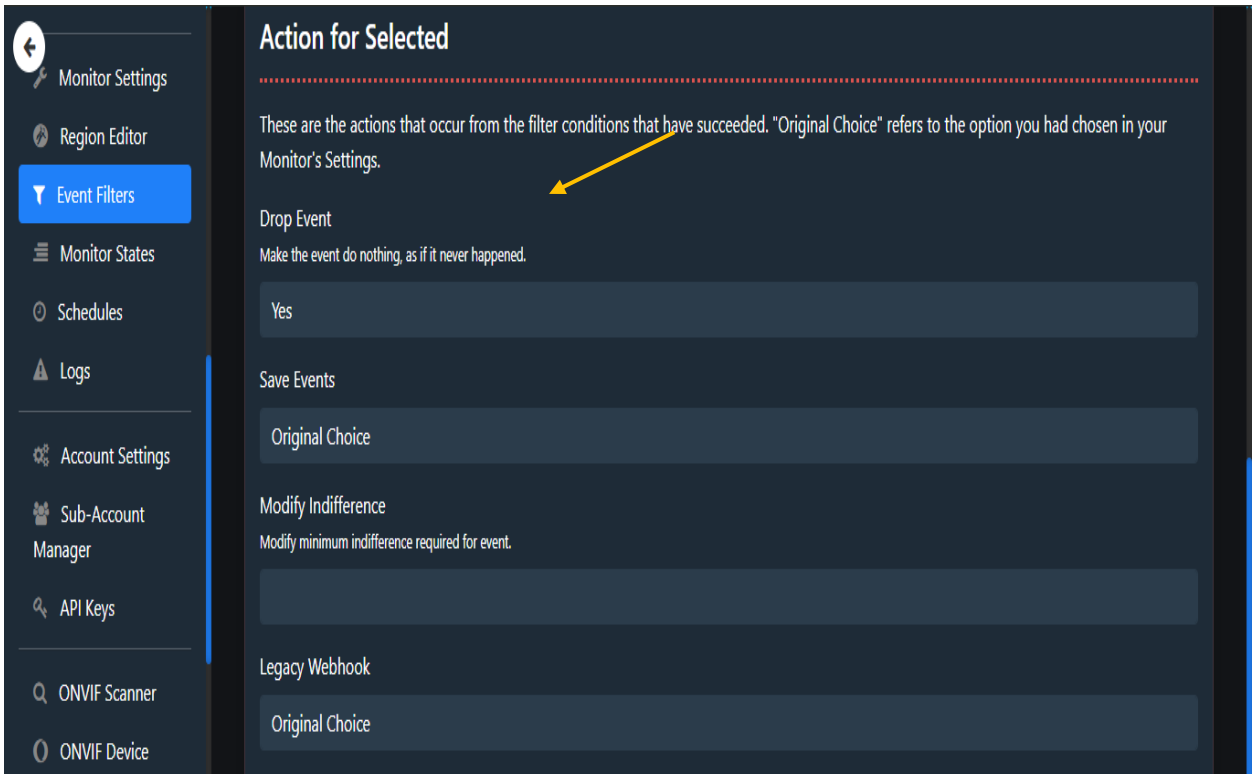


Figura 130: Activación de eventos

Creación de horarios para los eventos

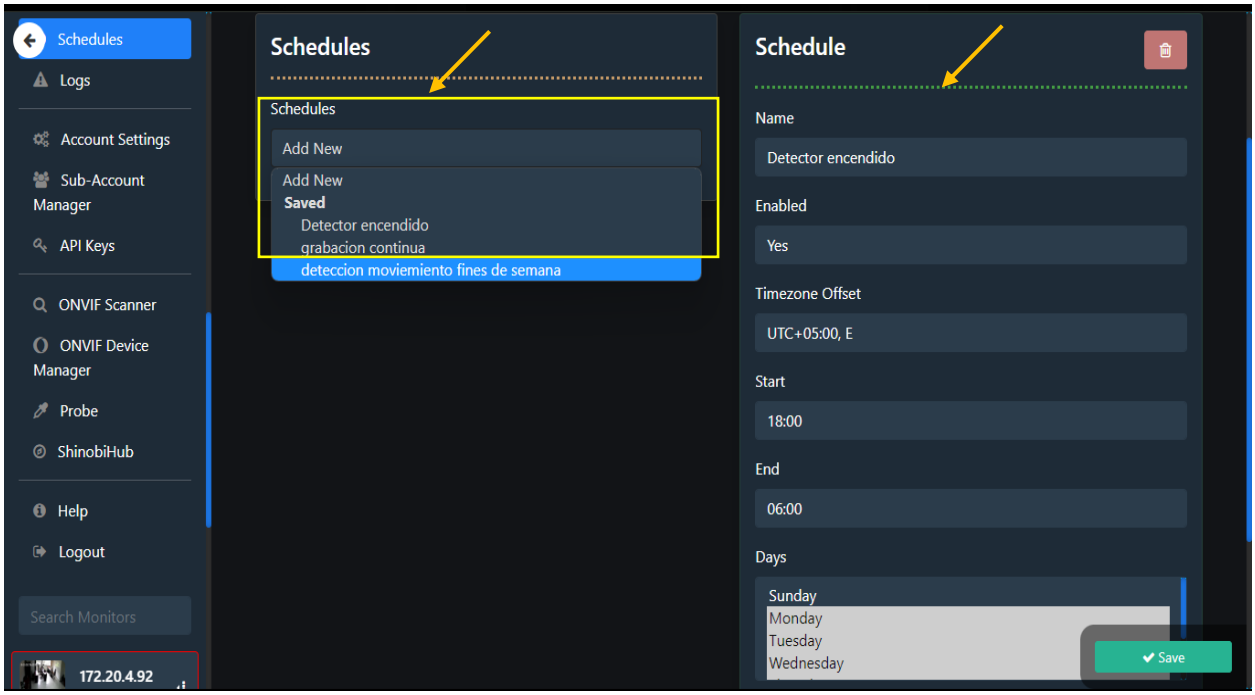


Figura 131: Programación de estados en eventos

En la configuración de cuenta podemos anexar algún tipo de notificación por medio de API

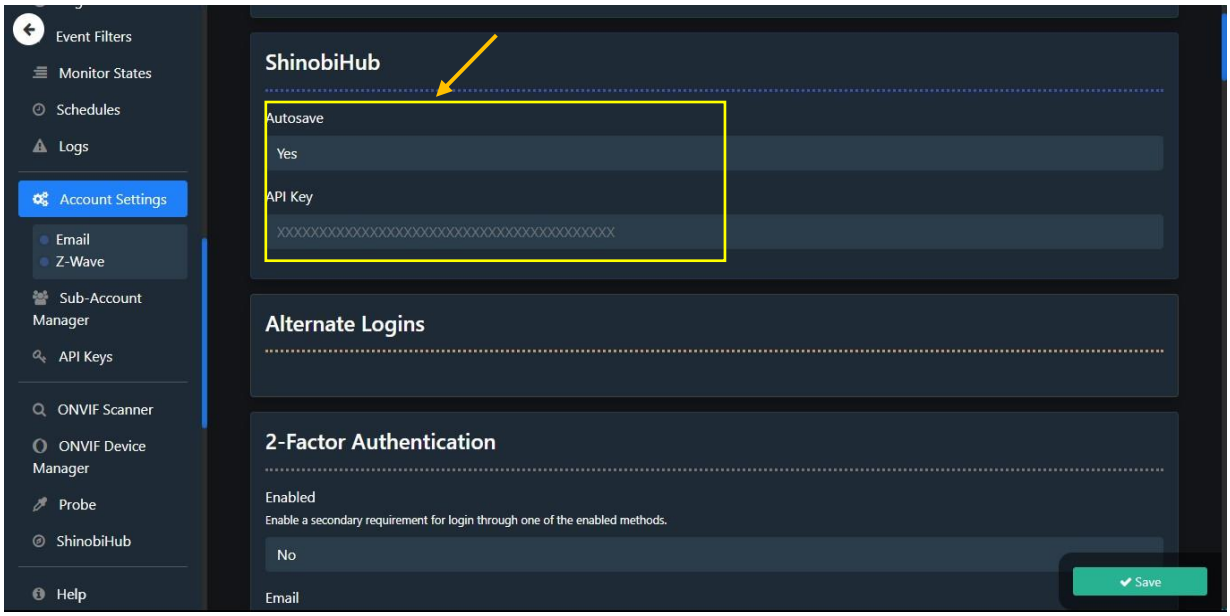


Figura 132: Configuración de cuenta

El escáner ONVIF nos ayuda a ingresar las cámaras al sistema solo con la IP y las credenciales de la cámara

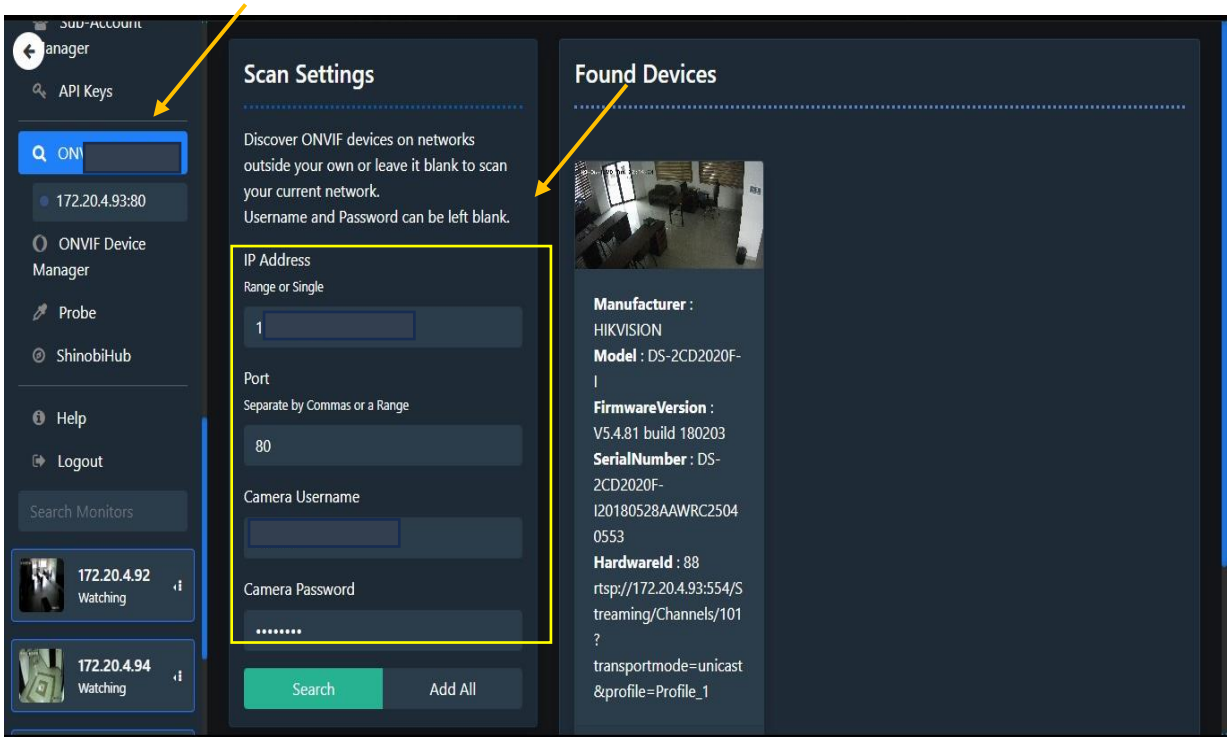


Figura 133: Ingreso de cámaras

Ingreso de cámara de forma manual usando los datos resto de las cámaras

Figura 134: Administración de cámaras en red

Configuraciones preestablecidas de cámaras que se encuentran en la base de datos de Shinobi

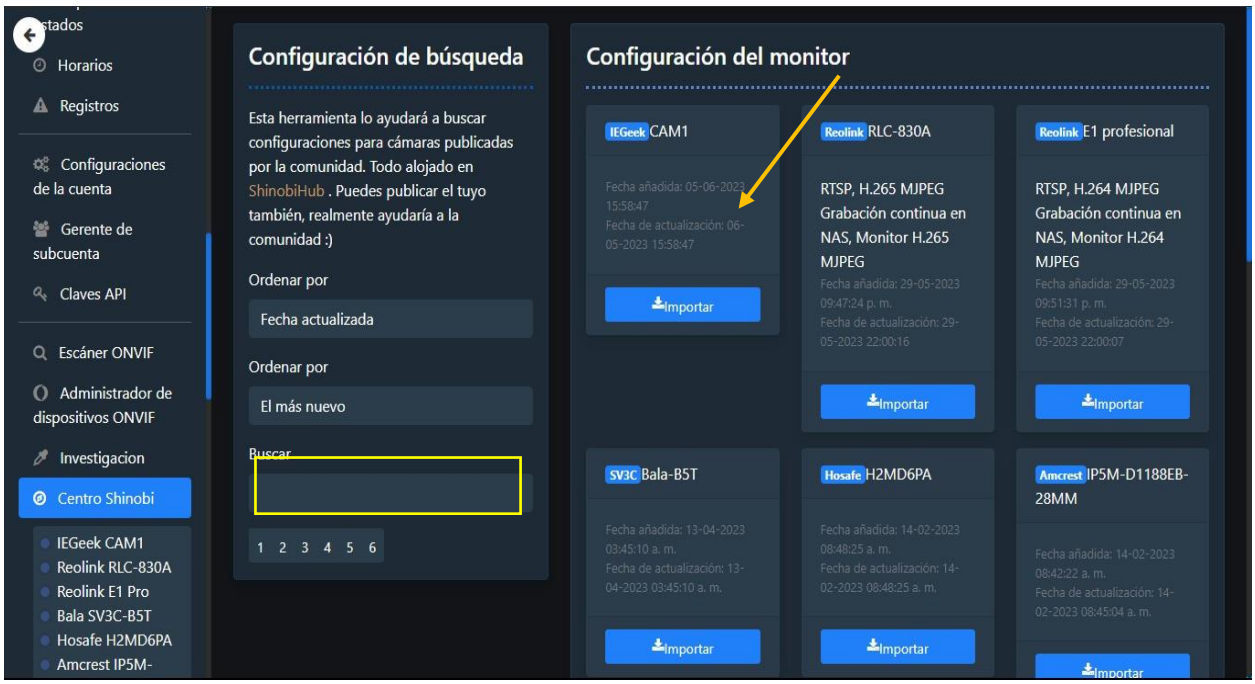


Figura 135: Configuraciones predeterminadas de cámaras

Dirección de almacenamiento de forma local

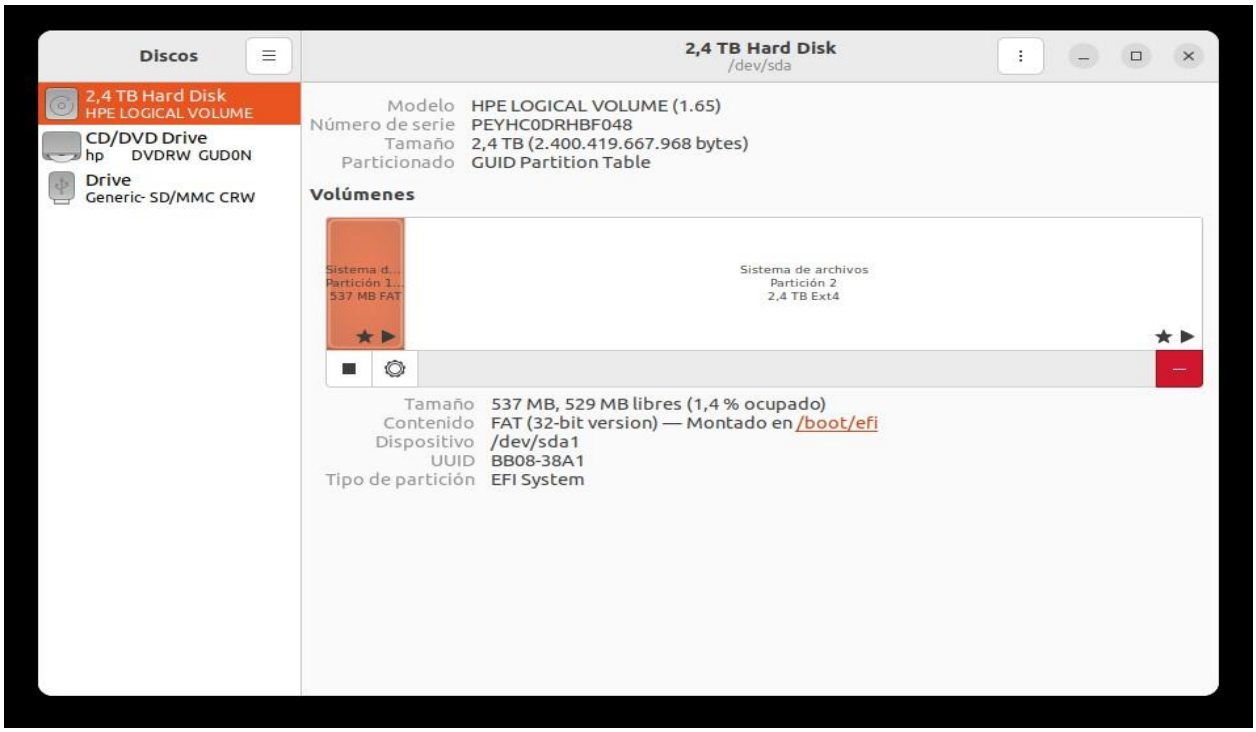


Figura 136: Capacidad de almacenamiento

Carpetas contenedoras del sistema y almacenamiento de videos

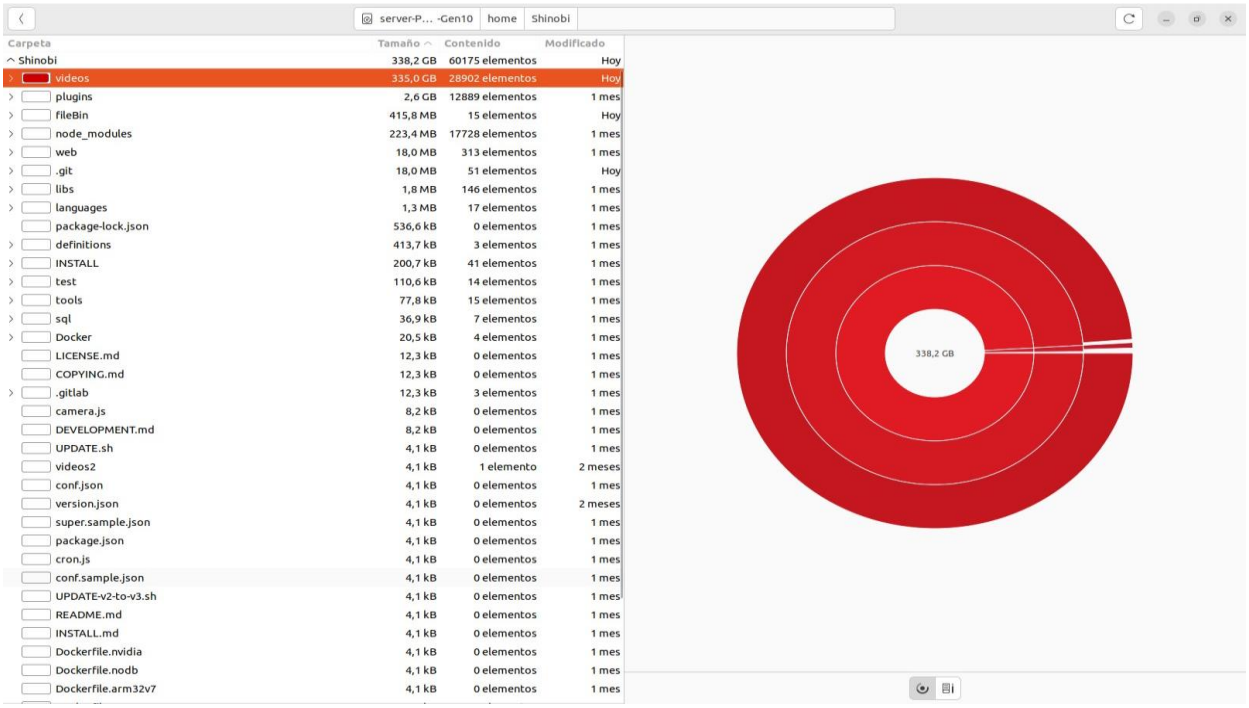


***Figura 137*:** capacidad de almacenamiento

Carpeta contenedora con los videos de las cámaras

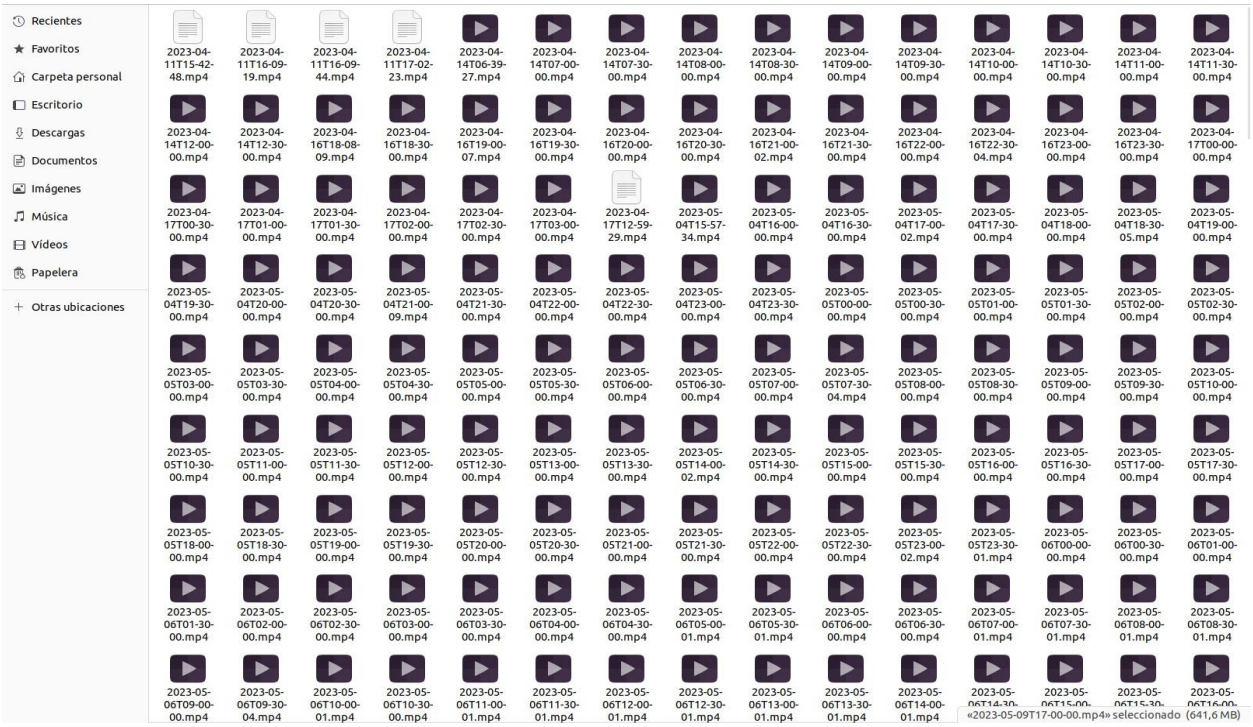


Figura 138: Carpeta Raíz del sistema

Anexo 8: Fotografías

Figura 139. Instalación de cámaras en aulas

Figura 140: Instalación de cámaras en aula de profesores