UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI

FACULTAD DE INDUSTRIAS AGROPECUARIAS Y CIENCIAS AMBIENTALES

CARRERA DE COMPUTACIÓN

PLAN DE INVESTIGACIÓN

Tema: "Herramientas de monitoreo de datos para infraestructura tecnológica"

Trabajo de titulación previa la obtención del
título de Ingeniero en Ciencias de la Computación

AUTORES: Guerrón Tapia Brayan David
Guevara Castillo Jhonatan Paúl

TUTOR: MSC. Milton del Hierro Mosquera

Tulcán, 2022

CERTIFICADO JURADO EXAMINADOR

Certifico que el estudiante Guerrón Tapia Brayan David con el número de cédula 0402082986 ha elaborado el trabajo de titulación: "Herramientas de monitoreo de datos para infraestructura tecnológica"

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.....

Del Hierro Mosquera Milton Gabriel, MSc.

TUTOR

Tulcán, septiembre de 2022

CERTIFICADO JURADO EXAMINADOR

Certifico que el estudiante Guevara Castillo Jhonatan Paúl con el número de cédula 0402127344 ha elaborado el trabajo de titulación: "Herramientas de monitoreo de datos para infraestructura tecnológica"

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......

Del Hierro Mosquera Milton Gabriel, MSc.

TUTOR

Tulcán, septiembre de 2022

AUTORÍA DE TRABAJO

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

Nosotros, Guerrón Tapia Brayan David con cédula de identidad número 0402082986 y Guevara Castillo Jhonatan Paúl con cédula de identidad número 0402127344 declaramos: que la investigación es absolutamente original, auténtica, personal y los resultados y conclusiones a los que hemos llegado son de nuestra absoluta responsabilidad.

f.....
Guerrón Tapia Brayan David
AUTOR

f.....
Guevara Castillo Jhonatan Paúl
AUTOR

Tulcán, septiembre de 2022

ACTA DE CESIÓN DE DERECHOS DEL TRABAJO DE TITULACIÓN

Nosotros, Guerrón Tapia Brayan David y Guevara Castillo Jhonatan Paúl declaramos ser autores de los criterios emitidos en el trabajo de investigación "Herramientas de monitoreo de datos para infraestructura tecnológica" y eximimos expresamente a la Universidad Politécnica Estatal del Carchi y a sus representantes legales de posibles reclamos o acciones legales.

f.....
Guerrón Tapia Brayan David
AUTOR

f.....
Guevara Castillo Jhonatan Paúl
AUTOR

Tulcán, septiembre de 2022

AGRADECIMIENTO

Damos gracias a Dios por permitirnos culminar una etapa más de nuestra vida profesional, por darnos la vida y seguir luchando cada día, por no abandonarnos en los momentos más difíciles y conocer gente maravillosa quien aporta un granito de arena a nuestro desarrollo personal.

Agradecemos a nuestros padres que en todo momento han sido un pilar fundamental en nuestras vidas, que con un amor incondicional y su arduo trabajo lograron sacarnos adelante, pese a las dificultades de la vida siempre estuvieron apoyándonos para que seamos profesionales. El apoyo de nuestros abuelitos y tíos que son una fuente de inspiración para cada día seguir luchando por nuestras metas, a nuestros hermanos que siempre nos dieron palabras de ánimo.

Al servicio Integrado de Seguridad ECU 911 por abrir la puerta de su institución para la realización de nuestro proyecto, un agradecimiento especial al área de Tecnología por su colaboración, predisposición y amabilidad.

Agradecemos infinitamente a la Universidad Politécnica Estatal del Carchi por ser el alma mater de nuestro desarrollo profesional, la cual nos brindó excelentes servicios académicos e institucionales, a sus docentes por permitirnos aprender de sus valiosos conocimientos que serán parte de nuestra vida.

A la Carrera de Computación que ha sido testigo de nuestra formación integral como profesionales y personas, a sus catedráticos y directivos que nos brindaron todo el apoyo necesario para la culminación para la obtención del título de ingeniería.

A nuestro tutor el MSc. Milton del Hierro por su dedicación y paciencia nos brindo su mano para finalizar con el trabajo de Titulación, además de compartirnos sus conocimientos para encaminarnos al buen desarrollo de nuestro proyecto de investigación.

A todos muchas gracias.

DEDICATORIA

El presente trabajo de titulación se lo dedico a Dios por guiar mi vida desde el inicio de mi carrera hasta el fin, ayudándome a centrarme en lo bueno de la vida.
A mis padres Darwin Pantoja y Mónica Castillo quienes me dieron su amor incondicional e hicieron un increíble esfuerzo laboral por verme convertido en un profesional.
A mi Familia por su apoyo moral y amor absoluto desde el inicio hasta el final de mi carrera profesional.
A mis hermanos, tíos y amigos que siempre estuvieron apoyándome en mi desarrollo profesional.
A mis profesores por trasmitirme sus conocimientos día a día.
A Liceth Hernández que, con su amor, paciencia y apoyo, fue en mi vida estudiantil y personal una gran ayuda y motivación, para seguir adelante y no dejarme vencer por las adversidades que se me presentaban.

Jhonatan Guevara

Dedico este logro a Dios, que me ha bendecido para seguir adelante con mi vida y me ha dado fortaleza y sabiduría.

A mi padre por ser parte fundamental de mi vida que con su paciencia, consejos e infinito amor incondicional me ha motivado a conseguir los logros que siempre he anhelado, a mi hermano por acompañarme en mi vida y brindarme su apoyo.

A mi familia que me ha transmitido sus consejos y su apoyo en los momentos que se ha necesitado.

Contenido

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

ÍNDICE DE ANEXOS

RESUMEN

El presente trabajo de investigación titulado “Herramientas de monitoreo de datos para infraestructura tecnológica” se realizó en el Servicio Integrado de Seguridad ECU 911 de la ciudad de Tulcán. El objetivo principal fue el análisis e implementación de una herramienta de monitoreo de datos para verificar el estado de conexión de los dispositivos tecnológicos de videovigilancia IP que cuenta la institución y así saber cuándo presentan algún fallo o desconexión. Mediante la comparativa de las herramientas más relevantes de monitoreo de datos, se determinó que Pandora FMS ofrece las características en la resolución de requerimientos que fueron necesarios para la comprobación de conexión a los diferentes dispositivos conectados a la infraestructura de la red en un determinado periodo de tiempo, ya que este software de monitorización recoge los datos de cualquier sistema, genera alertas en base a esos datos y muestra gráficos, informes y mapas mediante el uso de protocolos TCP/IP (Protocolo de Control de Transmisión/ protocolo de internet), SNMP (Simple Network Management Protocol) , ICMP (Internet Control Message Protocol) y PING (Packet Internet Grouper); Al momento en que el software detecta que no existe comunicación en los dispositivos, emite una alerta mediante diferentes medios de comunicación ya sea por medio de correo electrónico o aplicaciones de dispositivos móviles. Para guiar la investigación se utilizó un enfoque mixto, y así se recolectó información verídica de la problemática y sobre los requerimientos que debe cumplir la herramienta de

monitoreo de datos, además se utilizaron 4 tipos de investigaciones que aportaron en la indagación entre ellos se encuentra la investigación exploratoria, descriptiva, aplicada y documental donde se aplicaron entrevistas y encuestas al área de tecnología, área operativa y al gerente, lo que permitió conocer las necesidades como se maneja la información, almacenamiento de datos, pasos a seguir cuando se daña un dispositivo.

Palabras Claves: redes, Monitoreo de datos, Pandora FMS.

ABSTRACT

This research titled "Data monitoring tools for technological infrastructure" was carried out in the Integrated Security Service ECU 911 in the town of Tulcán.

The main objective was the analysis and implementation of a data monitoring tool to verify the connection of technological devices such as IP video surveillance cameras that the institution has and then to know when they fail or are disconnected. Through the comparison of the most relevant data monitoring tools, it was determined that Pandora FMS offers the characteristics required to verify that the different devices are connected with the network infrastructure in a certain period of time. Furthermore, this monitoring software collects data from any system, generates alerts based on that data and displays graphs, reports and maps through the use of TCP/IP protocols (Transmission Control Protocol / Internet Protocol), SNMP (Simple Network Management Protocol), ICMP (Internet Control Message Protocol) and PING (Packet Internet Grouper). When the software detects that there is no communication in any of the infrastructure devices, it emits an alert through different means of communication, either by email or mobile device applications. To meet this objective, the CISCO network development methodology called TOP-DOWN was taken into account, which allowed determining an orderly and hierarchical network proposal. A mixed approach was used to guide the research. In the same way, true information was collected on the problem and the requirements that the data monitoring tool must meet. In addition, 4 types

of research were used that contributed to the investigation, such as exploratory, descriptive, applied and documentary research, which applied interviews and surveys in the areas of technology, operations, and management. This allowed knowing the needs about information management, data storage and steps to follow when a device is damaged.

Keywords: networks, data monitoring, Pandora FMS.

INTRODUCCIÓN

A medida que avanza el tiempo aparecen nuevas tecnologías que brindan al usuario un mejor control de su entorno, permitiendo obtener información más eficaz y eficientemente. Los servicios Integrados de Seguridad son instituciones que atienden emergencias y requerimientos de la ciudadanía mediante el uso de dispositivos tecnológicos a través de una infraestructura de red.

En Ecuador el ECU 911 es el servicio Integrado de Seguridad que opera los 365 días del año, las 24 horas del día, abarcando instituciones como la Policía Nacional, Fuerzas Armadas y Salud Pública para la resolución de emergencias presentadas por la ciudadanía mediante llamadas al número 911. Esta institución cuenta con varias formas de atender estas emergencias, una de ellas es la visualización de video a través de cámaras IP ubicadas en diferentes puntos estratégicos distribuidos en todo el Ecuador, sin embargo, cuando una cámara presenta desconexiones o sufre algún fallo, los funcionarios tecnológicos no se informan inmediatamente cuando sucede este hecho.

Por lo tanto, el estudio tiene como objetivo principal implementar una herramienta de monitoreo de datos para la infraestructura tecnológica que optimice el manejo de

información en el ECU 911 y trazar un marco teórico y metodológico que sirva como base para el desarrollo de la investigación. La importancia de esta investigación se fundamenta en la adquisición de conocimiento sobre fundamentos de red, procesos de visualización y gestión de sistemas de monitoreo de equipos electrónicos.

El enfoque mixto de investigación permitió analizar y dimensionar las variables de estudio sobre herramientas de monitoreo de datos e infraestructura tecnológica. Se estableció la modalidad de campo, descriptiva, documental y exploratoria para recolectar información sobre infraestructura tecnológica y sistemas de monitoreo de datos, por otra parte, mediante un censo se aplicó una encuesta a 4 funcionarios del área administrativa y tecnológica, con esto se cuantificó los indicadores y se determinó la viabilidad del proyecto.

La construcción de la propuesta está completamente enfocada al desarrollo del sistema y fue guiada por los modelos de la metodología en redes, telecomunicaciones y la información recolectada con los instrumentos de investigación, dando lugar a la implementación de la herramienta de monitoreo de datos, las tecnologías utilizadas se centran en el lenguaje de programación PHP5 y sistema operativo CentOS.

Adicionalmente, se pueden añadir varios resultados que tiene este problema como es el desconocimiento del tiempo que ha pasado una cámara desconectada, los puntos más frecuentes que suceden estos hechos, las gráficas del comportamiento de dispositivos, la falta de reportes para los dispositivos, entre otros. Esta información es de importancia para poder analizarla con el área tecnológica y poder realizar las respectivas correcciones o mantenimiento.

I. PROBLEMA

1.1. PLANTEAMIENTO DEL PROBLEMA

En Ecuador, los dispositivos tecnológicos que operan en el Servicio Integrado de Seguridad ECU 911 son de suma importancia para la resolución de los problemas presentados de la ciudadanía a las diferentes brigadas establecidas dentro de la institución, como lo es la Policía Nacional, el cuerpo de Bomberos, Salud pública y las Fuerzas Armadas, es por eso que al fallar las cámaras, servidores, computadores entre otros, no solo obstaculizan ejercer un mejor trabajo internamente también la ciudadanía se ve afectada al no poder ser atendida adecuadamente.

La infraestructura tecnológica es una de las fortalezas que permite atender en forma ininterrumpida las 24 horas del día y los 365 días del año, cualquier requerimiento (Coordinación General de Planificación y Gestión, 2014). No obstante, los cambios tecnológicos actuales hacen que el Sistema Integrado de Seguridad haga un limitado uso de las herramientas de monitoreo de datos que brinden información acerca del estado de los dispositivos conectados a la infraestructura tecnológica para así obtener reportes de las diferentes cámaras y servidores que operan dentro del centro operativo local.

Es evidente las quejas que presentan los afectados cuando una cámara falla debido a que en el momento en que existen hurtos, asaltos, robo de vehículos, entre otros actos vandálicos,

los dispositivos se encuentran situados en lugares estratégicos para evitar estos incidentes. Sin embargo, cuando se realiza los procedimientos pertinentes para obtener el video de videovigilancia para poder identificar al delincuente, se informa que la cámara presento fallos en su funcionalidad, ocasionando inconformidad a la ciudadanía (Argoti, 2022).

Por ejemplo, en Ambato, en el Sector La Joya se ha evidenciado un suceso negativo, donde un vehículo fue desvalijado mientras estaba parqueado fuera de su hogar, el afectado levantó la denuncia en la policía nacional y realizó los pasos respectivos para obtener el video de videovigilancia. Lamentablemente, le informaron que las cámaras de su sector no funcionan porque se encontraban en desconexión, esta respuesta indignó al usuario (El Comercio, 2019).

En Tulcán, la institución de seguridad ciudadana posee áreas y equipos que son críticos para la operatividad normal del centro. Por tanto, es sumamente importante conocer de manera pronta y centralizada el estado y alarmas de cada uno de los equipos. Los sistemas que funcionan en esta institución operan de manera descentralizada, es decir, la información no está gestionada de la mejor manera para la toma de decisiones por parte del área tecnológica y administrativa.

Según Argoti (2022) cuando una cámara se daña provoca una serie de problemas tanto para la institución como para la ciudadanía, por lado de la institución el equipo de tecnología no recibe alertas inmediatas de los dispositivos caídos, para obtener dicha información, se debe seguir una serie de pasos que son demorosos, por lo tanto, la reparación del dispositivo lleva tiempo.

El servicio integrado de seguridad ECU 911 Tulcán, en una entrevista realizada, menciona que no cuenta con una base de datos que le permita almacenar la información de las fechas en que una cámara se dañó o sufrió algún altercado, esto genera desconocimiento de información para el equipo de administración sobre los puntos más frecuentes en los que ocurre estos incidentes. El gerente no puede acceder a la información de dispositivos funcionando actualmente sin la intervención del equipo de tecnología.

1.2. FORMULACIÓN DEL PROBLEMA.

El escaso uso de sistemas de monitoreo genera una inadecuada gestión de los dispositivos tecnológicos en el Servicio Integrado de Seguridad Ecu 911 del Cantón Tulcán.

1.3. JUSTIFICACIÓN

La investigación se llevará a cabo para determinar una herramienta de monitoreo de datos para la infraestructura tecnológica del ECU 911 Tulcán, con la finalidad de optimizar el manejo de información, facilitando la toma de decisiones de los diferentes sistemas que forman parte de la infraestructura tecnológica. Es así como, contar con una herramienta que brinde información y alertas es de vital importancia tanto por el área administrativa como para el personal de tecnología encargado de los periféricos y cámaras ubicados en toda la provincia del Carchi

Mediante el estudio de una herramienta de monitoreo de datos de los diferentes sistemas del Centro Operativo Local, como lo es el de las cámaras y servidores, se pretende proponer una solución para la gestión de información haciendo uso de tecnologías de información y comunicación que permitan la toma de decisiones al área administrativa y tecnológica.

El ECU 911 tiene la necesidad de contar con tecnología de punta, procesos técnicos y procedimientos actualizados para realizar esfuerzos conjuntos bajo solo una línea de mando de las autoridades locales. Es por eso, que utilizar una herramienta de esas características es de vital importancia para el personal del área administrativa.

Así pues, los principales beneficiarios de este proyecto serán los funcionarios del área tecnológica, administrativa y operativa ya que al tener una herramienta que permita monitorear y conocer las alertas de los diferentes dispositivos tecnológicos que operan en el centro local es de gran importancia para su respectiva corrección y mantenimiento, para así tener disponibilidad de visualización de las cámaras y servidores para el beneficio de los ciudadanos de la provincia del Carchi.

El presente proyecto cuenta con la apertura de la institución de Servicio Integrado de Seguridad ECU 911, la cual nos facilitó la información acerca de los diferentes procesos de manejo de información y la infraestructura tecnológica que operan, con los datos proporcionados permitió comprender y trabajar en la herramienta de monitoreo de datos y en el documento de investigación. Cabe recalcar que para la construcción del proyecto se utilizaron recursos económicos propio, también equipos tecnológicos, los cuales permitieron su posterior ejecución.

1.4. OBJETIVOS Y PREGUNTAS DE INVESTIGACIÓN

1.4.1. Objetivo General

Implementar una herramienta de monitoreo de datos para la infraestructura tecnológica que optimice el manejo de información en el Servicio Integrado de Seguridad ECU 911.

1.4.2. Objetivos Específicos

- Recolectar información de distintas fuentes bibliográficas acerca de las herramientas de monitoreo de datos y su infraestructura tecnológica para la sustentación de la investigación realizada.
- Elaborar un marco metodológico para la investigación de herramientas de monitoreo de datos y su relación con el desarrollo de la investigación.
- Establecer una propuesta de red para los procesos de monitoreo y optimización de equipos tecnológicos en el Sistema Integrado de Seguridad Ecu 911.
- Implementar la herramienta de monitoreo de datos para la infraestructura tecnológica en el área de tecnología de esta institución.

1.4.3. Preguntas de Investigación

- ¿Cómo la fundamentación bibliográfica ayuda a profundizar el conocimiento de las herramientas de monitoreo de datos y la infraestructura tecnológica?
- ¿La elaboración del marco metodológico permitirá obtener información de los procesos administrativos para el desarrollo del Sistema de Monitoreo?
- ¿El uso de la metodología de red Top Down permitirá un adecuado planeamiento del desarrollo de la propuesta?
- ¿Cómo una solución informática ayudará en la gestión de información en la infraestructura tecnológica del Servicio Integrado de Seguridad ECU 911?

II. FUNDAMENTACIÓN TEÓRICA

2.1. ANTECEDENTES INVESTIGATIVOS

Existen varios proyectos, investigaciones y tesis de América Latina y Europa que se han ido desarrollando alrededor del tema propuesto, algunos de los más relevantes que se han escogido para fundamentarse en este tema son los siguientes.

En la tesis de (Once, 2017) presenta el tema de tesis previo a la obtención de título denominado "*Aplicación de monitoreo de los dispositivos de una red utilizando tecnología JAVA"*, en el cual tiene como propósito el desarrollo de una aplicación para el monitoreo del estado de los elementos de la red, así como emitir alertas que ayuden al monitoreo, esto mediante la utilización del protocolo SNMP y la utilización de librerías JMAPI.

El investigador plantea como solución el desarrollo de una aplicación usando el lenguaje JAVA y a la misma vez usando el protocolo SNMP, además se menciona que la herramienta está enfocada para la administración en el monitoreo de redes y a la misma vez facilitara de acciones efectivas en la toma de decisiones de un equipo.

La conclusión de este proyecto es que mediante el uso del protocolo SNMP se puede verificar el estado de la conexión de los equipos de la red, y que mediante su aplicación se puede mostrar alertas visuales que permiten determinar la disponibilidad de un equipo.

Resumiendo, el investigador plantea una solución informática para el monitoreo de dispositivos de una red, permitiendo informar cuantos dispositivos están conectados o activos a una misma red, logrando reducir los errores de conexión y ayudando a priorizar los trabajos de mantenimiento o reparación.

El presente texto de (Garcia y Roa, 2020) con su trabajo previo a la obtención de título de ingeniería denominado "*Diseño de una herramienta de monitoreo y control de servidores utilizando como eje principal Cacti. Aplicado a una PYME mediana"*, el cual tiene como objetivo principalmente el diseño de una herramienta de monitoreo y control de servidores en una institución empleando el aplicativo Cacti, además, basándose en objetivos secundarios como levantar requerimientos funcionales y no funcionales, y la propuesta de un modelo de gestión de incidentes. El investigador plantea la implementación de una herramienta Open Source que facilitara el monitoreo de hardware y software del datacenter, permitiendo detectar en la red problemas y notificando vía correo electrónico, SMS.

Los autores concluyen que Cacti es una herramienta Open Source que es capaz de monitorear diferentes dispositivos en este caso servidores de una manera eficaz y que es muy útil en cualquier empresa ya que siempre se tendrá información de los equipos en cuanto a tiempos de respuesta, CPU, memoria y consumo de red.

Para empezar (Quispe, 2018) con su trabajo previo a la obtención de título de ingeniería en sistemas denominado "*Implementación de un sistema de monitoreo y control de red, para un canal de televisión, basado en herramientas open source y software libre*", el cual tiene como objetivo principalmente implementar un sistema de monitoreo y control de red, basado en herramientas open source y software libre para un canal de televisión. Basándose en objetivos secundarios como monitorear equipos y servicios críticos y no críticos dentro de la infraestructura de red y toma de decisiones sobre las acciones de control y monitoreo de la red.

En la investigación en el desarrollo de la propuesta se utilizó herramientas de licencia gratis u open source como Nagios y CentOS 7, además mencionan que realizó un estudio de diseño cuasi experimental y de tipo descriptivo y también menciona que utiliza un muestreo probabilístico aleatorio y simple. El autor concluye que se llevó a cabo con plena satisfacción la implementación del sistema de monitoreo, al igual que se logró aumentar positivamente en el monitoreo de equipos y servicios críticos para los encargados de red del área de Soporte del canal Willax.

En resumen, menciona que la utilización de herramientas Open Source como lo es NAGIOS la cual le permite, monitorear de manera permanente los dispositivos que están conectados a la red y a la misma vez realizar reportes de fallas de los equipos conectados.

Según (Vargas, 2018) en su trabajo de titulación previo a la obtención de grado en Ingeniería Informática denominado "*Diseño e implementación de un sistema de visualización de datos de fuentes abiertas*", presenta como objetivo crear una plataforma completa de visualización de datos, partiendo desde la recogida de estos de fuentes de acceso público, su análisis, almacenamiento y el servicio de consulta por parte de los usuarios, siempre tomando en cuenta el requisito de permitir diferentes analizadores y fuentes de datos.

El investigador plantea en el desarrollo una arquitectura basada en los contenedores de Docker, ya que menciona que permite desplegar las aplicaciones directamente en un servidor además se detalla, que el contenedor debe alojar la aplicación y los datos se gestionan en volúmenes y a la misma vez se deben enlazar con el contenedor principal. El trabajo fue

realizado recolectando información importante para desarrollar una herramienta que permita la visualización de datos obtenidos de diferentes fuentes planteando cómo utilizar los datos recolectados.

En conclusión, el tema de investigación presenta nuevas herramientas de obtención de datos y nuevas herramientas por poder pasar a producción una aplicación y además da entender en qué momento es necesario utilizar la información recolectada o los datos de ciertas APIS.

En la Universidad Tecnológica de El Salvador, el trabajo de graduación presentado por los autores (Rivera y Aguilar, 2020) denominado "*Evaluación de diferentes herramientas utilizando software libre para el monitoreo de una red de datos a nivel empresarial"* el cual tiene como propósito evaluar diferentes herramientas para el monitoreo de una red empresarial utilizando software libre.

El trabajo está enfocado a comparar la herramienta de monitoreo de red adecuada para detectar posibles problemáticas antes que ocurra en colapso o caída de las redes dentro de la empresa investigada. Los autores concluyen que la implementación de un sistema de monitoreo para cualquier institución o empresas es fundamental ya que ayuda a prevenir fallos al igual de tener un control interno sobre los equipos de la empresa.

El autor (Moreira, 2019) en su informe de trabajo de titulación previo a la obtención de título de magíster en tecnologías de la información y comunicación en sistemas distribuidos propone como tema "Comparativa entre herramientas de monitoreo de red de computadoras aplicadas a la empresa Puerto Atún" el cual planteo como objetivo el comparar herramientas de monitoreo de red para el análisis de amenazas y componentes defectuosos de la empresa en la que investigó. El trabajo de investigación como una de sus conclusiones, realizó una comparativa de las diferentes herramientas de monitoreo de red de las cuales pudo seleccionar la que mejor característica y operatividad ofrece al usuario.

Para los autores (Morales y Moreno, 2020) desarrollan el tema de "*Sistema de aplicaciones móviles para el mejoramiento de la comunicación entre la comunidad y estación de bomberos del municipio de Sahagún"* teniendo como propósito diseñar y desarrollar un sistema de notificaciones para el cuerpo de bomberos y la comunidad de Sahagún.

Además, menciona que en la parte del desarrollo se tomó en cuenta llevar a cabo un sistema de control de alertas de control de incidencias, capturando los datos del GPS además se menciona que las alertas generadas, mandan directamente un aviso al cuerpo de bomberos y

aceptar la solicitud, además las herramientas de desarrollo del front-end fue Flutter y para la recepción de datos o el backend se utilizó Firebase.

Los autores concluyen que con la implementación de sistema de alertas tempranas o SAT desarrollados en el framework Flutter comunican de cualquier tipo de eventualidad o urgencia, además, menciona que con el desarrollo permitió mejorar la comunicación, entre la comunidad y las personas de primeros auxilios, para ello el uso de esta solución tecnológica en tiempo real y que emplea el geoposicionamiento.

Por último, el trabajo de investigación realizado por los autores (Amaya y Sarria, 2019) denominado *"Gestión de infraestructura tecnológicas en entidades públicas"* el cual tiene como objetivo general conocer el estado de la infraestructura tecnológica en instituciones educativas siguiendo un modelo técnico de diseño de TOP DOWN. En este trabajo se insta a desarrollar procesos de diseño e implementación de infraestructura tecnológica para entidades de gobierno.

Los autores concluyen que el modelo TOP DOWN es el mejor modelo para diseñar una infraestructura tecnológica, la cual permite abarcar desde las consideraciones más generales hasta las más detalladas.

2.2. MARCO TEÓRICO

A continuación, se van a exponer todos los apartados que se consideren importantes para el estudio de las herramientas de monitoreo de datos para infraestructura tecnológica

2.2.1. Datos

En computación, la palabra datos es toda información que tiene un atributo o una variable que recibe el computador por diferentes medios. Las computadoras simbolizan los datos, por ejemplo: texto, imágenes, sonido y video como valores binarios que son representados como 0 y 1 siendo la unidad más pequeña llamada 'bit'.

La palabra datos describe todo lo que un ordenador puede hacer. Al nivel de los elementos sobre los que se construyen las computadoras, los datos se representan como una secuencia de dígitos binarios. (Gonzales, 2019).

Es importante señalar que un dato no tiene sentido en sí mismo, se utiliza en la toma de decisiones o en la realización de cálculos a partir de un adecuado procesamiento, teniendo en cuenta su naturaleza y contexto.

2.2.1.1. Tipos de datos

Un tipo de dato es un atributo de los datos que indica al ordenador sobre la clase de datos que se va a trabajar, para así poder poner restricciones en que valores pueden tomar los datos y qué operaciones se puede realizar.

En informática, los datos son representaciones simbólicas (numéricas, alfabéticas, algorítmicas, etc.) de un determinado atributo o variable cualitativa o cuantitativa, o sea: la descripción codificada de un hecho empírico, un suceso, una entidad.

Los datos son, así, la información (valores o referentes) que recibe el computador a través de distintos medios, y que es manipulada mediante el procesamiento de los algoritmos de programación. Su contenido puede ser prácticamente cualquiera: estadísticas, números, descriptores, que por separado no tienen relevancia para los usuarios del sistema, pero que en conjunto pueden ser interpretados para obtener una información completa y específica.

Los tipos de datos más comunes utilizados en computación son:

Tabla 1. Tipos de Datos

Tipo	División	Dato	Tamaño	Características
Numérico	Real	Float Double	• 32 bits • 64 bits	Tipo de dato formado por una variable numérica que almacenan números muy grandes y cuentan con una parte decimal.
	Entero	Byte Short Int Long	• 8 bits • 16 bits • 32 bits • 64 bits	Tipo de dato formado por una variable numérica que no cuenta con parte decimal.
Texto	Carácter	Char	• 21 bits	Tipo de dato formado por una unidad o símbolo que puede ser una letra, un número, una mayúscula o un signo de puntuación.
	Cadena	Short	• 16 bits	Tipo de dato formado por un conjunto de caracteres dispuestos de forma consecutiva.
Lógico	Bolean	Boolean	• 8 bits	Tipo de dato que puede representar dos valores: verdadero o falso.

Fuente: Elaborado por Autores

2.2.2. Herramientas de monitoreo de datos

Las herramientas de monitoreo de datos son importantes para cualquier empresa o institución, ya que garantizan la integridad de la infraestructura de tecnologías de la información y comunicación.

2.2.2.1. Definición de herramientas de monitoreo

Según la RAE el término ‘monitorear’ significa la acción de observar mediante aparatos especiales el curso de uno o varios parámetros fisiológicos o de otra naturaleza para detectar posibles anomalías. Para la presente investigación se denominará al término monitorizar como el acto de observar el comportamiento de los componentes de la infraestructura tecnológica, siendo las herramientas de monitoreo, tecnologías que permiten conocer el estado del funcionamiento de un dispositivo o un conjunto de dispositivos a través de un monitor o una pantalla mediante un programa informático.

Las herramientas de monitoreo son sistemas de diagnóstico que se utilizan en telecomunicaciones, servidores o redes para encontrar componentes defectuosos, lentos o

que hayan sufrido alguna desconexión con el fin de notificar a los administradores mediante correo electrónico, SMS, etc. Estas herramientas de monitoreo están diseñadas a través de un conjunto de software y servicios para administrar y monitorear la infraestructura de TI de cualquier empresa que desee tener conocimiento del estado de los dispositivos tecnológicos. (GreenCore, 2015).

Así pues, el monitoreo de datos es el proceso en el cual un software informático tiene la capacidad de procesar, evaluar y revisar proactivamente los componentes dentro de una empresa o institución, lo cual ayuda al usuario a obtener datos mediante paneles, alertas e informes.

2.2.2.2. Gobernanza de datos

También es conocido como *"Data Goverance"* o gobierno de datos, es un término que está relacionado con monitoreo de datos, ya que es un proceso en el cual se garantiza que los datos cumplan con estándares cuando ingresan a un sistema.

La Data Governance es una gestión global de la disponibilidad, integridad, facilidad de uso, y seguridad de los datos de una empresa, el principio de utilizar esta gestión es para que las empresas puedan especificar quien es el responsable de los controles y decisiones de información, los mismos que deben estar almacenados respaldados y protegidos contra diferentes incidentes accidentales o humanos. (PowerData, 2019, p. 3).

Aplicar la data Governance es entre una de las mejores prácticas para el logro de objetivos en el que se encuentran, la mejora continua de la calidad de los datos, lograr un equilibrio entre las tecnologías de información y las funciones de negocio, organizar la gestión de datos para que sean operados de manera que sea equiparable a una 'fábrica de datos' entre otros beneficios que dependen de cada empresa. (PowerData, 2019).

Los principios de la gobernanza de datos son los siguientes:

Tabla 2. Principios de gobernanza de datos

Principio	Descripción
Integridad	Los datos ingresados al sistema deben ser exactos e íntegros para trabajar con seguridad en ellos.
Transparencia	Todo debe estar expuesto de manera accesible y expuesto de manera clara para todos los integrantes.

Audibilidad	Todos los procesos, decisiones y controles deben ir acompañados de la documentación correspondiente.
Responsabilidad	Se debe determinar responsables para cada proceso, control y toma de decisiones.
Gestión	Deben existir diferentes responsables en la gestión de datos que aporten al proceso.
Control y Balance	Se definirán responsables para introducir controles y balances entre el negocio y la tecnología.
Estandarización	Se dará soporte a la estandarización de datos de la empresa.
Gestión del cambió	Se crearán actividades para la gestión del cambio como valores de datos de referencia, datos maestros y metadatos.

Fuente: Elaboración de los autores

Es importante verificar que las herramientas de monitoreo de datos cumplan con el principio de gobernanza de datos ya que mediante ellas se puede garantizar que los datos sean de confianza, que estén bien documentados y que permitan trabajar adecuadamente en cualquier proyecto.

2.2.2.3. Niveles de monitorización

La monitorización de datos se puede dividir en dos grupos los cuales son:

Nivel interno

Este se centra en la atención a los servicios y aplicaciones de la infraestructura de la red, evaluando su adecuado funcionamiento

- **Monitorización por agente Software:** La organización de datos de las herramientas de monitorización de datos se realizan a través de una entidad llamada agente que pertenece a un grupo más genérico llamado grupo, esto permite que la información se ordene de manera lógica y jerárquica basada en grupos, agentes, grupos de módulos, y módulos los agentes software deben ser instalados en el sistema y solo puede acceder a la información contenida en él.

Nivel externo

Analiza y se centra en los diferentes servicios que están instalados, como por ejemplo el servicio de correo, impresión, base de datos, FTP entre otros, sin tener en cuenta los dispositivos y componentes que intervienen para su producción.

- **Monitorización Remota:** También conocida como RMM (Remote monitoring and management) A menudo se lo conoce como supervisión y gestión remotas; los servicios involucrados en este conjunto de características son los componentes básicos de la gestión de TI. Las capacidades de RMM pueden variar según el proveedor, pero los conceptos básicos siguen siendo los mismos: una herramienta remota para acceder a sus dispositivos, monitorear la disponibilidad y los umbrales definidos, la capacidad de analizar y recibir alertas para varias mediciones de dispositivos, al mismo tiempo que puede administrar los dispositivos y garantizar que permanezca actualizado y funcional para su usuario final.

Se dice que una herramienta de monitoreo tiene un buen servicio cuando es capaz de combinar ambos niveles, con el fin de poder integrar la calidad de los servicios, como el monitoreo de la infraestructura y sus componentes (Fábregas, 2018, p. 117)

2.2.2.4. Tipos de Monitoreo

Los recursos de hardware son fundamentales para el rendimiento del servidor y los problemas de hardware se pueden evitar antes de que afecten a sitios web. Monitorear dispositivos electrónicos nos permite rastrear los recursos de servidores web o dispositivos conectados a Internet, además de dispositivos como cámaras IP.

El monitoreo de recursos permite correlacionar los resultados para un análisis en profundidad. Por ejemplo, al monitorear los recursos del servidor, puede asociar la recepción de cámaras de red para generar una respuesta en el servidor local. (Dotcom, 2020).

- **Monitorización Pasiva**

La monitorización pasiva nos permite dos funciones clave de operación, por un lado, el análisis de eventos posteriores: al construir un perfil histórico de flujos de tráfico y señalización, se puede realizar un análisis para buscar tráfico anómalo, como ataques distribuidos de denegación de servicio, o señalización inusual o indicativa, como el exceso de llamadas o la alta actividad de retransmisión.

La monitorización pasiva es ideal para construir una comprensión detallada de los patrones de uso, planear las actualizaciones de la red y del sistema para adaptarse al crecimiento de la demanda e identificar oportunidades para nuevos servicios (Ferri, 2019

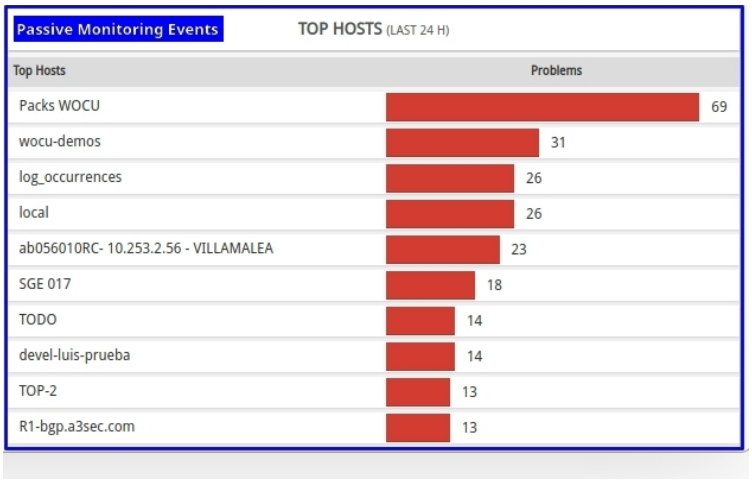


Figura 1. Monitorización Pasiva
Fuente: Tipos de monitoreo según Alba Ferrari 2018

- **Monitorización Activa**

Las monitorizaciones activas se pueden utilizar para "sondear" un dispositivo o servicio, obteniendo información sobre el estado de este cada cierto tiempo. La monitorización activa se debe emplear para proporcionar visibilidad del rendimiento de nivel de servicio (SLA) que utilizado de esta manera nos advierte de forma temprana de una posible degradación del rendimiento, incluso antes de que el cliente lo notifique, aumentado la proactividad de nuestros equipos operativos (Ferri, 2019).

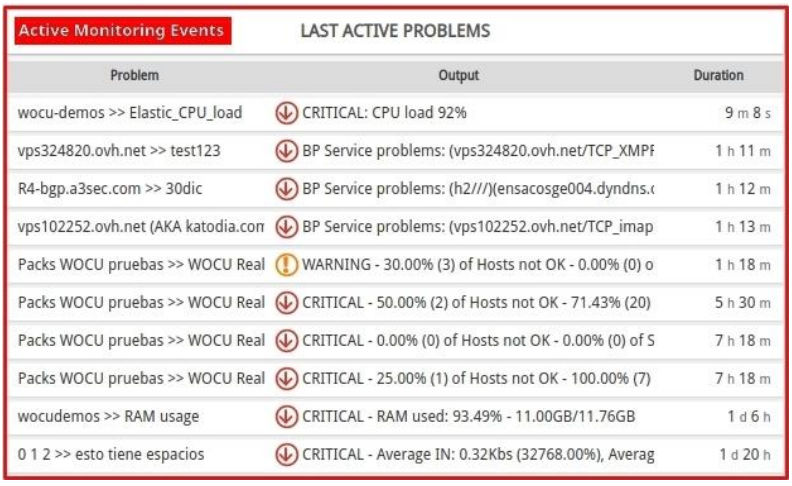


Figura 2. Monitorización Activa
Fuente: Tipos de monitoreo según Alba Ferrari 2018

- **Monitorización ICMP**

El ICMP o conocido por el Protocolo de control de mensajes de internet, es parte del conjunto de protocolos IP siendo utilizado como medio para enviar mensajes de error e información operativa. Este tipo de monitoreos se usa cuando un host no puede ser alcanzado, cuando los tiempos de respuesta expiran, cuando un servicio no está disponible, entre otros. Es decir, se maneja por mensajes de error y control necesarios para que el sistema original evite o corrija el problema detectado (CISCO,2013).

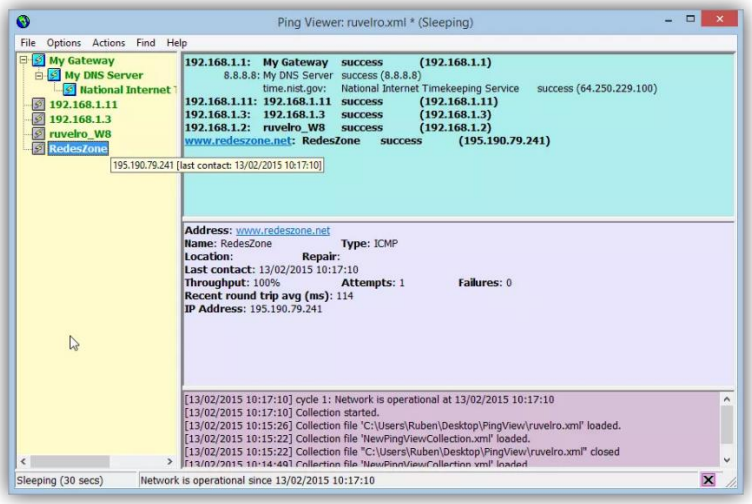


Figura 3. Monitorización ICMP
Fuente: Monitorización de equipos con Ping según José Antonio 2021

- **Monitorización TCP**

TCP o Protocolo de control de transmisión muchas veces es utilizado para aplicaciones que necesitan que la comunicación a través de la red sea confiable, debido a que el protocolo TCP confía en que los datos que emite el cliente al servidor sean recibidos sin errores respetando el orden en que fueron enviados, en el monitoreo de datos las comprobaciones TCP comprueban si el puerto de destino está abierto o no enviando como por ejemplo una cadena de texto y esperar a que sea recibido.

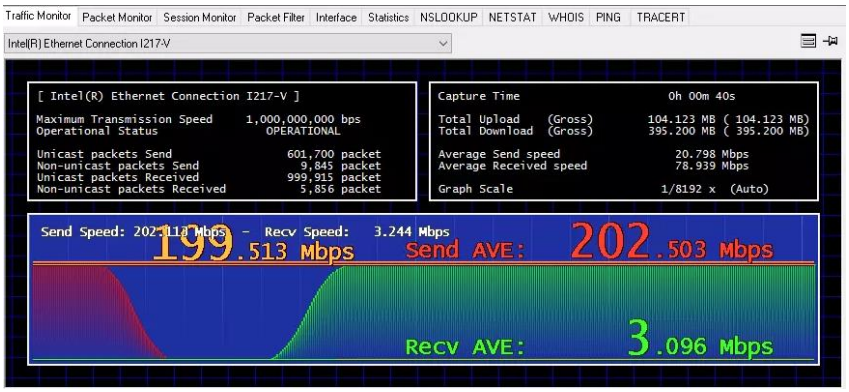


Figura 4. Monitorización TCP
Fuente: TCP Monitor Plus según Rubén Velazco 2017

- **Monitorización SNMP**

Protocolo simple de administración de Red o SNMP es un protocolo que trabaja en la capa de aplicación en la cual facilita la comunicación entre varios dispositivos de red, en los que se encuentran, routers, stwiches y todos los dispositivos de red en la infraestructura tecnológica.

El funcionamiento del monitoreo SNMP se utiliza en servicios no orientados a la conexión y permiten enviar un grupo de mensajes entre los administradores y los agentes, utilizar este tipo de protocolo establece que las tareas de administración no afectaran al rendimiento del sistema porque se evita utilizar mecanismos de control y recuperación como TCP.

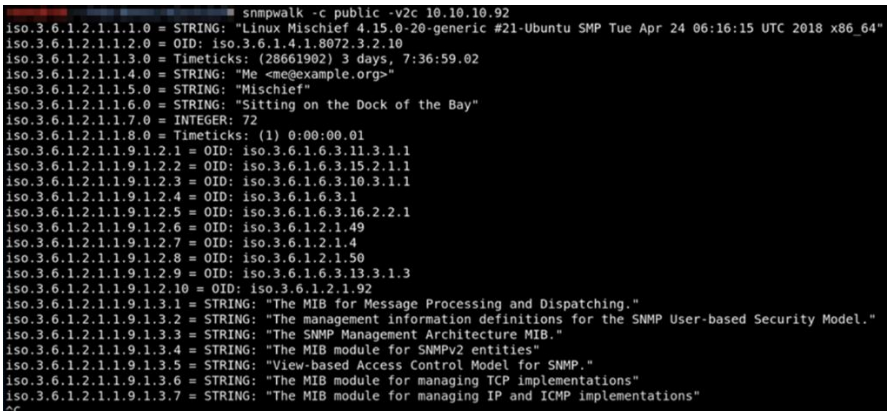


Figura 5. Monitorización SNMP
Fuente: TCP Monitor Plus según Rubén Velazco 2017

- **Monitorización por estados**

La monitorización por estados permite que el usuario establezca umbrales para definir cualquier dato en tres o más posibles estados, generalmente son, NORMAL, WARNING, CRITICAL, se utiliza generalmente para monitorear y fuentes de energía, baterías y

generadores. Consiste en el proceso de recopilar, analizar y señalar las ocurrencias de eventos a los administradores en procesos del sistema operativo, reglas de base de datos, entre otros, utilizando tanto hardware como software.

2.2.2.6. Características de herramientas de monitoreo

Las herramientas de software para el monitoreo de la red pueden reducir las interrupciones de la red y permitir que las empresas o instituciones operen de manera más fluida, reduciendo costos y evitando pérdidas financieras. Para aquellas organizaciones pequeñas que no tienen un presupuesto de software de monitoreo de red, la mejor opción es comenzar con software gratuito y software de monitoreo de red de código abierto, lo que puede reducir el tiempo y el dinero gastado en administración y gestión. (Opmanager, 2020).

Las diferentes disciplinas de administración de servicios requieren herramientas que mediante diversos grados de sofisticación faciliten su proceso. Es así como las herramientas de monitoreo y control deben ser robustas y tener amplio alcance para satisfacer los requerimientos de la empresa, algunas de las características que deben tener estas herramientas son:

Tabla 3. Características de las herramientas de monitoreo de datos

Características	**Descripción**
Alta disponibilidad	Deben operar bajo ambientes de alta disponibilidad como clústers.
Arquitectura compatible	Las herramientas de monitoreo deben ser compatibles con la infraestructura instalada.
Adaptabilidad	Las herramientas de monitoreo deben operar en redes donde se combinan diferentes topologías
Agilidad de notificaciones	Se debe notificar a los técnicos responsables cuando los servicios presenten algún inconveniente de la forma más rápida posible.
Presentación gráfica	La interfaz gráfica debe ser simple y mostrando cualquier anomalía detectada.
Autodescubrimiento	Deben tener la capacidad de identificar los cambios que se hagan a la infraestructura.
De bajo impacto	Las herramientas de monitoreo deben ser agentes de supervisión livianos, causando el impacto más mínimo a la infraestructura.

Escalabilidad	Las herramientas de monitoreo deben tener la capacidad de crecer a medida que crece la cantidad de objetos manejados.
Interoperabilidad	Las herramientas de monitoreo deben integrarse con otras herramientas de administración de servicios.
Base de datos	Deben almacenar los datos del funcionamiento de la infraestructura.
Seguridad	Las herramientas de monitoreo deben cumplir con los requerimientos de seguridad necesarios.

Fuente: Elaboración de los autores

2.2.2.7. Herramienta de monitoreo Pandora FMS

Pandora FMS (Flexible Monitoring System) es un software de monitorización de elementos de cualquier sistema e infraestructura de red, permitiendo conocer el estado de cualquier hardware o software, siendo capaz de detectar cuando una interfaz de red se ha caído, es una herramienta que está diseñada para ofrecer características modulares, multiplataforma, y de fácil personalización que se puede adaptar en diferentes entornos de hardware o software contando con un sistema de informes configurables que monitorizara el cumplimiento de los sistemas alertando a los usuarios compartiendo la información presentada. (Pandora FMS, 2020)

Es un software de código abierto para monitorear y medir varios elementos. Monitorear sistemas, aplicaciones o dispositivos de red. Debido a que tiene un registro histórico de datos y eventos, puede comprender el estado de cada elemento del sistema a lo largo del tiempo. Pandora FMS está orientado a entornos de gran escala y puede gestionar miles de sistemas con o sin agentes, por lo que se puede utilizar en grandes clústeres, centros de datos y diversas redes. (Capterra, 2020).

Las características que nos brinda Pandora FMS son muy amplias y dependiendo de qué versión o cuáles son los requisitos que necesiten las empresas o instituciones, puede haber más o menos características, pero entre las más destacables son:

Tabla 4. Características de las herramientas de monitoreo de datos

Características	**Descripción**
Mesurable	Puede medir y cuantificar el estado (bien, mal o valores intermedios) y almacenarlos en un valor numérico o alfabético.

Versátil	Pandora FMS puede monitorizar software: Sistemas operativos, servidores, aplicaciones. y hardware: cortafuegos, proxies, bases de datos, VPN, routers, switches entre otros.
Base de datos	Tiene una base de datos que puede generar informes, estadísticas, niveles de adecuación de servicio (SLA) e informes personalizados.
Presentación gráfica	Ofrece una interfaz gráfica que simplifica las operaciones mediante una interfaz web.
Seguridad	Ofrece servicios de niveles de control de acceso basados en roles.
Monitorización por protocolos	Se puede hacer uso de los protocolos SNMP y pruebas de red (TCP/IP), ICMP, IPv4/6 para monitorizar cualquier dispositivo de red.

Fuente: Elaboración de los autores

Arquitectura de Pandora FMS

El software Pandora FMS es extremadamente modular a su vez sencilla y monolítica, la parte vital de Pandora es la base de datos donde se almacena toda la información como podemos observar en la imagen, la base de datos utilizada es MySQL, además consta de diversos elementos como el procesamiento de datos como los Servidores, la consola que permite la visualización de los datos de la base de datos y a su misma vez la interacción con el usuario (PANDORA FMS, 2022).

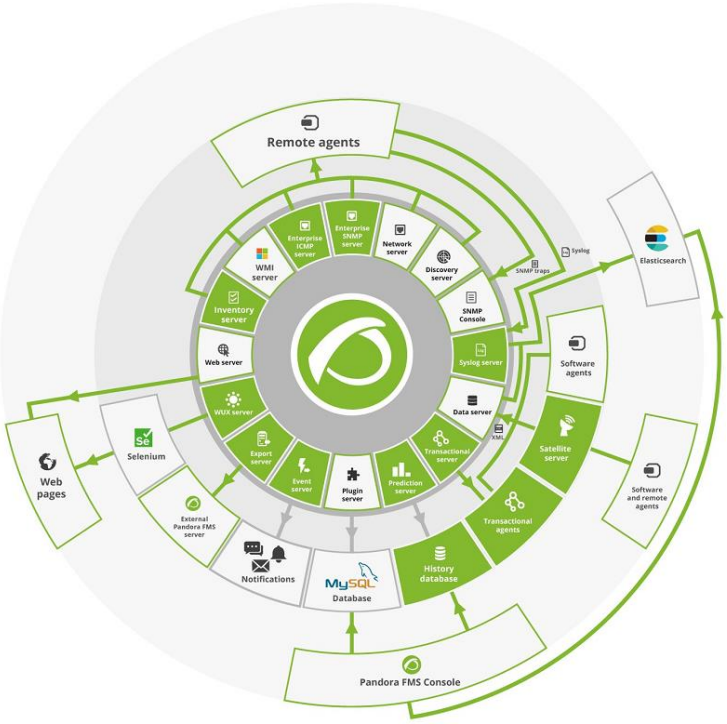


Figura 2. Arquitectura de Pandora FMS
Fuente. PANDORA FMS (2022)**,** Arquitectura Pandora FMS.

El componente más vital y donde se almacena todo es la base de datos (actualmente solo se soporta en sistemas producción MySQL, pero PostgreSQL y Oracle están soportados también).
Todos los componentes de Pandora FMS se pueden replicar y funcionar en un entorno de HA puro (Activo/Pasivo) o en un entorno clusterizado (Activo/Activo con balanceo de carga).

También se describen métodos de disponer de un backend SQL en alta disponibilidad. Pandora FMS consta de diversos elementos, entre ellos, los que se encargan de recolectar y procesar los datos son los servidores. Los servidores, a su vez, introducen los datos recolectados y procesados en la base de datos. La consola es la parte encargada de mostrar los datos presentes en la base de datos y de interactuar con el usuario final. Los Agentes Software son aplicaciones que corren en los sistemas monitorizados (servidores generalmente), y recolectan la información para enviársela a los servidores de Pandora FMS.

- **Partes fundamentales Pandora FMS**

Agentes Pandora FMS

El Agente de Pandora FMS es simplemente un elemento organizativo creado en la Consola web de Pandora FMS y que está asociado a un grupo de Módulos (o elementos individuales de monitorización). Además, este agente puede tener (opcionalmente) asociadas una o más direcciones IP.
Un agente de software se ejecuta en el sistema operativo que recopila información como por ejemplo la carga de CPU, memoria libre o espacio en disco, cualquiera que sea la verificación para ejecutar en el sistema, corresponde al módulo. Por lo tanto, se recopilan datos separados para cada módulo en cada ejecución.
Los Agentes Software se instalan en los equipos que desean monitorizarse localmente, extrayendo la información desde el propio equipo. Se utilizan principalmente en servidores para monitorización de recursos de la máquina (CPU, RAM, discos) y aplicaciones instaladas (MySQL, Apache, JBoss). Generalmente, la monitorización de servidores y

equipos se llevará a cabo con Agentes Software mientras que la monitorización de equipos de red se hará de forma remota sin la instalación de ningún software.

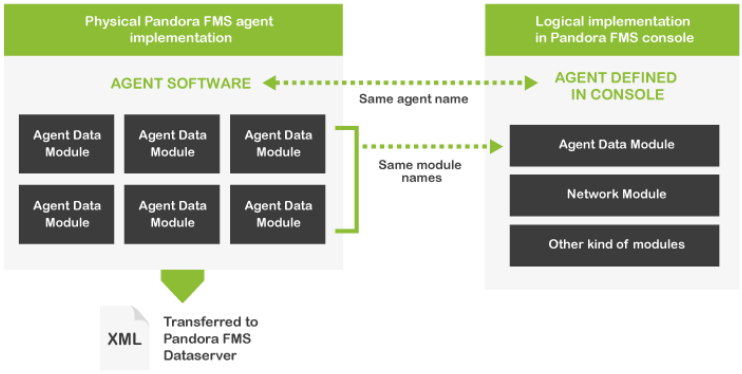


Figura 3. Arquitectura de un agente software en Pandora FMS

La palabra agente en Pandora FMS implica dos importantes y diferentes conceptos:

- El agente como unidad organizativa y contenedora de información.
- El agente software, que consiste en un proceso software que mantiene ejecutándose el agente de Pandora FMS en un equipo.
- Elemento organizativo en la consola de Pandora FMS.
- Lleva asociado un grupo de módulos.

Estructura de Agente Software

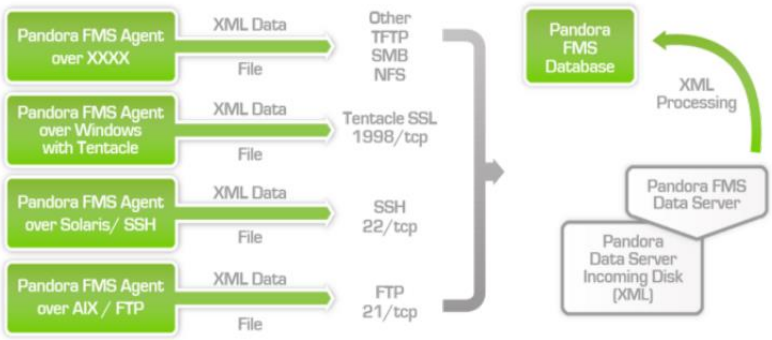


Figura 4. Estructura de un agente software
Fuente: Pandora FMS (2021).

Cuando hablamos de los agentes de software, nos referimos al software remoto que se está ejecutando en el sistema donde recoge la información. No son lo mismo que el concepto de Agente como unidad contenedora. Organizan la información recogida en módulos. Un módulo para cada dato. Los módulos pueden ser de diferentes tipos (numéricos, incrementales, texto, imagen, entre otros). El agente ejecuta cada módulo, produciendo el

XML final, y lo envía al servidor a través de la red. Hay agentes para todos los sistemas operativos del mercado.

Esquema lógico de un agente

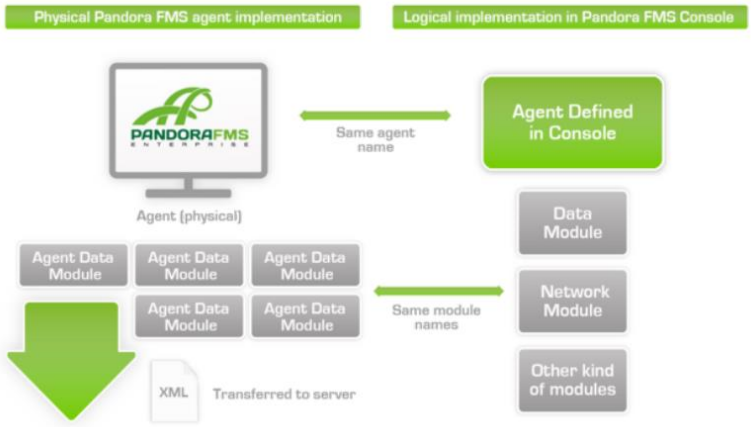


Figura 5. Esquema lógico de un agente software
Fuente: Arquitectura Pandora FMS Documentación 2021

Cada agente recolecta varias (porciones) de información. Esta se organiza en un único paquete y se almacena en un solo fichero que llamaremos paquete de datos.

El proceso de copia del paquete de datos del agente al servidor se realiza de forma regular (Síncrona), es decir, cada cierto tiempo definido en el agente, que se puede modificar para no llenar la base de datos con información superflua o para no cargar la red ni resultar perjudicial para el rendimiento del sistema.

El intervalo predeterminado es de 300 (segundos), lo que equivale a cinco minutos. Valores menores de 100 (segundos) no se recomiendan ya que puede afectar al rendimiento del sistema anfitrión, además de cargar excesivamente la base de datos y el sistema de proceso central.

Módulos Pandora FMS

Este fichero de datos es una estructura XML y su nombre se forma mediante la combinación del nombre del anfitrión u host donde está el agente, un número de serie diferente para cada paquete de datos y la extensión .data que indica que es un paquete de datos.

Figura 6. Estructura de los módulos XML de Pandora FMS
Fuente: Arquitectura Pandora FMS Documentación 2021

El fichero de datos XML que genera el agente es el corazón de Pandora FMS. En él se contiene un paquete de datos con la información recogida por el Agente. Este paquete de datos tiene un diseño compacto, flexible y ligero que permite que cualquier usuario pueda utilizar los agentes de Pandora FMS o sus propios desarrollos para generar información y que esta sea procesada en Pandora FMS.

Sistema de Alertas Pandora FMS

Una alerta es la reacción de Pandora FMS a un valor incorrecto de un Módulo. Dicha reacción es configurable y puede consistir en cualquier cosa que pueda ser desencadenada por un script configurado en el Sistema Operativo donde corre el servidor de Pandora FMS que procesa el Módulo.

En Pandora FMS, las alertas funcionan mediante la definición de unas condiciones de disparado, unas acciones elegidas para esa alerta, y finalmente la ejecución de unos comandos en el servidor de Pandora FMS, que se encargarán de llevar a cabo las acciones configuradas.

El sistema general de alertas asocia una única alerta por cada Módulo y está alerta a su vez puede llevar a cabo una o varias acciones.

Existen varios tipos de alertas:

- Alertas simples.
- Alertas sobre eventos.
- Alertas sobre traps SNMP.

Estructura Sistema de Alertas Pandora FMS

Figura 7. Estructura de una alerta en Pandora FMS
Fuente: Arquitectura Pandora FMS Documentación 2021

Las alertas se componen de:

- **Comandos:** Especifican qué se hará; será la ejecución que realizará el servidor de Pandora FMS al disparar la alerta. Puede ser escribir en un log, enviar un mensaje de correo electrónico o un mensaje de texto (SMS), ejecutar un script, etc.
- **Acciones:** Especifican cómo se hará, son las personalizaciones de los argumentos del comando, permiten personalizar la ejecución como tal, pasando al comando parámetros particulares como nombre del Módulo, Agente, etc.
- **Plantillas:** Especifican cuándo se hará, definen las condiciones para disparar la acción o acciones. Por ejemplo: cuando el Módulo pase a estado crítico.

Base de datos Pandora FMS

Pandora FMS utiliza una base de datos MySQL. Pandora FMS mantiene una base de datos asíncrona con todos los datos recibidos, realizando una cohesión temporal de todo lo que recibe y normalizando todos los datos de las diversas fuentes origen. Cada módulo de datos de cada agente genera una entrada de datos para cada paquete, lo que supone que un sistema real de producción puede tener del orden de diez millones de (datos), o átomos de información.

Estructura de la Base de datos

- Diseño no lineal. Con agrupación de la información en tiempo real (valores que permanecen iguales).

- Permite mayor capacidad de almacenamiento.
- No almacena información “real”, debido al intervalo de ejecución del agente, salvo los tipos de datos asíncronos.

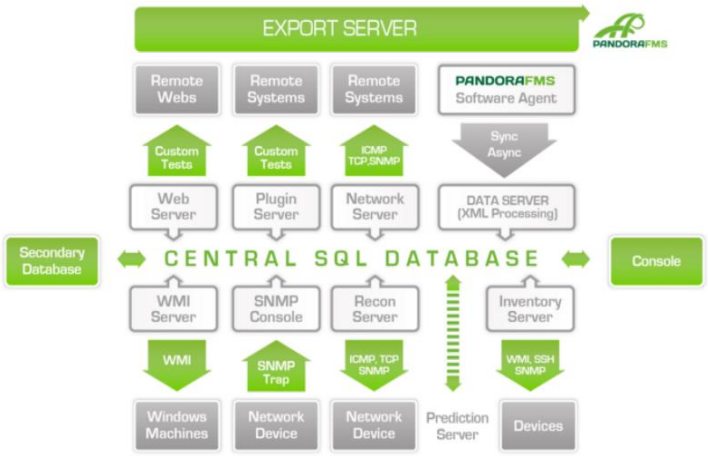


Figura 8. Central de datos en Pandora FMS
Fuente: Ingeniería De Pandora Fms 2021

Estos datos se gestionan automáticamente desde Pandora FMS, llevando a cabo un mantenimiento periódico y automático de la base de datos, esto permite que Pandora FMS no requiera ningún tipo de administración de base de datos ni proceso manual asistido por un operador o administrador.

Actualmente, Pandora FMS implementa una compactación de datos en tiempo real para cada inserción, además de realizar una compresión de datos basada en interpolación. Por otro lado, la tarea de mantenimiento permite borrar automáticamente los datos que sobrepasen cierta antigüedad.

El sistema de procesamiento de Pandora FMS almacena solo datos «nuevos»: si entra un valor duplicado en el sistema, no se almacenará en la base de datos. Esto es muy útil para mantener la base de datos reducida, y funciona para todos los tipos de módulo de Pandora FMS (numérico, incremental, booleano y cadena de texto). Por ejemplo, en los datos de tipo booleano el índice de compactación es muy alto ya que son datos que difícilmente cambian. No obstante, se almacenan elementos «índice» cada 24 horas, de forma que exista una información mínima que sirva como referencia a la hora de compactar la información.

Pandora FMS permite la disgregación total de componentes, de manera que se puede equilibrar la carga de procesado de ficheros de datos y ejecución de módulos de red en diferentes servidores.

Esquema Base de datos Pandora FMS

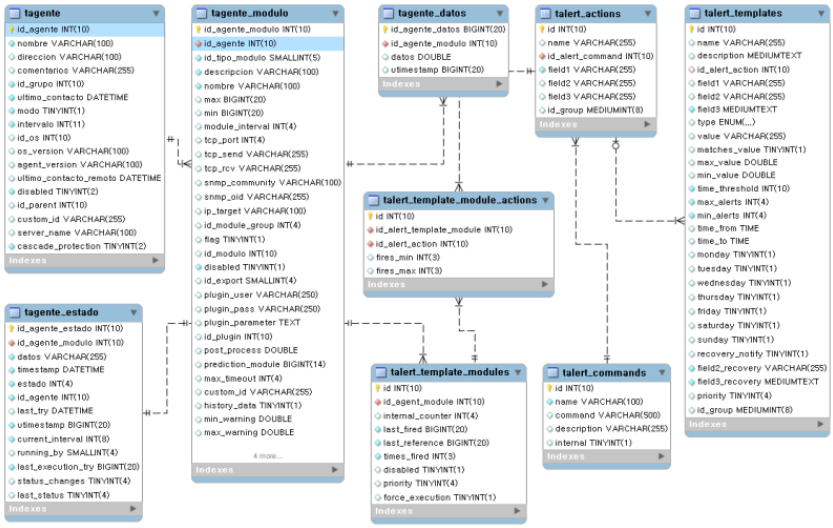


Figura 9. Tabla relacional de base de datos del servidor Pandora FMS

Según (PandoraFMS, 2022) Algunas de las tablas importantes en la base de datos de Pandora FMS son:

tagent_data: Son datos recibidos de cada módulo. Si para un mismo módulo el último dato recibido es el mismo que el anterior, no se añadirá (pero se actualizará en tagent_status). Los datos incrementales y de tipo cadena se guardan en tablas diferentes.

tagent_access: Agrega una nueva entrada cada vez que se reciban datos de un agente a cualquier servidor, pero nunca más de uno por minuto para evitar sobrecargar la base de datos. Se puede deshabilitar estableciendo agentaccess en 0 en el archivo de configuración pandora_server.conf.

taddress: Contiene las direcciones adicionales de los agentes.

tagent: Contiene la información de los agentes de Pandora FMS.

talert_snmp: Configuración de alertas SNMP.

talert_commands: Comandos que se pueden ejecutar a partir de acciones asociadas a una alerta (ej. enviar correo).

talert_actions: Instancia de comando asociada a cualquier alerta (por ejemplo, enviar correo al administrador).

talert_templates: Plantillas de alertas.

talert_template_module_actions: Instancia de una acción asociada a una alerta (ref. talert_template_modules).
talert_compound: Alertas compuestas, las columnas son similares a las de talert_templates.
talert_compound_elements: Alertas simples asociadas a una alerta compuesta, cada una con su correspondiente operación lógica (ref. talert_template_modules).
talert_compound_actions: Acciones asociadas a una alerta compuesta (ref. talert_compound).
tatachment: Archivos adjuntos asociados a una incidencia.
tconfig: configuración de la consola.
tconfig_os: Sistemas Operativos válidos en Pandora FMS.
tevent: Entradas de eventos. Los valores de prioridad son los mismos que los de las alertas.
tgroup: Grupos definidos en Pandora FMS.
tincidencia: Entradas de incidencia.
tlanguage: Idiomas disponibles en Pandora FMS.
tlink: Enlaces mostrados en la parte inferior del menú de la consola.
tnetwork_component: Componentes de red. Son módulos asociados a un perfil de red utilizado por el Recon Server. Después dan como resultado una entrada en tagent_module, por lo que las columnas de ambas tablas son similares.
tnetwork_component_group: Grupos para clasificar los componentes de la red.
tnetwork_profile: Perfil de red. Grupo de componentes de red que se asignará a las tareas de reconocimiento del Recon Server. Los componentes de red asociados al perfil darán como resultado módulos en los agentes creados.
tnetwork_profile_component: Componentes de red asociados a un perfil de red (rel. tnetwork_component/tnetwork_profile).

- **Data server**

Procesa la información enviada por los Agentes Software. Los Agentes Software recogen información de forma local de los sistemas en los que se encuentran instalados y construyen un paquete de información en formato XML. Estos paquetes en formato XML son enviados al servidor.
En el servidor son recibidos en un directorio específico, el servidor procesa todos los archivos que vayan llegando a este directorio de entrada y almacena la información en la base de datos.

- Recibe datos como ficheros XML.
- Lee los ficheros de un directorio de entrada.
- Los ficheros llegan ahí por diversos medios: SSH, FTP o Tentacle o por copia local.
- Multihilo.
- Funciona en HA.

Arquitectura Data Server

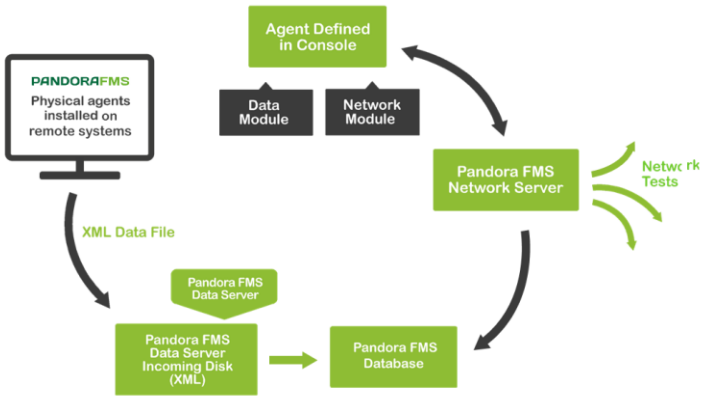


Figura 10. Arquitectura del servidor de datos de Pandora FMS
Fuente: Arquitectura Pandora FMS Documentación 2021

Consola Web Pandora FMS

La consola Web es la aplicación que permite gestionar Pandora FMS mediante un navegador conectado a Internet. Pandora FMS es una herramienta de gestión web. Gracias al sistema de permisos, pueden trabajar múltiples usuarios con diferentes permisos accediendo a la información del mismo setup de Pandora FMS sin que unos vean la información de otros.

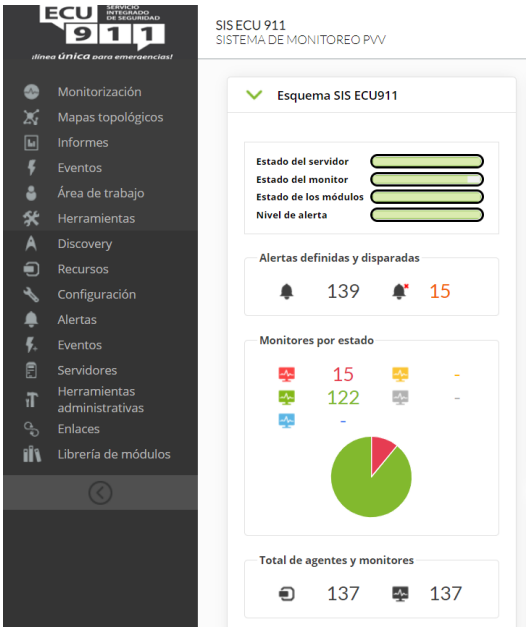


Figura 11. Consola web de Pandora FMS
Fuente: Arquitectura Pandora FMS Documentación 2021

2.2.2.8. Herramienta de Monitoreo Nagios

Nagios es un sistema de monitoreo de sistemas informáticos de código abierto. Está diseñado para ejecutarse en el sistema operativo Linux y puede monitorear dispositivos que ejecutan sistemas operativos (SO) Linux, Windows y Unix.

El software Nagios comprueba periódicamente los parámetros clave de la aplicación, la red y los recursos del servidor. Por ejemplo, Nagios puede monitorear el uso de la memoria, el uso del disco, la carga del microprocesador, la cantidad de procesos en ejecución y los archivos de registro. Nagios también puede monitorear servicios como el Protocolo simple de transferencia de correo (SMTP), el Protocolo de oficina postal 3 (POP3), el Protocolo de transferencia de hipertexto (HTTP) y otros protocolos de red comunes. Nagios inicia verificaciones activas y las verificaciones pasivas provienen de aplicaciones externas conectadas a la herramienta de monitoreo.

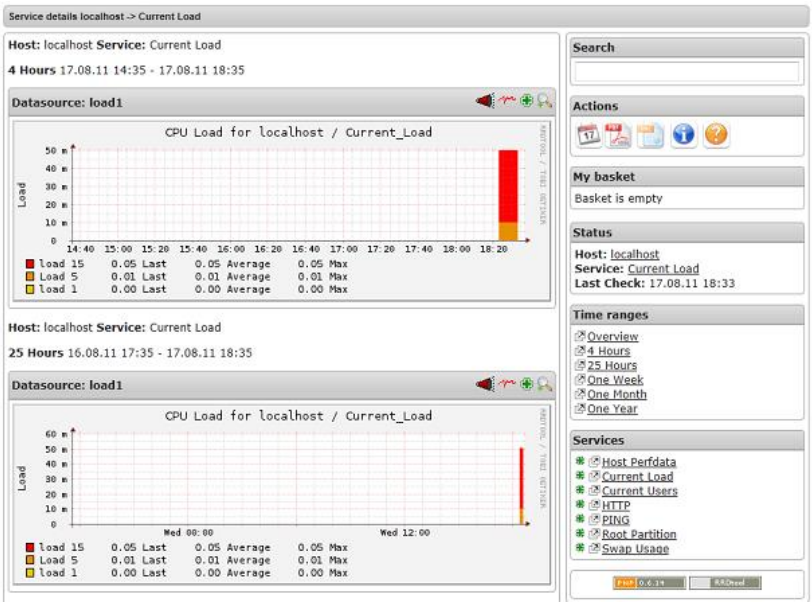


Figura 12. Pantalla principal de la herramienta de monitoreo Nagios
Fuente: Monitorizando equipos y servicios con Nagios + NagiosQl + PNP4Nagios por Carlos León

Su Core es la parte más importante de la herramienta y sobre el Core se pueden construir plugins para monitorizar elementos particulares, probablemente es la herramienta libre más conocida debido a que su gran uso es debido a que fue el primero que desarrolló una herramienta que cubría características indispensables en una monitorización de red.

Por esta razón, Nagios fue muy popular. Además, debido a su gran penetración de mercado inicial sigue siendo muy utilizada (Insoc, 2020).

En resumen, Nagios es un software Open Source que continuamente monitorea redes, aplicaciones y servidores. Puede encontrar y reparar problemas detectados en la infraestructura tecnológica y detener futuros inconvenientes antes que afecten al cliente dando completa información del estado de la infraestructura y su rendimiento algunas de sus características más importantes son las siguientes:

Tabla 5. Características de Nagios

Características	**Descripción**
Gratuito	Nagios este licenciado bajo los términos de una licencia GNU lo cual da posibilidades de copiar, distribuir o modificar la aplicación bajo ciertos parámetros

Multitarea	Nagios aparte de monitorizar dispositivos, servicios, puede monitorizar la carga del CPU, la memoria en uso, el espacio en disco, los procesos corriendo entre otros.
Versátil	Es capaz de monitorizar varios servicios de red (SMTP, POP3, HTTP, NTTP, ICMP, SNMP).
Presentación gráfica	Visualiza el estado de la red en tiempo real a través de una interfaz web, que permite generar informes y gráficas del comportamiento de los sistemas monitorizados.
Seguridad	Ofrece servicios de niveles de control de acceso basados en roles.

Fuente: Elaboración de los autores

Esquema de notificaciones Nagios

Nagios puede notificarnos cuando ha ocurrido algún problema en nuestra red o si este ya ha sido solucionado. Dichas notificaciones pueden ser por email o por cualquier otro medio configurado en nuestro sistema.

Nagios admite configurar notificaciones de contacto para hosts y servicios. La escalada de notificaciones de host y servicio se logra definiendo hosts y servicios en su archivo de configuración de objetos. Una vez que se escala una notificación, los contactos/grupos y las opciones de notificación para el objeto serán escritos por la configuración previamente establecida.

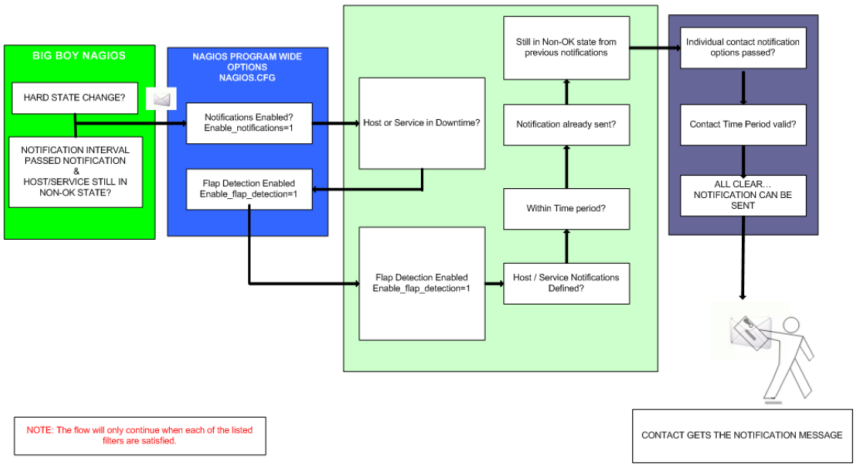


Figura 13. Estructura de alerta de Nagios
Fuente: Monitorizando equipos y servicios con Nagios León 2019

Cuando uno configura un servicio tiene las siguientes opciones:

D: DOWN: El servicio esta caída (no disponible).

U: UNREACHABLE: Dispositivo no está visible.

R: RECOVERY: (OK) Dispositivo recuperando

F: FLAPPING: La primera vez con un dispositivo sube, bajo o está en un estado indeterminado.

N: NONE: No manda ninguna notificación.

Arquitectura de la herramienta de monitoreo Nagios

Las API múltiples proporcionan una integración sencilla con aplicaciones internas y de terceros. Miles de complementos desarrollados por la comunidad amplían la funcionalidad de supervisión y alertas nativas. Los desarrollos personalizados de interfaz y addon están disponibles para adaptar Nagios XI a las necesidades exactas de su organización.

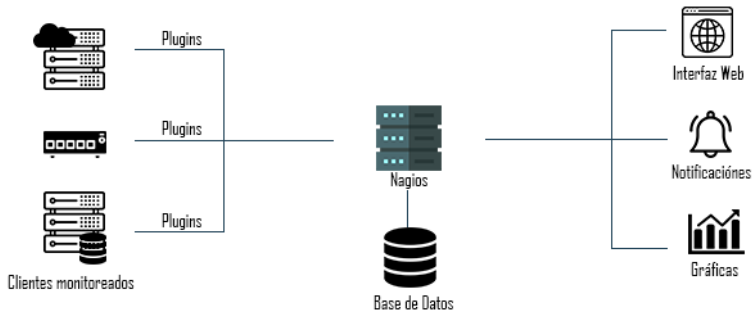


Figura 14. Funcionamiento interno de Nagios
Fuente: Arquitectura de Nagios 2018 por Alfredo Sánchez

2.2.2.9. Herramienta de Monitoreo Cacti

Cacti es una herramienta de monitoreo de código abierto que permite obtener datos e información provenientes a equipos conectados a la infraestructura tecnológica siendo capaz de crear gráficas ver su comportamiento en el tiempo en la monitorización de red. Ofrece una interfaz gráfica para RRDTool (Round Robin Data Tool) la cual significa que sirve para la creación de gráficos de datos en una serie de tiempo, enviando mensajes de comunicación a equipos para que respondan sobre algunas variables de desempeño de sus componentes. (Ramírez, 2017)

Tal como lo explica Cacti (2021) incluye un marco de recopilación de datos totalmente distribuido y tolerante a fallas, funciones avanzadas de automatización basadas en plantillas para dispositivos, gráficos y árboles, múltiples métodos de adquisición de datos, la capacidad de extenderse a través de complementos, funciones de administración de usuarios, grupos y

dominios basados en roles, además de un motor de tematización y compatibilidad con varios idiomas desde el primer momento.

Pantalla de monitorización de Cacti

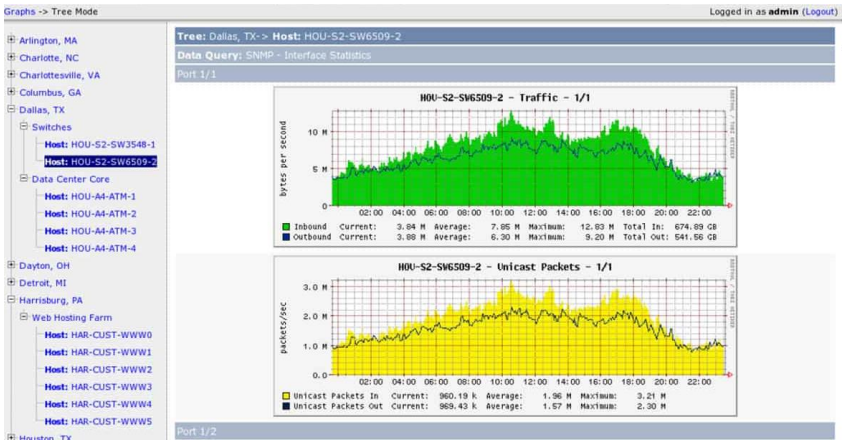


Figura 15. Interfaz de la aplicación Cacti
Fuente: IT software (2017) Cacti Monitoreo de red opensource

En resumen, Cacti es una herramienta de monitoreo de datos open source que utiliza dispositivos de la infraestructura de red que utilicen SNMP para la creación de gráficos RDDTool que pueden contener diferentes características como la conexión a la red, temperatura, voltaje entre otros, sus características más destacables son las siguientes:

Tabla 6. Características de Cacti

Características	**Descripción**
Gráficos	Cacti permite utilizar funciones de RRDTool para definir gráficos y crear información en arboles jerárquicos.
Dispositivos	Los dispositivos son utilizados en el centro de datos de Cacti que sirven para crear los gráficos RRDTool, El soporte de dispositivos Cacti está enfocado a dispositivos SNMP.
Recolección de datos remota	Cacti tiene un sistema de recopilación de datos a los dispositivos que se monitorean a través de conexiones de https MariaDB y MySQL teniendo la capacidad de funcionar, aunque el sistema central de Cacti no esté disponible.

Complementos	La aplicación de Cacti es muy robusta, pero se puede ampliar para realizar otras funciones mediante el uso de su arquitectura de complementos.
Plantillas	Permite la creación de plantillas asociadas tanto a la fuente de datos como a sus gráficas lo que facilita la reutilización con otros elementos del mismo tipo.

Fuente: Elaboración de los autores

Requerimientos de Instalación

Cacti requiere como mínimo lo siguiente para funcionar:

- Sistema operativo Linux como Debian, Gentoo, Redhat, Fedora o SUSE.
- Servicio web Apache.
- PHP
- MySQL
- RRDTool
- Si se usa SNMP se debe instalar net_snmp.

Arquitectura de la herramienta de monitoreo Cacti

La arquitectura de CACTI fue diseñada de manera simple. CACTI usa PHP para interactuar la interfaz de usuario para los usuarios finales con la base de datos MySQL. Sin embargo, hay una herramienta que crea un gráfico, que se llama Herramienta RRD.

Cuando CACTI funciona, envía una solicitud SNMP al objeto administrado para obtener la información. Luego lo envía a la base de datos MySQL. A continuación, la herramienta RRD utilizará la información de la base de datos para trazar un gráfico. Finalmente, la gráfica se mostrará en la interfaz de usuario, la cual está basada en PHP.

Arquitectura y Funcionamiento de la Herramienta de Monitoreo Cacti

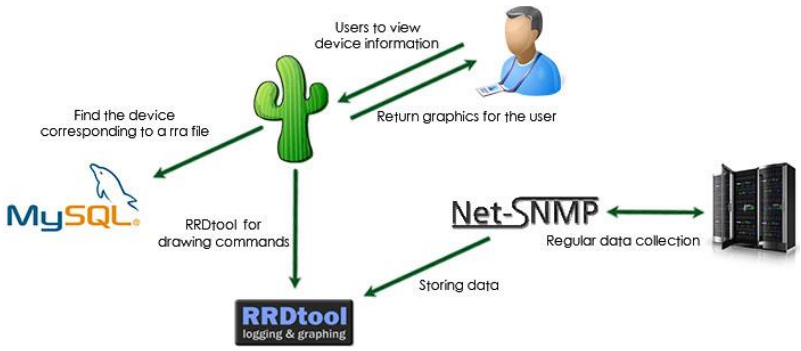


Figura 16. Principio de funcionamiento de Cacti
Fuente: Ri Xu Online (2016) Install the Cacti Server Monitor on Ubuntu Server

2.2.3. Infraestructura tecnológica

2.2.3.1. Definición de Infraestructura

Tal como menciona Acosta (2014) se entiende por infraestructura el dispositivo que permite la transmisión de la señal. Ejemplos: líneas, hornos microondas, satélites y vehículos. Los dispositivos y programas informáticos involucrados en la transmisión de información, como los sistemas operativos y los protocolos de comunicación, también llegan a los usuarios a través de sus propios dispositivos de acceso o se comparten a través de medios inalámbricos.

2.2.3.2. Tipos de infraestructura tecnológica

Existen dos tipos de infraestructura tecnológica, la parte del Hardware y Software. Dentro del conjunto Físico encontramos “elementos tan diversos como los reguladores de corriente, los sistemas de seguridad, las cámaras, los servidores de aplicaciones, los elementos de red, como routers, repetidores o cortafuegos, las computadoras personales, las impresoras, las tabletas, los teléfonos, copiadoras, proyectores, pizarrones interactivos, conmutadores, etc.”.

Por otra parte, el Software es denominado la parte no tangible dentro del mundo informático, es decir, “son los sistemas y programas que facilitan el funcionamiento de otras aplicaciones.”. Los sistemas operativos y programas informáticos tienen un papel fundamental dentro de la clasificación del Software, en este apartado encontraremos “bases de datos, procesadores de texto, herramientas de ofimática” entre otros (Xeral, 2018).

Hardware

El centro local Ecu 911 dentro de su infraestructura cuenta con equipos físicos (hardware), que cumplen ciertas funciones específicas, entre ellos podemos identificar a las cámaras ip, cámaras lectoras de placa, megáfonos y servidores.

2.2.3.3. Gestión de Infraestructura tecnológica en una Institución u Organización

Tal como mencionan (Amaya y Sarria, 2019) para lograr una gestión adecuada en la infraestructura tecnológica dentro de una institución es necesario tomar en cuenta varios requisitos técnicos, ya que al cumplir estas consideraciones el funcionamiento contará con facilidades en su manejo y gracias a esto se logrará optimizar varias funciones. De igual manera, es necesario "contar con un aparato estructural que satisfaga las demandas de la empresa" (p. 4).

2.2.3.4. Infraestructura tecnológica dentro del Ecu 911

El centro de operaciones ECU 911 es capaz de recibir llamadas de residentes y comunicarse internamente a través de teléfonos fijos o móviles. También se debe tomar en cuenta que todas las comunicaciones se almacenan en el dispositivo de servicio. El Ecu 911 cuenta con un software de llamada y atención que registra automáticamente cualquier incidente o llamada de emergencia que ingresa al centro operativo, este programa realiza registros exitosos dependiendo del tipo de configuración que se le asigne.

- **Red Nacional Troncalizada**

La Red Nacional Troncalizada RNT es la integración de varias redes de comunicación del estado que cumplen el estándar digital APCO25 aprobado por el Comité Intersectorial del SIS 911, conformándose como una red de misión crítica, y mediante la cual las entidades articuladas comparten todos los canales de comunicación disponibles de manera organizada e independiente, a fin de coordinar acciones en el ámbito de la seguridad.

Su objetivo es garantizar la óptima coordinación interinstitucional en el ámbito de seguridad y atención de emergencias, a través de una única infraestructura de comunicaciones a lo largo del país.

Red Nacional Troncalizada Ecu 911

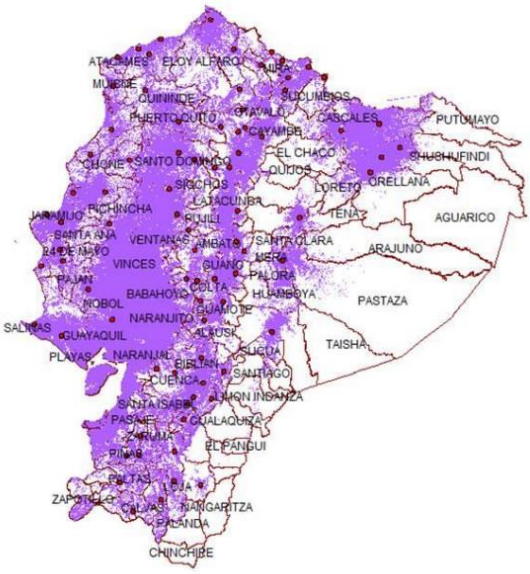


Figura 17. Red Nacional Troncalizada

Fuente: Coordinación General de Planificación y Gestión Estratégica (2015) Plan estratégico

2.2.3.5. Topología de Red

Según (Etece, 2021) hay tres topologías o modelos de diseño de red:

- **Redes en bus**

También conocidos como lineales, tienen un servidor al principio de la siguiente línea de clientes y tienen un único canal de comunicación llamado bus o backbone.

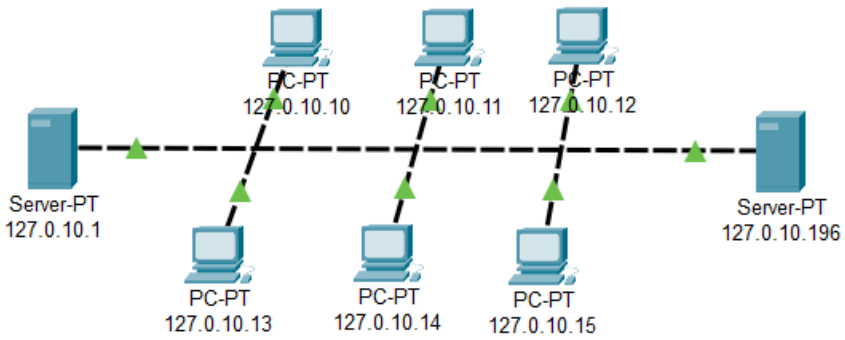


Figura 18. Esquema de topología en BUS
Fuente: Software Cisco Packet Tracer vers. 8.1.1

- **Redes en estrella**

Cada computadora tiene una conexión directa con el servidor, el servidor está en el medio de todo. Toda comunicación entre clientes debe pasar primero por el servidor.

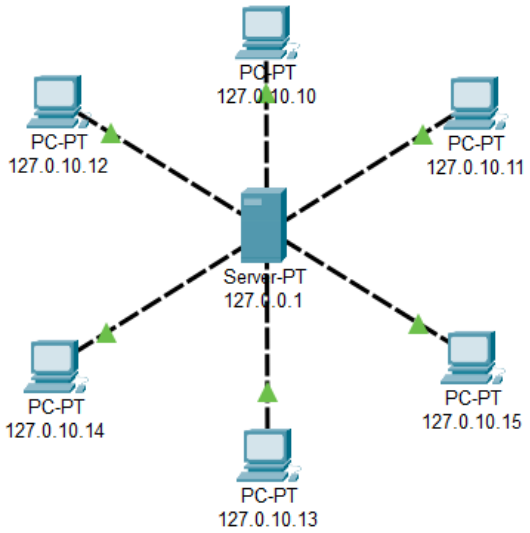


Figura 19. Esquema de topología en estrella
Fuente: Software Cisco Packet Tracer vers. 8.1.1

En anillo

También conocidos como circulares, conectan clientes y servidores en un circuito circular, aunque el servidor mantiene su jerarquía en el sistema.

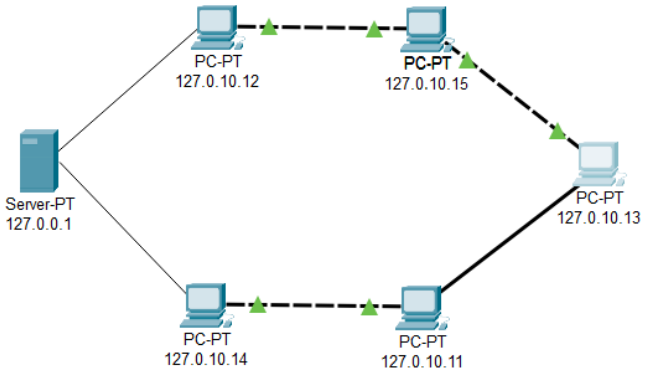


Figura 20. Esquema de topología en anillo
Fuente: Software Cisco Packet Tracer vers. 8.1.1

2.2.3.6. Tipos de Protocolos de red

Tal y como menciona (Fernandez, 2022) Existen diferentes protocolos de internet, que establecen distintas condiciones, para adaptarse al tipo de información que tienen que resguardar.

- **Protocolo TCP/IP**

El protocolo TCP/IP es el protocolo de comunicación básico de Internet y consta de dos protocolos, TCP e IP. El propósito es que las computadoras puedan simplemente comunicarse y transmitir información a través de la red.

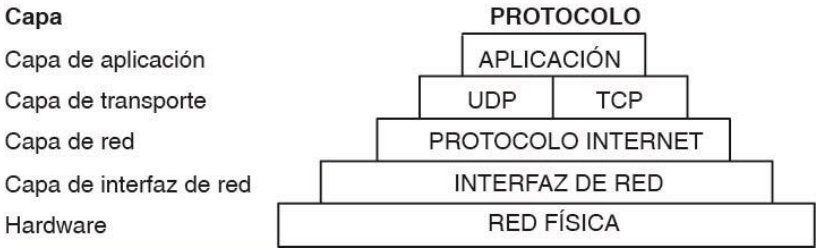


Figura 21. Conjunto de protocolos TCP/IP
Fuente: Protocolos TCP/IP IBM 2021

La capa de red de Internet pone el paquete en un datagrama de IP (Internet Protocol), pone la cabecera y la cola de datagrama, decide dónde enviar el datagrama (directamente a un destino o a una pasarela) y pasa el datagrama a la capa de interfaz de red. La capa de interfaz de red acepta los datagramas IP y los transmite como tramas a través de un hardware de red específico, por ejemplo, redes Ethernet o de Red en anillo.

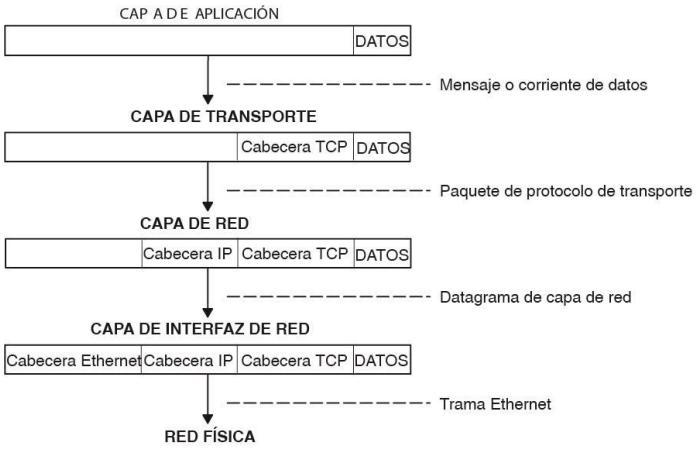


Figura 22. Conjunto de protocolos TCP/IP
Fuente: Protocolos TCP/IP IBM 2021

Esta figura muestra el flujo de información de las capas de protocolo TCP/IP del remitente al host. Las tramas recibidas por un sistema principal pasan a través de las capas de protocolo en sentido inverso. Cada capa quita la información de cabecera correspondiente, hasta que los datos regresan a la capa de aplicación.

- ✓ ***Protocolo Internet (IP) versión 6***

Internet Protocol (IP) versión 6 (IPv6 o IPng) es la siguiente generación de IP y se ha diseñado para ser un paso de desarrollo de IP versión 4 (IPv4).

- ✓ ***Rastreo de paquetes***

El rastreo de paquetes es el proceso mediante el cual puede verificar la vía de acceso a través de las capas hasta el destino.

- ✓ ***Cabeceras de paquete de interfaz de red***

En la capa de Interfaz de red, se adjuntan cabeceras de paquete a los datos de salida.

- ✓ ***Protocolos a nivel de red Internet***

Los protocolos a nivel de red Internet manejan las comunicaciones de máquina a máquina.

- ✓ ***Protocolos a nivel de transporte de Internet***

Los protocolos de nivel de transporte TCP/IP permiten a los programas de aplicación comunicarse con otros programas de aplicación.

- ✓ ***Protocolos a nivel de aplicación de Internet***

TCP/IP implementa protocolos de Internet de nivel superior en el nivel de programa de aplicación.

- ✓ ***Números asignados***

Por compatibilidad con el entorno de red general, se asignan números conocidos públicamente para las versiones, las redes, los puertos, los protocolos y las opciones de protocolo de Internet. Adicionalmente, también se asignan nombres conocidos públicamente a máquinas, redes, sistemas operativos, protocolos, servicios y terminales.

- ➢ **Protocolo HTTP**

HTTP (Protocolo de transferencia de hipertexto) se basa en www (World Wide Web) para transmitir mensajes a través de la red. Por ejemplo, cuando el usuario ingresa al navegador, la URL pasa los mensajes vía HTTP al servidor web solicitado por el usuario. El servidor web responderá y proporcionará resultados para los criterios de búsqueda solicitados.

El protocolo HTTP es el código o lenguaje en el que el navegador le comunica al servidor qué página quiere visualizar.

Figura 23. Proceso de comunicación HTTP
Fuente: Protocolo HTTP según Digital IONOS

- **Métodos de petición**

Un pedido HTTP usando telnet. El pedido (request), cabeceras de respuesta (response headers) y el cuerpo de la respuesta (response body) están resaltados.

HTTP define una serie predefinida de métodos de petición que pueden utilizarse. El protocolo tiene flexibilidad para ir añadiendo nuevos métodos y para así añadir nuevas funcionalidades. El número de métodos de petición se ha ido aumentando según se avanzaba en las versiones.1 Esta lista incluye los métodos agregados por (WebDAV, 2021).

Cada método indica la acción que desea que se efectúe sobre el recurso identificado. Lo que este recurso representa depende de la aplicación del servidor. Por ejemplo, el recurso puede corresponderse con un archivo que reside en el servidor.

- ✓ ***Get***

El método GET solicita una representación del recurso especificado. Las solicitudes que usan GET solo deben recuperar datos y no deben tener ningún otro efecto. (Esto también es cierto para algunos otros métodos HTTP.)

- ✓ ***Head***

Pide una respuesta idéntica a la que correspondería a una petición GET, pero en la respuesta no se devuelve el cuerpo. Esto es útil para poder recuperar los metadatos de los encabezados de respuesta, sin tener que transportar todo el contenido.

- ✓ ***Post***

Envía datos para que sean procesados por el recurso identificado en la URL de la línea petición. Los datos se incluirán en el cuerpo de la petición. A nivel semántico está orientado a crear un nuevo recurso, cuya naturaleza vendrá especificada por la cabecera Content-Type.

Ejemplos:

- ✓ ***Put***

Envía datos al servidor, pero a diferencia del método POST la URI de la línea de petición no hace referencia al recurso que los procesará, sino que identifica a los propios datos (ver explicación detallada en el RFC). Otra diferencia con POST es semántica (ver REST): mientras que POST está orientado a la creación de nuevos contenidos, PUT está más orientado a la actualización de estos.

- ✓ ***Trace***

Este método solicita al servidor que introduzca en la respuesta todos los datos que reciba en el mensaje de petición. Se utiliza con fines de depuración y diagnóstico ya que el cliente puede ver lo que llega al servidor y de esta forma ver todo lo que añaden al mensaje los servidores intermedios

- ✓ ***Options***

Devuelve los métodos HTTP que el servidor soporta para un URL específico. Esto puede ser utilizado para comprobar la funcionalidad de un servidor web mediante petición en lugar de un recurso específico.

- ✓ ***Connect***

Se utiliza para saber si se tiene acceso a un host, no necesariamente la petición llega al servidor, este método se utiliza principalmente para saber si un proxy nos da acceso a un host bajo condiciones especiales, como por ejemplo "corrientes" de datos bidireccionales encriptadas.

- ✓ ***Patch***

Su función es la misma que PUT, el cual sobrescribe completamente un recurso. Se utiliza para actualizar, de manera parcial una o varias partes. Está orientado también para el uso con proxy.

- ➢ **Protocolo FTP**

El Protocolo de transferencia de archivos (FTP) se usa comúnmente para transferir archivos a través de Internet. FTP utiliza un servidor cliente para compartir archivos en una computadora remota.

El acceso a FTP es un servicio básico incluido en cualquier tipo de alojamiento web. Eligiendo con Linube tu hosting compartido o un servidor cloud obtendrás acceso a través de FTP. El uso de FTP resulta fundamental para el acceso al servidor y una correcta gestión

de la página web. Si tu plan de alojamiento incluye un panel Plesk, podrás crear tantas cuentas FTP adicionales como necesites para directorios específicos.

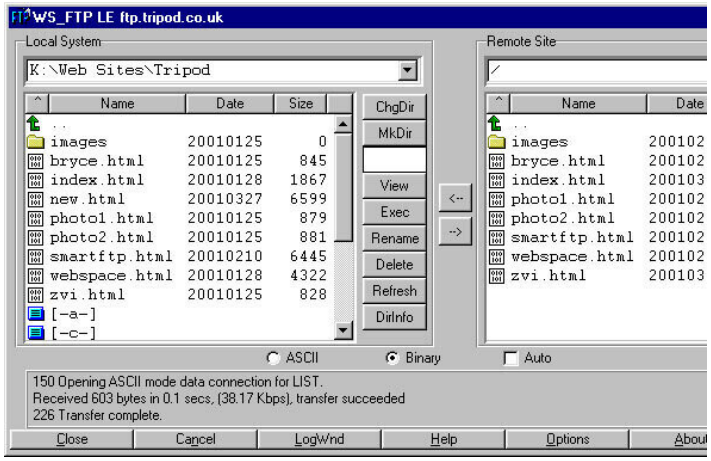


Figura 24. Protocolo FTP
Fuente: Protocolo FTP según Yubal Fernández

Este protocolo funciona entre ordenadores que estén conectados a una red TCP, que significa Transmission Control Protocol o Protocolo de control de transmisión. Este protocolo TCP da soporte a muchas tecnologías, entre ellas a Internet. Para que te hagas a la idea, la familia de protocolos que forman Internet se llama TCP/IP.

- ✓ ***Conexión Cliente-Servidor***

Las conexiones FTP tienen una relación de cliente y servidor. Esto quiere decir que un ordenador tiene que estar configurado como servidor FTP, ese en el que se aloja el contenido, y luego tú te conectas a él como un cliente.

- ➢ **Protocolo SSH**

SSH o Secure Shell, es un protocolo de administración remota que le permite a los usuarios controlar y modificar sus servidores remotos a través de Internet a través de un mecanismo de autenticación.

Proporciona un mecanismo para autenticar un usuario remoto, transferir entradas desde el cliente al host y retransmitir la salida de vuelta al cliente. El servicio se creó como un reemplazo seguro para el Telnet sin cifrar y utiliza técnicas criptográficas para garantizar que todas las comunicaciones hacia y desde el servidor remoto sucedan de manera encriptada.

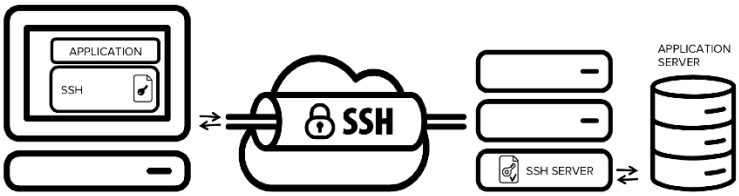


Figura 25. Protocolo SSH
Fuente: Como funciona SSH según Hostinger 2022

Hay tres tecnologías de cifrado diferentes utilizadas por SSH:

- ✓ ***Cifrado Simétrico***

El cifrado simétrico es una forma de cifrado en la que se utiliza una clave secreta tanto para el cifrado como para el descifrado de un mensaje, tanto por el cliente como por el host. Efectivamente, cualquiera que tenga la clave puede descifrar el mensaje que se transfiere.

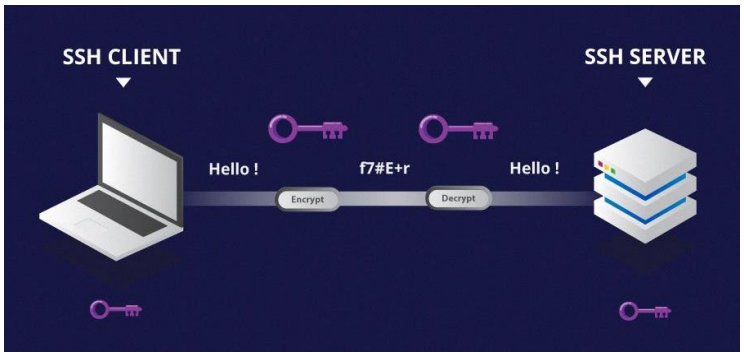


Figura 26. Cifrado Simétrico
Fuente: Como funciona SSH según Hostinger 2022

El cifrado simétrico a menudo se llama clave compartida o cifrado secreto compartido. Normalmente sólo hay una clave que se utiliza, o a veces un par de claves donde una clave se puede calcular fácilmente con la otra clave.

- ✓ ***Cifrado Asimétrico***

A diferencia del cifrado simétrico, el cifrado asimétrico utiliza dos claves separadas para el cifrado y el descifrado. Estas dos claves se conocen como la clave pública y la clave privada. Juntas, estas claves forman el par de claves pública-privada.

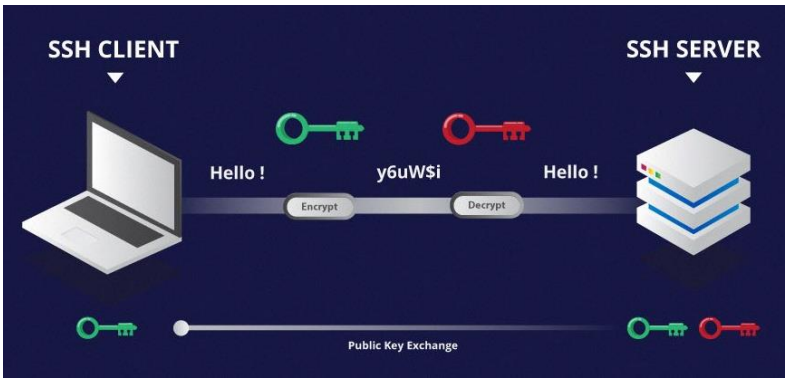


Figura 27. Cifrado Simétrico
Fuente: Como funciona SSH según Hostinger 2022

La clave pública, como sugiere el nombre, se distribuye abiertamente y se comparte con todas las partes. Si bien está estrechamente vinculado con la clave privada en términos de funcionalidad, la clave privada no se puede calcular matemáticamente desde la clave pública. La relación entre las dos claves es altamente compleja.

- ✓ ***Hashing***

El hashing unidireccional es otra forma de criptografía utilizada en Secure Shell Connections. Las funciones de hash unidireccionales difieren de las dos formas anteriores de encriptación en el sentido de que nunca están destinadas a ser descifradas. Generan un valor único de una longitud fija para cada entrada que no muestra una tendencia clara que pueda explotarse. Esto los hace prácticamente imposibles de revertir.

Figura 28. Cifrado Hashing
Fuente: Como funciona SSH según Hostinger 2022

- ➢ **Post-Office Protocol Version 3 (POP3)**

Es un protocolo de Internet estándar utilizado por varios clientes de correo electrónico. Se utiliza para poder recibir correo de un servidor remoto a través de una conexión TCP/IP.

Haciendo un poco de historia, POP3 se diseñó por primera vez en 198 y se ha convertido en uno de los más populares. Es utilizado por casi todos los clientes de correo electrónico conocidos, es muy simple de configurar, usar y mantener.

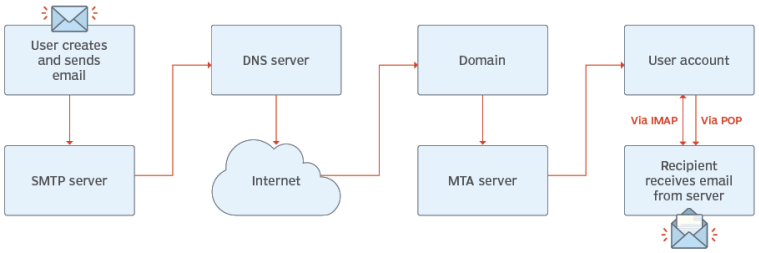


Figura 29. Protocolo POP3
Fuente: Post Office Protocol 3 Según CNNA 2019

- ✓ ***Puertos POP3***

POP3 funciona en los dos puertos siguientes de forma predeterminada:

Puerto 110: puerto predeterminado, no cifrado; y

Puerto 995: debe usarse cuando el usuario necesita conectarse usando POP3 de forma segura.

El servidor inicia el servicio POP3 escuchando en el puerto TCP 110. Cuando un cliente desea utilizar POP3 para recuperar correo electrónico, establece una conexión TCP con el host del servidor. Una vez establecida esta conexión, el servidor POP3 envía un saludo. En este punto, la sesión entra en el estado de autorización.

En el siguiente estado de transacción, el cliente y el servidor intercambian comandos y respuestas hasta que la conexión se cierra o se cancela. Los comandos del cliente consisten en palabras clave que no distinguen entre mayúsculas y minúsculas, posiblemente seguidas de argumentos. Las respuestas del servidor constan de un indicador de estado y una palabra clave, que puede ir seguida de información adicional.

Cuando el cliente emite el comando de salida, la sesión ingresa al estado de actualización. El servidor POP3 libera los recursos adquiridos durante el estado de la transacción y dice "adiós", que es cuando se cierra la conexión TCP. Una vez que la sesión POP3 ingresa al estado de actualización, el servidor POP3 elimina el mensaje.

- **Simple Mail Transfer Protocol (SMTP)**

Este protocolo, junto con los mencionados anteriormente, se considera uno de los servicios más valiosos de Internet. La mayoría de los sistemas que funcionan en Internet utilizan SMTP como método de envío/reenvío de correo electrónico.

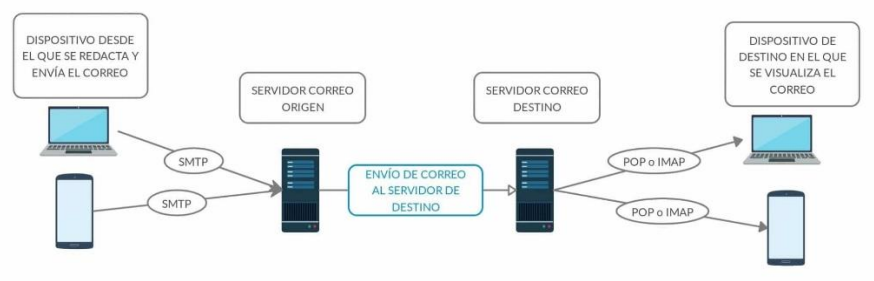


Figura 30. Protocolo SMTP
Fuente: SMTP: Qué es, cómo funciona y cómo se configura según Raiola 2020

Un servidor SMTP es un servidor de correo que se encarga de realizar el envío del mensaje de la forma más eficiente posible, empleando el protocolo SMTP. La ventaja del uso de un servidor SMTP para enviar el correo viene dada de las configuraciones avanzadas que suelen tener para mejorar la seguridad, evitar el envío de SPAM, evitar que el correo enviado se marque como spam.

Realmente, un servidor SMTP no es necesario como tal para enviar el correo. Desde tu propio ordenador puedes realizar el envío de correo sin pasar por ningún servidor de este tipo. Sin embargo, si no está preparado de forma adecuada es posible que te encuentres con múltiples problemas.

En la siguiente captura se realiza una conexión SMTP a uno de los servidores. Los pasos principales consisten en iniciar la conexión, autenticarse, indicar destino del mensaje, redactar el contenido y que el servidor lo acepte para enviarse.

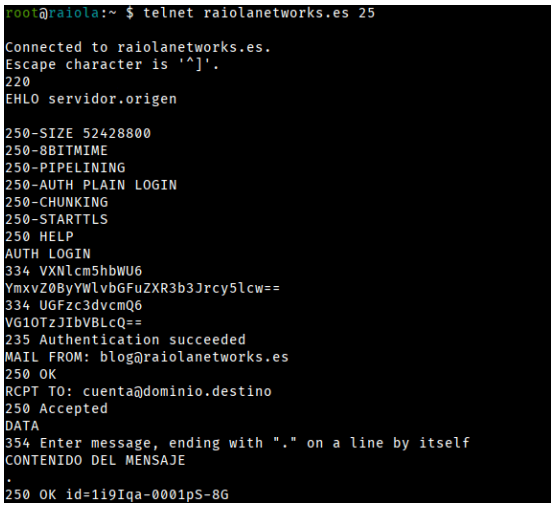


Figura 31. Protocolo SMTP
Fuente: SMTP: Qué es, cómo funciona y cómo se configura según Raiola 2020

- **Configuración y puertos para SMTP**

Para la conexión SMTP entre tu dispositivo y el servidor de correo hay que usar una cierta configuración.

Servidor saliente: Dirección del servidor de correo (en ocasiones sirve mail.tudominio).
Usuario: El usuario que tengas para tu servidor
Contraseña: La contraseña de tu cuenta de correo electrónico o usuario.
Puerto: Pueden estar personalizados en cada servidor, pero, por lo general, son: 25 (sin SSL), 587 (TLS) y 465 (SSL).

2.2.4. Base de datos

Una base de datos permite tener organizada la información de forma estructurada, esta estará almacenada de forma electrónica en una aplicación informática. Oracle (2022) La información en un base de datos está estructurada en filas y columnas en diferentes tablas para aumentar la eficiencia del procesamiento y la consulta de datos. A dicha información se puede acceder, modificar, actualizar, borrar y organizar la información de cada tabla cuando sea necesario.

En conclusión, para la investigación se ha optado por utilizar una base de datos relacional ya que si observamos la arquitectura de donde se obtendrá la información, Pandora FMS utiliza una base de datos relacional diseñada en MySQL.

Un esquema bien definido y funcional de una base de datos debe cumplir las siguientes características:

- **Integridad de los datos**

La integridad de los datos es la integridad, precisión y consistencia de los datos. Las bases de datos relacionales utilizan un conjunto de restricciones para imponer la integridad de los datos en la base de datos.

- **Transacciones**

Una transacción de base de datos es una o más sentencias SQL ejecutadas como una secuencia de operaciones que forman una sola unidad lógica de trabajo.

- **Conformidad con ACID**

Todas las transacciones de la base de datos deben ser compatibles con ACID (atómico, consistente, aislado y duradero) para garantizar la integridad de los datos.

2.2.4.1. Tipos de bases de datos según su orden

Según (Intelegia, 2020) la primera clasificación de bases de datos depende de la manera en la que se ordenan los datos.

A continuación, veremos los diferentes tipos de bases de datos que existen:

Bases de datos estáticas

Las bases de datos estáticas están diseñadas para leer datos. En otras palabras, solo almacenan y guardan datos. Luego se pueden analizar para comprender su comportamiento a lo largo del tiempo. En particular, se utilizan para realizar pronósticos estadísticos y guiar los procesos de toma de decisiones en un entorno empresarial.

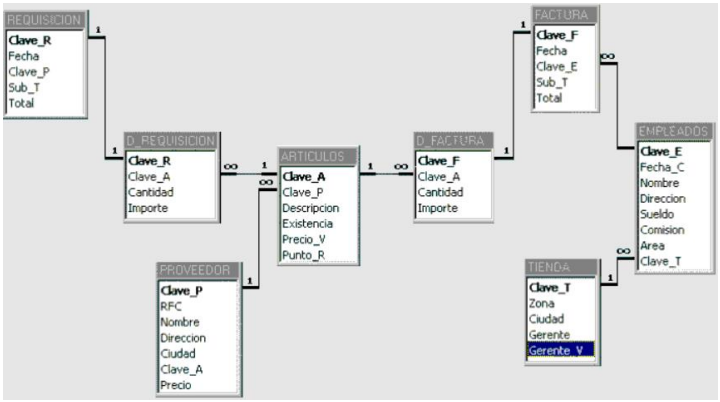


Figura 32. Ejemplo de esquema de base de datos estáticas.
Fuente: (Marcela, 2009).

Bases de datos dinámicas

Por el contrario, las bases de datos dinámicas pueden cambiar con el tiempo. Por lo tanto, los datos se pueden actualizar, modificar y eliminar. Por ejemplo, muchas tiendas cambian su inventario y los precios de los productos según la temporada, por lo que una base de datos dinámica es ideal.

Esquema de base de datos dinámicas

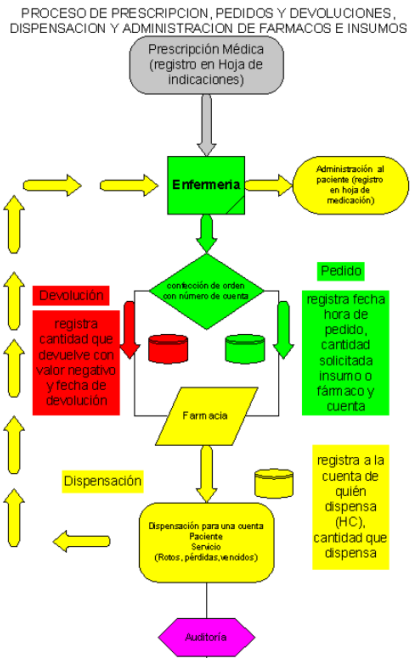


Figura 33. Ejemplo de esquema de base de datos dinámicas.

Fuente: Esquema de base de datos dinámicas (Marcela, 2019)

2.2.4.3. Bases de datos Relacionales

Según (Oracle, 2020) Una base de datos relacional es un tipo de base de datos que almacena y proporciona acceso a puntos de datos relacionados. Las bases de datos relacionales se basan en el modelo relacional, una forma intuitiva y sencilla de representar datos en tablas. En una base de datos relacional, cada fila de una tabla es un registro con un identificador único llamado clave.

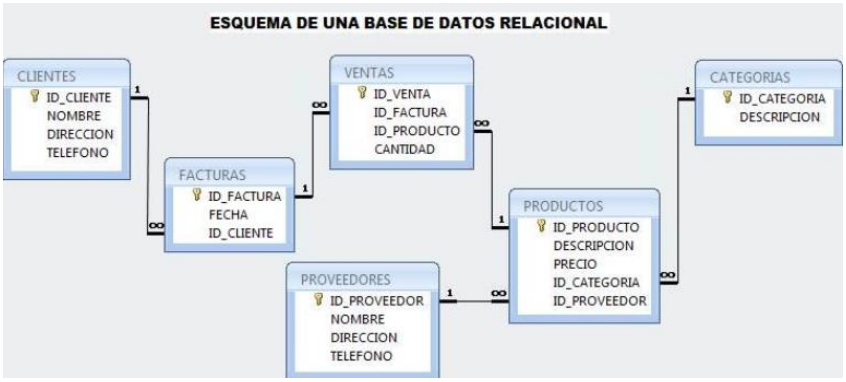


Figura 34. Ejemplo de esquema de base de datos relacionales.
Fuente: (Ayudaley, 2020).

Las columnas de la tabla contienen atributos de los datos y, por lo general, cada registro tiene un valor para cada atributo, lo que facilita establecer relaciones entre puntos de datos. Tal y como menciona (Amazon, 2022) Algunos aspectos importantes de las bases relacionales son:

- **Base de datos MySQL**

SQL o lenguaje de consulta estructurado es la principal interfaz utilizada para comunicarse con bases de datos relacionales. SQL se convirtió en un estándar ANSI (Instituto Nacional Estadounidense de Estándares) en 1986. Todos los motores de bases de datos relacionales populares admiten el estándar ANSI SQL.

La base de datos MySQL se lo conoce como un sistema de gestión de base de datos relacional permitiendo almacenar datos, esta dispone de una licencia de código libre y la otra con una versión comercial, todo esto es gestionado por la empresa de Oracle (Robledano, 2019).

Tabla 7. Características de las bases de datos MYSQL

Característica	**Descripción**
Arquitectura Cliente y Servidor	Funcionamiento se basa en cliente y servidor, esto quiere decir que el cliente y servidor se comunican entre sí.
Compatibilidad con SQL	SQL es un lenguaje generalizado dentro de la industria ya que es compatible con otro motor de base de datos.
Vistas	Ofrece la compatibilidad de poder configurar vistas personalizadas del mismo modo que se lo realiza en otra base de datos SQL.

Procedimientos Almacenados	MySQL posee características de no procesar las tablas directamente, esto se lo realiza mediante procedimientos.
Desencadenantes	Permite automatizar tareas en la base de datos.
Transacciones	Representa la actuación de diversas operaciones en la base de datos.

Fuente: Elaborado por Autores

- **Base de datos MariaDB**

MariaDB es una bifurcación de MySQL. En otras palabras, es un reemplazo directo mejorado de MySQL esto significa que puede sustituir el servidor MySQL estándar con la versión analógica del servidor MariaDB y aprovechar al máximo las mejoras en MariaDB sin necesidad de modificar el código de su aplicación.

MariaDB es rápido, escalable y robusto. Admite más motores de almacenamiento que MySQL. MariaDB también incluye muchos complementos y herramientas que lo hacen versátil para muchos casos de uso.

Tabla 8. Características de la base de datos MariaDB

Característica	**Descripción**
Mecanismos de Almacenamiento	Además de los mecanismos de almacenamiento estándar MyISAM, Blackhole, CSV, Memory y Archive, también se incluyen en la versión fuente y binaria de MariaDB los siguientes: Aria, XtraDB, PBTX, Cassandra entre otros.
Facilidad de Uso	Proporciona estadísticas de índices y tabla, para lo que añade nuevas tablas en INFORMATION_SCHEMA y nuevas opciones a los comandos FLUSH y SHOW para identificar la causa en la carga del SGBD.
Prestaciones	El optimizador de MariaDB -que se encuentra en el núcleo de cualquier SGBD- funciona claramente más rápido con cargas complejas.
Testeo	Más test en la distribución, así como la implementación de parches y distintas configuraciones para el sistema operativos de los tests.

Fuente: Elaborado por Autores

2.2.4.4. Bases de datos No relacionales

Las bases de datos no relacionales funcionan como un almacenamiento de datos que tiene características que la distinguen del grupo de base de datos relacionales las cuales se caracterizan por no utilizar un lenguaje SQL para sus consultas además de no trabajar con estructuras definidas, es decir, que los datos no se almacenan en tablas y los registros.

Las bases de datos al no tener una estructura definida se pueden organizar de diferentes maneras por ejemplo por documentos, por llaves, por columnas y por gráficos:

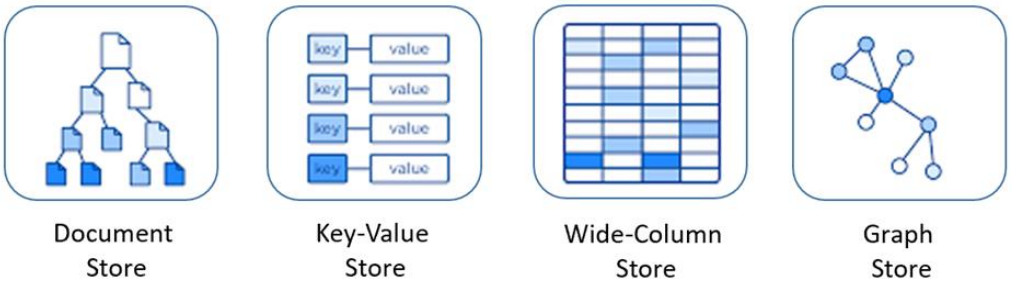


Figura 35. Ejemplo de esquemas de bases de datos no relacionales

Tabla 9. Características Base de datos No relacionales

Características	Descripción
Organización	La información no se almacena en tablas sino a través de documentos.
Utilidad	Son bases de datos muy útiles para organizar y gestionar información no estructurada, o cuando no se tiene una noción clara de los datos a almacenar.
Escalabilidad	Son bases de datos con alto grado de escalabilidad y están diseñadas para soportar grandes volúmenes de datos.
Flexibilidad	Son mucho más flexibles a la hora de crear esquemas de información, lo que las convierte en una solución ideal para el almacenamiento y gestión de datos no estructurados o semiestructurados.
Rendimiento	Garantizan un alto rendimiento, ya que están diseñadas para trabajar con modelos de datos concretos y patrones de acceso específicos.

Funcionalidades	Son muy funcionales, ya que cuentan con API exclusivas y proporcionan modelos de datos para trabajar con cada tipo de datos presentes en la base.

Fuente: Elaborado por Autores

2.2.5. Sistemas de videovigilancia

La videovigilancia es el proceso en el que cámaras digitales, mediante la utilización de imágenes de video, en tiempo real o mediante grabaciones ayudan a la observación de eventos, personas o intrusiones a espacios no autorizados permitiendo así detectar y realizar alguna corrección si es necesaria.

Los dispositivos de videovigilancia son tecnología de punta que sirven para monitorear actividades que pueden causar situaciones peligrosas. Se trata de un sistema de tecnología de vigilancia visual que utiliza cámaras modernas, esto permite una instalación de vigilancia ciudadana en lugares públicos. Aproximadamente 6.500 cámaras de circuito cerrado de televisión se han instalado y están en funcionamiento en todo el país. (Ecu911, 2021)

Gracias a la evolución tecnológica las cámaras de videovigilancia permiten obtener imágenes de resoluciones excelentes que funcionan en diferentes entornos de iluminación y condiciones medioambientales adversas, estas cámaras adoptan protocolos de comunicación más rápidos y seguros que permiten una mejor administración para su análisis, como la implementación de algoritmos de detección de personas, objetos y eventos.

La utilización de un sistema de videovigilancia en empresas o instituciones permiten que tengan un registro visual de áreas o espacios en los que necesiten observar en tiempo real permitiendo al usuario tener control de este, los sistemas de videovigilancia se pueden dividir en dos clases que tienen sus propios dispositivos, tecnologías y características.

Los sistemas de videovigilancia están diseñados para proveer acceso de video desde cualquier locación de red ya sea remota o local, combina los beneficios analógicos del Circuito Cerrado de Televisión (CCTV) con las ventajas que ofrecen los sistemas digitales para el tratamiento digital de las imágenes, para usarlos en detección de escenarios, rostros, distanciamiento social entre otros.

Adema existen los sistemas CCTV o llamado Circuito Cerrado de Televisión es un sistema de videovigilancia en el que varios equipos están conectados generando imágenes para supervisar diversos ambientes y actividades que se orientan a la seguridad, vigilancia u otras

actividades. Generalmente el CCTV tiene la característica que todos sus componentes están conectados siendo un sistema pensado para un limitado número de personas.

- **Cámara Fija IP**

Las cámaras IP son el medio por el cual el centro de operaciones ECU911 hace el mejor trabajo para prevenir accidentes o emergencias. La ECU del 911 es capaz de integrar cámaras digitales a través de conexiones cableadas (principalmente fibra óptica) e inalámbricas (como WiMax). También tenga en cuenta que todos los videos se almacenan en el dispositivo de servicio hasta por 3 meses (Ecu911, 2021).

Figura 36. Ejemplo de cámara IP fija
Fuente: Cámaras IP (2017) Cámara Hikvision

Según Tecnitran (2019) Una cámara IP fija se combina con su propia minicomputadora, lo que le permite reproducir el video por sí solo.

- **Cámaras Esféricas o Domo PTZ**

Como menciona Teledyne (2021) las cámaras domo son conocidas por su diseño discreto y ecológico. Por lo general, tienen una base de metal y policarbonato que envuelve la cámara, por lo que la cámara no se puede manipular ni destruir.

Estas cámaras generalmente se montan en los techos de oficinas o pasillos comerciales para monitorear grandes áreas. Los materiales hemisféricos para proteger este tipo de cámaras oscurecen la lente y hacen imposible ver hacia dónde apunta la lente para una mejor decisión, como humo o sombras.

Figura 37. Ejemplo de cámara tipo DOMO
Fuente: Cámara IP (2017) 8 Megapíxel Domo exterior

Características de las cámaras DOMO PTZ

De acuerdo con Cámaras de vigilancia (2021) las cámaras esféricas o domo cuentan con las siguientes características:

- ✓ Su ruta difiere significativamente de la de los modelos de grabadoras de terceros. su estilo es similar y es excelente para todo tipo de espacios.
- ✓ Además, como grabador de IP, puede conectarse a Internet para transferir video y ver el video en cualquier lugar en el mismo momento.
- ✓ Este tipo de videocámaras de videovigilancia IP también se pueden utilizar en interiores.
- ✓ Suelen instalarse en el techo y cuentan con una funda de protección que, entre otras cosas, las hace más seguras y duraderas para evitar daños

- ➢ **Cámaras Lectoras de Placa**

Es una cámara IP con un sistema de reconocimiento de placas, cuenta con una resolución alta de imagen y video, lo que hace de esta cámara la mejor opción para sistemas de estacionamiento, calles, zonas residenciales. Su función es reconocer la matrícula del coche y dar un mejor control y seguridad (Securtech, 2019).

Su función es reconocer la matrícula del coche y dar un mejor control y seguridad. Estas cámaras para matrículas cuentan con una lente de zoom ajustable eléctricamente y una

velocidad de obturación de hasta 1/8000 segundos, lo que le permite tomar fotografías de cualquier tipo de vehículos (imasdetres, 2021).

Figura 38. Ejemplo de cámara lectora de placas
Fuente: SYSCOM (2018) Reconocimiento de matrículas con Hykvision

- ***DVR (Digital Video Recorder)***

o DVR es un dispositivo electrónico de grabación en formato digital generalmente usados en los circuitos cerrados de televisión, se utiliza para para guardar y visualizar las imágenes que están localizadas en un disco duro de gran capacidad, un DVR puede conectarse a monitores VGA, LCD, RCA, teniendo la capacidad de conexión a internet permitiendo visualizar las cámaras de la infraestructura de red.

Tal como lo explica Rojas (2017) Los sistemas de administración de señales de video y grabación comúnmente se conocen como DVR (Digital Video Recorder) para los sistemas de video análogo. Para proyectos o aplicaciones pequeñas el mismo DVR con un software que la mayoría de los fabricantes proveen junto con el equipo cumple las funciones de administración de video y de grabación

Figura 39. Ejemplo de grabador de video digital.
Fuente: Rojas (2017) DVR Típico Standalone

- ***Servidores NVR***

Un NVR puede ser un dispositivo físico o un software que se instala en una computadora. Estos dispositivos graban y gestionan las imágenes digitales enviadas por las cámaras de seguridad analógicas y cámaras IP a través de una red (Sosio, 2021).

Figura 40. Ejemplo de servidor NVR
Fuente: JMTelecom (2019) NVR rack hasta 64 canales

- **Par trenzado UTP**

También conocido como cable de par trenzado es un tipo de cable que posee dos conductores eléctricos aislados entre sí y entrelazados para anular frecuencias de fuentes externas y evitar la diafonía de los cables adyacentes, el tipo de cable UTP proviene de las siglas de *'Unshielded twisted pair'* que contiene pares trenzados sin blindar. Este tipo de cables es utilizado en sistemas CCTV cuando la longitud exceden los 200 metros.

Figura 41. Ejemplo de Cable UTP
Fuente: Telecu (2019) Cable UTP Indoor CAT5E

- **Fibra Óptica**

La fibra óptica se trata de un medio de transmisión de datos mediante impulsos fotoeléctricos a través de un hilo construido en vidrio transparente u otros materiales plásticos con la misma funcionalidad. Estos hilos pueden llegar a ser casi tan finos como un pelo, y son precisamente el medio de transmisión de la señal.

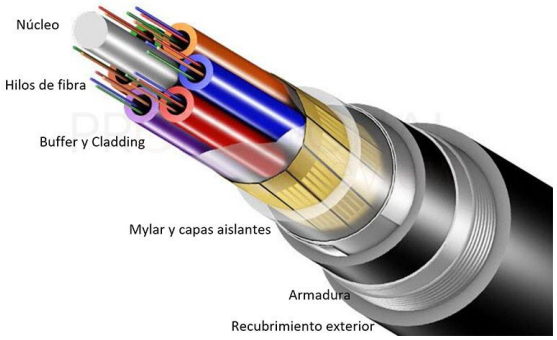


Figura 26. Ejemplo de Fibra Óptica
Fuente: Partes de un cable de fibra óptica por José Castillo 2018

- **Funcionamiento**

Al ser cables por los que viaja una señal luminosa, el modo de trasmisión no se basa en la transferencia de electrones a través de un material conductor. En este caso atendemos a los fenómenos físicos de la reflexión y refracción de la luz.

- **Tipos de fibra óptica y conectores**

En este caso debemos distinguir entre la fibra monomodo y la fibra multimodo. En la fibra monomodo, solamente se transmite un haz luminoso por el medio. Este haz será capaz de llegar, en el mejor de los casos hasta una distancia de 400 Km sin el uso de un repetidor, y se utiliza un láser de alta intensidad para generar este haz. Este haz es capaz de transportar hasta 10 Gbit/s por cada fibra.

En la fibra multimodo en cambio, se puede transmitir varias señales de luz por un mismo cable, que son generadas por LEDs de baja intensidad. Se usa para transmisiones de más corto alcance, siendo además más baratas y fáciles de instalar.

En cuanto a tipos de conectores de fibra óptica, podremos encontrar los siguientes:

- ✓ **SC:** Este conector es el que con mayor frecuencia veremos, ya que se utiliza para la transmisión de datos en conexiones de fibra monomodo. También existe una versión SC-Duplex que básicamente son dos SC unidos.

- ✓ **FC:** Este es otro de los más utilizados y tienen un aspecto similar a un conector de antena coaxial.
- ✓ **ST:** También es similar al anterior con un elemento central de unos 2,5 mm el cual está más expuesto.
- ✓ **LC:** En este caso el conector es cuadrado, aunque se mantiene el elemento central de igual configuración que los dos anteriores.
- ✓ **MT-RJ:** También es un conector dúplex y no se suele utilizar para fibras monomodo

- ➢ **Sistema Embebido**

Un sistema embebido (también conocido como "empotrado", "incrustado" o "integrado") es un sistema de computación diseñado para realizar funciones específicas, y cuyos componentes se encuentran integrados en una placa base (en inglés. "motherboard").

El procesamiento central del sistema se lleva a cabo gracias a un microcontrolador, es decir, un microprocesador que incluye además interfaces de entrada/salida, así como una memoria de tamaño reducido en el mismo chip.

Estructura de los sistemas embebidos

Los sistemas integrados varían en complejidad, pero, en general, constan de tres elementos principales:

- ✓ Hardware. El hardware de los sistemas integrados se basa en microprocesadores y microcontroladores. Los microprocesadores son muy similares a los microcontroladores y, por lo general, se refieren a una CPU (unidad central de procesamiento) que está integrada con otros componentes informáticos básicos, como chips de memoria y procesadores de señales digitales (DSP). Los microcontroladores tienen esos componentes integrados en un solo chip.
- ✓ Software y firmware. El software para sistemas integrados puede variar en complejidad. Sin embargo, los microcontroladores de grado industrial y los sistemas IoT integrados suelen ejecutar un software muy simple que requiere poca memoria.
- ✓ Sistema operativo en tiempo real. Estos no siempre se incluyen en los sistemas integrados, especialmente en los sistemas de menor escala. Los RTOS definen cómo funciona el sistema al supervisar el software y establecer reglas durante la ejecución del program

III. METODOLOGÍA

La metodología se puede entender como la manera en la que se realiza un proyecto investigativo. En ella, se definen los tipos de investigación, la modalidad de la investigación, los recursos que se emplean en el proyecto, entre otros, con el fin de establecer los principios o enfoques que se le otorgará al proyecto.

Para Niño Rojas (2011): "La metodología del proyecto incluye el tipo o tipos de investigación, las técnicas y los instrumentos que serán utilizados para llevar a cabo la indagación. Es el 'cómo' se realizará el estudio para el estudio para responder al problema planteado."

3.1. ENFOQUE METODOLÓGICO

3.1.1 Enfoque mixto

Esta investigación aplicó un enfoque mixto, porque hizo uso del paradigma cualitativo y cuantitativo. Cuantitativo porque la propuesta de desarrollo del software tiene las características de registrar, modificar, almacenar, administrar, controlar todos los datos. Cualitativo porque mediante uso de entrevistas se realizará el proceso y manejo de la información dentro del centro local para su posterior análisis y también tiene enfoque cualitativo debido a que se hará uso de entrevistas para recopilar información acerca del proceso del manejo de la información en el ECU 911 para su posterior análisis de información la cual está basado en una lógica y un proceso inductivo, es decir, explorar, describir y generar perspectivas propias de nuestra realidad.

Además, la aplicación posee las funcionalidades de otorgar información de la infraestructura tecnológica como lo son servidores y cámaras en el Ecu 911, por lo que existirá más posibilidades de interactuar con el mismo sistema e información generada.

3.1.2. Tipo de Investigación

Investigación exploratoria

Se considera este tipo de investigación como parte del proyecto, debido a que se realizará una indagación completa y profunda en varios medios de información, ya sea digital o físico, con las variables previamente definidas para abordar el problema planteado desde un punto de vista general.

Es así, como se comenzó con la realización del presente proyecto, explorando y familiarizándose con el objeto de estudio que en un principio era poco conocido, al acudir constante mente al lugar y dialogar de forma directa permitió comprender la problemática que existe en el Servicio Integrado de Seguridad ECU 911 al desconocer que cámara está en funcionamiento o con problemas, a su vez se pudo constatar las necesidades existentes y comprender los requisitos funcionales para el desarrollo de la aplicación, además, este tipo de investigación cimienta las bases para incluir el tipo de investigación descriptiva.

Investigación descriptiva

El tema de investigación maneja el tipo de investigación descriptiva debido a que se describen las características y la funcionalidad del software, su estructura y comportamiento. Adicional a esto, aporta con conocimientos que pueden servir de base para la mejora de softwares.

En la presente investigación se utilizó la investigación descriptiva porque se describieron todos los problemas o necesidades que tiene el Servicio Integrado de Seguridad ECU 911 además se describen los requisitos que debió cumplir el sistema de monitoreo en su desarrollo, también consta de diagrama de procesos, casos de uso.

Investigación Aplicada

Se utilizó la investigación aplicada en el desarrollo del presente proyecto debido a que se investigó en distintas fuentes cómo dar solución a nuestro problema y que herramientas de monitoreo se puede utilizar y esto permitió producir nuevos conocimientos que serán útiles para posteriores investigaciones, además fue utilizada porque utilizamos principios teóricos adquiridos en el transcurso de nuestra formación académica para generar conocimiento práctico y aplicarlo en la investigación.

Investigación Documental

La investigación documental se entiende como un proceso sistemático de indagación, recolección, análisis e interpretación de información en torno a un determinado tema.

La presente investigación tomo en cuenta la investigación documental como parte fundamental para la recolección de información con relación al objeto de estudio, por lo cual se utilizó repositorios, tesis, libros, artículos que permitan comprender la problemática y

como dar solución al problema, ademas pertimitió respaldar bibliograficamente el desarrollo de la documentación.

3.2. Idea a defender

El uso de una herramienta de monitoreo de datos para la infraestructura tecnológica optimiza el manejo de información en el Sistema Integrado de seguridad ECU 911

3.3. DEFINICIÓN Y OPERACIONALIZACIÓN DE VARIABLES

3.3.1. Definición de las variables

3.3.1.1. Herramientas de monitoreo (Variable Independiente)

Son sistemas de diagnóstico para telecomunicaciones, servidores o redes que buscan componentes defectuosos o lentos, con el fin de informar a los administradores mediante correo electrónico, SMS, entre otros.

3.3.1.2. Infraestructura tecnológica (Variable Dependiente)

Es el conjunto de sistemas (ordenadores, equipos de electrónica de red, equipos de almacenamiento, y demás elementos físicos) que tiene una institución o empresa.

Tabla 9. Definición y Operacionalización de variable independiente

	Variable	Definición	Dimensión	Indicador	Técnica	Instrumento
Variable Independiente	Herramienta de Monitoreo	Las herramientas de monitoreo son sistemas de diagnóstico que se utilizan en telecomunicaciones, servidores o redes para encontrar componentes defectuosos, lentos o que hayan sufrido alguna desconexión	Tipo de Monitoreo	• Táctica • Grupal • SNMP • Agente	Encuesta	Cuestionario
			Tipo de Alerta	• Estado Crítico (0) • Estado Normal (1)	Encuesta	Cuestionario
			Tipo de Informe	• Diario • Semanal • Mensual	Encuesta	Cuestionario

Tabla 10. Definición y Operacionalización de variable dependiente

	Variable	Definición	Dimensión	Indicador	Técnica	Instrumento
Variable Dependiente	Infraestructura tecnológica	Es el conjunto de sistemas (ordenadores, equipos de electrónica de red, equipos de almacenamiento, y demás elementos físicos) junto con la manera que se ha elegido para gestionarlos.	Cámaras Ip	• Tipo de Cámara • Conectividad • Banda Ancha	Encuesta	Cuestionario
			Servidores	• Conexión • Tiempo de Respuesta • Espacio en memoria	Encuesta	Cuestionario

Fuente: Autoría propia

La tabla muestra las variables de investigación y la implicación de los instrumentos e indicadores con el proyecto

3.4. METODOS UTILIZADOS

3.4.1. Método Analítico

En la presente investigación se utilizó el método analítico porque permitió analizar los procesos que fueron necesarios, se hizo un análisis sobre las herramientas de monitoreo de datos, metodología de desarrollo, también para la gestión de una herramienta de monitoreo se realizó un cuadro comparativo sobre las diferentes opciones dentro del mundo del monitoreo y analizar una por una las diferentes herramientas y luego del posterior análisis se elegio el que más se adapte a las necesidades.

3.4.2. Método Inductivo

El método inductivo fue importante en la investigación porque permitió acudir al Servicio Integrado de Seguridad ECU 911Tulcán y mediante la observación, entrevistas y encuestas se logró comprender el funcionamiento de cada una de las áreas, además conocer la problemática de forma directa y las necesidades que poseen, de acuerdo a la información obtenida se procedió a investigar en diferente fuentes como dar solución a la problemática planteada, para ello con los conocimientos obtenidos durante la etapa de estudio sobre tecnología permitió tener una visión general de herramienta de monitoreo de datos que se desea desarrollar

3.4.3. Método Deductivo

Se utilizó el método deductivo para la recopilación de información sobre el objeto de estudio, para ello se recolecto información similar a nuestra problemática, luego se procedió a categorizarla de acuerdo con las necesidades, esto permitió comprender y tomar decisiones en el desarrollo de la investigación, esto contribuye a una mejor comprensión sobre los problemas que se ocasionan al estar una cámara dañada y desconocer el hecho.

3.5. ANALISIS ESTADISTICO

Mediante los instrumentos utilizados para la obtención de información se utilizó un banco de preguntas semiestructuradas, cuestionarios los cuales sirvieron de guía para conocer de forma clara la situación en la que se encontraba nuestro objeto de estudio, obteniendo como resultado la comprensión del problema y las necesidades de la institución.

3.5.1. Técnicas e instrumentos

Para la recolección de información del tema de estudio se utilizó diferentes técnicas que permitieron fortalecer y aclarar las interrogantes, para ello se aplicó entrevistas, ficha de

observación, encuestas las cuales aportaron información verídica sobre la problemática existente, conocer los requerimientos funcionales de la solución informática.

Encuesta

Al área de tecnología y gerencia se les aplicó una encuesta con la finalidad de recolectar información para la presente investigación y medir las relaciones que tienen entre las variables de estudio que son las herramientas de monitoreo de datos y la infraestructura tecnológica para tomar decisiones acerca del desarrollo de la propuesta tecnológica.

3.5.2. Población

Debido a que los funcionarios que intervendrán en el estudio de la herramienta de monitoreo de datos es un número manejable, en la presente investigación la población se determinó el área de tecnología y administrativa como la población escogida para el censo.

La población de la presente investigación son 4 funcionarios los cuales están conformados por dos áreas en específico, la más importante es el área de tecnología y la segunda es el área de administración o gerencia. Ya que estas áreas son las encargadas de brindarnos la suficiente información a nuestro objeto de estudio.

Tabla 11. Población y muestra de la investigación

Censo	Funcionarios	Técnica
Área de Tecnología	3	Encuesta
Área de Administración	1	Encuesta

Fuente: Elaborado por autores

En la tabla 14 se describe las áreas y los funcionarios que participan en el censo que se realizara en el Sistema Integrado de Seguridad Ecu 911.

Tabla 12. Temas y número de preguntas encuesta Ecu área de tecnología Ecu 911

Temas de discusión	Número de preguntas	Instrumento
Herramientas de monitoreo	4	Cuestionario
Infraestructura tecnológica	2	Cuestionario
Cámaras IP	2	Cuestionario
Total	8	

Fuente: Elaborado por autores.

IV. RESULTADOS Y DISCUSIÓN

4.1. RESULTADOS

4.1.1.1 Resultados de la encuesta

Preguntas

1. **¿Cuándo una cámara o un servidor presenta alguna falla o desconexión el área de tecnología cuenta con algún proceso ya preestablecido?**

Existe un proceso llamado GLPI el cual consiste en administrar el área de tecnología mediante informes vía web.

Análisis: Tal cual nos menciona la ingeniera María José si existe un proceso de verificación de cámaras el cual es de gran ayuda al momento de desarrollar el aplicativo ya que nos servirá de guía para lograr una conexión con los registros de todas las cámaras funcionales y no funcionales del centro operativo Ecu 911.

2. **¿El centro local cuenta con una guía para el proceso de instalación de cámaras IP?**

Desde el centro de operaciones a nivel nacional envían un manual de instalación, gracias a este podemos dar de alta las cámaras y servidores disponibles en el centro local.

Análisis: En este caso como podemos observar el centro local cuenta con manuales de instalación para sus diferentes aplicativos, gracias a esto los diferentes integrantes del área de tecnología realizan la subida y posterior gestión de los diferentes periféricos existentes dentro del Ecu 911.

3. **¿El centro local cuenta con un servicio o herramienta específica para el control y monitoreo de cámaras y servidores?**

Actualmente el centro local cuenta con un aplicativo web llamado Cacti, pero no funciona de manera óptima ya que no está configurado ni cuenta con las diferentes extensiones necesarias para su adecuado funcionamiento.

Análisis: Tal como mencionan en la entrevista tener configurada de manera óptima y con todas sus dependencias la herramienta Cacti puede ayudar al monitoreo y la gestión de dispositivos, mediante la cual es posible verificar mediante los diferentes servicios el estado y funcionamiento de las cámaras.

4. **¿El software que utilizan para el monitoreo de dispositivos cuenta con un visualizador gráfico?**

Dentro del centro local contamos con la herramienta de monitoreo llamada Cacti, la cual nos ayuda a supervisar las cámaras y esta cuenta con un apartado gráfico que es de gran ayuda al momento de revisar las cámaras.

Análisis: Tal y como mencionan los entrevistados contar con una herramienta que tenga incorporado un sistema de visualización es de gran ayuda ya que los administradores podrán identificar con mayor exactitud el momento en el cual una cámara se cae o sufre una conexión.

5. **¿Como manejan los registros de cámaras y servidores caídos?**

Los reportes se manejan de manera manual por medio de informes diarios en el cual se detallan las cámaras y servidores en buen estado y caídos.

Análisis: Contar con un registro de cámaras y servidores de manera manual en la actualidad se lo puede tomar como una manera no tan eficiente.

6. **¿El área de tecnología cuenta con una base de datos dedicada a las cámaras y servidores?**

Para cámaras y servidores el área de tecnología cuenta con una base de datos general que es controlada por el centro nacional Ecu 911, en nuestro caso solo podemos registrar las cámaras.

Análisis: Para cualquier institución u organización es indispensable contar con un respaldo de la información generada de manera periódica.

ANÁLISIS DE LA ENCUESTA

Pregunta 1.

¿Está de acuerdo que el área de tecnología cuente con servicios para el monitoreo de datos de dispositivos tecnológicos?

Tabla 10.Tabla acerca de los resultados acerca de los servicios de monitoreo de datos.

Opciones	Respuesta	Porcentaje
Muy de acuerdo	4	100%
De acuerdo	0	0%
Ni de acuerdo ni en desacuerdo	0	0%

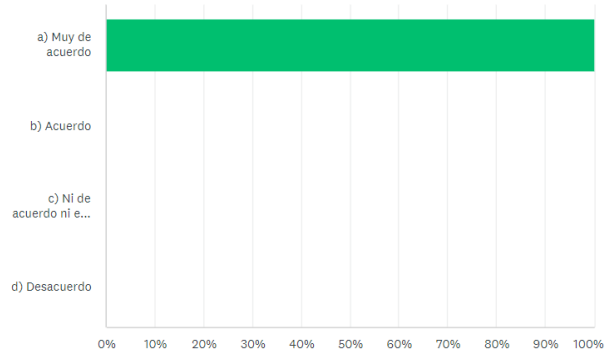


Figura 42. Servicios de monitoreo dentro del ECU 911

Fuente: Elaboración de autores

Análisis: Con lo que respecta a esta pregunta la mayoría de encuestados coincidieron en sus respuestas, esto quiere decir que ellos están de acuerdo que un servicio de monitoreo de herramientas tecnológicas será de gran ayuda en el ecu 911.

Pregunta 2.

¿Cuál es el promedio de cámaras IP que operan en la infraestructura tecnológica?

Tabla 11. Resultado de promedio de cámaras IP funcionales en el ECU 911

Opciones	Respuesta	Porcentaje
De 10 a 50	1	25%
De 100 a 200	3	75%
Mas de 200	0	0%

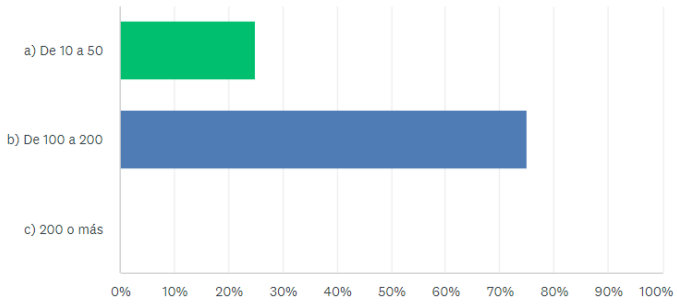


Figura 43. Resultados cámaras IP

Fuente: Elaboración de autores

Análisis: En este caso podemos notar un alto porcentaje de coincidencia en la opción de 100 a 200 cámaras por lo deducimos que el centro cuenta con más de 100 cámaras funcionales en toda la provincia.

Pregunta 3.

¿Conoce usted herramientas web que permitan monitorear dispositivos tecnológicos cada que sufren una desconexión?

Tabla 12. Resultados de herramientas web de herramientas de monitoreo

Opciones	Respuesta	Porcentaje
Si	**1**	**25%**
No	**3**	**75%**
No estoy seguro	**0**	**0%**

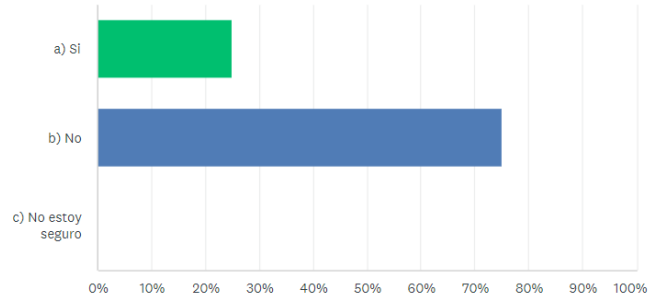


Figura 44. Resultado de monitoreo de dispositivos

Fuente: Elaboración de autores

Análisis: En esta pregunta logramos observar que la mayoría de encuestados tienen conocimientos acerca de aplicaciones que monitorean dispositivos y alertan sobre posibles fallas, por otro lado, solo una persona encuestada desconoce sobre estas aplicaciones.

Pregunta 4.

¿Cómo se reportan los errores que tienen las cámaras o servidores del centro local?

Tabla 13. Resultado de reportes de errores de dispositivos tecnológicos.

Opciones	Respuesta	Porcentaje
Escritura manual	0	0%
Digital (Computadora)	3	100%

Otros	0	0%

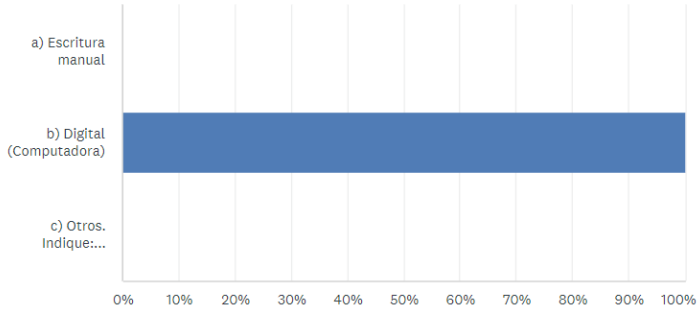


Figura 45. Reportes de cámaras caídas

Fuente: Elaboración de autores

Análisis: Como podemos observar en el gráfico el 100 % de encuestados coinciden que el registro de cámaras caídas se lo realiza de manera digital, esto nos ayuda a extraer información de cada dispositivo.

Pregunta 5.

¿Con que frecuencia se reportan los errores o caídas de cámaras o servidores?

Tabla 14. Resultado de frecuencia de reportes de errores

Opciones	**Respuesta**	**Porcentaje**
Mensual	1	25%
Semanal	0	0%
Diaria	3	75%
Otros	0	0%

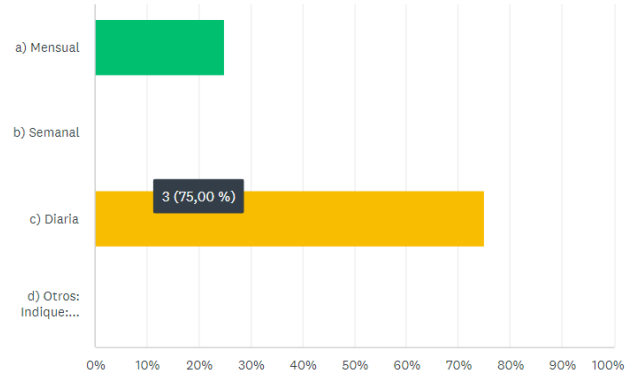


Figura 46. Frecuencia de reporte de errores

Fuente: Elaboración de autores

Análisis: Con respecto a esta pregunta la mayoría de encuestados supieron manifestar que la frecuencia con la que reportan las cámaras se realiza de manera diaria, aunque en ocasiones las realizan de manera mensual.

Pregunta 6.

¿Cuál cree que es la importancia de una herramienta de monitoreo de datos para el beneficio de la gestión administrativa?

Tabla 15. Resultados importancia de la herramienta de monitoreo de datos

Opciones	Respuesta	Porcentaje
Muy importante	3	75%
Importante	1	25%
Neutral	0	0%
Nada importante	0	0%

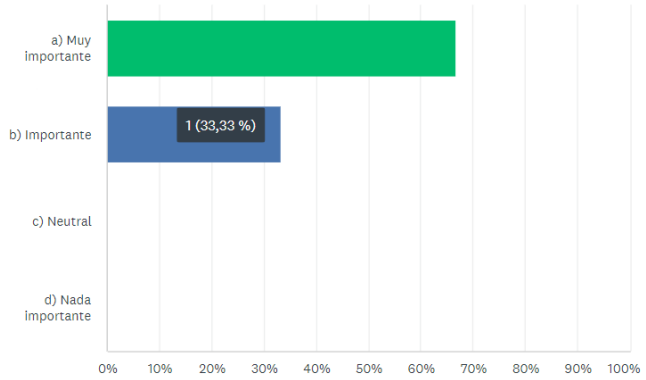


Figura 47. Importancia de una herramienta de monitoreo de datos

Fuente: Elaboración de autores

Análisis: En este caso podemos observar que la mayoría de encuestados coinciden que una aplicación de monitoreo de datos puede ser muy importante en la gestión de dispositivos ya que facilitaran el control y la gestión de las diferentes cámaras y dispositivos dentro del centro local. Por otro lado, solo una persona encuestada cree que la utilización de una aplicación de monitoreos de daros es importante para la gestión de dispositivos en el ecu 911.

Pregunta 7.

¿Cuál de las siguientes herramientas se utiliza dentro del Ecu 911?

Tabla 16. Uso de herramientas de monitoreo de datos en el ECU 911

Opciones	Respuesta	Porcentaje
Cacti	1	33.33 %
Nagios	1	33.33 %
Pandora	1	33.33 %
Kali Linux	0	0
GroudWork	0	0
Zenoss	0	0
Op5 Monitor	0	0

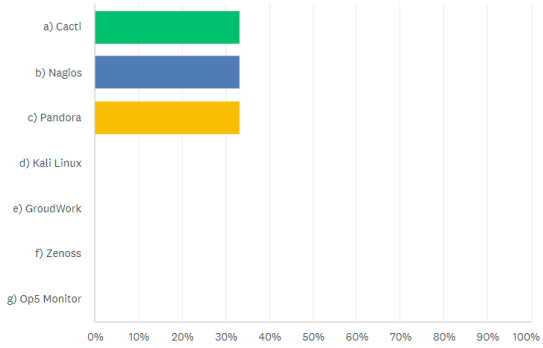


Figura 48. Herramientas de monitoreo en el ECU 911

Fuente: Elaboración de autores

Análisis: En esta pregunta cómo podemos observar cada encuestado eligió una herramienta de monitoreo distinta, esto nos lleva a suponer que el centro local cuenta con tres herramientas de monitoreo, las cuales nos pueden servir para el desarrollo del aplicativo.

Pregunta 8.

¿El Ecu 911 cuenta con un registro o base de datos del historial de las cámaras o servidores caídos?

Tabla 17. Resultado de registro de base de datos

Opciones	Respuesta	Porcentaje
Si	4	100 %

No	0	0 %

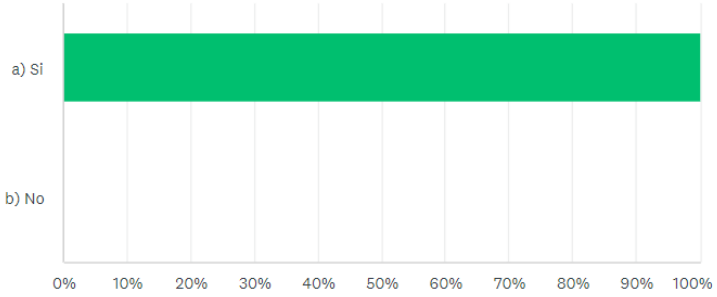


Figura 49. Registro de base de datos dentro del ECU 911

Fuente: Elaboración de autores

Análisis: Con respecto a esta pregunta el 100 % de encuestados coinciden que el ecu 911 cuenta con un registro de base de datos para las cámaras y servidores caídos, lo que nos beneficia ya que tendremos un archivo de apoyo para poder recolectar la información de cámaras y servidores caídos.

4.1.1.2 Propuesta

La propuesta se elaboró a partir del análisis de los resultados de la investigación y de un primer

acercamiento con los encargados del área tecnológica y administrativa, los cuales manifestaron la necesidad de contar con un software que verifique el estado de las cámaras existentes dentro del Servicio de Seguridad Ecu 911, por otro lado, los datos obtenidos de la encuesta dictan que es necesario implementar una herramienta de monitoreo de datos que verifique en tiempo real el estado y la ubicación de las cámaras como también un reporte visual generado periódicamente.

todas las fases correspondientes hasta concluir con las pruebas de aceptación que dan como resultado que el beneficiario se encuentra satisfecho con el producto entregado.

4.1.1.3. Factibilidad Organizacional.

- **Aspectos generales de la organización.**
  - **Institución:** Servicio Integrado de Seguridad Ecu 911
  - **Ubicación geográfica:** Tulcán, Calle Ricardo Descalzi, entre Alejandro Carrión y Agustín Cueva Tamariz
  - **Área:** Área de Tecnología

- **Sistema:** Herramienta de monitoreo de datos para infraestructura tecnológica en el Ecu 911
- **Objeto social:** Servicio público

Misión

"Gestionar en todo el territorio ecuatoriano, la atención de las situaciones de emergencia de la ciudadanía, reportadas a través del número 911, y las que se generen por video vigilancia y monitoreo de alarmas, mediante el despacho de recursos de respuesta especializados pertenecientes a organismos públicos y privados articulados al sistema, con la finalidad de contribuir, de manera permanente, a la consecución y mantenimiento de la seguridad integral ciudadana".

Visión

"Ser una institución nacional líder y modelo en la región para la coordinación de servicios de emergencia utilizando tecnología de punta en sistemas y telecomunicaciones, comprometidos con la calidad, seguridad, salud en el trabajo y el medio ambiente que permitan brindar un servicio único y permanente a la ciudadanía".

4.1.1.4. Factibilidad Técnica.

Para el desarrollo de este proyecto se elaboró una lista de los recursos que serán utilizados, tales como el hardware y software. La herramienta de monitoreo de datos se instaló y configuro dentro de un Kernel Linux y una base de datos MySQL, estos recursos fueron elegidos por ser Open Source, esto es un beneficio al no generar ningún costo en la investigación, añadiendo a ello se cuenta con los conocimientos necesario para su implementación.

Tabla 18. Recursos Software

Tipo de recurso	Nombre	Descripción	Cantidad
Software	Pandora FMS	Herramienta de monitoreo	1
	MySQL	Base de datos	1
	Packet Tracer	Software de simulación de redes	1
	Microsoft Office	Herramienta Ofimática	1

Fuente: Elaborado por Autores

Los investigadores cuentan con los equipos necesarios para el desarrollo del proyecto, además de una conexión a internet lo que facilita la comunicación en el equipo de trabajo, la organización dispone actualmente con un servidor y la infraestructura de red necesaria, se concluye que los recursos son aptos y existe una factibilidad técnica.

Tabla 19. Recursos Hardware

Tipo de recurso	Nombre	Descripción	Cantidad
Hardware	Equipo de Computación	Laptop HP OMEN 15 Laptop Gaming Acer Nitro	2
	Servidor	Dell T30 CPU E3	1
	Cámara Domo	Cámara de videovigilancia CIEC	1
	Router	Cisco C2951	1
	Switch	Cisco Catalyst 2960	1

Fuente: Elaborado por Autores

4.1.1.5. Factibilidad Operativa.

- **Situación actual**

En el Servicio Integrado de Seguridad Ecu 911 el almacenamiento del estado de conexión de las cámaras se registra de manera manual mediante el Software Excel, lo que dificulta verificar de manera inmediata las diferentes disposiciones. Lo que genera retraso en el mantenimiento de los diferentes dispositivos tecnológicos.

El área de tecnología no cuenta con métodos de almacenamiento adecuados. Los trámites correspondientes para la verificación manual de las cámaras resultan complejos para el personal de tecnología, puesto que necesitan estar presentes en el lugar donde se ubica la cámara para verificar el estado en tiempo real.

- **Situación ideal**

La herramienta de monitoreo de datos para infraestructura tecnológica va a verificar el estado de las diferentes cámaras que operan dentro del Ecu 911. Lo que permite centralizar la información y facilitar la gestión y mantenimiento de cada una de ellas. Por parte de la administración se cuenta con el apoyo necesario y se va a trabajar de forma coordinada con el jefe del área de tecnología para obtener los requerimientos necesarios que cumplan con las funcionalidades específicas de la herramienta.

4.1.1.2 Metodología de Red Top-Down

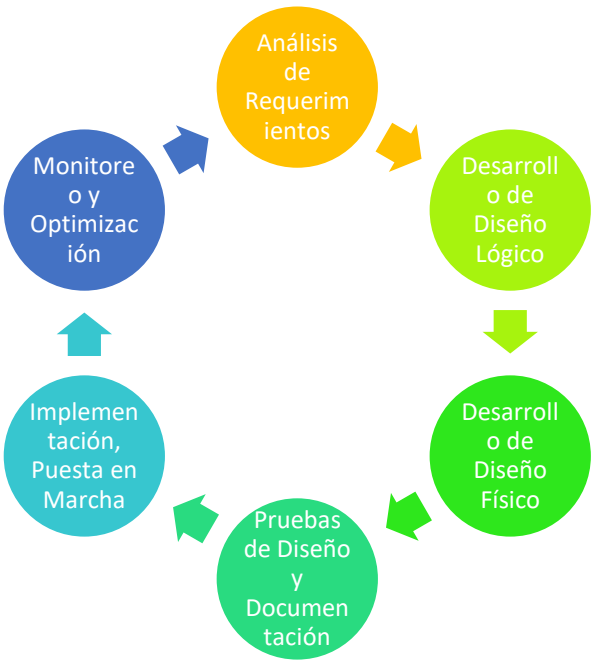


Figura 50. Metodología de red: Top-Down
Fuente: Elaboración de los autores.

Descripción de la metodología

El enfoque de arriba hacia abajo de Cisco tiene como objetivo diseñar redes de datos basadas en un modelo jerárquico e integrado. Esta metodología proporciona un proceso que permite identificar flujos y plantear problemas para su solución. Es importante cumplir con los requisitos técnicos, para lograr una funcionalidad, disponibilidad, escalabilidad, accesibilidad y seguridad óptimas.

4.1.2. Fase 1: Analizar Requerimientos

4.1.2.1. Estructura Organizacional Ecu 911 (Nacional, Zonal, Local)

Dirección Nacional

Actualmente el SIS ECU 911 tiene presencia en todo el territorio nacional con 7 Centros Zonales, 9 Centros Locales y 14 Salas operativas.

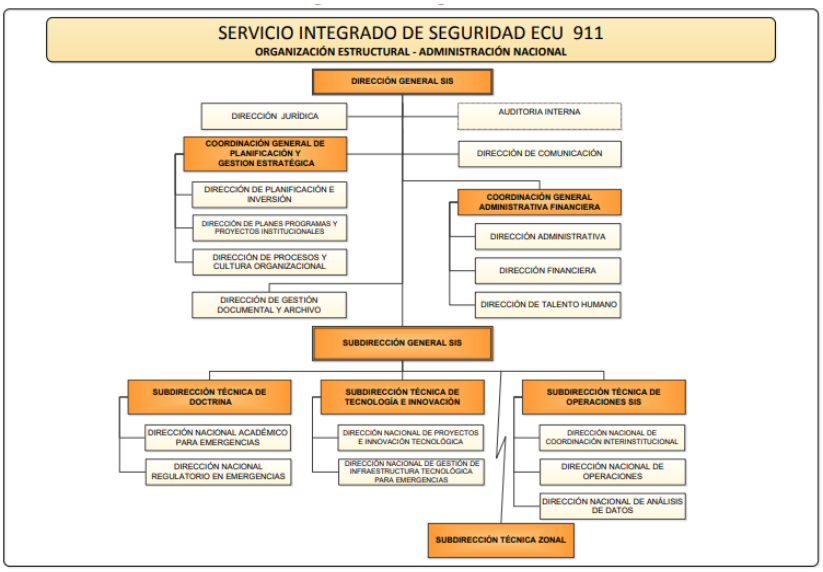


Figura 51. Administración Nacional Ecu 911
Fuente: Plan Estratégico 2020-2021 Ecu 911

Subdirección Técnica Zonal

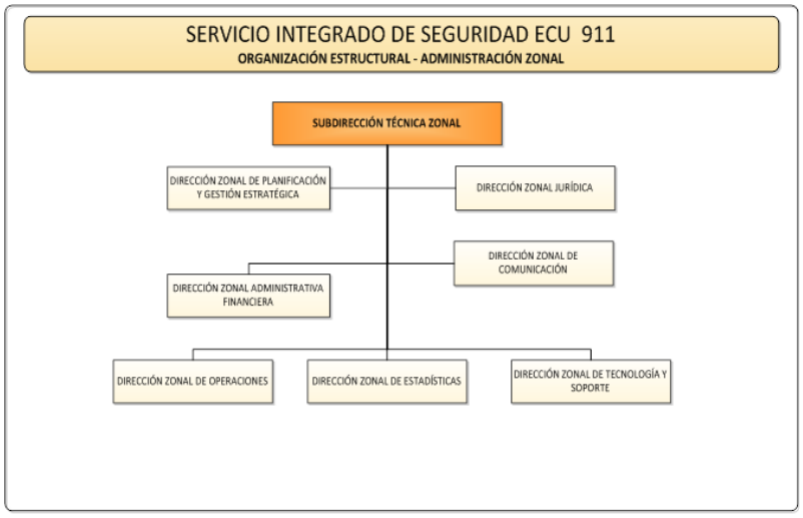


Figura 52. Subdirección Técnica Zonal
Fuente: Plan Estratégico 2020-2021 Ecu 911

La presencia en general de varios centros por zona surge con la finalidad de incidir en áreas de mayor atención de emergencias, necesidad que tienen las ciudades debido al tamaño de su población, así como fortalecer la seguridad en zonas de frontera; en tal virtud, éstos se han ubicado estratégicamente en base de un análisis minucioso e investigación con el fin de atender necesidades particulares en materia de seguridad.

Centro Operativo Local

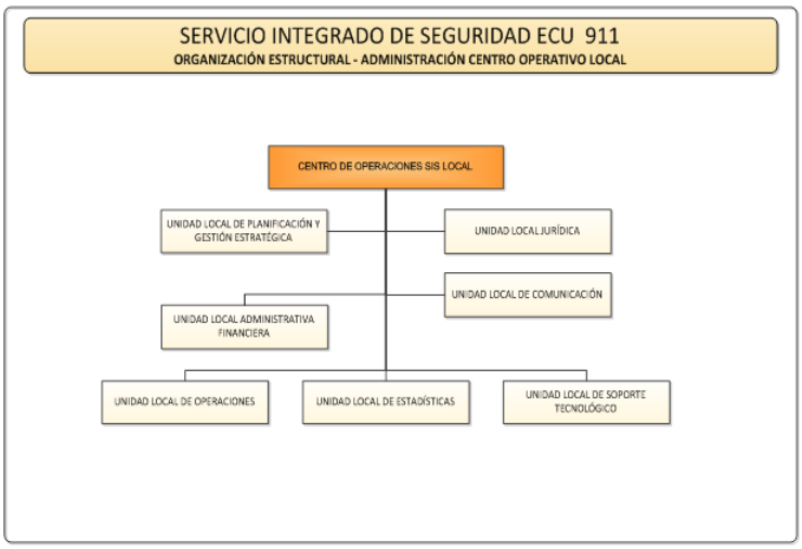


Figura 53. Centro Operativo Local
Fuente: Plan Estratégico 2020-2021 Ecu 911

Esta estructura no corresponde a un nivel de desconcentración, sino a una presencia a nivel territorial para la prestación de los servicios a nivel local, la misma que será coordinada a nivel zonal.

La organización estructural a nivel local se encuentra conformado por:

- **Centro Operativo Local**

Tiene como misión dirigir, controlar y mejorar continuamente la prestación del Servicio Integrado de Seguridad ECU 911 a nivel local como herramienta para garantizar el derecho de los habitantes a la seguridad integral establecido en la Constitución de la República.

- **Gestión Local de Soporte Tecnológico**

Tiene como misión controlar la eficiente operación de la infraestructura tecnológica base para el Servicio Integrado de Seguridad ECU 911 a nivel local.

4.1.2.3. Análisis de Requerimientos

En la fase de análisis del presente proyecto se realizó ciertas entrevistas a la Ing. Sistemas Informáticos, María José Argoti encargada del departamento informático del Ecu 911,

además se realizó ciertas encuestas para determinar las necesidades y las respectivas herramientas tienen en dicho laboratorio.

Como se puede apreciar en el gráfico los operarios que manejan las cámaras cada que sufren una desconexión, tienen que notificar por medio de un gestor de correo la cual desemboca en que el área de tecnología reciba esta solicitud con un retraso considerable de tiempo.

Representación 1 (Gestión de caída de cámaras)

Figura 54. Operaciones en ECU 911

Otro inconveniente que existe es la falta de una base de datos que recopile información de los sucesos como caídas, desconexiones o errores que tienen los dispositivos con su fecha y hora, así pues, el equipo de administración es muy difícil hacer una estadística de los puntos más frecuentes en los que ocurren estos incidentes.

Representación 2 (Base de datos Ecu 911)

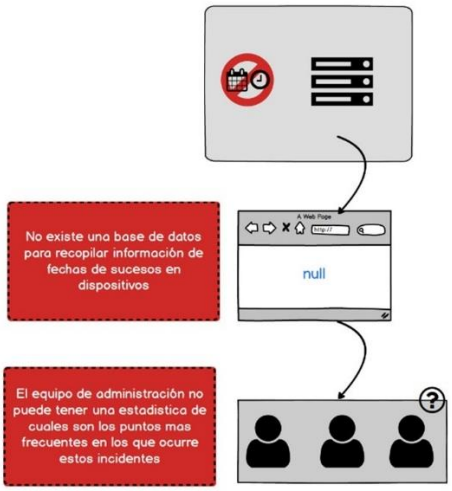


Figura 55. Registro de base de datos de errores de cámaras

En la gráfica se resume que un problema es que el gerente no puede acceder a la información de dispositivos funcionando actualmente sin la intervención del equipo de tecnología lo que es un inconveniente ya que en horarios no laborales o vacaciones no se puede acceder a esta información para hacer reportes, informes o exposiciones.

Representación 3 (Acceso a la información)

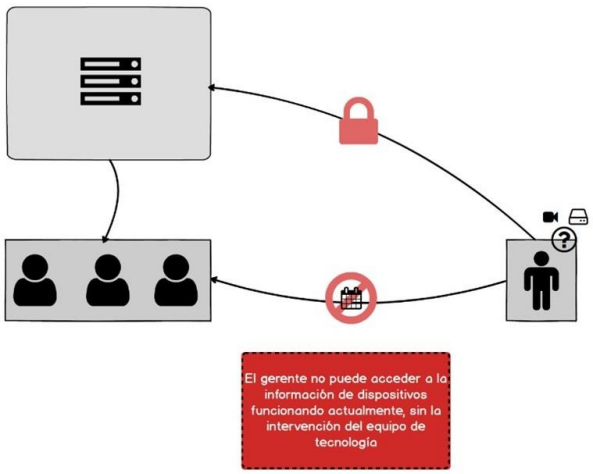


Figura 56. Acceso a la información de gerente

Gestión de Cámaras caídas

El manejo de las cámaras cuando estas no estén en funcionamiento o presente un desperfecto en pleno funcionamiento, el aplicativo tendrá la funcionalidad de mostrar notificaciones cuando la cámara deje de funcionar y mostrara los respectivos detalles.

Representación 4 (Gestión de cámaras caídas)

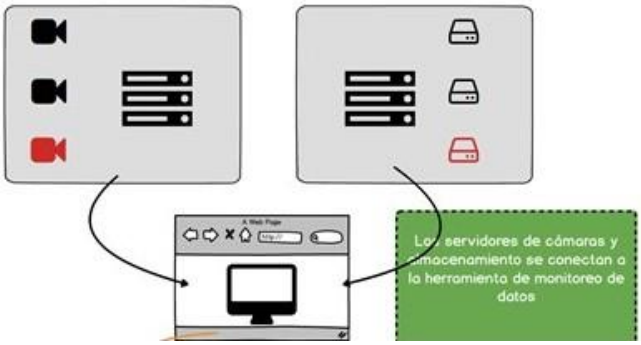


Figura 57. Gestión de la herramienta de monitoreo
Fuente: Elaboración de los autores.

4.1.2.4. Requerimientos para el Sistema de monitoreo

En la siguiente tabla se detalla los requerimientos funcionales para el desarrollo del proyecto:

Tabla 18. Requerimientos funcionales del proyecto

Identificación del Requerimiento	Requerimientos	Descripción
RF1	Iniciar sesión	Usuarios realizaran el ingreso con sus respectivas credenciales.
RF2	Listar	Listar cámaras por cada Cantón y su respectiva característica.
RF3	Notificar	Se realizará la notificación sobre la baja o la caída de las cámaras del sistema ECU 911.
RF4	Visualizar	Visualizar el estado en tiempo real de las cámaras del Ecu 911.
RF5	Informar	Contar con un sistema de informes periódicamente establecidos.

Fuente: Elaborado por Autores

4.1.3. Fase 2: Desarrollar Diseño Lógico.

Para realizar el diseño lógico de este proyecto se utiliza el programa Packet Tracer en su versión 8.1.1 (https://www.netacad.com/es). Se implementa un rango de clase C en la provincia del Carchi con una Ip Privada de red. Se opta por estas máscaras de subred porque se adecuan a las necesidades y naturaleza de los departamentos. Se habilita una conexión entre router y Hub en modo TRUNK (TRONCAL), para soportar el tráfico de todas las cámaras que pasan en el mismo todos los dispositivos están conectados al servidor en el que está instalado la herramienta de monitoreo de datos Pandora FMS para así poder verificar el estado de los dispositivos conectados a la infraestructura de red.

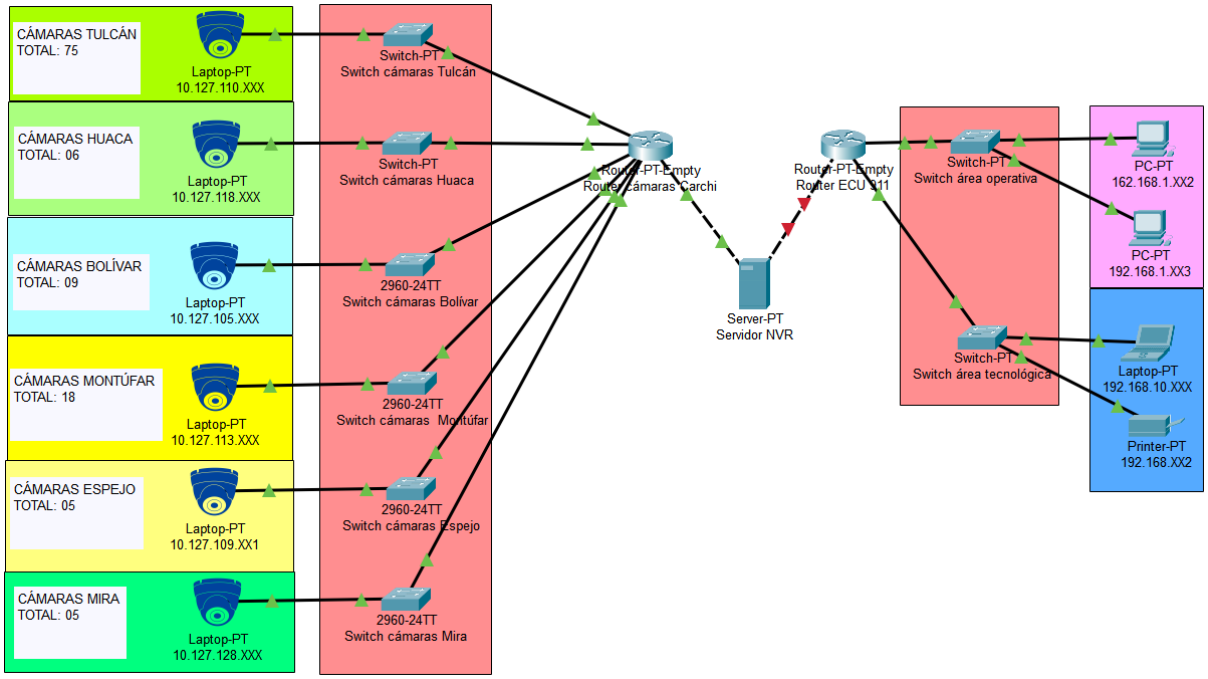


Figura 58. Propuesta diseño lógico

Fuente: Software Cisco Packet Tracer vers. 8.1.1

4.1.3.1 Direccionamiento y Hostname

Para la topología de red de las cámaras del Sistema Integrado Ecu 911 se ha tomado en cuenta las direcciones IP las cuales sirven para la configuración en el servidor Pandora FMS.

Tabla 19. Enrutamiento de Puertos de Cámaras Ecu 911

Cámara	Sistema Operativo	Dirección IP	Máscara de Red	Gateway por Defecto
PHUA-1	Embedded	10.127.118.XX	255.255.255.0	10.127.XX
PHUA-2	Embedded	10.127.118.XX	255.255.255.0	10.127.XX
PHUA-3	Embedded	10.127.118.XX	255.255.255.0	10.127.XX
PHUA-4	Embedded	10.127.118.XX	255.255.255.0	10.127.XX
PHUA-5	Embedded	10.127.118.XX	255.255.255.0	10.127.XX

Fuente: Elaborado por Autores

Cámaras Ecu 911 Cantón Bolívar

Tabla 20. Enrutamiento de Puertos de Cámaras Ecu 911 (Bolívar)

Cámara	Sistema Operativo	Dirección Ip	Máscara de Red	Gateway por Defecto
CBOLI-1	Embedded	10.127.101.XX	255.255.255.0	10.127.XX
CBOLI-2	Embedded	10.127.101XX	255.255.255.0	10.127.XX
CBOLI-3	Embedded	10.127.101.XX	255.255.255.0	10.127.XX
CBOLI-4	Embedded	10.127.101.XX	255.255.255.0	10.127.XX
CBOLI-5	Embedded	10.127.101.XX	255.255.255.0	10.127.XX
CBOLI-6	Embedded	10.127.101.XX	255.255.255.0	10.127.XX
CBOLI-7	Embedded	10.127.101.XX	255.255.255.0	10.127.XX
CBOLI-8	Embedded	10.127.101.XX	255.255.255.0	10.127.XX
CBOLI-9	Embedded	10.127.101.XX	255.255.255.0	10.127.XX

Fuente: Elaborado por Autores

Cámaras Ecu 911 Cantón Mira

Tabla 21. Enrutamiento de Puertos de Cámaras Ecu 911 (Mira)

Cámara	Sistema Operativo	Dirección Ip	Máscara de Red	Gateway por Defecto
MIR-1	Embedded	10.127.109.XX	255.255.255.0	10.127.XX
MIR-2	Embedded	10.127.109.XX	255.255.255.0	10.127.XX
MIR-3	Embedded	10.127.109.XX	255.255.255.0	10.127.XX

MIR-4	Embedded	10.127.127.XX	255.255.255.0	10.127.XX
MIR-5	Embedded	10.127.127.XX	255.255.255.0	10.127.XX
MIR-6	Embedded	10.127.109.XX	255.255.255.0	10.127.XX

Fuente: Elaborado por Autores

Cámaras Ecu 911 Cantón Espejo

Tabla 22. Enrutamiento de Puertos de Cámaras Ecu 911 (Espejo)

Cámara	**Sistema Operativo**	**Dirección Ip**	**Máscara de Red**	**Gateway por Defecto**
ESPE-1	Embedded	10.127.105.XX	255.255.255.0	10.127.XX
ESPE-2	Embedded	10.127.105.XX	255.255.255.0	10.127.XX
ESPE-3	Embedded	10.127.105.XX	255.255.255.0	10.127.XX
ESPE-4	Embedded	10.127.128.XX	255.255.255.0	10.127.XX
ESPE-5	Embedded	10.127.128.XX	255.255.255.0	10.127.XX
ESPE-6	Embedded	10.127.105.XX	255.255.255.0	10.127.XX
ESPE-7	Embedded	10.127.105.XX	255.255.255.0	10.127.XX
ESPE-8	Embedded	10.127.105.XX	255.255.255.0	10.127.XX
ESPE-9	Embedded	10.127.105.XX	255.255.255.0	10.127.XX
ESPE-10	Embedded	10.127.105.XX	255.255.255.0	10.127.XX
ESPE-11	Embedded	10.127.105.XX	255.255.255.0	10.127.XX

Fuente: Elaborado por Autores

Cámaras Ecu 911 Cantón Montúfar

Tabla 23. Enrutamiento de Puertos de Cámaras Ecu 911

Cámara	**Sistema Operativo**	**Dirección Ip**	**Máscara De Red**	**Gateway por Defecto**
MON-1	Embedded	10.127.113.XX	255.255.255.0	10.127.XX
MON-1	Embedded	10.127.113.XX	255.255.255.0	10.127.XX
MON -3	Embedded	10.127.113.XX	255.255.255.0	10.127.XX
MON -4	Embedded	10.127.113.XX	255.255.255.0	10.127.XX
MON -5	Embedded	10.127.113.XX	255.255.255.0	10.127.XX
MON-6	Embedded	10.127.113.XX	255.255.255.0	10.127.XX
MON -7	Embedded	10.127.113.XX	255.255.255.0	10.127.XX

MON -8	Embedded	10.127.128.XX	255.255.255.0	10.127.XX
MON -9	Embedded	10.127.113.XX	255.255.255.0	10.127.XX
MON -10	Embedded	10.127.128.XX	255.255.255.0	10.127.XX
MON -11	Embedded	10.127.127.XX	255.255.255.0	10.127.XX
MON -12	Embedded	10.127.127.XX	255.255.255.0	10.127.XX
MON -13	Embedded	10.127.127.XX	255.255.255.0	10.127.XX
MON -14	Embedded	10.127.127.XX	255.255.255.0	10.127.XX
MON -15	Embedded	10.127.128.XX	255.255.255.0	10.127.XX
MON -16	Embedded	10.127.128.XX	255.255.255.0	10.127.XX
MON -17	Embedded	10.127.128.XX	255.255.255.0	10.127.XX
MON -18	Embedded	10.127.128.XX	255.255.255.0	10.127.XX

Fuente: Elaborado por Autores

4.1.3.2. Diseño Físico

Equipos Físicos Ecu 911

Switch Cisco Catalyst 2960

Los switches Ethernet inteligentes de la serie Catalyst 2960 de Cisco tienen Conectividad Fast Ethernet y 10/100/1000 Gigabit Ethernet, lo que permite servicios de LAN mejorados para redes empresariales de nivel de entrada, medianas empresas y sucursales.

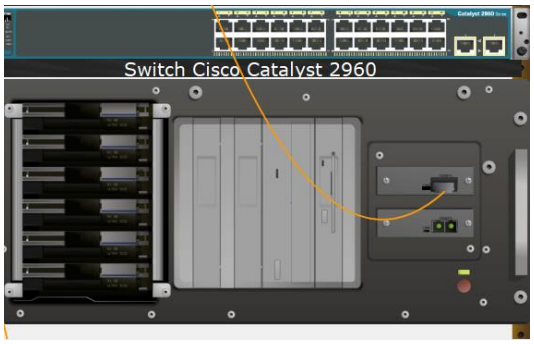


Figura 59. Servidor Físico Ecu 911
Fuente: Software Cisco Packet Tracer V.8.1.1

Existen varias configuraciones de modelo con la capacidad de conectar escritorios, servidores, teléfonos IP, puntos de acceso inalámbrico, cámaras IP u otros dispositivos de red.

Tabla 24. Características Switch Cisco Catalyst 2960

Características	• 1 RU de configuración fija • Imagen de base LAN • Puertos: 24 x 10/100 + 2 x Gigabit SFP combinado • Ancho de banda 16 Gbp • Taza de transferencia Máxima 1Gbit/s

Fuente: Switch Administrable capa L2 24 puerto por Hyperlink 2019

Equipos de Comunicaciones Ecu 911

Router Cisco C2951-CME-SRST/K9

Para la comunicación del Router con los diferente módulos de servicio de alta potencia y disponibilidad, es necesario realizar una conmutación Gigabit Ethernet con tecnología PoE mejorada, además, se debe supervisar la energía y la capacidad de control de tiempo que mejora el rendimiento general del sistema.

Figura 60. Router C2951
Fuente: Software Cisco Packet Tracer V.8.1.1

Características técnicas Router Cisco C2951-CME-SRST/K9

Tabla 25.

Características arquitectónicas	Descripción
Plataforma Modular	Los ISR de la serie Cisco 2900 son plataformas altamente modulares con varios tipos de ranuras.
Procesadores	La serie Cisco 2900 está impulsada por procesadores multinúcleo de alto rendimiento que pueden soportar las crecientes demandas de conexiones WAN.
Fabricación Multigigabit	La serie Cisco 2900 presenta un innovador Multi Gigabit Fabric (MGF) que permite una comunicación eficiente de módulo a módulo.

Fabricación Interconnectivity	Los servicios de comunicaciones unificadas en la sucursal se mejoran significativamente con el uso de un tejido de interconectividad TDM.
Puertos Gigabit Ethernet	Cuenta con tres puertos WAN Ethernet 10/100/1000 en Cisco 2921 y 2951 y habilita la conectividad de fibra.

Fuente: Cisco 2900 Series Integrated Services Routers Data Sheet

Equipos Físicos Cámaras Ecu 911

Cámaras Esféricas o Domo

Tabla 27. Características Cámara Domo CIEC

Características	Descripción
Movimiento	Giro Horizontal de 360 grados. Giro Vertical de 90 grados.
Almacenamiento	Almacenamiento de ubicaciones predeterminadas.
Vista	Con capacidad de visualización.

Fuente: Infraestructura Y Servicios Visibles Ecu 911 2020

Figura 51. Cámara Domo CIEC Ecu 911
Fuente: Infraestructura Y Servicios Visibles Ecu 911 2020

Un dispositivo integrado se ubicará en el "borde" de una red e interactuará con un servidor u ordenador para procesamiento y análisis adicionales, en lugar del método tradicional de

visión artificial de una cámara conectada al PC para el procesado de algoritmos de visión artificial.

Sistema Operativo dentro de las cámaras -

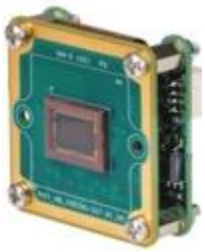


Figura 61. Sistema incrustado cámara DOMO

Fuente: Infraestructura Y Servicios Visibles Ecu 911 2020

Embedded Visión

Sistema embebido, empotrado o integrado a color para visión artificial, imagen industrial y seguridad. Ya que los sistemas de visión integrada están pensados para incorporarse a otros sistemas, cuentan con puntos de conexión o entrada simples como las interfaces GigE o USB. Son muy fáciles de configurar y suelen incluir un asistente o software informático que guía al usuario en la instalación a través de un ordenador.

Además, las cámaras incorporadas suelen ser intercambiables en muchos modelos, por lo que es fácil agregar un grupo de ellas o modificarlas según las exigencias de la actividad.

Tabla 28. Características Software incrustado en las cámaras

Características Embedded	Descripción
Tipo de Sensor	Sensor type
Cuadros por segundo	-
Rango Dinámico	12 bits
Peso	12 gramos
Interfaz	15-pin Raspberry Pi
Sistema Operativo	Variante de Linux

Fuente: Cámaras Aplicación Industrial

Diseño y Distribución Física Cámaras Ecu 911

Cantón Espejo

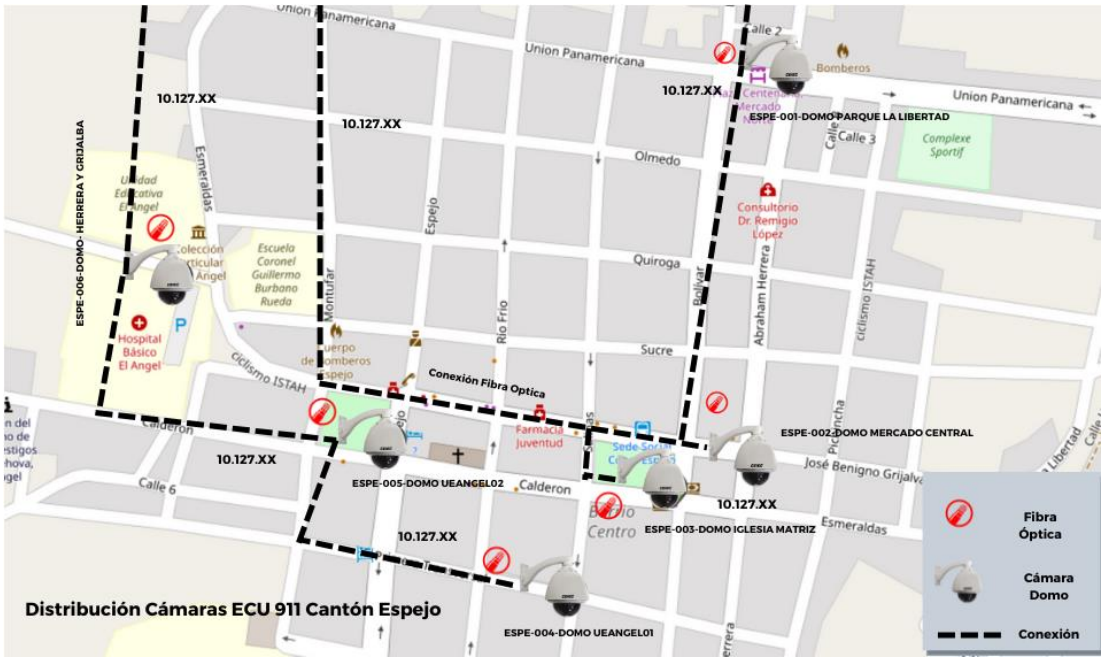


Figura 52. Cámaras Ecu 911 Espejo

Cantón Huaca

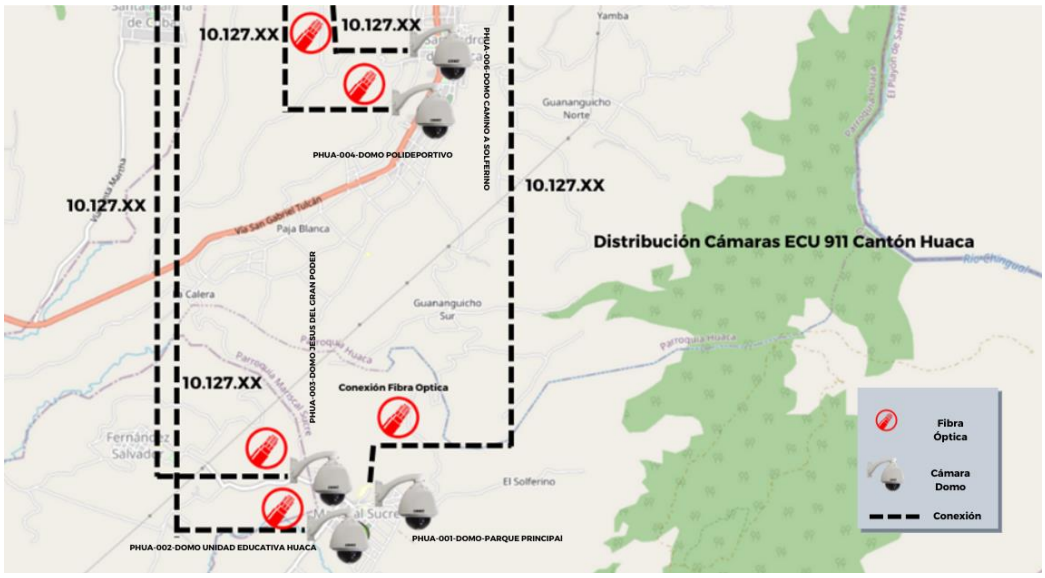


Figura 62. Cámaras Ecu 911 Huaca

Cantón Bolívar

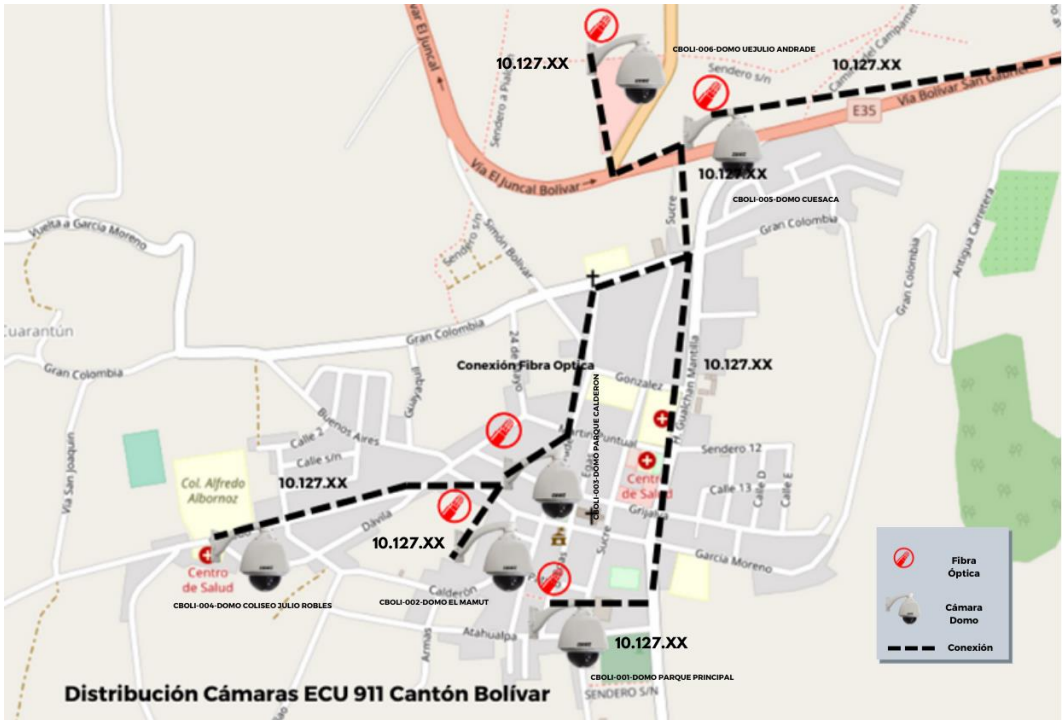


Figura 53. Cámaras Ecu 911 Bolívar

Cantón Montufar

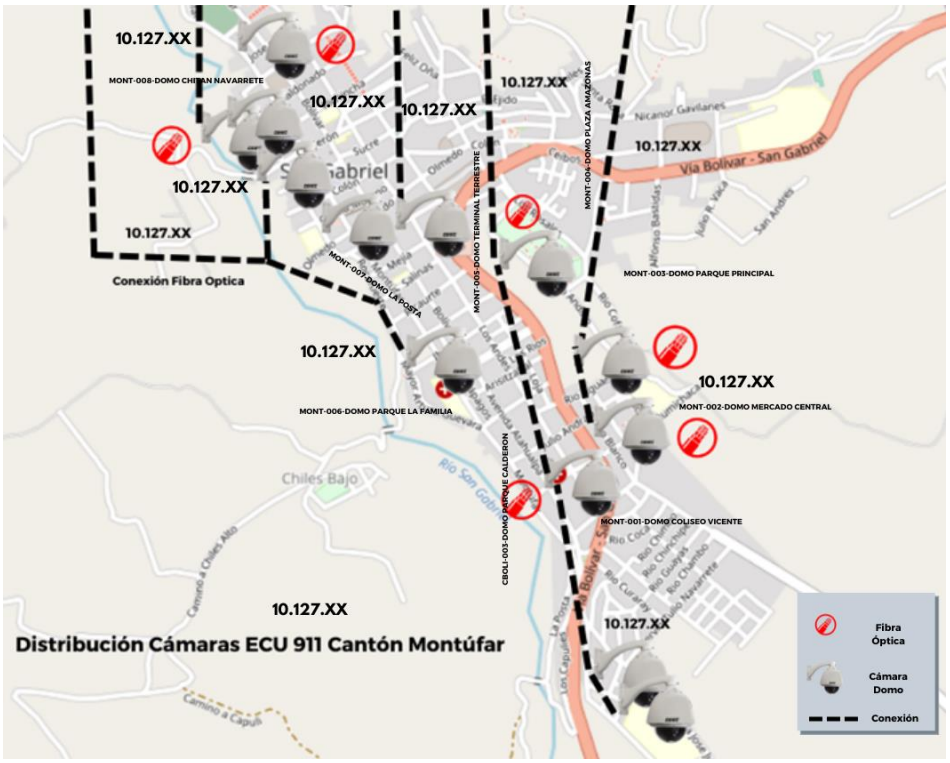


Figura 54. Cámaras Ecu 911 Mira

Distribución Física Cámaras Ecu 911 Matriz Tulcán

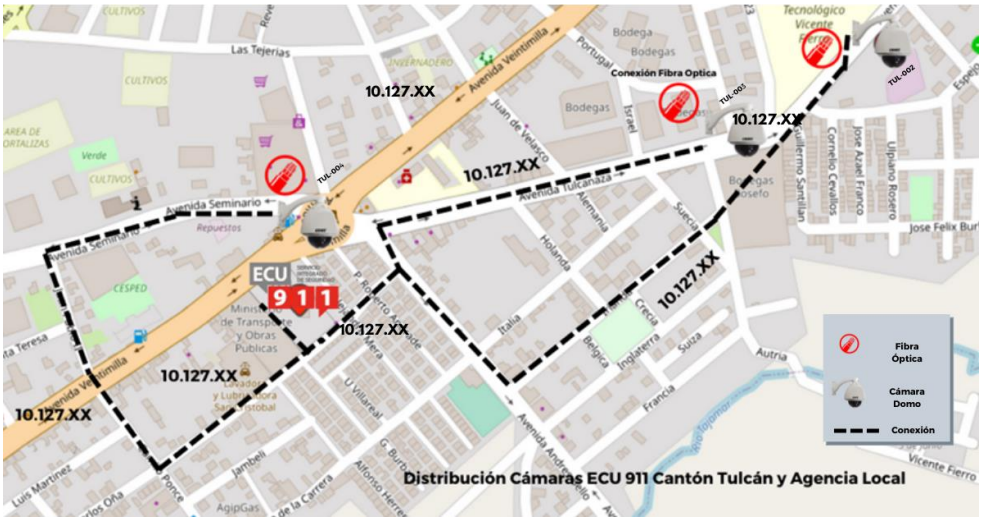


Figura 55. Distribución Cámaras Ecu 911 Agencia Local

4.1.4. Fase 4: Pruebas y Diseño

4.1.4.1 Documentación y Diseño del Sistema de Monitoreo de Cámaras

A continuación, presentaremos el diseño y las configuraciones que son necesarias para el correcto funcionamiento de la herramienta de monitoreo, para más información sobre la instalación y configuración interna consultar el anexo 4 Manual Técnico.

4.1.4.2 Creación de Agente y configuración inicial

En la página del Administrador de agentes, defina un nuevo agente llenando el formulario como se muestra en la siguiente captura de pantalla. Una vez que haya terminado, haga clic en Crear.

Figura 63. Creación de agente

4.1.4.3 Información del Agente

La información del Agente es de gran importancia al momento de verificar el estado del módulo, ya que verificaremos la correcta conexión con los dispositivos conectados a la red.

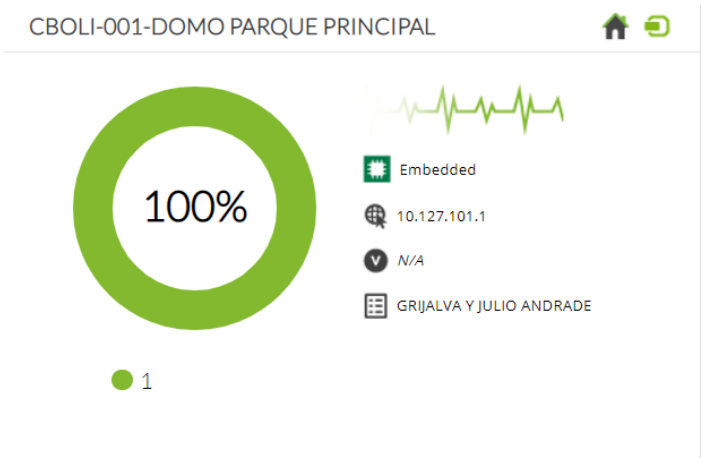


Figura 64. Estado del Agente

4.1.4.4 Contacto con el Agente

La información de los módulos de tráfico se visualizará para cada métrica pulsando en el icono de gráfica. Se mostrará una ventana con la gráfica de ese monitor y al pulsar en el icono de datos, una tabla con los datos.

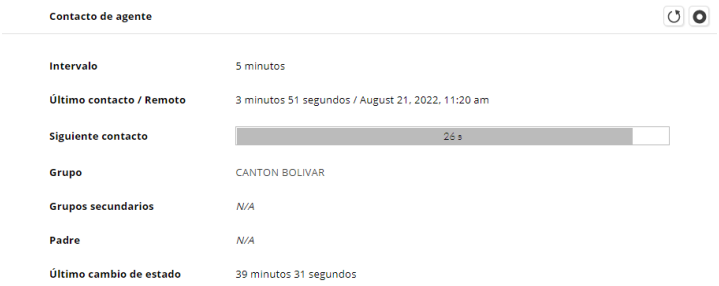


Figura 65. Contacto con el Agente

4.1.4.5 Creación de Módulos

La creación de módulos locales en la consola se realiza mediante un formulario donde, además de la configuración común de todo módulo (umbrales, tipo, grupo, etcétera) dispone de una caja de texto donde especificar los datos de configuración a establecer en el fichero de configuración del Agente Software.

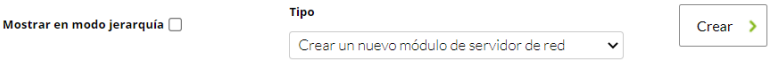


Figura 66. Creación de Módulo

Se creará un módulo para verificar si el host remoto está activo (se puede hacer ping).

Por defecto la herramienta de monitoreo implementa ciertos módulos de monitoreo de mediante un grupo de políticas conocidas como Basic Monitoring, en nuestro caso necesitaremos configurar un modelo de modulo bajo el protocolo ICMP el cual nos brindara una respuesta de conexión mediante el protocolo Ping.

4.1.4.6. Configuración de Módulo Ping

En esta parte de la configuración vamos a disponer de diferentes tipos de monitoreo, en nuestro caso utilizaremos una monitorización de tipo ICMP.

Como paso de verificación es necesario realizar una consulta ICMP desde el servidor de Pandora FMS hacia los agentes agregados correctamente.

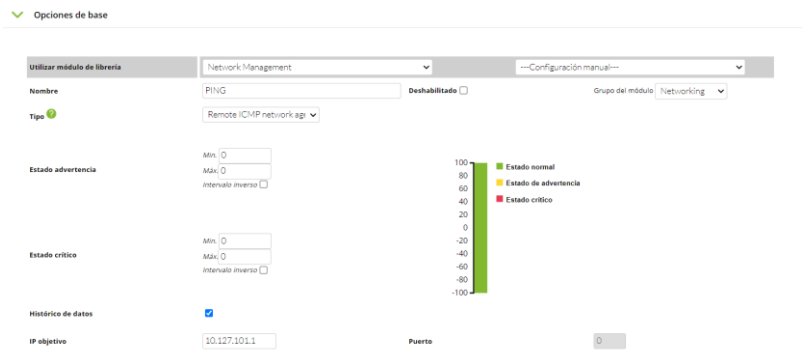


Figura 67. Configuración Módulo Ping

Como parte final de la configuración podemos observar que el módulo PING fue creado con éxito y funcionado normalmente.

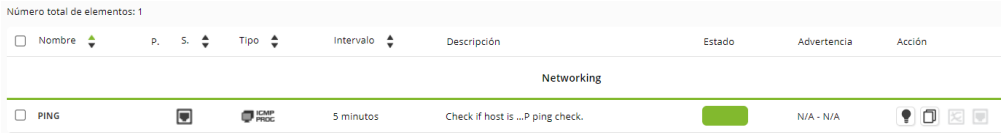


Figura 68. Módulo Ping

4.1.4.7. Configuración de Alertas

La configuración de alertas permite notificar al usuario acerca de un dispositivo que ha sufrido una falla o desconexión, en este apartado se determinaran los intervalos de estado de emergencia, asimismo como su tipo de monitoreo que se quiere realizar al dispositivo configurando su dirección IP, las alertas se mostraran en una ventana que se puede personalizar para ver una vista general de cómo está el estado de todos los dispositivos.

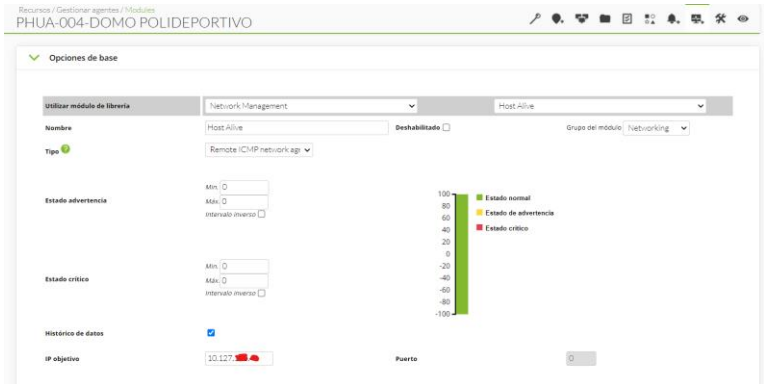


Figura 69. Ejemplo de configuración de alertas

Esta ventana nos permite personalizar como se va a mostrar la alerta si un dispositivo ha sufrido una desconexión.

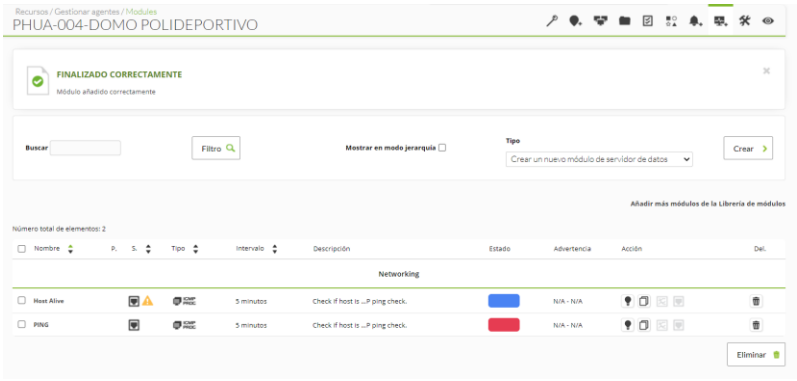


Figura 70. Asignación de alertas

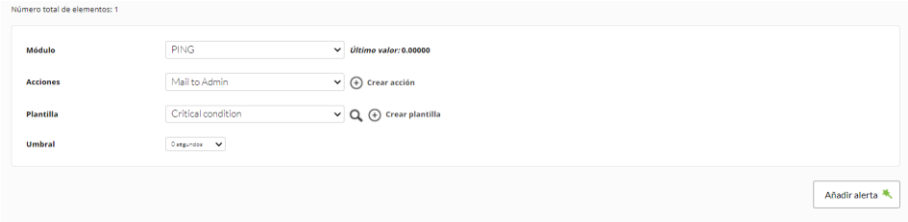


Figura 71. Añadir alerta

Este es un ejemplo completo de un dispositivo configurado en donde se muestra a que modulo pertenece, su estado (rojo-critico; azul-funcional) y las acciones que debe tomar

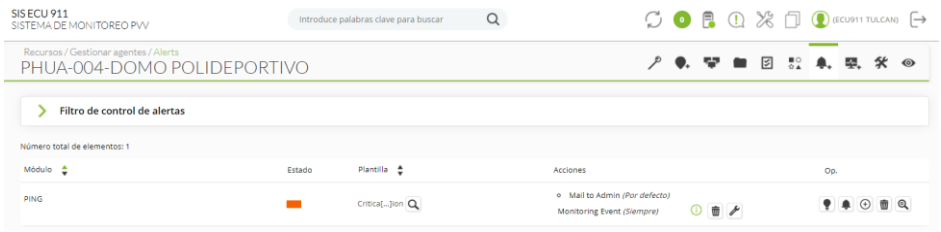


Figura 72. Disparo de alerta

Como paso final de la asignación de alertas la herramienta de monitoreo dispara una advertencia cuando el módulo cambia de estado normal a crítico, al momento de dispararse la alerta una notificación se enviará al correo eléctrico o dirección telegram establecida.

4.1.4.8. Alertas Vía Telegram

Como primer paso se configura la acción, que utiliza el mensaje de comando de Telegram, y se especifica el destinatario predeterminado más el contenido del mensaje.

El mensaje sirve para que el destinatario pueda solucionar la incidencia, y esto se puede lograr utilizando el sistema de macros incorporado de Pandora FMS. Una vez configurada la sección de comandos procedemos a añadir en el apartado de acciones.

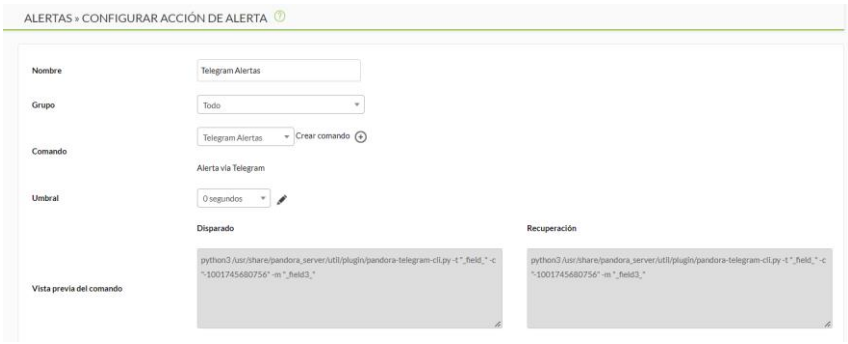


Figura 73. Script de Python 3 en comandos de alertas

Como resultado tenemos que se enviaron las alertas correctamente a nuestro servicio de telegram en nuestro teléfono smartphone.

Figura 74. Resultado de alerta de telegram de Pandora FMS

Como podemos observar la alerta se disparó al momento de cambiar de estado el agente que monitoreamos, en este caso en telegram creamos un grupo donde gracias a la ayude de un bot podemos recibir la notificación.

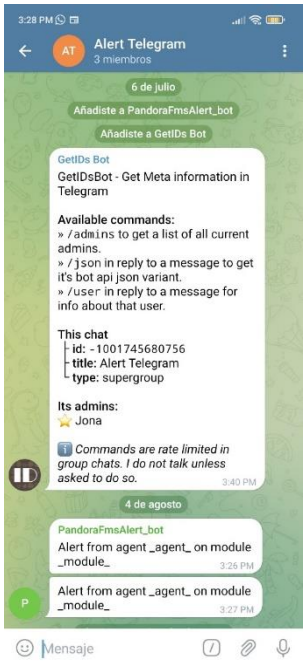


Figura 75. Resultado de alerta en Telegram

Como podemos observar la notificación llego satisfactoriamente a nuestro grupo de Telegram con el detalle de la alerta del agente y modulo correspondiente.

4.1.4.9. Creación de Informes

En un informe, la información que se va a presentar se organiza en elementos periódicamente establecidos. Existen diferentes tipos de elementos, que realizan cálculos y presentan información de formas muy diferentes. Por ejemplo, puede elegir un elemento de tipo gráfico simple que implemente gráficos individuales o un elemento de tipo Acuerdo de nivel de servicio (SLA) que represente el cumplimiento de una serie de monitores.

4.1.4.10 Configuración de Informes

Para crear un informe personalizado debemos darle un nombre, un grupo y los permisos de escritura que debe tener, además de la descripción que le vamos a dar al informe.

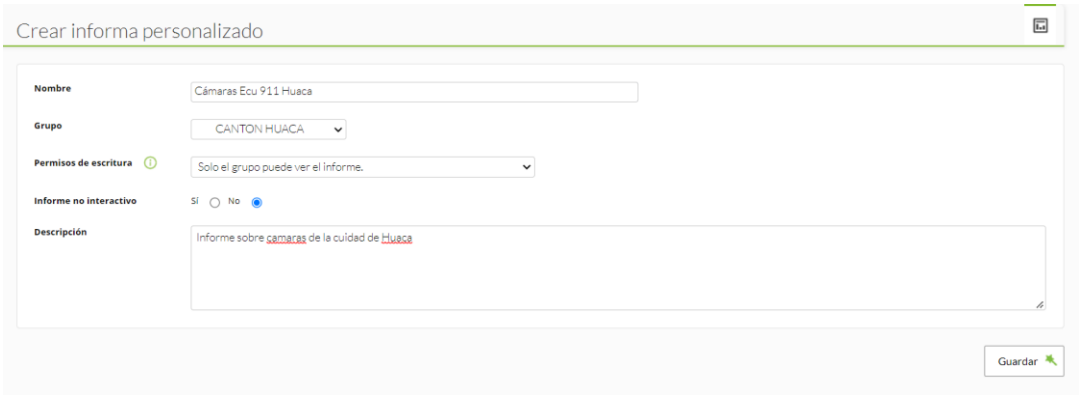


Figura 76. Creación de informe personalizado del Cantón Huaca

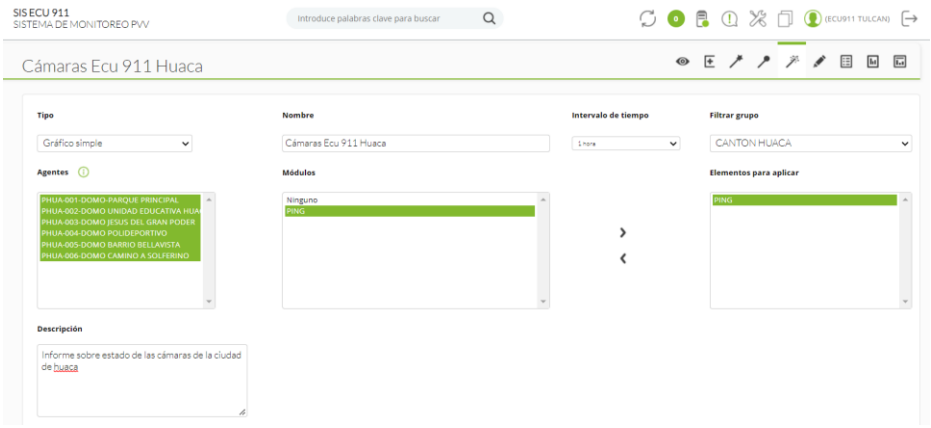


Figura 77. Configuración de Gráfico Simple

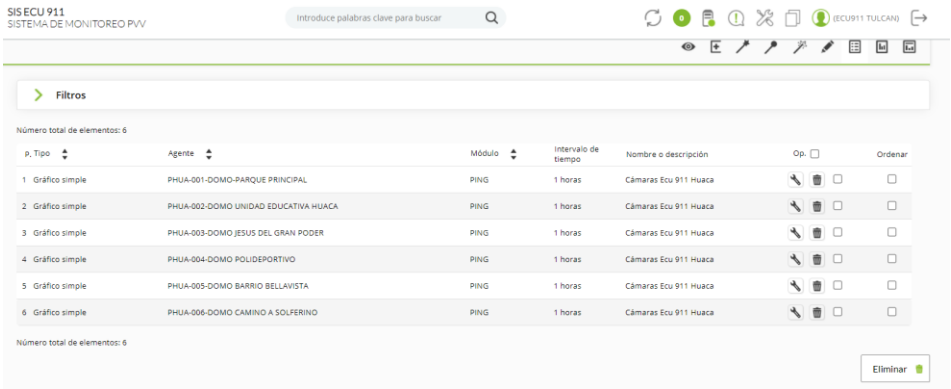


Figura 78. Lista de informes

4.1.4.11. Informe SLA

Todos los informes de Acuerdo de nivel de servicio (SLA) muestran información sobre el cumplimiento de una métrica, es decir, nos indican el porcentaje de tiempo que el módulo ha tenido un valor válido conocido.

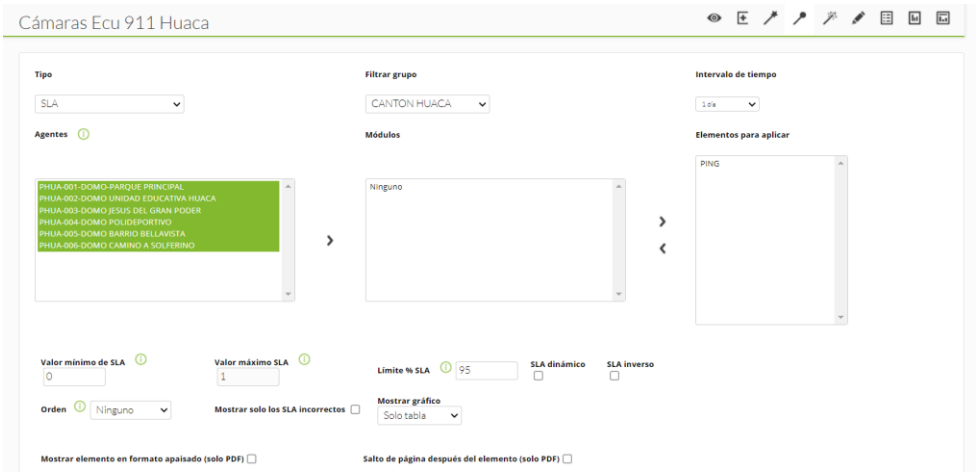


Figura 79. Configuración de informe SLA Cantón Huaca

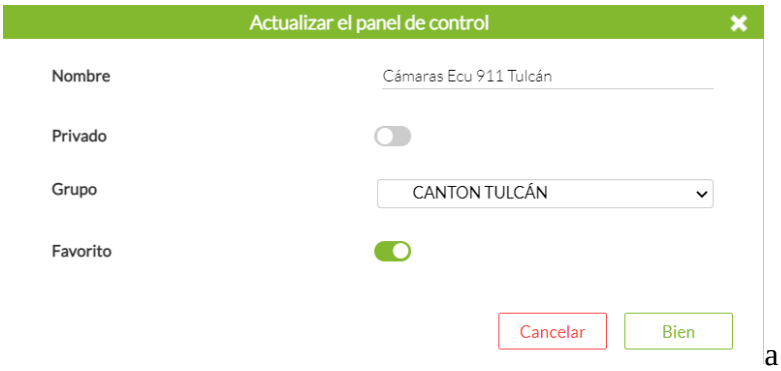
La configuración se realizará de la misma manera para los diferentes cantones que pertenecen al Servicio Integrado de Seguridad Ecu 911.

4.1.4.12. Informes Visuales

Los informes gráficos, también conocidos como informes visuales , implementan elementos gráficos para hacer que los datos sean visualmente más atractivos y para mejorar la usabilidad visualizando datos gráficamente en formatos de diagrama o gráfico.

4.1.4.13. Diseñar Modelos Dashboard De Las Cámaras Por Cantón

El Cuadro de mandos (Dashboard) es una funcionalidad de Pandora FMS que permite que cada usuario construya su propia página de monitorización. Se puede añadir más de una página, y en ella se pueden añadir mapas de monitorización, gráficas y resúmenes de estado, entre otros elementos (Pandora, 2022).



a

Figura 80. Creación del panel de control

En este apartado de configuración añadiremos el nombre que tendrá la Dashboard, como también al grupo que pertenecerá.

El siguiente paso es configurar el widget el cual contendrá diferentes apartados como el título, imagen de fondo, agente, modulo, y un icono que se verá reflejado en el cuadro final.

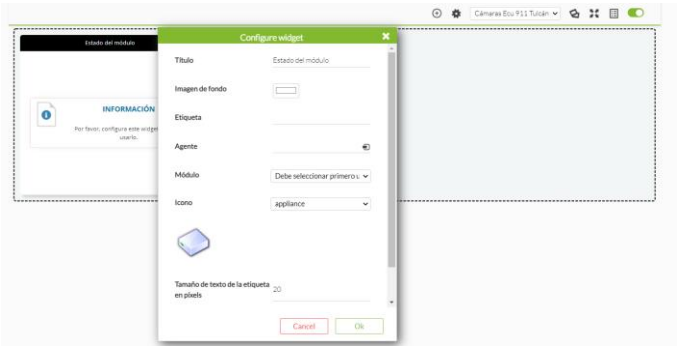


Figura 81. Configuración del widget

En este apartado añadiremos cada campo necesario para la visualización de cada agente con su respectiva información.

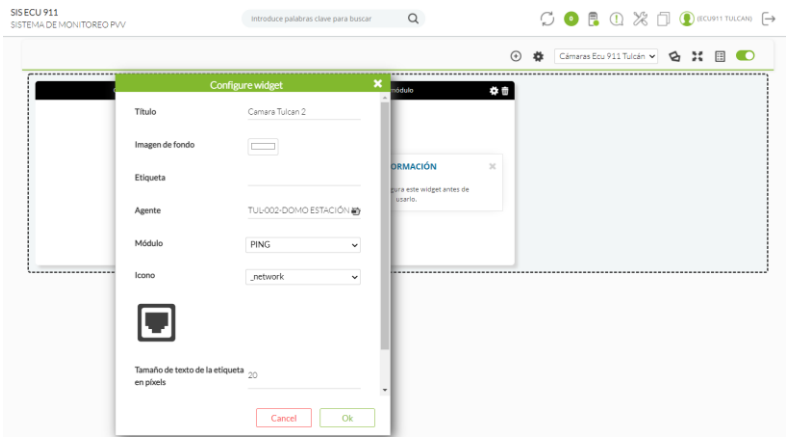


Figura 82. Insertar información al widget

4.1.4.14. Resultado Informes Visuales

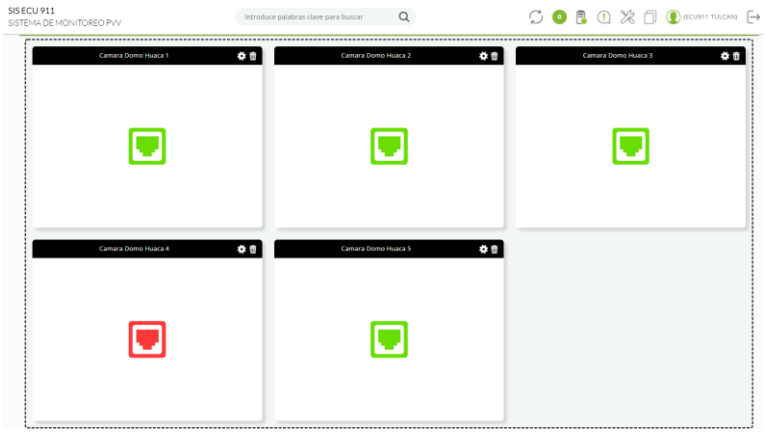


Figura 83. Dashboard de cámaras activas e inactivas

Como podemos observar el informe se lo presenta de manera grafica e interactiva, dentro del informe se configuro la visualización del estado de las cámaras con los colores representativos, en este caso el verde y rojo nos indicaran el estado activo e inactivo de los agentes establecidos previamente.

4.1.4.15. Diseño Mapa de Red

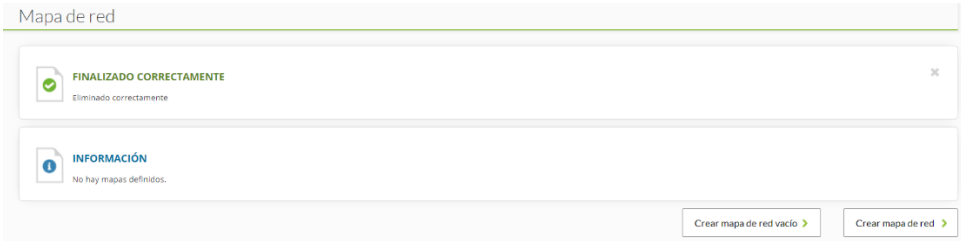


Figura 84. Creación de mapa de red

Realizamos la configuración inicial para crear un mapa de red.

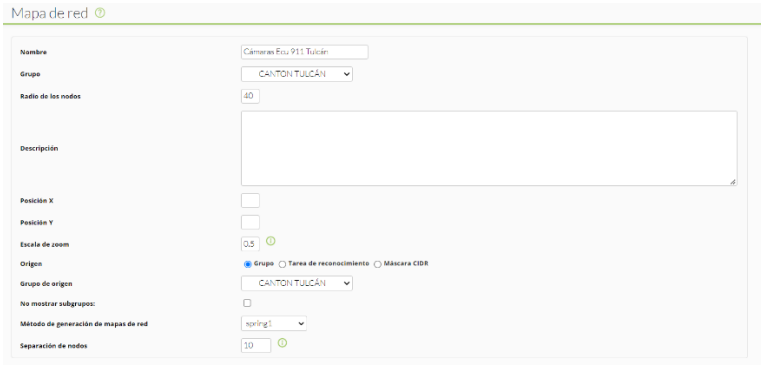


Figura 85. Configuración de mapa de red

En este apartado de la configuración debemos añadir el grupo en el cual queremos diseñar el mapa de red.

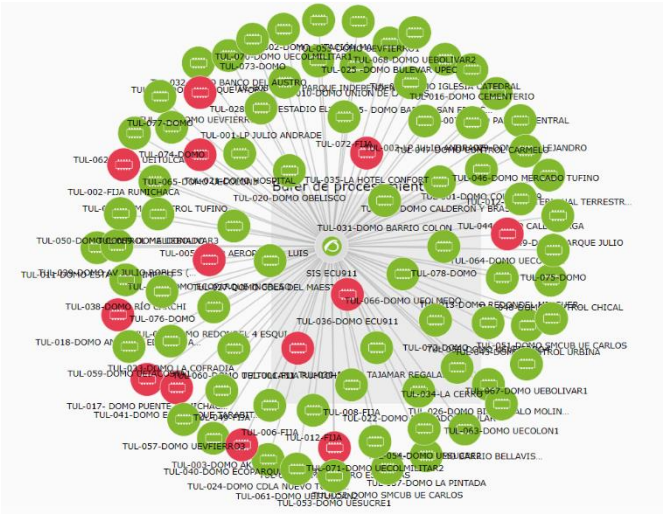


Figura 86. Mapa de red cámaras Ecu 911 Tulcán

El mapa de red nos brindara una información de gran importancia ya que se configuro bajo las especificaciones del área de tecnología, en el cual nos habían solicitado observar de manera general la distribución de las cámaras y su respetivo estado de conexión.

4.1.4.16. Creación de Capas Mapa GIS Ecu 911

Como primer paso para la creación y configuración de capas nos dirigimos a la opción de crear un nuevo mapa GIS.

Figura 87. Mapas GIS ECU 911

A continuación, se desplegará un asistente para la creación de cada una de las capas necesarias para la creación del mapa GIS, en este apartado ingresaremos en nombre del mapa y el grupo que pertenece, al igual que las coordenadas necesarias para el posicionamiento de cada figura.

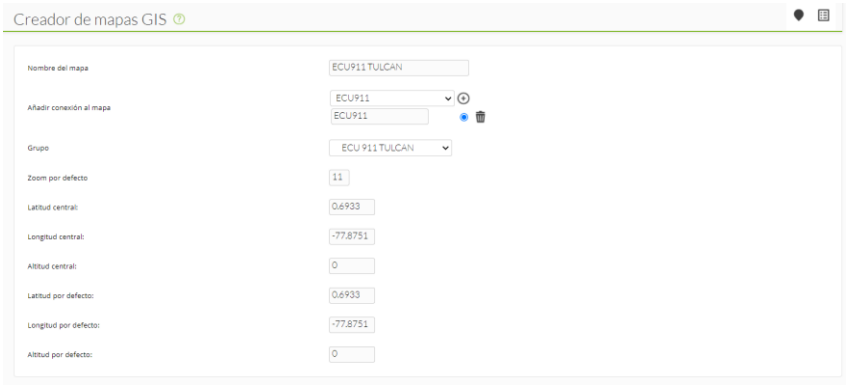


Figura 88. Creador de Mapa GIS

- **Asignación de agente**

En esta sección añadiremos los diferentes agentes de cada cantón a las capas creadas anteriormente.

Figura 89. Creación de Capa Cantón Bolívar

4.1.4.17. Capas Mapa GIS

Una vez realizadas las configuraciones necesarias por cada cantón se desplegará una lista con las capas generadas con éxito.

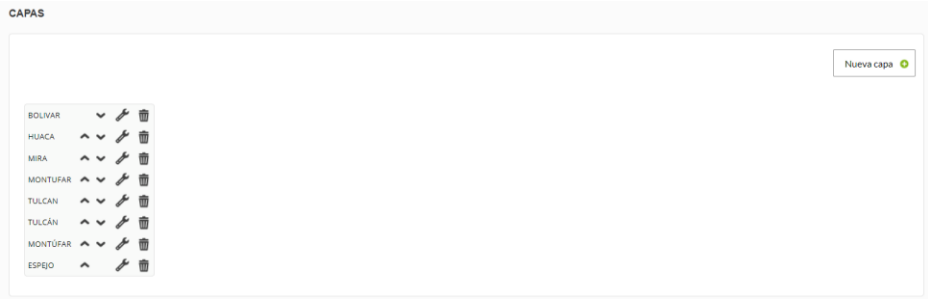


Figura 90. Capas Mapa GIS

4.1.4.18. Resultados Mapa GIS

Con este mapa se puede observar la posición actual, así como un pequeño resumen histórico de las posiciones de los agentes configurados.

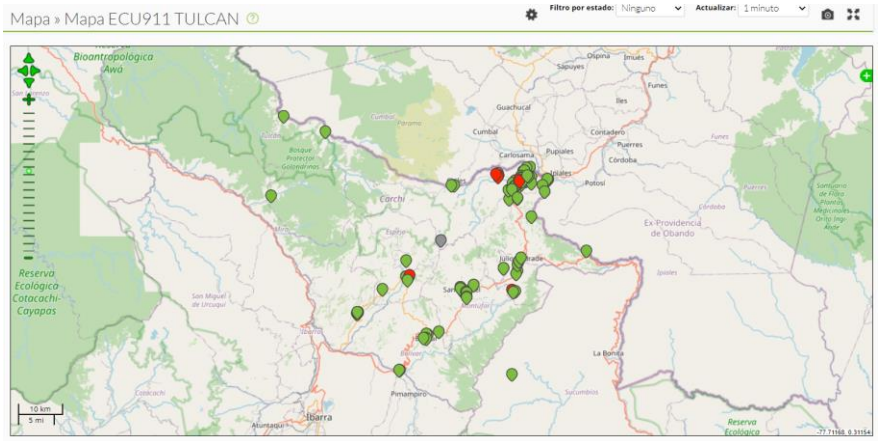


Figura 91. Mapa Gis Ecu 911

Mapa GIS Ecu 911 (Cámaras Estado Crítico)

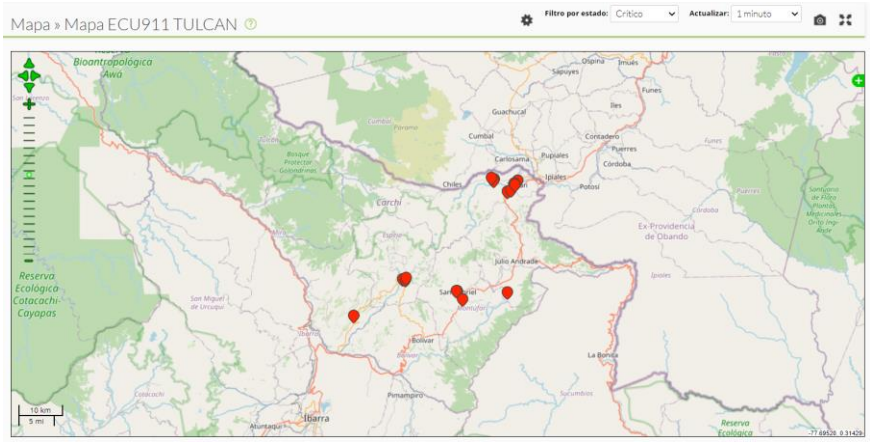


Figura 92. Mapa GIS Filtro Critico

Mapa Gis Ecu 911 (Cámaras Estado Normal)

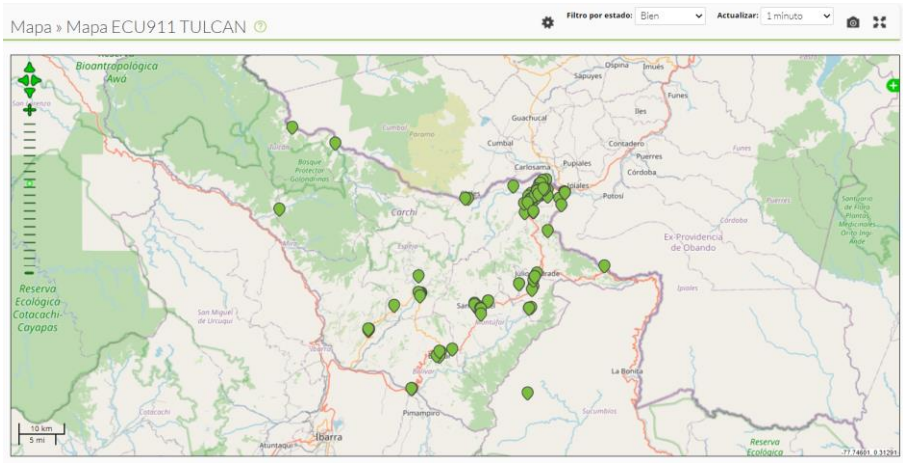


Figura 93. Mapa GIS Filtro Normal

4.1.4.19. Eventos Sonoros Cámaras Ecu 911

El sistema de eventos de Pandora FMS permite ver un registro en tiempo real de todos los acontecimientos que ocurren en los sistemas monitorizados.

La consola de eventos sonoros permite difundir las distintas alertas sonoras cuando se produce un evento. La melodía se oirá continuamente hasta que pause el evento sonoro o pulse el botón de OK.

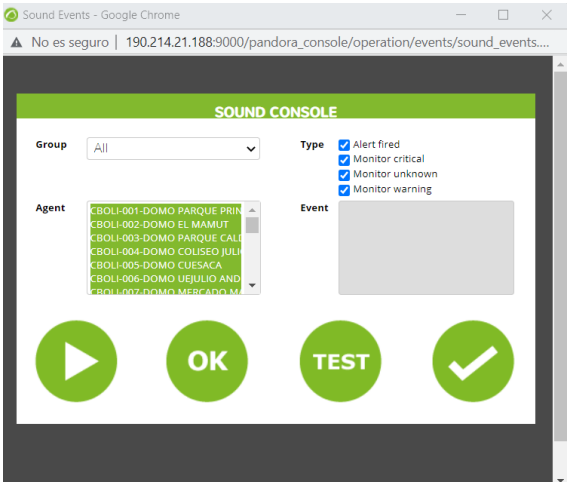


Figura 94. Consola de Eventos Sonoros

Lista de eventos que generan sonido, por defecto:

- El disparo de cualquier alerta.
- El paso de un módulo a estado warning.

- El paso de un módulo a estado critical.
- El paso de un módulo a estado unknown.

Disparo de evento sonoro

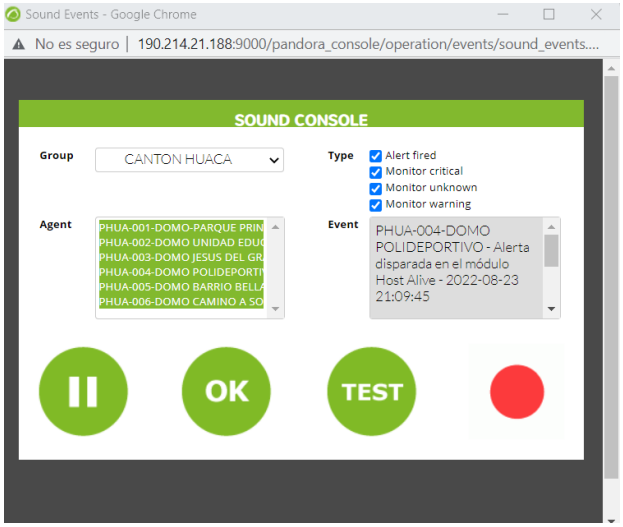


Figura 95. Disparo de Alerta Sonora

Los eventos sonoros se exploran cada 10 segundos de forma asíncrona, al suceder un evento la ventana comenzará a parpadear en rojo y vibrar, además, dependiendo de la configuración de su navegador o sistema operativo, la ventana mantendrá el foco y se posicionará por delante del resto de ventanas abiertas.

4.1.5 Fase 5: Implementación y Puesta En Marcha

4.1.5.1 Socialización con el área de Tecnología Ecu 911

Para el paso de socialización de la herramienta de monitoreo de datos, se precedió a familiarizar las características que ofrece Pandora FMS con la Msc. María José Argoti el cual es la encargada de administrar las cámaras del sistema de videovigilancia.

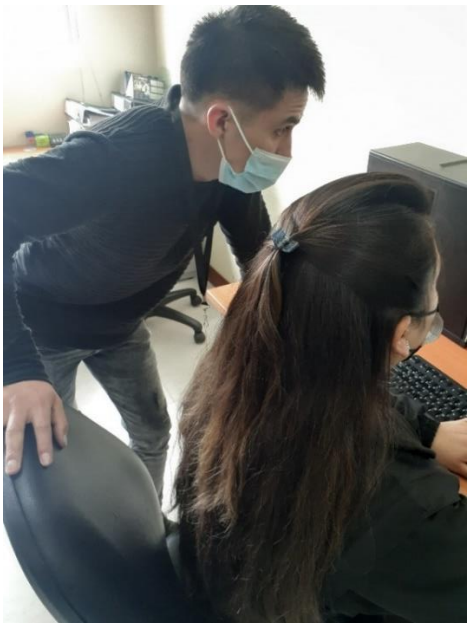


Figura 96. Socialización de la herramienta de monitoreo de datos.

4.1.5.2 Implementación de Pandora FMS en el Servicio Integrado de Seguridad Ecu 911

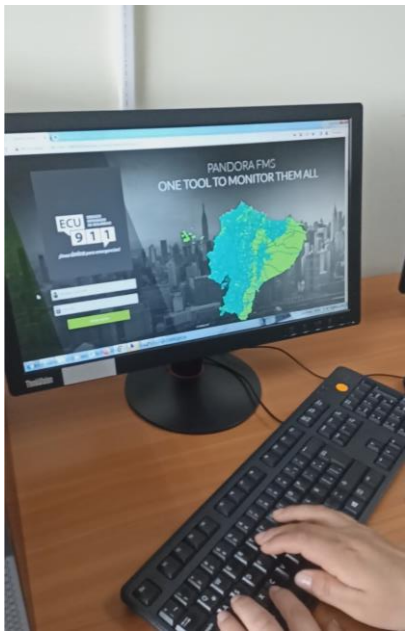


Figura 97. Pandora FMS en el servicio Integrado de Seguridad ECU 911.

Gracias a la colaboración del área de tecnología la cual nos brindó un servidor físico en el cual se logró la implementación y puesta en marcha de la herramienta de monitoreo de datos.

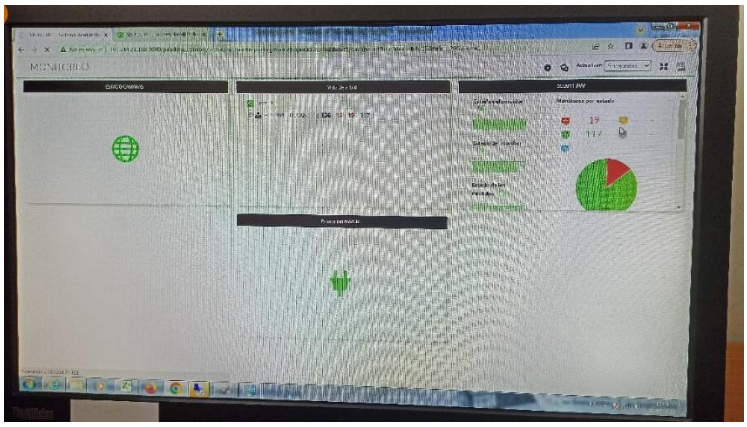


Figura 98. Pandora FMS implementado en el Ecu 911

4.1.6 FASE :6 Optimización Y Resultados

4.1.6.1 Resultados de Informes Cámaras Ecu 911

Informe Ecu 911 Cámaras Huaca

Como se puede apreciar en el siguiente gráfico se ha configurado una gráfica para poder visualizar los fallos que ha tenido durante un periodo de 1 mes antes de ser configurado el sistema de alertas y eventos y cuál es su comportamiento en el mismo.

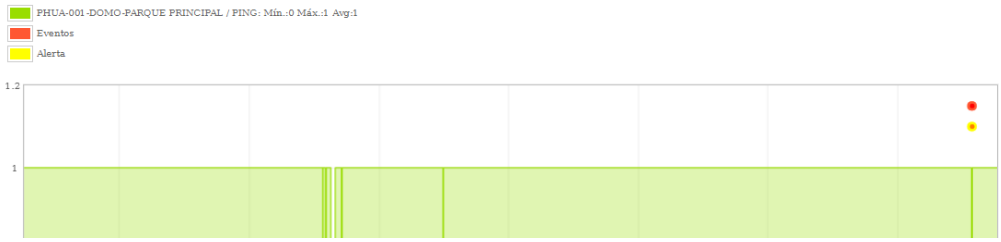


Figura 99. Informe Gráfico Simple Cámaras Huaca

Informe SLA Cantón Huaca

En el informe SLA ofrecido por la herramienta de monitoreo de datos se puede obtener un informe de cómo está actualmente el porcentaje de funcionamiento de los dispositivos conectados al servidor Pandora FMS en este caso de las cámaras del Cantón Huaca, por lo que se puede deducir que los funcionarios toman medidas respecto al momento del fallo de un dispositivo, para poder tener un 100 por ciento de funcionalidad.

Agente	Módulo	Valores max/min	Límite del SLA	Cumplimiento del SLA	Estado
PHUA-001-DOMO-PARQUE PRINCIPAL	PING	1 / 0	95%	100%	Bien
PHUA-002-DOMO UNIDAD EDUCATIVA HUACA	PING	1 / 0	95%	100%	Bien
PHUA-003-DOMO JESUS DEL GRAN PODER	PING	1 / 0	95%	100%	Bien
PHUA-004-DOMO POLIDEPORTIVO	PING	1 / 0	95%	100%	Bien
PHUA-005-DOMO BARRIO BELLAVISTA	PING	1 / 0	95%	100%	Bien
PHUA-006-DOMO CAMINO A SOLFERINO	PING	1 / 0	95%	100%	Bien

Figura 100. Informe SLA Cámaras Huaca

Informe Cámaras Ecu 911 Bolívar

Como se puede apreciar en el siguiente gráfico se ha configurado una gráfica para poder visualizar los fallos que ha tenido durante un periodo de 1 mes antes de ser configurado el sistema de alertas y eventos y cuál es su comportamiento en el mismo.

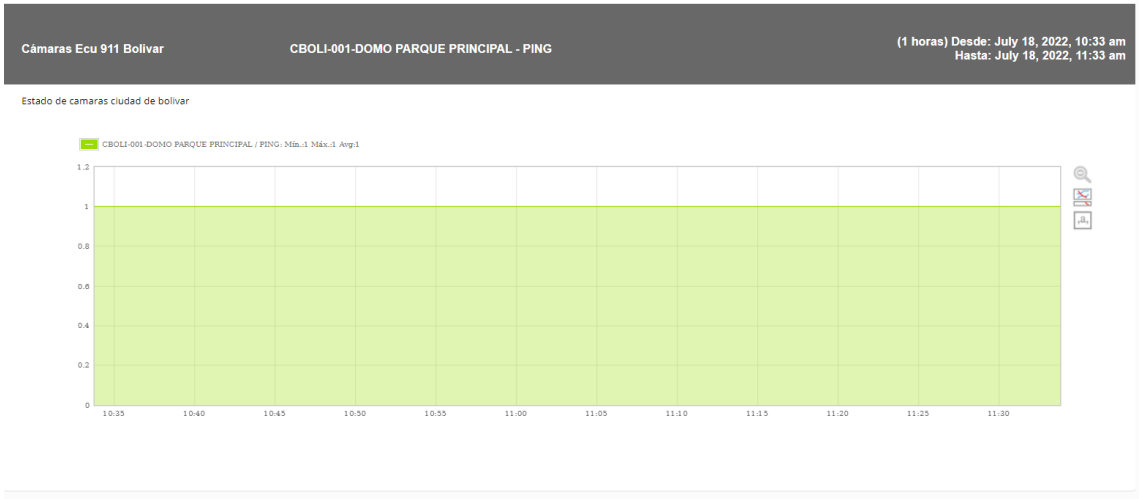
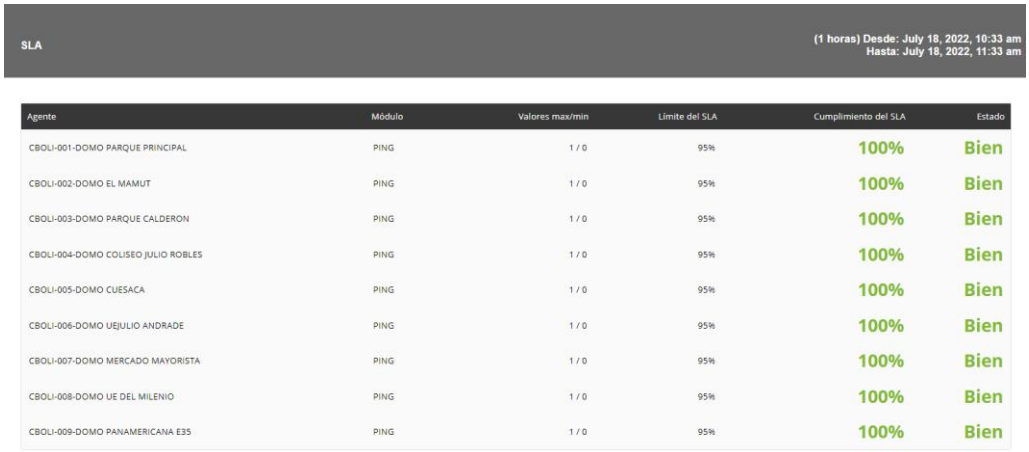


Figura 101. Informe Gráfico Simple Cámara Bolívar

Informe SLA Cantón Bolívar

En el informe SLA ofrecido por la herramienta de monitoreo de datos se puede obtener un informe de cómo está actualmente el porcentaje de funcionamiento de los dispositivos conectados al servidor Pandora FMS en este caso de las cámaras del Cantón Bolívar, por lo que se puede deducir que los funcionarios toman medidas respecto al momento del fallo de un dispositivo, para poder tener un 100 por ciento de funcionalidad.



SLA

(1 horas) Desde: July 18, 2022, 10:33 am
Hasta: July 18, 2022, 11:33 am

Agente	Módulo	Valores max/min	Límite del SLA	Cumplimiento del SLA	Estado
CBOLI-001-DOMO PARQUE PRINCIPAL	PING	1 / 0	95%	100%	Bien
CBOLI-002-DOMO EL MAMUT	PING	1 / 0	95%	100%	Bien
CBOLI-003-DOMO PARQUE CALDERON	PING	1 / 0	95%	100%	Bien
CBOLI-004-DOMO COLISEO JULIO ROBLES	PING	1 / 0	95%	100%	Bien
CBOLI-005-DOMO CUESACA	PING	1 / 0	95%	100%	Bien
CBOLI-006-DOMO UEJULIO ANDRADE	PING	1 / 0	95%	100%	Bien
CBOLI-007-DOMO MERCADO MAYORISTA	PING	1 / 0	95%	100%	Bien
CBOLI-008-DOMO UE DEL MILENIO	PING	1 / 0	95%	100%	Bien
CBOLI-009-DOMO PANAMERICANA E35	PING	1 / 0	95%	100%	Bien

Figura 102. Informe SLA Cámaras Bolívar

Informes Cámaras Ecu 911 Montúfar

Como se puede apreciar en el siguiente gráfico se ha configurado una gráfica para poder visualizar los fallos que ha tenido durante un periodo de 1 mes antes de ser configurado el sistema de alertas y eventos y cuál es su comportamiento en el mismo.

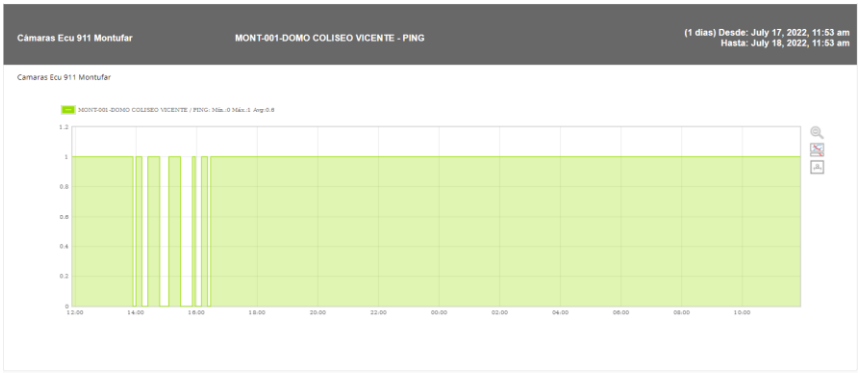


Figura 103. Informe Gráfico Simple Cámaras Montúfar

Informe SLA Cantón Montúfar

En el informe SLA ofrecido por la herramienta de monitoreo de datos se puede obtener un informe de cómo está actualmente el porcentaje de funcionamiento de los dispositivos conectados al servidor Pandora FMS en este caso de las cámaras del Cantón Huaca, por lo que se puede deducir que los funcionarios toman medidas respecto al momento del fallo de un dispositivo, para poder tener un 100 por ciento de funcionalidad.

Agente	Módulo	Valores max/min	Límite del SLA	Cumplimiento del SLA	Estado
MONT-002-DOMO MERCADO CENTRAL	PING	1 / 0	95%	100%	Bien
MONT-003-DOMO PARQUE PRINCIPAL	PING	1 / 0	95%	100%	Bien
MONT-004-DOMO PLAZA AMAZONAS	PING	1 / 0	95%	100%	Bien
MONT-005-DOMO TERMINAL TERRESTRE	PING	1 / 0	95%	100%	Bien
MONT-006-DOMO PARQUE LA FAMILIA	PING	1 / 0	95%	100%	Bien
MONT-007-DOMO LA POSTA	PING	1 / 0	95%	100%	Bien
MONT-008-DOMO CHITAN NAVARRETE	PING	1 / 0	95%	100%	Bien
MONT-009-DOMO	PING	1 / 0	95%	100%	Bien
MONT-010-DOMO PARQUE LA PAZ	PING	1 / 0	95%	100%	Bien
MONT-011-DOMO UECRISCOLON1	PING	1 / 0	95%	100%	Bien
MONT-012-DOMO UECRISCOLON2	PING	1 / 0	95%	100%	Bien
MONT-013-DOMO UEJJANDRADE1	PING	1 / 0	95%	100%	Bien
MONT-014-DOMO UEJJANDRADE2	PING	1 / 0	95%	100%	Bien
MONT-015-DOMO UEMAOÑA1	PING	1 / 0	95%	100%	Bien

Figura 104. Informe SLA Montúfar

Informes Cámaras Ecu 911 Espejo

Como se puede apreciar en el siguiente gráfico se ha configurado una gráfica para poder visualizar los fallos que ha tenido durante un periodo de 1 mes antes de ser configurado el sistema de alertas y eventos y cuál es su comportamiento en el mismo.

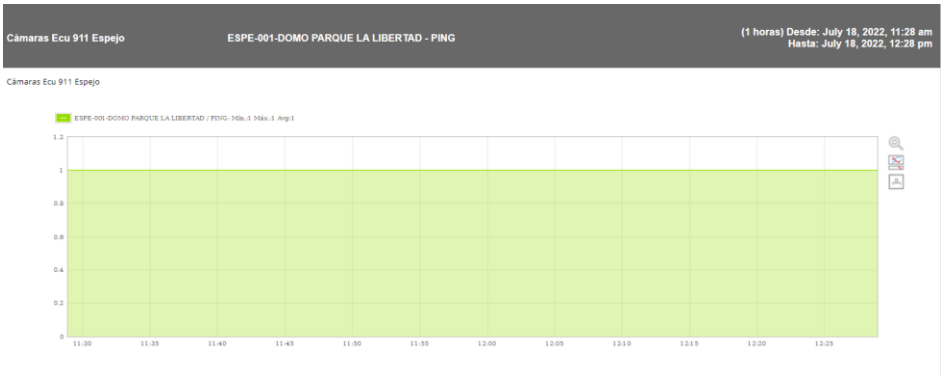


Figura 105. Informe Gráfico Simple Cámaras Espejo

Informe SLA Espejo

En el informe SLA ofrecido por la herramienta de monitoreo de datos se puede obtener un informe de cómo está actualmente el porcentaje de funcionamiento de los dispositivos conectados al servidor Pandora FMS en este caso de las cámaras del Cantón Huaca, por lo que se puede deducir que los funcionarios toman medidas respecto al momento del fallo de un dispositivo, para poder tener un 100 por ciento de funcionalidad.

Agente	Módulo	Valores max/min	Límite del SLA	Cumplimiento del SLA	Estado
ESPE-001-DOMO PARQUE LA LIBERTAD	PING	1 / 0	95%	100%	Bien
ESPE-002-DOMO MERCADO CENTRAL	PING	1 / 0	95%	100%	Bien
ESPE-003-DOMO IGLESIA MATRIZ	PING	1 / 0	95%	100%	Bien
ESPE-004-DOMO UEANGEL01	PING	1 / 0	95%	100%	Bien
ESPE-005-DOMO UEANGEL02	PING	1 / 0	95%	100%	Bien
ESPE-006-DOMO- HERRERA Y GRIJALBA	PING	1 / 0	95%	100%	Bien
ESPE-007-DOMO- HERRERA Y PANAMERICANA	PING	1 / 0	95%	100%	Bien
ESPE-008-DOMO- RED. BOTIJUELA Y PANAMERICANA	PING	1 / 0	95%	100%	Bien
ESPE-009-DOMO- PARR. SAN ISIDRO	PING	1 / 0	95%	100%	Bien
ESPE-010-DOMO- PARR. LA LIBERTAD	PING	1 / 0	95%	100%	Bien
ESPE-011-DOMO- ING. GUALCHAN	PING	1 / 0	95%	100%	Bien

Figura 106. Informe SLA Cámaras Espejo

Informes Cámaras Ecu 911 Mira

Como se puede apreciar en el siguiente gráfico se ha configurado una gráfica para poder visualizar los fallos que ha tenido durante un periodo de 1 mes antes de ser configurado el sistema de alertas y eventos y cuál es su comportamiento en el mismo.

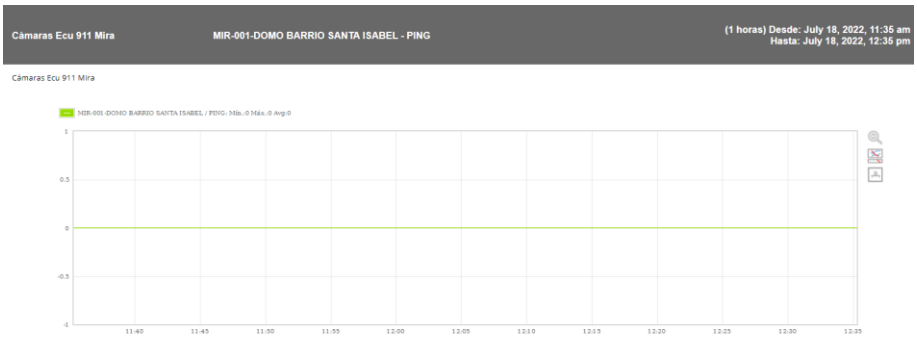


Figura 107. Informe Gráfico Simple Cámaras Mira

4.2. Discusión

El presente trabajo de investigación realizado en el servicio Integrado de Seguridad Ecu 911 cuyo problema fue que el limitado uso de una herramienta de datos no permite conocer el estado de diferentes dispositivos tecnológicos para proceder con sus respectivas correcciones y/o mantenimiento. Por lo que se estableció como objetivo general, el desarrollo de una herramienta de monitoreo de datos que facilite las tareas de monitorización de los estados de los dispositivos pertenecientes a la infraestructura tecnológica del ECU 911.

Para el desarrollo de una herramienta de monitoreo de datos para la infraestructura del Servicio integrado de seguridad ECU 911 se realizó las respectivas indagaciones bibliográficas referentes a el presente proyecto de diversos autores, las cuales fueron de ayuda para discernir las herramientas de datos prometedoras en el cumplimiento de este objetivo. Mediante encuestas realizadas a los respectivos funcionarios que trabajan en el área de tecnología se recolecto los respectivos requerimientos funcionales que requieren ser abarcados para solucionar la problemática.

En la tesis propuesta por Once (2017) llamada "Aplicación de monitoreo de los dispositivos de una red utilizando tecnología JAVA" el autor en una de sus conclusiones asegura que el uso del protocolo SNMP puede recuperar información de equipos conectados a una red, en la presente investigación se comparte que además del protocolo SNMP se pueden utilizar otros protocolos de red que cumplan este objetivo como lo es el protocolo ICMP, TC/IP a través de señales de ping entre otros. Además, el autor menciona que el lenguaje JAVA brinda varias alternativas al momento de gestionar una red mediante los complementos JMAPI.

En discusión con la tesis propuesta, la tecnología JAVA es una buena alternativa para administrar una red, sin embargo, presenta varios inconvenientes como, al ser una aplicación instalada en un computador solo funciona cuando está en ejecución, no emite ninguna alerta al presentarse un dispositivo escaneado en mal estado y solo utiliza el protocolo SNMP para conectar dispositivos que tengan esta tecnología.

La monografía presentada por los autores Garcia y Roa (2020) proponiendo como tema "Diseño de una herramienta de monitoreo y control de servidores utilizando como eje principal Cacti. Aplicado a una PYME mediana" desarrollaron una herramienta de monitoreo y control de servidores en una institución utilizando el aplicativo Cacti, afirmando que Cacti cubre un amplio rango de dispositivos de red en los que se pueden utilizar scripts,

consultas de datos y comandos para la recolección de datos, también utilizan la herramienta RRDTool la cual tiene la capacidad de generar cualquier tipo de gráfico para cualquier conjunto de datos siendo utilizada por como una de las herramientas de código abierto en una red.

Para discusión con la presente monografía, en el marco teórico se indago de la herramienta Cacti y como tiene diferentes características, ventajas y desventajas. Por lo que se puede afirmar que esta herramienta es muy utilizada por muchas empresas para visualizar el comportamiento de dispositivos mediante el tráfico de bytes y de paquetes en un periodo determinado de tiempo. Sin embargo, Cacti al utilizar el protocolo SNMP para monitorear los dispositivos puede limitarse a ciertas configuraciones, en el presente proyecto los dispositivos conectados a Pandora FMS utilizan el protocolo SNMP, ICMP y TC/IP por lo que no se mostraría un gráfico total de las cámaras que no utilicen protocolo SNMP, además de no contar con el sistema de alertas que nos ofrece Pandora FMS cada que un dispositivo se desconecta del servidor. Entonces se puede afirmar que Cacti es una buena herramienta para poder obtener gráficos de una red que utilicen protocolo SNMP y que no requieran un sistema de alertas de dispositivos.

Como siguiente discusión el autor Quispe (2018) con su trabajo de titulación denominado "Implementación de un sistema de monitoreo y control de red, para un canal de televisión, basado en herramientas open source y software libre", desarrollo un sistema de monitoreo utilizando la herramienta Nagios y plugins en el sistema operativo CentOS, el cual se lanzaran scripts automáticamente cada cierto tiempo a los equipos remotos, para comprobar si un equipo está funcionando, si la memoria está llena o si el servicio de un directorio esta activo. En el presente tema de investigación tiene una correlación en cuanto a los objetivos y lo que se quiere lograr por lo que se puede discutir que Nagios ofrece las mismas herramientas de Pandora FMS como alertas, informes y gestión de base de datos.

Entonces se puede discutir en que la utilización de herramientas de monitoreo de datos para la infraestructura de red se puede lograr aumentar la gestión y servicio para la mejora de toma de decisiones, el cual el autor también afirma en su respectivo informe.

Con el estudio y comparación de diferentes herramientas de monitoreo de datos se concluyó que la mejor opción para solventar estos inconvenientes es el sistema Pandora FMS el cual está diseñada para ser lo suficientemente flexible como para monitorear tanto herramientas como sistemas complejos y elementos de red ya sea usando SNMP o sondas de protocolos

TCP (snmp, ftp, dns, http, https, etc) lo cual para este proyecto se utilizó para el monitoreo de dispositivos de red el protocolo TCP/IP.

Una vez configurado y establecido todos los parámetros que se utilizaran en el Servicio Integrado de Seguridad ECU 911 se obtuvo los resultados que nos proporcionaba Pandora FMS en el cual se puede observar que existen cámaras que tienen un periodo de conexión inestable, esto puede favorecer a que mediante un envió de reportes desde la misma plataforma los funcionarios y gerente del establecimiento puedan tomar las medidas adecuadas para ver la causa del error ya sea dándole un mantenimiento al dispositivo o si es un caso pueda ser el mantenimiento a la infraestructura de red, detectando puntos donde haya un problema.

V. CONLUSIONES Y RECOMENDACIONES

5.1. CONCLUSIONES

- Se cumplió con el objetivo principal del tema de investigación propuesto, el cual es el desarrollo de una herramienta de monitoreo de datos para la infraestructura del Servicio Integrado de Seguridad ECU 911 mediante la instalación y configuración de la herramienta Pandora FMS.

- Mediante la realización de encuestas se logró determinar los requerimientos que son precisos para que la herramienta de monitoreo de datos sea adecuada en la resolución de los inconvenientes presentados en los dispositivos tecnológicos.

- Gracias a la investigación bibliográfica realizada en los medios virtuales y físicos se logró recopilar la información necesaria que permitió fundamentar teóricamente cada capítulo de la investigación, ayudando a comprender y entender los conceptos generales las herramientas de monitoreo de datos con relación a su manejo, integración, comunicación y aplicación y la relación que esta tiene con la infraestructura tecnológica, como sus tipos, componentes y características.

- A través de las encuestas realizadas a los diferentes integrantes del área de tecnología del Sistema Integrado Ecu 911 se llegó a la conclusión de que una herramienta de monitoreo es indispensable para la administración de dispositivos tecnológicos.

- El presente trabajo de investigación determinó que no existe una herramienta de monitoreo instalada idónea para visualizar el estado de los dispositivos tecnológicos en tiempo real dentro del área tecnológica.
- La propuesta de herramienta de monitoreo está configurada con Pandora FMS bajo un entorno cloud el cual estará disponible para ejecutarse en cualquier dispositivo capaz de tener accedo a un navegador web y conexión a internet.

5.2 RECOMENDACIONES

- En caso de expandir los dispositivos tecnológicos con mayor carga de datos se sugiere contratar una licencia con mayor capacidad de monitoreo y almacenamiento.

- Para una mejor experiencia tanto en rendimiento como en el funcionamiento se recomienda tener instalado en el servidor principal la consola y el servidor pandora.
- Se sugiere contar con las recomendaciones mínimas para la instalación del servidor Pandora Fms. Estas recomendaciones están calculadas suponiendo que cada agente tiene unos 5 módulos de media y que el muestreo medio es de cinco minutos.

- En caso de querer manejar la información de manera manual se recomienda la instalación de MySQL en un servidor independiente en lugar del mismo servidor local y posteriormente instalar Percona XTraDB.
- Se recomienda utilizar correos electrónicos corporativos (Gmail, Exchange, entro otros), todo esto para evitar que las alertas sean identificadas como contenido spam.

- Es recomendable utilizar Pandora Fms en ambientes no virtuales, ya que son demasiados los permisos y requisitos de acceso al disco lo que ocasionaría un funcionamiento inadecuado.

VI. REFERENCIAS BIBLIOGRÁFICAS

Academia Android. (11 de diciembre de 2014). *Android Studio v1.0: características y comparativa con Eclipse*. Obtenido de https://academiaandroid.com/android-studio-v1-caracteristicas-comparativa-eclipse/

Acosta, R. (2014). *La infraestructura de las tecnologías de la información y comunicación como mediadoras y el aprendizaje de la biología*. Obtenido de https://www.redalyc.org/pdf/993/99330402008.pdf

Amaya, D., & Sarria, M. (2019). *Gestión de infraestructura tecnológicas en entidades públicas*. Obtenido de https://repository.usc.edu.co/bitstream/handle/20.500.12421/4172/GESTI%C3%93N%20DE%20INFRAESTRUCTURA.pdf?sequence=3&isAllowed=y

Amazon. (2022). *Bases de datos relacionales*. Obtenido de https://aws.amazon.com/es/relational-database/#:~:text=Una%20base%20de%20datos%20relacional%20es%20una%20recopilaci%C3%B3n%20de%20elementos,en%20la%20base%20de%20datos.

Android Studio FAQs. (08 de diciembre de 2016). *Android Studio: ventajas, desventajas y principales características*. Obtenido de https://androidstudiofaqs.com/conceptos/ventajas-desventajas-android-studio

Android, A. (2014). Obtenido de https://academiaandroid.com/android-studio-v1-caracteristicas-comparativa-eclipse/

AppAnnie . (2021). *STATE OF MOBILE 2021*. Obtenido de https://www.appannie.com/en/go/state-of-mobile-2021/

ArgSeguridad. (16 de mayo de 2019). *Monitor para cámaras de seguridad*. Obtenido de https://es.rs-online.com/web/c/seguridad-y-herrajes-para-puertas-y-ventanas/videovigilancia/monitores-de-videovigilancia-cctv/

Arriaga, M. (2017). *Diseño de técnicas de análisis y visualización para los proyectos de la itdUMP*. Obtenido de http://oa.upm.es/52994/1/PFC_MARIA_ARRILLAGA_GONZALEZ_2017.pdf

Attardi, M. (septiembre de 2016). *Análisis del diseño de visualización interactiva de información* . Obtenido de http://mugi.webs.upv.es/wp-content/uploads/2016/11/Memoria_TFM_Mauro_Attardi.pdf

Ayudaley. (2020). Obtenido de https://ayudaleyprotecciondatos.es/bases-de-datos/jerarquicas/

BigData . (17 de diciembre de 2017). *RIAK KV: Casos de uso y características*. Obtenido de https://es.scribd.com/document/479675834/Riak-es-una-base-de-datos-NoSQL-distribuida-que-ofrece-alta-disponibilidad-docx

BiGeek. (28 de junio de 2018). *Redis para principiantes*. Obtenido de https://blog.bi-geek.com/redis-para-principiantes/

Bohorquéz, M. (05 de julio de 2020). *Modelo de calidad* . Obtenido de https://aprendamosiso25000.blogspot.com/2020/07/caracteristicas_5.html

CACTI. (2021). *About Cacti*. Obtenido de https://cacti.net/

Cámaras de vigilancia. (2021). *¿Cuáles son las mejores camara domo 360 grados hd?* Obtenido de https://www.camarasvigilancias.com/cuales-son-las-mejores-camara-domo-360-grados-hd/

Capterra. (2020). *¿Qué es Pandora FMS?* Obtenido de https://www.capterra.ec/software/151020/pandora-fms

Cardona, M. P. (14 de octubre de 2016). *Firebase, qué es y para qué sirve la plataforma de Google*. Obtenido de https://www.iebschool.com/blog/firebase-que-es-para-que-sirve-la-plataforma-desarroladores-google-seo-sem/

CISCO. (07 de enero de 2013). *Cisco IOS IP Command Reference*. Obtenido de https://web.archive.org/web/20130102124241/http://www.cisco.com/en/US/docs/ios/12_3/ipaddr/command/reference/ip1_i2g.html#wp1078496

Clarcat. (2021). *Xamarin*. Obtenido de https://www.clarcat.com/xamarin/

CodeCarbon . (03 de septiembre de 2020). *Major Advantages And Disadvantages Of Dart Language*. Obtenido de https://codecarbon.com/pros-cons-dart-language/

Cordinación General de Planificación y Gestión. (2014). *PLAN ESTRATÉGICO 2014-2017*. Obtenido de https://www.ecu911.gob.ec/wp-content/uploads/downloads/2014/05/PLAN-ESTRAT%C3%89GICO-2014-02-28.pdf

CTMA. (18 de marzo de 2021). *¿Qué es la norma ISO/IEC 25000? Calidad de software*. Obtenido de https://ctmaconsultores.com/norma-iso-25000/

Cummins, A. (10 de septiembre de 2013). *AIDE: Una IDE para programar Apps APK directamente en tu dispositivo Android*. Obtenido de https://geeksroom.com/2013/09/aide-una-ide-para-programar-apps-directamente-en-tu-dispositivo-android/78558/

D'Amato, J. (2016). *Plataforma abierta de gestión de cámaras IP y aplicaciones móviles para la seguridad civil ciudadana*. Obtenido de http://www.scielo.mec.pt/pdf/rist/n20/n20a05.pdf

Dart. (2021). *Dart overview*. Obtenido de https://dart.dev/overview

Digital Guide. (15 de agosto de 2018). *¿Qué es Ethernet (IEEE 802.3)?* Obtenido de https://www.ionos.es/digitalguide/servidores/know-how/ethernet-ieee-8023/

Dotcom. (2020). *Descripción general de los tipos de monitoreo disponibles*. Obtenido de https://www.dotcom-monitor.com/wiki/es/knowledge-base/descripcion-general-de-los-tipos-de-monitoreo-disponibles/

ECU911. (2021). *Cámaras de Videovigilancia*. Obtenido de https://www.ecu911.gob.ec/camaras-de-videovigilancia/

Fabregas, J. (2010). *Gerencia de servicios (Basado en ITIL)* . Obtenido de http://gsti.yolasite.com/resources/ITIL-08-Monitorizacion-Control.pdf

Ferri, A. (14 de febrero de 2019). *Monitorización activa vs. monitorización pasiva*. Obtenido de https://blog.a3sec.com/monitorizaci%C3%B3n-activa-vs.-monitorizaci%C3%B3n-pasiva

García, J., & Roa, C. (2020). *Diseño de una herramienta de monitoreo y control de servidores utilizando como eje principal CACTI. Aplicado a una PYME mediana.* Obtenido de https://repository.ucc.edu.co/bitstream/20.500.12494/16571/3/2020-Herramienta_monitoreo_servidores.pdf

Gimenez, A. (04 de agosto de 2017). *Xamarin, desarrollo multiplataforma nativo*. Obtenido de https://www.hiberus.com/crecemos-contigo/xamarin-desarrollo-multiplataforma-nativo/

GreenCore. (2015). *Herramientas de monitoreo*. Obtenido de https://www.greencore.co.cr/herramientas-de-monitoreo.html#:~:text=Son%20sistemas%20de%20diagn%C3%B3stico%20para,electr%C3%B3nico%2C%20sms%2C%20entre%20otros

Heidelberg. (2021). *Predictive Monitoring*. Obtenido de https://www.heidelberg.com/global/en/services_and_consumables/digital_services/predictive_monitoring_1/predictive_monitoring_1.jsp

Ibañez, A. M. (17 de septiembre de 2017). *ISO 9001:2015 base para la sostenibilidad de las organizaciones en países emergentes*. Obtenido de https://www.redalyc.org/journal/290/29055967003/html/

imasdetres. (2021). *Cámaras ANPR IP lectoras de placas*. Obtenido de https://imasdetres.com/mx/camaras-anpr-ip-lectoras-de-placas/

INSOC. (13 de abril de 2020). *Mejores herramientas de monitoreo 2020*. Obtenido de https://www.insoc.com.mx/post/mejores-herramientas-de-monitoreo-2020

Intelegia. (2020). *Tipos de bases de datos*. Obtenido de https://intelequia.com/blog/post/2062/tipos-de-base-de-datos

Java. (2022). *Conozca más sobre la tecnología Java*. Obtenido de https://www.java.com/es/about/

Karlson, C. (2016). *Control of critical data flows*. Obtenido de http://kth.diva-portal.org/smash/get/diva2:931374/FULLTEXT01.pdf

Leaty, J. (2012). *Sistema para la visualización de datos georreferenciados en ambientes web*. Obtenido de https://dspace.uclv.edu.cu/bitstream/handle/123456789/8797/Tesis%20Jorge%20Leaty%20Voronina.pdf?sequence=1&isAllowed=y

Lerena, S., Villanueva, D., Gonzáles, J., Lerena, J., Concepción, P., & Novoa, R. (20 de octubre de 2010). *PANDORAFMS Manual del administrador*. Obtenido de https://pandorafms.com/downloads/PDF/PandoraFMS_Manual_3.2_ES.pdf

Lizarraga, K. (09 de diciembre de 2020). *Implementación de Flutter para el desarrollo de aplicaciones móviles nativas en iOS y Android*. Obtenido de http://repositorio.upsin.edu.mx/formatos/A031LIZARRAGAOSUNAKEVINANTONIO6608.pdf

Marcela. (2009). *Base de datos estatica*. Obtenido de http://3.bp.blogspot.com/-n4uDAn-Go6Q/TV112f7pgLI/AAAAAAAAABg/vAgcaKjSpzA/s1600/estatica.gif

Miller, F. (05 de diciembre de 2018). *Las seis características principales de la red Ethernet y IP convergente realmente preparada para el futuro*. Obtenido de https://www.ciena.com.mx/insights/articles/The-top-6-features-of-a-truly-future-proof-converged-Ethernet-and-IP-network_es_LA.html

Molina, P., & Morales, C. (julio de 2015). *Norma ISO/IEC 25000*. Obtenido de https://revistas.udistrital.edu.co/index.php/tia/article/view/8373/11349

Mora, S. L. (17 de mayo de 2020). *Firebase: qué es, para qué sirve, funcionalidades y ventajas*. Obtenido de https://www.digital55.com/desarrollo-tecnologia/que-es-firebase-funcionalidades-ventajas-conclusiones/

Morales, S., & Moreno, L. (2020). *SISTEMA DE APLICACIONES MÓVILES PARA EL MEJORAMIENTO DE LA COMUNICACIÓN ENTRE COMUNIDAD Y ESTACIÓN*

DE BOMBEROS DEL MUNICIPIO DE SAHAGÚN. Obtenido de https://repositorio.unicordoba.edu.co/bitstream/handle/ucordoba/2702/SergioEricMoralesRicardo-LuisAngelMorenoSarabia.pdf?sequence=1&isAllowed=y

Naser, A., & Concha, G. (2011). *El gobierno electrónico en la gestión pública*. Obtenido de https://repositorio.cepal.org/bitstream/handle/11362/7330/1/S1100145_es.pdf

Nielfa, J. (2021). *Android Studio: El entorno de desarrollo oficial de Android*. Obtenido de https://scoreapps.com/blog/es/android-studio/

Niño Rojas, V. (2011). *Metodología de la investigación.* Bogotá: Ediciones de la U.

Novelec. (12 de enero de 2021). *Cámaras CCTV, tipos y características*. Obtenido de https://blog.gruponovelec.com/seguridad/camaras-cctv-tipos-y-caracteristicas/

Once, I. (2017). *Aplicación de monitoreo de los dispositivos de una red utilizando tecnologia JAVA*. Obtenido de https://dspace.uazuay.edu.ec/bitstream/datos/7420/1/13328.pdf

OpManager. (2020). *Herramientas gratuitas para el monitoreo de redes pequeñas*. Obtenido de https://www.manageengine.com/latam/network-monitoring/network-monitoring-tool.html

Oracle. (2020). *what-is-a-relational-database*. Obtenido de https://www.oracle.com/ar/database/what-is-a-relational-database/

Pandora. (2022). Obtenido de https://pandorafms.com/manual/es/documentation/04_using/09_dashboard

PANDORAFMS. (2020). *DOSSIER INFORMATIVO* . Obtenido de https://pandorafms.com/downloads/kit_de_prensa_Pandora.pdf

Pérez, E. (22 de diciembre de 2017). *LOS 7 PRINCIPIOS DE GESTIÓN DE LA CALIDAD EN ISO 9001*. Obtenido de https://www.3ciencias.com/wp-content/uploads/2018/01/art_2.pdf

Peris, L. (2016). Obtenido de https://luisperis.com/redis/

Peris, L. (18 de febrero de 2016). *Redis: Base de datos NoSQL*. Obtenido de https://luisperis.com/redis/

Piug, S. (2016). *FAULT DIAGNOSIS TOOLS IN MULTIVARIATE STATISTICAL PROCESS AND QUALITY CONTROL* . Obtenido de https://riunet.upv.es/bitstream/handle/10251/61292/Vidal%20-%20FAULT%20DIAGNOSIS%20TOOLS%20IN%20MULTIVARIATE%20STATISTICAL%20PROCESS%20AND%20QUALITY%20CONTROL.pdf?sequence=1

PowerData. (2020). *Desmitificando el Data Governance: Qué, cuándo, dónde y por qué*. Obtenido de https://www.powerdata.es/data-governance

PowerData. (2020). *El gobierno de datos eficaz*. Obtenido de https://f.hubspotusercontent30.net/hubfs/239039/%5BPWD%5D%20Ebooks%20Archivos/Ebook%2017.%20%5BPWD%5D%20Data%20Governance%20El%20gobierno%20de%20datos%20eficaz/EBOOK%20%7C%20El%20gobierno%20de%20datos%20eficaz.pdf

principiantes, R. p. (2018). Obtenido de https://blog.bi-geek.com/redis-para-principiantes/

Quispe, J. (2018). *IMPLEMENTACIÓN DE UN SISTEMA DE MONITOREO Y CONTROL DE RED, PARA UN CANAL DE TELEVISIÓN, BASADO EN HERRAMIENTAS OPEN SOURCE Y SOFTWARE LIBRE*. Obtenido de http://repositorio.unap.edu.pe/bitstream/handle/UNAP/9019/Quispe_Bustincio_Jhon_Watson.pdf?sequence=1&isAllowed=y

Ramírez, F. (21 de julio de 2017). *Cacti, Monitoreo de Red y Reportes Gráficos OpenSpurce*. Obtenido de https://itsoftware.com.co/content/cacti-sistema-recoleccion-datos-graficas/

Robledano, Á. (2019). Obtenido de https://openwebinars.net/blog/que-es-mongodb/

Robledano, Á. (28 de octubre de 2019). *Qué es MongoDB.* Obtenido de https://openwebinars.net/blog/que-es-mongodb/

Rojas, J. (2017). *DVR: qué son, tipos y cuáles son sus principales características*. Obtenido de https://www.tecnoseguro.com/faqs/cctv/dvr-que-es-tipos-caracteristicas

RS Components. (2020). *Monitores de Videovigilancia (CCTV)*. Obtenido de https://es.rs-online.com/web/c/seguridad-y-herrajes-para-puertas-y-ventanas/videovigilancia/monitores-de-videovigilancia-cctv/

Sanchez, A. (24 de junio de 2014). *AIDE una aplicación para programar desde tu Smartphone sin estar atado a tu PC*. Obtenido de https://www.azulweb.net/aide-una-aplicacion-para-programar-desde-tu-smartphone-sin-estar-atado-tu-pc/

SECURTECH. (2021). *CÁMARA LECTORA DE PLACA*. Obtenido de https://securtech.com.ec/productos/camaras-de-video-vigilancia/camara-lectora-de-placa/

Serrato, C. (18 de marzo de 2020). *Ventajas y desventajas de apps desarrolladas en Xamarin*. Obtenido de https://inmediatum.com/blog/ingenieria/ventajas-y-desventajas-de-apps-desarrolladas-en-xamarin/

Sosio, N. (2021). *Nvr – ¿Qué es un NVR para cámaras IP?* Obtenido de https://www.seguridadsos.com.ar/nvr/

Spiegato. (2022). *¿Qué es el desarrollo móvil de Java?* Obtenido de https://spiegato.com/es/que-es-el-desarrollo-movil-de-java

Tecnitran. (2019). *Cámaras IP fijas*. Obtenido de https://www.tecnitran.es/videovigilancia/camaras-de-videoviglancia-ip/camaras-ip-fijas/

Teledyne. (2021). *FLIR Quasar™ Premium Mini-Dome*. Obtenido de https://www.flir.com.mx/products/quasar-premium-mini-dome/

Universidad Camilo José Cela. (2021). *Riak; Sistema para todos los gustos.* Obtenido de https://master-bigdata.com/riak-sistemas-nosql-todos-los-gustos/

Universitat Oberta de Catalunya. (2021). *Espacio de recursos de ciencia de datos.* Obtenido de http://datascience.recursos.uoc.edu/es/riak-2/

Vargas, A. (junio de 2018). *Diseño e implementación de un sistema de visualización de datos de fuentes abiertas* . Obtenido de https://repositorio.uam.es/bitstream/handle/10486/688297/vargas_c%c3%a1novas_franciscoantonio_tfg.pdf?sequence=1&isAllowed=y

VegaGestión . (08 de Febrero de 2018). *https://vegagestion.es/la-infraestructura-tecnologica-definicion-tipos-e-importancia/*. Obtenido de https://vegagestion.es/la-infraestructura-tecnologica-definicion-tipos-e-importancia/

Xeral. (2018). *La infraestructura tecnológica: definición, tipos e importancia.* Obtenido de https://vegagestion.es/la-infraestructura-tecnologica-definicion-tipos-e-importancia/

VII. ANEXOS

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

Educamos para transformar el mundo

ACTA

DE LA SUSTENTACIÓN DE PREDEFENSA DEL DEL TRABAJO DE INTEGRACIÓN CURRICULAR:

NOMBRE BRAYAN DAVID GUERRÓN TAPIA **CÉDULA DE IDENTI** 0402082986
NIVEL/PARALELO: 0 **PERIODO ACADÉMI** 0

TEMA DEL TIC: Herramientas de monitoreo de datos para infraestructura tecnológica

Tribunal designado por la dirección de esta Carrera, conformado por:
PRESIDENTE: MSC. JAIRO VLADIMIR HIDALGO GUIJARRO
DOCENTE TUTOR: MSC. MILTON GABRIEL DEL HIERRO MOSQUERA
DOCENTE: MSC. JORGE HUMBERTO MIRANDA REALPE

De acuerdo al artículo 32: Una vez entregados los documentos; y, cumplidos los requisitos para la realización de la pre-defensa el Director/a de Carrera designará el Tribunal, fijando lugar, fecha y hora para la realización de este acto:

EDIFICIO DE AULAS 4 **AULA:** 108
FECHA: 18 de agosto de 2022
HORA: 16H30
Obteniendo las siguientes notas:

1) Sustentación de la predefensa:	4.80
2) Trabajo escrito	2.20
Nota final de PRE DEFENSA	**7.00**

Por lo tanto: **APRUEBA CON OBSERVACIONES** ; debiendo acatar el siguiente artículo:

Art. 36.- De los estudiantes que aprueban el informe final del TIC con observaciones.- Los estudiantes tendrán el plazo de 10 días para proceder a corregir su informe final del TIC de conformidad a las observaciones y recomendaciones realizadas por los miembros del Tribunal de sustentación de la pre-defensa.

Para constancia del presente, firman en la ciudad de Tulcán el 18 de agosto de 2022

MSC. JAIRO VLADIMIR HIDALGO GUIJARRO
PRESIDENTE

MSC. MILTON GABRIEL DEL HIERRO MOSQUERA
DOCENTE TUTOR

MSC. JORGE HUMBERTO MIRANDA REALPE
DOCENTE

Adj.: Observaciones y recomendaciones

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

ACTA

DE LA SUSTENTACIÓN DE PREDEFENSA DEL DEL TRABAJO DE INTEGRACIÓN CURRICULAR:

NOMBRE JHONATAN PAÚL GUEVARA CASTILLO **CÉDULA DE IDENTE** 0402127344
NIVEL/PARALELO: 0 **PERIODO ACADÉMI** 0

TEMA DEL TIC: Herramientas de monitoreo de datos para infraestructura tecnológica

Tribunal designado por la dirección de esta Carrera, conformado por:
PRESIDENTE: MSC. JAIRO VLADIMIR HIDALGO GUIJARRO
DOCENTE TUTOR: MSC. MILTON GABRIEL DEL HIERRO MOSQUERA
DOCENTE: MSC. JORGE HUMBERTO MIRANDA REALPE

De acuerdo al artículo 32: Una vez entregados los documentos y cumplidos los requisitos para la realización de la pre-defensa el Directorio de Carrera designará el Tribunal, fijando lugar, fecha y hora para la realización de este acto.

EDIFICIO DE AULAS 4 **AULA:** 108
FECHA: 18 de agosto de 2022
HORA: 16H30
Obteniendo las siguientes notas:

1) Sustentación de la predefensa:	4.80
2) Trabajo escrito	2.20
Nota final de PRE DEFENSA	**7.00**

Por lo tanto: **APRUEBA CON OBSERVACIONES** ; debiendo acatar el siguiente artículo:

Art. 38.- De los estudiantes que aprueban el informe final del TIC con observaciones.- Los estudiantes tendrán el plazo de 10 días para proceder a corregir su informe final del TIC de conformidad a las observaciones y recomendaciones realizadas por los miembros del Tribunal de sustentación de la pre-defensa.

Para constancia del presente, firman en la ciudad de Tulcán el 18 de agosto de 2022

MSC. JAIRO VLADIMIR HIDALGO GUIJARRO
PRESIDENTE

MSC. MILTON GABRIEL DEL HIERRO MOSQUERA
DOCENTE TUTOR

MSC. JORGE HUMBERTO MIRANDA REALPE
DOCENTE

Adj.: Observaciones y recomendaciones

Anexo 1: Certificado de aprobación del Abstract

UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI
FOREIGN AND NATIVE LANGUAGE CENTER

Informe sobre el Abstract de Artículo Científico o Investigación.

Autor: Guerrón Tapia Brayan David - Guevara Castillo Jhonatan Paúl

Fecha de recepción del abstract: 16 de septiembre de 2022

Fecha de entrega del informe: 16 de septiembre de 2022

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
PENAFIEL ARCOS

Ing. Edison Peñafiel Arcos MSc
Coordinador del CIDEN

UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI
FOREIGN AND NATIVE LANGUAGE CENTER

ABSTRACT- EVALUATION SHEET

NAME: Guerrón Tapia Brayan David - Guevara Castillo Jhonatan Paúl **DATE:** 16 de septiembre de 2022

TOPIC: "Herramientas de monitoreo de datos para infraestructura tecnológica."

REMARKS 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: 1,5 ☐	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

1

Anexo 2: Informe Antiplagio

turnitin

Recibo digital

Este recibo confirma quesu trabajo ha sido recibido por Turnitin. A continuación podrá ver la información del recibo con respecto a su entrega.

La primera página de tus entregas se muestra abajo.

Autor de la entrega:	Guevara Guerrón
Título del ejercicio:	Tesis primera revisión
Título de la entrega:	Tesis primera revisión
Nombre del archivo:	TESIS_PREFINAL.pdf
Tamaño del archivo:	6.86M
Total páginas:	173
Total de palabras:	27,234
Total de caracteres:	164,769
Fecha de entrega:	10-ago.-2022 10:19a. m. (UTC-0500)
Identificador de la entre...	1881036729

UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI

FACULTAD DE INDUSTRIAS AGROPECUARIAS Y CIENCIAS AMBIENTALES

CARRERA DE COMPUTACIÓN

PLAN DE INVESTIGACIÓN

Tema: "Herramientas de minimoco de datos para infraestructura tecnológica"

Trabajo de titulación previa la obtención del título de Ingeniero en Ciencias de la Computación

AUTORES: Guerrón Tapia Brayan David
Guevara Castillo Jhonatan Paúl

TUTOR: MSC. Milton del Hierro Mosquera

Tulcán, 2022

Tesis primera revisión

INFORME DE ORIGINALIDAD

6%	6%	1%	3%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	docplayer.es Fuente de Internet	1%
2	www.redalyc.org Fuente de Internet	1%
3	blog.a3sec.com Fuente de Internet	1%
4	ayudaleyprotecciondatos.es Fuente de Internet	1%
5	repositorio.ug.edu.ec Fuente de Internet	1%
6	sites.google.com Fuente de Internet	1%
7	repositorio.unesum.edu.ec Fuente de Internet	1%
8	es.scribd.com Fuente de Internet	1%

ANEXO 3: SOLICITUD PROYECTO EN ECU 911

MAGISTER

Xavier Narváez

JEFE OPERATIVO DEL CENTRO LOCAL ECU 911 "TULCÁN"

Presente.

Reciba un atento y cordial saludo, a la vez que le deseamos éxitos en las funciones que usted acertadamente desempeña.

Nosotros, **Brayan David Guerrón Tapia** y **Jonathan Paúl Guevara Castillo** estudiantes del noveno nivel de la carrera de Computación de la Universidad Politécnica Estatal del Carchi, solicitamos de la manera más comedida se nos autorice realizar los trabajos de integración curricular en el área de **Tecnología**

Por la atención que se digne dar al presente, reciba nuestros agradecimientos.

Atentamente,

David Guerrón	Jonathan Guevara
CC: 0402082986	CC: 0402127344

ESTUDIANTES DE LA UPEC

Recibido
25-01-2021
11:50

SERVICIO INTEGRADO DE SEGURIDAD ECU 911

Oficio Nro. SIS-COL1T-2021-014-OF

Tulcán, 26 enero de 2021

ASUNTO: Autorización elaboración trabajo de integración.

Sr.
Brayan Guerrón
ESTUDIANTE UPEC

Sr.
Jonathan Guevara
ESTUDIANTE UPEC

De mi consideración:

Ante solicitud presentada para la elaboración de trabajo de integración curricular en el área de Tecnología Local, autorizó la elaboración de proyecto en el área indicada.

Con sentimientos de consideración y estima.

Atentamente,

Msc. Olmedo Xavier Narváez Montenegro
JEFE DEL CENTRO OPERATIVO LOCAL ECU 911 TULCÁN

SERVICIO INTEGRADO DE SEGURIDAD ECU 911 JEFATURA LOCAL TULCÁN

Dirección: Av. Veintimilla y Alejandro R. mera/Tulcán-Ecuador
Teléfono:593-2-961-002-www.ecu911.gob.ec

ANEXO 4: PREGUNTAS DE ENCUESTA

ENCUESTAS SEMIESTRUCTURADA

UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI

FACULTAD DE INDUSTRIAS AGROPECUARIAS Y CIENCIAS AMBIEgNTALES

CARRERA DE COMPUTACIÓN

ENCUESTA AL PERSONAL DEL ÁREA DE TECNOLOGÍA DEL ECU 911

OBJETIVO: Un saludo cordial de parte de los estudiantes quienes estamos desarrollando el tema de investigación: "Herramientas de monitoreo de datos para infraestructura tecnológica", el propósito de esta encuesta es para recolectar información acerca del área de tecnología del ECU 911, los datos obtenidos de esta encuesta serán confidenciales y no serán divulgados fuera de la investigación.

El monitoreo de datos es el seguimiento a determinadas acciones que podemos cuantificar y que nos arrojaran datos relevantes para la empresa, de acuerdo con este criterio conteste las siguientes preguntas.

1) **¿Está de acuerdo que el área de tecnología cuente con servicios para el monitoreo de datos de dispositivos tecnológicos?**

   a) Muy de acuerdo

   b) Acuerdo

   c) Ni de acuerdo ni en desacuerdo

   d) Desacuerdo

2) **¿Cuál es el promedio de cámaras IP que operan en la infraestructura tecnológica?**

   a) De 10 a 50
   b) De 100 a 200
   c) 200 o más

3) **¿Conoce usted herramientas que permitan monitorear dispositivos tecnológicos cada que sufren una desconexión?**

a) Si
b) No
c) No estoy seguro

4) ¿Cómo se reportan los errores que tienen las cámaras o servidores del centro local?

a) Escritura manual
b) Digital (Computadora)
c) Otros. Indique: _____

5) ¿Con que frecuencia se reportan los errores o caídas de cámaras o servidores?

a) Mensual
b) Semanal
c) Diaria
d) Otros: Indique: _____

6) ¿Cuál cree que es la importancia de una herramienta de monitoreo de datos para el beneficio de la gestión administrativa?

a) Muy importante
b) Importante
c) Neutral
d) Nada importante

7) ¿Cuál de las siguientes herramientas se utiliza dentro del Ecu 911?

a) Cacti
b) Nagios
c) Pandora
d) Kali Linux
e) GroudWork
f) Zenoss
g) Op5 Monitor

8) ¿El Ecu 911 cuenta con un registro o base de datos del historial de las cámaras o servidores caídos?

a) Si

b) No

ANEXO 5: MANUAL TÉCNICO PANDORA FMS

INSTALACIÓN DE PANDORA FMS

Requisitos mínimos hardware

Requisitos para la consola y el servidor

Hasta 500 agentes o 5.000 módulos

3GB de RAM y una CPU de un sólo núcleo a 2GHz de reloj. Disco duro rápido, 7200rpm o equivalente. Se supone que el 80% de los módulos tienen histórico y que la media de muestreo es de 5 minutos.

Hasta 2.000 agentes o 10.000 módulos

6GB de RAM y una CPU de doble núcleo a 2.5GHz de reloj y disco duro rápido (7.200 rpm o más). Se supone que el 80% de los módulos tienen histórico y que la media de muestreo es de 5 minutos. Deberá configurar muy bien MySQL para que aguante la carga.

Requisitos mínimos de software

La plataforma oficial de Pandora FMS es Linux. Desde la versión 5.1 también se soporta Windows Server. Oficialmente se soportan, para el servidor y la consola, las siguientes versiones:

Tabla

Requisitos de Software

Componente	Sistema Operativo
Pandora FMS 5.1 o superior	Windows Server (2003 o superior) RedHat Enterprise (RHEL) 6.x CentOS 6.x SLES 11 SP1 o superior Debian 5.x o superior.

Fuente: Elaborado por Autores

Requisitos de Base de datos

Antes de comenzar a instalar Pandora FMS, necesita tener un servidor de MySQL funcionando (Oracle y PostgreSQL se soportan, pero todavía de forma experimental). Esto significa que antes de instalar Pandora, necesita tener corriendo, bien configurado y operativo, el software de base de datos MySQL, puede estar en el mismo servidor físico donde quiere ejecutar Pandora FMS, o en un servidor independiente, de forma que la consola y el servidor, accedan a él a través de la red, vía TCP/IP. En resumen, necesitará:

1. Dirección IP de su MySQL Server, o 'localhost' si se instala en el mismo servidor de Pandora.
2. Usuario con privilegios para crear bases de datos y usuarios (generalmente root). Este usuario deberá poderse conectar desde la IP del servidor donde instalemos Pandora FMS.
3. Password del usuario con privilegios

Requisitos para el servidor

Aunque puede trabajar sobre cualquier sistema operativo con Perl 5.8 instalado y con iThreads habilitados, se recomienda y está soportado únicamente sobre Linux y FreeBSD. También funciona sobre sistemas Solaris.

Hay que destacar que Pandora FMS necesita un servidor MySQL para almacenar toda la información. Este servidor puede instalarse en cualquier plataforma soportada por MySQL (Windows, Linux, Solaris, etc).

Requisitos para la consola

De igual manera que el servidor, se recomienda su operación sobre sistemas Linux, pero dado que la interfaz web es una aplicación AMP pura (Apache, MySQL y PHP), podría trabajar teóricamente sobre cualquier sistema que lo soporte: Windows, Unix, etc.

Cuestiones previas a la instalación

MySQL

Necesitará un servidor MySQL operativo ANTES de instalar Pandora, ya que el siguiente paso tras instalar los paquetes de Pandora, es configurar el acceso a la BBDD de datos. Si

está instalando Pandora FMS a la vez que el servidor MYSQL, recuerde que tiene que arrancar y configurar el acceso al usuario root de MySQL. Esto se hace mediante dos comandos:

1. Arrancar:

```
Last login: Mon Aug 29 16:46:45 2022 from 190.107.236.28
[root@svr ~]# /etc/init.d/mysql start
```

2. Configurar el password de root

```
[root@svr ~]# cd .
[root@svr ~]# mysqladmin password <password>
```

Donde '<password>' es el password que establece para el usuario root. Este password se le pedirá en el proceso de instalación de Pandora FMS.

Orden de instalación de Pandora FMS

Es recomendable seguir el siguiente orden al instalar Pandora FMS:

1. **Instalar la consola**
2. **Instalar el servidor**

La razón es que la base de datos MySQL que usa el servidor se crea en el proceso de configuración inicial de la consola, y por ello para asegurar el correcto funcionamiento del servidor es recomendable realizar primero el proceso de instalación completo de la consola. Además, no es necesario que la consola y el servidor de Pandora FMS se encuentren alojados en la misma máquina, ya que es posible indicarle al servidor dónde se encuentra la base de datos MySQL mediante el archivo de configuración del servidor.

La instalación del agente la podemos realizar sin ningún problema antes o después de instalar el servidor y la consola ya que es independiente de estos y puede estar instalado en cualquier máquina.

Instalación Linux / CentOS

Lo primero de todo, deberá activar ciertos repositorios oficiales de CentOS para realizar la instalación de dependencias.

```
[updates]
name=CentOS-$releasever
Updates mirrorlist=http://mirrorlist.centos.org/?release=$releasever&arch=$basearch&re gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-6

[extras]
name=CentOS-$releasever
Extras mirrorlist=http://mirrorlist.centos.org/?release=$releasever&arch=$basearch&re gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-6
```

Añada el repositorio EPEL:

```
[EPEL]
Name = EPEL
baseurl = http://dl.fedoraproject.org/pub/epel/6/$basearch/
enabled = 1
gpgcheck = 0
```

Y actualice la información de sus repositorios:

```
[root@svr ~]# yum makecache
```

Instalación Pandora FMS

Para poder realizar esta instalación, necesita YUM y acceso a internet. Primero cree el repositorio oficial de Pandora para CentOS 6.

```
[root@svr ~]# vi /etc/yum.repos.d/pandorafms.repo
```

Instale Pandora FMS, junto con el servidor MySQL (es una dependencia opcional, pero necesitará un servidor MySQL si no tiene uno ya instalado o accesible en otro servidor).

```
[root@svr ~]# yum install pandorafms_console pandorafms_server mysql-server
```

Descargará todos los paquetes necesarios y dejará el sistema listo para su configuración y uso.

Instalación de la Consola

No existe fichero de paquetes de la consola de pandora para FreeBSD. Deberá instalar la consola de pandora utilizando el instalador.

```
[root@svr ~]# /usr/local/www/apache22/data/pandora_console
```

Instalación del Servidor

No existe fichero de paquetes del servidor de pandora para FreeBSD. Tendrá que instalar el servidor de pandora utilizando el instalador.

La ubicación del fichero y en la estructura del script de arranque son diferentes respecto a Linux.

Veremos las peculiaridades de FreeBSD más abajo.

Después de realizar la instalación, deberá añadir las siguientes líneas a /etc/rc.conf.

```
  GNU nano 2.3.1

pandora_server_enable="YES"
tentacle_server_enable="YES"
```

Script de inicio:

```
  GNU nano 2.3.1

/usr/local/etc/rc.d/pandora_server
/usr/local/etc/rc.d/tentacle_server
```

Fichero de configuración:

```
[root@svr ~]# /usr/local/etc/pandora/pandora_server.conf
```

util:

```
[root@svr ~]# /usr/local/share/pandora_server/util/*
```

Man pages:

```
[root@svr ~]# /usr/local/man/man1/*
```

Instalación del agente

Se deberá instalar el agente de pandora utilizando el instalador.

La localización de los ficheros y la estructura del script de inicio son diferentes respecto a Linux.

Después de la instalación, deberá añadir la siguiente línea a /etc/rc.conf.

Para habilitar el agente de pandora, se necesitan estos ajustes, de otro modo no se podrán iniciar el proceso.

Agente:

```
[root@svr ~]# /usr/local/bin/pandora_agent
```

Script de Arranque:

```
[root@svr ~]# /usr/local/etc/rc.d/pandora_agent
```

Fichero de configuración:

```
[root@svr ~]# /usr/local/etc/pandora/pandora_agent.conf
```

Plugins:

```
[root@svr ~]# /usr/local/share/pandora_agent/plugins/*
```

CONFIGURACIÓN INICIAL DESPUÉS DE LA INSTALACIÓN

El orden que debe seguir después de la instalación es:

1. Crear la base de datos, mediante el wizard de instalación de la consola web de Pandora FMS.

2. Modificar las configuración del servidor, incluyendo las credenciales de acceso a la BBDD generadas por el paso anterior.
3. Arrancar servidor.
4. Arrancar agente local (si se necesita).
5. Acceder a la consola de Pandora FMS por primera vez para comenzar a usar Pandora FMS.

Configuración Inicial de la Consola

Estamos suponiendo que va a ejecutar todos los componentes (Base de datos, Consola, Servidor y Agente) sobre la misma máquina. Si todavía no lo ha hecho, arranque el servidor MySQL y establezca una contraseña de administrador (root).

```
[root@svr ~]# /etc/init.d/mysql start
```

Y ahora establezca la password, por ejemplo "pandora123" para el usuario root de su MYSQL:

```
[root@svr ~]# mysqladmin password pandora
```

Ahora levante el servidor Apache en su servidor:

```
[root@svr ~]# /etc/init.d/apache2 start
```

Ahora ya puede entrar vía web a la dirección IP de su servidor para realizar la post-instalación de Pandora FMS vía web. Esta post-instalación sirve para crear la base de datos de Pandora FMS y configurar en el servidor de Pandora las credenciales de acceso (usuario, password y nombre de BD) a la BBDD establecidas por el usuario.

Si la IP de su servidor es, por ejemplo, 190.214.2.XX, ponga en su navegador.

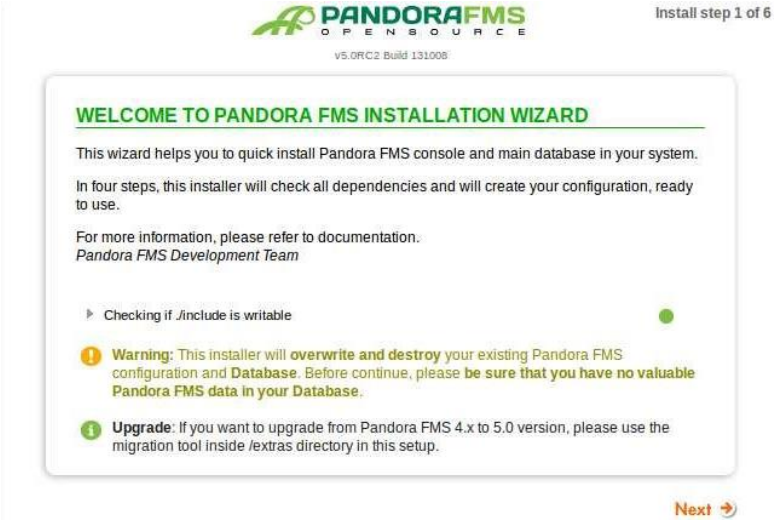
http://190.214.21.188:9000/pandora_console/install.php

A partir de ahora solo tiene que seguir los pasos que se le indican para crear la BBDD de Pandora FMS.

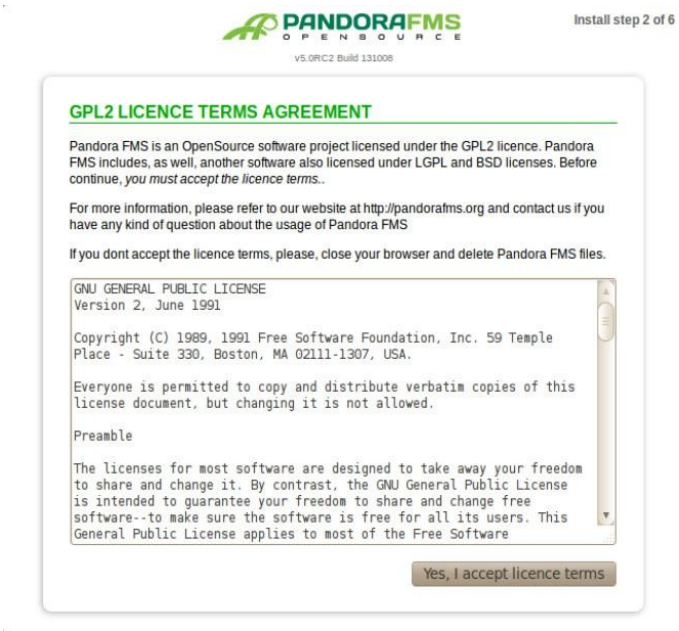
Instalación Software Pandora FMS

Paso 1. Instalación de Pandora con Wizard

Esta pantalla se utiliza para verificar que tiene todas las dependencias de software instaladas correctamente.



Paso 2. Aceptación de licencia



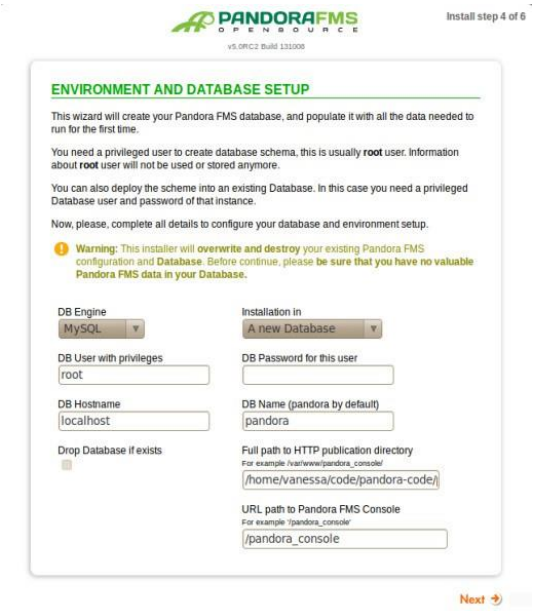
Paso 3. Instalación de Dependencias

En el caso de que necesite instalar alguna dependencia, será necesario reiniciar el servidor web para que éste las reconozca.

Paso 5. Configuración de base datos y acceso root

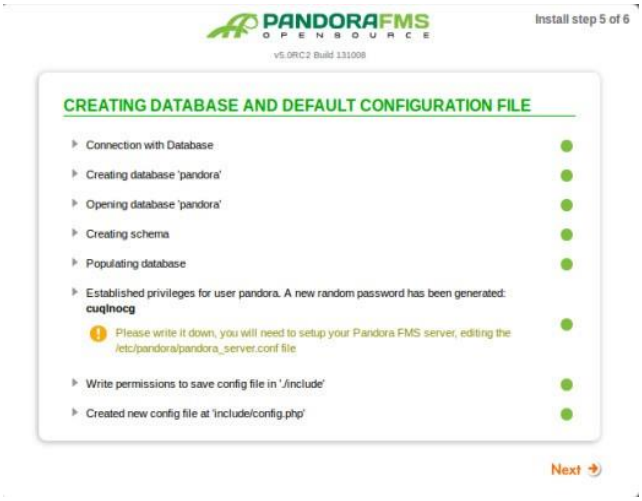
Aquí configura los datos de acceso a su servidor MySQL. Debe introducir la password de root que definió en el paso anterior.

Nota: Evite introducir espacios en el nombre de la base de datos.



Paso 6. Creación de la base de datos

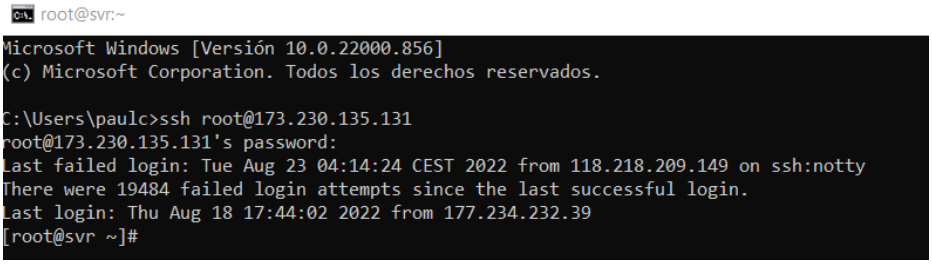
Aquí se muestra la contraseña de acceso a la base de datos.



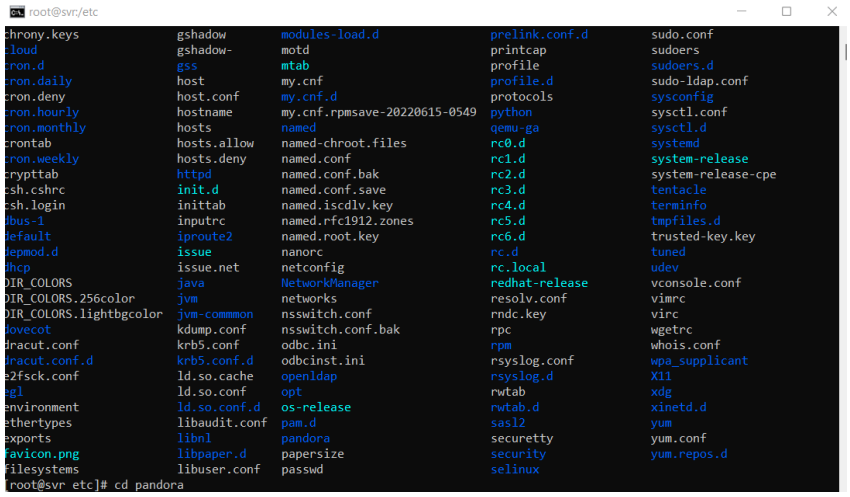
Paso 7. Finalización de la instalación.

Configuración de la base de datos dentro del servidor

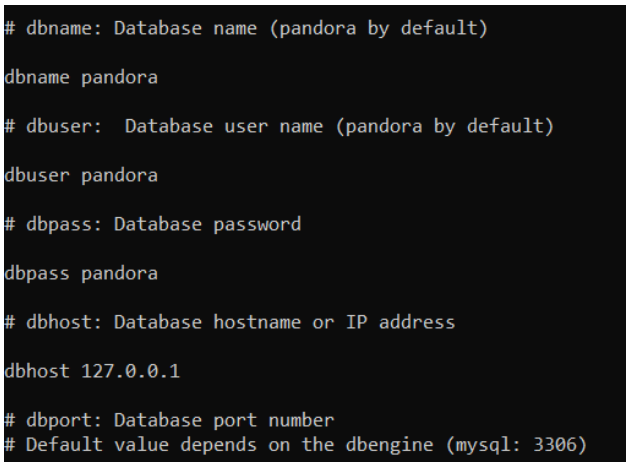
Ingreso a la base de datos en el servidor



Como primer paso para la configuración y designación de credenciales para la base de datos y puertos de comunicación es necesario acceder con el usuario y contraseña, en nuestro caso lo realizaremos por vía ssh.



El siguiente paso es comprobar los archivos que contiene nuestro servidor pandora, ya que aquí se realizaran las posteriores configuraciones.



Como último paso para la configuración de la base de datos es establecer un usuario y contraseña para su correcta conexión con los servicios que ofrece pandora, además de establecer el hostname o dirección IP del servicio de base de datos.

Respaldo y Recuperación Pandora FMS

Asegúrese de que su base de datos esté iniciada y en ejecución, y de que el servidor de Pandora FMS y el Agente software estén detenidos.

```
[root@localhost ~]# /etc/init.d/mysqld start
Starting mysqld: [ OK ]
[root@localhost ~]# /etc/init.d/pandora_server stop
Stopping Pandora FMS Server
[root@localhost ~]# /etc/init.d/pandora_agent_daemon stop
Stopping Pandora Agent.
```

Entonces, descomprima e importe la base de datos.

```
[root@localhost ~]# gunzip pandora.sql.gz
[root@localhost ~]# cat pandora.sql | mysql -u root -p pandora
Enter password: <enter the password in console>
```

Adicionalmente puede realizar la recuperación de la siguiente manera:

```
mysql –u root –p pandora
create database pandora;
use pandora;
source PATH BACKUP;
```

Recuperación de los ficheros de configuración

En primer lugar, recupere los ficheros de configuración de los Agentes y los servidores:

```
[root@localhost ~]# tar -zxvf pandora_configuration.tar.gz -C /
```

Recuperación del agente

Ahora, ejecute la recuperación del directorio del Agente Software:

```
[root@localhost ~]# tar -zxvf agent.tar.gz -C /
```

Recuperación del servidor

Restablezca el archivo principal del servidor de Pandora FMS, y cualquier otro archivo de plugin que tenga**:**

```
[root@localhost ~]# tar -zxvf pandora_server.tar.gz -C /
[root@localhost ~]# tar -zxvf my_plugin_folder.tar.gz -C /
```

Recuperación de la consola

Ahora ejecute una recuperación de la Consola, para restablecer las imágenes personalizadas, extensiones, etc.

```
[root@localhost ~]# tar -zxvf pandora_console.tar.gz -C /
```

Iniciar el servidor y el agente de Pandora FMS

El último paso es iniciar el servidor Pandora FMS y el Agente Software.

```
[root@localhost ~]# /etc/init.d/pandora_server start
[root@localhost ~]# /etc/init.d/pandora_agent_daemon start
```

Configuración Alertas vía Telegram

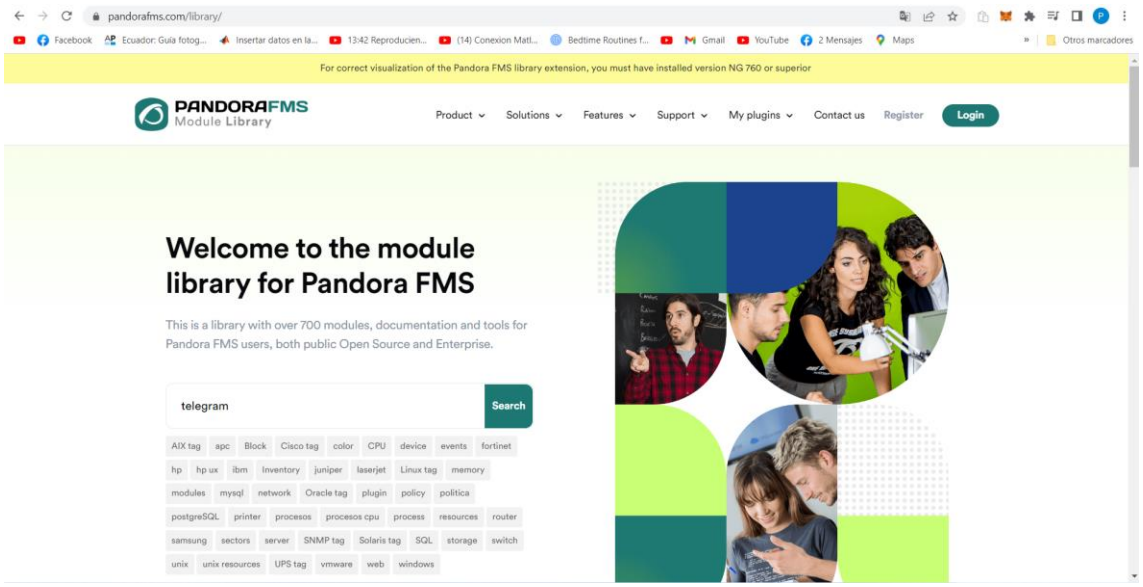


Figura 108. Ventana de vista de plugins de Pandora FMS

Buscamos el apartado de Telegram en donde nos mostrara los comandos para integrar en el servidor de pandora

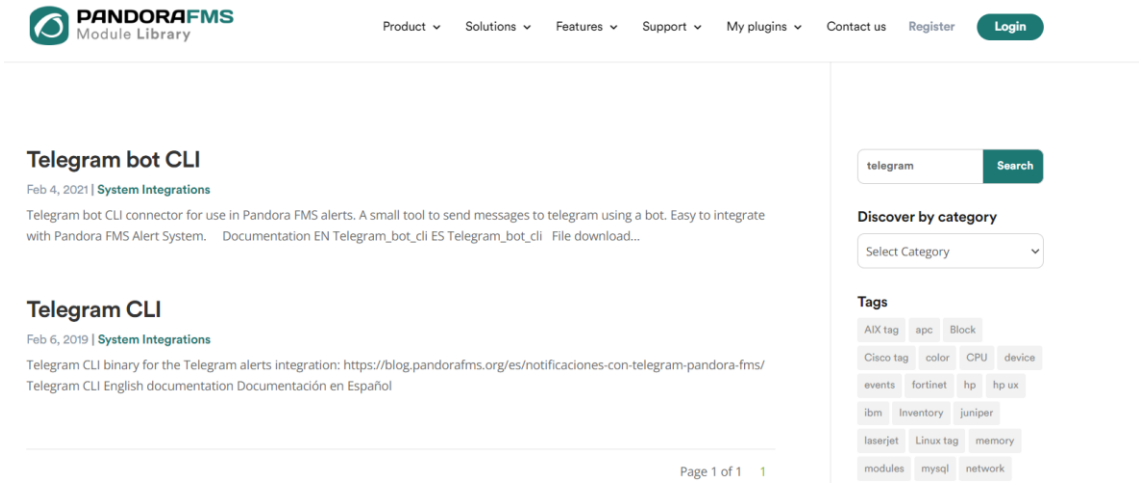


Figura 109. Ventana de plugins de Pandora (telegram)

Descargamos el archivo telegram-bot-cli para consecuentemente instalarlo en el servidor en donde este ubicado Pandora

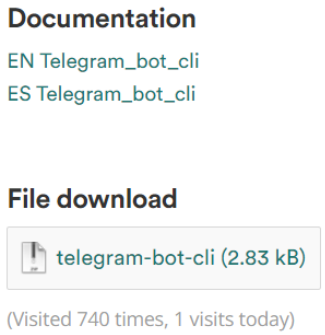


Figura 110. Archivo de descarga de telegram-bot-cli

Subimos el script a una ruta accesible en la máquina donde tengamos desplegado el servidor de Pandora FMS. No obstante, puede usar cualquier ubicación siempre que el servidor de pandora tenga acceso a esta.

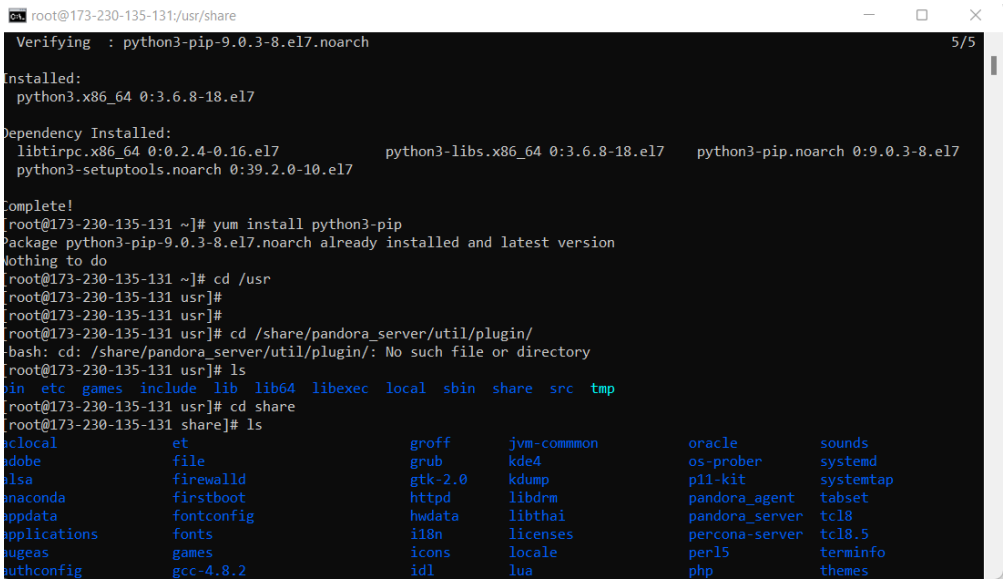


Figura 111. Configuración desde la consola para el script Telegram

Se procede da buscar la ruta donde se va a instalar el script de telegram en el servidor de Pandora en este caso en ‘plugins’

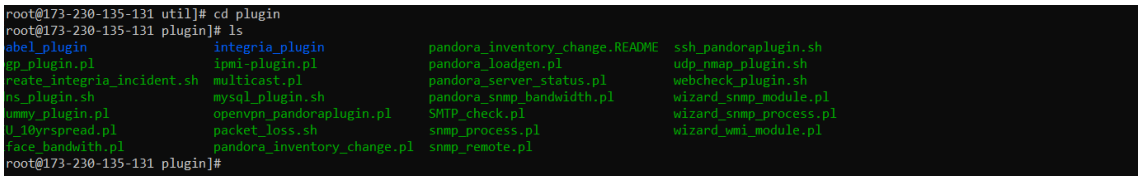


Figura 112. Directorio desde la consola de Pandora FMS

Una vez localizada la ruta, se procede a instalar el script previamente descargado de la página oficial, donde se procede a determinar los parámetros de: destinatario, mensaje, descripción, titulo, entre otros.

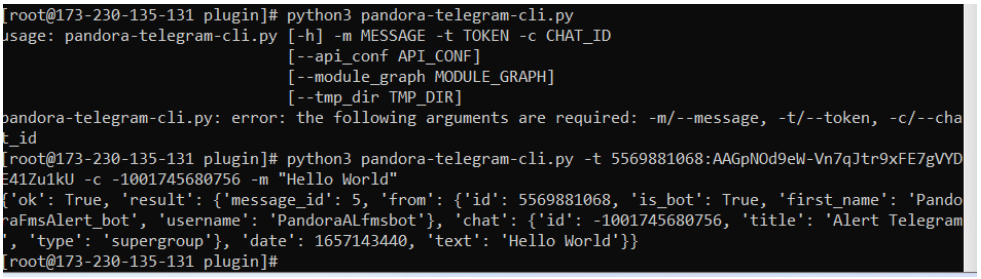


Figura 113. Configuración desde consola para el script Telegram

En esta parte de la configuración nos dirigimos a la consola web de pandora en la cual configuraremos un nuevo comando de alerta.

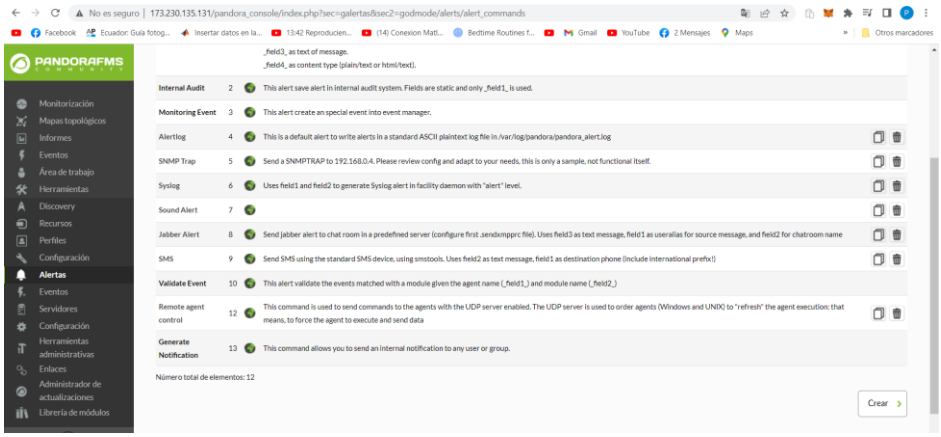


Figura 114. Creación de comando de alertas

En la parte de la configuración del comando insertamos un script de python3 el cual está instalado previamente en el servidor principal de pandora.

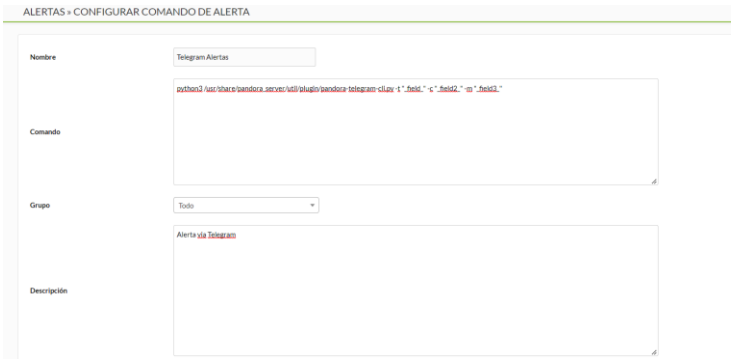


Figura 115. Script de Python 3 en comando de alertas

En la parte de descripción de los comandos procedemos a colocar las id de cada valor previamente configurado en telegram.

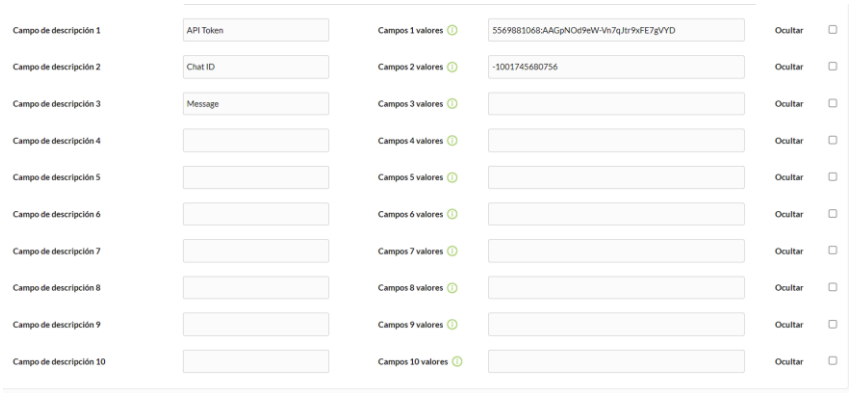


Figura 116. Inserción de ID en comandos de alertas

Manual de Usuario Creación de Informes Personalizados Ecu 911

Informes personalizados por cantón

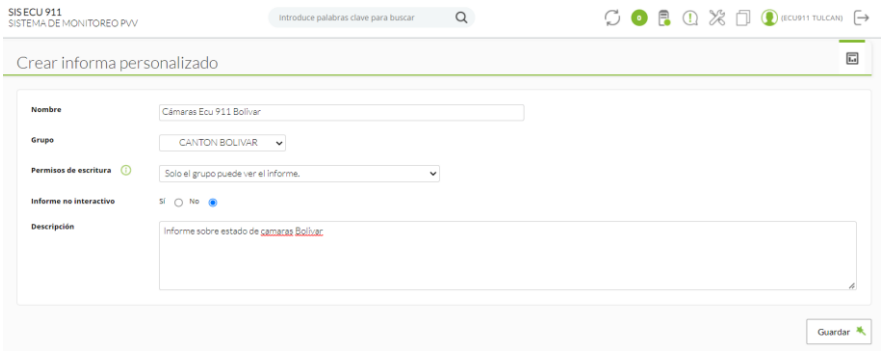


Figura 117. Creación de informe personalizado del Cantón Bolívar

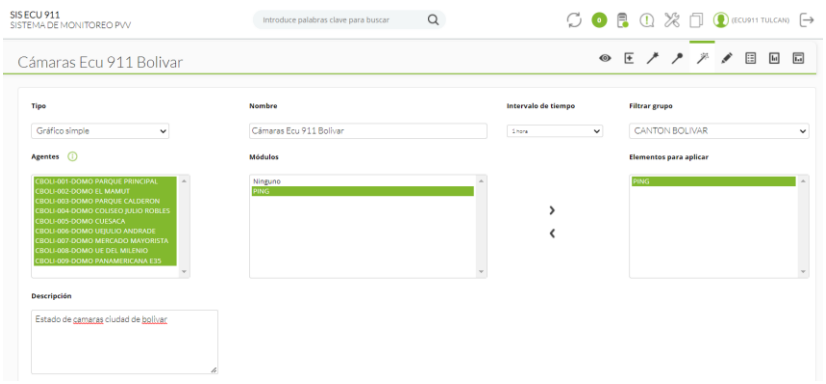


Figura 118. Configuración de informe personalizado del Cantón Bolívar

Informe SLA

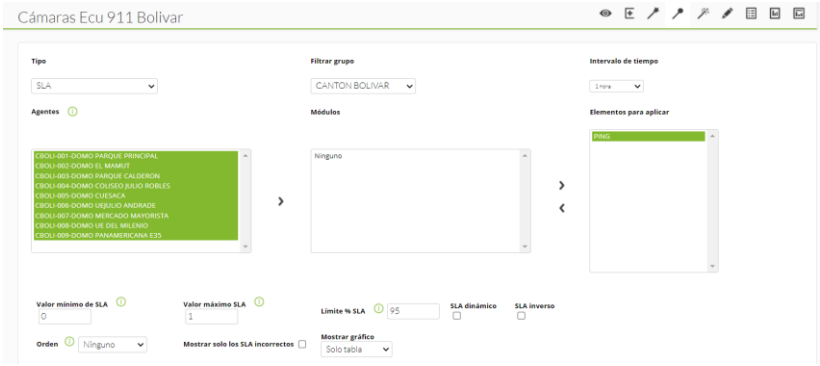


Figura 119. Creación de informe SLA del Cantón Bolívar

Montúfar Informes

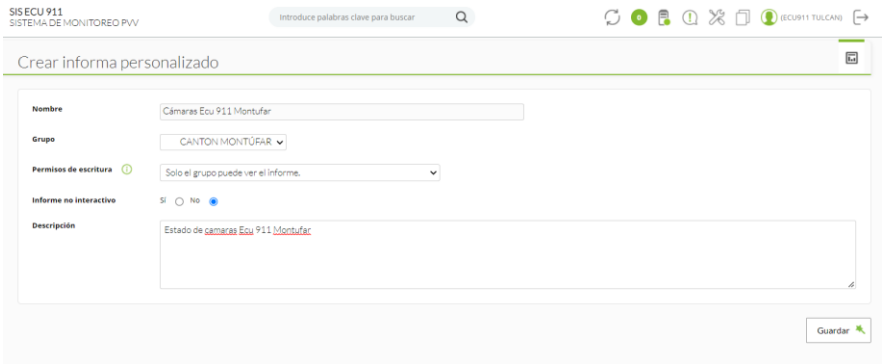


Figura 120. Creación de informe personalizado del Cantón Montúfar

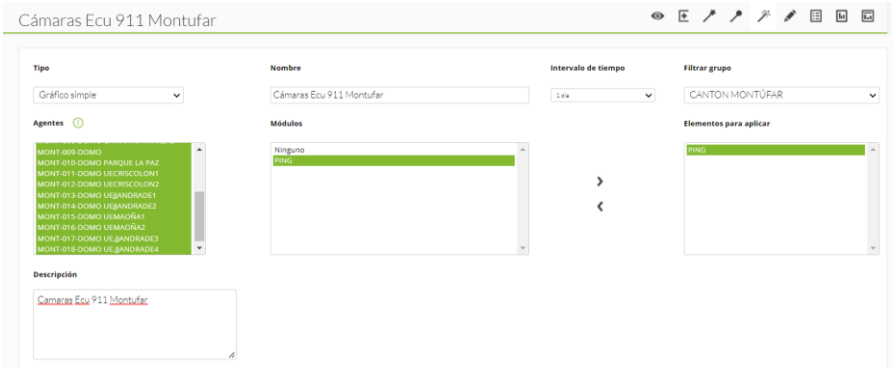


Figura 121. Configuración de informe personalizado del Cantón Montúfar

Espejo

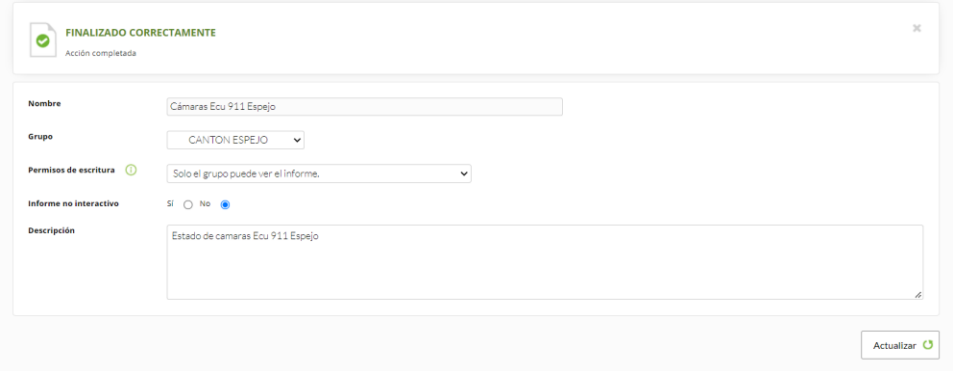


Figura 122. Creación de informe personalizado del Cantón Espejo

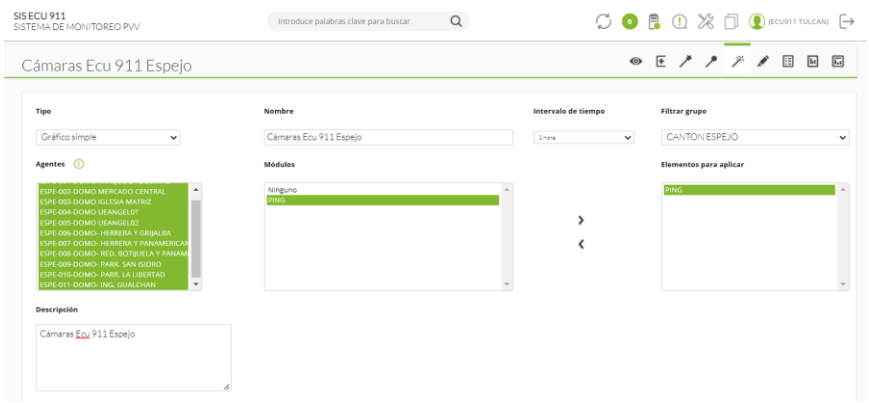


Figura 123. Configuración de informe personalizado del Cantón Espejo

MIRA

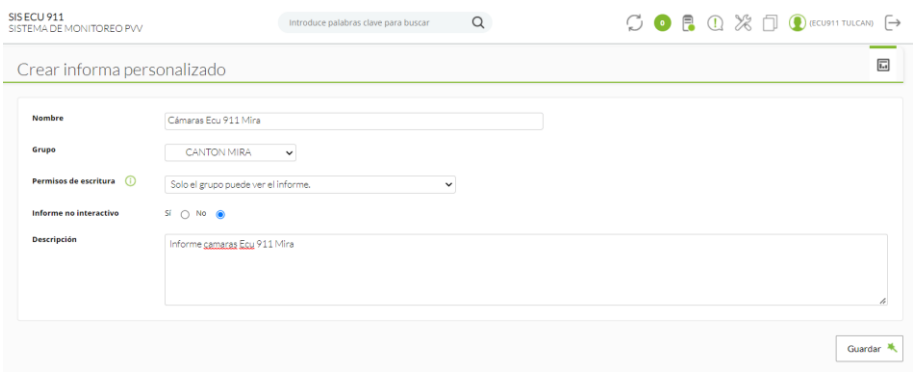


Figura 124. Creación de informe personalizado del Cantón Mira

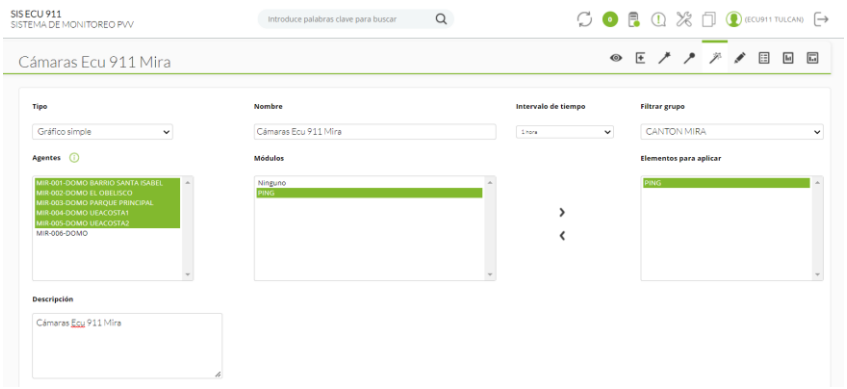


Figura 125. Configuración de informe personalizado del Cantón Mira

Creación de Informes Visuales

En este apartado de configuración añadiremos el nombre que tendrá la Dashboard, como también al grupo que pertenecerá. En este caso vamos a asociarlo a la ciudad de Huaca.

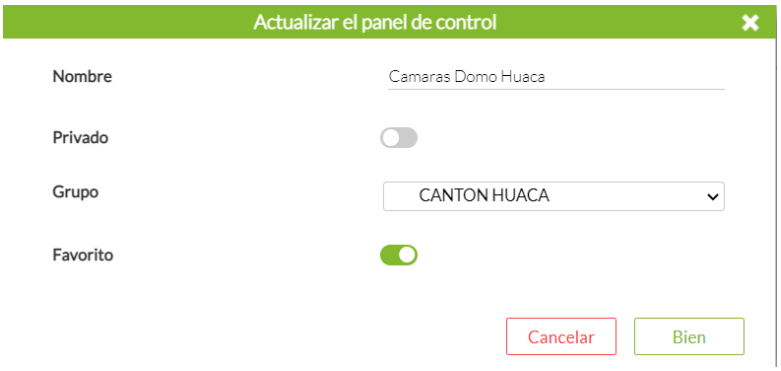


Figura 126. Configuración de Dashboard cantón Huaca

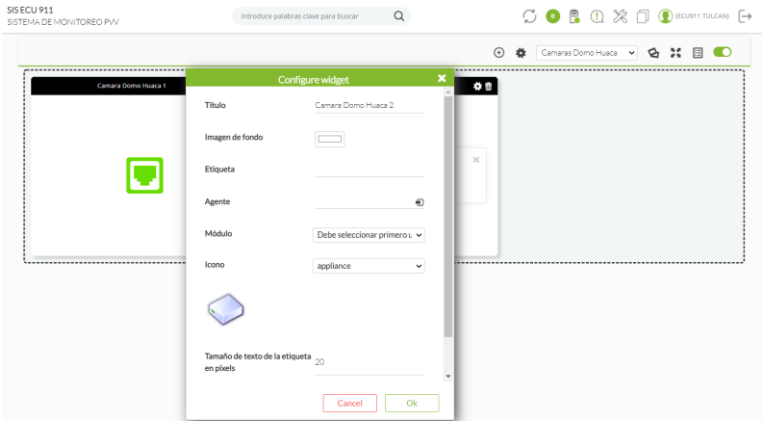


Figura 127. Configuración de Widget cámaras DOMO Huaca

En este apartado vamos a visualizar las cámaras activas e inactivas de la ciudad de Huaca. En este apartado de configuración añadiremos el nombre que tendrá el Dashboard, como también al grupo que pertenecerá. En este caso vamos a asociarlo al cantón Montúfar.

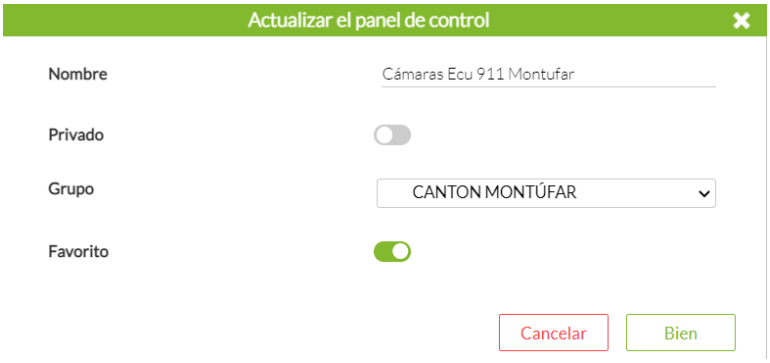


Figura 128. Configuración de Dashboard cantón Montúfar

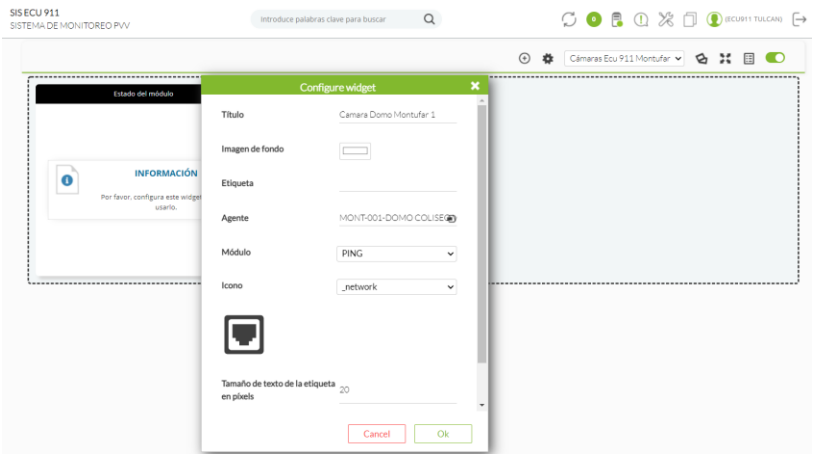


Figura 129. Configuración widget cantón Montúfar

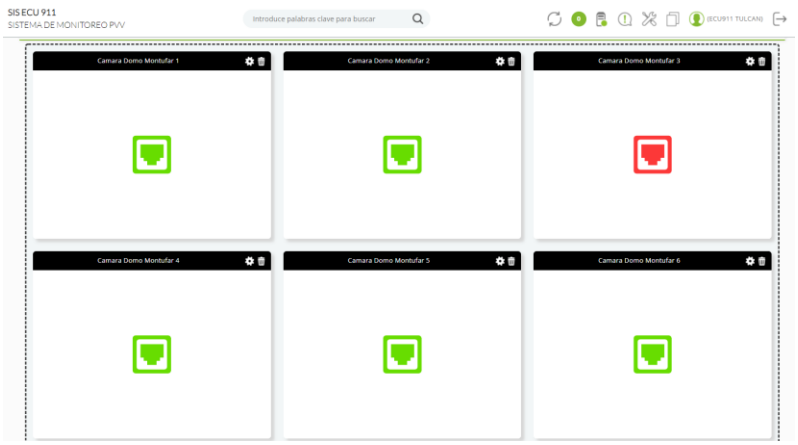


Figura 130. Dashboard de cámaras activas e inactivas Cantón Montúfar

En este apartado de configuración añadiremos el nombre que tendrá el Dashboard, como también al grupo que pertenecerá. En este caso vamos a asociarlo al cantón Espejo.

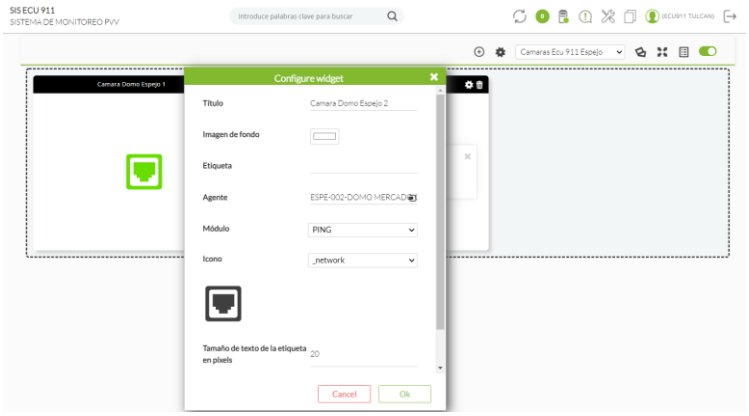


Figura 131. Configuración de Widget cantón Espejo

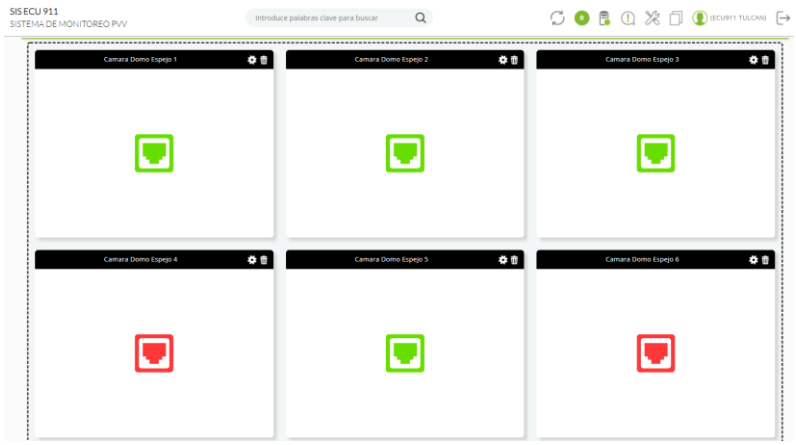


Figura 132. Dashboard de cámaras activas e inactivas Cantón Espejo

En este apartado de configuración añadiremos el nombre que tendrá el Dashboard, como también al grupo que pertenecerá. En este caso vamos a asociarlo al cantón Bolívar.

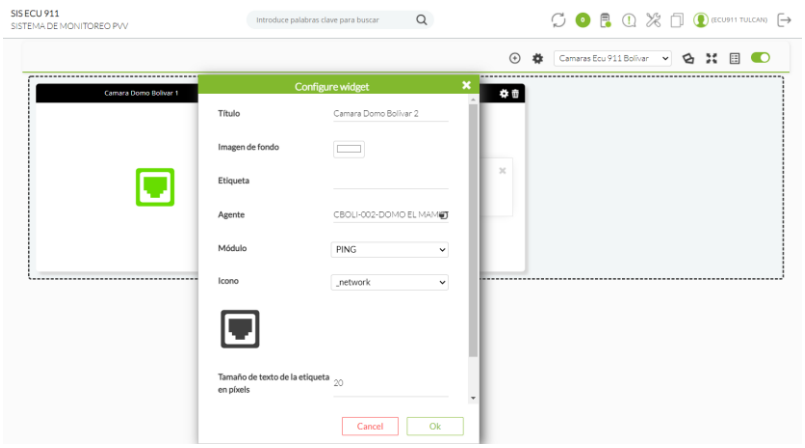


Figura 133. Configuración Widget Cantón Bolívar

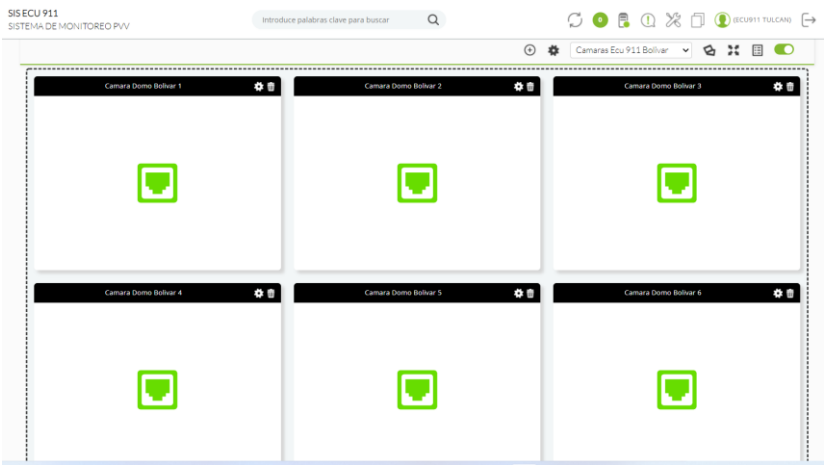


Figura 134. Dashboard de cámaras activas e inactivas Cantón Bolívar

En este apartado de configuración añadiremos el nombre que tendrá el Dashboard, como también al grupo que pertenecerá. En este caso vamos a asociarlo al cantón Mira.

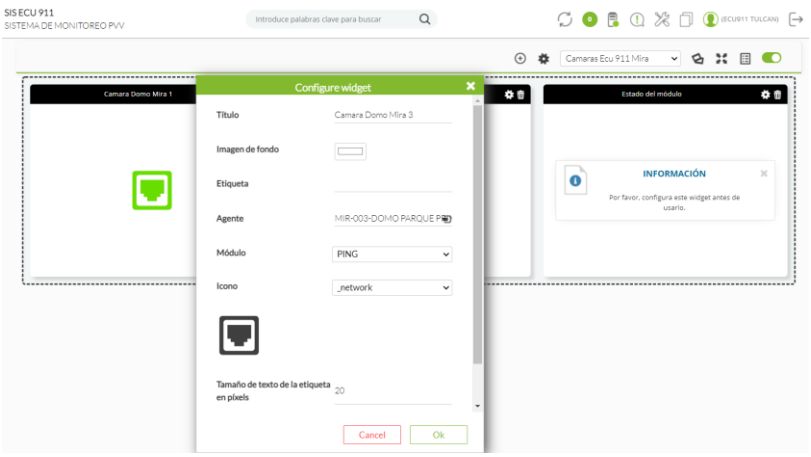


Figura 135. Configuración Widget Cantón Mira

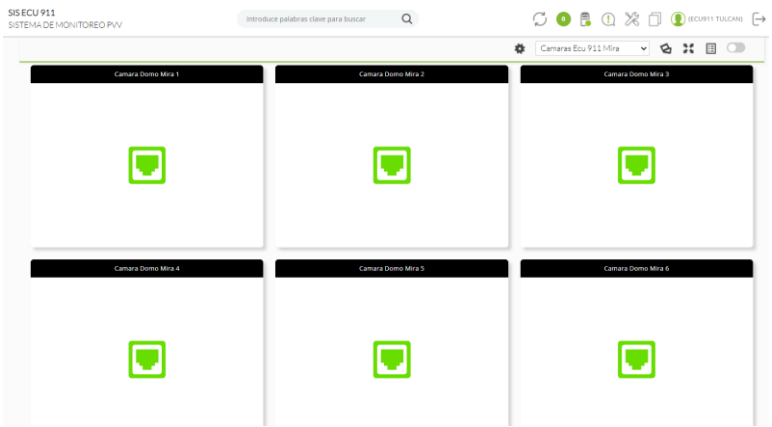


Figura 136. Dashboard de cámaras activas e inactivas Cantón Mira

Creación de mapas de red Ecu 911

Configuración mapa de red Cámaras Ecu 911 Bolívar

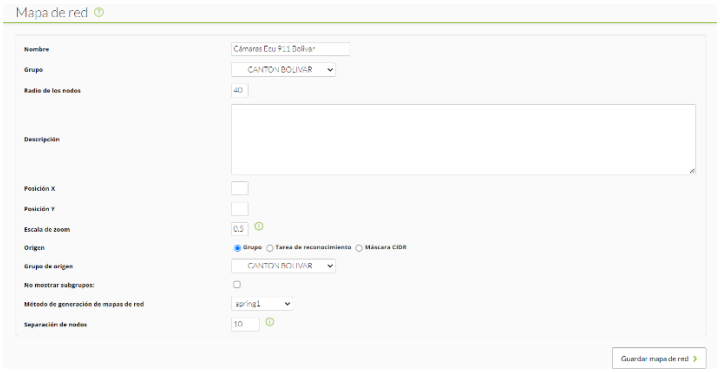


Figura 137. Configuración de mapa de red Bolívar

Resultado del escaneo de mapa de red cámaras Ecu 911 Bolívar

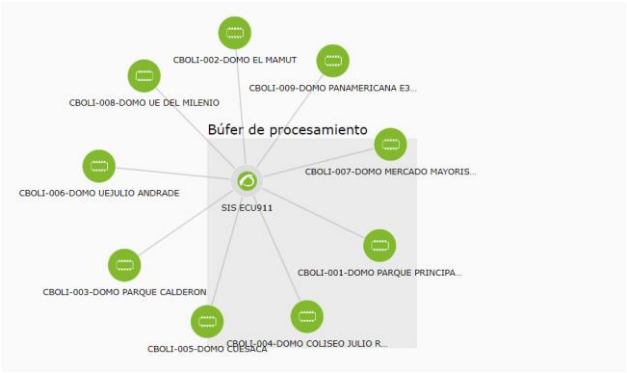


Figura 138. Mapa de red cámaras ECU 911 Bolívar

Configuración mapa de red cámaras Ecu 911 ciudad de Montúfar

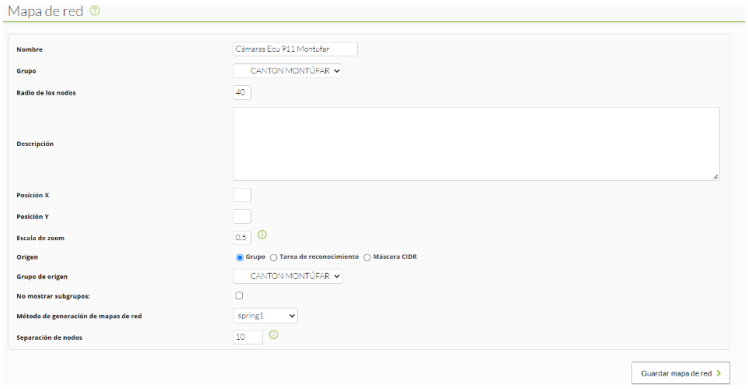


Figura 139. Configuración mapa de red Montúfar

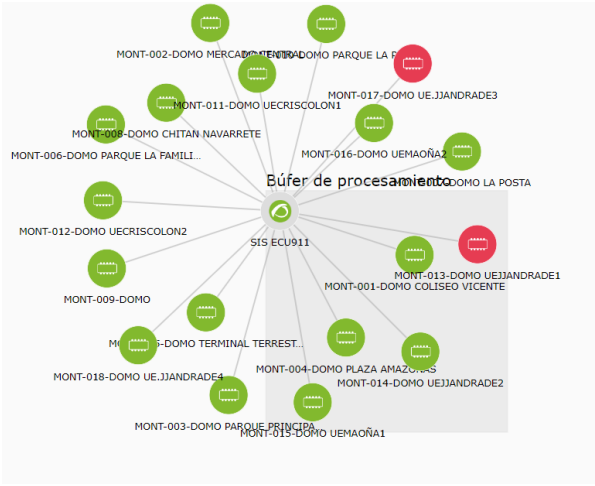


Figura 140. Mapa de red cámaras ECU 911 Montúfar

Configuración de mapa de red cámaras Ecu 911 de la ciudad de Huaca.

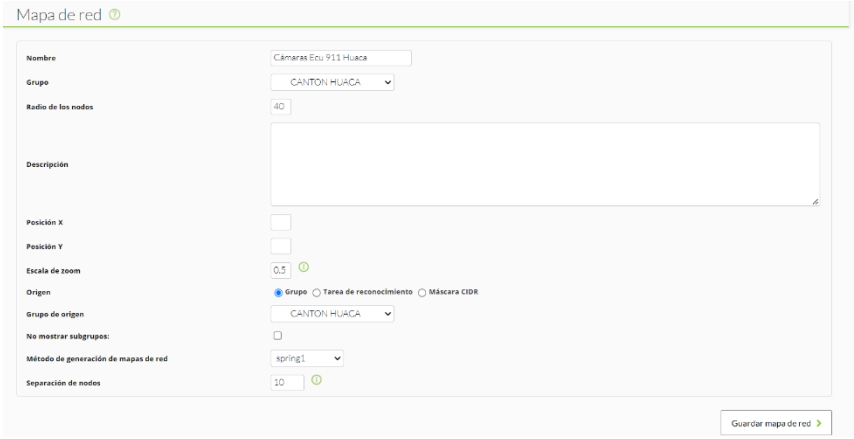


Figura 141. Configuración de mapa de red cámaras ECU 911 Montúfar

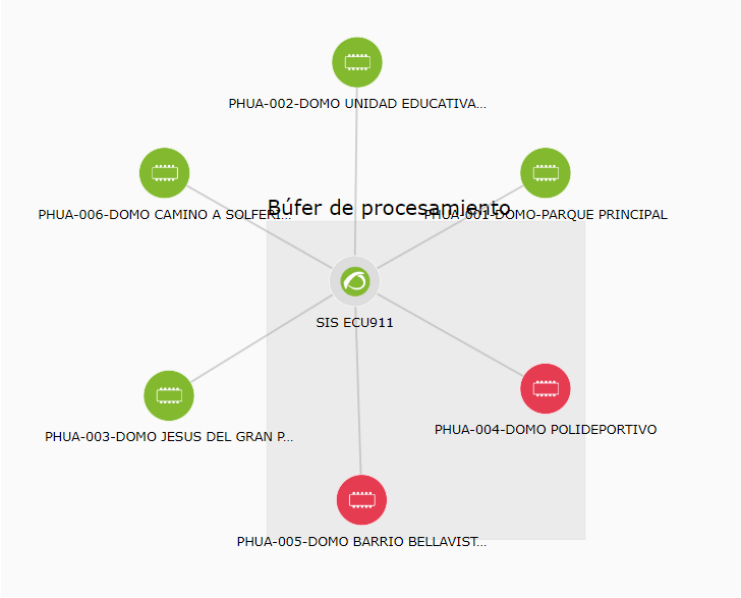


Figura 142. Mapa de red cámaras ECU 911 Montúfar

Configuración de mapa de red cámaras Ecu 911 cantón Espejo

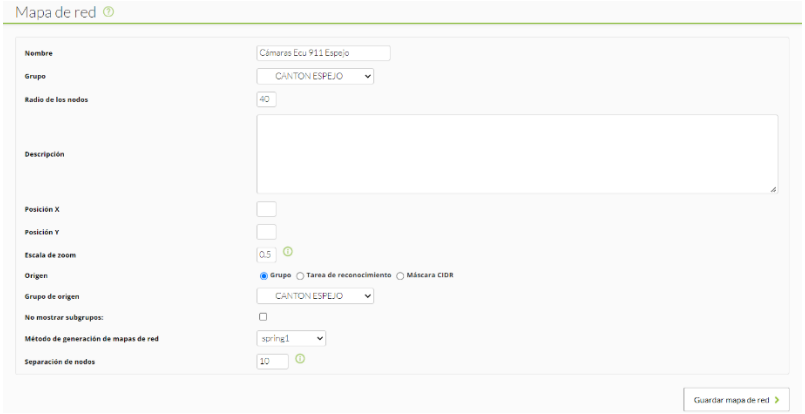


Figura 143. Configuración mapa de red cámaras ECU 911 Espejo

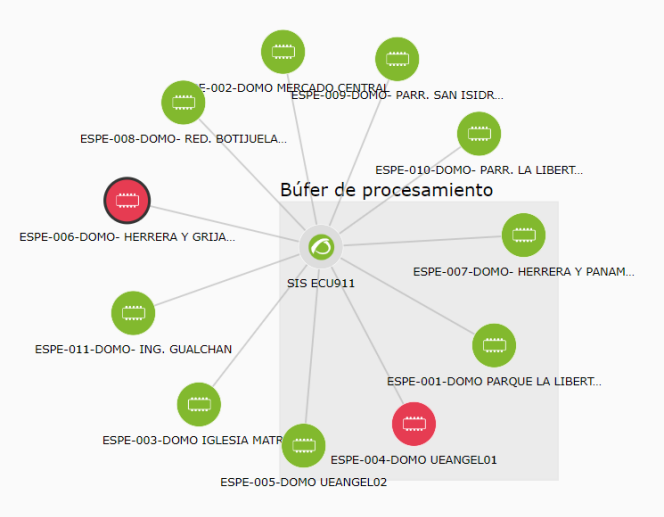


Figura 144. Mapa de red cámaras ECU 911 Espejo

Configuración de mapa de red cámaras Ecu 911 cantón Mira

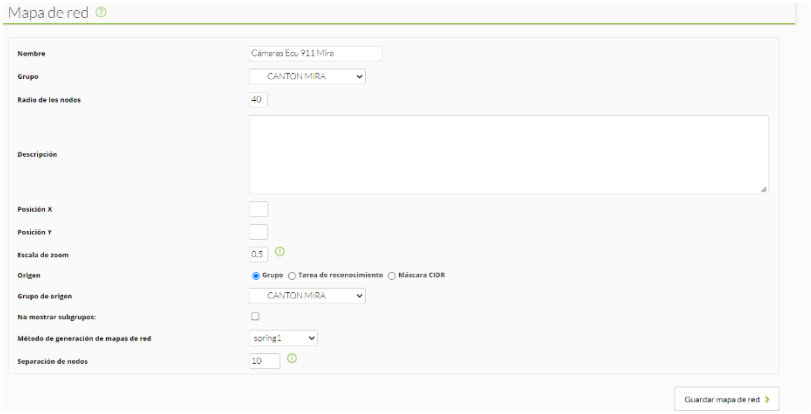


Figura 145. Configuración mapa de red cámaras ECU 911 Mira

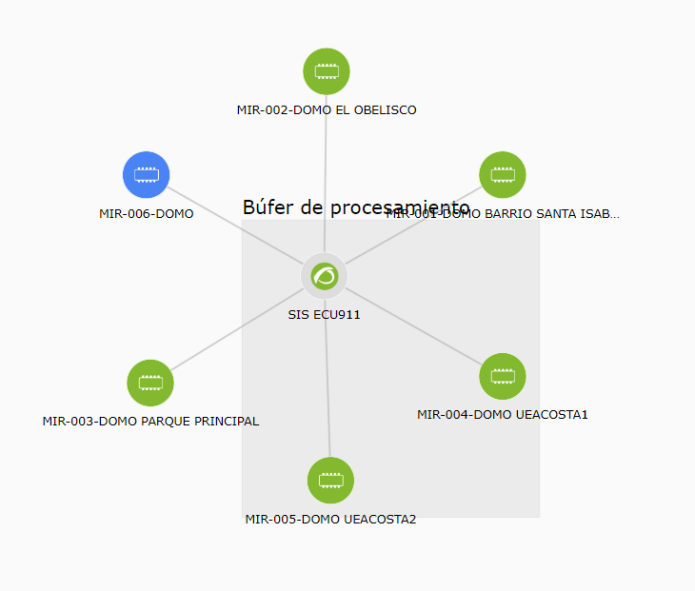


Figura 146. Mapa de red cámaras ECU 911 Mira

Creación de Mapas Gis Ecu 911

Asignación Agente Cantón Huaca

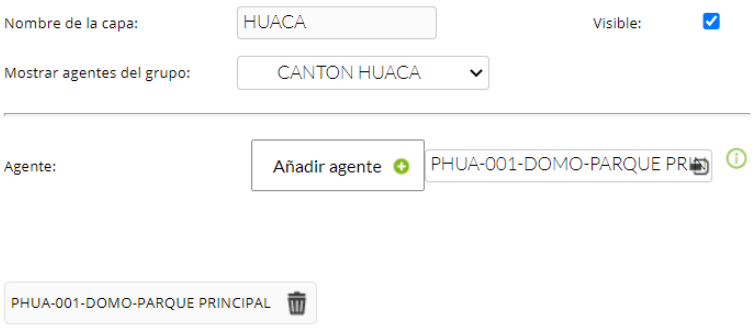


Figura 147. Creación de capa Cantón Huaca

Asignación Agente Cantón Mira

Figura 148. Creación de capa Cantón Mira

Asignación Agente Cantón Montufar

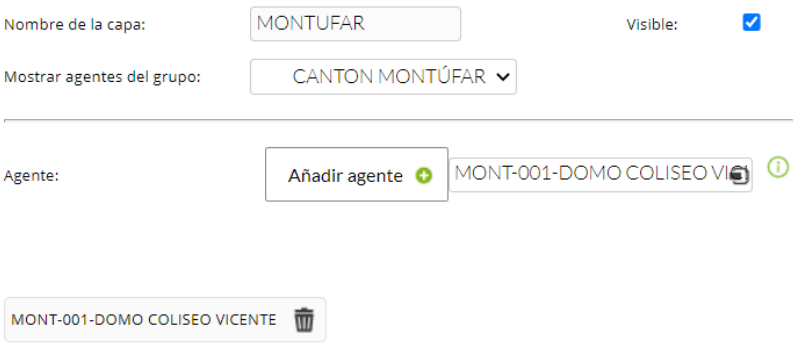


Figura 149. Creación de capa Cantón Montúfar

Asignación Agente Cantón Tulcán

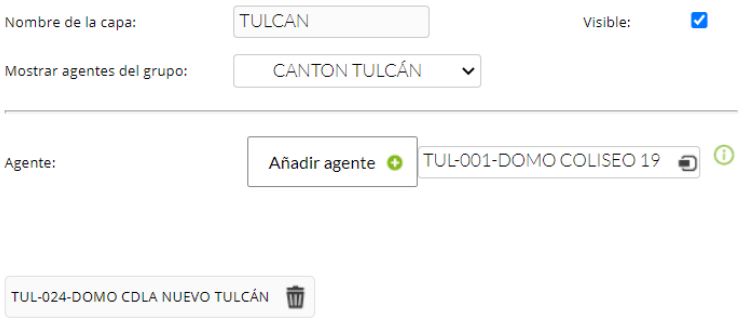


Figura 150. Creación de capa Cantón Tulcán

Asignación Agente Cantón Espejo

Figura 151. Creación de capa Cantón Espejo