UNIVERSIDAD RICARDO PALMA

FACULTAD DE INGENIERÍA

ESCUELA PROFESIONAL DE INGENIERÍA INFORMÁTICA

Sistema web de monitoreo de alertas de seguridad ciudadana en el área de informática de la empresa FIRINGS E.I.R.L. 2021-2022

TESIS

Para optar el título profesional de Ingeniero Informático

AUTORES

Miralles Delgado, Jose Andre
ORCID: 0000-0001-8673-7158

Tapia Sifuentes, Jhonatan Jesus
ORCID: 0000-0003-4071-7148

ASESOR

De Olazabal Leon, Edgard Eugenio
ORCID: 0000-0003-1727-3438

Lima, Perú

2022

Metadatos Complementarios

Datos del autor(es)
Miralles Delgado, Jose Andre
DNI: 75984518
Tapia Sifuentes, Jhonatan Jesus
DNI: 47877187

Datos de asesor
De Olazabal Leon, Edgard Eugenio
DNI: 10300161

Datos del jurado
JURADO 1
Escobar Aguirre, Jaime Luis
DNI: 10079628
ORCID: 0000-0002-7104-8525

JURADO 2
Palacios Pacherres, Luis Hector
DNI: 10145124
ORCID: 0000-0001-7635-3652

JURADO 3
Villanueva Gonzales, Eric Daguberto
DNI: 10611573
ORCID: 0000-0001-8609-552X

Datos de la investigación
Campo del conocimiento OCDE: 2.11.02
Código del Programa: 612286

DEDICATORIA

Dedico esta tesis especialmente a mi familia, quienes me apoyaron en todo momento siendo firme e insistente en el trabajo de la tesis y a las personas quienes me asesoraron durante el proceso del desarrollo.

Jose Andre, Miralles Delgado

Esta tesis está dedicada a todos mis seres amados; quienes, en conjunto, han sido el soporte perfecto para nunca decaer y siempre mantenerme firme en cada etapa del proceso del desarrollo de esta tesis.

Jhonatan Jesus Tapia Sifuentes

AGRADECIMIENTO

Nuestro sincero agradecimiento a nuestra alma mater, por habernos brindado los conocimientos de esta maravillosa carrera; a la empresa FIRINGS EIRL por abrirnos sus puertas; y a todas personas que de alguna manera nos apoyaron en el desarrollo de la tesis, entre ellos docentes y familiares.

Jose Miralles y Jhonatan Tapia

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

En la presente tesis se plantea crear un sistema web de monitoreo de alertas de Seguridad Ciudadana para la empresa FIRINGS E.I.R.L, en donde se requiere esencialmente la atención de las alertas reportadas durante el proceso de monitoreo.

De esta manera y como resultado, se logrará diferenciar la variedad de delitos correspondientes a un sector determinado para que los teleoperadores puedan actuar con mayor precisión y prioridad. A su vez, se podrá obtener información relevante para la mejora continua en la toma de decisiones acerca de la instalación de alertas y la instalación de alarmas; con el objetivo de buscar soluciones más eficientes sobre los procesos actuales.

Por ende, al tener una existente aplicación de escritorio de la empresa FIRINGS E.I.R.L con ciertos límites que no lograban ayudar en su totalidad el procesamiento de la información, se desea convertirlo en un sistema web, que llegue a identificar los delitos cometidos, monitorear las alertas a cargo de los teleoperadores y la obtención de reportes informativos según la toma de decisiones de la empresa.

Palabras Clave: Sistema web, monitoreo de alertas, alertas.

ABSTRACT

In this thesis, it is proposed to create a web system for monitoring Citizen Safety alerts for the company FIRINGS E.I.R.L, where attention to the alerts reported during the monitoring process is essentially required.

In this manner and as a result, it is possible to differentiate the variety of crimes corresponding to a sector so that telemarketers can act with greater precision and priority. At the same time, it was possible to obtain relevant information for continuous improvement in decision-making about attention to alerts and the installation of alarms; with the aim of seeking more efficient solutions on current processes.

Therefore, having an existing desktop application of the company FIRINGS E.I.R.L with certain limits that could not fully help the processing of information, it was desired to convert it into a web system, which can identify the crimes committed, monitor the alerts in charge of the telemarketers and the obtaining of informative reports according to the decision making of the company.

Keywords: Web system, Alert Monitoring System, Alerts

INTRODUCCIÓN

La empresa FIRINGS E.I.R.L es una empresa peruana con más de 12 años de trabajo dedicado a la investigación y desarrollo tecnológico de hardware y software enfocándose en la seguridad ciudadana. Así mismo en la importación, exportación, fabricación y distribución e instalación de sistemas de seguridad electrónicas, tanto videovigilancia como monitoreo según aplicación, de uso residencial, industrial y gubernamental.

En FIRINGS E.I.R.L., cuentan con un equipo de ingenieros que desarrollan equipos tecnológicos según la exigencia del mundo tecnológico de hoy en día, enfocados en presentar proyectos útiles y en mostrar soluciones para la seguridad ciudadana, que es una preocupación importante en la actualidad. Por ello tienen como objetivo ayudar en la solución integral fomentando y distribuyendo propuestas que rindan al máximo los conocimientos de uso de equipos de última generación para brindar seguridad con sus sistemas y tecnologías. Uno de esos productos es el software que actualmente poseen cuyas deficiencias son notorias y detectadas por el gerente general.

Por ende, en el presente trabajo de investigación se plantea convertir la aplicación de escritorio actual de monitoreo de alertas que tiene la empresa a un sistema web que cumpla las funciones de identificar, monitorear y reportar delitos según la toma de decisiones junto al trabajo de los teleoperadores, con el fin de superar las expectativas y obstáculos pendientes.

Se está utilizando la metodología de *Rational Unified Process* (RUP) cuyo objetivo es asegurar que la producción del software tenga una alta calidad en satisfacer las necesidades de los usuarios. Con ello el sistema web se desarrolló con Api JavaScript Google Maps, se utilizó el lenguaje de Java, Docker, MySQL, Socket IO, entre otros. Mostraremos los capítulos del proyecto, en su totalidad seis que son:

El Capítulo I, explicamos el problema, mencionamos los objetivos propuestos, la delimitación de la investigación y justificación e importancia.

El Capítulo II, mostramos los antecedentes para el proyecto, las bases teóricas, mencionamos la variable dependiente e independiente, así mismo la metodología que se está usando.

En el Capítulo III, se explica la hipótesis y matriz operacional.

El Capítulo IV, se explica al detalle la metodología de la investigación, el tipo y nivel que tiene, el diseño, la población y muestra, las técnicas e instrumentos, los criterios de validez, técnicas.

El Capítulo V, el desarrollo de la investigación, el uso de herramientas, los modelamientos que se usaron para el proyecto, las reglas, el plan de gestión de riesgo, las matrices, diagramas, modelos.

En el Capítulo VI, se muestran los resultados de la investigación.

Por último, presentamos las conclusiones y recomendaciones necesarias para el cumplimiento del proyecto y creación del sistema.

CAPÍTULO I: PLANTEAMIENTO DEL PROBLEMA

1.1. Descripción y formulación del problema general y específicos

1.1.1. Descripción del problema:

FIRINGS E.I.R.L es una empresa peruana de más de 12 años de experiencia en su sector dedicada a la investigación y desarrollo de soluciones tecnológicas de hardware y software para la seguridad ciudadana, así como, de importación, exportación, fabricación, distribución, instalación y puesta en marcha de sistemas de seguridad electrónica, sistema de video vigilancia para uso público gubernamental, industrial, residencial y doméstica.

FIRINGS E.I.R.L cuenta con soluciones tecnológicas de video-alarmas vecinales, que viene implementado en muchas municipalidades de Lima Metropolitana; esto para mejorar la seguridad ciudadana de dichas zonas con un monitoreo constante de video vigilancia. Actualmente, la empresa ha desplegado una aplicación de escritorio en la municipalidad de San Borja, donde hay un personal encargado de hacer contacto con los vecinos que reportan una emergencia por medio del aplicativo móvil “Vecino”.

La aplicación de escritorio muestra solamente en el mapa dónde se monitorea las alertas y la información básica de la persona que reporta su emergencia; y ahora, el gerente general quiere que de todas las alertas reportadas que lleguen en su sistema de monitoreo, puedan diferenciarse cuales corresponde a delitos, para que los teleoperadores puedan actuar con mayor prioridad.

A su vez, la aplicación de escritorio cuenta con limitaciones técnicas y funcionales debido a que fue desarrollada, en su tiempo, con un análisis básico para solucionar una necesidad urgente en un corto periodo de tiempo. Ahora, se desea implementar un sistema web que sea más eficiente en comparación de cómo viene operando la aplicación de escritorio.

Además, la empresa presenta la siguiente problemática, hay situaciones donde se instalan dos o más alarmas vecinales muy cercanas entre sí, lo que ocasiona que, un vecino al activar el “botón de pánico” de la aplicación móvil y tiene más

de una alarma cercana a su ubicación, sonarán las que se encuentren cercanas en el momento que se active. Por lo cual, la empresa desea obtener, mediante el sistema web, información que le permita mejorar la toma de decisiones al instalar las alarmas en puntos estratégicos.

Debido a lo expuesto anteriormente y las nuevas funcionalidades que el gerente general desea añadir, la empresa FIRING E.I.R.L desea transformar su programa de escritorio a un sistema web.

1.1.2. Problema General:

¿Cómo influye la implementación de un sistema web de monitoreo de alertas de seguridad ciudadana en el área de informática de la empresa FIRINGS E.I.R.L. 2021-2022?

1.1.3. Problema Específicos:

a) ¿Cómo influye la implementación de un sistema web de monitoreo de alertas de seguridad ciudadana en el área de informática de la empresa FIRINGS E.I.R.L. 2021-2022 en la identificación de los delitos?
b) ¿Cómo influye la implementación de un sistema web de alertas vecinales de seguridad ciudadana en el área de informática de la empresa FIRINGS E.I.R.L. 2021-2022 en la disposición de la vigilancia?
c) ¿Cómo influye la implementación de un sistema web de monitoreo de alertas de seguridad ciudadana en el área de informática de la empresa FIRINGS E.I.R.L. 2021-2022 en la prevención de la inseguridad?

1.2. Objetivos

1.2.1. Objetivo General

Determinar cómo influye la implementación de un sistema web de monitoreo de alertas de seguridad ciudadana en el área de informática de la empresa FIRINGS E.I.R.L. 2021-2022.

1.2.2. Objetivos Específicos

a) Determinar cómo influye la implementación de un sistema web de monitoreo de alertas de seguridad ciudadana en el área de informática de la empresa FIRINGS E.I.R.L 2021-2022 en la identificación de los delitos.

b) Determinar cómo influye la implementación de un sistema web de monitoreo de alertas de seguridad ciudadana en el área de informática de la empresa FIRINGS E.I.R.L 2021-2022 en la disposición de la vigilancia.

c) Determinar cómo influye la implementación de un sistema web de monitoreo de alertas de seguridad ciudadana en el área de informática de la empresa FIRINGS E.I.R.L 2021-2022 en la prevención de la inseguridad.

Comentado [LHPP1]: Los objetivos específicos no se alinean con los problemas

Comentado [JJTS2R1]: Corregido

1.3. Delimitación de la investigación: temporal espacial y temática

A finales del mes de abril, nos contactamos con la empresa FIRINGS E.I.R.L a través del gerente general Antonio Silvipaucar Sotelo, con el cual se concretaron una serie de reuniones donde se manifestó la situación actual de la empresa con el manejo de las "alertas vecinales".

Debido a la coyuntura actual y el avance de las nuevas tecnologías, la empresa, por medio del gerente general, está solicitando la implementación de un sistema web que reemplace a su aplicación de escritorio.

Por ende, para el presente proyecto de tesis, se describe específicamente los puntos limitantes de la investigación:

a) Delimitación Espacial

El proyecto propuesto se llevará a cabo en el área de informática de la empresa FIRINGS E.I.R.L, donde se realizará los múltiples escenarios del monitoreo de las alertas emergentes para su utilización de datos.

b) Delimitación Temporal

La presente investigación dispone de información desde el año 2021, y abarca hasta el mes de noviembre del presente año 2022.

c) Delimitación Temática

El alcance de la investigación incluye: Identificación de los delitos, monitoreo de alertas a cargo de los teleoperadores y reportes informativos para la toma de decisiones.

El alcance de la investigación no incluye: La integración del aplicativo móvil "Vecino" y la intervención del Serenazgo a la alerta.

1.4. Justificación e importancia

Sobre la importancia de esta investigación, se busca reemplazar la actual aplicación de escritorio de la empresa FIRINGS E.I.R.L por un sistema web que identifique los delitos de las incidencias, mejore los tiempos de respuesta de las alertas, y con ello tomar buenas decisiones para la implementación de las nuevas alarmas.

Acerca de la justificación, esta investigación permitirá a la empresa FIRINGS E.I.R.L tener una ventaja competitiva gracias a la implementación de una solución web de monitoreo de alertas, poniendo a la empresa a la vanguardia en tecnología con respecto al manejo de la seguridad ciudadana.

1.4.1. Limitaciones del Proyecto

Para el proyecto de tesis se ha decidido abarcar el proceso de "Monitoreo de alertas" en donde se incluye principalmente la atención de las alertas por parte de los teleoperadores y la gestión de las alarmas en el sistema web.

a) Las exclusiones del proyecto:
   - Conexión con servicios de cruce de información con el Registro Nacional de Identificación y Estado Civil (RENIEC) y la Policía Nacional del Perú.
   - Servidor dedicado de tramas de red.
   - Implementación de videovigilancia.

b) Restricciones del proyecto:
   - No incluye datos indebidamente ingresados.
   - No se admite el cambio de idioma.
   - Preparación de la infraestructura.
   - Integración con el sistema móvil de botón de pánico.
   - Comunicación directa con los equipos de alarma "FGS10".

c) Supuestos del proyecto:
   - El proyecto no será paralizado o cancelado.
   - El cliente brindará la información necesaria.
   - Los cambios serán previamente evaluados y aprobados.

CAPÍTULO II: MARCO TEÓRICO

2.1. Antecedentes del estudio de investigación

2.1.1. Antecedentes Internacionales

Chicaiza Guachi, K. G. (2020) en su investigación “Sistema de alarma comunitaria para el mercado San Juan de la Ciudad de Santiago de Píllaro” en la Universidad Técnica de Ambato. Facultad de Ingeniería en Sistemas, Electrónica e Industrial. Carrera Ingeniería Electrónica y Comunicaciones tiene como objetivo realizar un prototipo de sistema de alarma que no cuente con un sistema de seguridad ya que utiliza tecnología que permite a la población estar al tanto de situaciones de vandalismo, así como crímenes cerca del área donde residen en forma de medida de protección. Utilizando mensajería para envío de alertas y alarmas como, auditivas o visuales hacia las terminales o unidades policiacas.

Su metodología se divide en equipos y dispositivos, según el hardware que utilizan como herramienta y software según la configuración del sistema tales como: Sirena, Router, Disco Duro, Cámara IP para hardware. Python, Raspbian, *Visual Studio Code* como Software, igualmente seleccionan dispositivos de procesamiento que tenga la central de alarma y que les permita controlar los eventos que ocurren en diferentes lugares específicos. Con eso en mano, logran manipular la emisión de alarmas enviándolas a través de mensajes.

Concluye que se logra tener un óptimo rendimiento al ejecutar las tareas asignadas en la programación, mostrando el sistema óptimo y funcional al momento de ser instalado e incorporado. También se muestra la optimización de la memoria teniendo videos captados por cámara almacenados en un disco externo, lo que ayudó al servidor a no colapsar, optimizando el procesamiento.

Mollericona, Tinini y Paredes (2007) en su libro “La seguridad ciudadana en la ciudad de El Alto - Fronteras entre el miedo y la acción vecinal” de Fundación para la Investigación Estratégica en Bolivia (PIEB). Tiene como objetivo contribuir la comprensión de problemas y procesos de cambio de la ciudad, otorgando la posibilidad de realizar reuniones o talleres con el fin de lograr

investigar a El Alto, la inseguridad que tienen y como está es posible lograr obteniendo una tercerización de la seguridad al cuidado de los policías privados y colegas.

Su metodología es cualitativa donde permite explorar las acciones y reacciones vecinales mediante la construcción de mecanismos de prevención. Se aplican técnicas de recolección de información como: entrevistas, grupos focales y observación directa. Teniendo representantes de efectivos policiales, jefes de la fuerza especial de lucha contra el crimen, funcionarios y personal de empresas de seguridad. Así mismo, muestran información de asambleas vecinales donde se expone la problemática de la inseguridad del lugar y como se logra entender la toma de decisiones ante la inseguridad ciudadana.

En conclusión, sobresalen mecanismos locales de prevención contra la violencia e inseguridad a partir del interés de los vecinos que mencionan haber logrado, gracias a su disposición de vigilancia, tomar un punto medio para con los servicios privados, refiriéndose a la privatización de la seguridad. Barrios más residenciales tienen un despliegue de tercerizar a seguridades privadas que se le conocen como "pequeños ejércitos" donde utilizan medios para cumplir sus objetivos preventivos.

2.1.2. Antecedentes Nacionales

Jaulis Rua, J. J., & Vilcarromero Giraldo, J. R. (2015) en su investigación "Sistema de predicción de hechos delictivos para la mejora del proceso de prevención del delito en el distrito de La Molina utilizando minería de datos" de la Universidad San Martin de Porres. Tiene como objetivo su investigación mejorar el proceso de prevenir delitos que realizaron en tres comisarías, buscando la seguridad y el orden de la zona. Con su proyecto logran obtener predicciones que son útiles a futuro para el registro de datos y a sí mismo, plasmarlos como herramienta de prevención para las comisarías ubicadas en Santa Felicia.

En su metodología utilizan distintos recursos y herramientas para el proyecto, estas son: recursos humanos (las funciones de dos trabajadores) y el hardware

como herramienta que será de uso para ejecutar el proyecto. En sus trabajos de los empleadores, está el tema de análisis y modelado de un esquema de base de datos, diseño, desarrollo y realización de pruebas funcionales del sistema para con el proyecto.

Como conclusión, logran una mejora de la prevención de delitos en la comisaría de Santa Felicia, los trabajadores ven la simplificación de sus actividades gracias al sistema incorporado en la comisaría. Esto ayuda a la mejora de decisiones en la zona para prevenir actos delictivos en masa. De igual modo, el tiempo de acción se reduce considerablemente porque de ser una actividad manual hecho por los oficiales pasa a ser reemplazado por el sistema donde solo es necesario ejecutar y analizar los datos.

De la Criminalidad, C. E. I. (2021) en su libro “Perú: Anuario estadístico de la criminalidad y seguridad ciudadana 2015 - 2019” realizado por el Instituto Nacional de Estadística e Informática (INEI). Tienen como objetivo mostrar en base a la investigación y recopilación de información de los departamentos y ciudades de lima, la cantidad de crimen que existe en el país y asimismo de ciudadanos pendientes de la seguridad ciudadana que conviven.

En el libro se muestran registros administrativos sobre la delincuencia e inseguridad ciudadana que representan uno de los principales problemas del país, como la cantidad de ciudadanos robados a mano armada, secuestros, difamaciones, agresiones, entre otros. Así mismo, nos da información de cuantos ciudadanos tienen conocimiento sobre seguridad ciudadana o tienen a su mano alguna herramienta de alarma para precaución ante cualquier tipo de crisis.

En conclusión, la información que otorgan es de utilidad para poder implementar un sistema web que aporte a la ayuda en la seguridad ciudadana, teniendo en cuenta que la población actual está con una percepción muy alta de la inseguridad por diferentes contextos en base a su experiencia. Incluso muestran que los ciudadanos tienen poco conocimiento de la existencia de vigilancias en la zona donde viven, causando mayor crisis.

2.2. Bases teóricas vinculadas a las variables

2.2.1. Variable Dependiente

Seguridad Ciudadana

Para la Ley del Sistema Nacional de Seguridad Ciudadana (Ley N° 27933), seguridad ciudadana se refiere a "la acción integrada que desarrolla el Estado, en sus tres poderes, con la participación activa de la sociedad civil organizada y el sector privado de la población, destinada a asegurar la convivencia pacífica, la erradicación de la violencia y la utilización pacífica de las vías y espacios públicos. Así como a contribuir a la prevención de la comisión de delitos y faltas" (Presidencia del Consejo de Ministros [PCM], 2014, p.1).

En Perú, día a día vemos en nuestra realidad nacional como la seguridad ciudadana se encuentra atentada continuamente por los altos niveles de criminalidad que existe a raíz de la mala coordinación y comunicación que existe entre entidades públicas, siendo estos los principales actores para poder erradicar con este mal que tanto nos afecta; son ellos los que deberían brindar un mejor servicio hacia la región en cuanto a este aspecto refiere.

Es así como, en el Plan Nacional de Seguridad Ciudadana 2019-2023 plantea diversas soluciones y planteamientos en función a mejorar las estadísticas de criminalidad que existen en la actualidad, pero sabiendo clasificar cuales son los principales males a afrontar, de esta manera el Plan Nacional de Seguridad Ciudadana 2019 -2023 reconoce cuatro grupos a los cuales denomina "fenómenos" que amenazan constantemente la seguridad del ciudadano y estos están agrupados como: "muerte violenta, representado por delitos asociados a homicidios y muertes en accidentes de tránsito; delitos contra las mujeres, niños, niñas y adolescentes, materializado en feminicidios, violencia sexual, trata de personas, violencia doméstica y violencia contra niños, niñas y adolescentes; delitos patrimoniales en espacios públicos, compuestos por actos de robo, hurto y estafas, micro comercialización; y delitos cometidos por bandas criminales, expuesto en extorsiones, amenazas, intimidaciones y micro comercialización de drogas".

Producto a que, en muchas ocasiones, no existe un buen manejo por parte de las entidades públicas para resolver los fenómenos anunciados anteriormente, es el mismo ciudadano a pie el que toma sus propias decisiones y actúa, sea solo o en conjunto con sus vecinos, para salvaguardar tanto su integridad como la de su familia.

Por lo tanto, pasamos de una asociación de vecinos para comunicarse entre sí cuando existe alguna incidencia que perturbe la paz de la vecindad a que sea esta misma vecindad la que contrate un servicio de seguridad por terceros o en el mejor de los casos, que entidades públicas de mayor alcance sean las encargadas de esta mejor gestión para la seguridad.

Según Mollericona; Tinini y Paredes (2007, P. X). Los resultados de su investigación explican la reconfiguración de la seguridad pública a partir de la autogestión local de la seguridad. Por un lado, se tiene lo que se ha llamado la "terciarización" de la seguridad ciudadana, expresada en la contratación de empresas privadas de seguridad; y, por otro lado, la "colectivización de la seguridad", siendo su máxima expresión la conformación de brigadas vecinales de seguridad. Según Mollericona; Tinini y Paredes (2007, P. X) la presente investigación se asienta sobre una metodología cualitativa que permita explorar las complejas acciones y reacciones vecinales en la construcción de los mecanismos locales de prevención para la seguridad.

A partir de este enunciado, podemos concluir que un manejo óptimo del servicio de seguridad para el ciudadano puede ser tercerizado en beneficio a la comunidad. De esta manera, cualquier entidad privada especializada en el rubro de seguridad puede hacer uso de sus conocimientos para brindar mejores herramientas con la finalidad de contribuir con la baja en los niveles de delincuencia que pueda existir en nuestra sociedad desde un barrio, un distrito o toda una región.

a) Dimensiones:
    1) Percepción de la Seguridad:

Según Mollericona; Tinini y Paredes (2007, P. 43). Por lo general, la gente o los lugareños vincularían espontáneamente el aumento de la delincuencia y los delitos con un aumento de la inseguridad.

2) Gestión Local de la Seguridad:

Según Mollericona; Tinini y Paredes (2007, P. 60). Un ejemplo de externalización de la seguridad es la gestión local de la seguridad, que se realiza en ocho de los quince planes de Ciudad Satélite. La disposición y la evaluación son dos componentes de intervención sumamente particulares de esta tercerización.

3) Reacción ciudadana:

Según Mollericona; Tinini y Paredes (2007, P. 35). En los últimos años, el aumento de la inseguridad y la ineficacia de la policía en la ciudad de El Alto han llevado a la sociedad a tomar medidas preventivas y punitivas contra la delincuencia, al mismo tiempo que busca métodos alternativos de prevención.

b) Indicadores

1) Delitos

Estos sucesos afectan la calidad de vida de la población, pues, en muchos casos, los vecinos viven angustiados. Mollericona; Tinini y Paredes (2007, P. 44)

2) Disposición de vigilancia

La disposición de la vigilancia surge inicialmente con la "semana de prueba" del servicio, a partir del convenio firmado entre la seguridad privada y los vecinos, seguido por la negociación sobre la ubicación de las casetas de vigilancia según los puntos registrados como espacios inseguros por los vecinos. (Mollericona; Tinini y Paredes, 2007, P. 60)

3) Prevención de la Inseguridad

Estos mecanismos de prevención son actualmente una de las estrategias vecinales utilizadas para afrontar la inseguridad en su barrio o en la calle, y

se consolidan en función de las características socioeconómicas y culturales de la sociedad. (Mollericona; Tinini y Paredes,2007, P. 38)

2.2.2. Variable Independiente

a) Metodología Variable Independiente

Api JavaScript Google Maps

Es un servicio de Google que usa tecnología de geolocalización de mapas 2D debido a lo bien que se puede usar para rastrear alertas, esto siendo relevante para el proyecto. Se utiliza una especie de identificador (Interfaz de programación de aplicaciones) para permitir el uso de aplicaciones con Google Maps. Primero debemos solicitarlo y luego lo insertamos a nuestro sitio web. (Cubel, 2018).

Apache NetBeans IDE

NetBeans es un IDE (*Integrated Development Environmen*t) o "Entorno de Desarrollo Integrado", gratuito y de código abierto. Cabe señalar que se emplea en la creación de aplicaciones de escritorio, móviles, corporativas y web que utilizan, entre otras plataformas, HTML5 y Java. (Fantino, 2021).

Arquitectura JMX

La especificación Java conocida como *Java Management Extensions* (JMX) define la arquitectura de operación, que facilita la gestión de aplicaciones y servicios (Ver Figura 1). Como veremos más adelante, esta tecnología permite a los desarrolladores de Java vincular sus aplicaciones con las soluciones de gestión y operación existentes. (Oracle,2022).

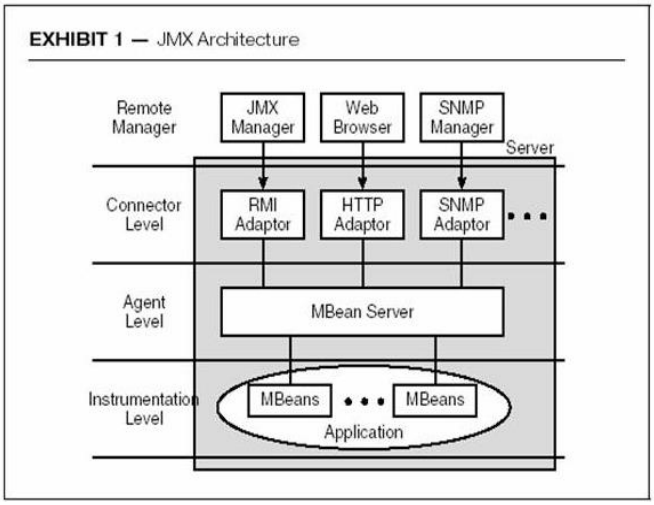


Figura 1. Arquitectura JMX. Diseño arquitectónico de la composición desde el nivel de servidor a la aplicación.
Fuente: Santiago Pereira, Instrumentación de componentes Java usando JMX (2005)

Docker

Según (Jsitech, Jason Soto, 2022). Es un proyecto de código abierto basado en contenedores de Linux; Esencialmente, es un motor de contenedores que crea contenedores sobre el sistema operativo y automatiza la implementación de aplicaciones dentro de ellos utilizando características del Kernel de Linux como espacios de nombres y controles de grupo.

Se deben comprender los siguientes tres componentes para comprender completamente cómo funciona Docker internamente (Ver Figura 2):

1) Imágenes de Docker (*Docker Images*)

   Una imagen de Docker puede tener instalado el sistema operativo CentOS o Ubuntu con apache, pero solo podemos crear contenedores basados en esta configuración porque las imágenes de Docker son plantillas de solo lectura. Si hacemos cambios en el contenedor ya lanzado, al detenerlo esto no se verá reflejado en la imagen. Más adelante entenderemos esta parte.

2) Registros de Docker (*Docker Registries*)

Los registros de Docker guardan las imágenes, estos son repositorios públicos o privados donde podemos subir o descargar imágenes. El Hub de Docker ofrece una colección de imágenes para nuestro uso y ofrece el registro público como servicio. Los registros de Docker básicamente son el componente de Distribución de Docker.

3) Contenedores de Docker (Docker Containers)

Todo lo necesario para ejecutar una aplicación está contenido en un contenedor Docker. Se utiliza una imagen de Docker para generar cada contenedor. Cada contenedor funciona como una plataforma separada.

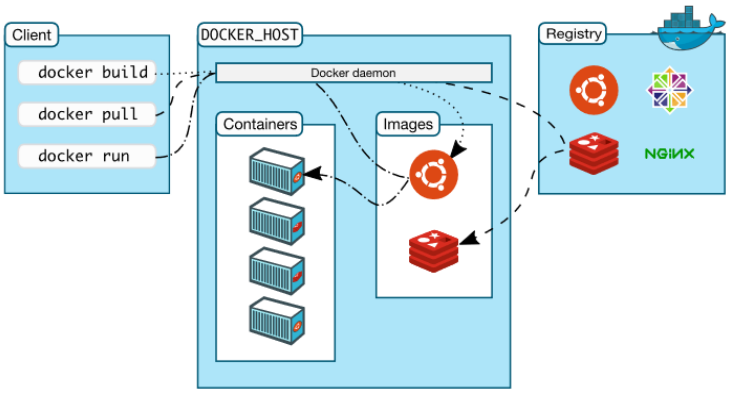


Figura 2. Arquitectura Docker. Componentes fundamentales del Docker.
Fuente: (Jsitech, Jason Soto, 2022)

Diagram.net

Con la ayuda de Diagrams.net, una aplicación web gratuita y de código abierto, se puede crear una amplia gama de diagramas utilizando cualquier navegador web. También se puede acceder a una versión de escritorio de la herramienta para Windows, Linux y macOS. (VictorD3D, 2020)

DBeaver

Las bases de datos más conocidas del mercado (MySQL, Oracle, DB2, SQL Server, PostgreSQL, etc.), así como varias bases de datos NoSQL, son compatibles con DBeaver, un gestor universal de base de datos (BBDD) multiplataforma. (DBeaver Community, 2022).

Firebase Storage

Se puede guardar imágenes y videos tomados por los usuarios de una aplicación usando el *Cloud Storage*. Los usuarios podrán descargar subir fotografías y videos, así como descargarlas usando este servicio. El contenido que usa una aplicación también puede almacenarse en la nube, lo que le permitiría a uno, como desarrollador, actualizar o cambiar el diseño visual de nuestra aplicación sin tener que publicar una nueva versión en el *store*. (Herrera, 2022).

Google Cloud

Google Cloud Platform es una *suite* de infraestructuras y servicios que Google utiliza internamente y pone a disposición de cualquier organización que lo solicite. Es adaptable a una amplia gama de actividades comerciales. (Google, 2022).

Java

Según el sitio web oficial de Java, es un lenguaje de programación sencillo y comprensible que tiene más de 9 millones de usuarios en todo el mundo. De hecho, se ha clasificado constantemente en las primeras posiciones de la lista de lenguajes de programación a lo largo del siglo XXI y está presente en más de 7 mil millones de dispositivos. (Carranza, 2021).

Java Development Kit

Un entorno de desarrollo de software que se utiliza para crear programas y subprogramas de Java se denomina Kit de desarrollo de Java (JDK). Se incluyen *Java Runtime Environment* (JRE), un intérprete/cargador (Java), un compilador (Javac), un archivador (Jar), un generador de documentación (Javadoc) y otras herramientas necesarias para el desarrollo de Java. (Walton, 2022).

JSF (*JavaServer Faces*)

Un *framework* de interfaz de usuario de componentes del lado del servidor para aplicaciones web basadas en tecnología Java se llama *JavaServer Faces*.

Una *Application Programming Interface* (API) o su traducción al español, Interfaz de Programación de Aplicaciones, se representa como componentes para una *User Interface* (UI) o su traducción al español, Interfaz de Usuario, cuya funcionalidad ocupa en: Manejar eventos, validar en el servidor y conversión de datos, definir la navegación de páginas y soporte de internacionalización y accesibilidad.

Además, para expresar los componentes en una página *Java Server Pages* (JSP) y conectar los componentes a los objetos del servidor, se utilizan dos bibliotecas de etiquetas JSP únicas. (Junta de Andalucía, 2020)

MySQL

Uno de los gestores de bases de datos más utilizados en el mundo es MySQL y cuenta con doble licencia. Es de código abierto, por un lado, pero también tiene una versión comercial controlada por la compañía Oracle. (Gilfillan, 2003)

MySQL Workbench

Diseñar, modelar, crear y administrar bases de datos visualmente es posible con MySQL Workbench. Tiene todos los componentes que un modelador de datos necesita para construir modelos ER (*Entity Relationship Model)* intrincados, hacer ingeniería directa e inversa, y brinda una funcionalidad crucial para completar tareas desafiantes de documentación y administración de cambios, que normalmente requieren mucho tiempo y esfuerzo. (Damian, 2017).

Maven

En la búsqueda de una herramienta simplificada para hacer uso en la construcción de software se encuentra Maven.

Según (García, 2015) menciona:

> Una de las herramientas más útiles a la hora de utilizar librerías de terceros es Maven. Maven se utiliza en la gestión y construcción de software. Posee la capacidad de realizar ciertas tareas claramente definidas, como la compilación del código y su empaquetado. Es decir, hace posible la creación de software con dependencias incluidas dentro

de la estructura del JAR (*Java Archive*). Es necesario definir todas las dependencias del proyecto (librerías externas utilizadas) en un fichero propio de todo proyecto Maven, el POM (*Project Object Model*). Este es un archivo en formato XML que contiene todo lo necesario para que a la hora de generar el fichero ejecutable de nuestra aplicación este contenga todo lo que necesita para su ejecución en su interior.

Así, Maven es la herramienta adecuada para cualquier proyecto basado en Java en donde se busque principalmente la simplificación de los procesos.

MyBatis

Un *framework* de persistencia con soporte para SQL, procedimientos almacenados y mapeos sofisticados se llama MyBatis (anteriormente conocido como iBatis). Como resultado, la programación se simplifica en comparación con la *Java Database Connectivity* (JDBC) y se puede personalizar mediante el *Extensible Markup Language* (XML) o su traducción al español, Lenguaje de Marcado Extensible, o anotaciones. (Mybatis, 2022).

PrimeFaces

PrimeFaces es una librería de componentes visuales de código abierto para *JavaServer Faces* (JSF) que contiene componentes para crear sitios web personalizados y fáciles de usar, así como aplicaciones web. (Wieldt, 2014).

Realtime Database GC

Realtime Database proporciona un árbol *JavaScript Object Notation* (JSON) que se puede usar para almacenar una colección de datos sencillos y ejecutar operaciones básicas de lectura y consulta en ellos. (Herrera, 2022).

Sistema Web

Las aplicaciones de software que se pueden usar al conectarse a un servidor web a través de Internet o una intranet usando un navegador se denominan sistemas web. (San Juan, 2016)

Spring Framework

Al ser una plataforma Java de código abierto, fue creada inicialmente por Rod Johnson y estuvo disponible originalmente en junio de 2003 bajo la licencia Apache 2.0. Desde entonces, se ha convertido en el framework corporativo de Java más apreciado para escribir código rápido, ligero y reutilizable, dado que su objetivo es controlar, administrar, estandarizar y resolver posibles problemas relacionados con la programación. Con el fin de proporcionar un modelo completo tanto para la configuración como para la programación de aplicaciones comerciales creadas en Java, sin preferencia por una plataforma sobre otra, Spring brinda soporte de infraestructura a nivel de aplicación. (Muradas 2018).

Socket IO

Son una tecnología que permite la comunicación entre el cliente y el servidor en ambas direcciones a través de un único socket TCP (*Transmission Control Protocol*) (Ver Figura 3). Ya que no tenemos que pedir los datos; el servidor nos lo proporcionará cuando haya nuevos, y en base a esto se podría considerarse una buena alternativa a AJAX (*Asynchronous JavaScript and XML*) como tecnología para obtener datos del servidor. (Carlos Azaustre, 2015).

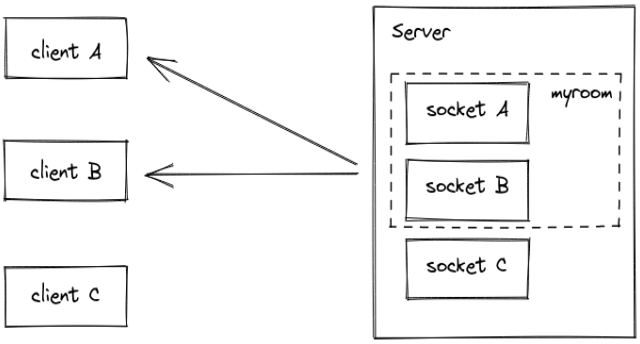


Figura 3. Diagrama del Socket.io. Demostración en la comunicación de canales bidireccionales usando eventos de respuesta.
Fuente: Rooms | Socket.IO (2022)

Según (Socket.IO, 2022). Se elige como solución el uso del Socket.io en vez de un websocket común por las siguientes consideraciones:

- Rendimiento: Socket.io generalmente se usa para establecer la conexión, lo que brinda al servidor y al cliente una ruta de comunicación económica.
- Confiable: En caso de problemas al reanudar la búsqueda prolongada de HTTP (*Hypertext Transfer Protocol*), se puede restablecer. Además, el cliente intentará restablecer automáticamente la conexión si se interrumpe.
- Escalable: Escala a múltiples servidores y entrega fácilmente eventos a cada cliente conectado.

2.2.3. Metodología

Metodología RUP

Según (Vera; Córdova; López; Pacheco, 2019) en su análisis de la metodología RUP en el desarrollo de software académico mediante la herramienta DJANGO menciona que el *Rational Unified Process* o por sus siglas RUP, es un proceso de ingeniería de software que suministra un enfoque para asignar tareas dentro de una organización de desarrollo, cuyo objetivo es asegurar que la producción del software tenga como consideración una alta calidad en satisfacer las necesidades de los usuarios bajo cualquier requerimiento descrito.

Las fases de esta metodología comienzan desde la fase de inicio o diseño, en el que se identifican los riesgos asociados al proyecto, se elaboran planes de las fases y de la iteración posterior. En la fase de elaboración se diseña la solución preliminar, se seleccionan casos de usos que permiten definir la arquitectura base del sistema y se desarrollará el primer análisis del dominio del problema.

En la fase de desarrollo o construcción se trata en completar la funcionalidad del sistema, se clarifican los requisitos pendientes, se administran los cambios de acuerdo a las evaluaciones realizadas por los usuarios, e iterativamente se realizan mejoras para el proyecto.

Por último, en la fase de transición, se considera el cierre del proyecto cuyo propósito es asegurar que el software esté disponible para el usuario final, se ajustan los errores y defectos encontrados en las pruebas de aceptación, se capacitan a los usuarios y se provee el soporte necesario.

2.3. Definición de términos básicos

Los términos básicos que se están empleando en el presente trabajo son las siguientes:

Alertas

Según la Oficina de Coordinación de Asuntos Humanitarios (OCHA, 1992), una alerta es un período anterior a la ocurrencia de un desastre, declarado con el fin de tomar precauciones específicas, debido a la probable y cercana ocurrencia de un desastre.
A partir de esta definición se podría concluir que las alertas son sucesos o incidencias donde terminan siendo reportadas a las localidades pertinentes en referencia a algo emergente o alarmante para el ciudadano.

Alarmas

Según (Pérez, Gardey, 2013) definen a las alarmas o equipos de alarmas son dispositivos instalados en los lugares altos del lugar, y tienen como finalidad llamar la atención a los ciudadanos cercanos, indicando comúnmente a algo emergente sobre la situación.

Botón de Pánico

Según (Poder Judicial del Perú, 2021). Es una funcionalidad como complemento a un sistema de alarmas cuyo objetivo es notificar a la central receptora de monitoreo, la incidencia o suceso que está presentando actualmente la persona que activó dicha función.

Delito

Según el Ministerio de Justicia y Derechos Humanos (2017), en su presentación sobre "La Teoría Del Delito" define qué delito es toda acción y omisión culposa penada por ley, pudiendo ser esta una acción pasiva o activa en función a la conducta punible de quien lo cometa.

Además, según ideas de los juristas Von Liszt y Beling, un delito sería el comportamiento humano voluntario que actúa antijurídica y culpablemente pudiendo ser éste susceptible a una pena.

Para el Código Penal Peruano, actualizado al mes de junio del 2022, en el segundo libro sobre Delitos, los delitos en relación a la situación actual del país se pueden clasificar en: delitos contra la vida, el cuerpo y la salud, delitos contra la dignidad humana, delitos contra el honor, delitos contra la familia, delitos contra la libertad, delitos contra el patrimonio, delitos contra la confianza y la buena fe en los negocios, delitos contra los derechos intelectuales, delitos contra el patrimonio cultural, delitos contra el orden económico, delitos contra el orden financiero y monetario, delitos tributarios, delitos contra la seguridad pública, delitos ambientales, delitos contra la tranquilidad pública, delitos contra la humanidad, delitos contra el estado y la defensa nacional, delitos contra los poderes del estado y el orden constitucional, delitos contra la voluntad popular, delitos contra la administración pública y delitos contra la fe pública.

Emergencia

Según el Instituto Nacional de Seguridad y Salud en el trabajo de España (2022), una emergencia es una situación individual o colectiva que se presenta de manera inesperada, pudiendo o no afectar la integridad física de las personas, los bienes y/o al medio ambiente. La magnitud de esta, podría llegar a convertirse en una situación de calamidad pública.

Software Desktop

Según (Pedamkar, 2022). A diferencia de las aplicaciones web, el software desktop o de escritorio se puede ejecutar desde el lado local del ordenador y se instala en la computadora o el sistema de almacenamiento.

Teleoperador

Según (Gil, 2018). El teleoperador es el especialista encargado de atender a un usuario mediante un medio de comunicación, cualquier incidencia, consulta o reclamo que suceda en un tiempo indeterminado.

En función a esta tesis, el teleoperador es el encargado de monitorear las alertas de emergencia de los vecinos, inspeccionando la información adquirida y siendo el principal intermediario de las llamadas hechas por el vecino.

Vecino

Según (Significados, 2022). Es el término que se le da a una persona que habiendo vivido durante un tiempo determinado en una vecindad se le han adquirido los derechos propios de esta.

Para el presente estudio, los vecinos son usuarios de la aplicación móvil “Vecino” de la empresa, y son los encargados de enviar la alerta cuando emerge cualquier tipo de incidencia en su ubicación actual.

CAPÍTULO III: SISTEMA DE HIPÓTESIS

3.1. Hipótesis

3.1.1. Hipótesis general

La implementación de un sistema web de monitoreo de alertas de seguridad ciudadana influye positivamente en el área de informática de la empresa FIRINGS E.I.R.L. 2021-2022.

3.1.2. Hipótesis específicas

a) La implementación de un sistema web de monitoreo de alertas de seguridad ciudadana en el área de informática de la empresa FIRINGS E.I.R.L. 2021-2022 influye positivamente en la identificación de los delitos.
b) La implementación de un sistema web de monitoreo de alertas de seguridad ciudadana en el área de informática de la empresa FIRINGS E.I.R.L. 2021-2022 influye positivamente en la disposición de la vigilancia.
c) La implementación de un sistema web de monitoreo de alertas de seguridad ciudadana en el área de informática de la empresa FIRINGS E.I.R.L. 2021-2022 influye positivamente en la prevención de la inseguridad.

3.2. Variables

3.2.1. Definición conceptual de las variables

Se toman en cuenta las siguientes variables:

a) Variable dependiente: Seguridad ciudadana
b) Variable independiente: Sistema web

Con respecto a las dimensiones se tiene lo siguiente:

a) Percepción de la seguridad
b) Gestión local de la seguridad
c) Reacción ciudadana

De las dimensiones, obtenemos los siguientes indicadores respectivamente:

a) Delitos
b) Disposición de la Vigilancia
c) Prevención de la inseguridad

3.2.2. Matriz de Consistencia y de Operacionalización

Se realizó una matriz de la variable “Seguridad Ciudadana” (Ver Tabla 1) para lograr obtener las dimensiones necesarias para el proyecto e investigación. Así mismo obtener información de los conceptos principales según casos reales sobre seguridad ciudadana tales como “El Alto” de Mollericona, Tinini y Paredes (2007) logrando obtener las definiciones necesarias para la Matriz de Operacionalización (Ver Anexo 2).

A partir de la realización de la Matriz de Operacionalización se pudo generar los elementos claves para la Matriz de Consistencia (Ver Anexo 3) logrando obtener los problemas, objetivos e hipótesis tanto principales como específicos, todo esto a partir de la relación entre variables como sus dimensiones.

Comentado [LHPP3]: Debe ir como anexo

Comentado [P4R3]: Corregido

Comentado [LHPP5]: Debe ir como anexo

Comentado [P6R5]: Corregido

Tabla 1. Matriz de fuente-libro: Se intentó buscar 5 fuentes bibliográficas sobre la variable dependiente “Seguridad Ciudadana”.

N°	Definición
1	Según **(Dammert, 2007)** “El crecimiento de la violencia y la inseguridad ciudadana es un fenómeno social de gran trascendencia que está afectando la vida de las personas a nivel mundial. No obstante, los niveles en que se expresa este fenómeno no son homogéneos. Ello ha generado un extenso debate alrededor de este complejo tema, que busca dictaminar las causas y posibles consecuencias de las múltiples violencias que aquejan nuestras sociedades."
2	Según **(Juan Yhonny Mollericona P.; Ninoska Tinini M.; Adriana Paredes Cruz, 2007)** “Los resultados de esta investigación explican la reconfiguración de la seguridad pública a partir de la autogestión local de la seguridad. Por un lado, se tiene lo que se ha llamado la 'terciarización' de la seguridad ciudadana, expresada en la contratación de empresas privadas de seguridad; y por otro, la 'colectivización de la seguridad', siendo su máxima expresión la conformación de brigadas vecinales de seguridad.”
3	Según **(Villaplana Jiménez, 2021)** “Este artículo muestra y analiza la incorporación del gobierno abierto a las políticas de seguridad pública a partir de casos relevantes y pioneros puestos en práctica a nivel global. La seguridad pública se presenta como una necesidad irrenunciable de las sociedades, frente a amenazas como el terrorismo, la criminalidad, las catástrofes y los episodios de violencia colectiva. Se revisa, brevemente, el estado actual del gobierno abierto como estilo de gobierno y se identifican las principales organizaciones responsables de la materia en el panorama internacional. Se pone en relieve el alto potencial de aplicación del gobierno abierto a las políticas públicas de seguridad,

	siendo especialmente útil para desarrollar medidas anticorrupción, de prevención del delito y de eficiencia policial, entre otras.”
4	Según **(INEI 2021)** “La delincuencia y la inseguridad ciudadana constituye uno de los principales problemas en nuestra sociedad. Por ello, analizar los diferentes aspectos de esta problemática nacional a través de las estadísticas, contribuyen a conocer la incidencia y las zonas geográficas donde se genera la violencia, que cada vez es más frecuente en el país. Esta publicación está estructurada en trece capítulos en los cuales se abordan temas asociados a violencia, criminalidad y seguridad ciudadana, tales como denuncias por comisión de delitos, estadísticas policiales, fiscales, municipales, defensa pública; estadísticas del sistema judicial penal del Poder Judicial, población penitenciaria; feminicidio, violencia, victimización, gobernabilidad y principales problemas que afectan al país.”
5	Según **(Arraiza, 2016)** “El Centro de Investigaciones Municipales Aplicadas y la Fundación Konrad Adenauer presentan el Manual de gestión municipal con el fin de aportar una herramienta que permita mejorar la gestión de los gobiernos locales a partir de la eficiencia y la búsqueda del bien común. El objetivo de los contenidos del presente manual es dar a conocer nociones teóricas y prácticas para todas las personas involucradas en los procesos de toma decisión e implementación de políticas públicas del municipio: autoridades, funcionarios, empleados, concejales, asesores, consultores, estudiantes y ciudadanos.”

Fuente: Elaboración Propia

CAPÍTULO IV: METODOLOGÍA DE LA INVESTIGACIÓN

4.1. Tipo y Nivel

La investigación es de tipo aplicada ya que buscamos resolver el planteamiento que tiene la empresa FIRINGS E.I.R.L. de mejorar su actual sistema de alerta mediante la realización de un sistema web que podrá funcionar cumpliendo las necesidades que requiere dicha empresa.

Dado que el presente estudio necesita el enfoque cuantitativo de tipo exploratoria para la recopilación y análisis correspondiente en la identificación de delitos y el enfoque cualitativo de tipo narrativo para recolectar información en base a la experiencia sobre el tema del monitoreo de alertas; por ende, dada las razones anteriores, se utilizará el enfoque mixto en el presente estudio.

Comentado [LHPP7]: Es inconsistente, debe aclarar si va a tener un enfoque mixto o cuantitativo

Comentado [JJTS8R7]: Corregido

4.2. Diseño de investigación

Para el presente trabajo de investigación, se estarían tomando en cuenta un conjunto de alarmas configuradas por parte del área técnica cuya información se utilizará para la funcionalidad que compete durante el monitoreo; así mismo, tener a disposición las alertas generadas por el software desktop de la empresa FIRINGS E.I.R.L, cuya utilidad se usarán como fuente de datos primarios para el proceso de atención y de monitoreo. Por último, la información del teleoperador registrado en el software desktop. Todo ello servirá para la demostración de cada escenario propuesto de la investigación.

4.3. Población y muestra

La empresa FIRINGS E.I.R.L plantea utilizar el sistema web de monitoreo de alertas para diversas entidades de carácter público o privado, teniendo como característica principal del usuario, el querer mejorar su sistema de seguridad actual. De esta manera, se expone según las variables que mencionamos:

Para el indicador “delitos”, la población de estudio será la cantidad de incidencias generadas por el software desktop de las cuales la empresa FIRINGS E.I.R.L será responsable de brindar la relación de alertas para la clasificación del delito y el análisis del contexto de la alerta.

Para el indicador “disposición de la vigilancia”, la población de estudio se analiza a partir de las reuniones que tuvimos con el gerente general y de los ingenieros a cargo del desarrollo del software “Botón de Pánico”, donde en sí nos explicaron al detalle, el proceso de monitoreo de alertas y sus funcionalidades básicas.

Para el indicador “prevención de la inseguridad”, la población de estudio será la comprobación del funcionamiento de los equipos “FGS10” y la cantidad total que tienen almacenado en su local, cuyos criterios de aceptación son: El funcionamiento de sirena este operativo y que se apliquen en un área de influencia no mayor a los 300 metros.

Según el análisis realizado con la relación brindada por la empresa FIRINGS E.I.R.L. que comprende el volumen de data de alertas desde el año 2021, se determinó un promedio histórico de 800 alertas mensuales. Por ello, en la presente investigación determinamos como muestra, el 25% del promedio histórico mensual de alertas reportadas, que serían unas 200 alertas.

4.4. Técnicas e instrumentos de recolección de datos

4.4.1. Tipos de técnicas e instrumentos

Debido a que se utiliza un enfoque mixto de investigación. Se utilizará para el enfoque cuantitativo la técnica de fichaje mediante fichas de registro de alertas; para el enfoque cualitativo se utilizará las técnicas de entrevista y observación siendo el primero utilizado mediante un cuestionario enfocado a los temas de seguridad y funcionamiento del sistema que utiliza la empresa FIRINGS E.I.R.L. El segundo siendo un cuaderno de notas e imágenes para la recopilación tanto visual como comparativa de datos proporcionados en las entrevistas o reuniones.

Acerca de los instrumentos que se utilizaron, ver más en Anexo 1.

4.4.2. Criterios de validez y confiabilidad de los instrumentos

Se toman en cuenta las siguientes variables:

a) Variable dependiente: Seguridad ciudadana
b) Variable independiente: Sistema web

Con respecto a las dimensiones se tiene lo siguiente:

a) Percepción de la seguridad
b) Gestión local de la seguridad
c) Reacción ciudadana

De las dimensiones, se obtiene los siguientes indicadores respectivamente:

a) Delitos
b) Disposición de la Vigilancia
c) Prevención de la inseguridad

4.4.3. Procedimientos para la recolección de datos

Para la obtención de datos en función a los métodos de investigación utilizados para este estudio, la empresa FIRINGS E.I.R.L nos otorgará un documento de "Término de Referencia" o por sus siglas TDR, y la base de datos del software desktop donde se obtendrá los datos de incidencias ocurridas para poder identificar y clasificar los delitos, como el estado en que se encuentre, los datos del denunciante, lugar de la incidencia, entre otros datos relevantes para el proyecto.

Se obtendrá una entrevista virtual bajo el consentimiento del gerente general de la empresa FIRINGS E.I.R.L, el cual nos brindará información útil para la realización del sistema de monitoreo web necesario para su empresa.

Así mismo dentro de la entrevista se nos otorgará registro visual del funcionamiento de las alarmas, proporcionándonos los pros y contras de la misma.

4.5. Técnicas para el procesamiento y análisis de la información

La información que nos brindó el gerente de la empresa FIRINGS E.I.R.L. en las reuniones previas al inicio del proyecto se manifestó las características y funcionalidades que deberá tener el nuevo sistema web, estas son consideradas fundamentales para el desarrollo de la solución acorde a las necesidades del gerente.

Se implementará una base de datos mejorada con respecto a la que se encuentra en funcionamiento con el aplicativo de escritorio que cuenta la empresa actualmente; esta nueva base de datos tendrá mayor integridad y consistencia de datos que su predecesora.

Finalmente, se contará con reportes informativos que brindaran información relevante para la toma de decisiones a futuro por parte de la empresa FIRINGS E.I.R.L en relación a la mejora continua en sus procesos actuales en relación a la seguridad ciudadana.

CAPÍTULO V: DESARROLLO DE LA SOLUCIÓN

5.1. Diagnóstico

Para comenzar sobre el desarrollo de la solución propuesta, explicaremos qué herramienta se estará utilizando para el análisis del negocio y del sistema, y sus respectivos elementos, con el propósito de acercarnos a un mejor entendimiento acerca de la metodología que se aplicará.

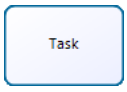
5.1.1. Herramientas

Se está utilizando la herramienta "*Diagrams.net*" para modelar los diagramas BPMN (*Business Process Modeling Notation*) para el diagnóstico del desarrollo, donde fielmente se está usando los elementos básicos para el modelado. Según (Help Bizagi, 2022), entre los elementos que se están utilizando son:

Comentado [LHPP9]: Todas las iniciales deben especificarse su significado para que todo lector lo entienda

Comentado [JJTS10R9]: Corregido

Tabla 2. Tabla de Herramientas Diagrams.net para el modelado BPMN.

Elementos	Descripción	Símbolo
Puerta de enlace exclusiva	De divergencia: Se utiliza para crear caminos alternativos dentro del proceso, pero solo uno se selecciona. De convergencia: Se utiliza para unir caminos alternativos.	
Puerta de enlace inclusiva	De divergencia: Representa un punto de ramificación en donde las alternativas se basan en expresiones condicionales. De convergencia: Se utiliza para unir una combinación de caminos paralelos alternativos.	
Tareas	Es una actividad atómica dentro de un flujo de proceso. Se utiliza cuando el trabajo en proceso no puede ser desglosado a un nivel más bajo de detalle.	
Tarea de Servicio	Es una tarea que utiliza algún tipo de servicio que puede ser web o una aplicación automatizada.	
Evento de inicio	Indica dónde se inicia un proceso. No tiene algún comportamiento particular.	

Evento de inicio de mensaje	Se utiliza cuando el inicio de un proceso se da al recibir un mensaje de un participante externo.	
Evento fin	Indica que el flujo termina.	
Evento Intermedio de Tiempo	Indica un retraso durante el proceso. Puede ser utilizado dentro de un flujo secuencial para indicar un tiempo de espera.	
Evento Intermedio de Mensaje	Indica que un mensaje puede ser recibido o enviado. Un proceso esperaría por el mensaje para continuar el flujo.	
Subproceso	Es una actividad cuyos detalles internos han sido modelados utilizando tareas, compuertas, eventos y flujos de secuencia.	

Fuente: Elaboración Propia

Con la misma herramienta, también se podrá realizar el modelamiento UML o "*Unified Modeling Language*" para el análisis del sistema y análisis de diseño. Según (Kde Umbrello, 2022), se comprende los elementos más comunes a los cuales se usan se mencionan en la siguiente tabla:

Tabla 3. Tabla de Herramientas Diagrams.net para el modelado UML

Elementos	Descripción	Símbolo
Actor	Un conjunto coherente de roles que juegan los usuarios cuando interaccionan con los casos de uso. Cualquier cosa con comportamiento (hardware, software, personas).	
Caso de Uso	Descripción de un conjunto de secuencias de acciones que ejecuta un sistema y que produce un resultado observable para un actor particular.	
Dependencia o instancia	Relación entre dos elementos en la que un cambio en uno de ellos afecta al otro (elemento dependiente)	

Asociación unidireccional	Relación entre dos o más clases que implica conexiones entre sus instancias. Puede ser bidireccional o unidireccional, dependiendo de si ambas conocen la existencia la una de la otra o no.	
Generalización	Relación taxonómica entre un elemento más general y otro más concreto.	
Clase Entidad	Una clase define los atributos y los métodos de un conjunto de objetos. Todos los objetos de una clase comparten el mismo comportamiento y poseen el mismo conjunto de atributos.	
Clase No Persistente	Es una clase personalizada que simboliza una estructura de datos no persistente; es decir, que no se guarda la información.	

Fuente: Elaboración Propia

5.1.2. Modelamiento BPMN AS-IS

En primer lugar, se explicará explícitamente cómo están estructurados los procesos que abarcan en el negocio, las actividades o tareas que intervienen a ello y describiendo desde un inicio a fin, el comportamiento del flujo de la información.

a) AS1: Monitoreo de Alertas

Cuando ocurre una incidencia, el usuario abre la aplicación “Vecino” desde su dispositivo móvil, donde le mostrará un formulario que debe ser llenado con los datos solicitados, así como la captura de una evidencia fotográfica. Luego de llenado el formulario, esta información viaja en comunicación vía TCP (*Transmission Control Protocol*) al software desktop.

En el mapa de monitoreo del teleoperador, se refleja la alerta con los datos reportados por el vecino. Consiguientemente, el teleoperador procederá a inspeccionar la alerta reportada, verificando la información de la alerta y del usuario que reportó dicha alerta.

Finalmente, el teleoperador procedería a comunicarse con el vecino, atendiendo de manera insistente lo ocurrido sobre la incidencia (Ver Figura 4).

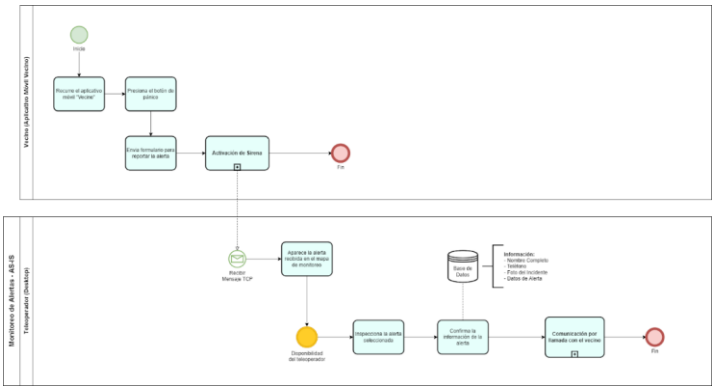


Figura 4. Diagrama del Modelamiento BPMN Monitoreo de Alertas AS-IS
Fuente: Elaboración Propia

b) AS2: Activación de Sirena

Se comprende que el equipo de alarma esté configurado para cuando reciba algún mensaje vía TCP (*Transmission Control Protocol*) o su traducción al español "Protocolo de Control de Transmisión", y este active su sirena durante un tiempo programado, y luego apagarse (Ver Figura 5).

Comentado [LHPP11]: Especificar esta inicial

Comentado [JJTS12R11]: Corregido

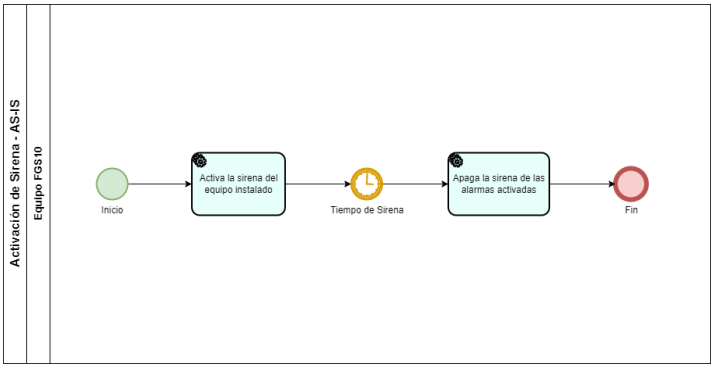


Figura 5. Diagrama del Modelamiento BPMN Activación de Sirena AS-IS.
Fuente: Elaboración Propia.

c) AS3: Comunicación por llamada con el vecino

Se comprende en que el teleoperador tenga el deber de llamar al vecino quien se encuentra en una emergencia, la información del vecino lo vería en una larga lista de contactos con sus respectivos teléfonos. Cuando lo llama, si el vecino no contesta la llamada, se concluye la atención de la alerta y la da por cancelada bajo el motivo “no responde”; de lo contrario, procede a atenderlo (Ver Figura 6).

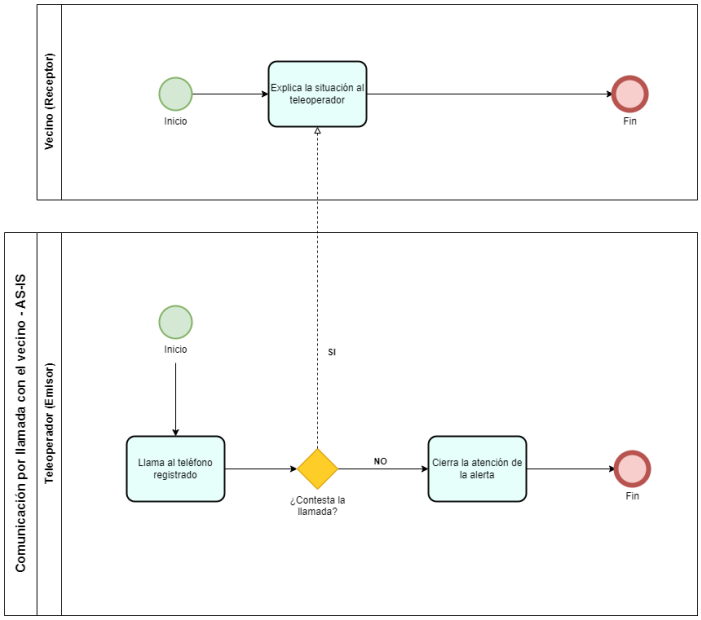


Figura 6. Diagrama del Modelamiento BPMN Comunicación por llamada con el vecino AS-IS.
Fuente: Elaboración Propia.

d) AS4: Generar Reportes

Hace referencia a que el gerente utiliza la opción de “Generar reportes” en el software desktop para hacer consulta de los gráficos estadísticos por cada tema, ya sea por armas, por ubicación, por persona, por incidente o por imágenes. Esta información es útil para la recolección de datos (Ver Figura 7).

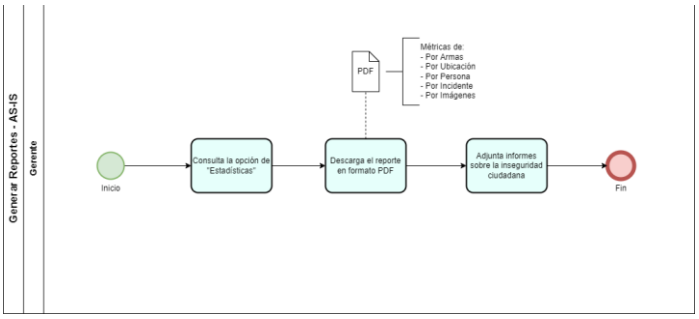


Figura 7. Diagrama del Modelamiento BPMN Generar Reportes AS-IS.
Fuente: Elaboración Propia.

5.1.3. Modelamiento BPMN TO-BE

Sobre el modelamiento TO-BE, se representará el modelado al negocio después de la implementación de nuestra solución propuesta, en donde se plasmará la idea desde una perspectiva de desarrollo, de las nuevas actividades que se adecuarán a los procesos anteriormente mencionados y crear un enfoque más centralizado al monitoreo para todo tipo de alertas existentes.

a) BE1: Monitoreo de Alertas

Teniendo como participante al administrador, podrá enviar bajo una cierta frecuencia de tiempo las alertas preparadas de un archivo CSV (*Comma-Separated Values*) para el envío de una carga masiva de alertas por vía TCP (*Transmission Control Protocol*) y en caso que salga un error, se visualizará aquellas alertas que no se procesaron correctamente.

Por otro lado, teniendo como participante al teleoperador, este presenciará cualquier alerta que emerja en el mapa de monitoreo del sistema web en tiempo real. Durante la actividad del teleoperador, cabe resaltar que la proactividad de este ante cualquier emergencia, debe ser constante en todo momento, por ello habría un subproceso que maneje este tipo de casos mediante el manejo de sesiones.

Dependiendo de la llegada de la alerta en el mapa de monitoreo, el primer teleoperador que encuentre su disponibilidad podrá llegar a atenderlo de

manera inmediata sin mucha demora; a su vez, notificándose en cualquier momento las alertas provenientes durante el proceso de monitoreo. Finalmente, el teleoperador procederá a comunicarse con el reportante para poder identificar el delito correspondiente (Ver Figura 8).

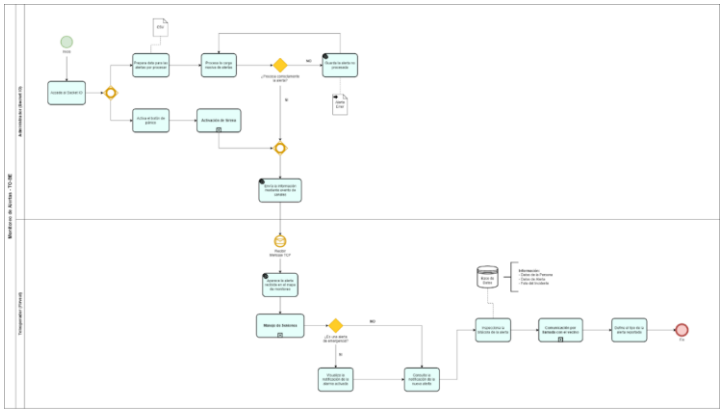


Figura 8. Diagrama del Modelamiento BPMN Monitoreo de Alertas TO-BE.
Fuente: Elaboración Propia.

b) BE2: Activación de Sirena

El equipo FGS10 activará su sirena si hubo una solicitud de alerta de emergencia cercana dentro del perímetro de su señal GSM (*Global System for Mobile communication*) o por su traducción al español "Sistema Global para las Comunicaciones Móviles", previamente configurada y durará en el tiempo programado previamente. Esto ayudaría en resolver qué alertas son participes a esta actividad de activación de la alarma y el comportamiento reflejado durante el monitoreo (Ver Figura 9).

Comentado [LHPP13]: Especificar la inicial

Comentado [JJTS14R13]: Corregido

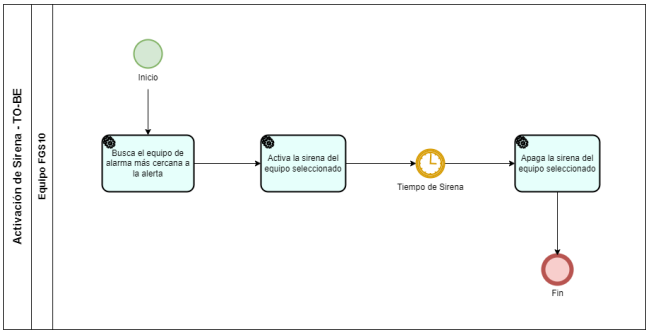


Figura 9. Diagrama del Modelamiento BPMN Activación de Sirena TO-BE.
Fuente: Elaboración Propia.

c) BE3: Manejo de Sesiones

Durante la labor de un teleoperador, se estaría facilitando el uso de sesiones respectivamente a su actividad durante el monitoreo de las alertas, con el fin de acatar el cumplimiento laboral de la atención de alertas y del rendimiento laboral.

Una de las formas que se podría aplicar para estos casos, sería el redireccionamiento al login a los usuarios que sobrepasen la inactividad establecida. Deberá el teleoperador iniciar la sesión para proceder a realizar sus deberes y así continuamente este subproceso se estaría repitiendo cada vez que se ausente durante la sesión que estableció. Como resultado, la sesión sería un recurso primario para la medición del trabajo del teleoperador y de la atención de la alerta (Ver Figura 10).

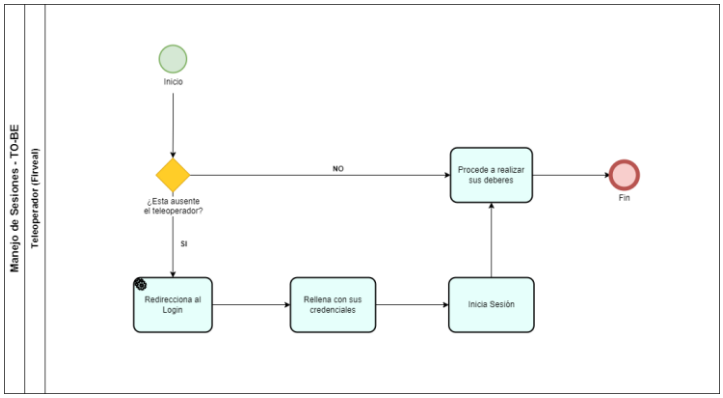


Figura 10. Diagrama del Modelamiento BPMN Manejo de Sesiones TO-BE.
Fuente: Elaboración Propia.

d) BE4: Generar Reportes

A comparación con el modelo AS-IS, se agrega la funcionalidad de poder visualizar el resultado de búsqueda del reporte correspondiente según lo filtrado, sin la necesidad de exportar primero el archivo. De esta forma, adicionalmente podrá revisar los reportes que genere desde el sistema web (Ver Figura 11).

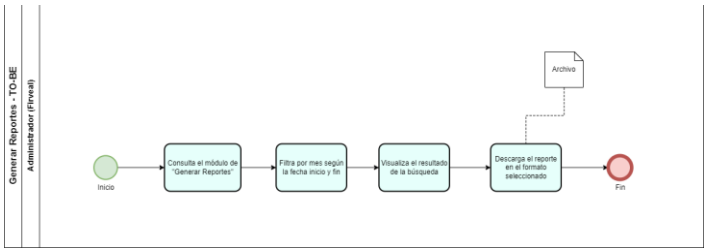


Figura 11. Diagrama del Modelamiento BPMN Generar Reportes TO-BE.
Fuente: Elaboración Propia.

e) BE5: Configurar Alarmas

Con respecto a los equipos de alarmas, es relevante saber la importancia acerca de la información de instalación y de configuración de las alarmas durante el proceso del monitoreo, conocer qué parámetros contiene esa información y de la ubicación exacta de las unidades, con el fin de saber estratégicamente donde posicionar estos elementos.

Para ello, se requiere gestionar el mantenimiento de las alarmas parametrizando su configuración e instalación, y de igual forma, conectarlo para realizar su respectiva simulación durante el monitoreo (Ver Figura 12).

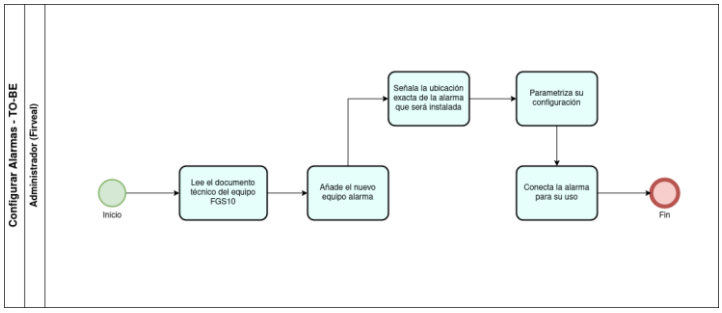


Figura 12. Diagrama del Modelamiento BPMN Configuración de Alarmas TO-BE.
Fuente: Elaboración Propia.

5.1.4. Reglas de Negocio

a) RN1: El teleoperador no puede atender más de una alerta a la vez.

b) RN2: En caso de que el teleoperador tenga impedimentos para la atención de una alerta, puede proceder a ceder el turno de la atención de la alerta a otro teleoperador.

c) RN3: Las alertas reportadas, deben tener una evidencia fotográfica al momento de generarse. Solamente la "alerta de emergencia" está exenta de esta evidencia, dado que es un proceso distinto.

d) RN4: Las sirenas sonarán siempre y cuando haya alguna alerta de emergencia cerca, con una duración mínima de 1 min a un máximo de 30 min.

e) RN5: Las sirenas de las alarmas solamente se activarán si el equipo está conectado.

f) RN6: La duración de las sirenas no deben superponerse unas sobre otras, y cada una debe sonar el tiempo que se tenga configurado.

g) RN7: Si aparece más de una alerta de emergencia dentro de la señal GSM (*Global System for Mobile communication*) de la alarma, se deberá resetear la duración del tiempo configurado de la alarma.

h) RN8: Las alertas, deben ser atendidas dentro de las 24 horas una vez generadas, caso contrario, pasarán a ser "no atendidas".

i) RN9: Las alertas de emergencia son las primeras en ser atendidas, tienen prioridad sobre las alertas comunes y no deben dejarse en espera.

j) RN10: La identificación del delito se realizaría siempre al cierre de su atención.

k) RN11: Los reportes informativos se deben generar a lo máximo cada mes.

5.1.5. Plan de Gestión de Riesgo

Se estará mencionando los posibles riesgos que consideramos tendrían un mayor impacto durante el transcurso del desarrollo de la solución.

Tabla 4. Tabla de Plan de Gestión de Riesgo

N.º	Descripción	Imp.	Prob.	Rie.	Contingencia	Mitigación
R5	Pérdida de información en la base de datos	5	3	15	Trabajar con el último backup subido en el repositorio	Realizar cada semana como mínimo un backup de la base de datos
R4	Ataque de virus informático	3	3	9	Hacer un checkout de los últimos cambios subidos al repositorio	Evitar el uso de programas externos o potencialmente maliciosos
R1	Demora en el desarrollo del software	4	2	8	Dar un plazo aproximado para el avance del desarrollo	Mostrar un prototipo para cada avance para que el sponsor se notifique del avance
R2	Incremento de errores/fallas	3	2	6	Manejar todas las excepciones posibles	Superar los bugfix como prioridad antes del desarrollo del siguiente caso de uso
R3	Incompatibilidad de hardware y/o software	4	1	5	Reestructurar las versiones de los componentes que se usan si lo requiere	Revisar las versiones correctas para el desarrollo de los proyectos.
R6	Distancia-miento del stakeholder	3	1	3	Obtener la carta de aprobación del interesado.	Se tratará de mantener en comunicación constante con el interesado

Fuente: Elaboración Propia

5.2. Metodología de desarrollo de la Solución

5.2.1. Requerimientos Funcionales

a) RF1: Iniciar Sesión

El sistema permite que los usuarios puedan ingresar a su sesión con sus credenciales.

b) RF2: Recuperar contraseña
   El sistema permite al usuario recuperar su contraseña en caso la haya olvidado.

c) RF3: Gestionar Usuarios
   El sistema permite que puedan crearse nuevos usuarios con la información personal correspondiente al trabajador.

d) RF4: Gestionar alarmas
   El sistema permite el mantenimiento de las alarmas instaladas, manejando principalmente la configuración establecida, así como los eventos y comandos que se están realizando durante su ejecución.

e) RF5: Ubicar alarmas
   El sistema permite mostrar mediante un mapa la ubicación geográfica de las alarmas instaladas.

f) RF6: Inspeccionar las alertas
   El sistema permite mostrar en el mapa, un icono por alerta que lleva al sistema, el cual muestra la información de la alerta generada.

g) RF7: Consulta notificaciones
   El sistema permite notificar al usuario cuando una alerta aparece durante el monitoreo o una alarma está activada.

h) RF8: Asignar delito
   El sistema permite que el teleoperador pueda asignar el delito correspondiente a la alerta inspeccionada.

i) RF9: Cargar alertas
   El sistema permite realizar la carga de alertas generadas al sistema web de manera automática y asíncrona.

j) RF10: Enviar alerta de emergencia
   El sistema permite realizar el envío de alertas comunes o de emergencia al sistema web de manera manual.

k) RF11: Generar reportes de alarmas

El sistema permite generar reportes mensuales (indicando fecha de inicio y fecha fin de ese mes) de todas las alarmas instaladas.

l) RF12: Generar reportes de alertas

El sistema permite generar reportes mensuales (indicando fecha de inicio y fecha fin de ese mes) de todas las alertas generadas en el mes.

m) RF13: Generar reportes de rendimiento

El sistema permite generar reportes mensuales (indicando fecha de inicio y fecha fin de ese mes) de los indicadores de evaluación para los teleoperadores registrados en el sistema.

5.2.2. Requerimientos No Funcionales

a) RNF1: Usabilidad

Se optará por usar como lenguaje el español para facilitar el acceso al usuario final del sistema. De igual manera, se introducirán algunas breves descripciones acerca de cada tarea por realizar en cada interfaz para la orientación del usuario.

b) RNF2: Disponibilidad

El sistema web estará disponible durante su despliegue, y se mantendrá desplegado salvo en ocasiones donde deba suspenderse las actividades por problemas técnicos o nuevas integraciones. En el caso del *websocket*, se mantendrá abierta la conexión de canales entre las aplicaciones participantes.

c) RNF3: Seguridad

Solamente podrán acceder al sistema el personal autorizado, además de contar con medidas de seguridad ante posibles ataques (Inyección SQL, Inyección HTML, etc.). Así mismo, contará el manejo de sesiones de los usuarios para facilitar el control de horas de uso del sistema y mitigar el abuso de peticiones externas a la web.

d) RNF4: Escalabilidad

Tanto el sistema web como el *websocket* contarán con la capacidad de permitir nuevas integraciones de desarrollo de funcionalidades adicionales o mejoras luego de su construcción y puesta en marcha inicial.

e) RNF5: Rendimiento en tiempo de respuesta

El sistema estará desarrollado para que el tiempo de respuesta de las solicitudes generadas y enviadas por los usuarios, tome el mínimo tiempo posible (siendo 650 milisegundos el mínimo óptimo establecido y 5 segundos como máximo óptimo).

f) RNF6: Soporte

El sistema será compatible con los navegadores más usados como el Google Chrome o Firefox, de forma que pueda ser accesible desde cualquier sistema operativo, ya sea del Windows o Linux.

g) RNF7: Amigable

Las interfaces del sistema web serán diseñadas para hacer la interacción con el usuario lo más dinámica y sencilla posible usando herramientas de diseño adecuadas para cualquier funcionalidad.

5.2.3. Diagrama de Actores del Sistema

Según el análisis previo, se obtiene el primer actor del sistema "Usuario", quien ocuparía a ser todo usuario que desee ingresar al sistema. También tenemos al "Administrador", cuyo rol es realizar las tareas administrativas y de gestión en el sistema. Y, por último, tendríamos al "Teleoperador" quien sería el encargado de monitorear las alertas (Ver Figura 13).

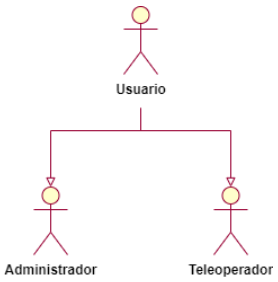


Figura 13. Diagrama de Actores del Sistema.
Fuente: Elaboración Propia.

5.2.4. Diagrama de Casos de Uso General

Como se tiene en cuenta que los principales objetivos que se requiere alcanzar son: La identificación del delito, mejorar la atención de las alertas y de la toma de decisiones. Entonces se obtienen los siguientes casos de uso del sistema (Ver Figura 14):

a) CUS1: Iniciar Sesión

   Permite acceder el sistema web desde una cuenta brindada por el administrador; los tipos de usuario al cual acceden al sistema son: El teleoperador y el administrador.

b) CUS2: Cambiar Contraseña

   Permite al usuario tener la disposición de cambiar su contraseña en caso se haya olvidado.

c) CUS3: Gestionar Usuarios

   Permite el mantenimiento de usuarios del sistema, gestionando su información personal y de poder restringir en el sistema a los usuarios sí es que lo amerita.

d) CUS4: Gestionar Alarmas

   Permite el mantenimiento de alarmas, gestionando principalmente su información configurable y de los eventos o comandos que esté realizando durante su periodo de funcionamiento.

e) CUS5: Ubicar Alarmas

   Permite encontrar específicamente dentro de un mapa la ubicación geográfica donde se colocaría la alarma.

f) CUS6: Atender Alertas

   Permite la visualización en tiempo real de las alertas emergentes en el mapa de monitoreo, la asignación de la atención del teleoperador, visualizar las alarmas activadas y de poder, inspeccionar las alertas.

g) CUS7: Consultar Notificaciones

Permite la consulta de cualquier notificación entrante durante el proceso de monitoreo, ya sea por la aparición de una nueva alerta o de la activación de una sirena de alguna alarma.

h) CUS8: Asignar Delitos de Alerta

Permite la asignación del delito correspondiente una vez definido en el cierre de la atención de la alerta por el teleoperador.

i) CUS9: Cargar Alertas

Permite el envío de alertas cargadas al sistema web con una frecuencia de tiempo programada.

j) CUS10: Enviar Alertas

Permite el envío de una alerta de emergencia del cual es el interruptor para la activación de la sirena de la alarma más cercana.

k) CUS11: Generar Reporte de Alarmas

Permite visualizar y generar reportes en detalle con respecto a las alarmas según el rango de fechas que se filtre.

l) CUS12: Generar Reporte de Alertas

Permite visualizar y generar reportes en detalle con respecto a las alertas según el rango de fechas que se filtre.

m) CUS13: Generar Reporte de Rendimiento

Permite visualizar y generar reportes en detalle con respecto al rendimiento de los teleoperadores sobre la atención de las alertas de los teleoperadores según el rango de fechas por filtrar.

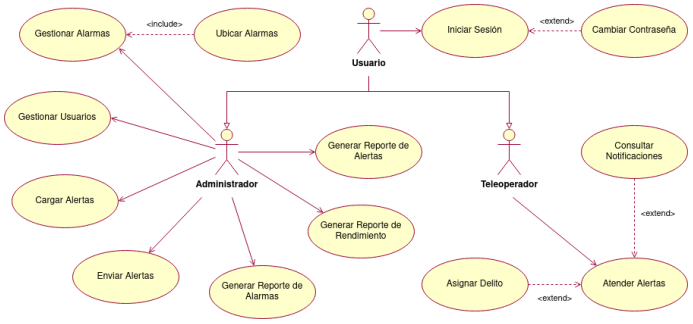


Figura 14. Diagrama de Casos de Uso General.
Fuente: Elaboración Propia.

5.2.5. Diagrama de Paquetes

Cada paquete indica el módulo perteneciente en el sistema, cuyos ciertos casos de uso correspondientes pertenecen a uno de los siguientes paquetes:

Tabla 5. Tabla de diagrama de paquetes

Entorno	Paquete	Caso de Uso
Firveal	Paquete Login	CUS1: Iniciar Sesión
		CUS2: Cambiar Contraseña
	Paquete Gestión	CUS3: Gestionar Usuarios
		CUS4: Gestionar Alarmas
		CUS5: Ubicar Alarmas
	Paquete Monitoreo	CUS6: Atender Alertas
		CUS7: Consultar Notificaciones
		CUS8: Asignar Delito
	Paquete Reporte	CUS11: Generar Reporte de Alarmas
		CUS12: Generar Reporte de Alertas
		CUS13: Generar Reporte de Rendimiento
Websocket	Paquete de Canales	CUS9: Cargar Alertas
		CUS10: Enviar Alertas

Fuente: Elaboración Propia

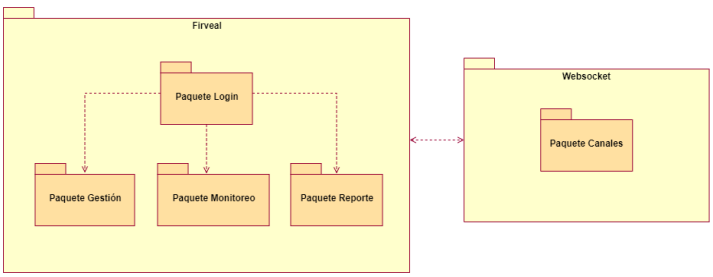


Figura 15. Diagrama de Paquetes.
Fuente: Elaboración Propia.

5.2.6. Matriz de Trazabilidad

Se muestra la tabla en relación de los casos de uso del sistema y de los requerimientos funcionales que fueron señalados anteriormente.

Tabla 6. Tabla de Matriz de Trazabilidad

Requerimientos Funcionales / Casos de Uso	CUS1 Iniciar Sesión	CUS2 Cambiar contraseña	CUS3 Gestionar Usuarios	CUS4 Gestionar Alarmas	CUS5 Ubicar Alarmas	CUS6 Atender Alertas	CUS7 Consultar Notificaciones	CUS8 Asignar Delito	CUS9 Cargar Alertas	CUS10 Enviar Alertas	CUS11 Generar Reporte de Alarmas	CUS12 Generar Reporte de Alertas	CUS13 Generar Reporte de Rendimiento
RFN01 Iniciar Sesión	↰												
RFN02 Recuperar Contraseña		↰											
RFN03 Gestionar Usuarios			↰										
RFN04 Gestionar Alarmas				↰									
RFN05 Ubicar Alarmas					↰								
RFN06 Inspeccionar las Alertas						↰							
RFN07 Consulta Notificaciones							↰						
RFN08 Asignar Delito a la Alerta								↰					
RFN09 Cargar Alertas al Monitoreo									↰				
RFN10 Enviar Alertas al Monitoreo										↰			
RFN11 Generar Reporte de Alarmas											↰		
RFN12 Generar Reporte de Alertas												↰	
RFN13 Generar Reporte de Rendimiento													↰

Fuente: Elaboración Propia

5.2.7. Casos de Uso Priorizados

Se identifican los casos de uso prioritarios basándose en los requerimientos descritos para el cumplimiento de la hipótesis de la solución que estimamos alcanzar.

En primer lugar, se identifican bajo los siguientes criterios:

a) Color rojo: Alta
b) Color Naranja: Secundaria
c) Color Azul: Opcional

Se obtiene como resultado:

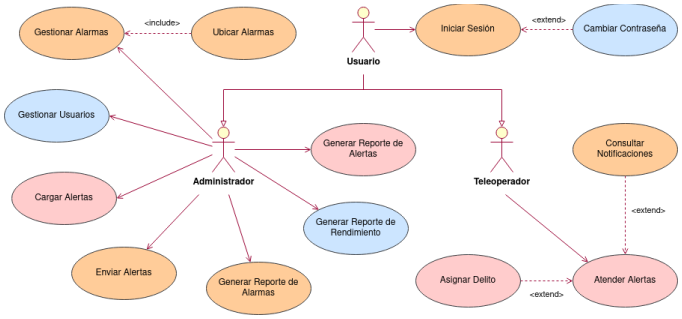


Figura 16. Diagrama de Casos de Uso Priorizados
Fuente: Elaboración Propia.

El siguiente paso es valorar los casos de uso según la prioridad mencionada y la dificultad en la complejidad de su desarrollo, con el objetivo próximo a saber el nivel de esfuerzo que conlleva la realización de los casos de uso del sistema.

a) Prioridad: 3=Alta, 2=Secundaria, 1=Opcional
b) Dificultad: 3=Alta, 2=Media, 1=Baja
c) Puntaje: Total entre la prioridad y la dificultad

Tabla 7. Tabla de Casos de Uso Priorizados

Nombre CUS	Actor	Paquete	Prioridad	Dificultad	Puntaje
Atender Alertas	Teleoperador	Paquete Monitoreo	3	3	6
Cargar Alertas	Administrador	Paquete Canales	3	3	6
Generar Reporte de Alertas	Administrador	Paquete Reporte	3	2	5
Asignar Delito	Teleoperador	Paquete Monitoreo	3	2	5
Consultar Notificaciones	Teleoperador	Paquete Monitoreo	2	3	5
Gestionar Alarmas	Administrador	Paquete Gestión	2	3	5
Generar Reporte de Alarmas	Administrador	Paquete Reporte	2	2	4
Enviar Alertas	Administrador	Paquete Canales	2	2	4
Ubicar Alarmas	Administrador	Paquete Gestión	2	2	4
Iniciar Sesión	Usuario	Paquete Login	2	2	4

Generar Reporte de Rendimiento	Administrador	Paquete Reporte	1	2	3
Gestionar Usuarios	Administrador	Paquete Gestión	1	2	3
Cambiar Contraseña	Usuario	Paquete Login	1	1	2

Fuente: Elaboración Propia

En conclusión, según como se muestra en la tabla de casos de uso priorizados, se desarrollará durante el transcurso de la elaboración de la solución, aquellos casos de uso cuyo puntaje es mayor o igual a "4" para demostrar la sustentación de las hipótesis.

5.2.8. Benchmarking

En la siguiente tabla, se ha realizado la comparación con 3 productos similares al desarrollado, siendo DeskAlerts, AlertMedia y AlertCops.

Con DeskAlerts se puede enviar rápida y fácilmente notificaciones de escritorio directamente a las pantallas de las computadoras de sus empleados que aparecen en un cuadro emergente. Este es un canal de comunicaciones internas deliberadamente disruptivo que atraviesa el desorden y el ruido digital, apareciendo de una manera que no se puede omitir, ignorar o minimizar, lo que le brinda la tranquilidad de que se están entregando sus comunicaciones corporativas. ([Página web de DeskAlerts], s.f.)

AlertMedia es una plataforma intuitiva que ofrece capacidades de comunicación líderes en la industria, respaldadas por un equipo de éxito del cliente receptivo y experimentado, para mantener a su fuerza laboral segura, informada y conectada cuando más importa. ([Página web de AlertMedia], s.f.)

AlertCops, es una aplicación española de la policía y guardia civil que, en caso de alerta, tu posición se envía al centro operativo más próximo y ante situaciones de riesgo colabora con las fuerzas policiales para ayudar a otros ciudadanos. ([Página web de AlertCops], s.f.).

Tabla 8. Tabla de Benchmarking para el proyecto de "Sistema Web de Monitoreo de Alertas"

Benchmarking para el Proyecto de Sistema Web de Monitoreo de Alertas de Seguridad Ciudadana para la Empresa FIRINGS E.I.R.L.										
Análisis Comparativo		Peso	Sistema Web de Monitoreo de Alertas FIRVEAL		Sistema de Notificaciones de Emergencia		AlertMedia		AlertCops	
N°	Características		Calificación del 1 al 3 sobre funcionalidad							
CUS01	Iniciar Sesión	2	3	6	3	6	1	2	3	6
CUS02	Cambiar Contraseña	1	1	1	2	2	1	1	3	3
CUS03	Gestionar Usuarios	1	1	1	3	3	3	3	3	3
CUS04	Gestionar Alarmas	2	3	6	1	2	1	2	1	2
CUS05	Ubicar Alarmas	2	3	6	1	2	1	2	1	2
CUS06	Atender Alertas	3	3	9	3	9	3	9	3	9
CUS07	Consultar Notificaciones	3	3	9	3	9	3	9	3	9
CUS08	Asignar Delito	3	3	9	1	3	3	9	3	9
CUS09	Cargar Alertas	3	3	9	2	6	2	6	1	3
CUS10	Enviar Alertas	3	3	9	3	9	3	9	3	9
CUS11	Generar Reporte de Alertas	3	3	9	2	6	3	9	2	6
CUS12	Generar Reporte de Alarmas	3	3	9	2	6	3	9	2	6
CUS13	Generar Reporte de Rendimiento	1	1	1	2	2	3	3	2	2
N°	Requerimientos No Funcionales									
RNF1	Usabilidad	2	2	4	3	6	1	2	3	6
RNF2	Disponibilidad	3	3	9	3	9	3	9	3	9
RNF3	Seguridad	2	2	4	1	2	3	6	3	6
RNF4	Escalabilidad	3	3	9	3	9	3	9	2	6
RNF5	Rendimiento en tiempo de respuesta	3	2	6	3	9	3	9	3	9
RNF6	Soporte	2	3	6	2	4	1	2	1	2
RNF7	Amigable	2	2	4	3	6	3	6	3	6
Puntaje				**126**		**110**		**116**		**113**
Especificaciones										
Sistema Operativo			Ubuntu 20.04		-		-		-	
Servidor de Base de Datos			MySQL 8		-		-		-	
Lenguaje de Programación			Java		-		-		-	
Requisitos Mínimos										
Procesador (Min)			Intel Core3 Duo 2.7GHz		Intel Core3 Duo 2.7GHz		Intel Core3 Duo 2.7GHz		Intel Core3 Duo 2.7GHz	
Memoria RAM (Min)			4GB		4GB		4GB		4GB	
Leyenda de Peso de las Funcionalidad										
1.- Baja (Cumple con bajas expectativas y con pocos datos)										
2.- Media (Cumple y con datos suficientes)										
3.- Alta (Cumple con altas expectativas y con datos suficientes)										

Fuente: Elaboración Propia

5.2.9. Especificación del Caso de Uso

ECUS7: Cargar Alertas

Tabla 9. Tabla de Especificaciones del Caso de Uso en Cargar Alerta

<table>
<tr><td>Términos</td><td colspan="4">Definición</td></tr>
<tr><td>Caso de uso</td><td colspan="4">Cargar alertas</td></tr>
<tr><td>Descripción general</td><td colspan="4">Permite el envío de alertas cargadas al sistema web con una frecuencia de tiempo programada.</td></tr>
<tr><td>Requerimiento funcional</td><td colspan="4">Rf10: Cargar Alertas</td></tr>
<tr><td>Precondición</td><td colspan="4">● Preparar una población cargada de alertas para procesar.</td></tr>
<tr><td>Criterios de aceptación</td><td colspan="4">● Provisionar el healthy del socket para la abierta conexión.
● Habilitar canales específicos para las alertas comunes.
● Enviar una o varias alertas cargadas al monitoreo.
● Se envía bajo una frecuencia de tiempo programable.</td></tr>
<tr><td>Actores</td><td colspan="4">Administrador</td></tr>
<tr><td rowspan="6">Flujo principal “habilitar canales”</td><td colspan="2">Actor</td><td colspan="2">Sistema</td></tr>
<tr><td>1</td><td>El administrador desea enviar alguna información como publicador del flujo a través de algún canal abierto.</td><td></td><td></td></tr>
<tr><td></td><td></td><td>2</td><td>Encapsula la información en el canal y reenvía como evento.</td></tr>
<tr><td colspan="4">Resultado</td></tr>
<tr><td>3</td><td colspan="3">Envía el mensaje a los consumidores del canal.</td></tr>
<tr><td colspan="4">Excepciones</td></tr>
<tr><td colspan="4">● Cuando se interrumpe el servidor del websocket, se encola las peticiones del publicador sobre el canal asignado. Eso quiere decir que cuando esté operativo el servidor, reanuda el proceso de envío.</td></tr>
<tr><td rowspan="8">Flujo principal “cargar alertas”</td><td colspan="2">Actor</td><td colspan="2">Sistema</td></tr>
<tr><td></td><td></td><td>1</td><td>Se muestra en un interfaz, un formulario para subir un archivo y un botón “enviar”. Además de una grilla con la información de la alerta y del vecino.</td></tr>
<tr><td>2</td><td>Adjunta un archivo con alertas cargadas.</td><td></td><td></td></tr>
<tr><td>3</td><td>Da clic en el botón “enviar”.</td><td></td><td></td></tr>
<tr><td></td><td></td><td>4</td><td>Encola cada alerta cargada del archivo adjuntado.</td></tr>
<tr><td></td><td></td><td>5</td><td>Se muestran las alertas que fueron correctamente procesadas.</td></tr>
<tr><td colspan="4">Resultado</td></tr>
<tr><td>6</td><td colspan="3">La alerta cargada fue enviada por el canal correspondiente.</td></tr>
<tr><td colspan="4">Excepciones</td></tr>
</table>

	● En caso haya algún error durante el proceso de envío, muestra la alerta que no fue procesada correctamente. ● Si el archivo no fue adjuntado correctamente, mostrará un mensaje de error.
Relación con otros casos de uso	Ninguna.
Prototipos	

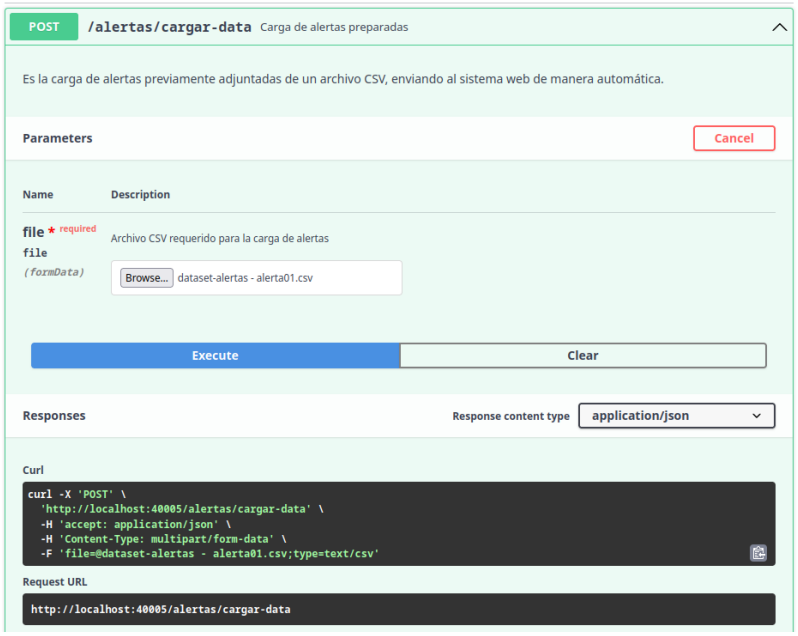


Figura 17. Prototipo del CUS Cargar Alertas con swagger editor.
Fuente: Elaboración Propia.

Fuente: Elaboración Propia

ECUS4: Atender Alertas

Tabla 10. Tabla de Especificaciones del Caso de Uso en Atender Alertas.

Términos	Definición
Caso de uso	Atender alertas
Descripción general	Permite la visualización en tiempo real de las alertas emergentes en el mapa de monitoreo, la asignación de la atención del teleoperador, visualizar las alarmas activadas y de poder inspeccionar las alertas.
Requerimiento funcional	Rf6: Inspeccionar las alertas
Precondición	● Debe haber iniciado sesión en el sistema web. ● Tener conexión abierta para el websocket.

<table>
<tr><td>Criterios de aceptación</td><td colspan="4">● Visualizar la aparición de alertas nuevas en el mapa de monitoreo.
● Visualizar la activación de sirena de una alarma.
● Emitir sonido de alarma.
● Inspeccionar una alerta pendiente.
● Asignación de atención de alertas a los teleoperadores.
● Cambio de estado de la atención de la alerta.</td></tr>
<tr><td>Actores</td><td colspan="4">Teleoperador</td></tr>
<tr><td rowspan="9">Flujo principal “visualizar alertas en mapa de monitoreo”</td><td colspan="2">Actor</td><td colspan="2">Sistema</td></tr>
<tr><td>1</td><td>Da clic en la opción de “Monitorear Alertas”.</td><td></td><td></td></tr>
<tr><td colspan="2"></td><td>2</td><td>Se muestra en todo el panel, el mapa de monitoreo. En el mapa estaría cargando todas las alertas y alarmas registradas durante la sesión del teleoperador. También el mapa debería proveer herramientas útiles para su navegación.</td></tr>
<tr><td colspan="2"></td><td>3</td><td>Cuando aparece una alerta, se mostrará como un marcador pintado en el mapa, cuyo color se identifica según su estado actual.</td></tr>
<tr><td>4</td><td>El teleoperador da clic sobre la alerta emergente.</td><td></td><td></td></tr>
<tr><td colspan="2"></td><td>5</td><td>Sobre la alerta, debe aparecer la siguiente información ordenadamente estructurada en su pop-up:
- Nombre de vecino
- DNI del vecino
- Estado (Pendiente o Asignado)
- Prioridad (Común o Emergencia)
- Teleoperador (Solo si alguien está asignado)
- Dirección
- Latitud
- Longitud
- Fecha de creación
También dentro del pop-up, se muestra un botón para inspeccionar la alerta a detalle.</td></tr>
<tr><td colspan="4">Resultado</td></tr>
<tr><td>6</td><td colspan="3">Se visualiza las alertas que emergieron desde el websocket durante el proceso de monitoreo. El teleoperador tendrá el criterio de elegir una alerta pendiente durante su sesión.</td></tr>
<tr><td colspan="4">Excepciones</td></tr>
</table>

<table>
<tr><td></td><td colspan="4">● Manejar excepciones de conexión rechazada con el websocket.
● Cuando haya más de una alerta en una zona en específico, se debe agrupar las alertas para que visualmente sea más ordenado y fácil de analizar.</td></tr>
<tr><td rowspan="11">Flujo principal “visualizar alarmas en mapa de monitoreo”</td><td colspan="2">Actor</td><td colspan="2">Sistema</td></tr>
<tr><td>1</td><td>Da clic en la opción de “Monitorear Alertas”.</td><td></td><td></td></tr>
<tr><td colspan="2"></td><td>2</td><td>Se muestra en todo el panel, el mapa de monitoreo. En el mapa estaría cargando todas las alertas y alarmas registradas durante la sesión del teleoperador. También el mapa debería proveer herramientas útiles para su navegación.</td></tr>
<tr><td colspan="2"></td><td>3</td><td>Las alarmas se muestran como un marcador pintado en el mapa, cuyo color se identifica según su estado actual.</td></tr>
<tr><td>4</td><td>El teleoperador da clic sobre alguna alarma.</td><td></td><td></td></tr>
<tr><td colspan="2"></td><td>5</td><td>Sobre la alarma, debe aparecer la siguiente información ordenadamente estructurada en su pop-up:
- Código de alarma
- Estado
- Etiqueta
- Dirección
- Latitud
- Longitud</td></tr>
<tr><td colspan="4">Resultado</td></tr>
<tr><td>6</td><td colspan="3">Se visualizan las alarmas desplegadas en el mapa de monitoreo listas para cualquier eventualidad.</td></tr>
<tr><td colspan="4">Excepciones</td></tr>
<tr><td colspan="4">● El sonido solo se escuchará a través del módulo cuando se active una sirena de alguna alarma.</td></tr>
<tr><td rowspan="5">Flujo principal “visualizar activación de la alarma”</td><td colspan="2">Actor</td><td colspan="2">Sistema</td></tr>
<tr><td colspan="2"></td><td>1</td><td>Aparece una alerta de emergencia cerca del perímetro de la alarma.</td></tr>
<tr><td colspan="2"></td><td>2</td><td>Automáticamente la alarma detecta la cercanía de la alerta, activando su sirena durante un tiempo configurado.</td></tr>
<tr><td colspan="2"></td><td>3</td><td>Emite un sonido de alarma en el módulo como indicador del evento.</td></tr>
<tr><td>4</td><td>Visualiza la activación de la alarma en el mapa de monitoreo.</td><td></td><td></td></tr>
</table>

<table>
<tr><td rowspan="4"></td><td colspan="3">Resultado</td></tr>
<tr><td>5</td><td colspan="2">El teleoperador verifica cuál alerta de emergencia activó la sirena de la alarma, procediendo a su inmediata atención.</td></tr>
<tr><td colspan="3">Excepciones</td></tr>
<tr><td colspan="3">Ninguna.</td></tr>
<tr><td rowspan="10">Flujo principal “inspeccionar alerta”</td><td colspan="2">Actor</td><td>Sistema</td></tr>
<tr><td>1</td><td>Da clic sobre la alerta pendiente en el mapa.</td><td></td></tr>
<tr><td></td><td>2</td><td>Se muestra el pop-up con su información correspondiente a la alerta.</td></tr>
<tr><td>3</td><td>Si el teleoperador está decidido en atender la alerta, da clic en el botón “Inspeccionar Alerta”.</td><td></td></tr>
<tr><td></td><td>4</td><td>Abre un panel conteniendo la información en detalle de la alerta y del vecino, entre ellas son:
<u>Información de Alerta:</u>
- Dirección
- Latitud
- Longitud
- Estado de Alerta (Asignado o Pendiente)
- Prioridad (Común o Emergencia)
- Foto (En caso sea una alerta común)
- Fecha de creación
<u>Información de Atención:</u>
- Tipo de alerta
- Observación
- Estado de atención
- Teleoperador asignado
<u>Información de Vecino:</u>
- Nombre del vecino
- DNI
- Teléfono #1
- Teléfono #2
- Sexo
Edad</td></tr>
<tr><td colspan="3">Resultado</td></tr>
<tr><td>5</td><td colspan="2">El teleoperador tendría la información detallada sobre la alerta inspeccionada.</td></tr>
<tr><td colspan="3">Excepciones</td></tr>
</table>

	● Cuando el teleoperador comienza a inspeccionar la alerta, automáticamente se le asigna con un estado “Asignado”. ● Adicionalmente, el estado de la atención comenzará como “Verificado”, puesto que el teleoperador empezó a inspeccionar la alerta y debe proceder a terminarlo o ceder a otro teleoperador. ● En caso de que el teleoperador no sea capaz de atender la alerta una vez inspeccionado, puede ceder el turno a otro teleoperador disponible.
Relación con otros casos de uso	Ninguna.
Prototipos	

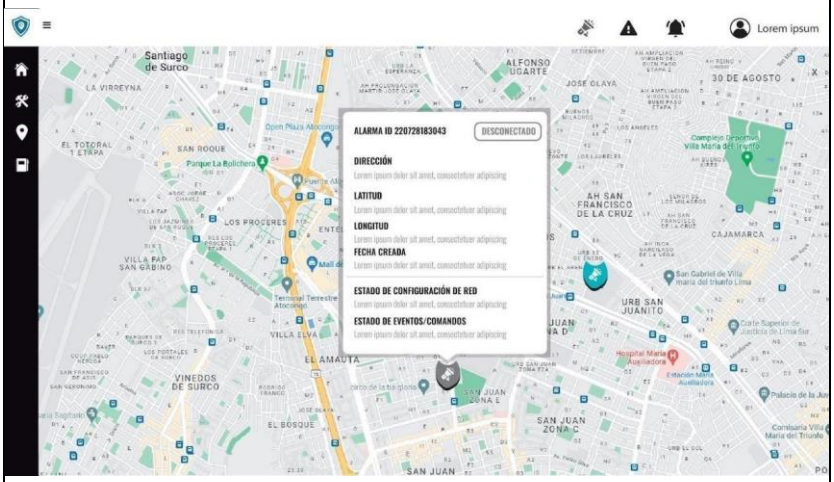


Figura 18. Prototipo del CUS Atender Alertas donde se muestra la información resumida de la alarma.
Fuente: Elaboración Propia.

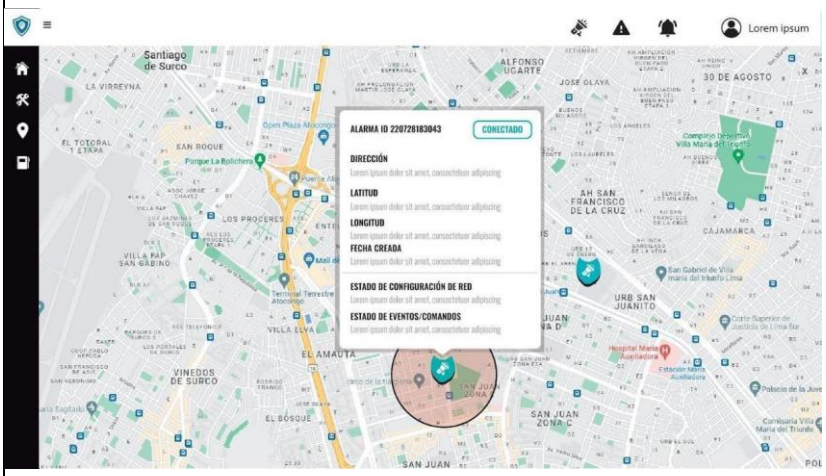


Figura 19. Prototipo del CUS Atender Alertas donde se muestra la alarma conectada.
Fuente: Elaboración Propia.

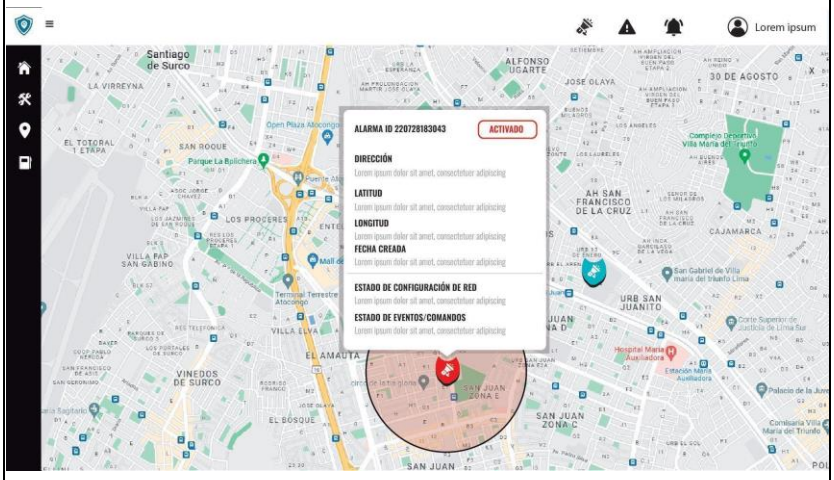


Figura 20. Prototipo del CUS Atender Alertas donde la alarma se encuentra en estado activado por sirena.
Fuente: Elaboración Propia.

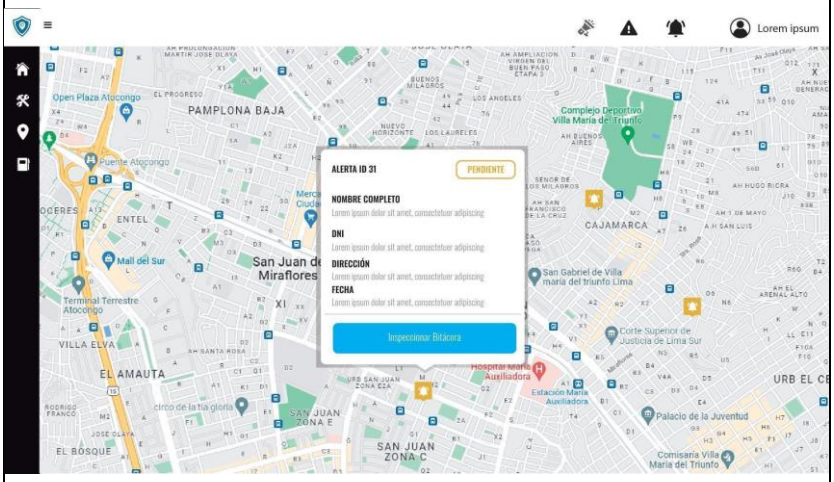


Figura 21. Prototipo del CUS Atender Alertas donde se muestra la información de la alerta común entrante.
Fuente: Elaboración Propia.

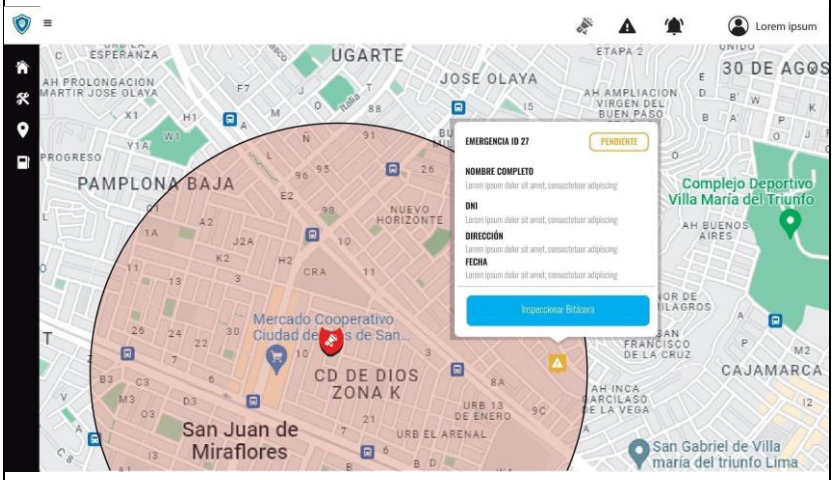


Figura 22. Prototipo del CUS Atender Alertas donde se muestra la información de alerta de emergencia entrante.
Fuente: Elaboración Propia.

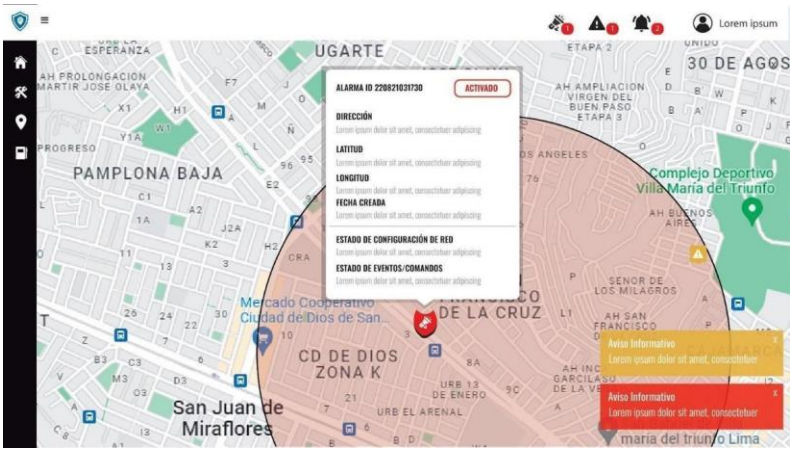


Figura 23. Prototipo del CUS Atender Alertas donde se activa la sirena de alarma cuando detecta una alerta de emergencia cercana.
Fuente: Elaboración Propia.

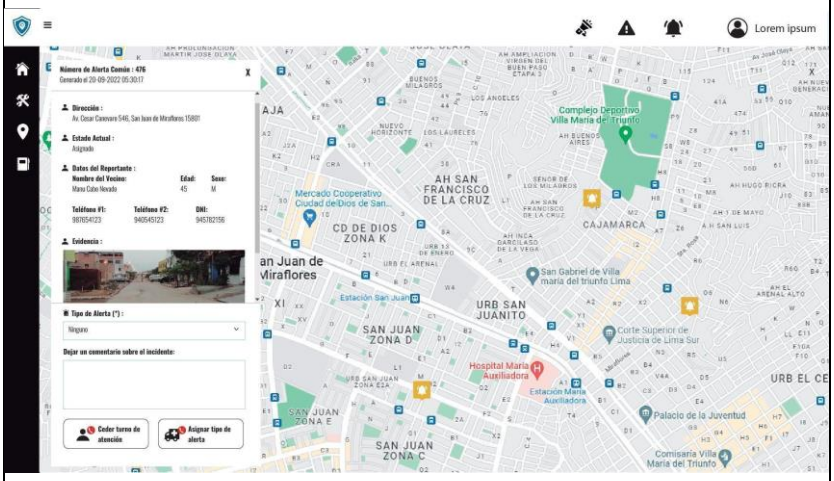


Figura 24. Prototipo del CUS Atender Alertas donde se muestra el detalle de la alerta cuando el teleoperador lo inspecciona, a su vez el teleoperador automáticamente se le asigna a esa alerta.
Fuente: Elaboración Propia.

Fuente: Elaboración Propia

ECUS6: Asignar Delito

Tabla 11. Tabla de Especificaciones del Caso de Uso en Asignar Delito

<table>
<tr><td>Términos</td><td colspan="4">Definición</td></tr>
<tr><td>Caso de uso</td><td colspan="4">Asignar delito</td></tr>
<tr><td>Descripción general</td><td colspan="4">Permite la asignación del delito una vez definido en el cierre de la atención de la alerta por el teleoperador.</td></tr>
<tr><td>Requerimiento funcional</td><td colspan="4">Rf9: Asignar el Delito</td></tr>
<tr><td>Precondición</td><td colspan="4">● Debe haber iniciado sesión en el sistema web.
● Tener conexión abierta para el websocket.
● La asignación comienza después de la correspondiente inspección.</td></tr>
<tr><td>Criterios de aceptación</td><td colspan="4">● Asigna el delito que corresponde.</td></tr>
<tr><td>Actores</td><td colspan="4">Teleoperador</td></tr>
<tr><td rowspan="11">Flujo principal “asignar tipo de alerta”</td><td colspan="2">Actor</td><td colspan="2">Sistema</td></tr>
<tr><td>1</td><td>El teleoperador abre el panel del detalle de la alerta.</td><td></td><td></td></tr>
<tr><td></td><td></td><td>2</td><td>Además de la información en detalle de la alerta, vecino y la atención, también se muestra un botón llamado “Cerrar Atención” en la parte inferior.</td></tr>
<tr><td>3</td><td>Da clic en el botón “Cerrar Atención”.</td><td></td><td></td></tr>
<tr><td></td><td></td><td>4</td><td>Se abre un pop-up con un formulario acerca de la definición del delito, los campos son los siguientes:
- Delito
- Observación</td></tr>
<tr><td>5</td><td>Rellena el formulario indicando el delito.</td><td></td><td></td></tr>
<tr><td></td><td></td><td>6</td><td>Aparece un mensaje de registro exitoso.</td></tr>
<tr><td colspan="4">Resultado</td></tr>
<tr><td>7</td><td colspan="3">Se registra correctamente el delito.</td></tr>
<tr><td colspan="4">Excepciones</td></tr>
<tr><td colspan="4">● El campo de “delito” es obligatorio y el de “observación” es opcional.
● Una vez que se defina el delito, el estado de atención de la alerta se cambia a “Atendido”.
● A su vez, como se considera el cierre de la alerta, deja de aparecer en el mapa de monitoreo.</td></tr>
<tr><td>Relación con otros casos de uso</td><td colspan="4">Cus6 - Atender Alertas</td></tr>
<tr><td rowspan="2">Flujo secundario “ceder el turno de atención”</td><td colspan="2">Actor</td><td colspan="2">Sistema</td></tr>
<tr><td></td><td></td><td>1</td><td>En el detalle de la alerta, se podrá visualizar un botón</td></tr>
</table>

				“Salir” en una esquina del panel.
	2	En caso que el teleoperador necesite ceder la atención de una alerta, da clic en el botón “Salir”.		
			3	Muestra un mensaje de advertencia indicando si realmente desea salir de la atención de la alerta.
	4	Da clic en el botón “Continuar” del pop-up.		
	Resultado			
	5	La alerta cambiaría al estado “pendiente”, en espera de la atención por parte de algún otro teleoperador disponible.		
	Excepciones			
	Ninguna.			
Prototipos				

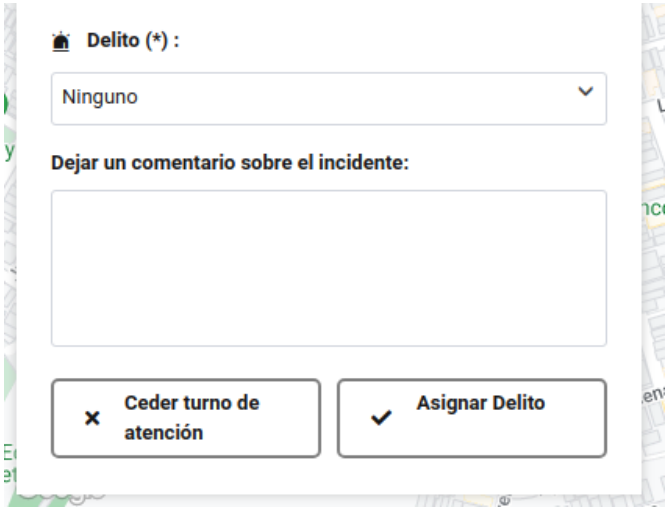


Figura 25. Prototipo del CUS Asignar Delito en donde el teleoperador define el delito correspondiente a la alerta inspeccionada.
Fuente: Elaboración Propia.

Fuente: Elaboración Propia

ECUS10: Generar Reporte de Alertas

Tabla 12. Tabla de Especificaciones del Caso de Uso en Generar Reporte de Alerta

<table>
<tr><td>Términos</td><td colspan="4">Definición</td></tr>
<tr><td>Caso de uso</td><td colspan="4">Generar Reporte de Alertas</td></tr>
<tr><td>Descripción general</td><td colspan="4">Permite visualizar y generar reportes en detalle con respecto a las alertas según el rango de fechas que se filtre.</td></tr>
<tr><td>Requerimiento funcional</td><td colspan="4">Rf13: Generar reportes de alertas</td></tr>
<tr><td>Precondición</td><td colspan="4">● Debe haber iniciado sesión en el sistema web.</td></tr>
<tr><td>Criterios de aceptación</td><td colspan="4">● Visualizar el reporte generado sobre las alertas.
● Exportar el reporte generado.</td></tr>
<tr><td>Actores</td><td colspan="4">Administrador</td></tr>
<tr><td rowspan="4">Flujo principal “visualizar reporte generado”</td><td colspan="2">Actor</td><td colspan="2">Sistema</td></tr>
<tr><td>1</td><td>Da clic en la opción de “Consultar Alertas”.</td><td></td><td></td></tr>
<tr><td colspan="2"></td><td>2</td><td>Se muestra un formulario en el lado superior indicando:
- Fecha Inicio
- Fecha Fin
Y un botón llamado “Filtrar”.
Por otro lado, como contenido tenemos una grilla donde se muestra la siguiente información:
<u>Por alerta común:</u>
- Nombre del Vecino
- DNI
- Dirección
- Observación
- Tipo de Alerta
Se enlista un registro o más en las siguientes columnas:
- Teleoperador que atendió la alerta
<u>Por alertas de emergencia:</u>
- Nombre del Vecino
- DNI
- Dirección
- Observación
- Tipo de Alerta
Se enlista un registro o más en las siguientes columnas:
- Teleoperador que atendió la alerta
- Alarma relacionada</td></tr>
<tr><td>3</td><td>Según el criterio del administrador, filtra las fechas rellenando los campos de fecha.</td><td></td><td></td></tr>
</table>

<table>
<tr><td rowspan="5"></td><td></td><td></td><td>4</td><td>Se actualiza la información de la grilla con las fechas filtradas. También se muestra gráficos estadísticos acerca de:
- Según la prioridad de la alerta.
- Según la asignación sobre la alerta.
- Según la atención de la alerta.
- Según el tipo de alerta.</td></tr>
<tr><td colspan="4">Resultado</td></tr>
<tr><td>5</td><td colspan="3">Se generó el reporte de alertas según lo filtrado.</td></tr>
<tr><td colspan="4">Excepciones</td></tr>
<tr><td colspan="4">● Se requiere que las fechas filtradas sean por cada mes y tengan coherencia en el rango de fechas; en caso contrario, se mostrará un mensaje de validación.</td></tr>
<tr><td rowspan="10">Flujo secundario “exportar reporte”</td><td colspan="2">Actor</td><td colspan="2">Sistema</td></tr>
<tr><td>1</td><td>Según el criterio del administrador, filtra las fechas rellenando los campos de fecha.</td><td colspan="2"></td></tr>
<tr><td colspan="2"></td><td>2</td><td>Se actualiza la información de la grilla con las fechas filtradas. También se muestra gráficos estadísticos acerca de:
- Según la prioridad de la alerta.
- Según la asignación sobre la alerta.
- Según la atención de la alerta.
- Según el tipo de alerta.</td></tr>
<tr><td>3</td><td>Da clic en el botón “Exportar”.</td><td colspan="2"></td></tr>
<tr><td colspan="2"></td><td>4</td><td>Abre un pop-up indicando que tipo de archivo desea exportar el reporte generado.</td></tr>
<tr><td>5</td><td>Selecciona el tipo de archivo que desea exportar.</td><td colspan="2"></td></tr>
<tr><td colspan="4">Resultado</td></tr>
<tr><td>6</td><td colspan="3">Descarga el reporte generado según el tipo de archivo seleccionado.</td></tr>
<tr><td colspan="4">Excepciones</td></tr>
<tr><td colspan="4">● Se requiere que las fechas filtradas sean por cada mes y tengan coherencia en el rango de fechas; en caso contrario, se mostrará un mensaje de validación.
● No se puede exportar si el reporte no está generado.</td></tr>
<tr><td>Relación con otros casos de uso</td><td colspan="4">Ninguna.</td></tr>
<tr><td colspan="5">Prototipos</td></tr>
</table>

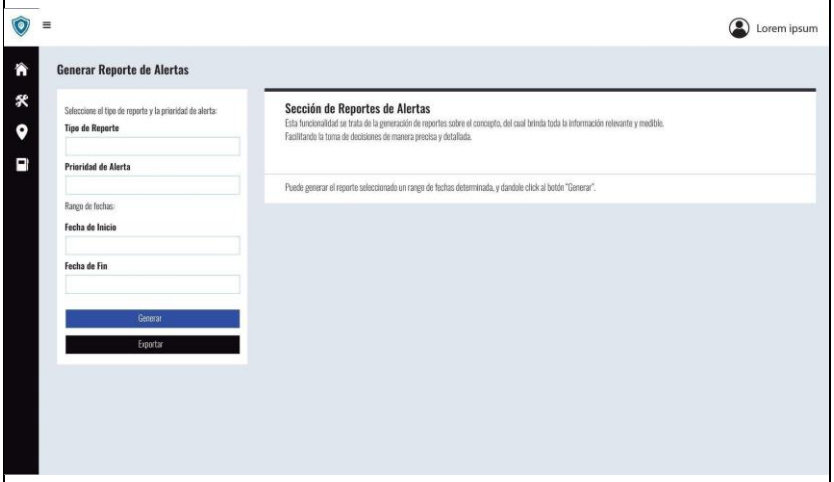


Figura 26. Prototipo del CUS Generar Reporte de Alertas donde podrá filtrar según el tipo de reporte, la prioridad de alerta y un rango de fechas.
Fuente: Elaboración Propia.

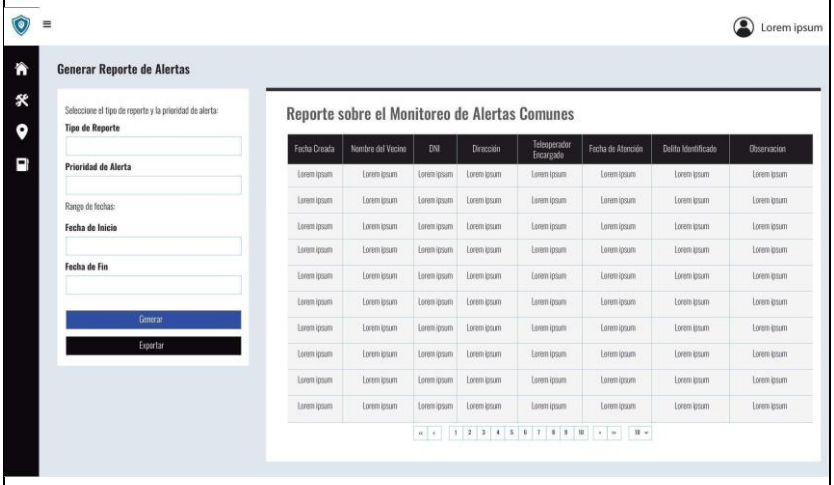


Figura 27. Prototipo del CUS Generar Reporte de Alertas donde se muestra el reporte generado acerca del monitoreo.
Fuente: Elaboración Propia.

Figura 28. Prototipo del CUS Generar Reporte de Alertas donde se muestra el reporte generado acerca de asignación sobre las alertas.
Fuente: Elaboración Propia.

Figura 29. Prototipo del CUS Generar Reporte de Alertas donde se muestra el reporte generado acerca de la atención de la alerta.
Fuente: Elaboración Propia.

Figura 30. Prototipo del CUS Generar Reporte de Alertas donde se muestra el reporte generado acerca de la identificación de delitos.
Fuente: Elaboración Propia.

Fuente: Elaboración Propia

5.2.10. Diagrama de Clase de Análisis

Para el caso de uso “Cargar Alertas”, se está utilizando la información de las alertas y del vecino para el procesamiento de las alertas cargadas.

Además de eso, se tiene como clases no persistentes, la habilitación de canales y del “*healthcheck*”, cuyo propósito es facilitar el mantenimiento del *websocket* ante cualquier eventualidad y del envío de información mediante canales (Ver Figura 31).

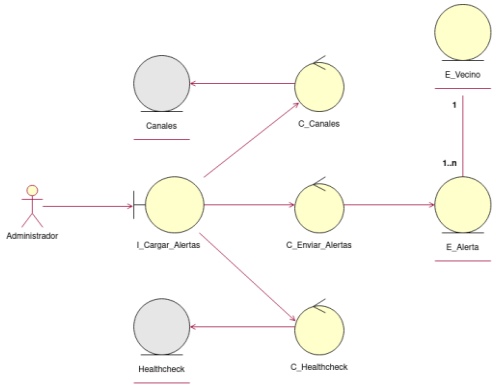


Figura 31. Diagrama de clase de análisis al cargar alertas
Fuente: Elaboración Propia.

Para el caso de uso “Atender Alertas” (Ver Figura 32), al contemplar los flujos descritos en la especificación, se desarrolla entre las siguientes funcionalidades:

a) Activación de Sirena: Se realiza el evento de sirena por parte de la alarma y de la cercanía de una o muchas alertas.
b) Inspeccionar Alerta: Se realiza con la atención entre la alerta y el usuario teleoperador.
c) Visualizar las alertas y alarmas: En conjunto, se verá reflejado las alertas y alarmas interactuando durante el monitoreo.
d) Comunicación de los canales: Se contempla además la comunicación abierta con el *websocket*.

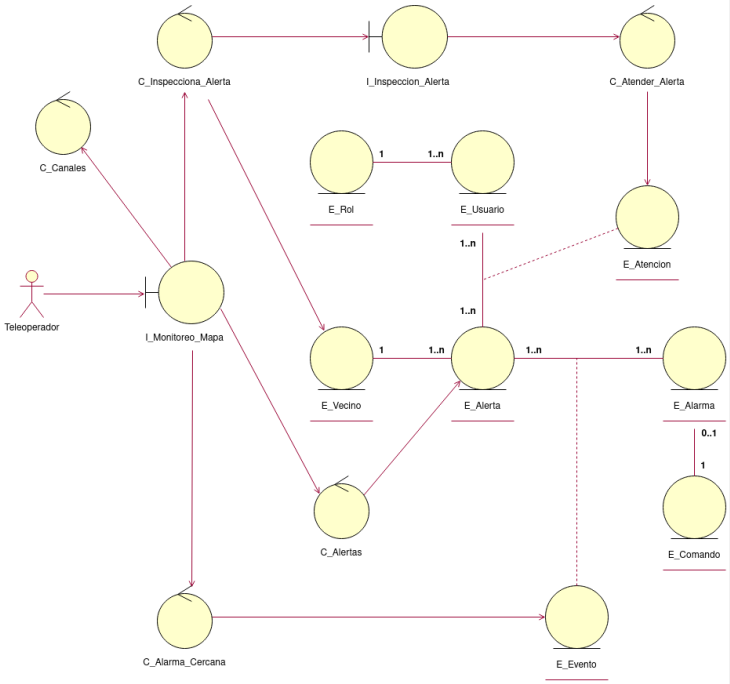


Figura 32. Diagrama de clase de análisis del CUS Atender Alertas
Fuente: Elaboración Propia.

Para el caso de uso “Asignar Tipo de Alerta” (Ver Figura 33), se desarrolla a partir de la persistencia entre la alerta y la definición del tipo de alerta al cual pertenecería.

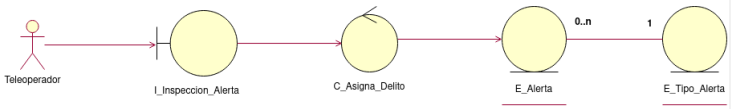


Figura 33. Diagrama de clase de análisis al asignar delito
Fuente: Elaboración Propia.

Para el caso de uso "Generar Reporte de Alerta" (Ver Figura 34), se utiliza la información de la alerta y del vecino para los reportes generados; además generar los estadísticos útiles en cuanto a valores medibles sobre la atención de la alerta.

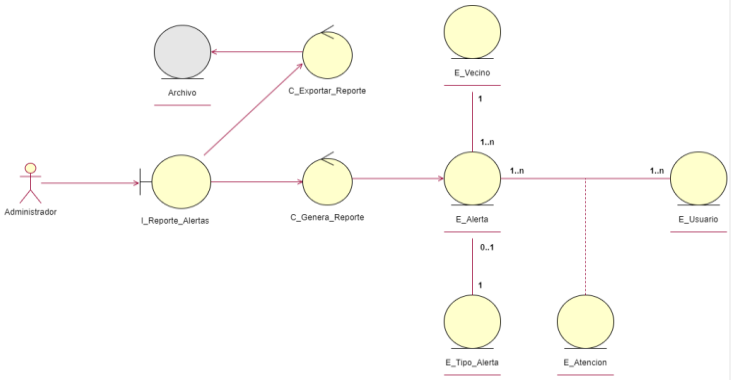


Figura 34. Diagrama de clase de análisis al generar reportes de alerta
Fuente: Elaboración Propia.

5.2.11. Modelo Conceptual

Las entidades que analizamos en las clases de análisis, al integrarlas, obtendremos como resultado el modelo conceptual (Ver Figura 35).

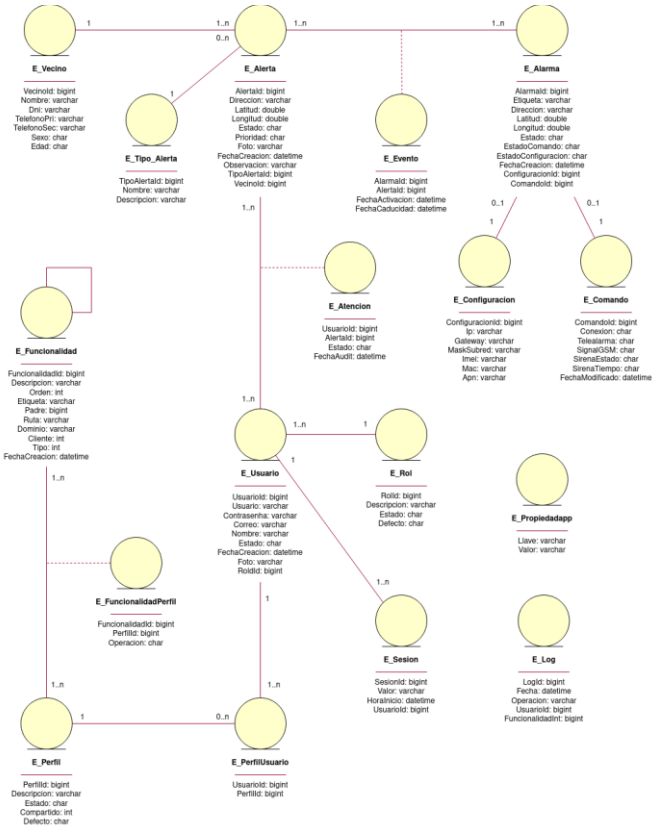


Figura 35. Gráfico del modelo conceptual capturado desde el análisis del sistema
Fuente: Elaboración Propia.

5.2.12. Diagrama de Estados

Para el caso de uso “Cargar Alertas” (Ver Figura 36), se requiere cumplir la siguiente condición:

Al conectar una alarma configurada, comenzará con el estado de sirena en “Desactivado”, preparándose para cualquier eventualidad cercana a su señal GSM (*Global System for Mobile communication*) para poder activarse su sirena. En caso que haya una alerta de emergencia cercana a su ubicación, se cambia de estado a “Activado” durante un tiempo programado.

Cuando se acaba el tiempo de sirena, automáticamente la sirena de la alarma se desactiva, cambiando de estado a “Desactivado”.

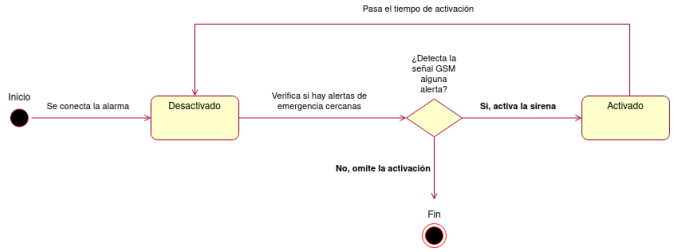


Figura 36. Diagrama de estado al cargar alertas
Fuente: Elaboración Propia.

Para el caso de uso “Atender Alertas” (Ver Figura 37), se requiere cumplir la siguiente condición:

Cuando aparece una nueva alerta, el estado de la alerta inicial será como “Pendiente”, y seguirá manteniéndose con este estado hasta ser atendido por algún teleoperador disponible. Otra condición relacionada a la calidad de atención de un teleoperador, es que se verifique si la alerta está siendo atendida por otro teleoperador; si no lo está, entonces procede a inspeccionar la alerta y cambia de estado a “Asignado”, de lo contrario, entonces procede a buscar otra alerta pendiente.

También se contempla el hecho de que, si el teleoperador tenga dificultades en la recepción de atención sobre una alerta durante el proceso de atención, tiene la opción de poder ceder la atención a otro teleoperador disponible; de ser así, cambiaría a estado “Pendiente”.

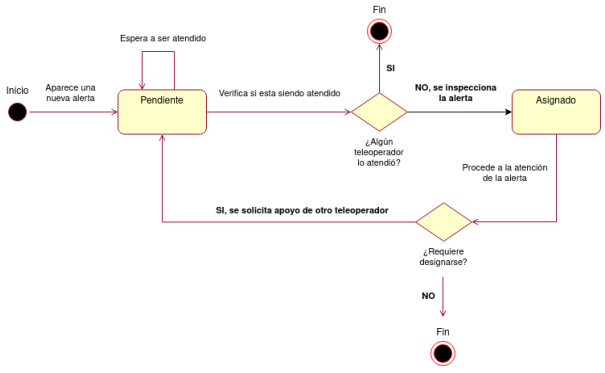


Figura 37. Diagrama de estado al atender alertas
Fuente: Elaboración Propia.

Para el caso de uso “Asignar Delito” (Ver Figura 38), se requiere cumplir la siguiente condición:

Cuando la alerta ha sido inspeccionada por algún teleoperador, contará como estado “Verificado”; ayudando en cierta forma en saber desde qué punto en el tiempo se llegó a verificar la alerta. Después el teleoperador, a criterio personal, deberá proceder a su respectiva atención al vecino quien reportó la alerta; en donde cabe mencionar que este proceso solo fluctuaría en la vida real y no se refleja en el sistema.

Una vez que culminó con la investigación sobre la alerta, se define el delito al cual pertenece y cambiando de estado de la atención a “Atendido”.

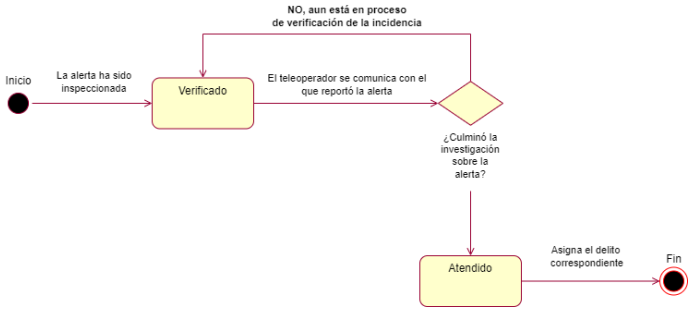


Figura 38. Diagrama de estado al asignar delito
Fuente: Elaboración Propia.

5.3. Arquitectura

5.3.1. Diagrama de Despliegue

Sobre el despliegue del sistema, es de suma importancia el levantamiento de ciertos componentes de software como el Docker para el despliegue del *websocket*; así mismo, exponer los puertos correspondientes para cada nodo que se requiera, incluyendo al del servidor web (Ver Figura 39).
Entre los nodos, tenemos los siguientes:

Client Side

Es el ordenador del usuario donde navegará al sistema web o al *websocket*, aunque para su demostración, se realizará de manera local para no asumir gastos de dominios.

Docker Containers

En los contenedores, se levantará la instancia del *websocket* con una conexión abierta para cualquier petición TCP (*Transmission Control Protocol*) que se solicite, y además se usará el *Node* con su versión respectiva para la inicialización del proyecto y su *build* de todas las librerías NPM (*Node Package Manager*) que se necesite.

FirvealWS

Es el servidor web del cual se refiere a todo proceso perteneciente al monitoreo de alertas y a su vez se considera el nodo principal para la realización de nuestra variable independiente.

GitHub Repository

Se publica en un repositorio GitHub, los cambios de todos los proyectos incluyentes a la solución, y se trabaja de manera paralela para que ordenadamente se realice un *workflow* adecuado.

Google API Services

Se utilizan para el almacenamiento de las imágenes o fotos que son subidas a través de distintas fuentes de información.

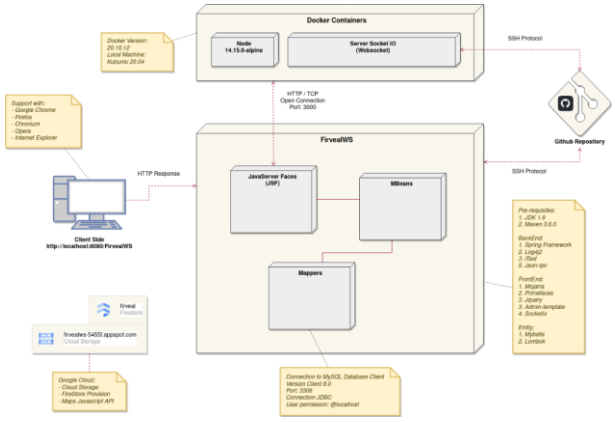


Figura 39. Diagrama de Despliegue sobre la arquitectura del proyecto
Fuente: Elaboración Propia.

5.3.2. Diagrama de Componentes

Se muestran los siguientes diagramas de componentes que se utilizarán en el desarrollo de código para la solución.

FirvealWS

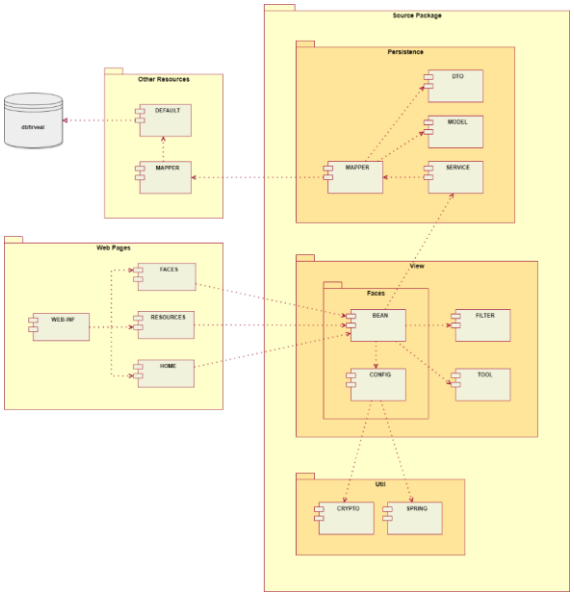


Figura 40. Diagrama de componentes sobre el FirvealWS
Fuente: Elaboración Propia.

Server Socket IO

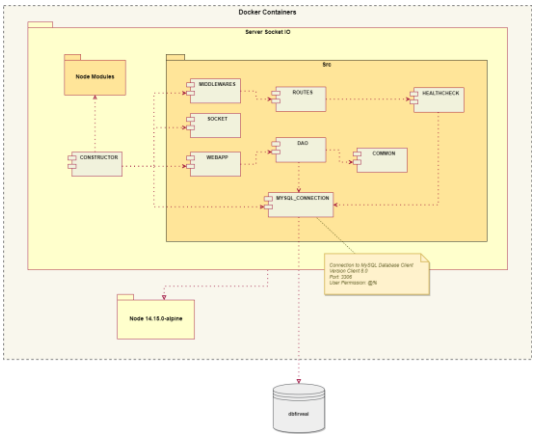


Figura 41. Diagrama de componentes sobre el Server Socket IO
Fuente: Elaboración Propia.

5.3.3. Vista Lógica

Para la aplicación web, se está utilizando la arquitectura JMX que sostiene los siguientes alineamientos:

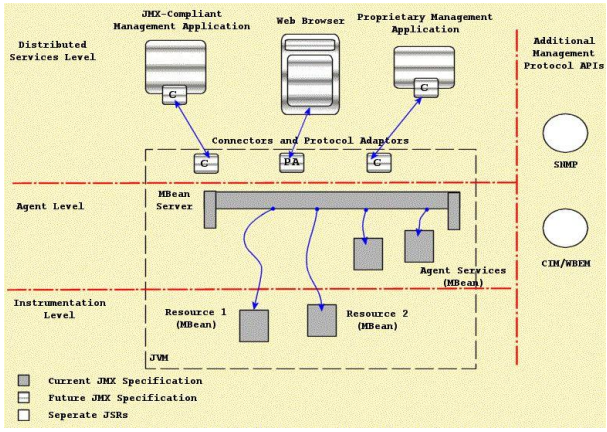


Figura 42. Vista Lógica de la Aplicación Web basado en arquitectura JMX
Fuente: Chapter 2. The Jboss JMX Microkernel. Docjobs, (2022).

Por el lado del websocket, nos estamos basando en la arquitectura del socket.io para la intercomunicación de los teleoperadores durante el monitoreo de alertas. Teniendo como hincapié mantener la conexión abierta para cualquier pase de información disponible.

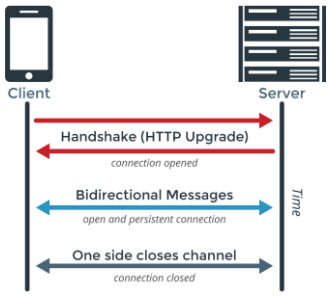


Figura 43. Vista Lógica de la Arquitectura Socket IO
Fuente: Abdulkerim Karaman, Medium, (2019).

5.4. Modelamiento de Clases de Diseño

5.4.1. Modelo Físico

A partir del modelo conceptual, se constituye en detalle al modelo físico, en donde se contribuirá el almacenamiento de la información del sistema.

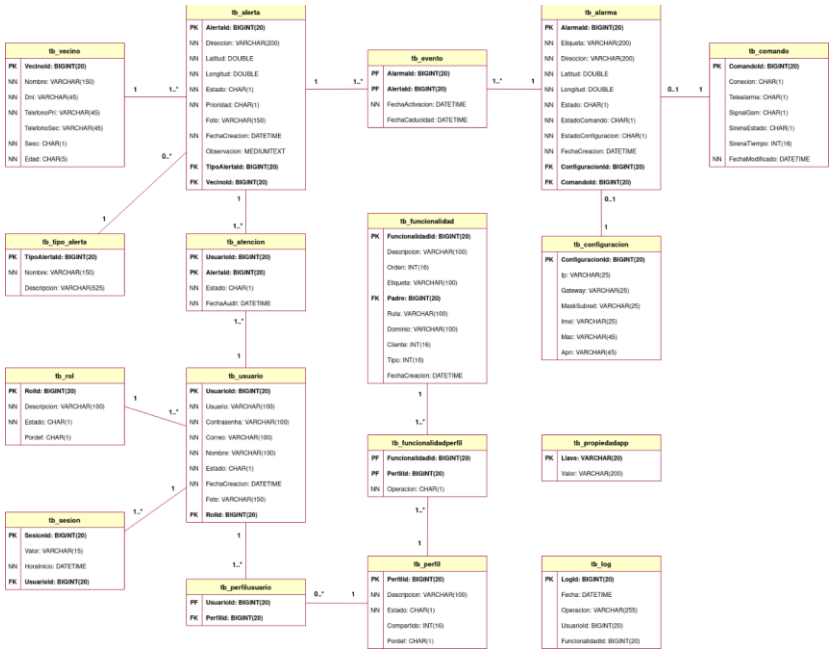


Figura 44. Modelo físico a partir del modelo conceptual diseñado
Fuente: Elaboración Propia.

5.4.2. Diagrama de Clases de Diseño

Se presentan los diagramas de diseño que describen detalladamente las clases representadas durante el desarrollo del software, indicando que objetos y métodos se estarán utilizando.

CUS Cargar Alertas

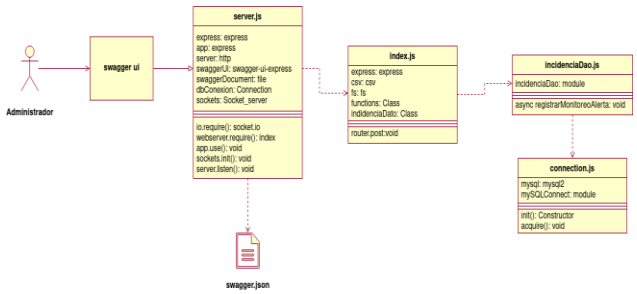


Figura 45. Diagrama de Clase de Diseño del CUS Cargar Alertas acerca del desarrollo de envío de alertas mediante los canales.
Fuente: Elaboración Propia

CUS Atender Alertas

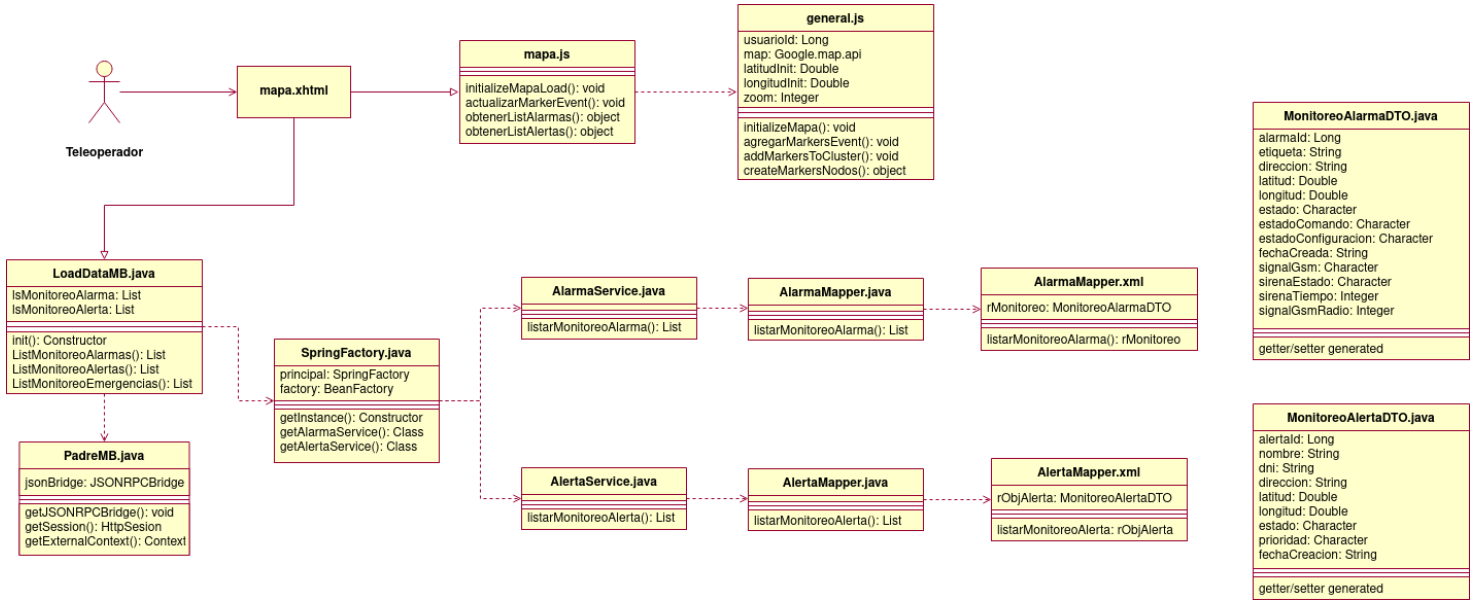


Figura 46. Diagrama de Clase de Diseño del CUS Atender Alertas acerca del despliegue de objetos alertas y alarmas en el mapa de monitoreo.
Fuente: Elaboración Propia

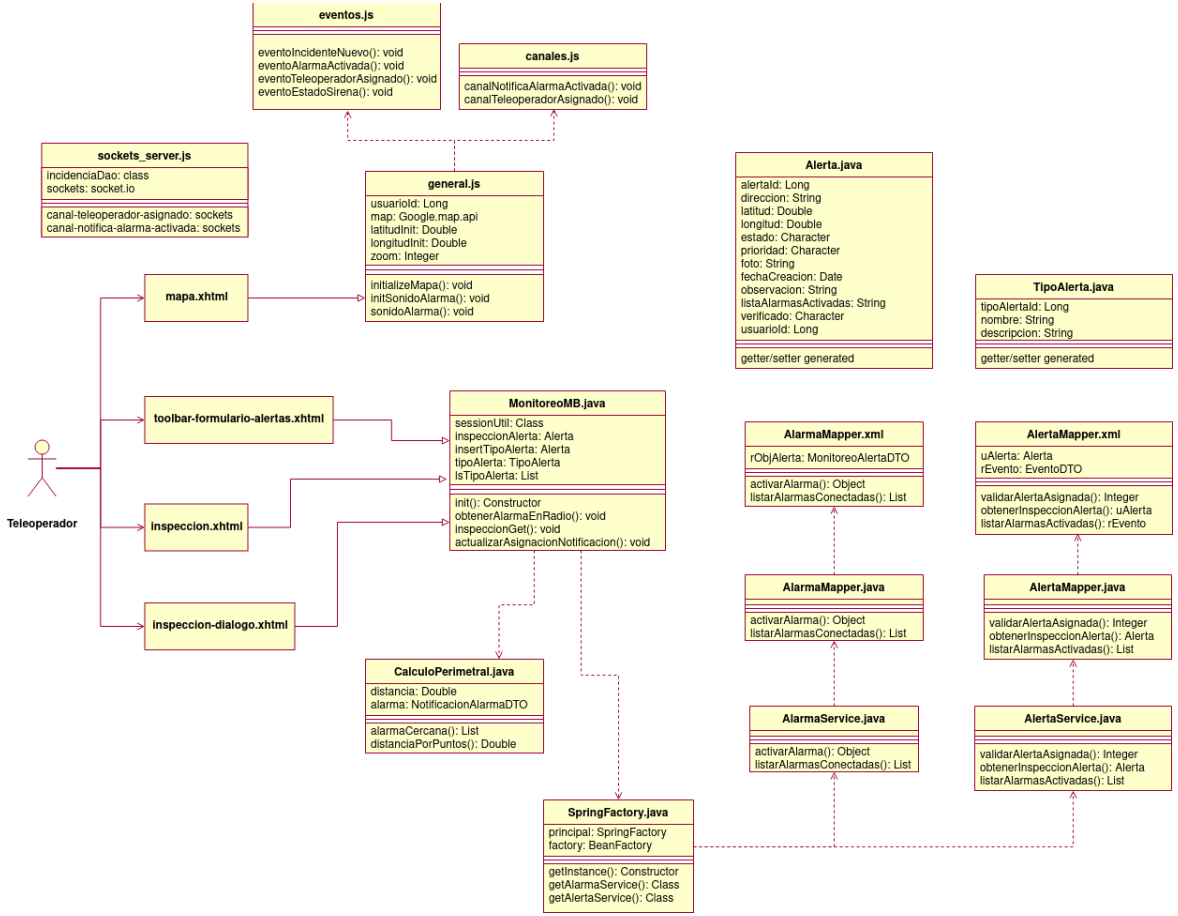


Figura 47. Diagrama de Clase de Diseño del CUS Atender Alertas acerca de todo el proceso de monitoreo de alertas antes de la atención de la alerta. Fuente: Elaboración Propia.

CUS Asignar Delito

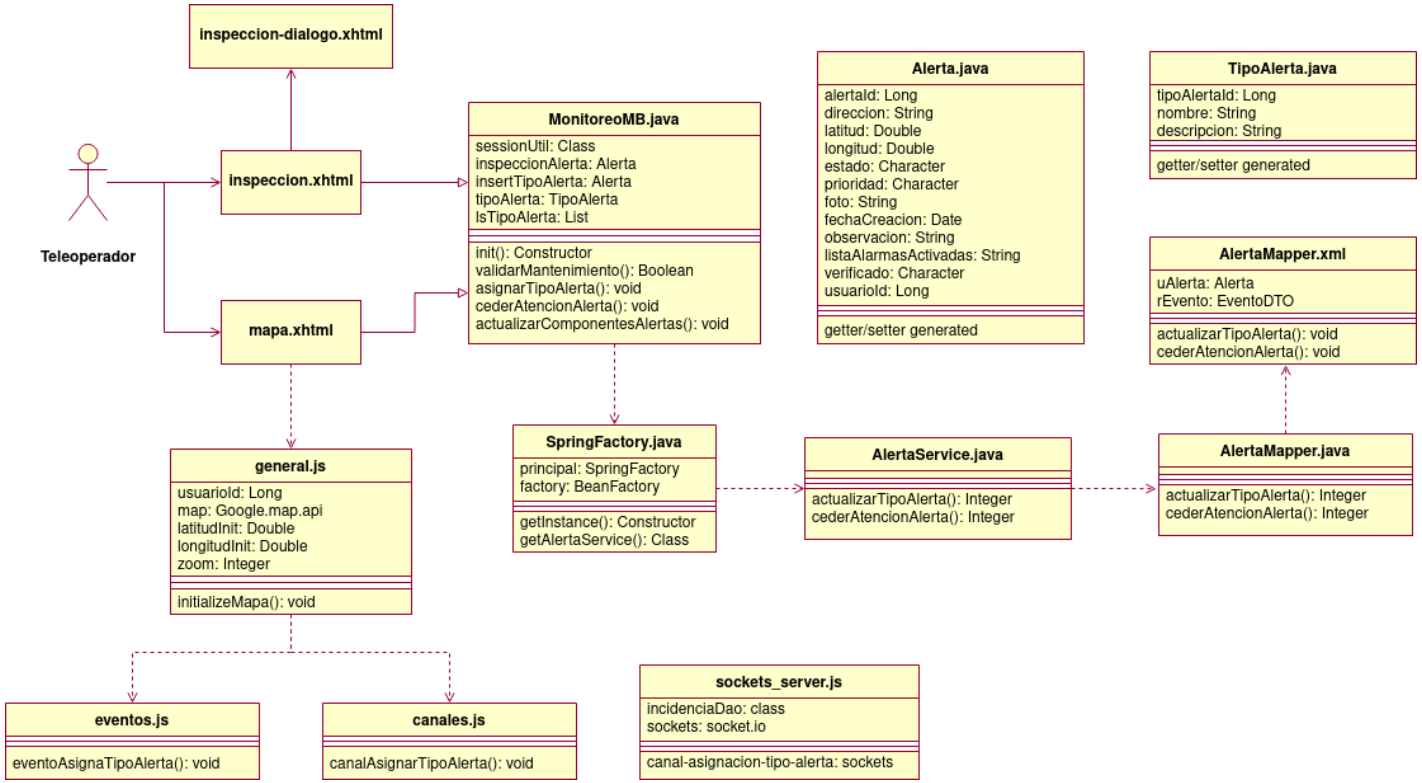


Figura 48. Diagrama de Clase de Diseño del CUS Asignar Delito con respecto a la actualización del estado de alerta a “Atendido” y ceder la atención de la alerta.
Fuente: Elaboración Propia.

CUS Generar Reporte de Alerta

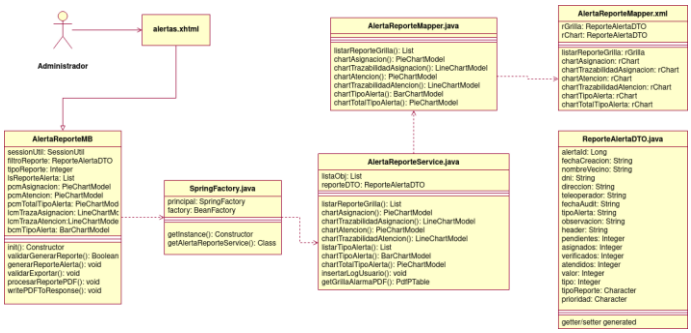


Figura 49. Diagrama de Clase de Diseño del CUS Generar Reporte de Alerta.
Fuente: Elaboración Propia.

5.4.3. Diagrama de Secuencia de Diseño

Se presentan los diagramas de secuencia que dan soporte al desarrollo de código, describiendo de manera detallada la secuencia de la implementación a realizar.

CUS Cargar Alertas

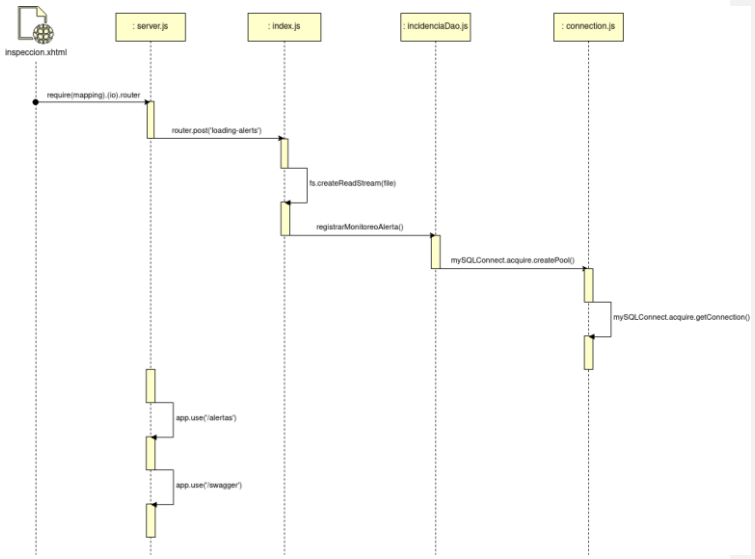


Figura 50. Diagrama de Secuencia de Diseño del CUS Cargar Alertas.
Fuente: Elaboración Propia.

CUS Atender Alertas

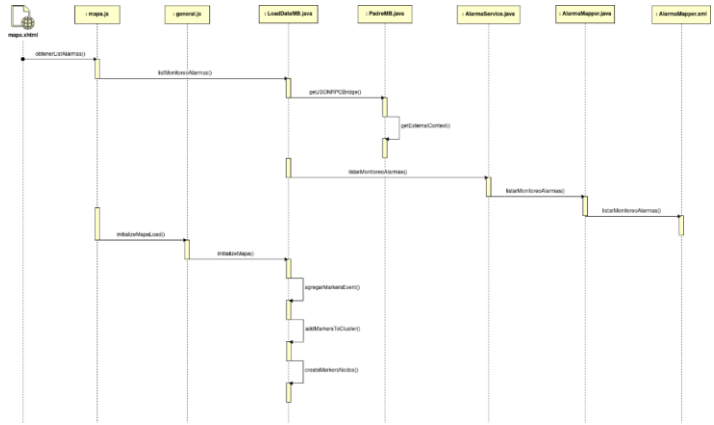


Figura 51. Diagrama de Secuencia de Diseño del CUS Atender Alertas con respecto al despliegue de alarmas en el mapa de monitoreo.
Fuente: Elaboración Propia.

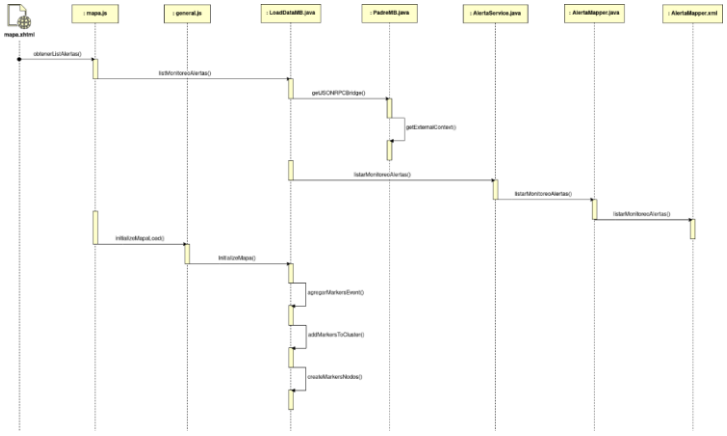


Figura 52. Diagrama de Secuencia de Diseño del CUS Atender Alertas con respecto al despliegue de alertas en el mapa de monitoreo.
Fuente: Elaboración Propia.

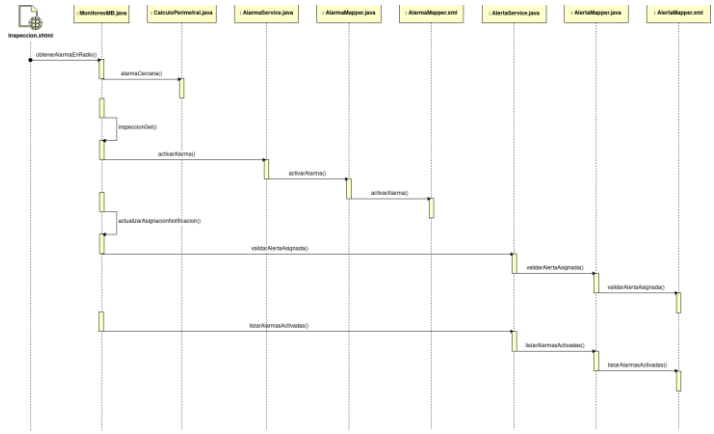


Figura 53. Diagrama de Secuencia de Diseño del CUS Atender Alertas con respecto a la activación de sirena de alarma.
Fuente: Elaboración Propia.

Figura 54. Diagrama de Secuencia de Diseño del CUS Atender Alertas acerca del intercambio de información con el websocket para la asignación del teleoperador.
Fuente: Elaboración Propia.

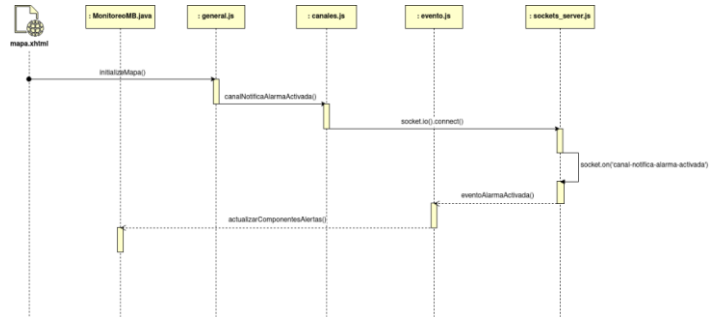


Figura 55. Diagrama de Secuencia de Diseño del CUS Atender Alertas acerca del intercambio de información con el websocket para la activación de sirena.
Fuente: Elaboración Propia.

CUS Asignar Delito

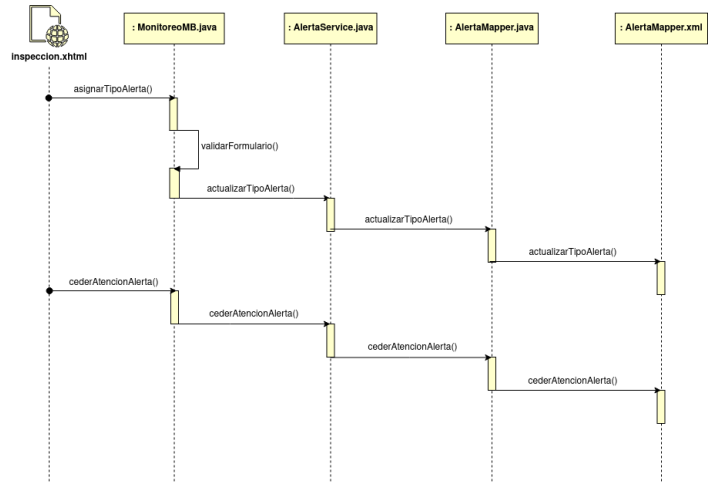


Figura 56. Diagrama de Secuencia de Diseño del CUS Asignar Delito con respecto a la asignación del delito correspondiente y el flujo de ceder la atención de la alerta.
Fuente: Elaboración Propia.

Figura 57. Diagrama de Secuencia de Diseño del CUS Asignar Delito acerca del intercambio de información con el websocket para la atención de la alerta.
Fuente: Elaboración Propia.

CUS Generar Reporte Alertas

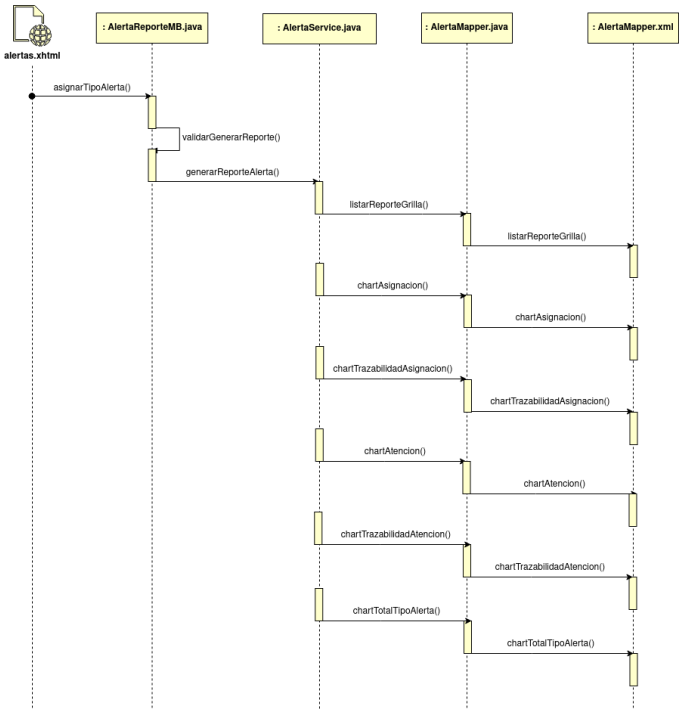


Figura 58. Diagrama de Secuencia de Diseño del CUS Generar Reporte de Alerta acerca de la consulta de reportes.
Fuente: Elaboración Propia.

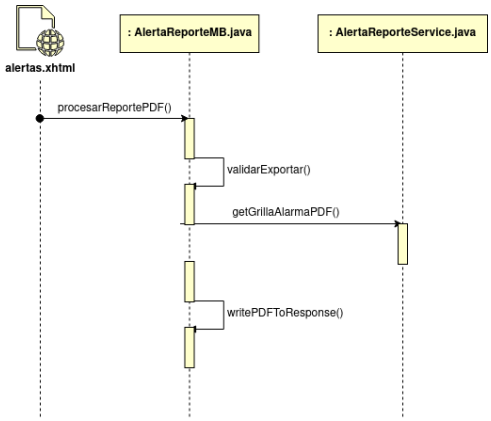


Figura 59. Diagrama de Secuencia de Diseño del CUS Generar Reporte de Alerta acerca de la exportación de reportes.
Fuente: Elaboración Propia.

5.5. Pruebas

5.5.1. Plan de Pruebas

a) Introducción

La finalidad del presente plan de pruebas es detallar y documentar la planificación de las pruebas del sistema web y comprobar el correcto funcionamiento de este.

b) Alcance

El alcance es definido a base de la realización de los casos de usos priorizados, cuyos objetivos se deben efectuar al respectivo flujo de la solución.

c) Referencias

Para el presente documento, se estará efectuando diversos tipos de pruebas para verificar la validez del sistema y de sus funcionalidades, tomando en cuenta los requerimientos solicitados por el cliente.

d) Requerimiento de pruebas.

A continuación, se detallan los requerimientos que fueron probados:

1) Pruebas funcionales.

La siguiente lista de requerimientos fue probada:

- Cargar alertas.
- Generar reporte de alertas.
- Asignar tipo de alerta.
- Atender alertas.

2) Pruebas de seguridad.

Sobre estas pruebas, se ha realizado la autenticación de usuarios durante el manejo de sesiones que acontece durante todo el proceso de monitoreo de alertas. Las pruebas de cargas de usuarios incluso son importantes en esta solución, puesto que la intercomunicación de canales debe estar disponible en todo momento para las eventualidades que se realizan durante el monitoreo.

3) Pruebas de requisitos tecnológicos.

Para las pruebas de requisitos tecnológicos se revisó el funcionamiento del sistema en los siguientes navegadores:

- Google Chrome.
- Mozilla Firefox.
- Safari.

4) Pruebas de Estrés

Para estas pruebas, se debe realizar cúmulos de peticiones y ejecuciones durante el monitoreo de alertas, garantizando la disponibilidad de cada alerta entrante al sistema web de manera asíncrona.

A su vez, también se comprueba la creación de canales por cada usuario que intenta interactuar en el mapa de monitoreo, de ser así se unirá los canales de su respectiva actividad. Para saber las pruebas implicadas en la carga de alertas y del tráfico de red, ver más en Anexo 4 y 5.

e) Tipos de Pruebas.

A continuación, se listan los tipos de pruebas realizadas para la validación del funcionamiento del sistema web:

1) Pruebas unitarias.

Durante el desarrollo del sistema web, se procedió a depurar el código fuente, conforme se iba avanzando en su implementación e igualmente realizando el debug al sistema validando el correcto funcionamiento de la solución.

2) Pruebas de integración.

Fueron realizadas para comprobar la conexión con la base de datos y los componentes utilizados en el desarrollo del sistema web; además, se verificó la conexión entre los canales configurados del websocket y el sistema web.

3) Pruebas de aceptación.

Tras realizar el despliegue del sistema web, se realizaron las pruebas de aceptación en conjunto con las pruebas de integración,

donde se verifica el correcto funcionamiento del sistema web con todos los componentes desplegados.

4) Pruebas de caso de uso.

Culminadas las pruebas unitarias y de integración, se procedió con las pruebas de caso de uso, con las cuales se verificó el correcto funcionamiento e implementación de los flujos básicos y secundarios de los casos de usos desarrollados en el sistema web. Una vez culminada estas pruebas, se dio pase a las pruebas de aceptación.

5) Pruebas no funcionales.

Tras realizarse las pruebas de caso de uso, se realizaron las pruebas no funcionales, donde se determinó el buen comportamiento del sistema web en base a los requerimientos no funcionales anteriormente descritos.

f) Características principales del software:

A continuación, se detallan las características generales probadas:

- Monitoreo de Alertas en tiempo real.
- Intercomunicación de aplicaciones mediante canales.
- Asignación del Delito.
- Carga Masiva de Alertas.
- Generación de Reportes de Alertas.
- Exportación de Reportes.

g) Características secundarias del software:

- Notificaciones de Alertas Comunes.
- Notificaciones de Alertas de Emergencia.
- Notificaciones de Activación de Sirena.
- Mantenimiento de Alarmas.
- Ubicar la Posición de Alarma.
- Iniciar Sesión.
- Generación de Reportes de Alarmas.

- Ejecución de “Enviar Alertas”.

h) Responsabilidad de casos de pruebas.

El sistema fue aprobado por el gerente general de la empresa FIRINGS E.I.R.L una vez validado la demostración de las características que posee el sistema web.

i) Secuencia de pruebas.

Se aprovechó el modelo de pruebas elaborado propiamente en el desarrollo del sistema web, así como su implementación y despliegue.

5.6. Informes de Pruebas

5.6.1. Importancia del trabajo

La importancia de este trabajo es verificar el correcto funcionamiento del sistema web desarrollado que satisfaga los requerimientos previamente detallados y que el producto final sea del agrado del gerente general de la empresa FIRINGS E.I.R.L.

5.6.2. Propósito del trabajo

El propósito de este trabajo es verificar que el software cumpla con todos los requerimientos anteriormente detallados, capturando las incidencias o defectos detectados en el sistema web para su respectiva corrección.

5.6.3. Casos de pruebas.

a) CUS: Cargar alertas.

Tabla 13. Tabla de Casos de Pruebas del CUS Cargar Alertas

N° Caso	Descripción del Caso de Prueba/ Objetivo	Dato de Entrada	Acción	Resultado Esperado	Resultado Obtenido	Estado
01	Ejecutar el endpoint sin subir un archivo	Subir Archivo	Clic	Mostrar Mensaje de error “No ha seleccionado un archivo”	Muestra mensaje de error correspondiente	OK
02	Seleccionar más de un archivo y subirlos	Archivo	Clic	No debe permitir subir más de un archivo	Sólo permite subir a lo	OK

					mucho un archivo	
03	Dejar en blanco una columna requerida en el archivo CSV y luego subirlo y ejecutar el endpoint	Archivo	Clic	Mostrar mensaje de error “Debe rellenar correctamente todos los campos requeridos”	Muestra mensaje de error correspondiente	OK
04	Adjuntar un archivo CSV con diferentes columnas y ejecutar el endpoint	Archivo	Clic	Mostrar mensaje de advertencia que se guíen de la plantilla.	No permite adjuntar un archivo que no sea tipo CSV	OK
05	Ejecutar el endpoint con un archivo que no sea CSV	Archivo	Clic	Mostrar mensaje de error “Tipo de archivo incorrecto”	No permite ejecutar un archivo que no sea tipo CSV	OK
06	Cancela la ejecución del endpoint durante el proceso de envío de alertas	Archivo	Clic	No debe permitir la interrupción durante la ejecución	Se validó la ejecución continua tras una interrupción	OK
07	El healing del servidor se deteriora durante el envío de alertas	Alertas Enviadas	Ninguno	El sistema muestra un mensaje de error 503	Muestra mensaje de error correspondiente	OK
08	Se pierde la comunicación del websocket con el sistema web durante el envío de alertas	Alertas Enviadas	Ninguno	Indica mensajes de error acerca de la conectividad con el sistema web.	Muestra mensaje de error correspondiente	OK

Fuente: Elaboración Propia

b) CUS: Atender alertas.

Tabla 14. Tabla de Casos de Pruebas del CUS Atender Alertas

N° Caso	Descripción del Caso de Prueba/ Objetivo	Dato de Entrada	Acción	Resultado Esperado	Resultado Obtenido	Estado
01	Durante el envío de alertas comunes, la comunicación con el websocket se perdió.	Alertas enviadas	Ninguno	El sistema presenta mensajes indicando la desconexión.	Muestra mensaje de error correspondiente por consola	OK
02	Durante el envío de alertas de emergencia, la comunicación con el websocket se perdió.	Alertas enviadas	Ninguno	El sistema presenta mensajes indicando la desconexión.	Muestra mensaje de error correspondiente por consola	OK
03	Durante el envío de alertas comunes, el teleoperador se ausentó durante su sesión en el sistema.	Alertas enviadas	Ninguno	El sistema cierra la sesión del usuario y lo redirecciona al login	Se cerró la sesión y redirecciono al login	OK
04	Durante el envío de alertas de emergencia, el teleoperador se ausentó durante su sesión en el sistema	Alertas enviadas	Ninguno	El sistema cierra la sesión del usuario y lo redirecciona al login	Se cerró la sesión y redirecciono al login	OK
05	Inspeccionar una alerta que ha sido ocupada por otro teleoperador	Estado actual del teleoperador	Clic en el detalle de alerta.	Muestra mensaje de error “La alerta está asignada a	Muestra mensaje de error correspondiente	OK

				otro teleoperador"		
06	Inspeccionar otra alerta en donde el teleoperador ha sido actualmente asignado a una alerta.	Estado actual del teleoperador	Clic en el detalle de alerta	Muestra mensaje de error "Debe culminar la atención de la alerta actual para atender otra"	Muestra mensaje de error correspondiente	OK
07	Inspecciona una alerta después de haber estado ausente durante un lapso de tiempo largo	Estado actual del teleoperador	Clic en el detalle de alerta	El sistema cierra la sesión del usuario y lo redirecciona al login	Se cerró la sesión y redireccion o al login	OK
08	Inspecciona una alerta cuando la comunicación con el websocket se perdió	Estado actual del teleoperador	Clic en el detalle de alerta	El sistema presenta mensajes indicando la desconexión.	Muestra mensaje de error correspondiente por consola	OK

Fuente: Elaboración Propia

c) CUS: Asignar Delito

Tabla 15. Tabla de Casos de Pruebas del CUS Asignar Delito

N° Caso	Descripción del Caso de Prueba/ Objetivo	Dato de Entrada	Acción	Resultado Esperado	Resultado Obtenido	Estado
01	Asignar delito sin la selección de ningún delito.	Seleccionar datos	Clic	Mostrar Mensaje de error "No ha seleccionado un archivo"	Muestra mensaje de error correspondiente	OK
02	Escribir la mayor cantidad de caracteres en	Datos por teclado	Clic	El campo no permite más caracteres del	El campo solo registra el máximo	OK

	la casilla de observación y proceder a asignar el delito.			máximo configurado.	de caracteres permitidos	
03	Realiza más de un clic al momento de asignar un delito en el formulario.	Clic	Clic	El botón se bloquea luego de realizar el primer clic	Botón bloqueado luego del primer clic	OK
04	Estar ausente tras un lapso de tiempo y proceder a asignar el delito.	Clic	Clic	El sistema cierra la sesión del usuario y lo redirecciona al login	Se cerró la sesión y redireccionó al login	OK
05	Estar ausente tras un lapso de tiempo y procede a ceder el turno de atención.	Clic	Clic	El sistema cierra la sesión del usuario y lo redirecciona al login	Se cerró la sesión y redireccionó al login	OK
06	Cuando el socket deja de emitir comunicación con el sistema web y el teleoperador procede a asignar el delito.	Seleccionar datos	Clic	Muestra mensaje de error “No hay comunicación para proceder con la operación”	Muestra mensaje de error correspondiente por interno	OK
07	Cuando el socket deja de emitir comunicación con el sistema web y el teleoperador procede a ceder el turno de atención.	Seleccionar datos	Clic	Muestra mensaje de error “No hay comunicación para proceder con la operación”	Muestra mensaje de error correspondiente por interno	OK

Fuente: Elaboración Propia

d) CUS: Generar reporte de alertas.

Tabla 16. Tabla de Casos de Pruebas del CUS Reporte de Alerta

N° Caso	Descripción del Caso de Prueba/ Objetivo	Dato de Entrada	Acción	Resultado Esperado	Resultado Obtenido	Estado
01	Dejar los campos vacíos y Generar Reporte	Ninguno	Clic en botón “Generar”	Mostrar el mensaje de error “Debe llenar los campos”	Muestra mensaje de error correspondiente	OK
02	Dejar el campo de “tipo de reporte” vacío y llenar los demás campos seleccionando una opción.	Seleccionar datos	Clic en botón “Generar”	Mostrar el mensaje de error “Debe llenar el campo tipo de reporte”	Muestra mensaje de error correspondiente	OK
03	Dejar el campo de “prioridad de alerta” vacío y llenar los demás campos seleccionando una opción.	Seleccionar datos	Clic en botón “Generar”	Mostrar el mensaje de error “Debe llenar el campo prioridad de alerta”	Muestra mensaje de error correspondiente	OK
04	Dejar el campo de “fecha inicio” vacío y llenar los demás campos seleccionando una opción.	Seleccionar datos	Clic en botón “Generar”	Mostrar el mensaje de error “Debe llenar el campo fecha inicio”	Muestra mensaje de error correspondiente	OK
05	Dejar el campo de “fecha fin” vacío y	Seleccionar datos	Clic en botón “Generar”	Mostrar el	Muestra mensaje de error	OK

	llenar los demás campos seleccionando una opción.			mensaje de error “Debe llenar el campo fecha fin”	correspondiente	
06	Ingresar manualmente datos a los campos de la ventana mostrada.	Ingresar datos por teclado	Clic en botón “Generar”	Los campos no deben poder ser editados manualmente	No se editan los campos, son solamente de lectura.	OK
07	Colocar un formato de fecha diferente al configurado en el campo.	Ingresar datos por código fuente	Clic en botón “Generar”	Debe mostrar mensaje de error de formato invalido	Muestra mensaje de error correspondiente	OK
08	Ingresar una fecha inicio superior a la fecha fin.	Seleccionar datos	Clic en botón “Generar”	Muestra mensaje de error “fecha inicio superior a la fecha fin”	Muestra mensaje de error correspondiente	OK
09	Exportar el reporte de alertas sin haberlo generado previamente	Hacer clic	Clic en botón “Exportar”	Muestra mensaje de error “Debes generar el reporte”	Muestra mensaje de error correspondiente	OK
10	Exportar el reporte luego de haberlo generado	Hacer clic	Clic en botón “Exportar”	Se debe descargar el reporte	Descarga el reporte	OK

Fuente: Elaboración Propia

CAPÍTULO VI: RESULTADOS DE LA INVESTIGACIÓN

6.1. Análisis de los indicadores

6.1.1. Descriptivos

En el presente estudio, realizamos la comparación de la aplicación de escritorio de la empresa FIRINGS E.I.R.L de una forma descriptiva en cuanto a sus características y luego se describirán los indicadores a cumplir por el sistema web Firveal. Los resultados descriptivos de estas medidas son:

a) Indicador: Delitos

- No existe un registro de atención al cual el teleoperador pueda presentar los casos resueltos a identificar.
- La información que presenta acerca de los delitos no describe a detalle el tipo de delito al que pertenece la alerta.
- La tarea al cual uno identifica el delito lo hace el vecino al momento de reportar una alerta mediante un formulario.

b) Indicador: Disposición de vigilancia

- Las notificaciones que recibe el teleoperador sólo se activan cuando una alerta de cualquier índole pasa por una alarma instalada, omitiendo las reglas impuestas acerca de la activación de la sirena de alarma.
- La respuesta del software desktop ante los eventos que acontece durante el monitoreo o las alertas entrantes al mapa, no se efectúa en tiempo real.
- Demora en la recepción de alertas alrededor de 8 segundos aproximados hasta que aparezca la alerta en el mapa de monitoreo.
- El Software Desktop no tiene implementada la funcionalidad de asignación de alerta a los teleoperadores.
- El estado actual de la activación de la sirena no se refleja a como se presenta en el mapa de monitoreo.
- La desactivación de la sirena de alarma después del tiempo prolongado no se refleja en el mapa de monitoreo.

c) Indicador: Prevención de la Inseguridad

- No presenta reportes específicos en relación a un rango en el tiempo o el cómo se han ido desarrollando las alertas durante sus apariciones.
- Se demora en la exportación de reportes, puesto que intenta recopilar toda la información almacenada en la base de datos.
- Se tiene como resultado según el planteamiento anteriormente señalado del capítulo 4, que el porcentaje de delitos identificados por el software desktop es de 100.00%.

6.1.2. Inferenciales

Al entender la situación que representa actualmente el funcionamiento del software desktop que tiene FIRINGS E.I.R.L, el propósito de nuestra solución es llevar a cabo el cumplimiento de cada indicador anteriormente mencionado con el uso del sistema web Firveal. Para saber más acerca de las funcionalidades implementadas en el sistema web, ver en Anexo 6.

Por ende, se mencionan los positivos resultados que abarcaría en cada indicador, son los siguientes:

a) Indicador: Delitos

- Se implementará al 100% la funcionalidad de la identificación de delitos sobre la alerta reportada.
- Se utilizará como referencia del Plan Nacional de Seguridad Ciudadana 2019-2023, los tipos de delitos que conlleva un incidente; de esta forma, se normaliza la información que viene manejando el software desktop.
- El teleoperador será responsable en identificar el delito al que pertenezca la alerta reportada por el vecino, reduciendo el esfuerzo del vecino en un 100% en reportar cualquier tipo de alerta.

b) Indicador: Disposición de vigilancia

- Se implementará la funcionalidad al 100% acerca de la activación de la sirena de la alarma mediante la proximidad de una alerta de emergencia.

- Se demuestra que el sistema web tendrá disponibilidad al 100% de su capacidad para poder recibir alertas enviadas por el websocket, y lo mismo sucede para el caso del websocket en viceversa; cumpliendo positivamente la intercomunicación en tiempo real.
- Se ha calculado que el sistema deberá reducir el 62.50% del tiempo de respuesta cuando una alerta aparece en el mapa de monitoreo.

  ((TAD - TSW) * 100) / TAD = RTR

  TAD = Tiempo de Aplicación Desktop (8 segundos)

  TSW = Tiempo del Sistema Web (3 segundos)

  RTR = Reducción del Tiempo de Respuesta (62.50%)
- El sistema web tendrá implementada la funcionalidad de asignación de alertas a los teleoperadores en tiempo real.
- El estado de activación de la sirena de la alarma se observará en el mapa de monitoreo debido a la implementación del websocket para saber constantemente su estado actual.
- Se implementará al 100% la característica que implica la desactivación de la sirena después de caducar su tiempo programado.

c) Indicador: Prevención de la Inseguridad

- Mejorará al 100% en la generación de reportes de alertas y alarmas, con respecto al volumen de datos y búsqueda en un rango de tiempo.
- Mejorará en el diseño y exportación de los reportes de alertas y alarmas.
- Como resultado obtenido según indicado en el Anexo 6, el porcentaje de delitos identificados por el sistema web “Firveal” será de un 100.00%.

  (DR * 100) / TAM = PDI

  TAM = Total de Alertas Mensuales (200 alertas)

  DR = Delitos Reportados (200 alertas identificadas)

  PDI = Porcentaje de Delitos Identificados (100%)

6.2. Discusión de la Hipótesis

En cuanto a nuestra primera hipótesis específica, el sistema web de monitoreo de alertas planteado para la empresa FIRINGS E.I.R.L si cumplirá en influir positivamente en la identificación de los delitos, dado que ahora se ha implementado el requerimiento de esta funcionalidad sobre las alertas reportadas operadas por el teleoperador en el mapa de monitoreo, reduciendo favorablemente el esfuerzo de partícipes externos.

En cuanto a nuestra segunda hipótesis específica, el sistema web de monitoreo de alertas si cumplirá en influir positivamente en la disposición de vigilancia, debido a que ahora las alarmas se activan según la proximidad de una alerta de emergencia, además de la reducción del tiempo de respuesta de la aparición de alertas en el mapa de monitoreo y la asignación de alertas a los teleoperadores en tiempo real.

En cuanto a nuestra tercera y última hipótesis específica, el sistema web de monitoreo de alertas si cumplirá en influir positivamente en la prevención de la inseguridad, debido a que ahora se cuenta con reportes cuya información es relevante y precisa para la toma de decisiones en cuestión a la mejora continua sobre los procesos actuales del negocio en relación a la prevención de la inseguridad ciudadana. Tales como la identificación de los delitos, operatividad de las alertas y la actividad de las alarmas.

Por consiguiente, al cumplirse todas las hipótesis específicas, nuestra hipótesis general también se cumplirá.

CONCLUSIONES

1. La primera hipótesis específica se cumplirá ya que ahora se lograrán identificar los delitos de las alertas reportadas y el proceso es más ágil para los teleoperadores.

2. La segunda hipótesis específica se cumplirá ya que ahora habrá mayor efectividad en la atención de las alertas, lo cual mejorará considerablemente el tiempo de respuesta de las alertas en el mapa de monitoreo.

3. La tercera hipótesis específica se cumplirá ya que ahora se generarán reportes con información de mayor precisión para la toma de decisiones en el manejo de la seguridad ciudadana a futuro.

4. La hipótesis general se cumplirá dado que todas las hipótesis específicas se cumplirán logrando así influir positivamente en la identificación de los delitos, la disposición de la vigilancia y la prevención de la inseguridad.

RECOMENDACIONES

1. Se recomienda supervisar la proactividad de los teleoperadores durante el proceso del monitoreo y atención en el sistema; dado que, gracias a la accesibilidad de la información que maneja el sistema web Firveal, se podrá saber en tiempo real el estado actual de las alertas y quienes lo intervienen.

2. Se recomienda implementar el diseño actual del sistema web “Firveal” adecuándose con las tecnologías que posee actualmente la empresa; de esta forma se escala positivamente la intercomunicación de las aplicaciones con el websocket, para obtener mayor eficiencia en la recepción y ejecución de las alertas y las alarmas en general.

3. Se recomienda realizar reportes mensuales, para tener un volumen de datos consistente y amplio que ayudarán a la toma de decisiones con respecto al manejo de la seguridad ciudadana.

4. Se recomienda la implementación del sistema web, en zonas de distritos inseguros, donde la tasa delictiva sea superior a la normal, para con ello, poder identificar los delitos, mejorar la disposición de la vigilancia y ayudar en la prevención de la inseguridad.

REFERENCIAS BIBLIOGRÁFICAS

Arraiza, E. (2016). *Manual de Gestión Municipal*. Argentina. Recuperado de: https://www.kas.de/c/document_library/get_file?uuid=ca6339ee-acec-5a87-7b2c-a4bf43d21f8b&groupId=287460

Asociación de Academias de la Lengua Española (2022). Diccionario de la lengua española [versión electrónica]. Madrid, España: Real Academia Española, https://dle.rae.es/

Bizagi Limited (2022). *Bizagi: User guide Modeler*. Colombia: Bizagi Limited. Recuperado de https://help.bizagi.com/process-modeler/es/index.html?gateways.htm

Carranza, A. (05 de diciembre de 2021). Conoce qué es Java y diseña aplicaciones móviles de ensueño. [Mensaje en un blog]. Recuperado de https://www.crehana.com/blog/desarrollo-web/que-es-java/

Congreso de la República. (2014). *Ley N° 29733, Ley del Sistema Nacional de Seguridad Ciudadana - Capítulo I. Gob. Perú.* Recuperado de https://www.gob.pe/institucion/congreso-de-la-republica/normas-legales/331205-27933

Cubel, E. (07 de Setiembre de 2018). ¿Sabes cómo incluir Google Maps gratis en tu web? Experiencias. [Mensaje en un blog]. Recuperado de https://www.uup.es/blog/google-maps-gratis-en-tu-web/

Chicaiza Guachi, K. G. (2020). *Sistema de alarma comunitaria para el mercado San Juan de la Ciudad de Santiago de Píllaro* (tesis de pregrado) Universidad Técnica de Ambato. Facultad de Ingeniería en Sistemas, Electrónica e Industrial. Carrera Ingeniería Electrónica y Comunicaciones. Ambato. Ecuador de la Criminalidad, C. E. I.

DBeaver Community (2022) *About Overview*. DBeaver Community. Recuperado de https://dbeaver.io/about/

Damián, A. (04 de Setiembre de 2017). MySQL Workbench, herramienta visual para el diseño de bases de datos. [Mensaje en un blog]. Recuperado de https://ubunlog.com/mysql-workbench-bases-datos/

Dammert, L. (2007). *Perspectivas y dilemas de la seguridad ciudadana en América Latina.* Ecuador. Recuperado de https://biblio.flacsoandes.edu.ec/libros/digital/40089.pdf

Diario oficial del Bicentenario, El Peruano. (29 de Julio de 2020). *Normas Legales Actualizadas. Editora Perú.* Recuperado de https://diariooficial.elperuano.pe/pdf/0034/codigo-penal-29.07.2020.pdf

Euroinnova, International Online Education. (2022). *Funciones de un teleoperador*. Granada, España: Euroinnova. Recuperado de https://www.euroinnova.edu.es/funciones-de-un-teleoperador#iquestqueacute-es-un-teleoperador

Fantino, J. (5 de noviembre de 2021). ¿Qué es NetBeans? Crea aplicaciones con Java a la velocidad de la luz. [Mensaje en un blog]. Recuperado de https://www.crehana.com/blog/desarrollo-web/que-es-netbeans/

García, A. (15 de junio de 2015). *¿Qué es Maven y para qué se utiliza?* Panamá: Panamá Hitek. Recuperado de http://panamahitek.com/que-es-maven-y-para-que-se-utiliza/

Gil, I. (19 de abril de 2018) Trabajar de teleoperador. Todo lo que necesitas saber. Fundación Adecco. [Mensaje en un blog]. Recuperado de https://fundacionadecco.org/blog/trabajar-teleoperador-lo-necesitas-saber/

Gilfillan, I. (2003). *La Biblia de MySQL*. Madrid, España: Anaya Multimedia

Google (19 de agosto de 2022). Ventajas de Google Cloud. California, EU: Google LLC. Recuperado de https://cloud.google.com/why-google-cloud/

Hensgen, P. (2001). *Manual de Umbrello UML Modeller*. KDE documentation. Recuperado de https://docs.kde.org/stable5/es/umbrello/umbrello/uml-elements.html

Herrera, J. (11 de abril de 2022). Almacenamiento de datos en la nube con Firebase, ¿Qué es Cloud Storage? [Mensaje en un blog]. Recuperado de https://www.paradigmadigital.com/dev/que-es-firebase-cloud-storage/

Herrera, J. (18 de mayo de 2022). Cloud Firestore y Realtime Database, ¿Qué base de datos elegir con Firebase? [Mensaje en un blog]. Recuperado de https://www.paradigmadigital.com/dev/cloud-firestore-realtime-database-base-datos-firebase/

INEI. (2021). *Anuario estadístico de criminalidad y seguridad ciudadana 2015-2019 Perú. Instituto Nacional de Estadística e Informática.* Recuperado de: https://www.inei.gob.pe/media/MenuRecursivo/publicaciones_digitales/Est/Lib1805/libro.pdf

Instituto Nacional de Seguridad y Salud en el trabajo. (2022) *Seguridad en el trabajo - Emergencias*. España. Recuperado de https://www.insst.es/emergencias

Jaulis Rua, J. J., & Vilcarromero Giraldo, J. R. (2015). *Sistema de predicción de hechos delictivos para la mejora del proceso de prevención del delito en el distrito de La Molina utilizando minería de datos.* (tesis de titulación) Universidad San Martin de Porres, Lima, Perú

Juneau, J. (2014). PrimeFaces in the Enterprise. [Mensaje en un blog]. Recuperado de https://www.oracle.com/technical-resources/articles/java/java-primefaces.html

Junta de Andalucía. (2020). *JavaServer Faces (JSF).* Andalucía, España: Marco de Desarrollo de la Junta de Andalucía. Recuperado de http://www.juntadeandalucia.es/servicios/madeja/contenido/recurso/101

Karaman, A. (3 de febrero de 2019). React Native - Socket IO (Kur Bilgilerini Push Etme). [Mensaje en un blog]. Recuperado de https://medium.com/bilişim-hareketi/react-native-socket-io-kur-bilgilerini-push-etme-881e349e12d6

Ministerio del Interior. (2018). *Propuesta de Plan Nacional de Seguridad Ciudadana 2019 - 2023. El Perú Primero.* Recuperado de https://www.gob.pe/institucion/mininter/informes-publicaciones/610391-plan-nacional-de-seguridad-ciudadana-2019-2023

Ministerio de Justicia y Derechos Humanos. (2017). *Teoría del Delito*. Perú. Recuperado de https://www.minjus.gob.pe/wp-content/uploads/2017/03/Teoria-Del-Delito.pdf

Mollericona, J. Y., Tinini, N., & Paredes, A. (2007). *La seguridad ciudadana en la ciudad de El Alto: fronteras entre el miedo y la acción vecinal* (No. 7). La Paz: Fundación Pieb. Recuperado de https://www.academia.edu/44403354/La_seguridad_ciudadana_en_la_ciudad_de_El_Alto_Fronteras_entre_el_miedo_y_la_acción_vecinal

Muradas, Y. (05 de junio de 2018). Qué es Spring Framework y por qué usarlo. OpenWebinars. [Mensaje en un blog]. Recuperado de https://openwebinars.net/blog/conoce-que-es-spring-framework-y-por-que-usarlo/

MyBatis (19 de septiembre de 2022). *Introducción ¿Qué es Mybatis? Delaware, Eu:* Apache Software Foundation. Recuperado de https://mybatis.org/mybatis-3/es/index.html

Oracle (2022) *Lesson: Overview of the JMX Technology.* Texas, EU: Oracle Java Documentation. Recuperado de https://docs.oracle.com/javase/tutorial/jmx/overview/index.html

Pedamkar, P. (2022). What is Desktop Software? [Mensaje en un blog]. Recuperado de https://www.educba.com/what-is-desktop-software/

Pérez, J. y Gardey, A. (2013). Definición de Alarma. [Mensaje en un blog]. Recuperado de https://definicion.de/alarma/

Poder Judicial del Perú. (18 de octubre de 2021). *Poder Judicial instala 'Botón de pánico' en teléfonos celulares de 1264 mujeres víctimas de violencia.* Recuperado de https://www.gob.pe/institucion/pj/noticias/546373-poder-judicial-instala-boton-de-panico-en-telefonos-celulares-de-1264-mujeres-victimas-de-violencia

San Juan, V. (27 de abril de 2016). Ventajas de los sistemas web. [Mensaje en un blog]. Recuperado de https://www.aeurus.cl/blog/ventajas-de-los-sistemas-web

Socket IO. (2022). *Rooms. Socket.IO*. California, EU: Socket.IO. Recuperado de: https://socket.io/docs/v3/rooms/

Soto, J. (2022). Acerca del libro. Nueva York, EU: Gitbooks. Recuperado de https://jsitech1.gitbooks.io/meet-docker/content/index.html

Universidad de Alicante. (2016). *Diccionario y glosario en riesgos. Vocabulario de uso frecuente en riesgos y desastres.* Alicante, España: Universidad de Alicante. Recuperado de https://web.ua.es/es/labclima/diccionario-y-glosario-en-riesgos.html

Vera Paredes, D. A., Córdova Martínez, L. C., López Bermúdez, R. M. y Pacheco Mendoza, S. R. (2019). Análisis de la metodología RUP en el desarrollo de software académico mediante la herramienta DJANGO. *Revista Científica Mundo de la Investigación y el Conocimiento. Vol. 3(2)*, 964-979. Recuperado de: https://recimundo.com/index.php/es/article/view/486/629

VictorD3D. (18 de mayo de 2020). ¿Qué es diagrams.net? [Mensaje en un blog]. Recuperado de https://conocimientolibre.mx/que-es-diagrams-net/

Villaplana Jiménez, F. R. (2021). Recursos digitales de colaboración y de seguridad pública. Mejorando la autoprotección ciudadana. *RIPS: Revista de Investigaciones Políticas y Sociológicas. Vol.* 20(2). Recuperado de: https://doi.org/10.15304/rips.20.2.7989

Walton, A. (17 de febrero de 2022). Diferencias entre JDK, JRE y JVM. [Mensaje en un blog]. Recuperado de https://javadesdecero.es/fundamentos/diferencias-jdk-jre-jvm/

Wieldt, T. (21 de abril del 2014). New Tech Article: PrimeFaces in the Enterprise. [Mensaje en un blog]. Recuperado de https://blogs.oracle.com/java/post/new-tech-article-primefaces-in-the-enterprise

ANEXOS

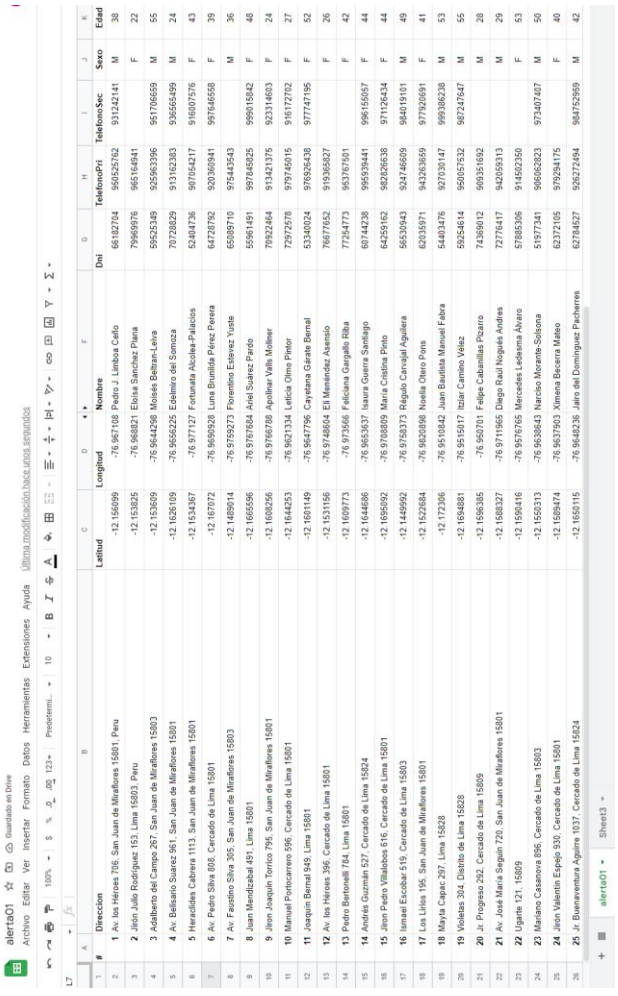
Comentado [LHPP15]: No esta el manual de instalación ni de usuario

Comentado [P16R15]: Corregido

Anexo 1: Instrumentos de recolección de datos

Relación de Alertas Generados para la Investigación

La empresa FIRINGS E.I.R.L nos brindó una relación de datos de alertas generados por la aplicación vecino y recopilados desde la base de datos de *Firebase.* Se considera como la población al cual nosotros utilizaremos durante la investigación.



#	Direccion	Latitud	Longitud	Nombre	Dni	TelefonoPri	TelefonoSec	Sexo	Edad
1	Av. los Héroes 706, San Juan de Miraflores 15801, Peru	-12.1586099	-76.987108	Pedro J. Limbaca Cielo	66182704	950525762	931242141	M	38
2	Jirón Julio Rodriguez 153, Lima 15803, Peru	-12.153825	-76.968821	Eloisa Sanchez Plana	79969976	965164941		F	22
3	Adalberto del Campo 267, San Juan de Miraflores 15803	-12.153609	-76.9644298	Moisés Beltran Leiva	59525349	925963396	951706659	M	55
4	Av. Belisario Suárez 961, San Juan de Miraflores 15801	-12.1626109	-76.9656225	Edelmiro del Somoza	70728829	913162383	936565499	M	24
5	Heraclides Cabrera 1113, San Juan de Miraflores 15801	-12.1534367	-76.977127	Fortunata Alcolea-Palacios	52404736	907654217	916007576	F	43
6	Av. Pedro Silva 808, Cercado de Lima 15801	-12.167072	-76.9699328	Luna Brunilda Pérez Perera	64728792	920360941	997646558	F	39
7	Av. Faustino Silva 305, San Juan de Miraflores 15803	-12.1469014	-76.9759273	Florentino Estevez Yuste	65089710	975443543		M	36
8	Juan Mendizabal 491, Lima 15801	-12.1665596	-76.9767684	Ariel Suárez Pardo	55961491	997645525	999915842	F	48
9	Jiron Joaquin Torrico 795, San Juan de Miraflores 15801	-12.1608296	-76.9766788	Apolinar Valls Moliner	70922464	913421375	923314603	F	24
10	Manuel Portocarrero 596, Cercado de Lima 15801	-12.1644253	-76.9621334	Leticia Olmo Pintor	72972578	979745015	916172702	F	27
11	Joaquin Bermal 545, Lima 15801	-12.1661149	-76.9647796	Cayetana Gárate Bernal	53340024	976926438	977747195	F	52
12	Av. los Héroes 396, Cercado de Lima 15801	-12.1531156	-76.9748604	Eli Menéndez Asensio	76677652	919365827		F	26
13	Pedro Bartonelli 784, Lima 15801	-12.1609773	-76.973566	Feliciana Gargallo Riba	77254773	953767501		F	42
14	Andrés Guzmán 527, Cercado de Lima 15824	-12.1644686	-76.9653637	Isaura Guerra Santiago	60744236	995939441	996156057	F	44
15	Jiron Pedro Villalobos 616, Cercado de Lima 15801	-12.1695092	-76.9788809	María Cristina Pinto	64259162	982826638	971126434	F	44
16	Ismael Escobar 519, Cercado de Lima 15803	-12.1449992	-76.9758373	Régulo Carvajal Aguilera	56530943	924746609	984019101	M	49
17	Los Lirios 195, San Juan de Miraflores 15801	-12.1522684	-76.9820898	Noelia Otero Pons	62035971	943263659	977920691	F	41
18	Mayta Capac 297, Lima 15828	-12.172306	-76.9510842	Juan Bautista Manuel Fabra	54403476	927030147	999386238	M	53
19	Violetas 304, Distrito de Lima 15828	-12.1654881	-76.9515017	Itziar Camino Vélez	59254614	950057532	987247647	M	55
20	Jr. Progreso 292, Cercado de Lima 15809	-12.1596385	-76.950701	Felipe Cabanillas Pizarro	74369012	999351692		M	28
21	Av. José María Seguín 720, San Juan de Miraflores 15801	-12.1568327	-76.9711965	Diego Raúl Noguès Andres	72776417	942659313		M	29
22	Ugarte 121, 15809	-12.1596416	-76.9576765	Mercedes Ledesma Álvaro	57885306	914502350		F	53
23	Mariano Casanova 896, Cercado de Lima 15803	-12.1550313	-76.9638643	Narcisa Morante-Solsona	51977341	966062823	973407407	M	50
24	Jirón Valentín Espejo 930, Cercado de Lima 15801	-12.1589474	-76.9637903	Ximena Becerra Mateo	62372105	979294175		F	40
25	Jr. Buenaventura Aguirre 1037, Cercado de Lima 15824	-12.1650115	-76.9648236	Jairo del Domínguez Pacheres	62784527	926272494	984752999	M	42

Manual de Desarrollo del Equipo de Alarma "FGS10 v1.0"

Se ha utilizado la información brindada por la empresa FIRINGS acerca de los equipos de alarmas que tienen almacenados en su local. En ellos se reflejan los eventos o comandos que se tienen configurado por defecto en los equipos "FGS10".

Descripción de Comandos FGS10 v1.0

El presente documento describe las tramas de comunicación entre el Servidor y las Telealarmas FIRINGS, las cuales usan Ethernet o GPRS para comunicarse.

Formato general de la trama (ASCII): CABECERA | ID | OPCODE | DATA |

CABECERA : FGS10 (FGS: Firings, 10: Telealarma)
ID : Fecha y Hora de primera conexión de la Telealarma al Servidor (*)
OPCODE : Código de Operación de la Trama (2 dígitos)
DATA : Depende del OpCode

(*) Formato: **YYMMDDhhmmss**, por ejemplo, si la primera vez que se conectó una Telealarma al Servidor fue el 8 de diciembre del 2020 a las 17:29:36 entonces su ID será 201208172936.
Cuando una telealarma es programada/actualizada con un nuevo firmware, ésta tendrá un ID=000000000000, el Servidor al detectar este equipo le enviará la trama "ACTUALIZAR ID".

Tramas enviadas por la Telealarma al Servidor

ESTADO GSM: La Telealarma informa al Servidor su estado cada 20 segundos.
FGS10 | ID | 01 | CONEXIÓN | SEÑAL_GSM | TELEALARMA | SIRENA |

DATA	Descripción	VALOR	
CONEXIÓN	Comunicación entre la Telealarma y el Servidor	0: GPRS	1: ETHERNET
SEÑAL_GSM	Barras de señal GSM	0-5	
TELEALARMA	Estado de la Telealarma	0: Reposo 1: Perifoneo 2: Pánico GSM	
SIRENA	Estado de la sirena	0: Desactivada	1: Activada

Ejemplo: FGS10|000000000000|01|1|0|0|0|

EVENTO GSM: El usuario llamó o envió sms a la Telealarma.
FGS10 | ID | 02 | USUARIO | EVENTO_GSM |

DATA	Descripción	VALOR
USUARIO	Número del usuario	Ejemplo: "991234567", "+51991234567", "015278945"
EVENTO_GSM	Evento en la Telealarma	1: Perifoneo GSM 2: Pánico GSM por llamada 3: Pánico GSM por SMS

Ejemplo: FGS10|000000000000|02|991234567|1|

PÁNICO RF: El usuario disparó la sirena usando un transmisor RF
FGS10 | ID | 03 | CÓDIGO_RF |

DATA	Descripción	VALOR
CÓDIGO_RF	Código RF del transmisor del usuario	6 caracteres

Ejemplo: FGS10|000000000000|03|6FC420|

PETICIÓN RF: Envía al Servidor el código RF del transmisor a registrar
FGS10 | ID | 04 | CÓDIGO_RF |

DATA	Descripción	VALOR
CÓDIGO_RF	Código RF del transmisor que se desea registrar	6 caracteres

Ejemplo: FGS10|000000000000|04|6FC420|

CLAVE SMS: Respuesta al comando LEER CLAVE SMS
FGS10 | ID | 20 | CLAVE_SMS |

DATA	Descripción	VALOR
CLAVE	Clave de la Telealarma	4 caracteres

Ejemplo: FGS10|000000000000|20|1234|

TIEMPO DE SIRENA: Respuesta al comando LEER TIEMPO DE SIRENA
FGS10 | ID | 21 | TIEMPO_SIRENA |

DATA	Descripción	VALOR
TIEMPO SIRENA	Tiempo en segundos que permanece activada la sirena	0-180

Ejemplo: FGS10|000000000000|21|5|

MODO TELEALARMA: Respuesta al comando LEER MODO TELEALARMA

FGS10 | ID | 23 | LLAMADAS | SMS | RF | MONITOR_UART |

DATA	Descripción	VALOR
LLAMADAS	Permiso de una llamada entrante	0: Acepta TODAS las llamadas 1: Acepta SOLO llamadas registradas
SMS	Permiso de un SMS entrante	0: Acepta TODOS los SMS's 1: Acepta SOLO SMS's registrados
RF	Permiso de un transmisor RF	0: Acepta TODOS los transmisores RF's 1: Acepta SOLO transmisores RF's registrados
MONITOR_UART	Permite monitorear la comunicación UART	0: Monitor deshabilitado 1: Monitor habilitado

Ejemplo: FGS10|000000000000|23|1|0|1|1|

APN: Respuesta al comando LEER APN

FGS10 | ID | 24 | APN |

DATA	Descripción	VALOR
APN	APN para conectar por GPRS la telealarma al Servidor	1-15 caracteres

Ejemplo: FGS10|000000000000|24|claro.pe|

DIRECCIÓN: Respuesta al comando LEER DIRECCIÓN

FGS10 | ID | 25 | DIRECCIÓN |

DATA	Descripción	VALOR
DIRECCIÓN	Dirección (ubicación) de la telealarma.	1-40 caracteres

Ejemplo: FGS10|000000000000|25|Av. Loreto 152|

NÚMERO DE SERVICIO: Respuesta al comando LEER NÚMERO DE SERVICIO

FGS10 | ID | 26 | NÚMERO_SERVICIO |

DATA	Descripción	VALOR
NÚMERO_SERVICIO	Número al que se reporta la telealarma tras el formateo o test.	Ejemplo: "991234567", "+51991234567"

Ejemplo: FGS10|000000000000|26|991234567|

IMEI: Respuesta al comando LEER IMEI

FGS10 | ID | 27 | IMEI |

DATA	Descripción	VALOR
IMEI	Imei de la telealarma.	15 caracteres

Ejemplo: FGS10|000000000000|27|863986031167386|

MAC: Respuesta al comando LEER MAC

FGS10 | ID | 40 | MAC |

DATA	Descripción	VALOR
MAC	Dirección MAC de la Telealarma	Ejemplo: 00-08-DC-01-02-03

Ejemplo: FGS10|000000000000|40|00-08-DC-01-02-03|

GATEWAY: Respuesta al comando LEER GATEWAY

FGS10 | ID | 41 | GATEWAY |

DATA	Descripción	VALOR
GATEWAY	Dirección IP del enrutador	Ejemplo: 192.168.1.1

Ejemplo: FGS10|000000000000|41|192.168.1.1|

MASCARA DE SUBRED: Respuesta al comando LEER MASCARA DE SUBRED

FGS10 | ID | 42 | MASK_SUBRED |

DATA	Descripción	VALOR

MASK_SUBRED	Máscara de subred	Ejemplo: 255.255.255.0

Ejemplo: FGS10|000000000000|42|255.255.255.0|

IP TELEALARMA: Respuesta al comando LEER IP TELEALARMA

FGS10 | ID | 43 | IP_TELEALARMA |

DATA	Descripción	VALOR
IP_TELEALARMA	Dirección IP Local de la Telealarma	Ejemplo: 192.168.1.27

Ejemplo: FGS10|000000000000|43|192.168.1.27|

IP PÚBLICA Y PUERTO SERVIDOR: Respuesta al comando LEER IP Y PUERTO SERVIDOR

FGS10 | ID | 45 | IP_SERVIDOR | PUERTO_SERVIDOR |

DATA	Descripción	VALOR
IP_SERVIDOR	Dirección IP del Servidor	Ejemplo: 190.117.54.230
PUERTO_SERVIDOR	Puerto del Servidor	1024-65535

Ejemplo: FGS10|000000000000|45|190.117.54.230|5555|

RESPUESTA LEER MEMORIA: Respuesta al comando LEER PÁGINA DE MEMORIA

FGS10 | ID | 83 | DATA |

DATA	Descripción	VALOR
DATA	Bytes leídos, (formato hex.) separados por un espacio.	Byte (hex): 00-FF

Ejemplo: FGS10|000000000000|83|01 BC 54 ... 7D|

RESPUESTA LEER EEPROM: Respuesta al comando LEER EEPROM

FGS10 | ID | 85 | DATA |

DATA	Descripción	VALOR
DATA	Bytes leídos, (formato hex.) separados por un espacio.	Byte (hex): 00-FF

Ejemplo: FGS10|000000000000|85|01 BC 54 ... 7D|

RESPUESTA A COMANDO:

FGS10 | ID | 99 | RESPUESTA_CMD |

DATA	Descripción	VALOR
RESPUESTA_CMD	Respuesta al último comando recibido	1: Comando ejecutado correctamente 2: Error en la memoria de la Telealarma 3: Espacio insuficiente en memoria 4: Elemento eliminado 5: Elemento encontrado 6: Elemento no encontrado 7: Error en el último comando

Ejemplo: FGS10|000000000000|99|1|

Cuestionario acerca del Alcance del Proyecto

Tuvimos la oportunidad de entrevistar mediante cuestionarios preparados al gerente general de la empresa FIRINGS E.I.R.L sobre el negocio y su relación con el proyecto nuevo, y a un ingeniero técnico quien es responsable de los equipos de alarma "FGS10" acerca de las alarmas y las bondades que tienen las aplicaciones activas de la empresa.

Para el gerente general, las preguntas contestadas fueron las siguientes:

a) ¿Cómo se están identificando las alertas actualmente?
   Las alertas provienen de la activación de botón de pánico de la aplicación "Vecino", accionado por el vecino quien auxilia por una situación en peligro. Estas alertas se consideran de máxima prioridad, por lo que el teleoperador debe atenderse con urgencia; sin embargo, puede haber alertas que no se consideren como de emergencia, sino como aquellas alertas que son enviadas como casos por resolver de manera no urgente. Para este segundo caso se estaría desarrollando en este nuevo proyecto.

b) ¿Cómo el teleoperador procede a atender una alerta activada por el botón de pánico?
   El teleoperador debe estar atento en cuanto aparezca alguna alerta en el mapa de monitoreo; cuando lo vea, comienza a inspeccionar la información que conlleva aquella alerta y procede a llamar al vecino que reportó la alerta.

c) En el supuesto que haya más de dos alertas, ¿El teleoperador tiene la obligación de decidir por su cuenta cuál de las alertas atender primero? ¿O existe alguna regla que en principio se debe seguir?
   Para empezar, si bien es cierto que las alertas activadas por el botón de pánico son prioritarias, dependiendo del caso, se efectúa esta coordinación con los usuarios finales del software quienes son los teleoperadores que atienden las alertas y se adecuan según las reglas impuestas por el negocio o entidad que utilicen nuestro software desktop.

d) ¿Actualmente cómo se está identificando los delitos de las alertas?

En el sistema no hay funcionalidad que indique qué tipo de delito se está identificando la alerta durante o después de su debida atención. Por lo que usualmente dejamos que el teleoperador resuelva las alertas con llamadas de servicio público y utilicen más la alerta como informativo.

e) En cuanto al tiempo de respuesta, ¿Cuánto demora la llegada de la alerta hacia el software desktop como promedio?
En promedio, el tiempo que llega la alerta al mapa del software desktop es muy relativo, aunque mientras haya más alertas entrando al mapa de monitoreo, suele aumentar el tiempo de llegada de la alerta. La última vez tuvimos un reporte del usuario final indicando que se demoró como unos 8 segundos para que la alerta aparezca en todas las pantallas de los teleoperadores.

f) ¿Usualmente cuánto tiempo demora el software desktop en asignar la incidencia a un teleoperador?
No tenemos incorporado la funcionalidad de asignación de alertas a los usuarios teleoperadores; más bien, esto se desarrollará en el nuevo proyecto.

g) ¿Qué información les parece relevante acerca de la toma de decisiones sobre la seguridad ciudadana?
Tenemos opiniones acerca de que la información de los reportes es muy básica como para recolectar al detalle toda información acerca de los delitos y alertas. Para el nuevo proyecto se están solicitando métricas que ayuden a tomar mejores decisiones a los interesados, incluso para nosotros.

h) ¿Cuáles son los actuales desafíos que expone el software desktop?
Según el TDR (Documento de Término de Referencia) que hemos planificado estos meses, es que se desea optimizar la atención de las alertas con un sistema web que facilite al usuario durante el monitoreo de las alertas, puesto que tenemos muchos impedimentos al tener un software desktop, como por ejemplo la demora de la llegada de las alertas o de la reportería de las alertas.

Para el ingeniero técnico, las preguntas contestadas fueron las siguientes:

a) ¿Cuál es el propósito de los equipos de alarma “FGS10”?
   Las alarmas sirven como herramientas para detectar algún tipo de incidencia en el lugar e indicar la procedencia en el mapa de monitoreo. Es una tecnología que nosotros tenemos en nuestras manos y que quisiéramos utilizar como medio de advertencia en el monitoreo de las alertas.

b) ¿Tienen algún control de información acerca de los equipos de alarmas?
   Actualmente no manejamos ningún Excel o documento que ordene esa información, aunque nos gustaría tener alguno para poder guardarlas en una base de datos y utilizarlas para el control de ciertos eventos que provee el equipo “FGS10”.

c) ¿El software actual está diseñado para una gran cantidad de alertas entrantes al mapa de monitoreo?
   Si con diseño te refieres a que, si soporta muchas alertas en el mapa de monitoreo, entonces si lo hace. Aunque a veces suele demorar bastante por la gran carga de alertas entrantes al desktop. El tráfico de peticiones incluso llega a demorarse tanto que algunas alertas no llegan al mapa de monitoreo, por lo que en esos casos aún lo tenemos pendiente a resolver.

d) En el caso que el servidor de la central se caiga o tenga fallos técnicos, ¿Cuánto tiempo tardaría aproximadamente en estabilizar el servidor?
   Si te refieres al Router, no nos demoramos casi nada en resolverlo, puesto que vamos presencialmente a revisarlo; sin embargo, durante la inspección, se pierden las alertas entrantes de la aplicación “Vecino”. En cuanto a los equipos “FGS10” recogemos el equipo desinstalando de su ubicación y llevándonos a su respectiva revisión. En cuanto Firebase, tenemos problemas en renovar cada cierto tiempo la cuenta original donde está almacenada la base de datos y las imágenes, ya que es muy molesto realizarlo.

e) ¿Dónde se están almacenando las imágenes capturadas por los vecinos?

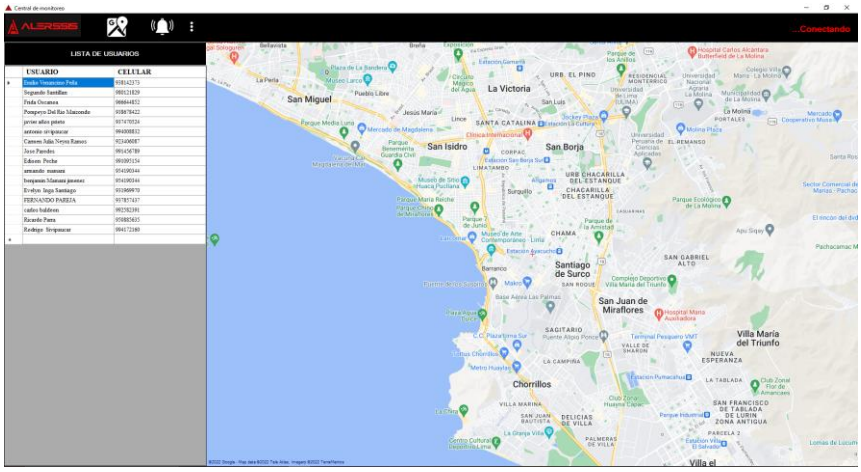
En la plataforma Firebase, en un servicio donde se almacenan las imágenes con una cuenta que manejamos.

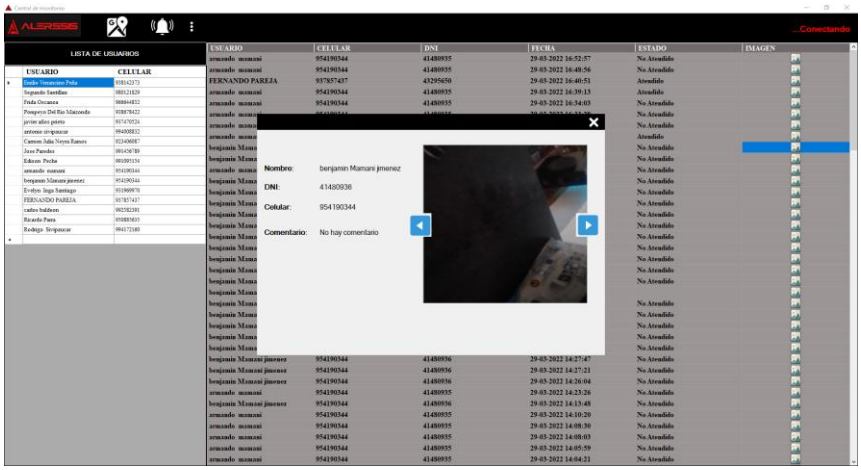
f) ¿Cuáles son los actuales desafíos que exponen las aplicaciones activas de la empresa a nivel de infraestructura o de hardware?

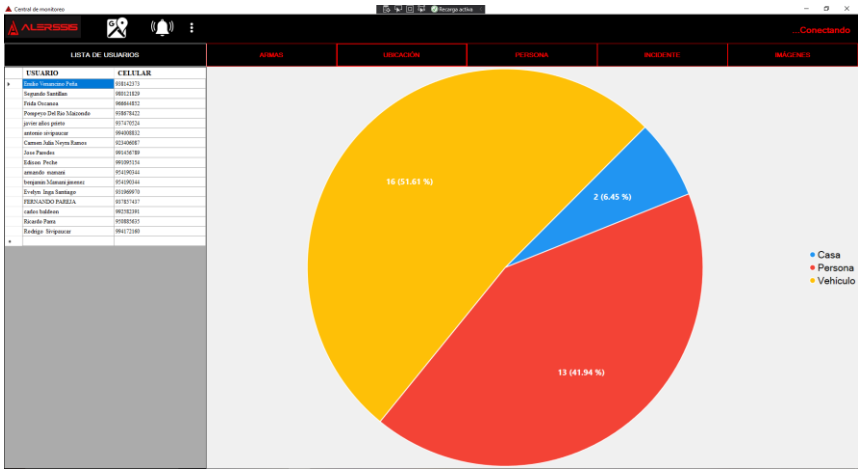
A nivel de infraestructura se requiere la disponibilidad de la información de las alertas en caso que haya problemas con el servidor o por parte del Router que envían estas alertas al mapa de monitoreo; si resolvemos esto, podemos integrar cualquier aplicación que tengamos al sistema web. Además de que tengamos la facilidad de saber la estabilidad del servidor y de su acceso, cosa que no nos demoremos mucho en resolver conflictos de red o de las aplicaciones.

Sistema de Monitoreo de Alertas del Software Desktop

La empresa FIRINGS E.I.R.L nos brindó el código fuente del software desktop para entender con mayor precisión el funcionamiento de cada módulo presentado en el programa; así mismo, con la garantía de la conexión remota con la base de datos del Firebase.






Central de monitoreo
Recarga activa
...Conectando
LISTA DE USUARIOS
ARMAS
UBICACIÓN
PERSONA
INCIDENTE
IMÁGENES
USUARIO
CELULAR
16 (51.61 %)
2 (6.45 %)
13 (41.94 %)
Casa
Persona
Vehiculo

Resultado del Proceso de Monitoreo del Software Desktop

Se tuvo la oportunidad de presenciar la instalación del equipo de alarma "FGS10" en el poste de una calle por "La Molina". En ella, como ejemplo, se aprecia, aparte de la videovigilancia instalada, los megáfonos que son parte de la estrategia del uso del equipo de alarma y el equipo instalado en la parte inferior del poste.

El planteamiento de la instalación del equipo "FGS10" en un poste proviene de la idea del gerente general, por lo que actualmente se está aplicando en la práctica esta estrategia.

Por lo tanto, una vez que se active esta alarma, enviará una alarma en el mapa de monitoreo del software desktop, indicando que la alarma ha activado su sirena; dependiendo del tipo de telealarma que sea.

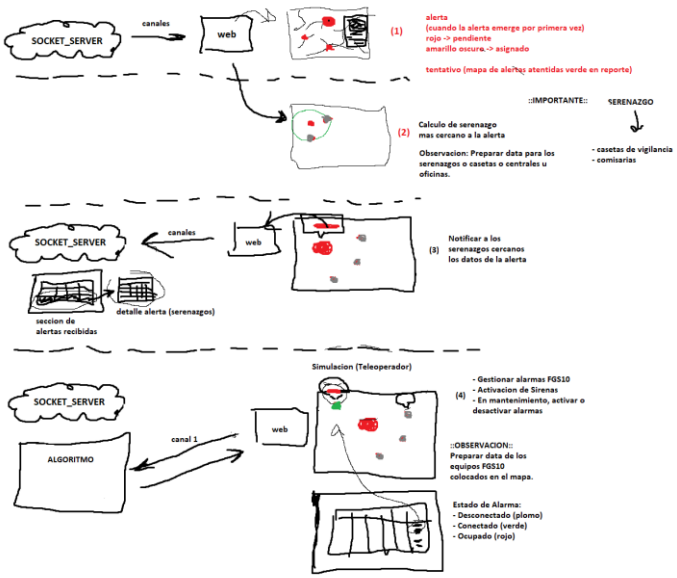
Según la base de datos de Firebase, indica que de 800 alertas mensuales que fueron capturadas en el mapa de monitoreo y guardadas en la base de datos, son 800 el total de alertas que son consideradas como “atendidas”. Así que, utilizando la siguiente fórmula brindada por el ingeniero técnico, se podrá determinar el porcentaje de delitos identificados con la cantidad de delitos reportados por el botón de pánico entre el total de alertas mensuales.

(DR * 100) / TAM = PDI

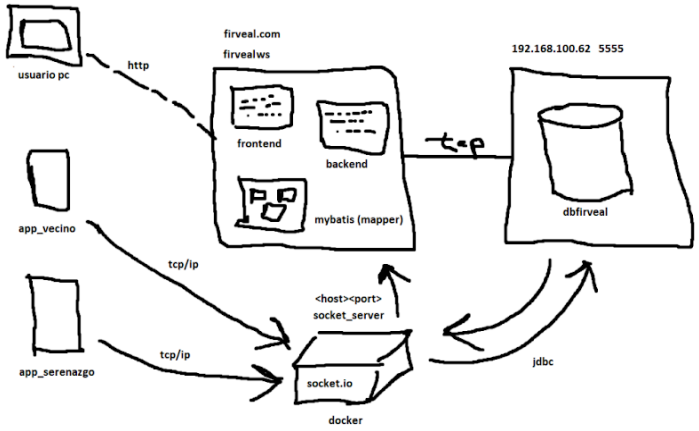
TAM = Total de Alertas Mensual (800 alertas)
DR = Delitos Reportados (800 alertas consideradas)
PDI = Porcentaje de Delitos Identificados (100%)

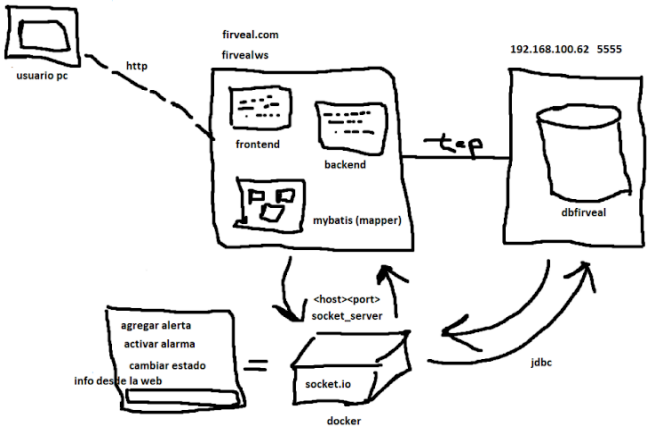
Como resultado, se obtendría un porcentaje de 100.00% de alertas reportadas como delitos durante un mes promedio en producción con el software desktop. Teniendo esto en cuenta, debemos mejorar este resultado comparado con nuestra solución propuesta para la identificación de delitos.

También se ha diagramado en forma de boceto lo planificado para el nuevo proyecto de FIRINGS E.I.R.L. junto con el ingeniero técnico y el gerente general, en donde se aprecia por un lado los procesos que conlleva el monitoreo en la implementación de un posible sistema web y la infraestructura sugerida.



Cabe resaltar, que estas ideas no estuvieron completas en la forma inicial del proyecto, pero gran parte de ellas fueron consideradas para la investigación y para el desarrollo de la variable independiente.


usuario pc
http
firveal.com
firvealws
frontend
backend
mybatis (mapper)
192.168.100.62 5555
dbfirveal
tcp
app_vecino
tcp/ip
app_serenazgo
tcp/ip
<host><port>
socket_server
socket.io
docker
jdbc


usuario pc
http
firveal.com
firvealws
frontend
backend
mybatis (mapper)
192.168.100.62 5555
dbfirveal
tcp
agregar alerta
activar alarma
cambiar estado
info desde la web
=
<host><port>
socket_server
socket.io
docker
jdbc

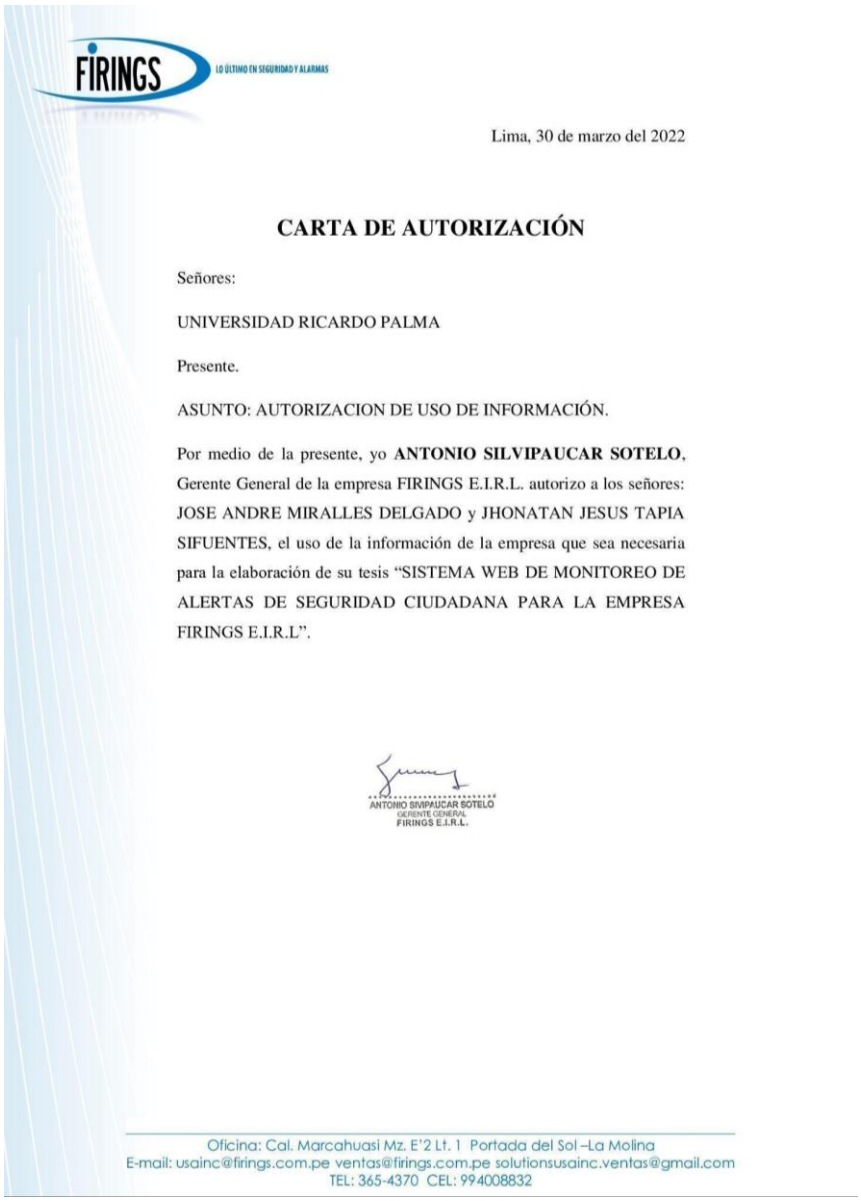
Anexo 2: Matriz de Operacionalización

Variable Dependiente	Definición Conceptual	Definición Operacional	Dimensiones	Indicador Instrumento	Ítem
Seguridad Ciudadana	La presente investigación se asienta sobre una metodología cualitativa que permita explorar las complejas acciones y reacciones vecinales en la construcción de los mecanismos locales de prevención. Según Mollericona; Tinini y Paredes (2007, P. X) explican sobre la seguridad pública a partir de la autogestión local. Sobre la "terciarización" de la seguridad ciudadana y, por otro, la "colectivización de la seguridad".	La seguridad ciudadana se evaluará tomando en cuenta la percepción, gestión local y reacción ciudadana; considerando para ello los delitos, la disposición de la vigilancia y la prevención de la inseguridad.	Percepción de la Seguridad	Indicador: Delitos Técnica: Fichaje Instrumento: Ficha de Registro de Delitos	PHM * PD = MI PHM: Promedio Histórico Mensual PDI: Porcentaje Determinado MI: Muestra de la Investigación
			Gestión Local de la Seguridad	Indicador: Disposición de la vigilancia Técnica: Entrevista Instrumento: Cuestionario	Entrevista con el gerente general y el ingeniero. Ver en Anexo 1.
			Reacción ciudadana	Indicador: Prevención de la inseguridad Técnica: Observación Instrumento: Cuaderno de notas	Resultado del Proceso de Monitoreo del Software Desktop

Anexo 3: Matriz de Consistencia

Problemas Principales	Objetivos Generales	Hipótesis General	Variables Independientes	Variables Dependientes	Indicador V.D.
¿Cómo influye la implementación de un sistema web de monitoreo de alertas de seguridad ciudadana en el área de informática de la empresa FIRINGS E.I.R.L. 2021-2022?	Determinar cómo influye la implementación de un sistema web de monitoreo de alertas de seguridad ciudadana en el área de informática de la empresa FIRINGS E.I.R.L. 2021-2022.	La implementación de un sistema web de monitoreo de alertas de seguridad ciudadana influye positivamente en el área de informática de la empresa FIRINGS E.I.R.L. 2021-2022.	Sistema Web	Seguridad Ciudadana	Delitos Disposición de la vigilancia Prevención de la Inseguridad
Problemas Específicos	Objetivos Específicos	Hipótesis Específicas			
P1: ¿Cómo influye la implementación de un sistema web de monitoreo de alertas de seguridad ciudadana en el área de informática de la empresa FIRINGS E.I.R.L. 2021-2022 en la identificación de los delitos?	OE1: Determinar cómo influye la implementación de un sistema web de monitoreo de alertas de seguridad ciudadana en el área de informática de la empresa FIRINGS E.I.R.L 2021-2022 en la identificación de los delitos.	HE1: La implementación de un sistema web de monitoreo de alertas de seguridad ciudadana en el área de informática de la empresa FIRINGS E.I.R.L. 2021-2022 influye positivamente en la identificación de los delitos.			
P2: ¿Cómo influye la implementación de un sistema web de alertas vecinales de seguridad ciudadana en el área de informática de la empresa FIRINGS E.I.R.L. 2021-2022 en la disposición de la vigilancia?	OE2: Determinar cómo influye la implementación de un sistema web de monitoreo de alertas de seguridad ciudadana en el área de informática de la empresa FIRINGS E.I.R.L 2021-2022 en la disposición de la vigilancia.	HE2: La implementación de un sistema web de monitoreo de alertas de seguridad ciudadana en el área de informática de la empresa FIRINGS E.I.R.L. 2021-2022 influye positivamente en la disposición de la vigilancia.			
P3: ¿Cómo influye la implementación de un sistema web de monitoreo de alertas de seguridad ciudadana en el área de informática de la empresa FIRINGS E.I.R.L. 2021-2022 en la prevención de la inseguridad?	OE3: Determinar cómo influye la implementación de un sistema web de monitoreo de alertas de seguridad ciudadana en el área de informática de la empresa FIRINGS E.I.R.L 2021-2022 en la prevención de la inseguridad.	HE3: La implementación de un sistema web de monitoreo de alertas de seguridad ciudadana en el área de informática de la empresa FIRINGS E.I.R.L. 2021-2022 influye positivamente en la prevención de la inseguridad.			

Anexo 4: Carta de aprobación de la empresa



FIRINGS
LO ÚLTIMO EN SEGURIDAD Y ALARMAS

Lima, 30 de marzo del 2022

CARTA DE AUTORIZACIÓN

Señores:

UNIVERSIDAD RICARDO PALMA

Presente.

ASUNTO: AUTORIZACION DE USO DE INFORMACIÓN.

Por medio de la presente, yo **ANTONIO SILVIPAUCAR SOTELO**, Gerente General de la empresa FIRINGS E.I.R.L. autorizo a los señores: JOSE ANDRE MIRALLES DELGADO y JHONATAN JESUS TAPIA SIFUENTES, el uso de la información de la empresa que sea necesaria para la elaboración de su tesis "SISTEMA WEB DE MONITOREO DE ALERTAS DE SEGURIDAD CIUDADANA PARA LA EMPRESA FIRINGS E.I.R.L".

ANTONIO SILVIPAUCAR SOTELO
GERENTE GENERAL
FIRINGS E.I.R.L.

Oficina: Cal. Marcahuasi Mz. E'2 Lt. 1 Portada del Sol –La Molina
E-mail: usainc@firings.com.pe ventas@firings.com.pe solutionsusainc.ventas@gmail.com
TEL: 365-4370 CEL: 994008832

Anexo 5: Acta de Confidencialidad

FIRINGS
LO ÚLTIMO EN SEGURIDAD Y ALARMAS

Lima, 01 de abril del 2022

ACTA DE CONFIDENCIALIDAD

A QUIEN CORRESPONDA.
Presente.

Por medio de la presente, JOSE ANDRÉ MIRALLES DELGADO y JHONATAN JESÚS TAPIA SIFUENTES nos comprometemos a no divulgar la información de tipo confidencial de manera verbal o escrita de la empresa FIRINGS E.I.R.L. con domicilio fiscal en Calle Marcahuasi Mz. E Lt. 1 Urb. Portada del Sol - La Molina, Lima, Perú.

Dicha información incluye:

- Datos personales de los clientes y trabajadores de la empresa.
- Información relacionada con los procedimientos, prácticas y políticas internas de la empresa.
- Información relacionada con la base de datos.

En caso de que FIRINGS E.I.R.L. detectara que estamos haciendo del conocimiento de terceros cualquier información relacionada con los términos antes expuesto, nos haremos acreedores a la sanción administrativa o legal que la empresa considere conveniente.

Jhonatan Tapia Sifuentes

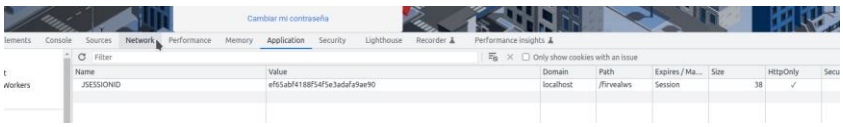
Jose Miralles Delgado

Oficina: Cal. Marcahuasi Mz. E'2 Lt. 1 Portada del Sol –La Molina
E-mail: usainc@firings.com.pe ventas@firings.com.pe solutionsusainc.ventas@gmail.com
TEL: 365-4370 CEL: 994008832

Anexo 6: Aseguramiento de calidad ante pruebas de seguridad y de estrés

En el caso de pruebas de seguridad, cada vez que el usuario no mantiene la sesión activa, se le considera como inactividad sobre el sistema web, provocando el redireccionamiento al interfaz de inicio sesión; con el fin de capturar todas las sesiones inactivas de los usuarios durante el proceso de monitoreo de alertas.

En referencia a las pruebas de seguridad, la autenticidad del usuario se asegura bajo el uso de tokens encriptados en cada sesión abierta. De esa forma, es más flexible el manejo de sesiones en cualquier navegador.



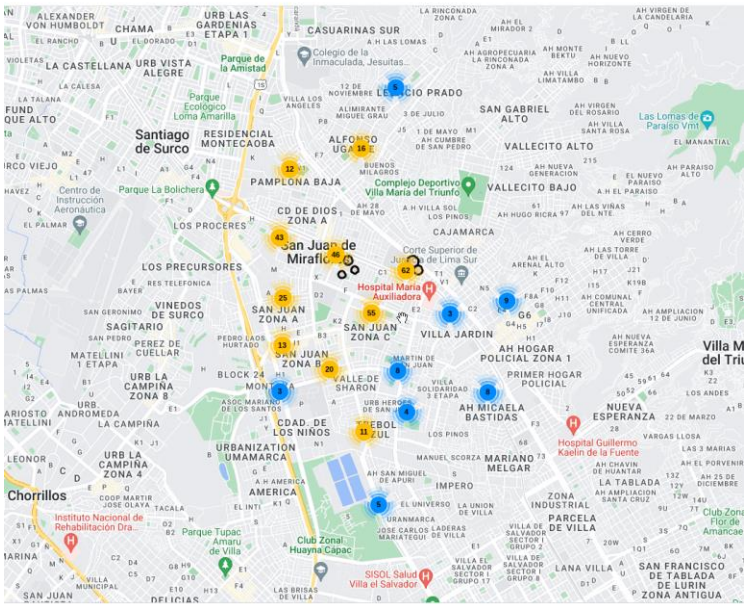
En cuanto a las pruebas de estrés, se debe mencionar la siguiente problemática anteriormente indicada por el gerente general:

En el Software Desktop:

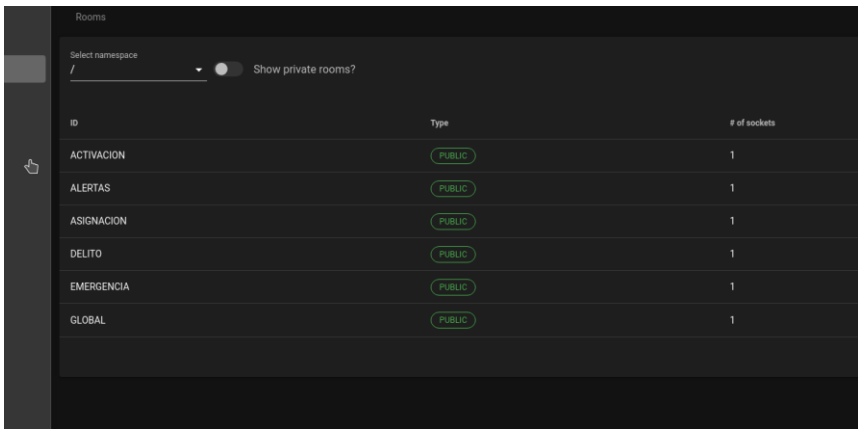
- 8 segundos para aparecer la alerta a todos los teleoperadores.

Entonces, considerando la masividad de alertas enviadas al mapa de monitoreo de nuestro sistema web “Firveal”, se obtiene una respuesta no mayor a 3 segundos en promedio por cada envío de alerta. Adicionalmente, no solamente el envío de alertas sería la única

actividad que el sistema estaría procesando durante el monitoreo, también se tiene en consideración que está procesando en tiempo real la asignación de teleoperadores sobre las alertas, la activación de sirenas y la asignación de los delitos.

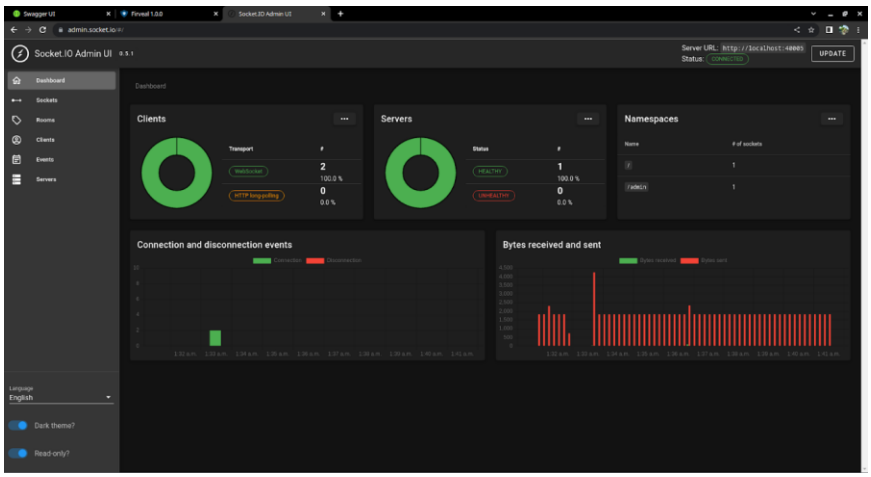


Finalmente, como evidencia, se registra en el socket los canales publicados de cada actividad para el monitoreo de alertas.



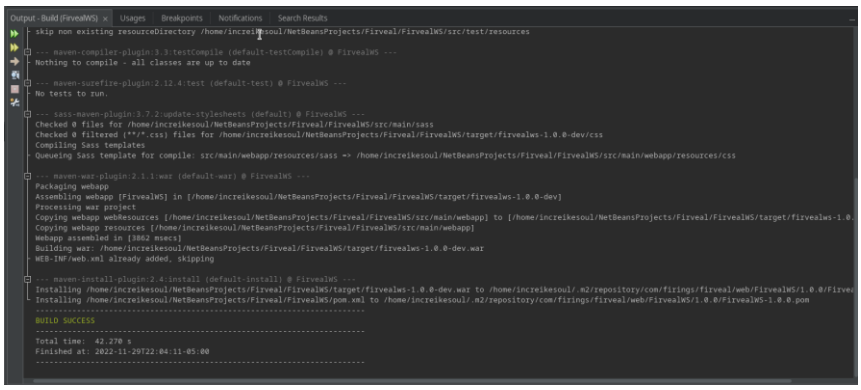
Anexo 7: Uso del dashboard del “Socket.io Admin UI”

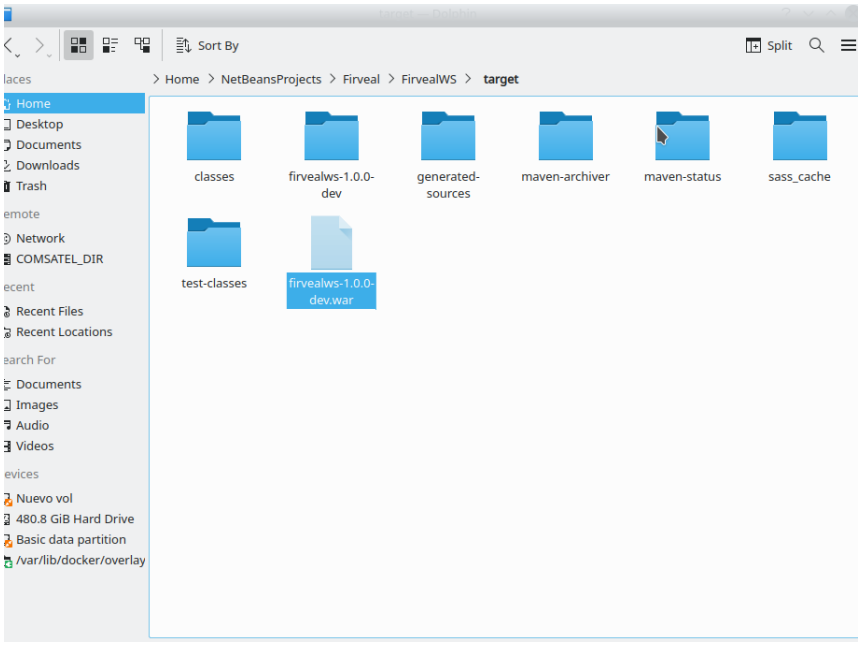
Se presenta una forma más dinámica y fácil de lectura en cuanto al control administrativo del websocket, un dashboard integrado cuya tecnología es compatible con los componentes utilizados en el socket. En ello, tiene bondades referentes a métricas, control de canales, control de eventos, gestión de clientes y gestión del servidor. A su vez, viendo en tiempo real la conectividad del websocket con las aplicaciones involucradas.



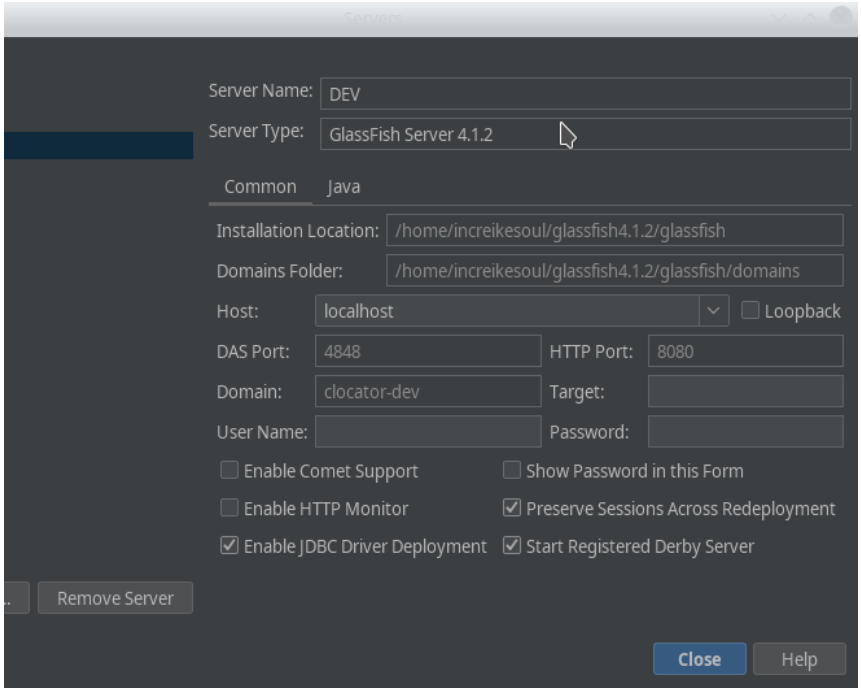
Anexo 8: Manual de Instalación

Se presenta el manual de instalación de los componentes del software; tanto el sistema web que es la aplicación Core de la solución, como el websocket. En primer lugar, el despliegue del sistema web requiere de un ejecutable generado por el distribuidor “Maven”, puesto que necesitamos que en este ejecutable contenga todas las dependencias requeridas por el proyecto web con el paquete de JDK 1.8.





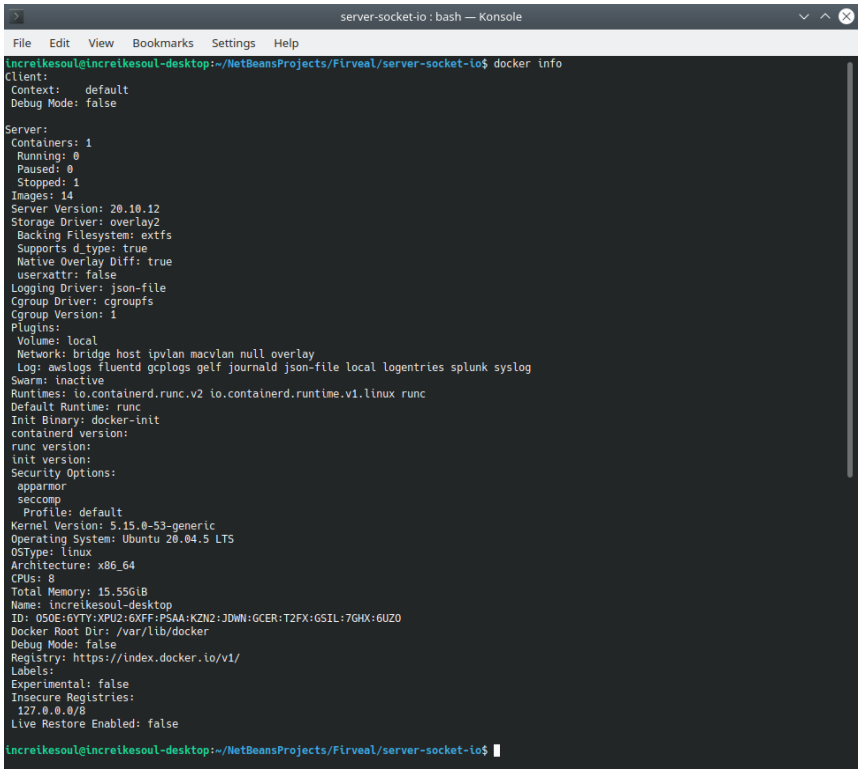
Además, debemos asegurar que la calidad de código esté correcta ante cualquier posible error de sintaxis o relacionado a ello; de lo contrario, ocasionará un conjunto de errores durante la construcción y el compilado del proyecto. Una vez hecho esto, se utilizará el ejecutable en un servidor web para su despliegue en algún host correspondiente, de preferencia: “Glassfish” de Sun Microsystems o “Tomcat” de Apache.



Otra configuración por mencionar es sobre el despliegue del websocket, cuyo componente también es considerado como “middleware”, es el encargado de conectar la comunicación bidireccional entre el mismo y el sistema web. Su instalación es un poco difícil de realizar, pero daremos un seguimiento detallado del cómo exponer sus servicios y la creación de sus canales.

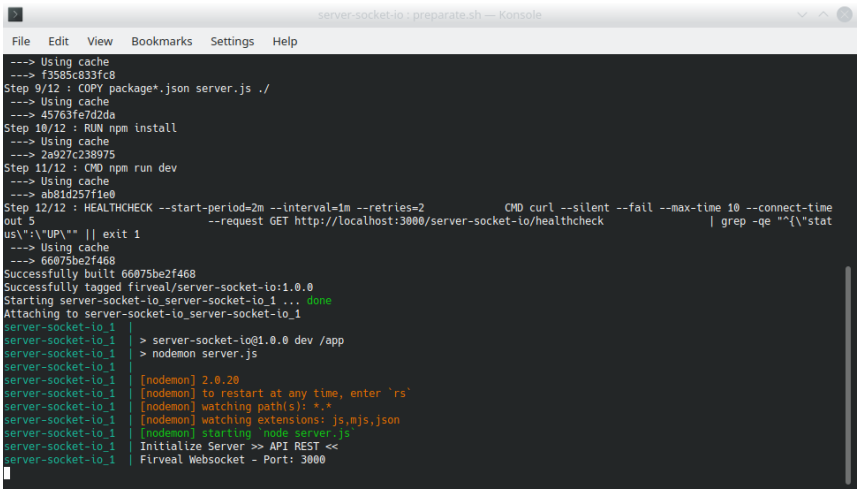
Lo primero que hay que hacer es utilizar el host que nos corresponda configurar, e instalar el Docker para la creación de contenedores. Dependiendo del sistema operativo que utilicemos, puede variar en gran medida la complejidad de configuración que requiera al instalar este componente, en especial cuando la capacidad de los recursos que tenga el sistema operativo sea limitada y difiera mucho en la decisión de ajustar ciertos parámetros

para las instalaciones solicitadas. En nuestro caso, el sistema operativo que utilizamos es la versión de Kubuntu 22.04 LTS del distribuidor Kernel Linux.

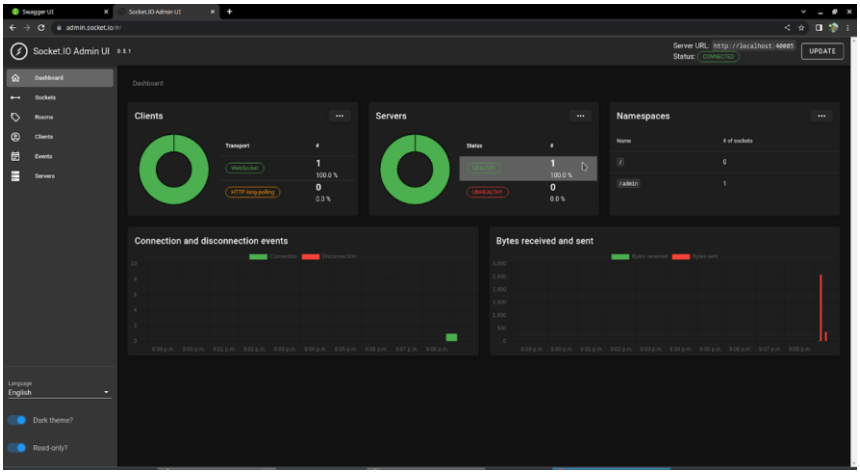


El siguiente paso es ejecutar unos comandos preparados para la ejecución de los siguientes procesos:

- Reconstrucción del proyecto websocket compilado
- Generación de la imagen Docker
- Creación del contenedor
- Instanciación del websocket en su respectivo contenedor.
- Exposición de puertos



Finalmente, tendríamos desplegado el websocket y el sistema web por completo. Como mención importante, se debe verificar si el healing del servidor está operativo para cualquier petición externo del websocket y si los canales han sido creados exitosamente; para ello, se utilizaría el “Admin UI” del websocket, cuya utilidad nos da la garantía de conocer información relevante del socket y su actual status.

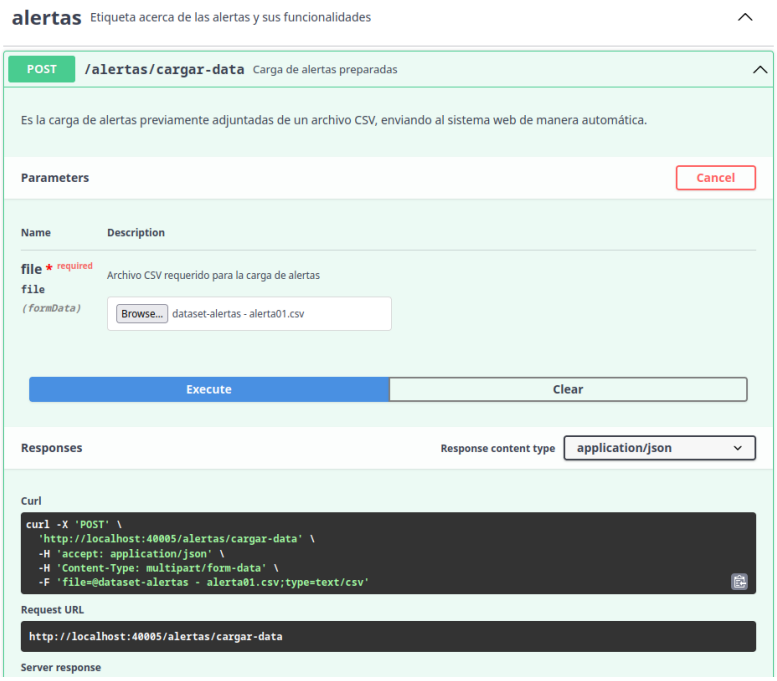


Anexo 9: Manual de Usuario

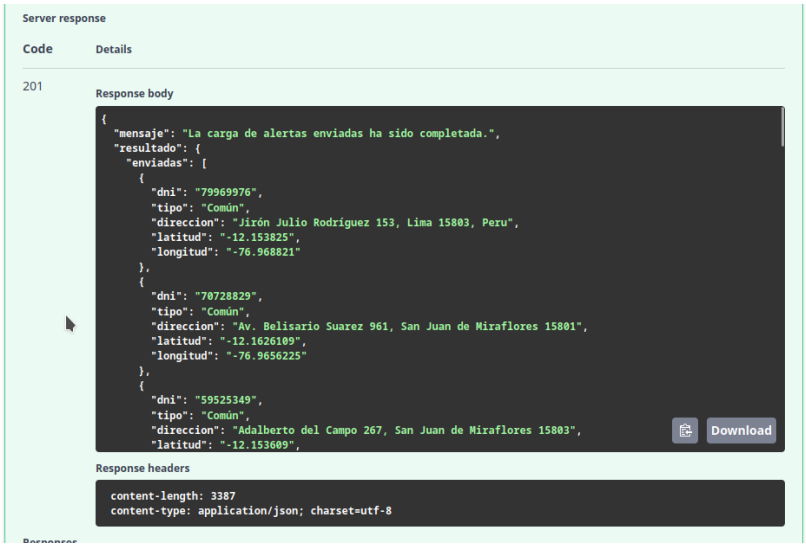
En este informe se estará mencionando cada una de las bondades que brinda el software “Firveal” con la finalidad de guiar al usuario las tareas que debe realizar durante el proceso de monitoreo y de atención.

1) Carga de alertas y envío de alertas

   Se visualizan dos servicios API preparados para la ejecución de una carga masiva de alertas para el envío asíncrono al sistema web. Y, por otro lado, un servicio que se utilizará para el envío de alertas desde algún consumo externo.



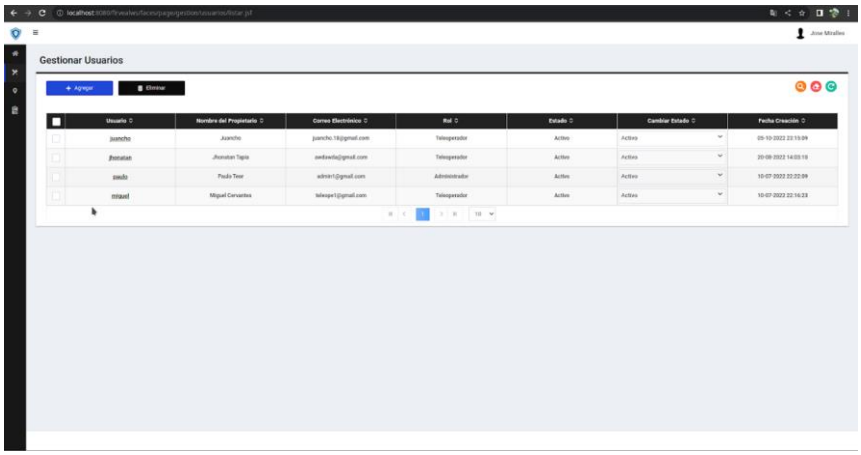
   Se debe adjuntar un archivo preparado cuya plantilla será enviada al gerente encargado del software, en esta plantilla incluye: Datos del vecino, Datos de la alerta y la ubicación de la alerta. Luego de adjuntar el archivo y de ejecutarlo, se procesará hasta completar todas las alertas cargadas al mapa de monitoreo; y una vez terminado, se mostrará las alertas enviadas y las alertas no enviadas.



2) Acceso al sistema web “Firveal”

El sistema permite al usuario acceder con credenciales registradas por el administrador, quien es el encargado de velar por toda la parte administrativa del sistema en general.

También se ha implementado un módulo para la gestión de usuarios para que puedan tener acceso al sistema, aportando un mayor manejo en la planificación del proceso de monitoreo y de atención con la creación de nuevos usuarios.



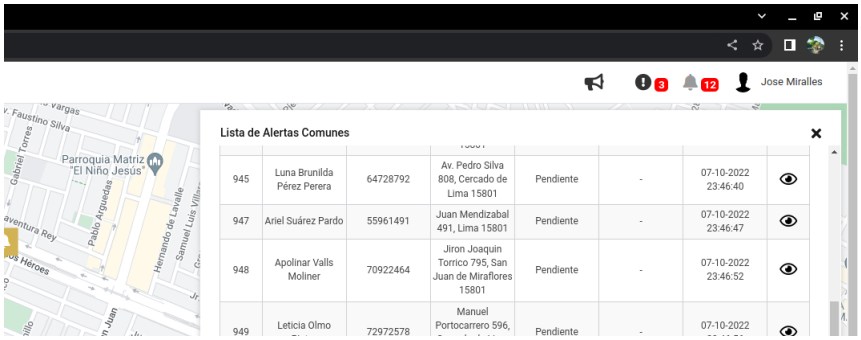
3) Mapa de Monitoreo y Atención de alertas

En el mapa se visualiza con el mayor panorama posible, todas las alertas pendientes emergiendo durante el monitoreo. El usuario quien sería el teleoperador, es el encargado de supervisar y atender las alertas comunes y de emergencia que aparezcan en el mapa de monitoreo.

Hay diferentes tipos de notificaciones de los cuales alertan al teleoperador cuando emerge una nueva alerta, entre ellas están:

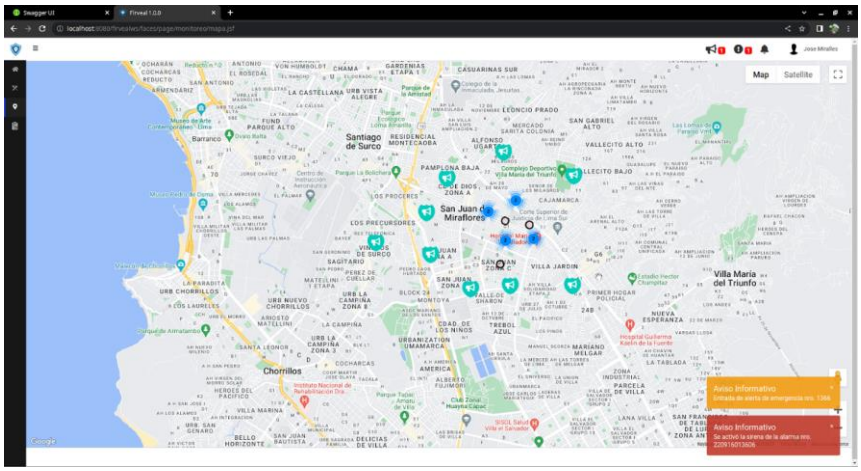
Las notificaciones del navegador superior

En el navegador superior, aparecen unos gadgets de iconos en el que cada uno representan respectivamente como notificaciones de alarmas, alertas comunes y alertas de emergencia; de las cuales cada una de ellas mostrarán su respectiva información.



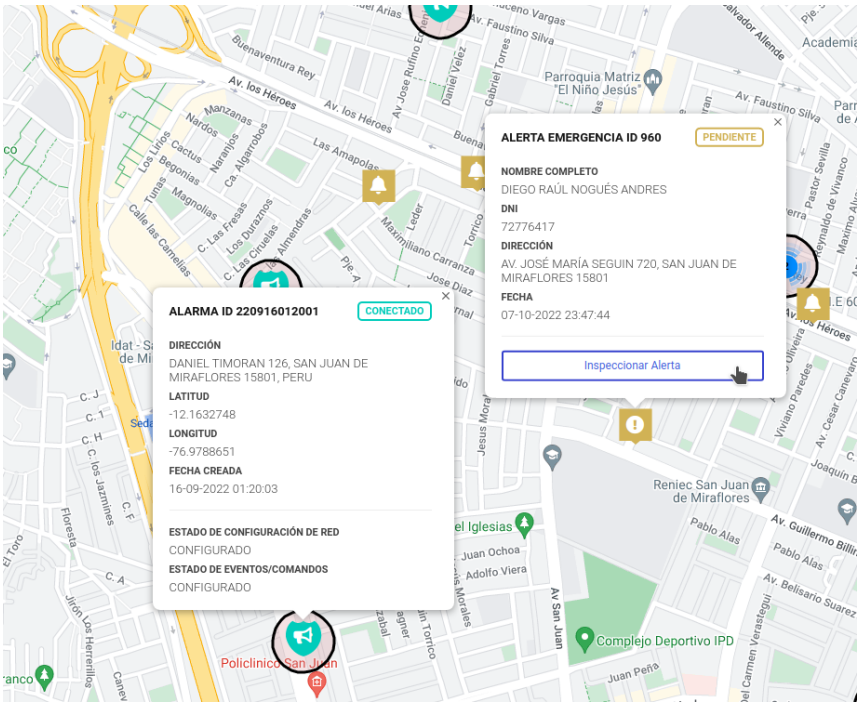
Las notificaciones de los PopUp

Otra de las formas de notificar al teleoperador al momento que emerge una alerta nueva, serían los PopUp informativos que salen en la esquina inferior derecha. Estos paneles mostrarán la información de la alerta nueva con un mensaje de alerta y acompañado con un sonido reconocible.

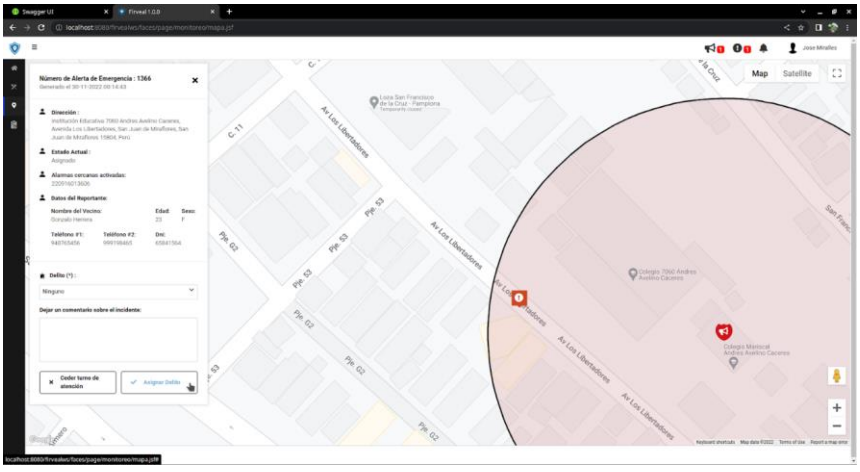


Las notificaciones en forma de apariciones en el mapa

Por último, durante el proceso de monitoreo, las alertas aparecerán en tiempo real en el mapa de monitoreo, notificando a todos los teleoperadores que se encuentren activos durante el instante. A su vez, se podrá ver en detalle la información relevante de la alerta para proceder a su debida atención.



Cuando el teleoperador procede a la atención de una alerta nueva, se abrirá un panel al lado izquierdo de la pantalla, detallando en relación a los datos de la alerta y del vecino. Por ende, el teleoperador tendrá el deber de atender, procediendo a seleccionar el tipo de delito al cual pertenece y un comentario para darle seguimiento al caso.



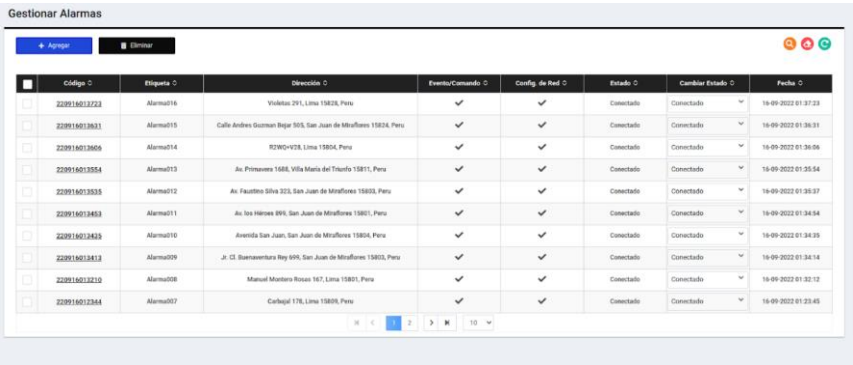
4) Generación de reportes de alertas y alarmas

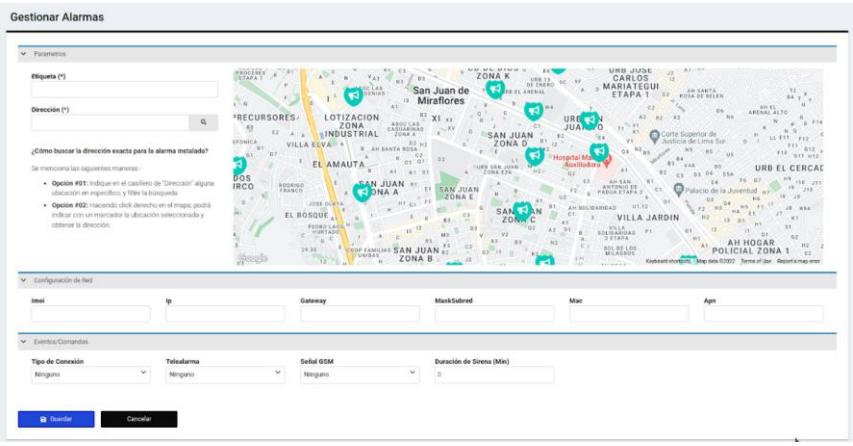
El sistema web “Firveal” también dispone un módulo de reportes para la consulta en caliente del resultado del proceso de monitoreo y atención de las alertas y las alarmas activas. En el caso de la reportería de las alertas, podrán seleccionar el tipo de reporte al cual se requiere saber, y según el tipo de alerta y un rango de fechas para situar el resultado.

Para el caso de la reportería de las alarmas, solo basta con seleccionar el tipo de reporte y según el rango de fechas para la generación del reporte.

5) Módulo de gestión de alarmas

El sistema web tendrá propiamente un módulo de gestión para las alarmas que estarían recién ingresando a la empresa o aquella que están listas para la activación de la sirena. Desarrollado para que el administrador, dado a su criterio, pueda gestionar la información que contenga de ellas como, por ejemplo: La ubicación de la alarma, la configuración de eventos o de su instalación.


Gestionar Alarmas
+ Agregar
Eliminar
Código
Etiqueta
Dirección
Evento/Comando
Config. de Red
Estado
Cambiar Estado
Fecha
220916013723 Alarma016 Violetas 291, Lima 15838, Peru Conectado 16-09-2022 01:37:23
220916013631 Alarma015 Calle Andres Guzman Bejar 505, San Juan de Miraflores 15824, Peru Conectado 16-09-2022 01:36:31
220916013606 Alarma014 R2WQ+V28, Lima 15804, Peru Conectado 16-09-2022 01:36:06
220916013554 Alarma013 Av. Primavera 1688, Villa María del Triunfo 15811, Peru Conectado 16-09-2022 01:35:54
220916013535 Alarma012 Av. Faustino Silva 323, San Juan de Miraflores 15803, Peru Conectado 16-09-2022 01:35:37
220916013453 Alarma011 Av. los Héroes 899, San Juan de Miraflores 15801, Peru Conectado 16-09-2022 01:34:54
220916012425 Alarma010 Avenida San Juan, San Juan de Miraflores 15804, Peru Conectado 16-09-2022 01:34:35
220916013413 Alarma009 Jr. Cl. Buenaventura Rey 699, San Juan de Miraflores 15803, Peru Conectado 16-09-2022 01:34:14
220916013210 Alarma008 Manuel Montero Rosas 167, Lima 15801, Peru Conectado 16-09-2022 01:32:12
220916012344 Alarma007 Carbajal 178, Lima 15809, Peru Conectado 16-09-2022 01:23:45


Gestionar Alarmas
Parametros
Etiqueta (*)
Dirección (*)
¿Cómo buscar la dirección exacta para la alarma instalada?
Configuración de Red
Imei
Ip
Gateway
MaskSubred
Mac
Apn
Eventos/Comandos
Tipo de Conexión
Ninguno
Telealarma
Ninguno
Señal GSM
Ninguno
Duración de Sirena (Min)
Guardar
Cancelar