Prototipo de plataforma digital para la gestión de incidentes en la infraestructura *on premise* de una *fintech* en Colombia

Yuli Paola Vargas Rodríguez

Universidad EAN
Facultad de Ingeniería
Ingeniería de Sistemas
Medellín, Colombia
10/12/2024

Prototipo de plataforma digital para la gestión de incidentes en la infraestructura *on premise* de una *fintech* en Colombia

Yuli Paola Vargas Rodríguez

Trabajo de grado presentado como requisito para optar al título de:
Ingeniera de Sistemas

Director:
Álvaro David Arévalo Salazar

Modalidad:
Monografía

Universidad EAN
Facultad de Ingeniería
Ingeniería de Sistemas
Medellín, Colombia
10/12/2024

Tabla de contenido

Tablas

Tabla de Ilustraciones

Resumen

La digitalización de procesos cotidianos como lo son el pago de facturas, hacer transacciones monetarias, recibir transferencias, entre otros, son resultado de la concentración de esfuerzos enfocados en el diseño de productos y servicios atractivos para toda la población. En este contexto, las fintech juegan un papel definitivo en la actualidad y en este orden, su continuo monitoreo para identificar y solucionar oportunamente posibles fallas en sus servicios e infraestructura. Es por esto que el presente proyecto tiene como objetivo el diseño de un prototipo web que centralice las alertas y trazas del monitoreo, la infraestructura y los servicios, de una colombiana, para aportar a la optimización de sistemas de monitoreo y mejorar la capacidad de acción de los equipos resolutores de incidentes críticos que afectan al usuario final. Para ellos se empleará un enfoque exploratorio, ya que se espera dimensionar la solución a un problema, para el estudio de caso del problema evidenciado en una fintech particular, pero en el futuro puede ser aplicado a otras corporaciones del mismo tipo. Por lo que se espera que los resultados de esta investigación son significativos, aporten a las opciones para desarrollar herramientas que optimicen la gestión de incidencias y mejoren la experiencia del cliente.

Palabras clave: monitoreo, Fintech, centralizar alertas, gestión de incidentes.

1. Introducción

Tras la incursión de la cuarta revolución industrial, ha sido notoria la transformación de procesos como la interacción de los consumidores con el sistema económico y sus instituciones bancarias. Al respecto, Daissy Rentería et. (2021), al se refieren a la incursión de las *fintech* (tecnología financiera), como una figura definitiva para suplir las demandas que están teniendo las corporaciones financieras en la actualidad, por parte de sus usuarios. Esta figura es entendida como: "la entrega de servicios financieros y bancarios a través de la innovación tecnológica moderna, incremental o disruptiva inducida por desarrollos de TI (tecnología de la información)." (Rentería et al., 2021, p. 18) En este orden, la digitalización de procesos financieros ha facilitado el acceso a productos y servicios como transferencias monetarias, pago de bienes, entre otros.

Sin embargo, las Fintech enfrentan desafíos relevantes debido que la transformación de sus procesos para la gestión de incidentes no se ha dado con la misma rapidez con que se ha migrado a herramientas tecnológicas más potentes sus productos y servicios, lo que limita la capacidad de respuesta de los grupos de monitoreo ante incidentes críticos, afectando la disponibilidad de los servicios de la compañía.

Investigaciones previas, dan cuenta de la relevancia que tiene hacer una observabilidad y monitoreo adecuados a los sistemas, pues de lo contrario se da lugar a largos tiempos de inactividad frente al cierre de vulnerabilidades o incidentes en los sistemas digitales de las Fintech, y esto finalmente se ve reflejado en la indisponibilidad de los canales de cara al cliente final. Esto resalta la relevancia que tiene la identificación y el desarrollo de nuevas herramientas que faciliten la gestión oportuna de incidentes.

Por lo anterior, este proyecto tiene como objetivo proponer una solución innovadora que optimice la respuesta y capacidad de acción de los grupos que realizan el monitoreo y la observabilidad en una *fintech*, mejorando así la eficiencia y la disponibilidad de sus servicios.

La relevancia de la presente investigación está dada por su potencial para contribuir en la consolidación de un ecosistema financiero más accesible y sólido, lo que resulta definitivo en una sociedad cada vez más digitalizada y mediada por soluciones tecnológicas. Por lo que en el presente documento, se presenta el planteamiento del problema, la pregunta de investigación, los objetivos, la justificación, seguido de la metodología empleada y los resultados esperados, finalizando con una discusión sobre las implicaciones de los hallazgos.

1.1. Definición del problema

La digitalización de los medios para adquirir productos o servicios de uso cotidiano, ha llevado a sectores como el financiero a la inclusión de procesos tecnológicos que anteriormente eran exclusivos y particulares al quehacer de las compañías tecnológicas. Las Fintech son ejemplo de las empresas que basan su oferta en innovadores productos y servicios financieros en soluciones tecnológicas, lo que les permiten tener sistemas más eficientes. (Rico Gómez, 2020)

Para 2021, de acuerdo a (Pérez Vásquez et al., 2023), " Colombia ocupa el tercer lugar en América Latina en términos de participación fintech, con un total de 279 empresas y un aumento del 39% en comparación con el año anterior." (p. 100) En este sentido (Areiza López et al., 2023), afirma que:

> La nueva industria Fintech, como lo señala la Superintendencia Financiera de Colombia, requiere de una gestión de riesgos acorde con las nuevas dinámicas del mercado debido a que algunas entidades han sido víctimas de incidentes cibernéticos, en general recibiendo millones de ataques trimestralmente. Se ha generado un aumento del 67% en las denuncias por delitos informáticos, los delitos de suplantación de identidad en línea han aumentado en un 602% y las transferencias no consentidas de activos en un 99%. (p. 2295)

Dado el impacto y la proyección de este sector, la gestión de posibles escenarios en los que haya fallas que afecten a los usuarios finales se da a través de procesos definidos por las compañías, basados en las normas internacionales ISO. Para el caso colombiano, la norma ISO 31000 define la gestión de riesgos en todas las actividades de una empresa, lo que incluye la implementación, evaluación, integración, diseño y mejora de la gestión de riesgos. Lo que demanda la aplicación de políticas, procedimientos y prácticas para la supervisión, revisión, consulta, evaluación, tratamiento, registro y notificación del riesgo. (ISO 31000, n.d.)

Ahora bien, esto implica para las *fintech* tener departamentos dedicados al soporte de los servicios de forma ininterrumpida dada su criticidad de cara a sus clientes finales: el costo del tiempo de inactividad y de las horas no productivas de los usuarios cuestan millones en

cada período anual, lo que indirectamente supone enormes pérdidas para las compañías. (Help Net Security, 2020)

De la necesidad que supone la alta disponibilidad surgen los departamentos especializados en las áreas de la infraestructura que posibilitan la continua disponibilidad de los servicios y la pronta resolución de incidentes cuando ocurren degradaciones. Al estar centralizados los departamentos, ofrecen la posibilidad de solventar cualquier incidencia que pueda surgir, además de gestionar las configuraciones y procedimientos necesarios para activar nuevamente los procesos que puedan tener inconvenientes. (Pérez Galán, 2023) Los departamentos especializados en las operaciones de redes o NOC (Network Operations Center) y SOC (Security operations center), son grupos especializados conformados por personal cualificado principalmente en tareas de administración de sistemas informáticos y, para el caso de las *fintech*, con conocimiento acerca del óptimo estado de los servicios y procesos (IBM, 2024), que soportan cada una de las aplicaciones y servicios transaccionales manejadas por la compañía.

Para realizar sus funciones los equipos requieren herramientas de monitoreo que les brinden información completa acerca del estado de las redes, la infraestructura, los servicios y demás procesos. Debido a que esta necesidad es transversal a las compañías de base tecnológica, en el mercado hay diversas soluciones de software enfocado en el monitoreo y la visualización de métricas, trazas, logs, entre otros, algunos de estos son: Grafana, Zabbix, Suricata, Nagios, Splunk, QRadar SolarWinds, ArcSight, Dynatrex, Wily, entre otros (Vázquez Pesado, 2020). El conjunto de estas soluciones brinda un monitoreo completo y robusto para los NOC y los SOC, a cargo de arquitecturas complejas y con una alta demanda de parte del usuario final, por lo que resulta necesario usar varias de ellas en simultaneo.
Al seleccionar herramientas de monitoreo de infraestructura se deben tener en cuenta factores como su funcionalidad, la practicidad de la interfaz de usuario, la generación de alertas, la integración con el centro de ayuda o *help desk* y la posibilidad de automatizar procesos e integrarse con otras herramientas. Para identificar la herramienta que mejor se ajuste a las necesidades del NOC, Hernantes et al., (2015) consideran:

> "a customizable alert service might be your best ally. When comparing systems, you might look at:
> • different alert methods (short message service [SMS], email, custom scripts, and so on),
> • the customization needed,
> • the supported OSs, and even
> • integration into your help desk system so that you can seamlessly integrate the monitoring system into your bug resolution processes." [un servicio de alerta personalizable puede ser su mejor aliado. A la hora de comparar sistemas, puede tener en cuenta:
> - diferentes métodos de alerta (servicio de mensajes cortos [SMS], correo electrónico, scripts personalizados, etc.),
> - la personalización necesaria,
> - los sistemas operativos compatibles, e incluso
> - la integración en su sistema de help desk para que pueda integrar perfectamente el sistema de supervisión en sus procesos de resolución de errores.] (p.89)

El autor menciona además que la herramienta debe ser compatible con la infraestructura, las capacidades del departamento de TI que hará uso de ella y los lenguajes de scripting o programación usados por la compañía; se deben tener en cuenta también los costos asociados al uso de aquellas que no son Open Source. Y, la herramienta debe ser flexible para permitir que la información nueva o adicional ayude a prever cualquier tendencia que pueda producirse en tiempo real.

Para el caso particular de la *fintech* de este caso de estudio, el problema radica en que la arquitectura, el monitoreo y la observabilidad del sistema financiero abordado, fue diseñada acorde a los recursos tecnológicos del momento, es decir, con infraestructura on premise y una escalabilidad reducida. Para el caso del monitoreo y la observabilidad, la actividad de los NOC y SOC se basa en la información obtenida por múltiples y complejas herramientas que si bien brindan detalles y precisión sobre lo que se monitorea, resulta ser demasiado e incluso redundante para los grupos de resolutores, lo que tiene incidencia en la disponibilidad de los servicios de cara al usuario final.

El escenario descrito representa un llamado a la generación de herramientas personalizadas acordes a los procesos de transformación digital y las necesidades de los NOC y

SOC, que permitan la gestión oportuna de los eventos e incidentes para mejorar la disponibilidad de los servicios y así reducir el impacto negativo en el negocio o servicio que se presta. Por lo anterior se plantea la siguiente pregunta de investigación:

Pregunta de investigación

¿Cómo desarrollar una plataforma que centralice los eventos e incidentes generados por diferentes herramientas de monitoreo, cumpliendo con los requerimientos del NOC de una *fintech* con amplio alcance en Colombia para 2024?"

1.2. Objetivos

Objetivo general

Diseñar el prototipo de una plataforma web que centralice las alertas generadas por las herramientas de monitoreo de una *fintech* en Colombia, cuyas funcionalidades se adecuen a las necesidades de los grupos de monitoreo que las gestionan.

Objetivos específicos

1. Diseñar la arquitectura, base de datos y diseño de *mockups* de la plataforma web, que den cuenta de la forma en que se incorporan los casos de uso y los requerimientos funcionales y no funcionales.

2. Definir las herramientas de programación, infraestructura y despliegue necesarios para desarrollar la plataforma, tras evaluar las restricciones al proyecto desde la mirada ambiental, económica, social y legal.

3. Validar el prototipo y sus funcionalidades con el líder técnico y *product owner* a cargo del monitoreo de las aplicaciones e infraestructura de la *fintech.*

1.3. Justificación

La relevancia y utilidad del proyecto presentado, se basa en la importancia de brindar información organizada, oportuna y analizada, en una plataforma que centralice la información vinculada al comportamiento de la infraestructura, que soporta los servicios de la fintech tomada como objeto de estudio, para así identificar estrategias técnicas que faciliten la mitigación de riesgos, agregando valor al servicio y herramientas para la gestión oportuna de incidencias. La iniciativa tiene una fuerte relevancia tecnológica, ya que busca optimizar la gestión de alertas en tiempo real, mejorando la eficiencia y seguridad operativa, mediante el el manejo de grandes volúmenes de datos y transacciones críticas, lo que facilita la priorización y respuesta ante incidentes.

Además, desde una perspectiva académica, el proyecto ofrece una oportunidad para explorar nuevas metodologías en la gestión de datos y la toma de decisiones automatizadas en el sector financiero. Tiene también un impacto social al contribuir a un ecosistema financiero digital más seguro y accesible, promoviendo la confianza de los usuarios en los productos y servicios de las compañía.

Desde la perspectiva económica, la mejora en la gestión de alertas puede reducir los costos asociados con fraudes y fallos operativos, aumentando la competitividad del sector y contribuyendo a la sostenibilidad y crecimiento de la industria fintech en Colombia. En conjunto, la solución ingenieril presentada es consecuente con la visión de la Universidad EAN, ya que no solo optimiza procesos tecnológicos, sino que también fortalece la seguridad y confiabilidad de los servicios financieros digitales, beneficiando tanto a empresas como a usuarios.

2. Análisis de requerimientos

2.1. Intención del Producto

El prototipo está enfocado en las necesidades del NOC y SOC de la fintech específica para mejorar la eficiencia frente a la gestión del monitoreo. Además de la obtención de datos, métricas, logs y demás que sean de utilidad para identificar tendencias. Se platea para ello el desarrollo de una plataforma que consuma los datos generados por diferentes herramientas de monitoreo para centralizar la generación de alertas y filtrar casos que se encuentren duplicados, sean falsos positivos y demás que produzcan ruido a los grupos de resolutores de alertas críticas.

2.2.Verificación de parámetros de diseño

El conjunto de normas ISO 25000 (SQRE – Requisitos y evaluación de calidad de sistemas y software) constituye el marco regulatorio internacional para la industria del desarrollo de software. Estos indican que los parámetros de diseño deben estar orientados a la calidad y, por lo tanto, deben cubrir las ocho características establecidas por ISO 25010 para las propiedades estáticas del software y dinámicas de los sistemas.

2.3.Diagnóstico actual

El protocolo para la identificación, escalamiento y gestión de alertas en el NOC y SOC de la Fintech particular funciona a partir de múltiples procesos y matrices de escalamiento que no se encuentran automatizadas, por lo que los agentes o resolutores deben acudir de manera simultánea a las herramientas de monitoreo vigentes, esto tiene consecuencias en los tiempos de acción frente a fallas masivas de cara al usuario final.

2.4.Prototipo de la plataforma

Con el objetivo de garantizar una interfaz intuitiva y fácil de usar, el prototipo simplificado de la plataforma para centralizar el monitoreo se basará en los principios de usabilidad, accesibilidad y experiencia del usuario identificados durante el proceso de diagnóstico.

2.5.Análisis de Factibilidad

Se realizará un estudio de la factibilidad técnica, financiera y ecológica del prototipo diseñado. Esto abarcará la valoración de los recursos requeridos para su puesta en marcha, además del posible impacto en cuanto a costos, ventajas y sostenibilidad ambiental.

3. Especificaciones del Producto

El análisis de requerimientos funcionales y no funcionales de la plataforma web, está basado y es conforme al estándar IEEE Std 830-1998.

3.1.Perspectiva

El producto que en este caso es una plataforma web hace parte de un sistema mayor al comprenderse como una herramienta adicional, para el grupo de monitoreo, que será gestionada por actores dentro de la organización, con variados roles.

3.2.Funcionalidad

El producto tiene como funcionalidad principal presentar el listado de alertas que se generan cuando la herramienta principal de monitoreo identifica que los umbrales, configurados para cada alerta, han sido superados. Este listado será filtrado por la herramienta para identificar posibles falsos positivos, casos repetidos, alertas erróneas, entre otros.

Características de los usuarios

Tabla 1.

Características de los usuarios

Tipo de usuario	Resolutor con conocimiento de uso de plataformas web y de los procesos para la gestión de alertas.
Formación	Ingeniero de sistemas/telecomunicaciones/electrónico
Habilidades	Capacidad de resolución de incidentes críticos.
Actividades	Dar gestión o delegar alertas críticas.

3.3.Restricciones

Los lenguajes de programación, frameworks, gestores de bases de datos, sistemas operativos, virtualizadores, entre otros, deben alinearse a las tecnologías que actualmente usa el cliente ya que la plataforma se integrará al ecosistema digital con el que trabaja en la actualidad el cliente para la resolución de incidentes en el grupo de monitoreo.

3.4. Evolución previsible del sistema

La integración con otras plataformas que puedan contener información sobre el servicio afectado o su grupo resolutor serán integradas en posteriores actualizaciones de la plataforma. De igual manera serán incluidos módulos adicionales con nuevas funcionalidades a solicitud del cliente.

4. Requisitos específicos

El nivel de detalle de los requisitos debe ser el suficiente para que el equipo de desarrollo pueda diseñar un sistema que satisfaga los requisitos y los encargados de las pruebas puedan determinar si éstos se satisfacen.

Tabla 2.

Requisito funcional 1

Número de requisito	RF1
Nombre de requisito	Almacenamiento en Base de datos de los eventos enviados por la herramienta de monitoreo Zabbix.
Tipo	☒ Requisito ☐ Restricción
Fuente del requisito	[Inserte aquí el texto]
Prioridad del requisito	☐ Alta/Esencial ☐ Media/Deseado ☐ Baja/ Opcional

Se requiere almacenar de forma temporal las alertas enviadas por Zabbix para posteriormente darles tratamiento y generar un ticket en caso de que se superen los umbrales definidos como críticos.

Tabla 3.

Requisito funcional 2

Número de requisito	RF2
Nombre de requisito	Procesamiento de alertas almacenadas en la Base de datos
Tipo	☒ Requisito ☐ Restricción
Fuente del requisito	Cliente
Prioridad del requisito	☒ Alta/Esencial ☐ Media/Deseado ☐ Baja/ Opcional

A través de un script se deben procesar las alertas para su posterior clasificación.

Tabla 4.

Requisito funcional 3

Número de requisito	RF2.1
Nombre de requisito	Clasificación de alertas con descripción duplicada.
Tipo	☒ Requisito ☐ Restricción
Fuente del requisito	Cliente
Prioridad del requisito	☒ Alta/Esencial ☐ Media/Deseado ☐ Baja/ Opcional

Tabla 5.

Requisito funcional 4

Número de requisito	RF2.2
Nombre de requisito	Clasificación de alertas suprimida/irrelevante.
Tipo	☒ Requisito ☐ Restricción
Fuente del requisito	Cliente
Prioridad del requisito	☒ Alta/Esencial ☐ Media/Deseado ☐ Baja/ Opcional

Tabla 6.

Requisito funcional 5

Número de requisito	RF 2.3
Nombre de requisito	Clasificación de alertas por falso positivo
Tipo	☒ Requisito ☐ Restricción
Fuente del requisito	Cliente
Prioridad del requisito	☒ Alta/Esencial ☐ Media/Deseado ☐ Baja/ Opcional

Tabla 7.

Requisito funcional 6

Número de requisito	RF 2.4
Nombre de requisito	Clasificación de alertas abierta para gestión
Tipo	☒ Requisito ☐ Restricción
Fuente del requisito	Cliente
Prioridad del requisito	☒ Alta/Esencial ☐ Media/Deseado ☐ Baja/ Opcional

Tabla 8.

Requisito funcional 7

Número de requisito	RF 2.4.1
Nombre de requisito	Asignación de número de ticket a la alerta abierta para gestión
Tipo	☒ Requisito ☐ Restricción
Fuente del requisito	Cliente
Prioridad del requisito	☒ Alta/Esencial ☐ Media/Deseado ☐ Baja/ Opcional

Tabla 9.

Requisito funcional 8

Número de requisito	RF 3
Nombre de requisito	Asignación de resolutor en turno
Tipo	☒ Requisito ☐ Restricción
Fuente del requisito	Cliente
Prioridad del requisito	☒ Alta/Esencial ☐ Media/Deseado ☐ Baja/ Opcional

Tabla 10.

Requisito funcional 9

Número de requisito	RF 4
Nombre de requisito	Consulta a la BD para mostrar información específica sobre cada alerta, será mostrada en una tabla.
Tipo	☒ Requisito ☐ Restricción
Fuente del requisito	Cliente
Prioridad del requisito	☒ Alta/Esencial ☐ Media/Deseado ☐ Baja/ Opcional

Tabla 11.

Requisito funcional 10

Número de requisito	RF 5
Nombre de requisito	En la vista específica de alertas del front end se tendrá actualizado en tiempo real información detallada de la alerta
Tipo	☒ Requisito ☐ Restricción
Fuente del requisito	Cliente
Prioridad del requisito	☒ Alta/Esencial ☐ Media/Deseado ☐ Baja/ Opcional

4.1.Requisitos funcionales

- Comprobación de caracteres en los campos que tengan *textbox.*
- Autenticación de usuarios por LDAP
- Recepción de alertas, procesamiento, clasificación y generación de *tickets* en caso de que se cumplan las condiciones para dicha acción.
- La plataforma debe responder a diferentes formatos de los datos ya que no se encuentran estandarizados en todas las herramientas que los generan.

4.2. Requisitos no funcionales

Requisitos de rendimiento

El número esperado de usuarios simultáneamente conectados son 100 por hora y número de transacciones por segundo que deberá soportar el sistema son 500, ya que en caso de una caída masiva se espera que la plataforma funcione de manera óptima.

Seguridad

- Registro de ficheros con "logs" de los servidores en los que se encuentre alojada la plataforma.
- Excepciones a nivel de firewall y ciberseguridad completadas ya que algunas reglas pueden dificultar la comunicación entre plataformas.
- Restricciones de comunicación entre determinados módulos.

Disponibilidad

El software debe tener alta disponibilidad por lo que se recomienda infraestructura redundante.

Otros requisitos

Se espera realizar una evaluación respecto a las normativas vigentes en los países con operarios que accedan a la plataforma a resolver los incidentes.

4.3. Funcionalidades Clave

- Agrupamiento de alertas por servicio/aplicación/servidor
- Trazabilidad de la alerta a través del botón opciones disponible para cada una.
- Creación de ventanas de mantenimiento.
- Gestión de usuarios en la plataforma por rol.
- Vista para configurar la integración con herramientas de monitoreo adicionales.

5. Marco de referencia

5.1. Monitoreo de infraestructuras informáticas

Las compañías que ofrecen productos y servicios digitales de base tecnológica, requieren controlar las distintas aplicaciones, su disponibilidad y rendimiento. Con la intención de actuar eficazmente frente a la restauración de los servicios cuando ocurre una degradación, resulta definitivo el uso de herramientas para la supervisión o monitoreo, pues permiten identificar a partir de métricas las causas de los fallos (Hernantes et al., 2015). Estas, proporcionan un punto de partida cuantitativo que facilitan a los NOC y SOC la mejora en su capacidad de respuesta, optimización del rendimiento y consolidación de la integridad de los sistemas.

De acuerdo a Fernández (2024), las herramientas para el monitoreo de sistemas basan sus funcionalidades en los siguientes conceptos :

Indisponibilidad: tiempo en el que un sistema se encuentra inaccesible.
Alerta: notificación automática que se genera cuando se detectan condiciones anómalas identificadas a partir de las parametrizaciones definidas.
Consumo de recursos: a partir de los umbrales definidos para la línea base en cada elemento de configuración, se mide continuamente si el consumo de recursos como memoria, ocupación en disco C para sistema operativo Windows; SWAP para Linux, CPU, entre otros, se encuentra por debajo de los umbrales para así prevenir un fallo en los servidores.
Métrica[1]: Son medidas cuantificables que ayudan a los responsables de TI a administrar el departamento y a los CIO o directores de TI a comprender el valor de la tecnología y cómo es importante para la empresa en su conjunto. (Atlassian, 2024)
Frecuencia de supervisión: para cada ítem configurado se establece la regularidad con que se van a recopilar datos para validar si el comportamiento está dentro de los umbrales o no.

[1] Algunas de las métricas más habituales: MTTR, Tiempo de actividad, Coste por ticket, Satisfacción del cliente y Acuerdos de nivel de servicio (SLA). Ver: https://www.atlassian.com/es/itsm/service-request-management/it-metrics-and-reporting

5.2.Usos potenciales del monitoreo

La recopilación de los datos relacionados al comportamiento de los elementos configurados se usa inicialmente para la generación de alertas y la posterior resolución del problema que las ocasionó. Además, se usan los datos para hacer análisis e informes en los que se describen las tendencias del sistema y los tiempos de respuesta de los equipos. Se utilizan también para la generación de tableros que permiten visualizar con mayor facilidad las áreas críticas, cuantificar los niveles de afectación y demás que se requieran a través de gráficos (Mallón, 2022), lo que facilita la accesibilidad a la información a los diferentes roles en el proyecto.

5.3.Herramientas de monitoreo

Nagios

Nagios es uno de los instrumentos de software libre más reconocidos para supervisar infraestructuras de tecnología de la información, tales como estaciones de usuario final, servicios de TI y componentes de red en funcionamiento. Posee una versión de código abierto sin costo, Nagios Core. La versión de pago de Nagios XI ofrece una interfaz web actualizada y de fácil manejo que mejora la deficiente interfaz de Nagios Core. Esta interfaz optimizada dispone de un panel interactivo que ofrece una perspectiva global de gran envergadura de los hosts, servicios y equipos de red. Ofrece tendencias y diagramas de planificación de capacidad que facilitan a las entidades el planeamiento de las renovaciones de infraestructura. La instalación es sencilla, sin embargo, la administración de las configuraciones para la ejecución de dispositivos y pruebas presenta una curva de aprendizaje pronunciada. (Nagios Enterprises, 2017)

Zabbix

Es un programa Open Source que puede adaptarse a entornos de recopilación de datos a gran escala. Recopila datos precisos y de rendimiento mientras supervisa servidores, dispositivos de red y aplicaciones. Cuando se superan los límites aceptables, Zabbix puede notificar a los

administradores de red por correo electrónico o SMS. Al igual que Nagios, Zabbix tiene una comunidad de soporte muy activa. Además, en su versión estándar, incluye una excelente interfaz gráfica de usuario web, así como funciones de generación de informes y gráficos que combinan las funciones de supervisión y tendencias. (Zabbix SIA, 2024)

Hyperic

El programa Hyperic es una iniciativa de VMware para la supervisión y gestión de entornos virtuales, y está disponible en dos versiones: una gratuita de código abierto llamada Hyperic HQ y otra de pago llamada vFabric Hyperic. La instalación es simple y toma unos minutos. Hyperic ofrece una interfaz de usuario personalizable y bien diseñada. Se puede guardar el cuadro de mando y editarlo para incluir gráficos que se utilizan con frecuencia, por ejemplo. El software maneja cualquier sistema operativo, web, aplicación o servidor de base de datos de manera efectiva, y las alertas se pueden enviar como SMS o correo electrónico. Hyperic puede encontrar, vigilar y administrar automáticamente software y recursos de red. Además, tiene una comunidad de apoyo activa. (Hyperic, inc., 2024)

SolarWinds

SolarWinds está disponible como software como servicio y como solución autoalojada. Además, cuenta con un gran apoyo de la comunidad y ofrece soporte nativo para VMware. Con formularios personalizables y acceso móvil, su interfaz de usuario es fácil de entender. Los gráficos detallados muestran el rendimiento, la disponibilidad y las fallas de la red. Puede establecer alertas y tareas complejas basadas en reglas con facilidad. Además, ofrece paneles preconfigurados que puede personalizar según sus necesidades. Además, produce informes individualizados que pueden automatizarse mediante programación. (SolarWinds Worldwide, LLC, 2024)

5.4.Customización en el mercado *fintech*

Al definir qué herramientas de monitoreo se van a emplear, las *fintech* al igual que diversas compañías de base tecnológica, requieren identificar si estas son flexibles, satisfacen las necesidades de la organización y son escalables ya que deben ajustarse a futuras modificaciones según los productos desarrollados para los clientes finales. Lucia Fernández (2024), describe una serie de factores a considerar para hacer dicha elección:
¿qué elementos se van a monitorizar?, ¿cuál es su compatibilidad con aplicaciones de uso frecuente en la compañía?, ¿qué licencias maneja?, ¿qué grado de complejidad tiene su gestión y configuración?, ¿es escalable?, ¿es posible personalizar la gestión de alertas?, ¿tiene capacidad para monitorear máquinas virtuales?, ¿es posible visualizar los componentes del sistema?, ¿brinda informes del estado del sistema?, ¿monitorea usando agentes?, ¿tiene capacidad de almacenamiento de datos históricos?.

Estos factores no son menores teniendo en cuenta la diversidad y complejidad de ítems que pueden requerir ser monitoreados, por lo mismo es común que las compañías usen la combinación de varias herramientas Open Source o licenciadas.

5.5.Normativas relevantes para el diseño del prototipo: Modelo de Aseguramiento de Calidad de Software según la Norma ISO 25000

El modelo de aseguramiento de calidad de software (SQA) según las normas ISO 25000, específicamente ISO/IEC 25010:201(International Organization for Standardization (ISO), 2024), se enfoca en evaluar las características de calidad del producto, asegurando que cumpla con las expectativas de los usuarios y requisitos del negocio. Para el proyecto Raccoonwatch, cuyo objetivo es diseñar la arquitectura de una plataforma web que centralice las alertas generadas por las herramientas de monitoreo de una Fintech en Colombia, este modelo proporciona una estructura robusta que garantiza la fiabilidad, seguridad, eficiencia del software a desarrollar, además del cumplimiento de los requisitos expresados por los grupos de monitoreo que lo gestionarán.

El proceso de aseguramiento de calidad se basaría en las siguientes dimensiones clave de calidad:

Usabilidad

La interfaz de la plataforma debe ser intuitiva y fácil de usar para los grupos de monitoreo, quienes serán los principales usuarios del sistema. Para ello, se realizó la revisión de usabilidad al presentarles los Mockuos, lo que permite diseñar una interfaz centrada en el usuario y realizar pruebas de interacción para asegurar que el sistema se adapte a las necesidades y habilidades de los gestores.

Funcionalidad

La plataforma debe cumplir con todas las funcionalidades requeridas para gestionar, centralizar y priorizar las alertas generadas por las herramientas de monitoreo. Esto incluye la capacidad de personalizar las alertas, la integración con diferentes sistemas de monitoreo, y la correcta gestión de roles de usuario según las necesidades específicas de los equipos de monitoreo. Se deben realizar pruebas de validación para garantizar que todas las características del sistema operen según lo especificado en los requisitos.

Eficiencia

La eficiencia del sistema es clave en un entorno de monitoreo en tiempo real. Más específicamente, la capacidad de la plataforma para procesar alertas y realizar tareas sin consumir recursos excesivos. Se deben realizar pruebas de rendimiento, como las de velocidad de respuesta y uso de recursos, para garantizar que la plataforma pueda manejar grandes volúmenes de alertas sin generar cuellos de botella.

Fiabilidad

Dado que el entorno Fintech es crítico y maneja datos sensibles, la plataforma debe ser altamente fiable. Se deben llevar a cabo pruebas exhaustivas de estabilidad y resistencia, incluyendo pruebas de recuperación ante fallos, carga y simulaciones de incidentes. Además, la plataforma debe

garantizar una alta disponibilidad y una correcta gestión de errores para minimizar los riesgos operativos, por lo que se propuso una arquitectura contenerizada que diminuye los tiempos de indisponibilidad.

Mantenibilidad

La plataforma debe ser fácil de mantener y actualizar, permitiendo la incorporación de nuevas funcionalidades o ajustes según evolucione la tecnología o cambien las necesidades de los grupos de monitoreo. Esto implica una arquitectura modular y el uso de buenas prácticas de codificación que faciliten la extensión y corrección de posibles errores. Además, se debe contar con documentación detallada y pruebas de regresión.

Compatibilidad

La plataforma debe ser compatible con diferentes navegadores web, dispositivos y sistemas operativos para asegurar que los usuarios puedan acceder a ella desde diversas plataformas. Las pruebas de compatibilidad deben asegurarse de que la plataforma funcione correctamente en los entornos más comunes utilizados por los usuarios.

Seguridad

Dado el manejo de datos sensibles, en el contexto Fintech, la plataforma debe ser segura, cumpliendo con las legislaciones nacionales frente al manejo de la información personal y los estándares de privacidad y protección de datos, autenticación y controlando el acceso. Se deben realizar pruebas de seguridad, como pruebas de penetración y validación de las medidas de cifrado, para proteger tanto la integridad como la confidencialidad de la información.

Implementación de la Norma ISO 25000 en el prototipo

Para implementar este modelo de aseguramiento de calidad en el proyecto del prototipo de la plataforma web, se tienen en cuenta las directrices de la norma ISO 25000. Por lo que se definen los objetivos de calidad en base a las necesidades del NOC, a su vez, son identificados los riesgos potenciales en el proceso de desarrollo. Se realiza también el análisis de los requisitos funcionales y no funcionales, alineados con los objetivos del negocio y las expectativas de los usuarios.

Se planea además la implementación de pruebas continuas durante el ciclo de desarrollo, lo que asegura la validez de los criterios de calidad como la funcionalidad, fiabilidad, usabilidad y seguridad. Para ello se propone realizar pruebas unitarias, pruebas de integración y pruebas de aceptación del usuario.

Adicional a ello, son consideradas las revisiones periódicas del proyecto, involucrando a los grupos de monitoreo y stakeholders para asegurar que el prototipo cumpla con los estándares de calidad requeridos.

Finalmente, se considera de alta relevancia llevar una documentación clara del desarrollo y la calidad del software, siempre actualizada y disponible, incluyendo las especificaciones del sistema, los resultados de las pruebas, los informes de seguridad y los manuales de usuario.

De esta forma, el proyecto de investigación puede cumplir con las expectativas de calidad, garantizando que la plataforma desarrollada no solo sea funcional y eficiente, sino también segura, confiable y fácil de usar, lo cual es esencial para su adopción exitosa en el entorno fintech colombiano.

6. Análisis de restricciones

6.1. Ambientales

Si bien las soluciones digitales suelen ser planteadas como de bajo impacto ambiental, se debe reconocer que la infraestructura que soporta una aplicación web tiene impactos en el medio ambiente que no son despreciables. El uso de electricidad para mantener los servidores encendidos, el aire acondicionado para mantener el hardware en condiciones y el consumo de internet para generar alta disponibilidad en los servicios son algunos de los factores que deben ser considerados al generar soluciones tecnológicas. (Guamán et al., 2021) Por lo que se recomienda hacer una evaluación consciente de los recursos necesarios para generar la solución y de igual manera, propender por estrategias que minimicen la necesidad de usar hardware que consuma una alta cantidad de recursos energéticos. Una solución es dimensionar el tamaño al que se espera escalar la aplicación en el futuro e identificar si es posible alojar en un mismo servidor varias aplicaciones.

6.2. Económica

Respecto al factor económico, las *fintech* miden la relación costo beneficio sobre las inversiones que hacen a nivel de hardware y software, por lo que al momento de presentar la propuesta se recomienda hacer una análisis de costos no sólo del producto actual sino de lo que se espera sea invertido en los momentos en que se requiera escalar la aplicación y la manera en que se brindará este soporte. Al respecto López Vargas y Vázquez Chávez (2016), proponen un conjunto de buenas prácticas cuyo objetivo es mejorar la gestión y provisión de servicios de tecnologías de información, teniendo presente que el desarrollo de software es cada vez un mercado más competitivo, por lo que una adecuada atención al cliente y soporte resultan definitivos cuando se está negociando un producto digital.

Ahora bien, respecto al costo del desarrollo de la plataforma para centralizar las alertas, se deben tener en cuenta los costos fijos de producción que incluyen el valor de los servidores en los que se va a alojar el aplicativo, su mantenimiento, el costo del equipo desarrollador y del equipo que administre la plataforma, este último se encargará de realizar las configuraciones adicionales y re parametrizaciones necesarias hacia los ítems y elementos de la infraestructura de la Fintech.

6.3. Social

Al evaluar posibles restricciones sociales a la iniciativa, no se logra identificar ninguna relevante, ya que los avances tecnológicos responden al contexto socio-histórico de las poblaciones humanas y en este caso, una plataforma hace parte de lo que en la actualidad representa los avances de la sociedad desde los campos científicos, culturales, económicos, técnicos, entre otros.

6.4. Salud y Seguridad

En Colombia, el decreto 1443 de 2014 y la norma 1562 del 2012, tienen como objetivo disminuir las labores repetitivas en el trabajo de los analistas de TI, que puedan afectar la salud de los empleados a corto y mediano plazo. Por lo tanto, el efecto de las automatizaciones para disminuir las tareas repetitivas y su volumen mediante tareas programadas, disminuye la posibilidad de sufrir consecuencias en su salud.

6.5. Legales

Debido a que la propuesta se plantea en un escenario financiero real, las pruebas realizadas con el prototipo no serán registradas en el presente documento ya que se debe mantener la confidencialidad del negocio. Sin embargo, durante la sustentación con jurados se presentarán las pruebas, funcionalidades, vistas y demás elementos que conforman la plataforma.

7. Metodología para la selección y desarrollo de la solución

La metodología que permite identificar y desarrollar la solución seleccionada para el problema planteado, a saber, la centralización de alertas enviadas por diversas herramientas de monitoreo se describe a continuación.

El Enfoque Metodológico usado es el exploratorio-descriptivo, ya que se busca identificar las características técnicas necesarias para diseñar un prototipo web para la gestión de incidentes, a su vez son descritos los procesos actuales del NOC y posibles formas para optimizar su gestión mediante la integración de herramientas.

Metodología

El esquema de prototipado iterativo en el que se diseña, prueba y mejora el prototipo en función de las observaciones y restricciones identificadas. Lo que asegura que el prototipo evolucione hacia una solución funcional basada en retroalimentación constante.

Fases del Trabajo

Fase 1: Diagnóstico Inicial
Objetivo: Comprender a fondo el problema actual en el NOC.
Actividades
- Revisión de procesos existentes.
- Identificación de herramientas actualmente utilizadas.
- Levantamiento de requisitos iniciales.

Fase 2: Análisis y Diseño
Objetivo: Definir los requisitos del prototipo y crear los modelos iniciales.
Actividades
- Identificación de casos de uso.

- Diseño de mockups y diagramas de arquitectura (bases de datos, procesos, flujo de información).
- Selección de tecnologías y herramientas.

Fase 3: Desarrollo del Prototipo

Objetivo: Construir una versión inicial del prototipo.

Actividades

- Implementación de funciones básicas.
- Integración con datos ficticios simulados.
- Preparación de un entorno controlado para pruebas.

Fase 4: Validación y Pruebas

Objetivo: Evaluar el prototipo bajo condiciones simuladas.

Actividades

Simulación de problemas típicos del NOC/SOC.

Identificación de fallos y áreas de mejora.

Ajustes iterativos al prototipo.

Fase 5: Documentación y Propuesta Final

Objetivo: Consolidar el aprendizaje y los resultados en un informe final.

Actividades

Documentación técnica del prototipo.

Redacción del análisis de resultados.

7.1.Instrumentos para recopilación y validación de información

Los métodos definidos para la recolección de datos son entrevistas a grupos focales ya que permiten explorar a detalle las percepciones de quienes participan, también la observación participante como método etnográfico (Guber, 2019) para tener mayor contexto de las interacciones diarias que tiene los analistas y superiores con el uso de las herramientas de monitoreo y observabilidad actuales.

Categorías conceptuales para diseño de instrumentos

Para diseñar los instrumentos de recolección de datos identificar temas, patrones y significados a partir de las experiencias de los analistas del NOC, con relación a la usabilidad de una plataforma, se definen las siguientes categorías conceptuales:

Características contextuales

1. Experiencia Previa

   - Feedbaack sobre la plataforma actual u opiniones sobre el sistema actual que utilizan, que pueden contrastarse con las expectativas hacia la nueva plataforma.

   - Expectativas de los analistas
2. Percepciones, deseos y anticipaciones que tienen los analistas sobre la plataforma, como:
   - Funcionalidades deseadas
   - Integración con otros sistemas

3. Cultura Organizacional
   a. Actitudes hacia el cambio y la adopción de nuevas tecnologías en la fintech.

Categorías relacionadas con la usabilidad

1. Satisfacción del usuario

   Grado de satisfacción general con la experiencia de uso.

   Opiniones sobre características específicas de la plataforma.
2. Aprendizaje

   Tiempo necesario para que los analistas se familiaricen con la plataforma.

   Disponibilidad de documentación y recursos de soporte.
3. Facilidad de uso

   ¿Qué tan intuitiva es la interfaz?

   Claridad en la navegación y la disposición de los elementos.

Categorías relacionadas con la eficiencia operativa

1. Colaboración

   Fomento del trabajo en equipo y la comunicación entre analistas.
2. Percepción sobre si la centralización de datos facilita decisiones más informadas y rápidas.
3. Productividad
4. Reducción de errores

Impacto en la toma de decisiones

1. La centralización de datos podría influir en la toma de decisiones y mejorar su calidad
2. Disponibilidad de datos filtrados y clasificados en tiempo real

Diseño de Instrumentos

Le entrevista posibilita explorar las expectativas, percepciones y experiencias de los analistas en relación con la usabilidad de la plataforma y su impacto en la eficiencia operativa. Las preguntas estarán basadas en las categorías conceptuales descritas previamente que fueron tomadas del marco teórico.

7.2. Población y muestra

Partiendo de la identificación del NOC del centro de monitoreo de la fintech como la población objetivo y usuario final de la plataforma, se recurrirá a un grupo conformado por analistas Nivel 1 y Nivel 2. Dichas fuentes primarias brindan los datos acerca de sus expectativas respecto a la usabilidad de una plataforma para centralizar los datos de monitoreo, así como su percepción sobre el potencial impacto de dicha plataforma en la eficiencia operativa.

Además, para tener en cuenta dos perspectivas, la segunda población objetivo son los líderes de las áreas de monitoreo y observabilidad, supervisores y el *product owner* del proyecto, que aceptaron participar voluntariamente de las actividades para la recolección de datos.

La muestra no probabilística o dirigida, fue tomada a partir de la participación voluntaria de 10 analistas de nivel 1 y 2, del NOC de una *fintech* de Colombia, con al menos tres años de experiencia en la resolución de incidentes de infraestructura y 3 analistas que ocupan roles de liderazgo para los Niveles 1 y 2.

Se identificó a los participantes por su especialidad en el manejo de plataformas tecnológicas para la centralización de datos. Además, se tomaron en cuenta factores de inclusión como la experiencia en el sector y el rol dentro de la organización. Se estableció el tamaño de la muestra para lograr una saturación de datos, para facilitar un análisis detallado de las expectativas y percepciones acerca de una nueva plataforma.

7.3. Recolección de datos

La recolección de datos para el estudio de caso inició el día 24 de septiembre del año en curso, se realizó la entrevista semi-estructurada a 3 analistas Nivel 1 y a 3 Nivel 2, que se encontraban en el turno 6 am – 2 pm en el centro de monitoreo de Niquia en la ciudad de Medellín. La aplicación de la entrevista tomó 1 hora en total para los dos grupos, luego de esta, se realizó la observación participante cuyas notas fueron registradas en el formato diseñado para dicho registro.

Este día se sostuvo además un encuentro de 1 hora con el grupo focal conformado por el líder técnico de monitoreo representantes de la Fintech, el líder técnico de monitoreo representante de una consultora de tecnología y el *product owner* de una consultora tecnológica, un total de 3 participantes y la entrevistadora.

Al grupo focal se le presentaron los *Mocups* del prototipo de plataforma, posteriormente se plantean las preguntas abiertas del Anexo 1.

El día 25 de septiembre se siguió la misma dinámica durante el turno de la tarde que va entre las 2 pm – 10 pm, en ese caso se aplicó la entrevista a 2 analistas Nivel 1 y a 2 Nivel 2.

En todos los casos se contó con la aprobación para hacer uso de los datos recolectados con fines académicos e investigativos.

Nota: Debido a las restricciones para acceder a sitios web distintos de los corporativos, las entrevistas, sesión con grupo focal y toma de notas a partir de la observación participante se realizó en formatos físicos.

Conversación con grupos focales

Al visitar el centro de monitoreo principal de la fintech y reunir a varios analistas para discutir colectivamente sus expectativas y percepciones sobre la plataforma. Esto fomenta la interacción y puede revelar diferentes perspectivas sobre la usabilidad y el impacto en la eficiencia operativa.
El registro se dio partiendo de la observación del trabajo de los analistas en su entorno laboral y al participar parcialmente de las actividades cuando surge una incidencia, al tiempo que se toman notas sobre cómo interactúan con las herramientas actuales y sus procesos de monitoreo. Esto proporciona un contexto valioso para comprender sus expectativas.

7.4. Sistematización de datos

Una vez se aplicaron las entrevistas semi-estructuradas, se realizó la conversación con el grupo focal conformado por los líderes de las áreas de monitoreo y realizada la observación participante, se procedió a la sistematización de los datos recolectados.
Debido a que se el procesamiento y análisis de resultados se realiza con el Software Atlas TI, se transcribió la información, discriminada por preguntas y participantes, en un archivo Word. (ver Anexo 2 y 3).

7.5. Procesamiento y análisis de datos

Basados en el paradigma interpretativo y en el diagrama de flujo presentado por Hernández-Sampieri & Mendoza (2018), tras la recolección y revisión de los datos se realiza una codificación abierta, es decir se realiza una “comparación constante entre ellas para generar o descubrir categorías y designarles un código o nombre”. (p. 468)
Dicho proceso se realiza mediante el software de análisis de datos cualitativos Atlas ti. Inicialmente se realiza la codificación manual para las preguntas realizadas a los analistas Nivel 1 y 2. (Figura 1 y 2).

Ilustración 1.

Codificación de las respuestas de las entrevistas

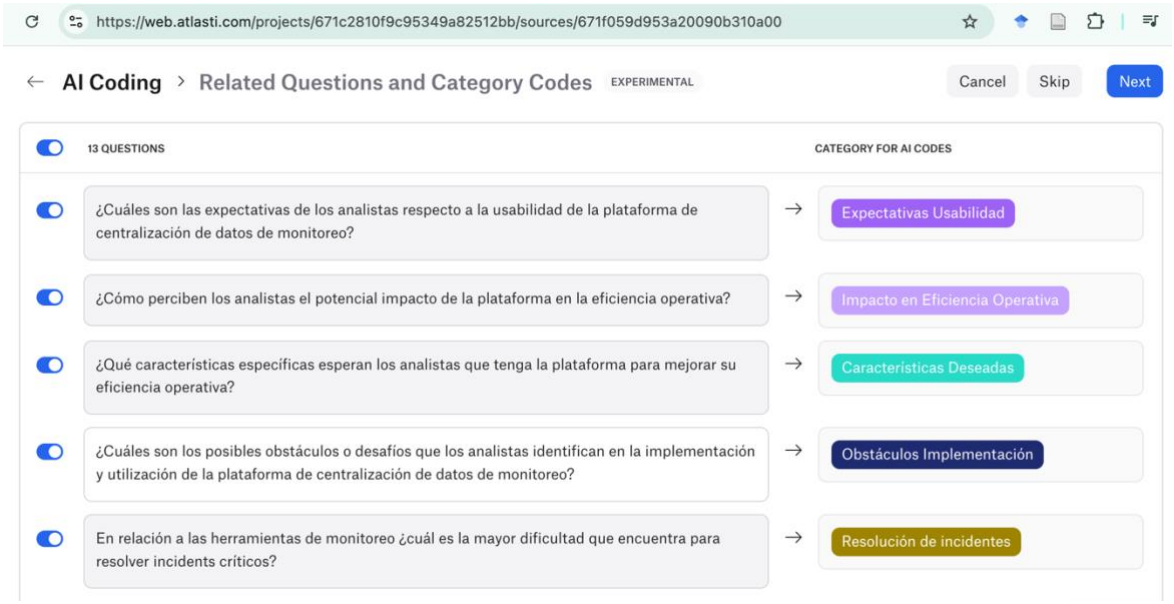
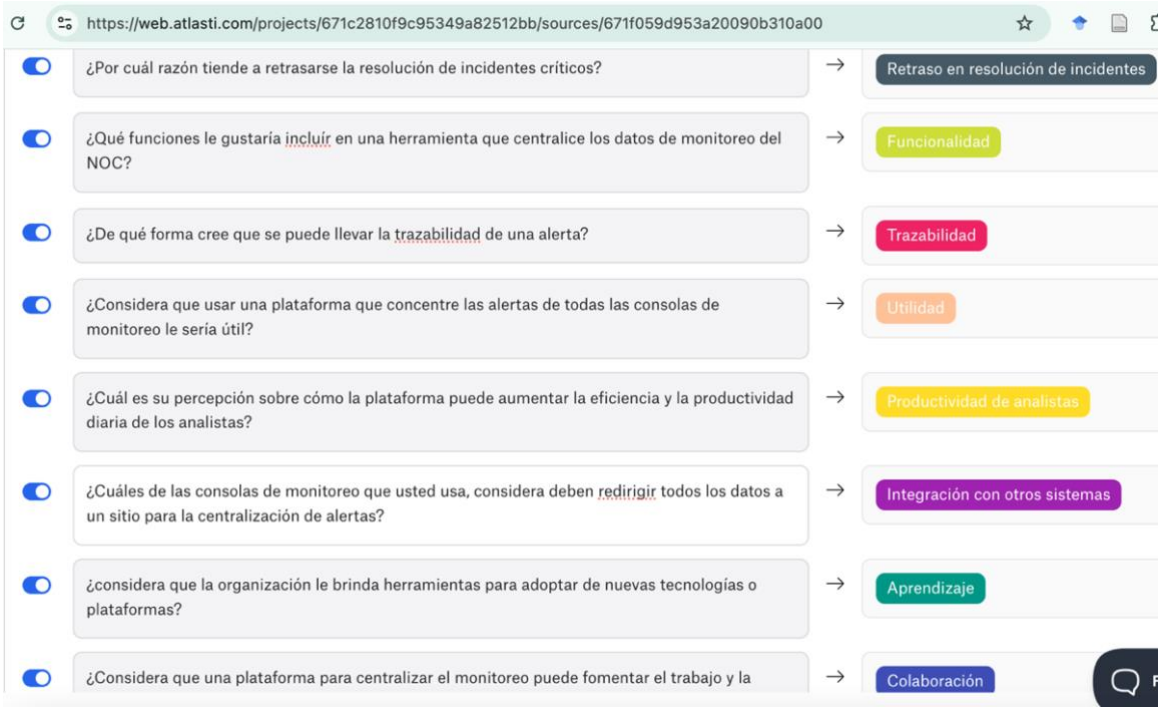


Ilustración 2.

Codificación de las respuestas de las entrevistas



La codificación inicial se realizó de manera manual y la siguiente de manera automática empleando el software. Se produjeron entonces 438 códigos sugeridos para las respuestas:

Ilustración 3.

Codificación de las respuestas de las entrevistas

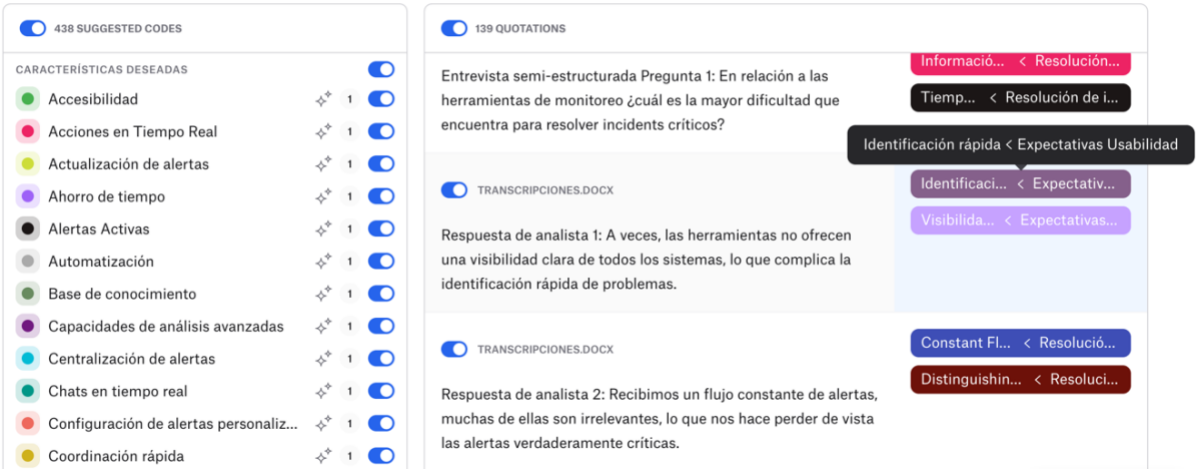
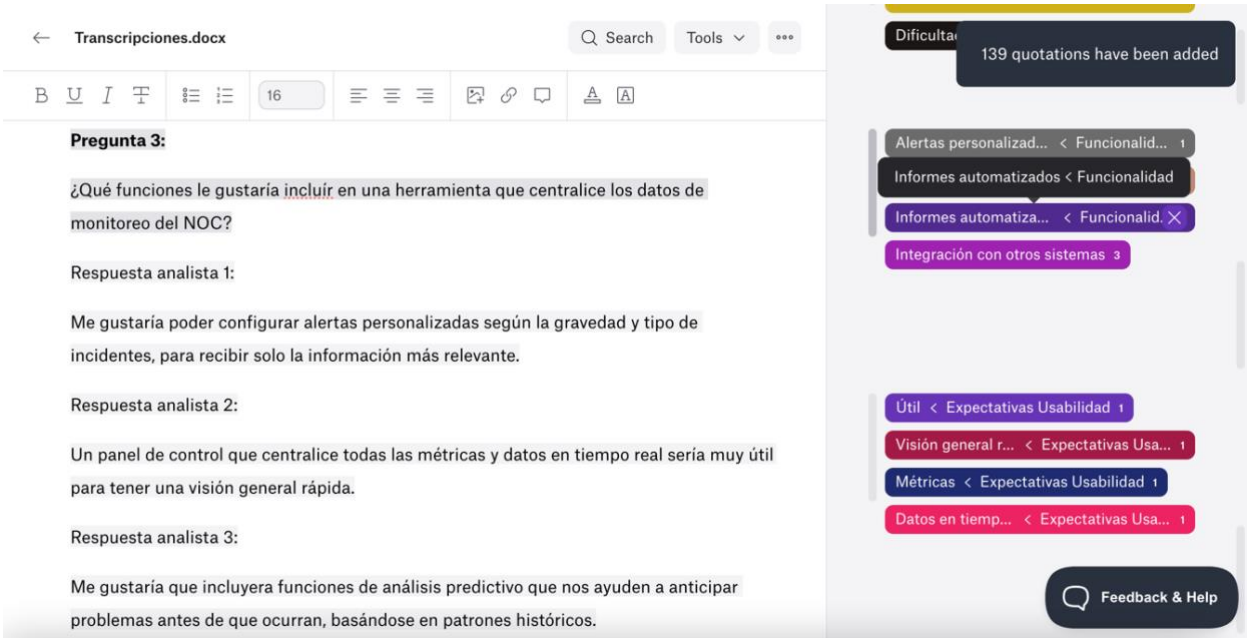


Ilustración 4.

Codificación de las respuestas de las entrevistas



8. Resultados Obtenidos

A partir de la identificación de requerimientos funcionales, no funcionales, el diseño de los casos de uso, las interfaces de usuario y el diseño de la arquitectura basada en microservicios, se realizó el prototipo de la plataforma para centralizar los datos de monitoreo de una *fintech* colombiana.
A continuación, se presentan los hallazgos y análisis derivados del desarrollo del proyecto, abordando tanto los aspectos técnicos como los impactos prácticos del mismo.

8.1.Stack tecnológico usado

Para el desarrollo de la aplicación se consideraron las tecnologías presentadas a continuación:

Tabla 12.

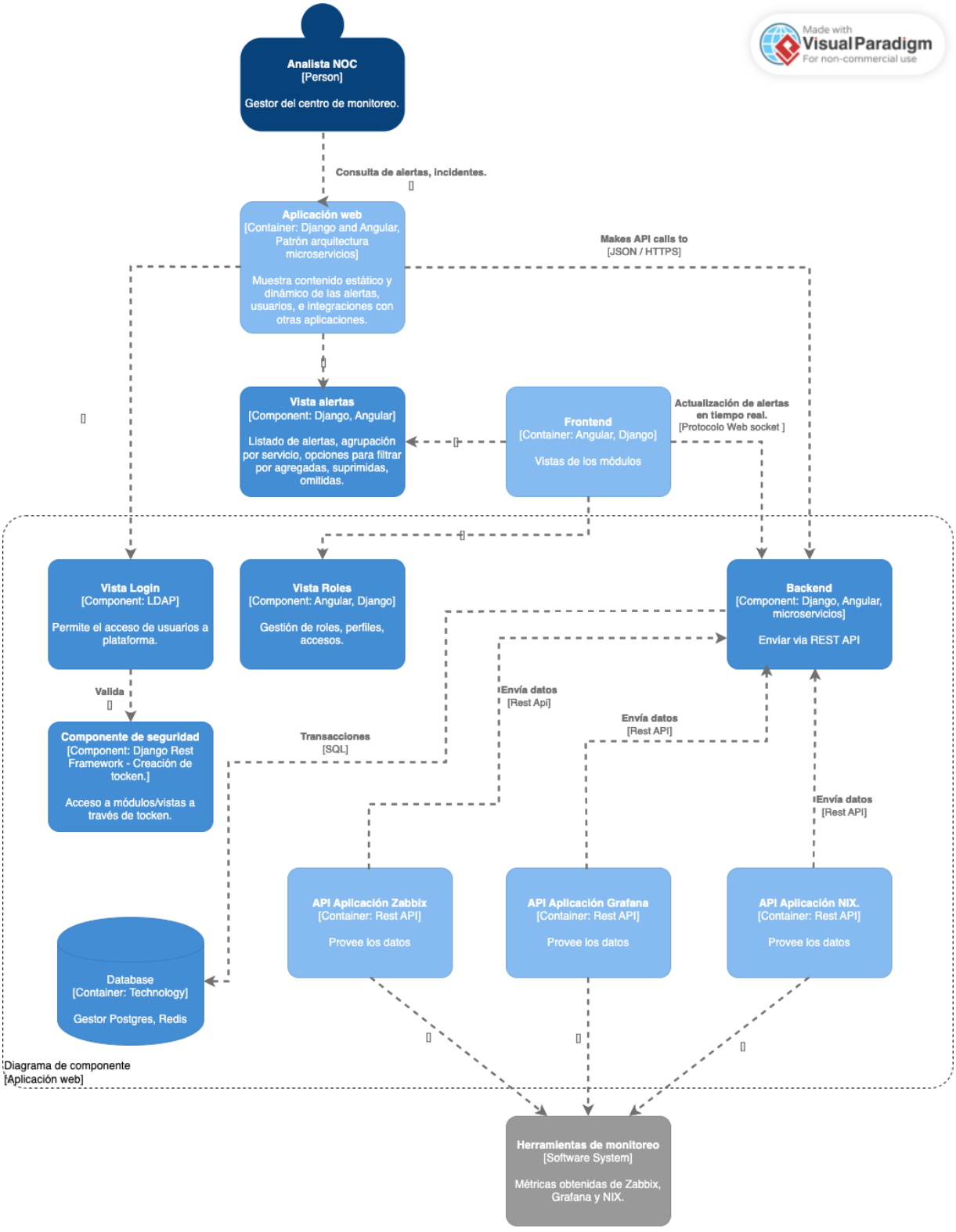
Stack de tecnologías y uso

Item tecnológico	Tecnología	Uso en el sistema
Gestor base de datos	PostgreSQL	Almacena datos de monitoreo
Lenguajes de programación	Python, JavaScript	Desarrollo Back-End, Front-End
IDE	Visual Studio Code	Codificación
Contenedores	Kubernetes, Docker	Se aloja la aplicación. Se consideran 2 master y 3 worker para Back-End, Front-End y 2 contenedores aadicionales para BD.
Encolamiento alertas	RabitMQ	Evita sobrecarga de la plataforma
Control de versiones	GitLab	Local en servidor RHEL.

8.2.Diseño de arquitectura

La plataforma fue modelada de acuerdo a una arquitectura basada en microservicios, empleando las APIs de las plataformas de monitoreo con la que cuenta la Fintech y contenerizada para mejorar la alta disponibilidad de esta. A continuación se presenta el diagrama de componentes, modelo C4.

Ilustración 5.
Diagrama de componentes modelo C4

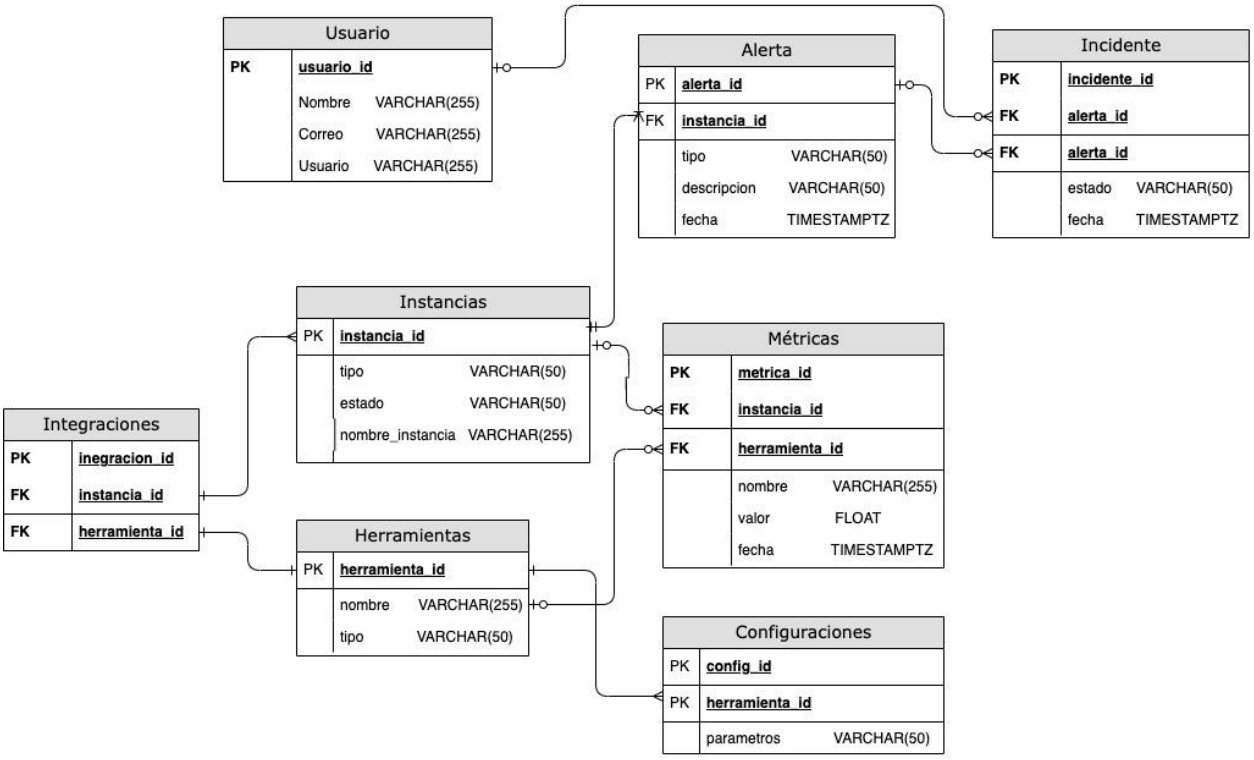


8.3.Modelo de Base de datos

Respecto a la base de datos se presenta el modelo relacional que da cuenta de las entidades, sus atributos y relaciones.

Ilustración 6.

Diagrama relacional de la base de datos



8.4.Prototipo de la solución de ingeniería

La siguiente es la primera fase del desarrollo de las funcionalidades del centralizador, se presentan los módulos de alertas, exportar archivo de acuerdo con los filtros, validar los detalles de un evento listado y parametrización de alertas.

Ilustración 7.
Vista alertas

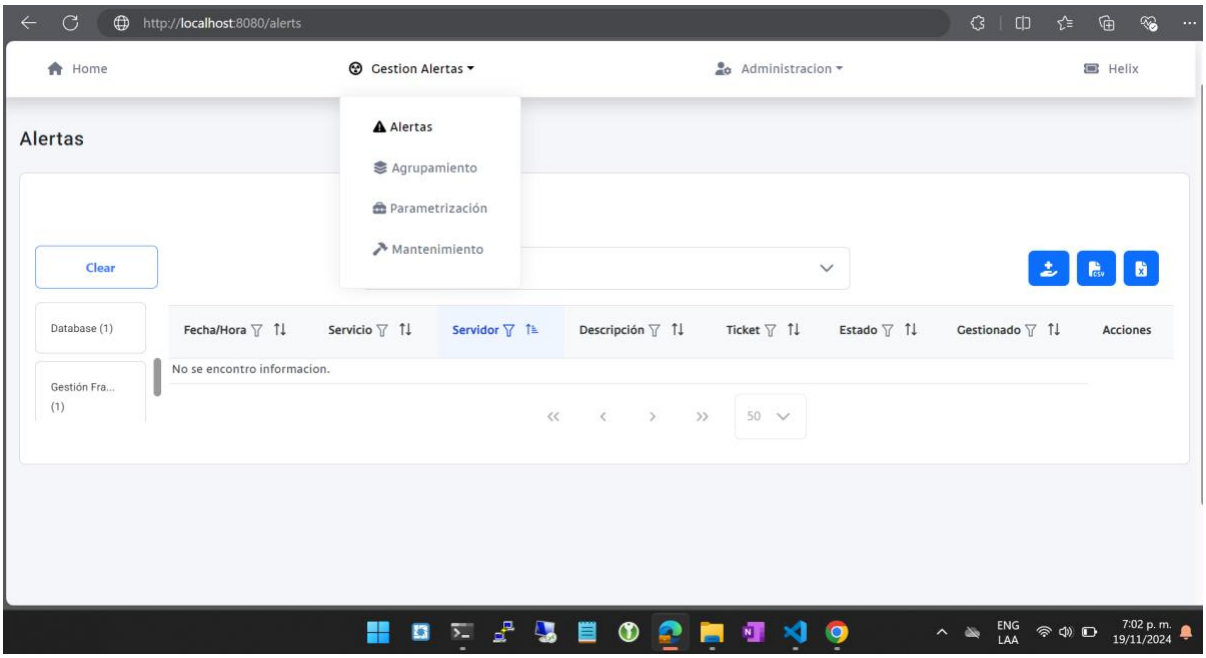


Ilustración 8.
Vista exportar archivo

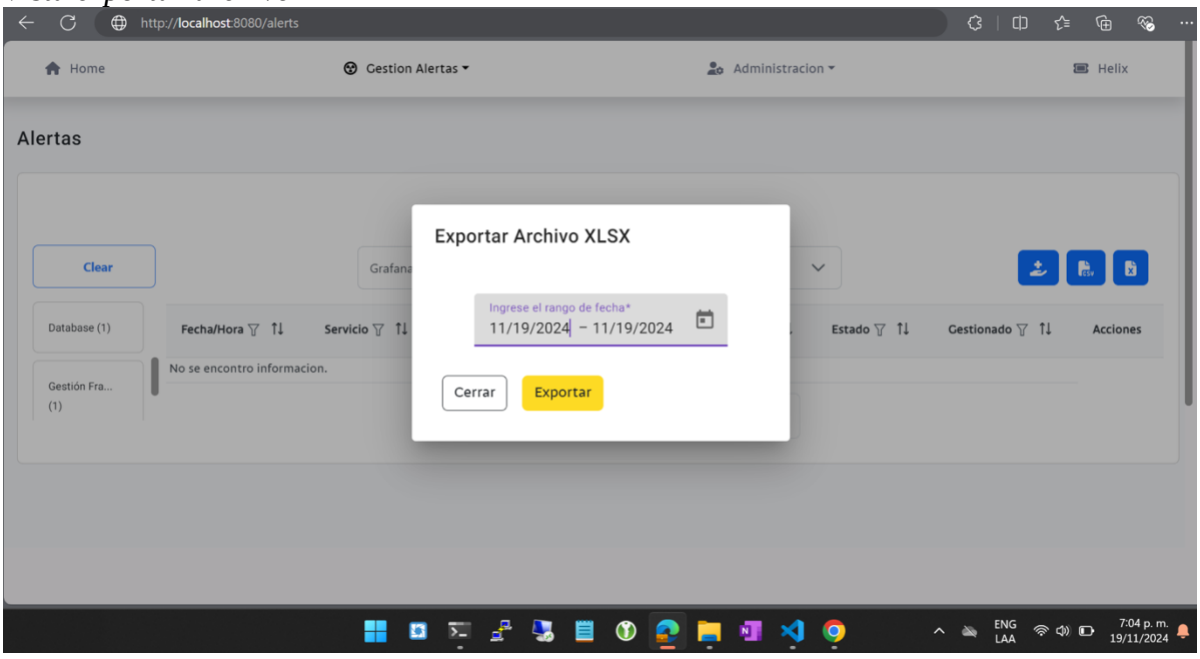


Ilustración 9.
Vista detalle de eventos

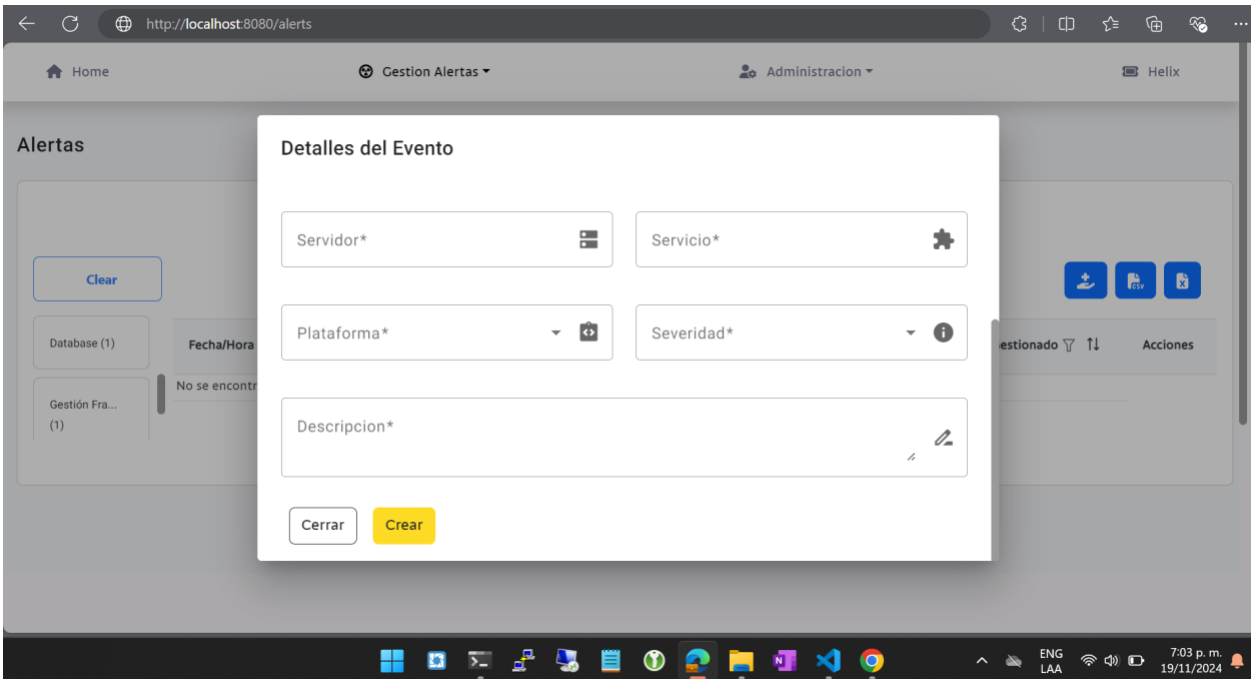
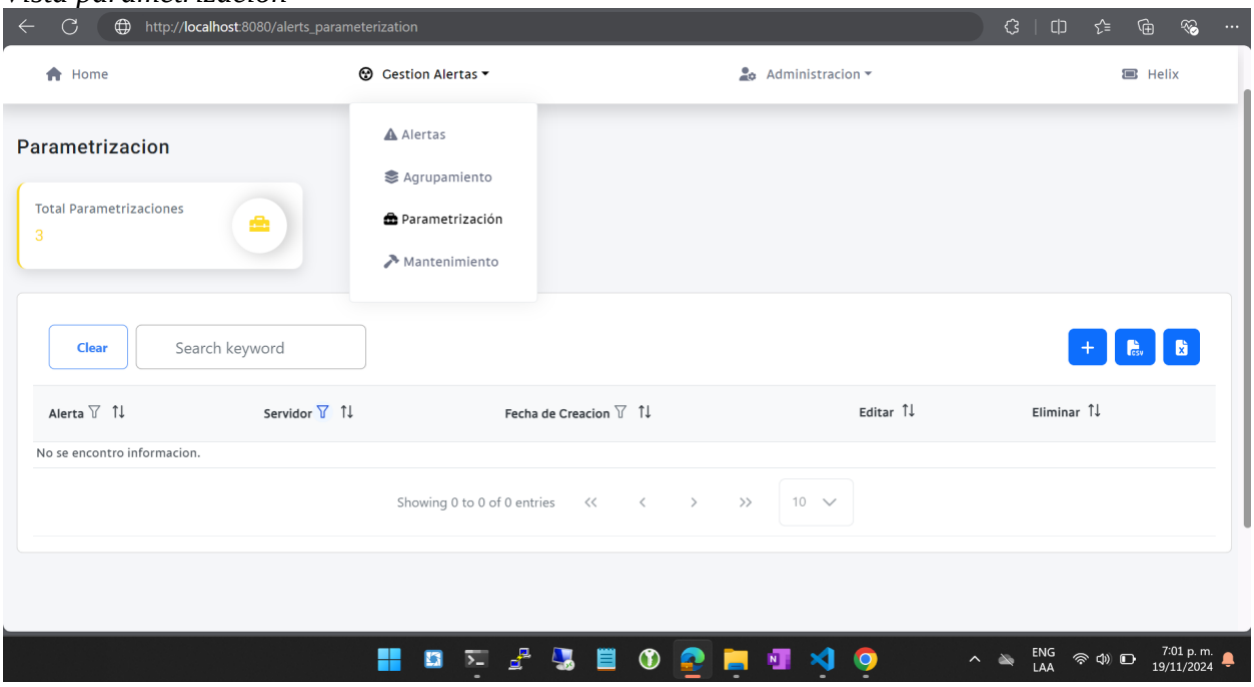


Ilustración 10.
Vista parametrización



8.5.Validación con Expertos

Se sostuvo un espacio de socialización del prototipo con los analistas del NOC, líderes de monitoreo de la Fintech y un *Product Owner*.
En esta se dio visto bueno al prototipo, las historias de usuario y los requerimientos identificados. Se sugirió, además, considerar la integración de la plataforma con herramientas específicas para la observabilidad como Prometheus, Elastic search y Kibana.
La perspectiva de observabilidad integra no sólo el monitoreo, incluye además las trazas, métricas y logs de los diferentes elementos de configuración de las compañías.

8.6.Impacto Técnico y Práctico

La arquitectura de la plataforma se diseñó para contenerización considerando la criticidad del servicio que presta, así, los *pods* se recrean automáticamente en caso de que haya una falla o se reinicien los otros que componen el *cluster* de *Kubernetes*. Dicha tecnología no se encuentra implementada por la Fintech por lo que se generó inicialmente un impacto tecnológico. Este impacto se ve reflejado además en la alta disponibilidad del monitoreo y la posibilidad de aportar en la gestión de los agentes del NOC.

9. Análisis de costos

El análisis de costos para la plataforma centralizadora de alertas debe cubrir diversos aspectos que permiten entender los costos operativos, inversión inicial y necesidades de capital de trabajo para asegurar su correcto funcionamiento.
A continuación, se propone un desglose de los distintos tipos de costos para la plataforma, así como las metodologías para calcularlos. Este análisis ayudará a evaluar la viabilidad financiera de la plataforma y optimizar la toma de decisiones.

9.1. Costos Directos

Son aquellos que se pueden atribuir directamente a la operación de la plataforma y su actividad principal. Estos costos están directamente vinculados con el procesamiento y monitoreo de las alertas.

Licencias de Software

- Grafana Enterprise (si se utiliza la versión de pago).

- Licencia de Dynatrace (según el número de hosts, usuarios o métricas monitoreadas).

- Licencia de Zabbix (si se usa la versión Enterprise o servicios adicionales).

Infraestructura de TI

- Servidores y Hardware (si la plataforma se ejecuta en servidores on-premises).

- Red de comunicaciones: costos asociados con la transferencia de datos entre las herramientas de monitoreo, los servidores y la base de datos.

Costos de desarrollo y mantenimiento

- Desarrolladores: salarios de los desarrolladores encargados de la integración de las herramientas, personalización de la plataforma y mantenimiento continuo.

- Soporte técnico: costos del equipo de soporte para garantizar el funcionamiento correcto de la plataforma de monitoreo.

9.2. Costos Fijos

Independientemente de la cantidad de alertas, usuarios o volumen de datos procesados. Estos costos no dependen de la producción o uso de la plataforma.

Salarios de Personal Administrativo

- Personal de gestión, administrativo, y otros cargos no directamente involucrados en la operación de la plataforma.

Software de Administración y Seguridad

- Herramientas de gestión de proyectos, comunicación y seguridad herramientas de CI/CD, antivirus, entre otros.

Servicios Públicos

- Consumo de electricidad, internet y otros gastos operacionales relacionados con las oficinas.

9.3. Gastos Generales

Son aquellos que no se pueden asignar directamente a la producción o actividad operativa, pero que son necesarios para el funcionamiento de la plataforma. Por lo general, son costos compartidos entre diversas áreas de la organización.

Marketing y Publicidad: para promover la plataforma o atraer nuevos clientes.

Gastos Legales y Consultoría

- Consultoría relacionada con la integración de nuevas herramientas o la mejora de la plataforma.

- Servicios legales para la gestión de contratos y licencias de software.

Costos de capacitación: Entrenamiento para el personal técnico y no técnico

9.4. Costos de Inversión

Se requieren para la adquisición de activos que serán utilizados a largo plazo. En este caso, estos costos están relacionados con la compra de servidores, software y otras infraestructuras necesarias para montar y operar la plataforma.

Infraestructura de TI

- Compra de servidores físicos, almacenamiento y redes internas.

- Licencias de software a largo plazo (como una licencia perpetua de Grafana o Zabbix).

Desarrollo y Diseño de la Plataforma

- Costos iniciales para la personalización de la plataforma, diseño de la interfaz, implementación de nuevas funcionalidades.

9.5. Capital de trabajo

Los recursos monetarios necesarios para financiar las operaciones diarias de la plataforma, que incluye la adquisición de materiales, el pago de personal, gastos operativos y otros costos variables, permiten mantener las operaciones mientras se esperan los ingresos o financiamiento adicional.
Este capital de trabajo, para el caso de la plataforma centralizadora, es asumido por la *fintech*, ya que el monitoreo es una de las áreas o departamentos de la compañía.

10. Conclusiones

La elaboración de un prototipo de plataforma digital para la gestión de incidentes en la infraestructura *on premise* de una *fintech* en Colombia, permite identificar opciones de mejora frente a los procesos que sigue el NOC, frente a la gestión de alertas y resolución de incidentes. La plataforma se presenta así como una opción que les permite re evaluar los procesos que se han seguido para la supervisión del estado de los productos y servicios de base tecnológica, ofrecidos por la compañía.

La solución de ingeniería presentada aquí resulta innovadora y oportuna acorde a la revisión hecha por expertos del área de monitoreo y sus potenciales usuarios, por lo que se considera un aporte basado en el aprendizaje del programa ingeniería de sistemas, acorde a los principios de la Universidad EAN.

Referencias

Areiza López, A., Bravo Sepúlveda, M., Bedoya Londoño, D. A., Zapata Molina, C. E., Guerrero Latorre, J. H., & Romero Díaz, P. A. (2023). Taxonomy Of Operational Risks inFintech: A Systematic Literature Review. https://dspace.tdea.edu.co/handle/tdea/3966

Atlassian. (2024). Métricas de TI: Cuatro prácticas recomendadas. Atlassian. https://www.atlassian.com/es/itsm/service-request-management/it-metrics-and-reporting

Fernández, L. (2024). Diseño de una solución integrada de monitorización para entornos distribuidos [Master Thesis, ETSI_Informatica]. https://oa.upm.es/id/eprint/82859

Guamán, C. R. S., Vivar, S. A. M., Rivera, D. P. P., & Jadan, B. E. V. (2021). Impacto ambiental por consumo de energía eléctrica en los Data Centers. Dilemas contemporáneos: Educación, Política y Valores. https://doi.org/10.46377/dilemas.v8i.2786

Help Net Security. (2020, April 24). The true costs incurred by businesses for technology downtime. Help Net Security. https://54.212.120.136/2020/04/24/technology-downtime/

Hernantes, J., Gallardo, G., & Serrano, N. (2015). IT infrastructure-monitoring tools. IEEE Software, 32(4), 88–93.

Hyperic, inc. (2024). Hyperic HQ Enterprise. https://catalog.redhat.com/software/applications/detail/156777

IBM. (2024, May 14). ¿Qué es un centro de operaciones de red? | IBM. https://www.ibm.com/mx-es/topics/network-operations-center

ISO 31000:2018. (n.d.). ISO. Retrieved September 29, 2024, from https://www.iso.org/standard/65694.html

López Vargas, Y., & Vázquez Chávez, A. (2016). La Gestión de Servicios de soporte técnico en el ciclo de vida del desarrollo de software. Revista Cubana de Ciencias Informáticas, 10, 46–60.

Mallón, X. (2022, March 23). ¿Qué es la monitorización y por qué es tan importante? https://keepcoding.io/blog/que-es-la-monitorizacion-de-sistemas/

Nagios Enterprises. (2017). Nagios Enterprises [Computer software]. Nagios Enterprises. https://assets.nagios.com/training/selfpaced/materials/Nagios_StartUp_Guide.pdf

Pérez Galán, A. J. (2023). Creación y gestión de un NOC (Network Operations Center). https://openaccess.uoc.edu/handle/10609/148101

Pérez Vásquez, M. A., Prieto Baldovino, F. H., Díaz Pertuz, L. A., & Noboa Silva, A. (2023). The Neobanks: A new business model in the global financial ecosystem in times of Covid-19 and its impact on the colombian economy. Económicas CUC, 44(2). https://search.ebscohost.com/login.aspx?direct=true&profile=ehost&scope=site&authtype=crawler&jrnl=01203932&AN=174831367&h=cvKpVpfgjHjVzRLzTIGipA4FsJm65nzm%2FJ7W3PoQ5RjqyP5AE3kslkhQaoygUdvPs7GVnx%2FPPpe6ZSjh8rJFQA%3D%3D&crl=c

Rentería, D., Vélez, I., Giraldo, M. L. M., & Villa, L. F. (2021). Las fintech, una revolución para la banca tradicional. Revista Ibérica De Sistemas e Tecnologias De Informação, E41, 17–29.

Rico Gómez, J. C. (2020). La digitalización del sector financiero: La revolución Fintech. https://uvadoc.uva.es/handle/10324/43537

SolarWinds Worldwide, LLC. (2024). SolarWinds: Simple, Powerful, Secure IT. https://www.solarwinds.com/company

Vázquez Pesado, D. (2020). Security analytics with Elastic. https://openaccess.uoc.edu/handle/10609/117789

Zabbix SIA. (2024). Zabbix: The Enterprise-Class Open Source Network Monitoring Solution. https://www.zabbix.com/la/index

Anexos

Prototipo de una herramienta de observabilidad para optimizar la gestión de incidencias en infraestructura tecnológica

Seminario de Investigación

Ingeniería de Sistemas - Universidad EAN

Entrevista semi-estructurada

Fecha: **Hora:**

Lugar (ciudad y sitio específico):

Entrevistador:

Entrevistado **Nombre:** **Edad:** **Rol:**

A continuación se presentan preguntas abiertas en relación al contexto de las actividades para el monitoreo y la observabilidad de infraestructura o relacionadas con la usabilidad de las plataformas/consolas; relativas a la eficiencia operativa y al impacto en la toma de decisiones.

1. En relación a las herramientas de monitoreo ¿cuál es la mayor dificultad que encuentra para resolver incidents críticos?

2. ¿Por cuál razón tiende a retrasarse la resolución de incidentes críticos?

3. ¿Qué funciones le gustaría incluir en una herramienta que centralice los datos de monitoreo del NOC?

4. ¿De qué forma cree que se puede llevar la trazabilidad de una alerta?

5. ¿Considera que usar una plataforma que concentre las alertas de todas las consolas de monitoreo le sería útil?

Prototipo de una herramienta de observabilidad para optimizar la gestión de incidencias en infraestructura tecnológica

Seminario de Investigación

Ingeniería de Sistemas - Universidad EAN

Entrevista semi-estructurada a grupo focal

Tras presentar los Mocups del prototipo de plataforma, se plantean las siguientes preguntas abiertas al grupo de turno en el NOC:

1. ¿Cómo describe el grado de satisfacción general con la experiencia de uso?

2. ¿Cuáles son sus opiniones frente a las características específicas de la plataforma?

3. ¿Qué tan intuitiva es la interfaz?

4. ¿Hay claridad en la navegación y la disposición de los elementos?

5. ¿Qué funcioanlidad le agregaria?

Otros comentarios

Prototipo de una herramienta de observabilidad para optimizar la gestión de incidencias en infraestructura tecnológica

Seminario de Investigación

Ingeniería de Sistemas - Universidad EAN

Formato para registro de notas durante la observación participante

Observaciones: