Levantamiento de Requerimientos

**13 de febrero del 2024**

# Visión general

En el presente documento, se observa la transcripción de un archivo de audio en el cual se puede detallar el diálogo que se sostuvo entre el cliente y los ingenieros que llevaron a cabo este análisis para el desarrollo del proyecto Fault Trace sistema de detección de fallas de sistemas distribuidos.

# Objetivos

1. **Realizar un levantamiento de requerimientos para obtener información para el desarrollo del proyecto Fault Trace.**

A continuación se presenta la entrevista la cual se le realizó al cliente para poder obtener información para el desarrollo del proyecto Fault Trace.

## Identificadores:

Cesar Gutierrez Francisco ( Cliente)

Kevin Miguel Ceron Escalante (Integrante del equipo de desarrollo)

Perez Gonzalez Arando Fidel (Integrante del equipo de desarrollo)

## [00:00.000 --> 00:15.360] Bueno señor César Gutiérrez, queremos hacerle una entrevista hacerle una entrevista para conocer un poquito más sobre la idea que tiene.

# [00:16.360 --> 00:17.360] ¿Quién eres, perdón?

## [00:17.360 --> 00:18.360] Ah bueno, perdón, sí.

## [00:18.360 --> 00:19.360] Mi nombre es Kevin Cerón, mi compañero es…

### [00:18.360 --> 00:19.360] Fidel Pérez.

# [00:19.360 --> 00:20.360] ¿Son especialistas en qué?

### [00:20.360 --> 00:21.360] Somos ingenieros en sistemas computacionales.

# [00:21.360 --> 00:22.360] ¿Y ustedes me van ayudar en qué?

### [00:22.800 --> 00:26.160] Con su proyecto sobre el sistema de monitoreo, Fault Trace.

## [00:26.160 --> 00:29.640] Ajá, sobre su proyecto Fault Trace.

## [00:29.640 --> 00:34.200] Queremos justo darnos una idea un poquito más profunda de lo que tiene en mente.

### [00:34.200 --> 00:37.200] Y venimos a hacer su levantamiento de requerimientos.

# [00:37.200 --> 00:38.200] Ok, adelante.

## [00:38.200 --> 00:39.200] Ok.

## [00:39.200 --> 00:46.200] Bueno, primero le queríamos preguntar cuál es la problemática que tiene

# [00:48.040 --> 00:49.040] Yo no tengo ninguna problemática.

### [00:49.040 --> 00:50.040] Acerca de su proyecto...

### [00:50.040 --> 00:51.040] Bueno, acerca de su proyecto…

## [00:51.040 --> 00:56.040] O bueno, ¿qué objetivo quiere conseguir con este proyecto?

# [00:56.040 --> 01:06.040] Yo tengo una empresa de desarrollo de software y evidentemente quiero comercializar, ampliar nuevas oportunidades y tener un nuevo producto en el mercado.

# [01:17.040 --> 01:24.840] Ya que he dado a conocer que existen pocos software que generan este tipo de asistencia.

# [01:24.840 --> 01:30.760] La mayoría de mis clientes son clientes empresariales corporativos muy grandes.

# [01:30.760 --> 01:33.880] Y qué sucede con estos clientes?

# [01:33.880 --> 01:40.360] Lo que pasa es que tienen sistemas muy robustos, o sistemas muy grandes por decirlo así.

# [01:40.360 --> 01:42.200] Que interactúan entre sí.

# [01:42.200 --> 01:48.360] y no tienen cómo monitorear justamente partes de fallas que se presentan.

# [01:48.360 --> 01:54.640] Entonces tienen que establecer unos protocolos contingentes. Inclusive pueden

# [01:54.640 --> 01:59.640] tener a una persona validando el sistema manualmente para ver si existe alguna

# [01:59.640 --> 02:05.240] falla. Sin embargo, si contienen o mantienen alertas que te puedan avisar

# [02:05.240 --> 02:09.620] justo en el momento que te empieza a fallar algún servicio o alguna

# [02:09.620 --> 02:15.340] conectividad o justo un servicio o alguna conectividad que existe entre estos

# [02:15.340 --> 02:20.860] sistemas, pues obviamente la reacción es más pronta y qué quiere decir? Que

# [02:20.860 --> 02:26.580] puedes actuar de una manera más eficiente para poder lograr con

# [02:26.580 --> 02:29.980] la atención que se requiere y la mejora que tienes que tener dentro de tu software

## [02:30.980 --> 02:34.980] Ok, perfecto.

### [02:35.420 --> 02:39.780] ¿Qué espera lograr con este sistema?

# [02:39.780 --> 02:43.380] Lo que espero lograr con este sistema, lo que esperamos todas las compañías de software, tener un posicionamiento en

# [02:43.380 --> 02:48.380] el mercado, poder vender el producto y justamente

# [02:48.380 --> 02:51.380] ayudar a mis clientes.

### [02:51.380 --> 03:01.580] Bueno, dentro que ya nos menciona la parte del objetivo principal a resolver

### [03:01.580 --> 03:08.060] ¿cuál es el propósito que va a tener este sistema de monitoreo?

## [03:08.060 --> 03:12.860] O sea, ¿qué objetivos concretos quiere?

# [03:12.860 --> 03:18.900] ¿Qué objetivos concretos? Mira, los objetivos concretos aún no están definidos, puesto que no tengo...

# [03:18.940 --> 03:24.860] Yo como cliente tengo la expectativa de que sufren mis clientes,

# [03:24.860 --> 03:29.580] tengo la visibilidad de las plataformas que se utilizan y cómo se pueden implementar. Los problemas o los objetivos principales son para mí el

# [03:36.460 --> 03:44.100] monitoreo de los recursos que tiene un servidor, ya sea virtual, ya sea virtual ya sea físico,

# [03:44.460 --> 03:50.500] esa es una. Otra sería los cuellos de botellas que son principalmente uno de

# [03:50.500 --> 03:54.660] esos son los problemas más importantes que se atacarán aquí. ¿Qué sucede si yo

# [03:54.660 --> 03:59.420] tengo un sistema de llamadas nacional y en ese momento hay una contingencia nacional? Ese sistema se va a saturar. ¿Por qué? Porque se va a hacer un cuello de botella

# [04:03.700 --> 04:07.380] y toda una nación va a estar hablando a ese sistema. Ese sistema tiene una capacidad.

# [04:07.380 --> 04:13.620] Justamente, le van a ayudar a determinar al cliente

# [04:14.180 --> 04:20.180] que sepa actuar qué tan grande tiene que ser su sistema para poder soportar esos niveles de contingencia. Se llaman altos picos de funcionalidad

# [04:26.580 --> 04:31.180] que van a ayudar a determinar cuál es el máximo nivel de capacidad que yo debo

# [04:31.180 --> 04:35.700] de tener para poder cubrir, si no el 100, el máximo de la atención que yo requiero para todos mis clientes, para los clientes de mis clientes.

## [04:40.420 --> 04:44.780] ¿O sea requiere establecer parámetros, los parámetros como normales?

# [04:44.780 --> 04:49.660] Claro, exacto.

### [04:44.780 --> 04:49.660] Bueno, desde lo que me está mencionando es que principalmente… yo sé que tiene

### [04:49.660 --> 04:54.940] otras expectativas o llegará a monitorear otros este tipo de sistemas

### [04:54.940 --> 04:58.780] pero lo que me está comentando es que tiene que enfocarse en la parte de telecomunicaciones, de llamadas.

# [04:58.780 --> 05:05.980] No necesariamente porque puedo tener un

# [05:05.980 --> 05:10.660] sistema que se encuentre, puede ser una base de datos y puede ser una base de

# [05:10.660 --> 05:16.340] datos que almacene o gestione. Entonces vamos a suponer en

# [05:16.340 --> 05:20.060] telecomunicaciones, hablando de telecomunicaciones para un sistema de

# [05:20.060 --> 05:25.460] llamadas. Tú generas llamadas y estos sistemas de comunicaciones denominados

# [05:25.460 --> 05:30.500] IBRs generan llamadas o request o almacenan información en la base de

# [05:30.500 --> 05:35.060] datos y ese cuello de botella que ya generamos en un principio de esta

# [05:35.060 --> 05:39.860] conversación, pues justamente se deriva a todos los demás subsistemas. ¿Qué pasa

# [05:39.860 --> 05:45.860] si yo tengo un IVR que puede soportar un número de llamadas que yo puedo

# [05:45.860 --> 05:49.620] soportar? Vamos a suponer un millón de llamadas, voy a tener cubierta las

# [05:49.620 --> 05:53.780] llamadas, pero qué pasa si mi base de datos no da ese ancho?

# [05:53.780 --> 05:57.260] Entonces todo tiene que ser calibrado en base a los cuello de botellas que se

# [05:57.260 --> 06:02.980] van a generar. Ahora, otra de las cosas es, no necesariamente puede ser para un

# [06:02.980 --> 06:07.940] sistema de call center o un sistema de base de datos, puede ser para un sistema

# [06:07.940 --> 06:14.700] res, puede ser para un sistema web, que a lo mejor vamos a suponer Amazon, que es

# [06:14.700 --> 06:19.500] una plataforma que ya está entre comillas estable ahorita, pero qué pasa si tiene

# [06:19.500 --> 06:23.380] una gran demanda? Entonces el sistema empieza a alentar.

# [06:23.380 --> 06:30.100] Esos picos tú vas a poder determinar, ok, en las compras del mes de diciembre por

# [06:30.100 --> 06:34.740] ejemplo que son masivas o en enero que están las ofertas o en noviembre que

# [06:34.740 --> 06:40.140] hay ofertas o en julio que hay ofertas. Esos meses que son como muy propios donde

# [06:40.140 --> 06:44.500] generar muchas ventas generan una alta demanda y un incremento de uso de

# [06:44.500 --> 06:49.980] estos sistemas, ya sean webs o demás. Entonces, ¿cómo me va a ayudar el monitoreo?

# [06:49.980 --> 06:52.820] El monitoreo me va a ayudar a saber cuánto tengo que crecer en la

# [06:52.820 --> 06:57.420] infraestructura, si es que la tengo que crecer, si no la tengo que crecer, cuánto

# [06:57.420 --> 07:02.940] la tengo que disminuir, inclusive si se pueden tomar decisiones de por cluster

# [07:02.940 --> 07:07.740] en ciertas temporadas voy a hacer que mi sistema crezca para reducir costos y en

# [07:07.740 --> 07:11.500] ciertas temporadas voy a hacer que disminuya mi sistema de almacenamiento

# [07:11.500 --> 07:16.060] para reducir costos. Recuerden que la importancia de la parte del monitoreo

# [07:16.060 --> 07:21.580] son tomar decisiones financieras, que es reducir costos en el caso de tener una

# [07:21.580 --> 07:28.700] emergencia, poder reducir gastos en cómo poder generar un soporte, el que

# [07:28.700 --> 07:33.740] si por ejemplo tengo un sistema de ventas y mi sistema de ventas empieza a

# [07:33.740 --> 07:38.100] colapsar porque tuve una promoción de diciembre, un ejemplo, yo puedo determinar

# [07:38.100 --> 07:44.540] que las ventas se puedan realizar y que no se tengan o que muchas

# [07:44.540 --> 07:50.300] veces cuando alguien va a contratar, vamos a hablar de no

# [07:50.300 --> 07:57.060] telecomunicaciones sino de otro servicio como televisión de paga, ¿sale? ¿qué pasa?

# [07:57.060 --> 08:01.940] si tienes una oferta de televisión de paga por algún evento como el mundial o

# [08:01.940 --> 08:09.660] como el básquetbol, las olimpiadas etcétera, entonces todo mundo quiere

# [08:09.660 --> 08:13.620] comprar y adquirir el evento o una pelea de box, todo mundo quiere comprar y

# [08:13.620 --> 08:18.380] entonces el sistema se satura y se cae, entonces justamente es para eso, para

# [08:18.380 --> 08:23.020] determinar qué tengo que hacer en esos momentos o qué pasa si estoy vendiendo

# [08:23.020 --> 08:28.340] y de repente mi CRM al que se conecta las ventas o mi ERP en el que gestiono

# [08:28.340 --> 08:34.100] mis clientes llega a colapsar o empieza a alentarse, ¿cómo puedo ayudar a mis

# [08:34.100 --> 08:37.820] clientes a determinar qué tanto tiene que crecer su infraestructura o qué

# [08:37.820 --> 08:42.620] implementaciones tiene que realizar para que su sistema esté entre comillas lo más

# [08:42.620 --> 08:45.300] sano posible?

### [08:48.500 --> 08:54.260] bien este nos mencionó anteriormente que algunas partes de monitoreo, sus

### [08:54.260 --> 08:59.980] clientes, incluso no sé si usted ha hecho alguna vez este monitoreo, lo hacen de

### [08:59.980 --> 09:06.060] forma manual en ciertas partes y bueno no sé si actualmente utilizan sus

### [09:06.060 --> 09:11.100] clientes o especialmente usted algún sistema de gestión.

# [09:11.100 --> 09:15.540] Yo como tal no utilizó ningún sistema de gestión porque nosotros nos dedicamos a la realización

# [09:15.540 --> 09:19.980] e integración de sistemas, por lo tanto nosotros no requerimos de esas

# [09:19.980 --> 09:24.660] herramientas pero son herramientas que los clientes requieren

## [09:27.500 --> 09:32.460] y bueno perdón un poquito encaminado a lo que preguntaba mi compañero Fidel

## [09:32.460 --> 09:36.700] ¿Tiene conocimiento de alguna herramienta de monitoreo o alguna como un punto que nos sirva como de base?

# [09:36.700 --> 09:43.540] un punto base no como tal

## [09:43.940 --> 09:46.940] vale, no hay problema

### [09:51.900 --> 09:59.500] algunos otros puntos que enfrenta a sus clientes dentro de…

### [10:00.420 --> 10:05.860] en el problema de la falla en sistemas que prácticamente no sé a lo mejor que se

### [10:05.860 --> 10:12.740] les caigan en algún momento, sobre todo que sucede con las fallas

# [10:12.940 --> 10:17.260] las fallas, cuando un sistema ya está probado y validado no puede volver a fallar

# [10:17.260 --> 10:23.660] al menos que exista una intersección o una modificación en el sistema

# [10:23.660 --> 10:28.260] sale, voy a hablar por ejemplo de grandes corporativos cuando tienen sus

# [10:28.260 --> 10:34.340] actualizaciones en sus bases de datos, cuando una empresa ya tiene su base de

# [10:34.340 --> 10:39.220] datos determinada y de repente dicen “ahora vamos a agregar un campo nuevo a una tabla “

# [10:39.260 --> 10:44.940] y ahora los web services actualizan que tienen que reconocer un

# [10:44.940 --> 10:48.700] nuevo campo no tienen contemplado a veces el panorama

# [10:48.700 --> 10:53.900] completo de qué… qué otros sistemas impactan

# [10:53.900 --> 11:00.300] entonces por ende que sucede si yo a lo mejor hago un análisis de riesgo y digo

# [11:00.300 --> 11:03.860] voy a impactar este sistema y este sistema pero los corporativos ya son tan

# [11:03.860 --> 11:07.900] grandes que luego no tienen esa visibilidad de sobre qué sistema se

# [11:07.900 --> 11:11.660] encuentra justamente o qué impacta a esta base de datos qué pasa si hay

# [11:11.660 --> 11:15.580] otro tercer sistema que no está considerado dentro del riesgo y hago una

# [11:15.580 --> 11:19.940] modificación entonces el otro sistema va a empezar a colapsar ¿por qué? porque va

# [11:19.940 --> 11:24.180] a tener que tener una actualización del servicio que consume o de la base de

# [11:24.180 --> 11:29.900] datos que consume o de la comunicación que debe de tener o a lo mejor uno de

# [11:29.900 --> 11:34.220] los principales riesgos que existen es que cambien regularmente por seguridad

# [11:34.220 --> 11:39.460] cambian los passwords y las autenticaciones entonces qué pasa si yo

# [11:39.460 --> 11:43.700] cambio una autenticación dentro de un sistema y le pegó a otro que lo consume

# [11:43.700 --> 11:48.060] que no teníamos conocimiento que lo consume y que lo consume entonces ese

# [11:48.060 --> 11:52.580] sistema va a empezar a colapsar si me explico sin embargo si nosotros

# [11:52.580 --> 11:56.620] detectamos que en una base de datos ponemos en la entrada todas las

# [11:56.620 --> 12:01.060] peticiones que llegan y vemos que de repente empieza a ver una autenticación

# [12:01.260 --> 12:05.980] no permitida y se empieza a escribir muchas veces muchas veces muchas veces

# [12:05.980 --> 12:11.140] muchas veces podemos determinar de qué IP viene y podemos saber qué sistema es

# [12:11.140 --> 12:16.900] el que está siendo impactado a través de este tipo de monitoreos

### [12:20.420 --> 12:26.220] bueno dentro de... me comenta que no ha manejado alguna herramienta de monitoreo…

### [12:31.220 --> 12:35.340] bueno dentro de lo que algunas plataformas de monitoreo hacen es la

### [12:35.340 --> 12:39.900] detección de fallas medir los rendimientos de la parte de sus equipos

### [12:39.900 --> 12:44.620] donde esté instalado ya sean servidores, CPUs, la parte de red si tu

### [12:44.620 --> 12:50.100] red está en buen estado a lo mejor hay alguna falla como no sé ha utilizado

### [12:50.100 --> 12:56.820] speed donde usted da un clic y mide cuantos megabytes están subiendo y cuantos megabytes

### [12:56.820 --> 13:01.940] están bajando respecto a alguna experiencia si que ha tenido en alguno de

### [13:01.940 --> 13:07.820] ese tipo de… o ha visualizado que es lo que usted quiere que tenga de diferente su tipo de monitoreo

# [13:07.820 --> 13:14.620] actualmente conozco… no he trabajado con ningún sistema de

# [13:14.620 --> 13:18.460] monitoreo de manera

# [13:18.460 --> 13:22.900] directa que quiere decir que no lo he implementado yo como tal. No soy una

# [13:22.900 --> 13:28.060] persona que usa un sistema de monitoreo pero sin embargo si los clientes no

# [13:28.060 --> 13:32.100] consumen la mayoría de estos tipos de sistemas porque son sistemas que

# [13:32.100 --> 13:37.020] requieren gente muy especializada lo que yo quiero que sea un sistema amigable

# [13:37.020 --> 13:44.060] que me brinde notificaciones a las personas correctas

# [13:44.060 --> 13:49.780] y que sea fácil de interpretar como simplemente a una gráfica que me diga

# [13:49.780 --> 13:55.420] en este sistema hay un error y que me indica directamente a que IP o que

# [13:55.420 --> 13:58.540] servidor si está nombrado si está ubicado

# [13:58.540 --> 14:02.740] obviamente eso tendrá que ser una base de datos que tendría que tener toda esa

# [14:02.740 --> 14:07.140] información para poder mostrarle al cliente ya de forma directa de acuerdo

# [14:07.140 --> 14:11.340] a la arquitectura cuáles son los dispositivos si son físicos que están

# [14:11.340 --> 14:17.340] fallando si son virtuales en donde se alojan si son híbridos porque la

# [14:17.380 --> 14:22.260] comunicación está interrumpido inclusive por fallas de internet por fallas de

# [14:22.260 --> 14:26.300] ancho de banda inclusive por la misma arquitectura que ya tiene el cliente que

# [14:26.300 --> 14:32.380] a lo mejor a veces su cableado directamente su cableado no soporta el

# [14:32.380 --> 14:36.020] ancho de banda que debería de soportar

## [14:40.660 --> 14:45.660] aquí bueno justamente como ya nos mencionó pues ya empezamos a detectar un

## [14:45.660 --> 14:50.860] poquito hacia dónde va el proyecto esté por lo que hemos visto

## [14:50.860 --> 14:54.600] bueno se quiere monitorear la red para que cheque justamente si hay como

## [14:54.600 --> 14:57.700] alguna conexión sospechosa o algo saber de dónde viene

## [14:57.700 --> 15:01.980] este quiere estar checando el rendimiento los cuellos de botella que

## [15:01.980 --> 15:06.100] son de los problemas principales que tienen pero bueno entre esas cositas que

## [15:06.100 --> 15:10.860] ya hemos detectado también le quería preguntar, ¿usted tiene pensado algo

## [15:10.860 --> 15:15.460] específico que… bueno que requiera monitorear? no sé por ejemplo en el

## [15:15.460 --> 15:20.100] rendimiento podría monitorear cpu y almacenamiento que son cositas que

## [15:20.100 --> 15:24.260] justo vuelven a digo pueden llegar a causar estos cuellos de botella

# [15:24.260 --> 15:27.500] los recursos principales que me gustaría monitorear es el almacenamiento de

# [15:27.500 --> 15:33.500] disco duro justamente el uso de cpu para ver si hay algunas algunos software que

# [15:33.500 --> 15:39.500] se instalan y que generan mucho uso de cpu eso porque eso justamente va a

# [15:39.500 --> 15:44.140] ayudar a determinar al cliente que tiene que reestructurar o hacer una

# [15:44.140 --> 15:48.100] re ingeniería de los software que generan ese justamente

# [15:48.100 --> 15:54.620] desuso o mal uso del cpu y también la memoria ram que es uno de los

# [15:54.620 --> 15:58.940] principales elementos que pueden crecer y bajar muy rápidamente

# [15:58.940 --> 16:03.900] uno de los problemas que sí me gustaría atacar también es cuando

# [16:03.900 --> 16:08.420] quieren hackear los sistemas ¿Qué quiere decir esto? generan muchísimas

# [16:08.420 --> 16:13.380] peticiones al azar y todo es las peticiones un incremento en las

# [16:13.380 --> 16:20.260] peticiones muy notorio que no son comunes porque evidentemente generan

# [16:20.260 --> 16:24.620] los clientes en la mayoría generan sus históricos generan sus reportes

# [16:24.620 --> 16:28.620] entonces vamos a decir que en todo enero no tengo más de 30 mil

# [16:28.620 --> 16:34.340] requests en mi sistema es un ejemplo si qué pasa si el 18 de enero yo tengo de

# [16:34.340 --> 16:39.140] repente 200 mil requests hubo un comportamiento inusual y justamente el

# [16:39.140 --> 16:42.540] tipo este tipo de monitoreo me va a ayudar a determinar por qué se dio ese

# [16:42.540 --> 16:47.100] comportamiento a lo mejor una contingencia a lo mejor una promoción a

# [16:47.100 --> 16:50.780] lo mejor se esperaba o a lo mejor ni siquiera se esperaba ahí y es otro

# [16:50.780 --> 16:55.260] sistema que quiere tirar mi sistema

# [16:58.580 --> 17:04.100] algo que me gustaría monitorear mucho es el tipo de respuestas que se dan por

# [17:04.100 --> 17:11.820] cada uno de los servicios por ejemplo si tengo exitosos de los requests a

# [17:11.820 --> 17:19.380] cualquier tipo de servicio ya sea web service o res o un api que mis respuestas

# [17:19.380 --> 17:23.900] siempre sean exitosas así y que se tengan que se tenga un diccionario

# [17:23.900 --> 17:28.780] catalogado para determinar si por ejemplo yo respondo a un fail que ese

# [17:28.780 --> 17:36.100] fail no sea basado en… que sea basado en fallas que se puedan controlar si me

# [17:36.100 --> 17:40.860] explico como por ejemplo si yo tengo un sistema de datos y en ese sistema de

# [17:40.860 --> 17:45.300] datos ingrese mal mi contraseña pero porque realmente yo usuario la ingrese

# [17:45.300 --> 17:52.180] mal y que se determine que se detecte no sea lo mejor tres request mal y a lo

# [17:52.180 --> 17:55.340] mejor ya lo mande a que cambiara su contraseña por otro sistema ya lo

# [17:55.340 --> 18:01.020] cambió y ya puedo acceder a que haya algún robot que quiera tratar de volcar

# [18:01.020 --> 18:05.580] un password y que esté intentando intentando intentando intentando por eso

# [18:05.580 --> 18:11.340] es importante que yo sepa determinar en los request de los servicios el tipo de

# [18:11.340 --> 18:18.900] respuesta que brindan estos request y el tipo de de fallas que que también como

# [18:18.900 --> 18:24.980] request responden estos servicios por ejemplo un 404 quiere decir que el

# [18:24.980 --> 18:30.860] servicio está bajo y evidentemente en cuanto tú recibas un 404 eso es una

# [18:31.060 --> 18:36.140] alerta muy emergente porque porque el servicio ya no está contestando

# [18:36.140 --> 18:44.100] no es lo mismo que recibir un 205 204 o un 200 que son a lo mejor error de

# [18:44.100 --> 18:50.780] autentificación y por ejemplo en el análisis de datos de este monitoreo eso

# [18:50.780 --> 18:54.380] es justo lo que quiero que tú identifiques y que puedas determinar ok

# [18:54.380 --> 18:59.220] sabes que un usuario quiso hacer una compra a lo mejor tres veces y se le

# [18:59.220 --> 19:06.740] bloquea la cuenta o quiso hacer tres compras y no pudo pero ya no lo vuelve a

# [19:06.740 --> 19:11.820] intentar si me explicó entonces ese tipo de reportes son los que le van a

# [19:11.820 --> 19:17.980] ayudar a a a… los clientes a determinar qué acciones pueden hacer porque a lo

# [19:17.980 --> 19:21.500] mejor hay sistemas que son complejos de entender que el cliente a lo mejor no

# [19:21.500 --> 19:26.980] entiende sus flujos y también eso va a ayudar a que puedan tomar decisiones de

# [19:26.980 --> 19:32.260] cómo es simplificar procesos para ayudar a los clientes si tú ves si tú

# [19:32.260 --> 19:36.400] pones un nuevo sistema en marcha y ves que los clientes que para sí para los

# [19:36.400 --> 19:40.780] clientes no es un sistema amigable los clientes van a empezar a generar

# [19:40.780 --> 19:44.460] errores errores errores errores errores errores errores entonces eso te va a

# [19:44.460 --> 19:48.500] decir sabes que en la parte de autenticación generaste errores en la

# [19:48.500 --> 19:52.740] parte de compras generaste muchos errores en la parte de pagos generaste

# [19:52.740 --> 19:56.420] muchos errores en la parte de agregar productos al carrito generaste muchos

# [19:56.420 --> 20:00.100] errores si y qué quiere decir esto que entonces o el cliente no entiende cuál

# [20:00.100 --> 20:04.580] es el proceso de compra y hay que reestructurar ese proceso de compra o

# [20:04.580 --> 20:08.580] hay algo que no es adecuado de acuerdo a un comportamiento de este tipo de

# [20:08.580 --> 20:13.060] sistemas si me explico el monitoreo debe ser útil para cualquier tipo de

# [20:13.060 --> 20:18.420] sistema distribuido sin importar su índole no importa si es comunicaciones

# [20:18.420 --> 20:22.700] no importa si es un rp no importa si es un crm no importa si es un sistema web

# [20:22.700 --> 20:26.340] no importa el chiste es que sea un sistema distribuido inclusive no

# [20:26.340 --> 20:31.280] importa si es un sistema de domótica en donde tú puedas controlar focos y todo

# [20:31.280 --> 20:34.420] porque porque son a final de cuentas sistemas distribuidos en donde tú

# [20:34.420 --> 20:39.980] determinas el uso de luz el uso de principalmente el uso de iluminación el

# [20:39.980 --> 20:43.820] uso de aparatos electrodomésticos por ejemplo en una alberca la calefacción

# [20:43.820 --> 20:47.860] o sea que se puede implementar el monitoreo para cualquier tipo de

# [20:47.860 --> 20:52.500] sistema que tenga una conexión tal cual o fácil como un request o un response

# [20:52.500 --> 20:55.700] y una conexión directa

### [20:55.980 --> 21:01.500] ok bueno ya esa era prácticamente la siguiente pregunta

### [21:01.500 --> 21:04.740] si planea integrar ese sistema de monitoreo con otros tipos de herramientas

### [21:04.740 --> 21:08.340] y bueno aquí ya nos está indicando que está

### [21:08.340 --> 21:12.980] bueno a lo mejor hasta con alexa no?

# [21:12.980 --> 21:16.580] podría ser, claro alexa comunicame de todos los problemas que tiene mi casa. Sabes qué el foco número 4 no

# [21:16.580 --> 21:18.580] prende

# [21:25.820 --> 21:30.420] justamente vamos a ir lo que quiero es que sea por fases este sistema

# [21:30.420 --> 21:36.540] que no sea un sistema que sea de uno pruebas este obviamente quiero una

# [21:36.540 --> 21:41.300] propuesta de parte de ustedes una propuesta donde ustedes me van a decir

# [21:41.300 --> 21:45.060] vamos a empezar con el monitoreo a lo mejor de recursos de pc después el

# [21:45.060 --> 21:50.740] monitoreo de red después el monitoreo de servicios el monitoreo de puertos si

# [21:50.740 --> 21:56.820] me explico? el monitoreo de puerto de protocolos udp tcp y p este todos los

# [21:56.820 --> 22:03.340] protocolos existentes http https y demás si porque evidentemente este tipo de

# [22:03.340 --> 22:05.900] monitoreos va a cambiar dependiendo del tipo de protocolo que estamos

# [22:05.900 --> 22:11.700] trabajando entonces quiero justamente un sistema que abarque todo eso pero que

# [22:11.700 --> 22:18.780] sea por fases el tiempo el tiempo en el cual requiere el sistema no es un

# [22:18.780 --> 22:24.060] sistema que lo requiera en uno dos tres cuatro cinco meses es un sistema que

# [22:24.060 --> 22:29.660] quiero que vaya saliendo al mercado por fases de la misma manera que genere un

# [22:29.660 --> 22:34.060] prototipo en donde yo pueda probar primero la primera fase la segunda fase

# [22:34.060 --> 22:38.500] la tercera fase la cuarta fase la quinta fase y de manera inmediata poder ir

# [22:38.500 --> 22:42.460] vendiendo digamos así esas etapas

### [22:50.220 --> 22:53.220] y bueno

### [22:53.500 --> 22:58.140] nos ha mencionado pues sí bastante

### [22:58.140 --> 23:02.820] qué es lo que requiere la parte del sistema y hasta donde vamos a ir dirigiéndolo

### [23:03.220 --> 23:09.460] pero bueno tenemos una pregunta si usted tiene a la mejor pensado alguna

### [23:09.460 --> 23:16.180] tecnología ya haya visto a lo mejor de algún lado que es similar o que tenga

### [23:16.180 --> 23:18.380] usted alguna tecnología

# [23:18.380 --> 23:20.380] Algo con la cual podría comparar

## [23:20.380 --> 23:24.220] Bueno más que nada como no sé por ejemplo en temas de presupuesto no ha visto como alguna

## [23:24.220 --> 23:29.060] tecnología que ya le haya interesado para desarrollar este sistema

# [23:29.060 --> 23:32.540] podemos utilizar herramientas que ya existen en el mercado que nos ayuden a generar el

# [23:32.540 --> 23:37.540] monitoreo más fácil no estoy en contra de eso podemos utilizar algoritmos que

# [23:37.540 --> 23:43.780] ya existen lo que quiero es que sea un producto que sea fácil de utilizar ese

# [23:43.780 --> 23:49.580] es el objetivo principal que sea fácil de utilizar que sea fácil de implementar

# [23:49.580 --> 23:54.220] con los clientes y que no sea invasivo para sus sistemas esos son los puntos

# [23:54.220 --> 23:59.300] muy importantes que debe de tener el sistema y que debe de ser y también un

# [23:59.300 --> 24:05.100] punto muy importante el punto de seguridad que nos… que a pesar de que se

# [24:05.100 --> 24:11.740] instale los antivirus o los malwares que existen dentro del mercado este puedan

# [24:11.740 --> 24:15.140] convivir con este sistema

## [24:17.820 --> 24:21.980] y bueno perdón en la parte del presupuesto o sea dice que no hay ningún

## [24:21.980 --> 24:25.820] problema en usar software existente pero preferiría que fuera software libre o

## [24:25.820 --> 24:28.820] licenciado

# [24:29.300 --> 24:33.460] para el tema de presupuesto si es algún tema que tiene costo tendríamos que

# [24:33.460 --> 24:39.740] analizarlo primero tendrían que traer a la mesa el costo de la herramienta que se

# [24:39.740 --> 24:42.620] tendría que implementar si existe alguna herramienta que nos pudiera ayudar a

# [24:42.620 --> 24:49.340] mejorar se tendría que traer a la mesa si no obviamente pues si se puede

# [24:49.340 --> 24:55.220] utilizar de todo el tipo de software de libre licenciamiento es para mí sería

# [24:55.260 --> 25:02.340] muchísimo mejor sería lo más óptimo pero tampoco estamos cerrados a que

# [25:02.340 --> 25:08.500] podamos generar un ingreso un costo por por generar el monitoreo de la calidad

# [25:08.500 --> 25:12.380] que requiere el cliente inclusive podríamos ofrecer a lo mejor ciertas

# [25:12.380 --> 25:15.460] características de monitoreo a un cliente que no tengan costo y que tengan

# [25:15.460 --> 25:21.340] ciertas funciones limitadas y luego ya unas que tengan servicio plus por ejemplo

# [25:21.340 --> 25:25.340] así si eso ya sería una estrategia comercial que nosotros tendríamos que

# [25:25.340 --> 25:27.340] trabajar

### [25:31.940 --> 25:35.980] ¿cuáles son los riesgos que usted visualiza en la implementación de este sistema?

# [25:35.980 --> 25:41.780] no visualizo ningún riesgo por ahora porque tenemos herramientas para

# [25:41.780 --> 25:44.540] generar laboratorios

# [25:45.220 --> 25:49.020] tenemos herramientas para generar laboratorios y tenemos herramientas para

# [25:49.020 --> 25:53.140] poder generar pruebas de estrés o sea que quiere decir eso podemos generar un

# [25:53.140 --> 26:01.660] número n de request fallidos correctos este… para el tipo de los servicios no

# [26:01.660 --> 26:06.780] tengo problema con eso evidentemente podemos generar procesos que alteren la

# [26:06.780 --> 26:13.860] memoria ram o alteren el cp o sea para ese tipo de cuestiones para poder medir

# [26:13.860 --> 26:17.940] picos y demás nosotros podemos tener un laboratorio controlado donde podemos

# [26:17.940 --> 26:20.940] manejar eso

### [26:27.380 --> 26:31.900] existen restricciones presupuestarias o de tiempo para el desarrollo de este sistema

# [26:31.900 --> 26:40.180] de tiempo como tal no… de tiempo como tal no lo que sí es que por lo

# [26:40.180 --> 26:45.460] menos que en cuatro meses necesitamos un prototipo si no es terminado por lo

# [26:45.460 --> 26:52.180] menos sí con la idea terminada si no es poderlo utilizar si por lo menos

# [26:52.180 --> 26:57.740] documentado el prototipo documentado dentro de algo que sí me gustaría que

# [26:57.740 --> 27:04.380] trabajaran sería sobre la sobre la metodología de design thinking

### [27:06.900 --> 27:11.940] ya que está mencionando la parte de las metodologías tiene inconveniente que se

### [27:11.940 --> 27:16.180] utilice alguna más a parte de la que usted…

# [27:16.180 --> 27:18.500] no, pero la principal me gustaría que fuera esa…

# [27:19.460 --> 27:24.220] scrum por ejemplo podemos trabajar con scrum que sean a través de entregables

# [27:24.220 --> 27:30.980] y design thinking que te ayuda muy parecido scrum con entregables pero que

# [27:30.980 --> 27:37.460] son basados en experiencia de usuario y generando mejoras dentro de cada iteración

## [27:37.980 --> 27:44.820] justo nos podría servir para la parte del incremento y estar entregando pues las

## [27:44.820 --> 27:47.940] fases que requiere del proyecto

### [27:50.540 --> 27:53.540] bien

### [27:56.900 --> 28:02.780] bueno como nos mencionó también la parte de los usuarios va a tener una administración…

# [28:02.780 --> 28:08.140] justo, podemos generar roles de administración eso es

# [28:08.140 --> 28:12.740] importante para el sistema que va a controlar la parte de monitoreo no

# [28:12.740 --> 28:16.700] todos los usuarios van a tener la visibilidad de todo obviamente tiene que

# [28:16.700 --> 28:20.020] haber un usuario que va a tener el control y la gestión de los demás

# [28:20.020 --> 28:26.980] usuarios y por ejemplo vamos a suponer que yo tengo un una base de datos y son

# [28:26.980 --> 28:31.540] tres gestión, tres personas que gestionan esta base de datos a lo mejor otros tres

# [28:31.540 --> 28:35.100] servicios y es otro equipo de desarrollo que gestiona

# [28:35.100 --> 28:38.900] que ellos puedan ver, tener la visibilidad como usuario de sus

# [28:38.900 --> 28:41.900] sistemas

# [28:43.700 --> 28:49.620] de los sistemas con los que convives y de los sistemas que administras

# [28:52.620 --> 28:56.420] para eso me gustaría generar un árbol o una teoría de árboles en donde tú defines

# [28:56.940 --> 29:00.340] cuáles son los modos que le vas a asignar a cada usuario

## [29:00.340 --> 29:04.900] si justo eso lo podemos trabajar a futuro checando bien los usuarios y los

## [29:04.900 --> 29:09.220] permisos que va a tener cada usuario este bueno perdón aquí retomando un

## [29:09.220 --> 29:13.780] poquito lo de los usuarios y también desviándome un poquito, aparte de usted

## [29:13.780 --> 29:17.740] habría otras partes interesadas en este proyecto

# [29:17.740 --> 29:24.340] a qué te refieres a parte de mi?

## [29:24.340 --> 29:28.540] o sea por ejemplo ya tiene algún cliente pensado que pueda bueno que tenga a lo mejor algunos requisitos específicos

# [29:28.540 --> 29:33.660] no como tal ese cliente, si tenemos un cliente pero no tiene requisitos específicos el cliente es la

# [29:33.660 --> 29:39.500] compañía dish el cliente está asignado vamos a trabajar con el prototipo con

# [29:39.500 --> 29:43.740] este cliente una vez que ya esté desarrollado el prototipo

# [29:43.740 --> 29:48.700] dish nos va a dar la autorización para poder implementar en su arquitectura este

# [29:48.700 --> 29:55.100] sistema y poderlo utilizar y para empezarlo a probar va a ser digamos

# [29:55.100 --> 30:00.060] un trabajo colaborativo para poder sacar la primera versión

### [30:00.060 --> 30:05.300] bien usted está diciendo que sería la primera versión y bueno como lo estuvimos

### [30:05.300 --> 30:09.460] mencionando ese va a salir por fases

# [30:11.020 --> 30:16.620] lo que yo quiero en esa parte es que ustedes me determinen hasta dónde

# [30:16.940 --> 30:21.340] qué fases o qué módulos o qué características tendría el monitoreo

# [30:21.340 --> 30:27.060] en la primera fase esa propuesta ustedes me la tienen que traer eso es lo que yo

# [30:27.060 --> 30:29.980] quiero que ustedes me traigan la propuesta donde me digan de aquí a

# [30:29.980 --> 30:35.580] aquí vamos a monitorear a lo mejor recursos vamos a monitorear a lo mejor

# [30:35.580 --> 30:41.300] desconexión de red nada más y vamos a trabajar con un protocolo o un puerto EL 8080

# [30:41.300 --> 30:47.780] un ejemplo no? y justo eso

# [30:53.780 --> 31:01.540] con ese primer prototipo yo tengo que llevarlo con el cliente para explicarle

# [31:01.540 --> 31:05.700] qué es lo que va a ser el sistema obviamente ya estoy hablando de que de

# [31:05.700 --> 31:10.500] que va a ser un sistema ya más más robusto porque evidentemente aparte de

# [31:10.500 --> 31:15.540] generar el monitoreo voy a tener el front y el back end el que va a gestionar

# [31:15.540 --> 31:22.100] administrar y el que va a mostrar todo lo que están monitoreando aparte del

# [31:22.100 --> 31:27.540] que ya deben de tener el motor que va a analizar la data que están en estos

# [31:27.540 --> 31:30.260] nuevos de monitoreo

## [32:19.580 --> 32:23.700] le queremos hacer otra pregunta más que nada con la parte de implementación

## [32:23.700 --> 32:28.940] tendría este algún problema o más bien alguna preferencia en la manera en la

## [32:28.940 --> 32:32.260] que se va a instalar o sea por ejemplo tendría algún problema en que se tenga

## [32:32.260 --> 32:39.620] que instalar en conjunto con pues no sé con la aplicación con el sistema o sea

## [32:39.620 --> 32:44.140] que se tenga que instalar en todos los dispositivos que quiera monitorear

# [32:44.140 --> 32:50.980] a que te refieres con problemas?

## [32:50.980 --> 32:55.060] a bueno más que nada preferencia o sea digo la aplicación al final de cuentas la vamos a hacer de la manera más este bueno

## [32:55.060 --> 33:00.460] mejor optimizada posible para que justo no consuma…

# [33:00.460 --> 33:03.740] para la parte del laboratorio que van a tener van a tener un laboratorio virtual que es lo que se les

# [33:03.740 --> 33:08.660] va a poder proporcionar que va a tener máquinas virtuales con servidores linux

# [33:08.660 --> 33:13.460] windows algunos procesos que se van a estar ejecutando para poder probar los

# [33:13.460 --> 33:18.020] procesos evidentemente con quien podremos tener

# [33:18.020 --> 33:21.740] algún problema de instalar estos procesos o procedimientos ya con el

# [33:21.740 --> 33:27.260] cliente que tendrán que ser algunas autorizaciones algunas partes legales

# [33:27.260 --> 33:35.700] algunos temas de permisos sobre todo este pero no debe ser invasivo debe ser

# [33:35.700 --> 33:41.100] muy transparente lo más transparente que se pueda si obviamente primero se le va

# [33:41.100 --> 33:44.580] a mostrar al cliente en un ambiente controlado antes de que acepte que ya lo

# [33:44.580 --> 33:49.340] va a pasar a sus servidores y en sus servidores evidentemente van a tener

# [33:49.340 --> 33:53.220] otros problemas porque entre ellos serían pues el tema de seguridad que

# [33:53.220 --> 33:57.620] tiene cada corporativo que es muy diferente sí y que tendrían ustedes que contemplar justamente

### [33:57.620 --> 34:04.820] la parte de los accesos que nos está comentando

### [34:04.820 --> 34:09.420] esos son directamente con usted o hay alguna persona que se encarga de su

### [34:09.420 --> 34:13.580] empresa que nos estaríamos tendríamos que tener contacto directamente con él

# [34:13.580 --> 34:16.780] les proporcionaría un

# [34:17.500 --> 34:27.180] un vmwar para que ustedes puedan armar el laboratorio y evidentemente bueno yo

# [34:27.180 --> 34:33.060] les ayudaría en la elaboración del laboratorio con los servicios los

# [34:33.060 --> 34:37.940] sistemas operativos y los procesos que saturen la memoria ram o el disco duro

## [34:37.940 --> 34:45.420] bueno regresando un poquito a esta parte de normativas

## [34:45.460 --> 34:49.700] justo hay alguna normativa que tengamos que tomar en cuenta para el desarrollo

## [34:49.700 --> 34:53.580] de esta aplicación pues no sé incluso bueno puede ser de por ejemplo de

## [34:53.580 --> 34:57.060] almacenamiento de datos aunque vamos a seguir como con los estándares para

## [34:57.060 --> 35:03.140] sacar una aplicación al mercado

# [35:03.140 --> 35:08.900] como todo sistema ustedes tienen que tener en su sistema en el sistema que va a trabajar con la data del monitoreo tienen

# [35:08.900 --> 35:14.420] que tener justamente esa información de cuánta ram van a ocupar para qué

# [35:14.420 --> 35:18.860] capacidad de request y para cuántos nodos se tienen que tener ese análisis

# [35:18.860 --> 35:24.740] bien determinado si yo voy a si yo voy a monitorear 4 nodos de cada nodo voy a

# [35:24.740 --> 35:31.860] monitorear 16 puertos un ejemplo y esos 16 puertos me va a dar este me va a

# [35:31.860 --> 35:39.060] ver me va a generar un giga de información por día un ejemplo esas

# [35:39.060 --> 35:43.340] capacidades ustedes las tienen que me las tienen que brindar para que yo les

# [35:43.340 --> 35:46.700] pueda dar el laboratorio con las capacidades que requieren ya hablando

# [35:46.700 --> 35:51.860] de la integración de la plataforma que ustedes van a crear para las demás

# [35:51.860 --> 35:55.060] plataformas pues evidentemente son los recursos que ya tiene el cliente

# [35:55.060 --> 35:59.380] asignado para sus servidores y de ahí obviamente en donde ustedes van a operar

# [35:59.380 --> 36:04.940] su sistema esas cualidades ustedes me las tienen que brindar

# [36:05.020 --> 36:09.580] o sea tienen que sacar la medición de eso

## [36:09.580 --> 36:13.220] los recursos que vamos a consumir con nuestro sistema

## [36:13.220 --> 36:15.220] vale

### [36:16.060 --> 36:21.660] otra pregunta que tengas

## [36:21.660 --> 36:24.660] no por mi parte creo que ya sería todo no sé tú también alguna pregunta extra

### [36:25.100 --> 36:29.420] bueno ahorita nos estamos llevando una gran cantidad de información

## [36:29.420 --> 36:33.820] bueno igualmente pues queríamos ver si usted quería preguntarnos algo a nosotros tiene

## [36:33.820 --> 36:40.180] alguna inquietud

# [36:40.180 --> 36:45.460] nada me gustaría ver una propuesta justamente con todo lo que

# les acabo de comentar que es lo que quiero y ya que ustedes me trajeran una

# [36:45.460 --> 36:51.620] propuesta que yo pueda digerir un poco mejor ver este

# [36:51.620 --> 36:57.980] qué es lo que pueden ofrecer qué es lo que pueden realizar cómo lo realizan

# [36:57.980 --> 37:03.980] si me interesa saber me interesa saber aparte de cómo lo van a realizar

# [37:03.980 --> 37:08.660] cómo atacarán cada uno de los problemas que les comenté

### [37:08.660 --> 37:13.820] más que nada para desmenuzar cada punto más de detalle

# [37:15.020 --> 37:23.100] ¿Alguna otra duda?

## [37:23.100 --> 37:27.180] no por nuestra parte ya sería todo ya la siguiente sesión le traeremos una propuesta y justo ya podría ser un mejor análisis en la

# [37:27.180 --> 37:30.460] siguiente sesión nos van a traer una propuesta

# Análisis de Requerimiento

Lista de requerimientos identificados en este primer acercamiento con el cliente:

| ID | Nombre del requerimiento | Descripción |
| --- | --- | --- |
| RQ1 | Gestión de usuarios | El sistema debe incluir funcionalidades de gestión de usuarios que permitan a los administradores asignar roles con diferentes niveles de permisos y responsabilidades a los usuarios del sistema. |
| RQ2 | Detección de tipo de servidor | El sistema debe ser capaz de detectar si el servidor está físicamente alojado o virtualizado.  El sistema debe recopilar métricas relevantes por cada tipo de servidor .  Identificar plataformas de virtualización específica utilizada como VMware, Hyper-V, KVM entre otras.  Distinción entre recursos virtualizados.Diferencias entre servidores físicos y virtuales en las métricas(Esto ayudará a diferenciar claramente entre los recursos de los servidores físicos y virtuales y a entender cómo están usando los recursos en cada nivel de infraestructura).  El sistema debe ser capaz de adaptarse dinámicamente en función del entorno, considerar la posibilidad de que el sistema pueda adaptarse dinámicamente a cambios en el entorno como la migración de VM entre servidores físicos y virtuales |
| RQ3 | Detección del tráfico de red | El sistema debe ser capaz de analizar y registrar el tráfico de red entrante y saliente.  El sistema debe identificar patrones de tráfico inusuales que puedan identificar problemas de seguridad  El sistema debe ser capaz de analizar protocolos y aplicaciones.  El sistema debe ser capaz de analizar puertos.  El sistema debe ser capaz de realizar análisis de paquetes DPI, identificar firmas de malware.  El sistema debe ser capaz de generar un modelado basado en machine learning para modelar el comportamiento normal del tráfico de red y detectar desviaciones significativas de ese modelo.  El sistema debe ser capaz de generar un bloqueo o mitigación de anomalías existentes en la red, debe considerar posibilidades de capacidad de bloqueo de conexiones sospechosas.  El sistema debe tener una integración con sistema de gestión de eventos de información de seguridad. SIEM para permitir una mejor correlación entre eventos de una respuesta ante incidentes. |
| RQ4 | Notificaciones de eventos específicos | El sistema debe ser capaz de generar notificaciones de las métricas y el rendimiento de lo que está monitoreando, así mismo debe enviar una alerta en caso de encontrar anomalías así como cuando encuentre patrones detectados fuera del uso histórico, debe ser capaz de identificar sobrecalentamientos y saturación de cualquier tipo. |
| RQ5 | Respuestas y Fallas microservicios a monitorear | El sistema debe identificar los tipos de respuestas proporcionadas por los microservicios, así como detectar y registrar cualquier falla durante las mismas |
| RQ6 | Gestión de Recursos de la arquitectura | El sistema debe contar con funcionalidades de supervisión de recursos como son:   1. Almacenamiento del disco duro 2. El uso de la CPU 3. La memoria RAM   Recursos a nivel proceso, el sistema debe ser capaz de monitorear el uso global de recursos, el sistema puede proporcionar detalles a nivel proceso sobre que aplicaciones o servicios están consumiendo más recursos y en qué momento, esto será útil para identificar los (cuellos de botella, aplicaciones problemática y el rendimiento de cada sistema)  El sistema debe ser capaz de identificar tendencias y patrones. |
| RQ7 | Capacidad de configuraciones de umbrales y alertas | El sistema debe permitir a los administradores configurar umbrales para cada recurso monitoreado y generar alertas automáticas cuando se superan estos umbrales.  Las alertas deben ser configurables y pueden ser enviadas a través de diferentes canales de comunicación, como correo electrónico, mensajes de texto o notificaciones en la interfaz del usuario. |
| RQ8 | El sistema debe tener la facultad de integrarse a otros sistemas | La integración de sistemas debe ser mediante herramientas que faciliten su uso, APIS, Intercambio de información fácil de utilizar e interpretar información estructurada. |
| RQ9 | Generación de métricas para graficación | El sistema debe generar métricas y estadísticas a partir de los datos recopilados, que sean adecuados para ser visualizados en gráficos. |
| RQ10 | Gráficas en tiempo real | Se requiere que el sistema tenga gráficas que en tiempo real presente las métricas generadas.  Debe ser entendible para los usuarios finales, mostrando el estado actual de los recursos monitoreados de manera clara. |

| Requerimiento No Funcional | Nombre | Descripción |
| --- | --- | --- |
| RNF1 | Capacidad de Gestión y Escalabilidad de Datos | El sistema debe ser capaz de manejar grandes volúmenes de datos y escalar según sea necesario para adaptarse al crecimiento de la infraestructura de la red. |
| RNF2 | Monitoreo en Tiempo Real | El sistema debe tener un rendimiento óptimo, minimizando el impacto en los recursos del servidor mientras realiza el monitoreo en tiempo real y genera métricas. |
| RNF3 | Disponibilidad y Supervisión Continua con Respaldo en el sistema | El sistema debe estar disponible en todo momento para garantizar una supervisión continua de la infraestructura del mismo.  Se deben implementar medidas de redundancia y recuperación ante desastres para minimizar el tiempo de inactividad en caso de falla del sistema. |
| RNF5 | Seguridad | Se deben implementar medidas de seguridad robustas para proteger los datos sensibles recopilados por el sistema de monitoreo.  Esto incluye cifrado de datos, autenticación de usuarios y acceso controlado a las funciones del sistema. |

No componente

reglas logicas de comportamiento

comportamiento para encontrar los comportamientos

Comenzar con diagramas de casos de uso ( funciones del sistema)

forma general y paso por paso

Gestionamiento de usuario

1-logueo

2-entra al sistema y se verán los módulos de monitoreo de red

3

comenzar con la frase del front end

contrato de confidencialidad,

Seguimiento a requerimientos

Definición de la metodología

7-10 am CC1

Para el monitoreo de red se realizará una base de datos en el cual integraremos los campos como nombre dispositivo, Dirección IP, Tipo de dispositivo ( Físico o virtual) , modelo del dispositivo, marca y tipo de Sistema Operativo , requiere algún otro campo que se deba integrar a esta base de datos.

CONTEXTO

Durante el primer encuentro con el cliente, Cesar Gutiérrez, propietario de una empresa de desarrollo de software, se obtuvieron una serie de necesidades para el desarrollo de un nuevo proyecto que lleva por nombre Fault Trace Sistema para detectar fallas en sistemas distribuidos.César Gutiérrez está crear este sistema y ofrecer una solución que aborde las deficiencias actuales en el monitoreo de sistemas a sus clientes, los cuales actualmente no cuentan con un sistema integral para monitorear sus fallas y establecer protocolos contingentes. Además, no tienen acceso a un sistema de gestión de fallas que les proporcione notificaciones claras y una fácil interpretación de los problemas.

En términos de objetivos específicos, se identificaron diversas áreas clave, como el monitoreo de la red, rendimiento de servidores, la detección de cuellos de botella y altos picos de funcionalidad en los que los sistemas experimentan un aumento significativo en la actividad o la carga de trabajo. Estos picos pueden estar relacionados con períodos de alta demanda, eventos específicos o situaciones inesperadas que generan un aumento repentino en la actividad del sistema.El cliente también enfatizó la importancia del sistema de monitoreo en varias plataformas y sistemas de telecomunicaciones, bases de datos y microservicios.

En cuanto a la metodología de desarrollo, se acordó llevar a cabo el proyecto por fases, comenzando con el monitoreo de red y luego expandiéndose a otros recursos. Se espera utilizar prototipos por fases para realizar pruebas y correcciones, con un enfoque en la metodología de Design Thinking para guiar el proceso de desarrollo.

Se enfatizó la importancia de la transparencia y la comunicación durante todo el proceso de desarrollo para garantizar el éxito del proyecto

Elección de entrevista para la realización del segundo acercamiento con el cliente.

Semiestructurada :

En este tipo de entrevista es común que el entrevistador tenga un guión de preguntas formuladas con anterioridad, pero estas abren la posibilidad de hacer preguntas de seguimiento o le permiten a la persona entrevistada pedir aclaraciones o, incluso, hacer preguntas a los entrevistadores

Dentro del desarrollo de proyectos de tecnologías podemos aplicar lo siguiente para recabar y definir información obtenida antes y actual con las siguientes técnicas:

* **Entrevista de demostración:** En esta entrevista, se puede presentar un prototipo o maqueta inicial del sistema basado en los requisitos identificados hasta el momento. Esto permite al cliente visualizar cómo se están abordando sus necesidades y proporcionar retroalimentación específica sobre el diseño y la funcionalidad propuestos.
* **Entrevista de validación de requisitos:** En esta entrevista, se pueden presentar los requisitos identificados durante el primer encuentro con el cliente y solicitar retroalimentación adicional. Esto ayudará a confirmar si los requisitos capturados son precisos y completos, y si hay aspectos adicionales que el cliente desea agregar o modificar.
* **Entrevista exploratoria:** Esta entrevista tiene como objetivo explorar a fondo las necesidades y expectativas del cliente. Puede incluir preguntas abiertas para permitir que el cliente comparta sus ideas, preocupaciones y requisitos de manera más amplia.
* **Entrevista de priorización:** Durante esta entrevista, se puede discutir la prioridad de los diferentes requisitos identificados. Esto ayudará a entender qué características o funcionalidades son más importantes para el cliente y cuáles deberían recibir mayor atención durante el desarrollo

Cuestionario

1. ¿El sistema implica algunos roles de usuario? Si/No
2. ¿Cómo sería la gestión de usuarios? (Sí deberán haber roles predeterminados o por el contrario la empresa determinará los roles que necesita)
3. ¿Qué protocolos de red te gustaría que sean monitoreados?
4. ¿Cuáles son las plataformas de virtualización más comunes utilizadas por tus clientes?
5. ¿Cuál sería el nivel de priorización de las alertas generadas por el sistema?
6. ¿A través de qué tipo de interfaz te gustaría visualizar el monitoreo?
7. ¿Qué tipo de informes te gustaría que generará el sistema de monitoreo?
8. En el ámbito del monitoreo de red existen eventos y problemas de conectividad como son: fallos de conectividad con dispositivos, caídas de conexión a Internet, sobrecarga de ancho de banda, ataques de red, problemas de latencia, por mencionar algunos.

¿Qué tipos de eventos deberían configurarse para activar alertas automáticas en nuestro sistema de monitoreo o en su caso que otros tipos de eventos le gustaría agregar aparte de los ya mencionados?

1. ¿Qué criterios debería usar el sistema para determinar qué es considerado un patrón inusual?
2. Por la parte de ciberseguridad, existen patrones sospechosos, como intentos de acceso fallidos, tráfico de red anómalo, o actividades inusuales en los microservicios ¿Qué acciones se deberán tomar cuando se detecte un patrón sospechoso?
3. Durante el proceso de monitoreo se estará recopilando datos como; el tráfico de red, uso de recursos, entre otros. ¿Cómo le gustaría visualizar el resultado de la información monitoreada?(Se necesita contexto)
4. ¿Qué tipos de métricas son las que le gustaría recabar y observar en las **gráficas**? se necesita contexto.
5. ¿Cómo le gustaría y con qué notación se definieron los valores de los umbrales para la detección de niveles máximos o mínimos?
6. ¿Qué patrones deben ser identificados como sospechosos en los monitoreos de red, servidores y recursos? en qué tipo de monitoreo
7. ¿Qué puertos son los más comunes que usan sus clientes?
8. ¿Se almacena cifrada la información? y si sí ¿Cuál tipo de cifrado? (Cifrada, en crudo)
9. ¿Con qué frecuencia requiere que se realice el monitoreo?
10. En sistemas, actualmente, se puede filtrar la información ya sea por tipo, orden alfabético, fecha, etc, ¿Se aplicarán filtros a la información? y si sí, ¿cuáles? dame contexto
11. El monitoreo con agente implica instalar software especializado en dispositivos para recopilar datos de rendimiento y estado, mientras que el monitoreo sin agente utiliza protocolos estándar de red y tecnologías incorporadas en los sistemas operativos, como APIs y comandos ¿Le gustaría que su aplicación de monitoreo fuera con un agente o sin agente? contexto
12. ¿El sistema operativo debe detectarse en automático o por el contrario le gustaría que el usuario seleccione el sistema operativo que se piensa monitorear?
13. Dada la vulnerabilidad actual en nuestras credenciales de acceso , es crucial implementar medidas para abordar posibles intentos de acceso fallidos o comportamientos sospechosos relacionados con las cuentas de usuario. ¿Qué estrategias debería seguir el sistema para gestionar estas situaciones?

| **Tipo de Monitoreo** | **APIs Utilizadas** | **Agentes/ Instrumentación** | **Factores de Dificultad** | **Nivel de Dificultad** |
| --- | --- | --- | --- | --- |
| Monitoreo de Red | SNMP, NetFlow/sFlow/IPFIX | Nagios, Zabbix | Requiere conocimiento de protocolos de red, configuración de dispositivos de red. | Media |
| Monitoreo de Servidor | WMI (Windows), /proc (Linux/Unix) | Prometheus, New Relic | Necesita acceso al sistema operativo, puede requerir privilegios elevados. | Media |
| Monitoreo de CPU | Performance Counters (Windows), /proc(Linux/Unix) | Prometheus, Nagios | Depende de acceso a bajo nivel al sistema operativo, necesita configuración detallada para alertas precisas. | Media |
| Monitoreo de Memoria | /proc (Linux/Unix), Performance Counters (Windows) | Grafana, Datadog | Similar al monitoreo de CPU, pero puede ser más sencillo de interpretar. | Media |
| Monitoreo de Aplicaciones | JMX (Java), Prometheus exporters | Dynatrace, AppDynamics | Requiere integración profunda con la aplicación, puede necesitar cambios en el código de la aplicación. | Alta |
| Monitoreo de Seguridad | Syslog, Windows Event Log | Splunk, ELK Stack | Requiere configuración compleja y continua para identificar y correlacionar amenazas. | Alta |
| Monitoreo de Base de Datos | SQL, JMX (para algunas DBs) | SolarWinds, Redgate | Necesita conocimientos especializados en bases de datos, incluyendo consultas SQL para extracción de métricas. | Alta |
| Monitoreo de Infraestructura | SNMP, IPMI | Icinga, PRTG | Puede involucrar monitoreo físico y virtual, necesita configuración de hardware y red. | Media |
| Monitoreo de Logs | Syslog (Linux/Unix), Windows Event Log API | Splunk, ELK Stack, Loggly | Involucra la recolección, almacenamiento y análisis de grandes volúmenes de datos de log. Requiere filtrado y correlación eficientes. | Media |