

UNIVERSIDAD DE TARAPACÁ



UNIVERSIDAD DE TARAPACÁ
Universidad del Estado

FACULTAD DE INGENIERÍA

Departamento de Ingeniería en Computación e Informática

" Sistema de gestión y monitoreo de los equipamientos Informáticos del Departamento de Ingeniería en Computación e Informática "

Integrantes: Nicolás Vargas A.

Asignatura: Proyecto IV

Profesor: Diego Aracena P.

Empresa o
unidad: DGDT-UTA

Arica, 04 de Julio de 2024



Historial de avance

Fecha	Versión	Descripción	Autor(es)
10/04/2024	0.1	Se agregan los objetivo general y objetivos específicos, además de los, requisitos funcionales y no funcionales.	Nicolás Vargas A
20/04/2024	0.2	Se agrega la carta Gantt, la arquitectura del sistema y modelo de contexto utilizados para el proyecto	Nicolás Vargas A
28/04/2024	0.3	Se agrega la descripción de la empresa, metodología y herramientas	Nicolás Vargas A
02/05/2024	0.4	Se agrega la interfaz del front-end, diagramas de casos de uso	Nicolás Vargas A
07/05/2024	0.5	Se realizan mejoras sugeridas (arquitectura del sistema, diagrama de contexto, explicaciones de diagramas de flujo)	Nicolás Vargas A
08/05/2024	0.6	Se corrige errores (objetivos, carta Gantt y diagramas, se realizan mejoras y se agregan BPN	Nicolás Vargas A



Tabla de contenidos

I INTRODUCCIÓN	7
II DEFINICIÓN DEL PROYECTO	8
2.1 Contexto	8
2.2 Problema	8
2.3 Solución	8
2.4 OBJETIVOS	9
2.4.1 Objetivo General	9
2.4.2 Objetivos Específicos	9
2.5 Restricciones	9
2.6 Entregables	9
III REQUISITOS DEL PROYECTO	10
3.1 Requisitos funcionales	10
3.2 Requisitos no funcionales	11
V PLANIFICACIÓN DEL PROYECTO	12
5.1 Metodología	12
5.2 Herramientas	13
5.3 Carta Gantt	14
VI DISEÑO DEL PROYECTO	15
6.1 Arquitectura del sistema	15
6.2 Modelo de contexto	16
6.3 Diagrama de subsistemas	17
6.3 Diagrama de casos de uso	19



6.4 Diagramas BPM	20
6.4.1 Iniciar sesión	20
6.4.2 Visualizar Sistema	21
6.4.3 Gestión de usuarios	22
6.4.4 Gestión de servicios	23
6.4.5 Gestión de host	24
6.4.6 Generar Reportes	25
6.4.7 Configurar Alertas	26
VII Visualización del Front-End	27
VIII IMPLEMENTACIÓN	31
VII Conclusiones	40
REFERENCIAS	41
ANEXOS	42

Tabla de Figuras

Figura 1 Metodología Scrum.	12
Figura 2 Carta Gantt del proyecto.	14
Figura 3 Arquitectura a monitorear	15
Figura 4 Diagrama de contexto del proyecto.	16
Figura 5 Diagrama Iniciar Sesión.	20



Figura 6 Diagrama Visualizar sistema.	21
Figura 7 Diagrama Gestión de usuarios	22
Figura 8 Diagrama Gestión de servicios.	23
Figura 9 Diagrama Gestión de host.	24
Figura 10 Diagrama Generar Reportes	25
Figura 11 Diagrama Configurar alertas.	26
Figura 12 Pantalla inicio de sesión.	27
Figura 13 Pantalla principal	27
Figura 14 Mapa de la red monitoreada	28
Figura 15 Host monitoreados.	28
Figura 16 Sección de hostgroup del sistema.	29
Figura 17 Sección de services del sistema.	29
Figura 18 Sección de reportes del sistema.	30
Figura 19 Inicio de sesión	31
Figura 20 Página principal de Nagios.	31
Figura 21 Navegación por el sitio de Nagios	32
Figura 22 Mapa de la red monitoreada.	33
Figura 23 Host Monitoreados.	34
Figura 24 Servicios monitoreados.	35
Figura 25 Sección de hostgroup creados.	36
Figura 26 Gráficos parte 1 host seleccionado.	37
Figura 27 Gráficos parte 2 host seleccionado.	38
Figura 28 Icono de PDF.	39
Figura 29 PDF generado por el usuario	39
Figura 30 Impact Mapping del proyecto.	42
Figura 31 User story Mapping del proyecto	43



Tabla de Tablas

Tabla 1 Tabla requisitos funcionales	10
Tabla 2 Tabla requisitos no funcionales.....	11
Tabla 3 Herramientas a utilizar.....	13



I INTRODUCCIÓN

La Dirección de Gestión Digital y Transparencia de la Universidad de Tarapacá (DGDT) requiere implementar un sistema de monitoreo en tiempo real para visualizar el estado de los dispositivos y servicios de la infraestructura de red del Departamento de Ingeniería en Computación de la universidad de Tarapacá. Para esto se requiere de Nagios, el cual permitirá obtener información precisa sobre el funcionamiento y la disponibilidad de los dispositivos y servicios monitoreados. Con esta capacidad de monitoreo la DGDT podrá tomar decisiones informadas y responder de manera proactiva a cualquier problema que pueda surgir, garantizando así la continuidad de las operaciones.



II DEFINICIÓN DEL PROYECTO

2.1 Contexto

La Dirección de Gestión Digital y Transparencia de la Universidad de Tarapacá (DGDT) tiene como objetivo implementar un sistema de monitoreo en tiempo real de los dispositivos de red del Departamento de Ingeniería en Computación e Informática de la Universidad de Tarapacá. Este sistema estará diseñado para ofrecer una visualización detallada y actualizada del estado de los dispositivos y servicios.

2.2 Problema

La Dirección de Gestión Digital y Transparencia de la Universidad de Tarapacá (DGDT) busca abordar el problema de supervisar y gestionar la infraestructura de red del Departamento de Ingeniería en Computación e Informática. Esto implica monitorear la disponibilidad y el estado de los dispositivos de red y servicios para detectar y responder rápidamente a problemas que puedan surgir en los dispositivos que componen la red del Departamento de Ingeniería en Computación.

2.3 Solución

La solución consiste en implementar un sistema de monitoreo y gestión utilizando Nagios el cual permita supervisar la disponibilidad, rendimiento, dispositivos de red y servicios. Además de proporcionar alertas en tiempo real sobre problemas y permitir a los administradores de red tomar medidas.



2.4 OBJETIVOS

2.4.1 Objetivo General

Implementar un sistema de gestión y monitoreo de los equipamientos Informáticos del Departamento de Ingeniería en Computación e Informática.

2.4.2 Objetivos Específicos

- Determinar los requisitos, definir los hosts y servicios a monitorear.
- Implementar medidas de seguridad y configurar alertas y umbrales para el monitoreo.
- Establecer un sistema de notificaciones para alertar al equipo de problemas en tiempo real.
- Automatizar la generación de informes sobre el estado de la red y servicios.
- Documentar los procedimientos

2.5 Restricciones

1. El proyecto será ejecutado en un plazo de 3 meses.
2. El sistema debe estar instalado en un sistema Ubuntu Server.

2.6 Entregables

1. Bitácoras para registro de reuniones y acuerdos.
2. Documento de requisitos firmado por el cliente.
3. Informes de avance.
4. Informe final
5. Manual de usuario.
6. Producto final.



III REQUISITOS DEL PROYECTO

3.1 Requisitos funcionales

A continuación, se describen los requisitos funcionales que deberá tener el sistema.

Tabla 1 Tabla requisitos funcionales

Id requisito	Nombre	Descripción
Rf-01	Monitoreo de Dispositivos de Red	El sistema debe ser capaz de monitorear dispositivos de red como routers, switches y servidores para verificar su disponibilidad y rendimiento. Esto incluye la capacidad de detectar cambios en el estado de los dispositivos.
Rf-02	Monitoreo de Servicios	El sistema debe permitir la supervisión de servicios y aplicaciones críticas además se debe ser capaz de detectar fallos en la disponibilidad o en el funcionamiento de estos servicios y generar alertas correspondientes.
Rf-03	Gestión de Alertas	El sistema debe proporcionar una funcionalidad completa para la gestión de alertas, incluyendo la configuración de umbrales de alerta, la definición de destinatarios, etc.
Rf-04	Informes de Rendimiento	Se requiere la capacidad de generar informes periódicos sobre el rendimiento de la infraestructura de red y de los servicios monitoreados. Estos informes deben incluir estadísticas relevantes para la evaluación del rendimiento del sistema.
Rf-05	Iniciar Sesión con Privilegios	Los usuarios deben poder iniciar sesión en el sistema con sus credenciales personales, y dependiendo de sus privilegios, acceder a funcionalidades específicas.



3.2 Requisitos no funcionales

Tabla 2 Tabla requisitos no funcionales.

Id del requisito	Nombre	Descripción
RNF-01	Disponibilidad	El sistema debe estar disponible de manera continua, con un alto nivel de disponibilidad para garantizar que esté operativo en todo momento y que no haya interrupciones en la supervisión de la infraestructura de red.
RNF-02	Escalabilidad	El sistema debe ser escalable, permitiendo la incorporación de nuevos dispositivos y servicios a medida que la infraestructura de red crece, así como la capacidad de gestionar un número creciente de usuarios y de datos de monitoreo.
RNF-03	Seguridad	El sistema debe cumplir con los estándares de seguridad de la información, garantizando la confidencialidad, integridad y disponibilidad de los datos de monitoreo. Debe contar con mecanismos robustos de autenticación y autorización para proteger el acceso no autorizado.

V PLANIFICACIÓN DEL PROYECTO

5.1 Metodología

El proyecto utiliza la metodología SCRUM, que facilita una retroalimentación rápida entre el equipo de desarrollo y el cliente. Esto permite desarrollar prototipos tempranos y reducir el riesgo de errores en los requisitos del cliente. La metodología se implementa mediante reuniones semanales donde se revisan las tareas completadas y pendientes, se planifican las actividades para la próxima semana y se ajusta el proyecto según sea necesario para alcanzar los objetivos establecidos.

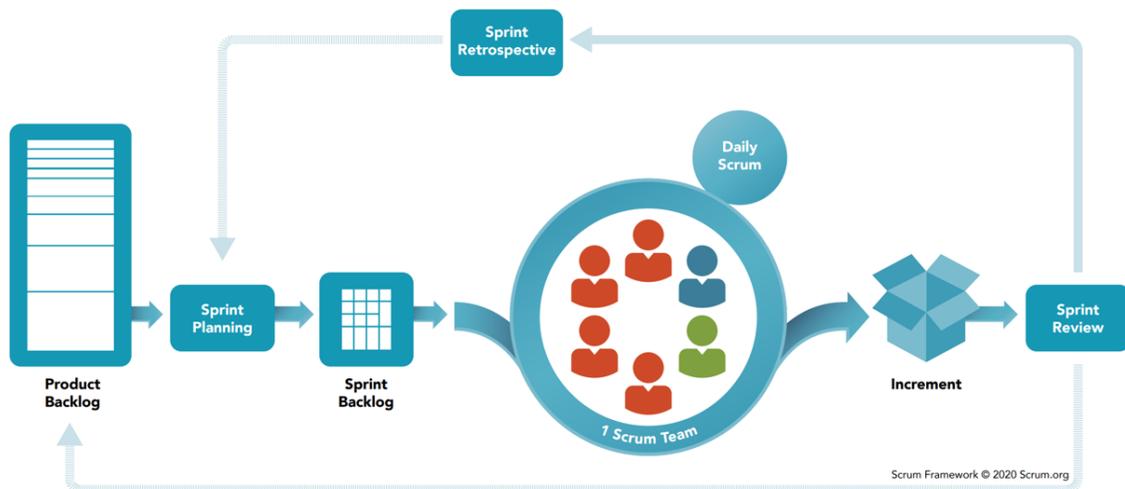


Figura 1 Metodología Scrum.



5.2 Herramientas

A continuación, se detallan las herramientas que serán utilizadas en el proyecto

Tabla 3 Herramientas a utilizar.

Nombre	Función
Ubuntu Server	Sistema operativo base para alojar Nagios y otros servicios necesarios.
Servidor Apache	Necesario para acceder a la interfaz web de Nagios y administrar el sistema de monitoreo.
Nagios Core	La parte central del sistema de monitoreo, responsable de realizar el monitoreo y generar alertas.
Nagios Plugins	Conjunto de scripts y herramientas que Nagios utiliza para realizar las verificaciones.
Cliente correo electrónico	Para recibir notificaciones por correo electrónico sobre eventos de monitoreo.
Nano	Editor de texto a través de consola
Firewall	Configurado para permitir el tráfico necesario para Nagios y sus componentes.
PNp4	Herramienta para gráficos, reportes y estadísticas en general



5.3 Carta Gantt

La figura 2, detalla la planificación del proyecto, entregables y su respectiva fecha de compromiso.

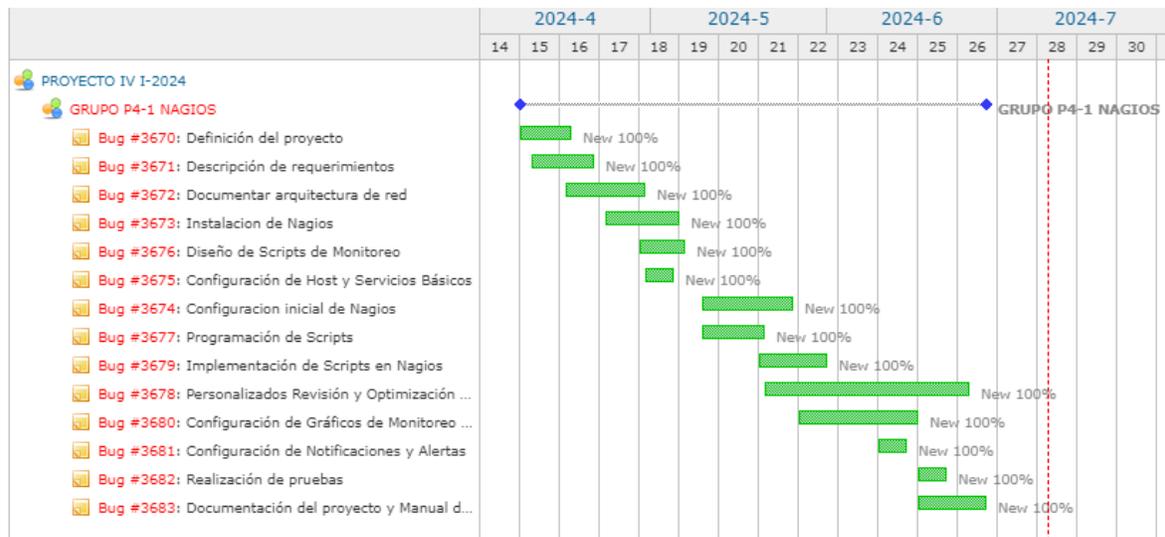


Figura 2 Carta Gantt del proyecto.



VI DISEÑO DEL PROYECTO

6.1 Arquitectura del sistema

La figura 3 detalla la arquitectura de la infraestructura de la red existente en el departamento de Ingeniería en Computación e Informática en el cual se desea monitorear Servidores, Switch, Access Point y Router.

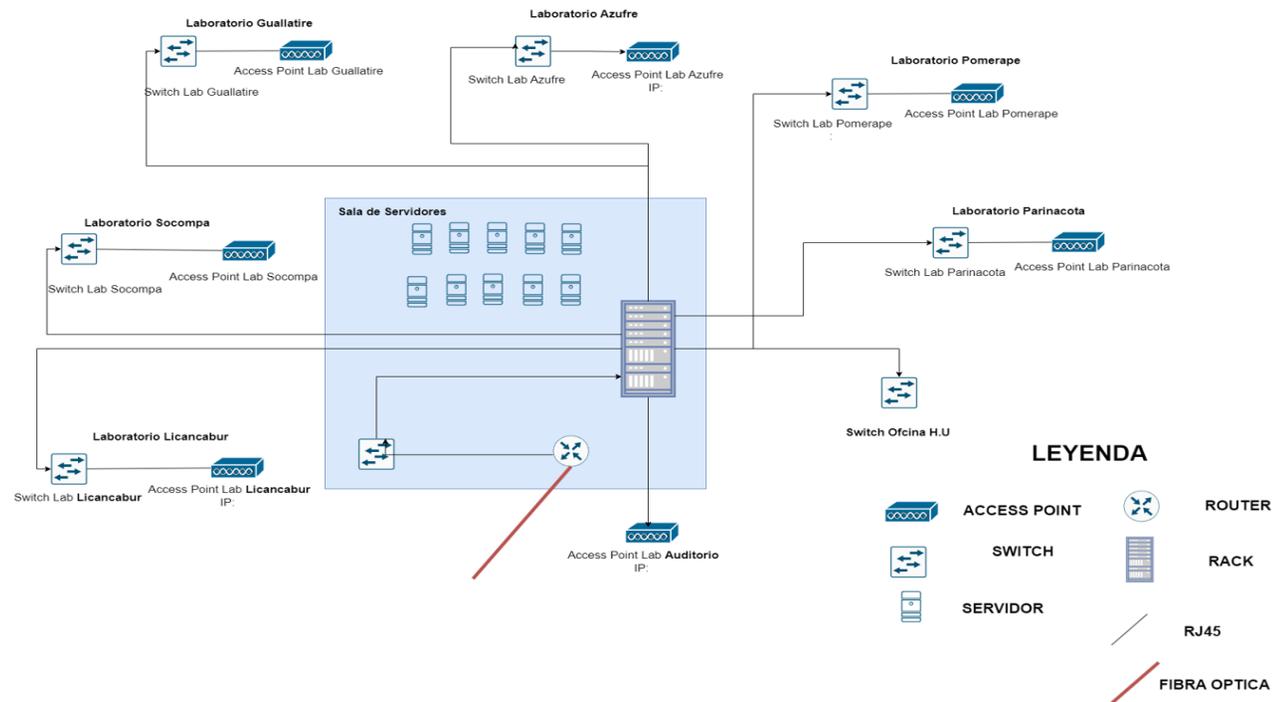


Figura 3 Arquitectura a monitorear



6.2 Modelo de contexto

La figura 5 muestra un diagrama de contexto del sistema de monitoreo de red utilizando Nagios en el cual se destacan:

Administradores: Configura, gestiona Nagios y recibe reportes de estado del sistema.

Dispositivos de Red: Son monitoreados por Nagios mediante chequeos de servicios.

Usuarios: Reciben notificaciones y alertas desde Nagios sobre el estado del sistema.

Servicios: Son monitoreados por Nagios para servicios como HTTP, SSH, etc.

Nagios: Software de monitoreo.

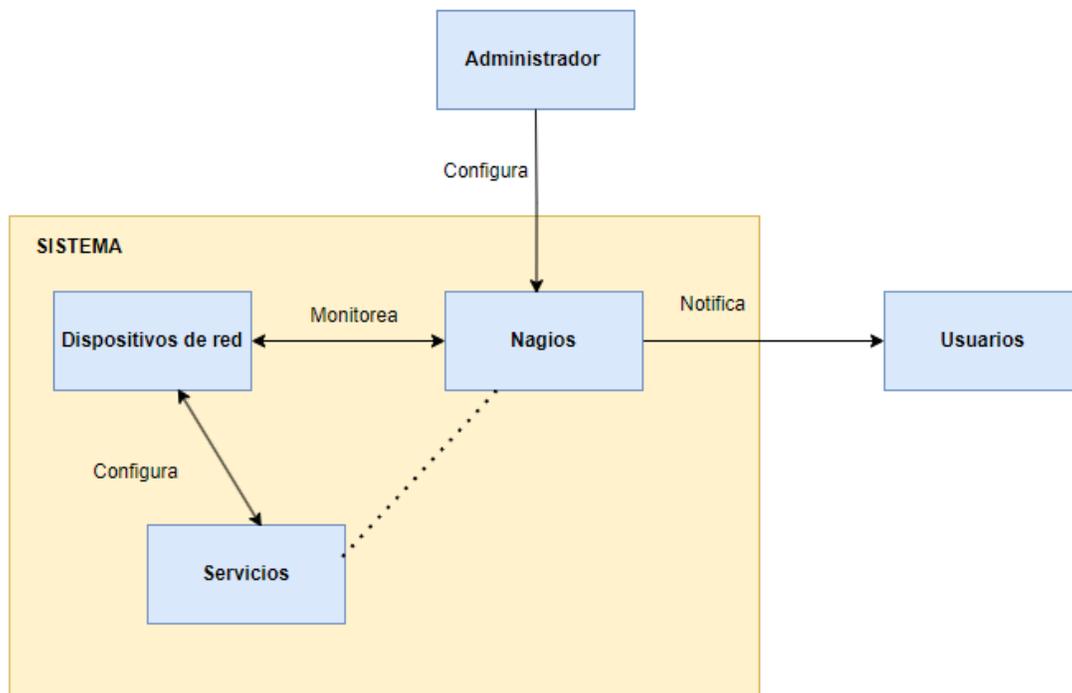


Figura 4 Diagrama de contexto del proyecto.



6.3 Diagrama de subsistemas

La figura 6 muestra un diagrama de subsistemas del sistema de monitoreo, para lo cual se detallan los subsistemas detectados

Gestión de servicios: Es el encargado de gestionar los servicios que serán monitoreados en el sistema, también se pueden crear, editar o eliminar según sea lo requerido.

Gestión de usuarios: Es el encargado de gestionar los usuarios que usaran el sistema, también se pueden crear, editar o eliminar según sea lo requerido. Solo pueden ser gestionados por el administrador.

Gestión de host: Es el encargado de gestionar los hosts que usara el sistema, también se pueden crear, editar o eliminar según sea lo requerido. Solo pueden ser gestionados por el administrador.

Gestión de alertas: Es el encargado de gestionar las alertas que usaran el sistema cuando se presente algún inconveniente. Solo pueden ser gestionados por el administrador.

Gestión de visualización de datos: Es el encargado de recopilar información de todos los dispositivos y servicios para visualizar mediante gráficos en tiempo real.

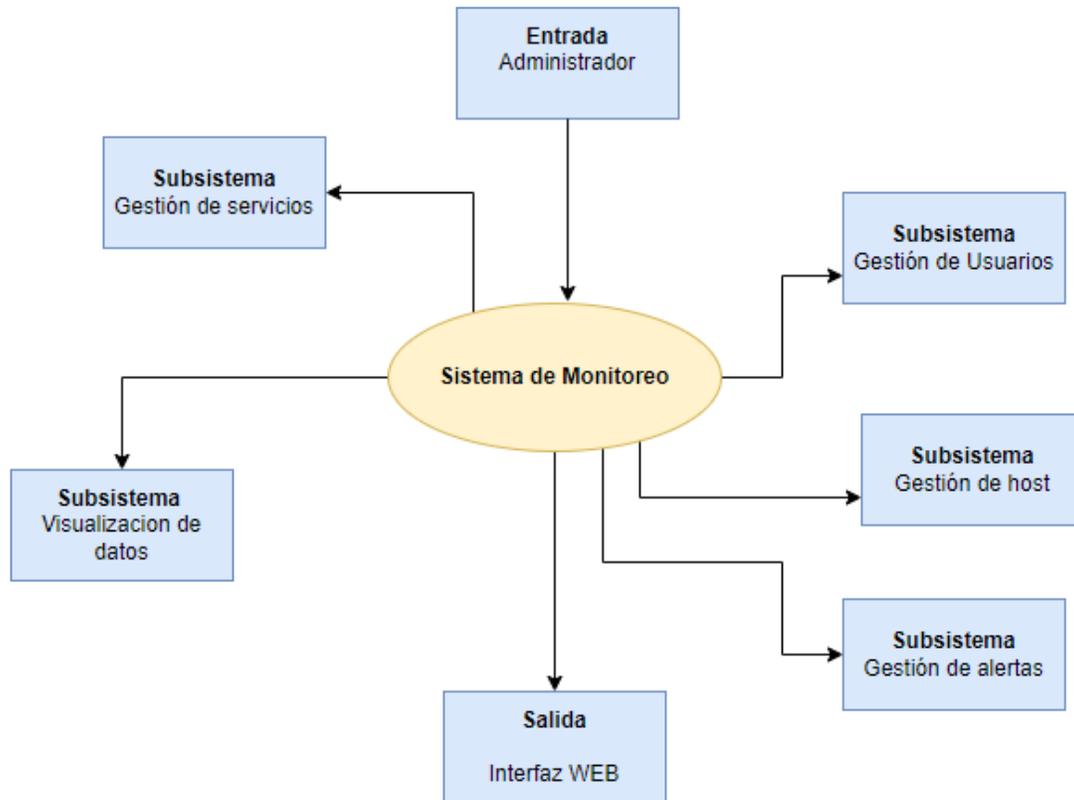


Figura 6 Diagrama de subsistemas.

6.3 Diagrama de casos de uso

La figura 7 muestra el diagrama de casos de uso del sistema que cuenta con dos usuarios: un administrador el cual puede agregar eliminar y modificar usuarios, servicios y host y un usuario sin privilegios el cual solo puede ver el monitoreo en tiempo real sin realizar cambios en el sistema

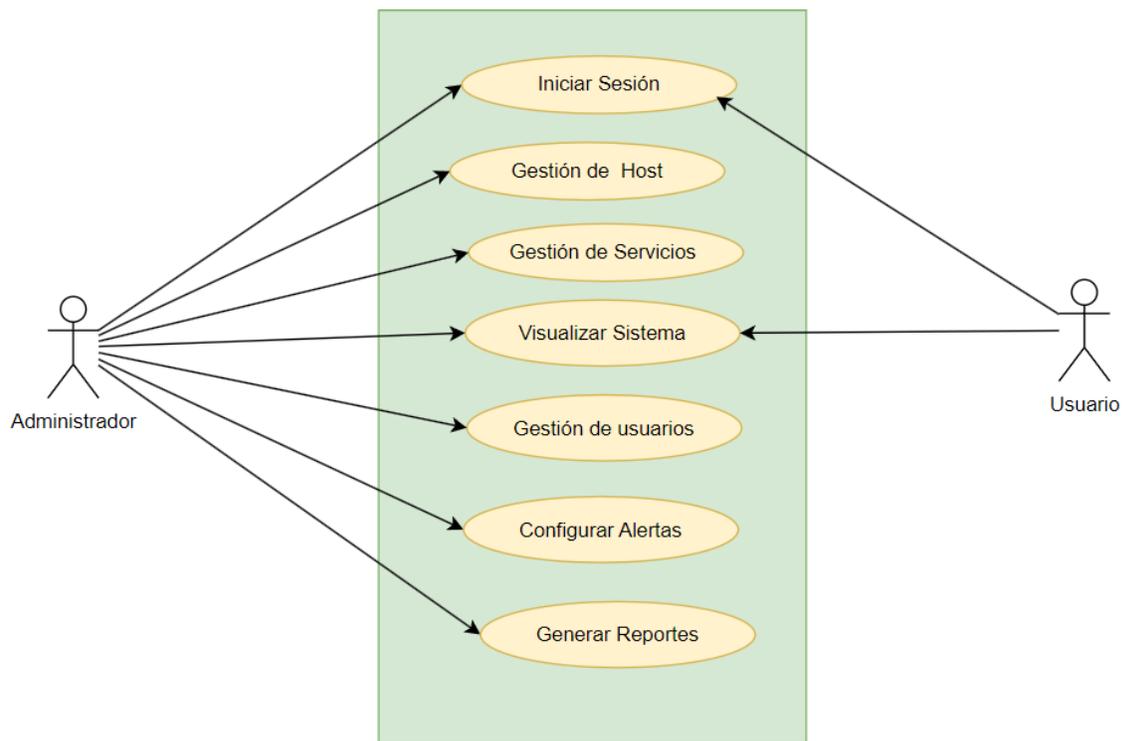


Figura 7 Diagrama de casos de uso de sistema.



6.4 Diagramas BPM

6.4.1 Iniciar sesión

La figura 7 muestra el flujo normal para un inicio de sesión comprobando si los datos ingresados son correctos o no, si los datos son correctos el usuario logra ingresar correctamente al sistema, de lo contrario muestra un mensaje de error.

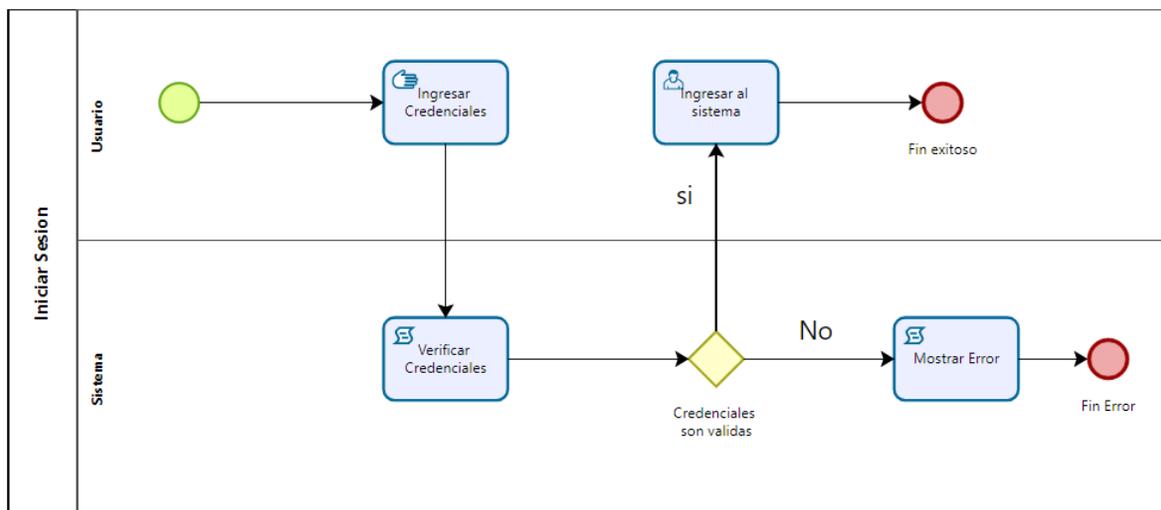


Figura 5 Diagrama Iniciar Sesión.



6.4.2 Visualizar Sistema

La figura 8 muestra el flujo normal para que un usuario visualice el sistema en el cual si el usuario desea moverse a otra sección puede hacerlo sin mayores problemas.

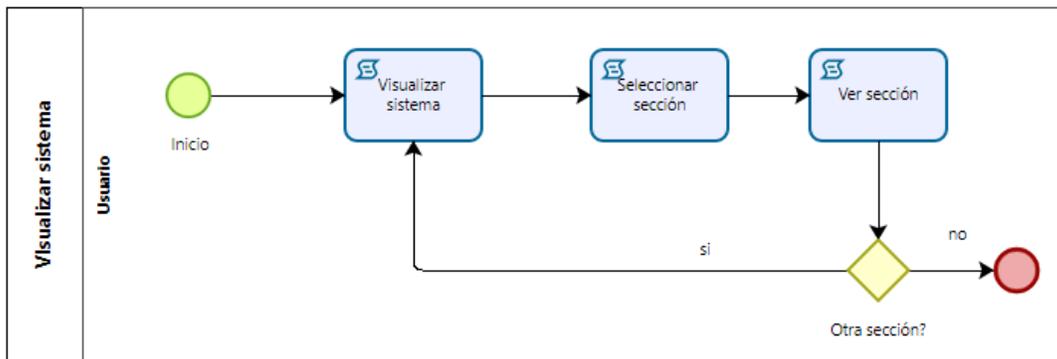


Figura 6 Diagrama Visualizar sistema.

6.4.3 Gestión de usuarios

La figura 9 muestra el flujo normal de gestión de usuarios donde pueden agregar, editar o eliminar usuarios según las necesidades de administrador del sistema.

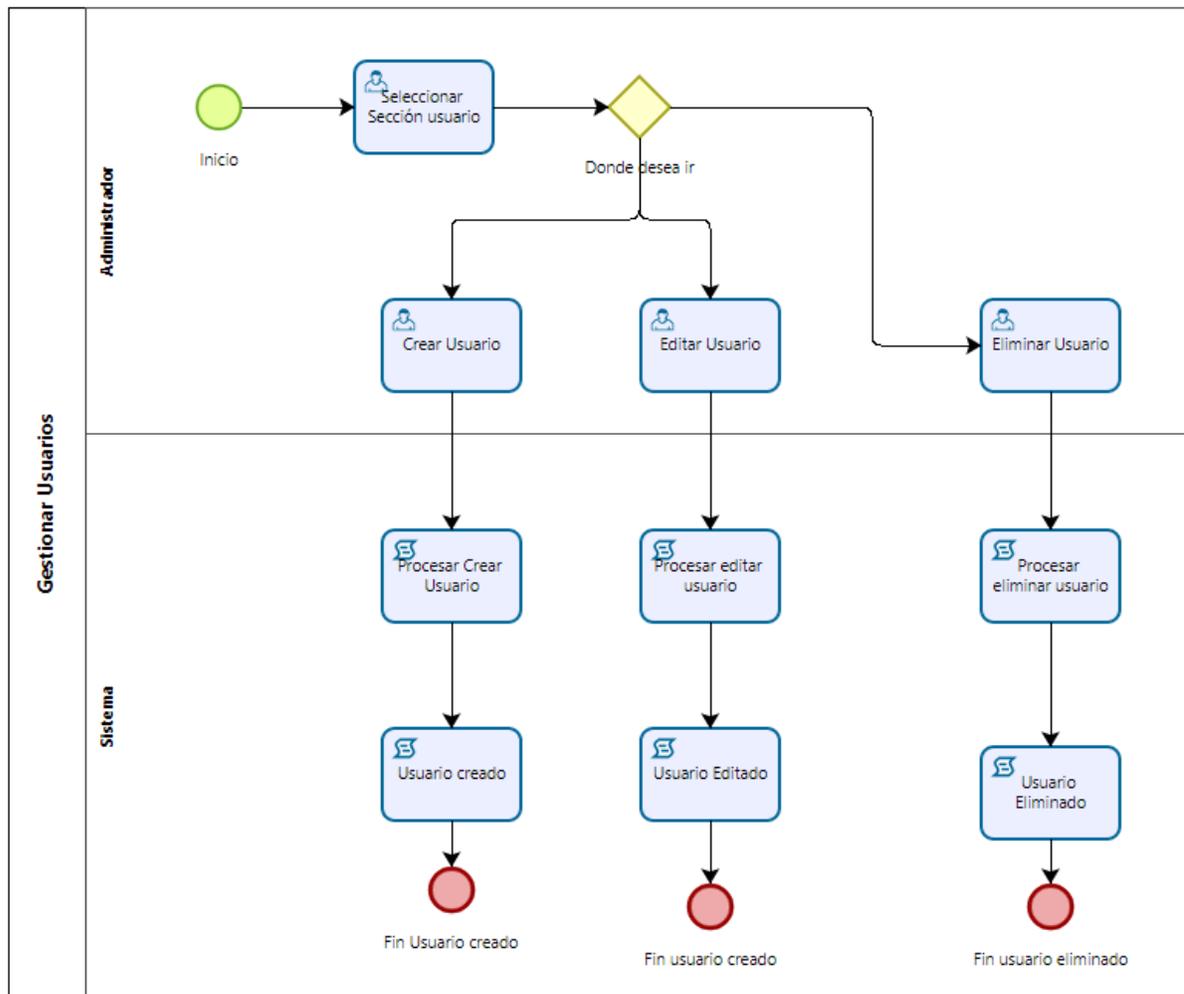


Figura 7 Diagrama Gestión de usuarios

6.4.4 Gestión de servicios

La figura 10 muestra el flujo normal de gestión de servicios en donde un usuario administrador puede agregar, editar o eliminar un servicio que se está monitoreando.

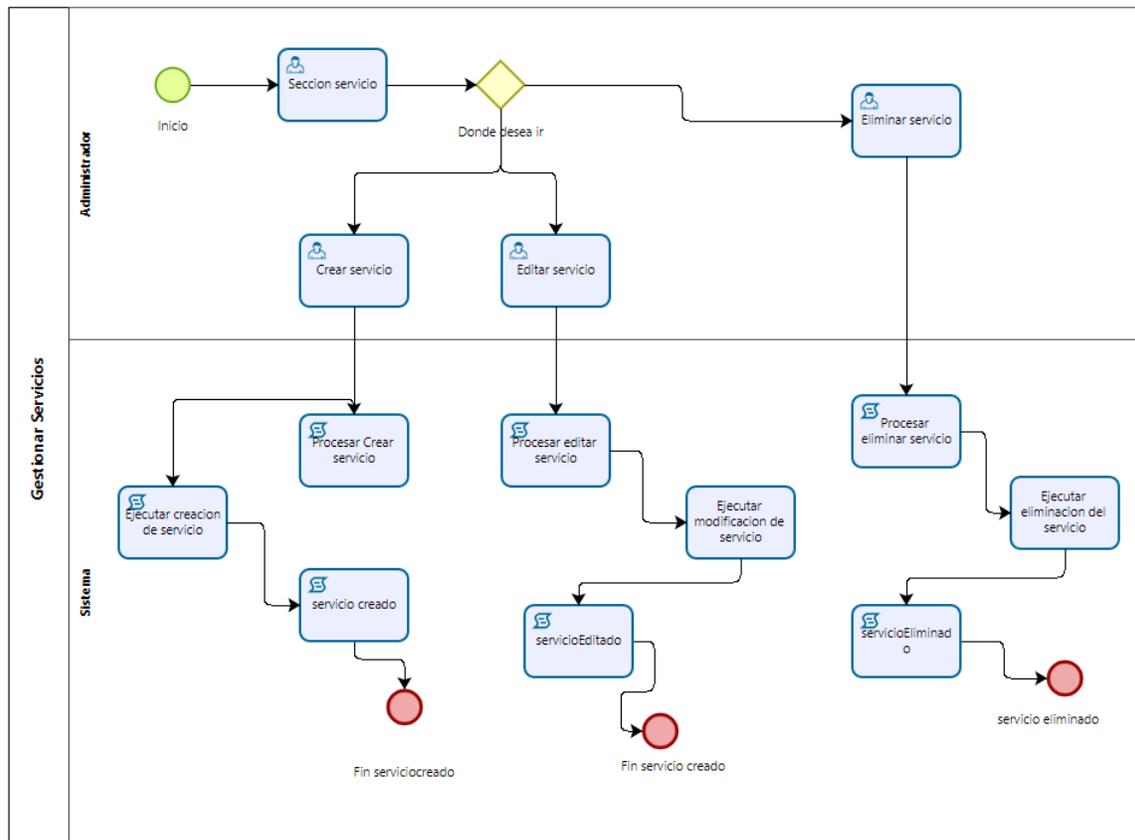


Figura 8 Diagrama Gestión de servicios.

6.4.5 Gestión de host

La figura 11 muestra el flujo normal de gestión de host en donde un usuario administrador puede agregar, editar o eliminar un host que se será monitoreado.

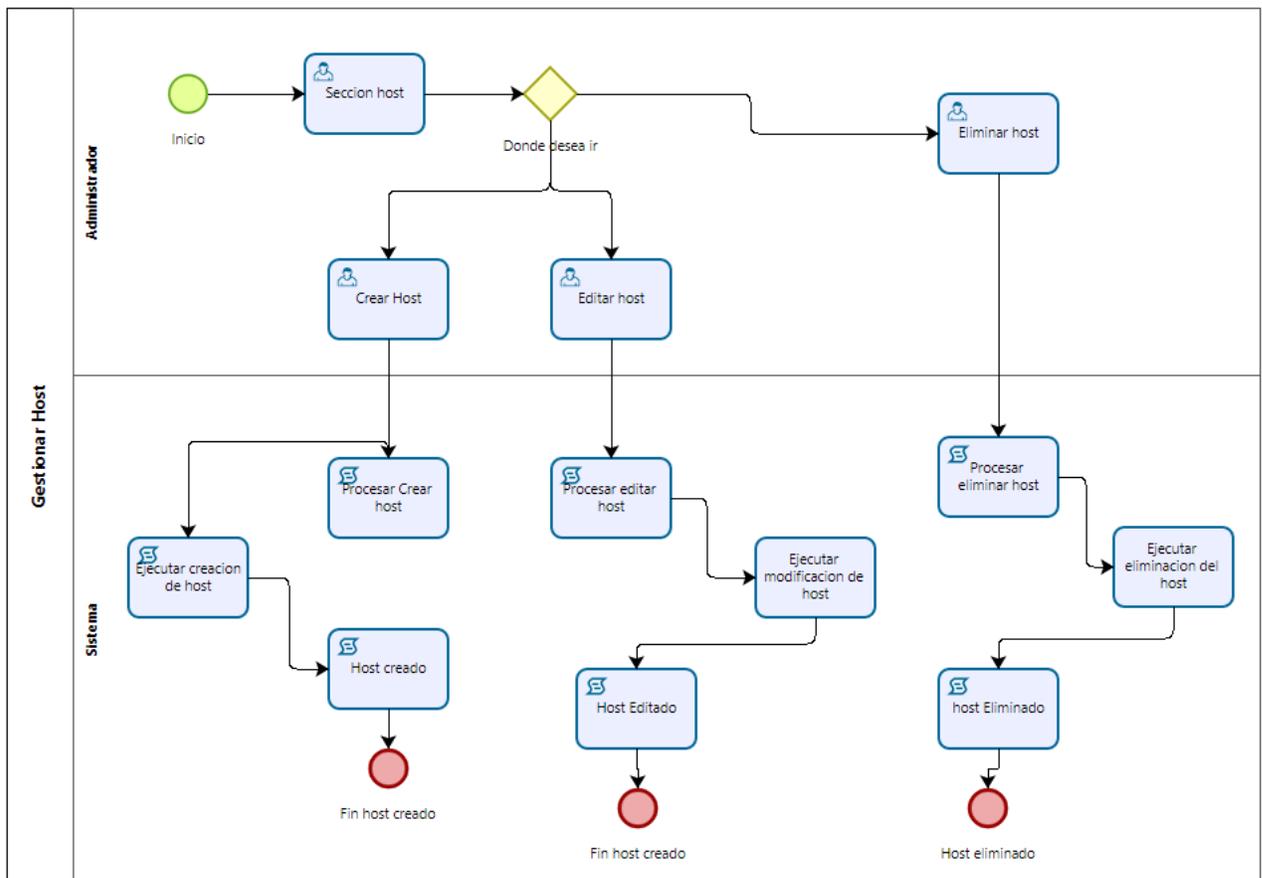


Figura 9 Diagrama Gestión de host.



6.4.6 Generar Reportes

La figura 12 muestra el flujo normal de como generar reportes estadísticos para un servicio o host seleccionado previamente por el administrador.

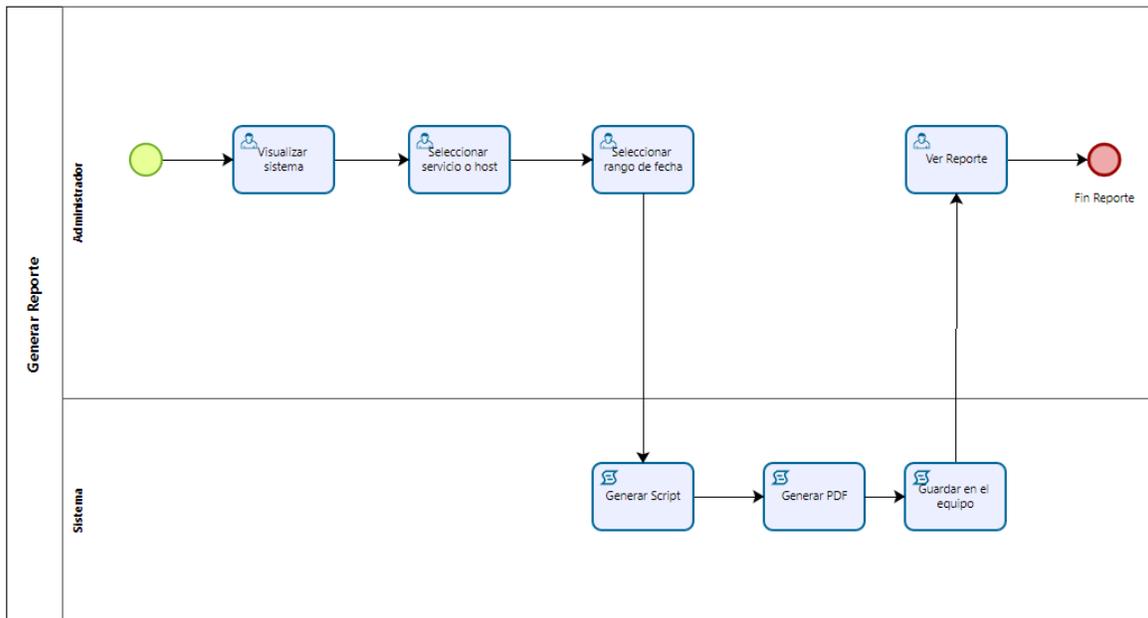


Figura 10 Diagrama Generar Reportes

6.4.7 Configurar Alertas

La figura 13 muestra el flujo normal del proceso de configurar alertas en donde un administrador configura las alertas en caso de que el sistema detecte un problema o un host o servicio se encuentre caído.

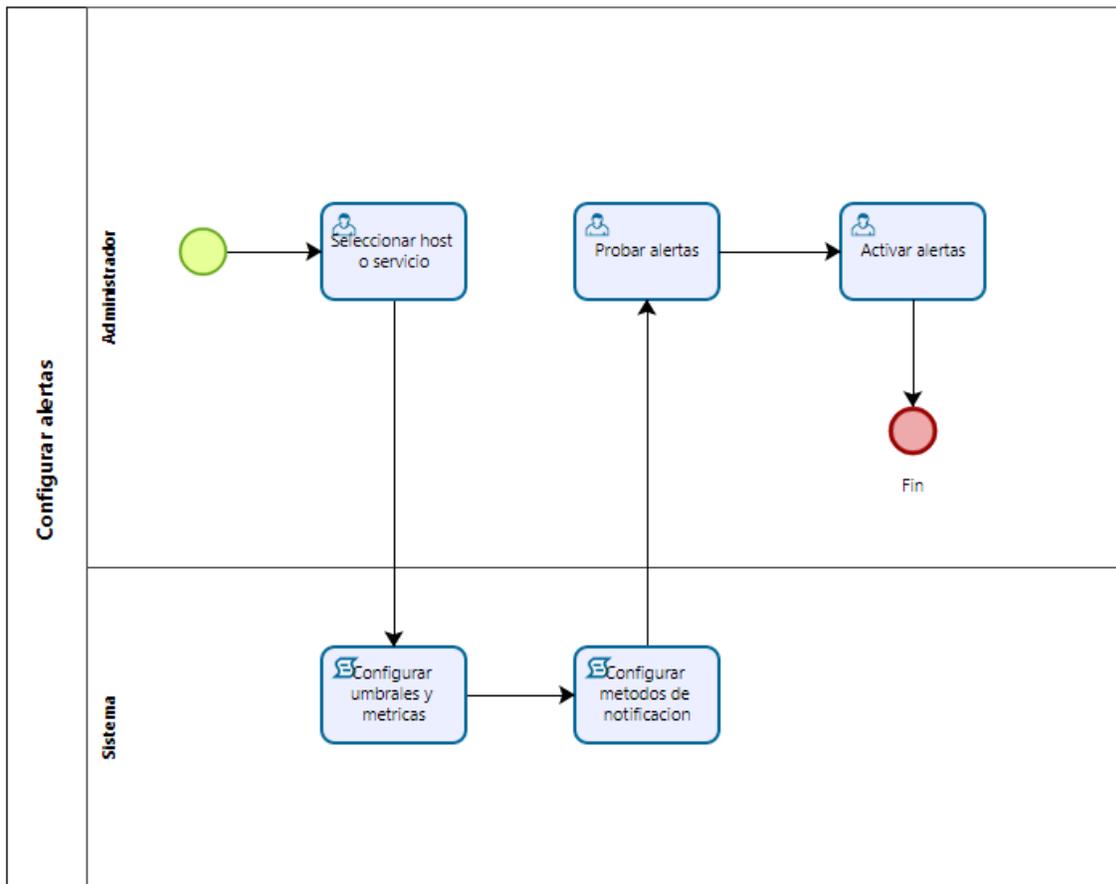


Figura 11 Diagrama Configurar alertas.

VII Visualización del Front-End

Se realizó en Balsamiq algunos prototipos de cómo se verá el sistema una vez que ya se encuentre implementado a continuación se detallan algunas secciones que se fueron realizadas. La figura 14 muestra cómo sería el inicio de sesión donde los usuarios deberán ingresar sus datos para validar sus credenciales.

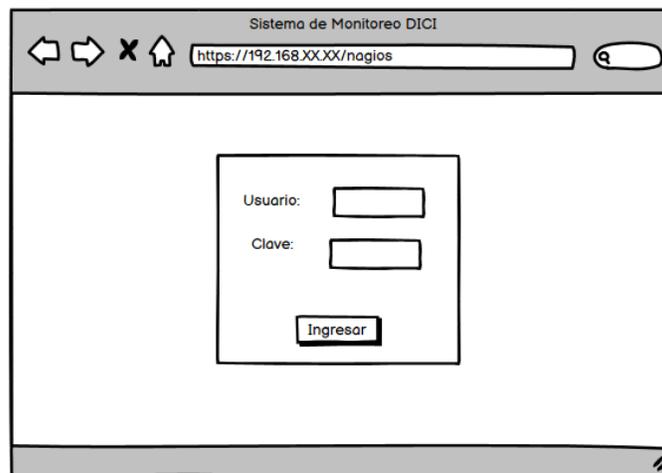


Figura 12 Pantalla inicio de sesión.

Si el inicio de sesión es exitoso se redirige a la siguiente pantalla tal como muestra la figura 15.



Figura 13 Pantalla principal

En la barra del lado izquierdo se encuentran las distintas secciones por donde se puede navegar se procederá a detallar estas secciones.

En la sección map (Figura 16), se puede ver el mapa completo de la red que se está monitoreando tal como muestra la siguiente figura.

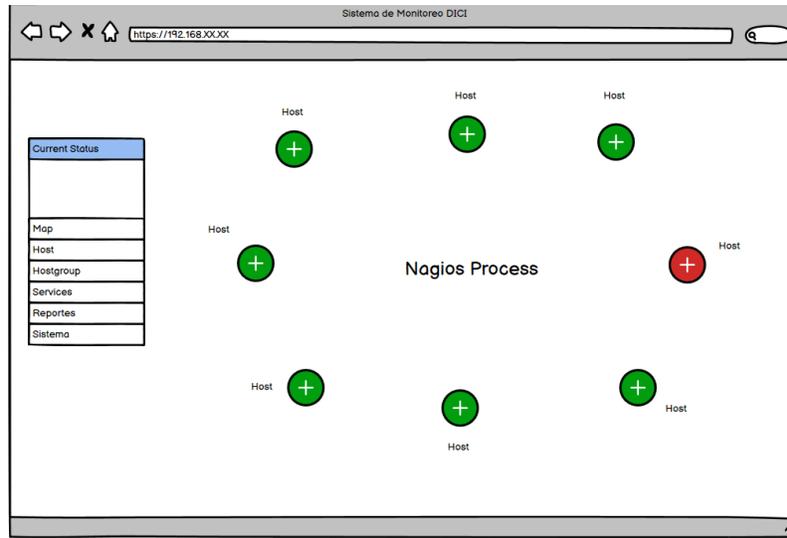


Figura 14 Mapa de la red monitoreada

Si se selecciona la sección host se mostrará en detalle los hosts que están siendo monitoreados y sus respectivas estadísticas tal como se muestra en la figura 17.

The screenshot shows a web browser window titled 'Sistema de Monitoreo DICI' with the URL 'https://192.168.XXX/nagios'. The main content area displays the title 'Hosts Monitoreados' and a table with the following data:

Host	Status	Last Check	Duration	Status
Name	Down	DD:MM:YY	HH:MM:SS	Information
Name	Up	DD:MM:YY	HH:MM:SS	Information
Name	Down	DD:MM:YY	HH:MM:SS	Information
Name	Up	DD:MM:YY	HH:MM:SS	Information
Name	Up	DD:MM:YY	HH:MM:SS	Information
Name	Up	DD:MM:YY	HH:MM:SS	Information
Name	Up	DD:MM:YY	HH:MM:SS	Information
Name	Up	DD:MM:YY	HH:MM:SS	Information

On the left side of the page, there is a navigation menu with the following items: 'Current Status', 'Map', 'Host', 'Hostgroup', 'Services', 'Reports', and 'Sistema'. The browser's address bar shows 'https://192.168.XXX/nagios'.

Figura 15 Host monitoreados.

Si se dirige a la sección hostgroup se mostrará en detalle los grupos monitoreados, estadísticas y más detalles de pueden ser de interés de algún usuario la pantalla será similar a la figura 18.

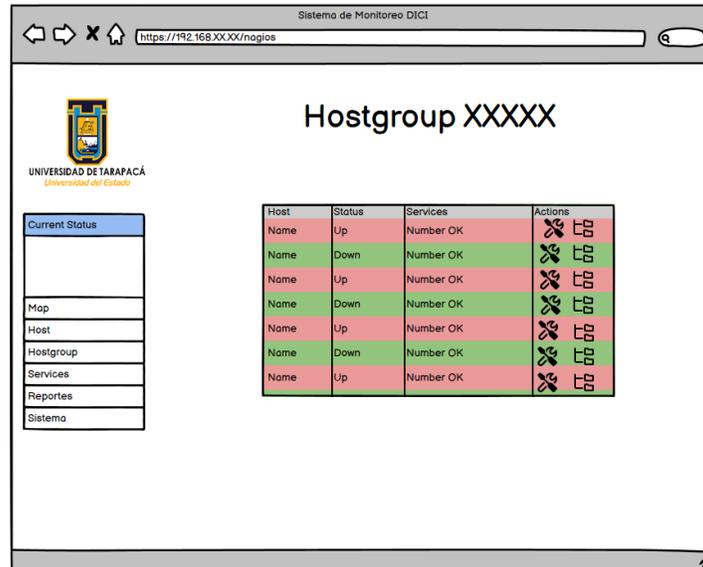


Figura 16 Sección de hostgroup del sistema.

En la sección de servicios se verá con más detalles los servicios que están siendo monitoreados, sus estadísticas y su comportamiento en tiempo real la pantalla será similar a la figura 19.

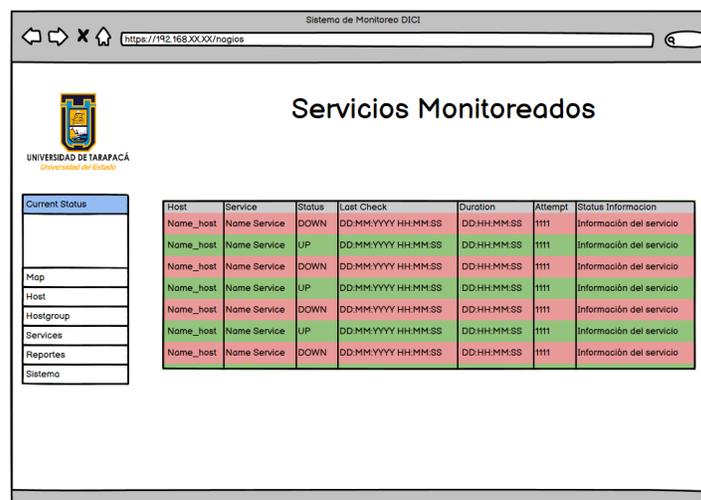


Figura 17 Sección de services del sistema.



Finalmente se tiene la sección de reportes en donde los usuarios podrán seleccionar un dispositivo o servicio y generar un reporte seleccionando un rango de fecha y mostrando uno que otro detalle de interés, la pantalla será similar a la figura 20 que se muestra a continuación.

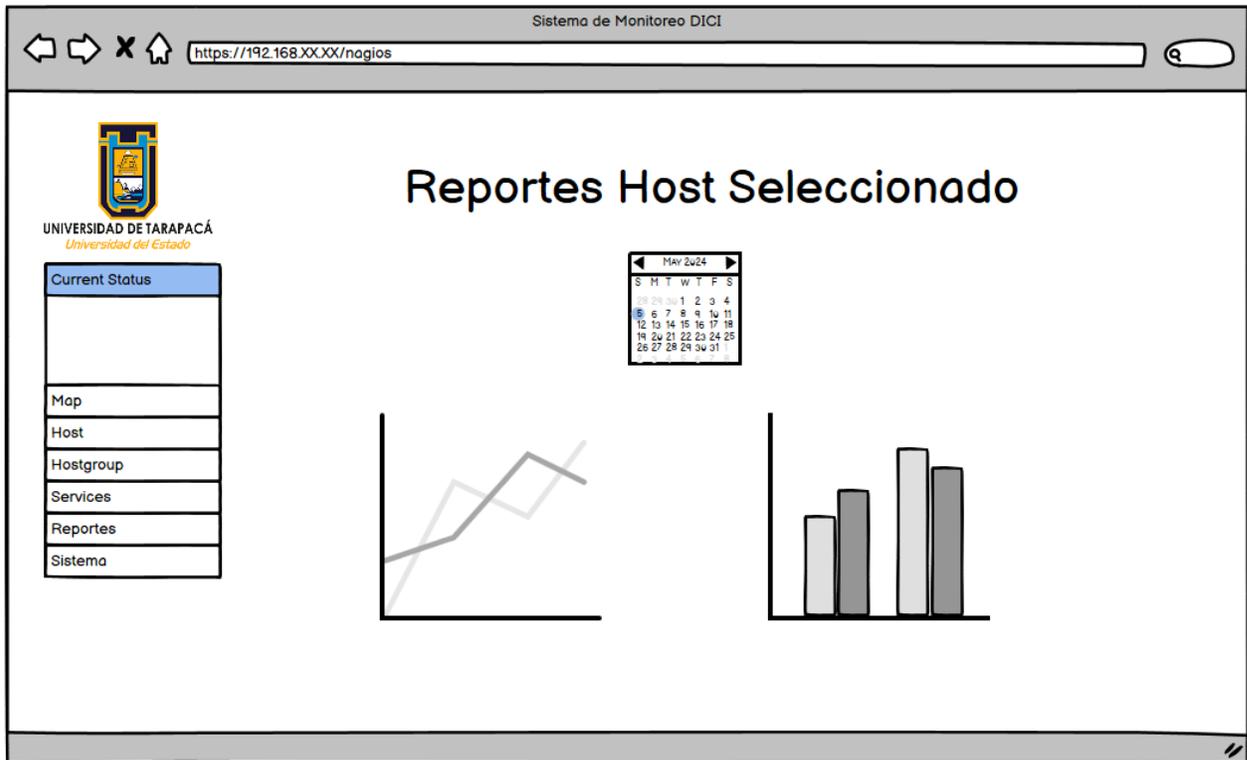


Figura 18 Sección de reportes del sistema.



VIII IMPLEMENTACIÓN

Se requiere acceder mediante un navegador web, en la barra de navegación se ingresa la dirección 146.83.109.245/nagios y se abrirá una ventana para que iniciemos sesión en el sistema tal como muestra la figura 21.

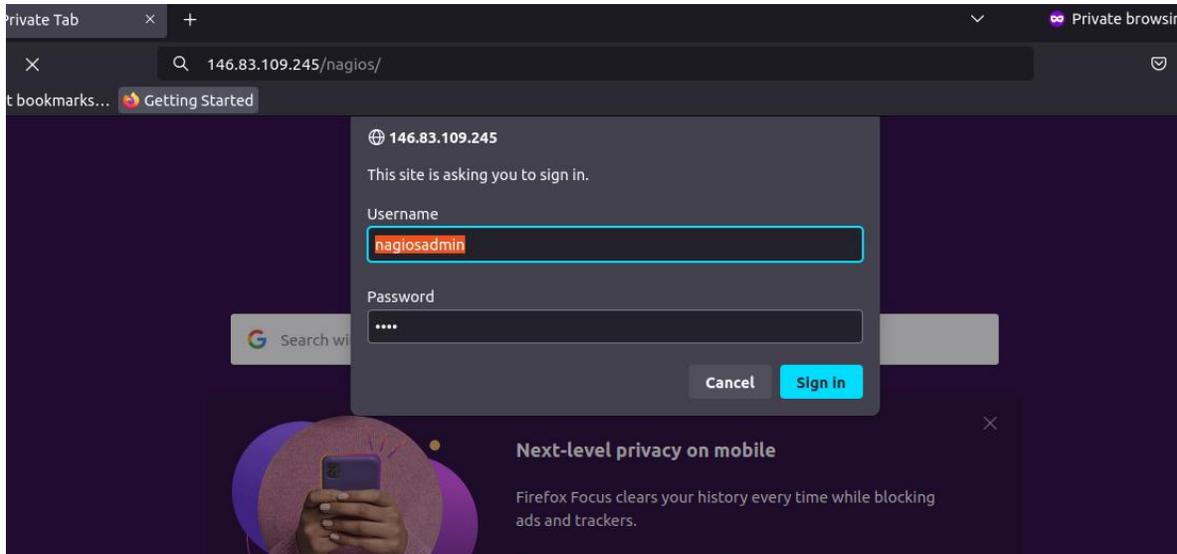


Figura 19 Inicio de sesión

Luego de iniciar sesión se redireccionará a una página similar a la figura 22.



Figura 20 Página principal de Nagios.



En la parte izquierda se nos mostrara un menú para navegar a través de la aplicación y seleccionar la sección a la que se desea ir, la navegación es como muestra la figura 23.

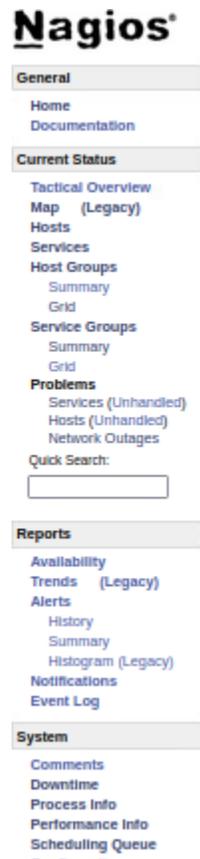


Figura 21 Navegación por el sitio de Nagios

Si seleccionamos la sección de Map, se nos mostrarán todos los dispositivos que están siendo monitoreados en el sistema tal como muestra la figura 24 (los dispositivos con borde rojo significan que están presentando algún problema en algunos de sus servicios), mientras que los verdes nos indican que están funcionando sin inconvenientes.

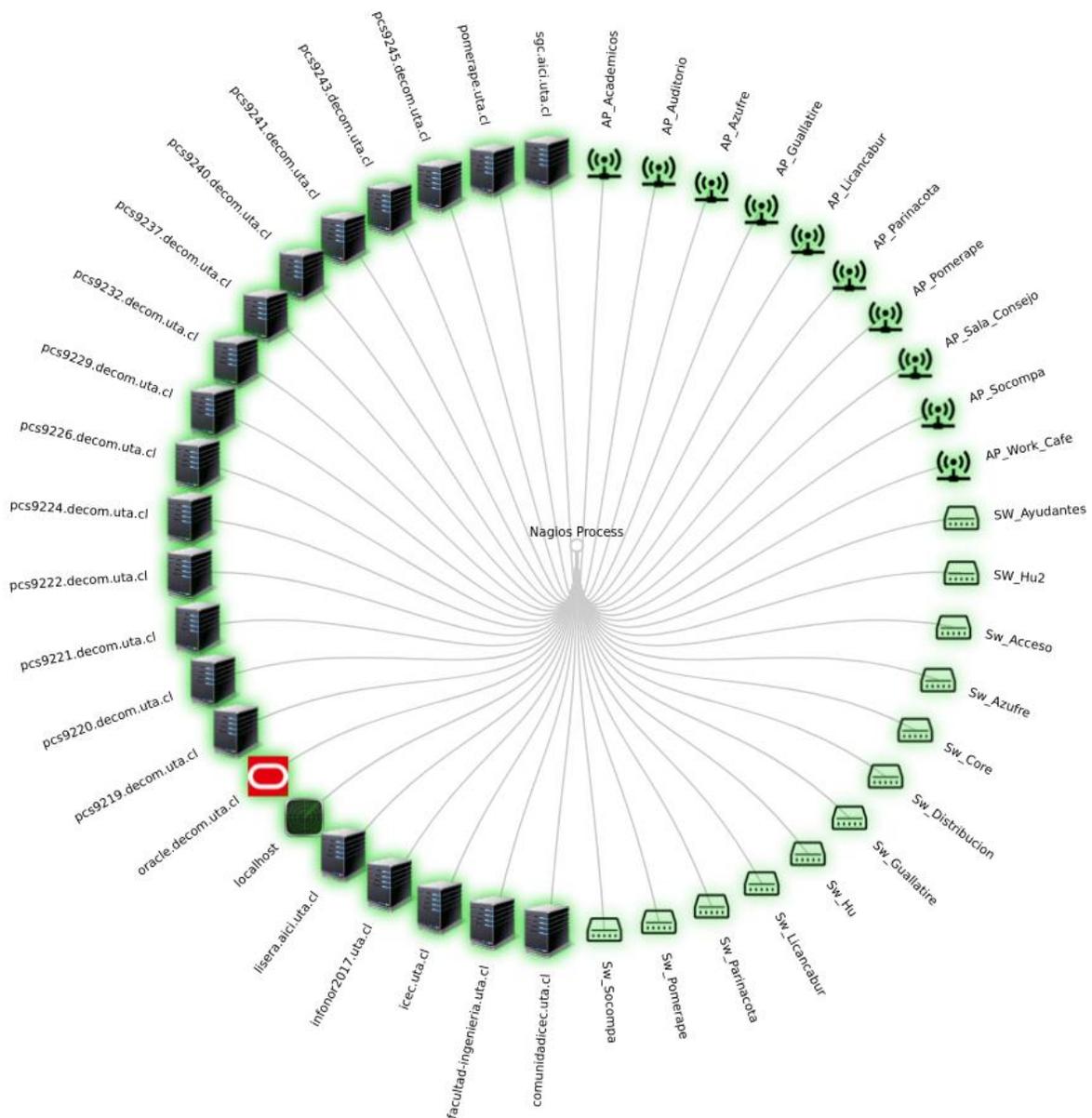


Figura 22 Mapa de la red monitoreada.



Si se hace clic en la sección de host nos mostrará un detalle de todos los dispositivos que están siendo monitoreados tal como muestra la figura 25, en el cual si el dispositivo esta apagado o sin respuesta se mostrará con color rojo en caso contrario estará en color verde.

Host Status Details For All Host Groups

Limit Results:

Host	Status	Last Check	Duration	Status Information
AP_Academicos	UP	07-03-2024 20:19:03	0d 1h 20m 1s	PING OK - Packet loss = 0%, RTA = 0.44 ms
AP_Auditorio	UP	07-03-2024 20:21:33	7d 11h 44m 32s	PING OK - Packet loss = 0%, RTA = 0.50 ms
AP_Azufre	UP	07-03-2024 20:21:40	15d 12h 46m 15s	PING OK - Packet loss = 0%, RTA = 0.48 ms
AP_Guallatire	UP	07-03-2024 20:21:49	6d 2h 14m 11s	PING OK - Packet loss = 0%, RTA = 0.52 ms
AP_Licancabur	UP	07-03-2024 20:21:54	2d 2h 40m 2s	PING OK - Packet loss = 0%, RTA = 0.56 ms
AP_Parinacota	UP	07-03-2024 20:23:32	0d 10h 30m 32s	PING OK - Packet loss = 0%, RTA = 0.50 ms
AP_Pomerape	UP	07-03-2024 20:22:09	1d 6h 36m 33s	PING OK - Packet loss = 0%, RTA = 0.55 ms
AP_Sala_Consejo	UP	07-03-2024 20:23:43	0d 3h 10m 21s	PING OK - Packet loss = 0%, RTA = 0.51 ms
AP_Socompa	UP	07-03-2024 20:22:21	2d 2h 40m 20s	PING OK - Packet loss = 0%, RTA = 0.55 ms
AP_Work_Cafe	UP	07-03-2024 20:22:28	34d 23h 48m 24s	PING OK - Packet loss = 0%, RTA = 0.48 ms
SW_Ayudantes	UP	07-03-2024 20:22:36	34d 0h 20m 1s	PING OK - Packet loss = 0%, RTA = 1.69 ms
SW_Hu2	UP	07-03-2024 20:22:42	5d 6h 16m 57s	PING OK - Packet loss = 0%, RTA = 2.14 ms
Sw_Acceso	UP	07-03-2024 20:21:33	34d 0h 11m 10s	PING OK - Packet loss = 0%, RTA = 1.13 ms
Sw_Azufre	UP	07-03-2024 20:22:56	29d 3h 44m 21s	PING OK - Packet loss = 0%, RTA = 1.66 ms
Sw_Core	UP	07-03-2024 20:21:33	9d 0h 37m 49s	PING OK - Packet loss = 0%, RTA = 1.09 ms
Sw_Distribucion	UP	07-03-2024 20:23:08	29d 3h 44m 21s	PING OK - Packet loss = 0%, RTA = 1.86 ms
Sw_Guallatire	UP	07-03-2024 20:23:17	29d 3h 44m 21s	PING OK - Packet loss = 0%, RTA = 2.68 ms
Sw_Hu	UP	07-03-2024 20:23:22	5d 6h 16m 40s	PING OK - Packet loss = 0%, RTA = 0.98 ms
Sw_Licancabur	UP	07-03-2024 20:23:29	9d 0h 36m 59s	PING OK - Packet loss = 0%, RTA = 3.38 ms
Sw_Parinacota	UP	07-03-2024 20:23:36	34d 0h 9m 46s	PING OK - Packet loss = 0%, RTA = 0.93 ms
Sw_Pomerape	UP	07-03-2024 20:23:43	34d 0h 9m 33s	PING OK - Packet loss = 0%, RTA = 1.41 ms
Sw_Socompa	UP	07-03-2024 20:23:50	29d 3h 44m 43s	PING OK - Packet loss = 0%, RTA = 0.90 ms
comunidadioec.uta.cl	UP	07-03-2024 20:18:59	24d 4h 30m 39s	PING OK - Packet loss = 0%, RTA = 0.26 ms
facultad-ingenieria.uta.cl	UP	07-03-2024 20:21:37	24d 4h 30m 25s	PING OK - Packet loss = 0%, RTA = 0.25 ms
ioec.uta.cl	UP	07-03-2024 20:19:10	6d 8h 0m 46s	PING OK - Packet loss = 0%, RTA = 0.26 ms
lsera.aiic.uta.cl	UP	07-03-2024 20:19:19	24d 4h 30m 18s	PING OK - Packet loss = 0%, RTA = 0.28 ms
localhost	UP	07-03-2024 20:19:24	43d 8h 12m 37s	PING OK - Packet loss = 0%, RTA = 0.06 ms
oracle.decom.uta.cl	UP	07-03-2024 20:19:31	29d 3h 44m 38s	PING OK - Packet loss = 0%, RTA = 0.35 ms
pcs9220.decom.uta.cl	UP	07-03-2024 20:19:37	24d 4h 30m 4s	PING OK - Packet loss = 0%, RTA = 0.20 ms
pcs9221.decom.uta.cl	UP	07-03-2024 20:19:48	24d 4h 29m 57s	PING OK - Packet loss = 0%, RTA = 0.24 ms
pcs9222.decom.uta.cl	UP	07-03-2024 20:19:51	9d 5h 9m 51s	PING OK - Packet loss = 0%, RTA = 0.22 ms
pcs9224.decom.uta.cl	UP	07-03-2024 20:19:58	16d 22h 1m 28s	PING OK - Packet loss = 0%, RTA = 0.25 ms
pcs9226.decom.uta.cl	UP	07-03-2024 20:20:05	8d 1h 5m 32s	PING OK - Packet loss = 0%, RTA = 0.29 ms
pcs9229.decom.uta.cl	UP	07-03-2024 20:20:12	8d 1h 5m 22s	PING OK - Packet loss = 0%, RTA = 0.46 ms
pcs9232.decom.uta.cl	UP	07-03-2024 20:20:18	24d 4h 29m 29s	PING OK - Packet loss = 0%, RTA = 0.49 ms
pcs9237.decom.uta.cl	UP	07-03-2024 20:20:25	8d 1h 5m 32s	PING OK - Packet loss = 0%, RTA = 0.43 ms
pcs9240.decom.uta.cl	UP	07-03-2024 20:20:32	24d 4h 29m 15s	PING OK - Packet loss = 0%, RTA = 0.52 ms
pcs9241.decom.uta.cl	UP	07-03-2024 20:20:39	8d 1h 5m 32s	PING OK - Packet loss = 0%, RTA = 0.24 ms

Figura 23 Host Monitoreados.



Si se hace clic en la sección de servicios nos mostrará un detalle de todos los servicios que están siendo monitoreados tal como muestra la figura 26, en el cual si un servicio esta critico o sin respuesta se mostrará con color rojo en caso contrario estará en color verde.

Host	Service	Status	Last Check	Duration	Attempt	Status Information
sgc.aici.uta.cl	Total Processes	OK	07-03-2024 20:17:52	24d 4h 25m 9s	1/3	PROCS OK: 150 processes with STATE = RSZDT
	Swap Usage	OK	07-03-2024 20:16:36	24d 4h 26m 28s	1/3	SWAP OK - 100% free (4095 MB out of 4095 MB)
	SSH	OK	07-03-2024 20:20:18	24d 4h 27m 46s	1/5	SSH OK - OpenSSH_7.4 (protocol 2.0)
	Root Partition	OK	07-03-2024 20:19:00	23d 5h 7m 16s	1/5	DISK OK - free space: / 8274 MB (36% inode=84%):
	Ping	OK	07-03-2024 20:21:28	3d 4h 35m 16s	1/5	PING OK - Packet loss = 0%, RTA = 0.59 ms
	Current Users	OK	07-03-2024 20:21:28	24d 4h 25m 11s	1/4	USERS OK - 1 users currently logged in
	Current Load	OK	07-03-2024 20:21:27	3d 4h 27m 1s	1/5	OK - load average: 0.02, 0.16, 0.15
pomerape.uta.cl	Total Processes	OK	07-03-2024 20:15:15	24d 4h 26m 33s	1/3	PROCS OK: 150 processes with STATE = RSZDT
	Swap Usage	OK	07-03-2024 20:13:58	24d 4h 27m 51s	1/3	SWAP OK - 100% free (4095 MB out of 4095 MB)
	SSH	OK	07-03-2024 20:21:28	24d 4h 24m 58s	1/5	SSH OK - OpenSSH_7.2p2 Ubuntu-4ubuntu2.4 (protocol 2.0)
	Root Partition	OK	07-03-2024 20:21:28	23d 5h 8m 19s	1/5	DISK OK - free space: / 8273 MB (36% inode=84%):
	Ping	OK	07-03-2024 20:21:28	3d 4h 34m 54s	1/5	PING OK - Packet loss = 0%, RTA = 0.36 ms
	Current Users	OK	07-03-2024 20:20:13	24d 4h 26m 35s	1/4	USERS OK - 1 users currently logged in
	Current Load	OK	07-03-2024 20:18:56	3d 4h 26m 50s	1/5	OK - load average: 0.13, 0.26, 0.17
pcs9247.decom.uta.cl	Total Processes	OK	07-03-2024 20:19:04	6d 7h 34m 23s	1/3	PROCS OK: 152 processes with STATE = RSZDT
	Swap Usage	OK	07-03-2024 20:17:48	6d 7h 35m 42s	1/3	SWAP OK - 100% free (4095 MB out of 4095 MB)
	SSH	OK	07-03-2024 20:22:38	0d 3h 46m 39s	1/5	SSH OK - OpenSSH_8.7 (protocol 2.0)
	Root Partition	OK	07-03-2024 20:20:12	6d 7h 38m 19s	1/5	DISK OK - free space: / 8274 MB (36% inode=84%):
	Ping	OK	07-03-2024 20:21:08	0d 3h 58m 13s	1/5	PING OK - Packet loss = 0%, RTA = 0.44 ms
	Current Users	OK	07-03-2024 20:21:28	6d 7h 34m 41s	1/4	USERS OK - 1 users currently logged in
	Current Load	OK	07-03-2024 20:17:44	3d 4h 22m 4s	1/3	OK - load average: 0.45, 0.34, 0.18
pcs9246.decom.uta.cl	Total Processes	OK	07-03-2024 20:16:27	3d 4h 34m 5s	1/3	PROCS OK: 148 processes with STATE = RSZDT
	Swap Usage	OK	07-03-2024 20:15:10	6d 7h 38m 21s	1/3	SWAP OK - 100% free (4095 MB out of 4095 MB)
	SSH	OK	07-03-2024 20:19:12	0d 3h 45m 5s	1/5	SSH OK - OpenSSH_8.7 (protocol 2.0)
	Root Partition	OK	07-03-2024 20:21:27	6d 7h 34m 41s	1/5	DISK OK - free space: / 8273 MB (36% inode=84%):
	Ping	OK	07-03-2024 20:18:37	0d 11h 5m 44s	1/5	PING OK - Packet loss = 0%, RTA = 0.40 ms
	Current Users	OK	07-03-2024 20:21:25	6d 7h 37m 4s	1/4	USERS OK - 1 users currently logged in
	Current Load	OK	07-03-2024 20:15:08	3d 4h 27m 21s	1/3	OK - load average: 0.06, 0.13, 0.10
pcs9245.decom.uta.cl	Total Processes	OK	07-03-2024 20:13:50	24d 4h 24m 0s	1/3	PROCS OK: 150 processes with STATE = RSZDT
	Swap Usage	OK	07-03-2024 20:18:59	24d 4h 25m 18s	1/3	SWAP OK - 100% free (4095 MB out of 4095 MB)
	SSH	OK	07-03-2024 20:21:27	3d 4h 35m 5s	1/5	SSH OK - OpenSSH_8.9p1 Ubuntu-3ubuntu0.10 (protocol 2.0)
	Root Partition	OK	07-03-2024 20:21:23	23d 5h 9m 36s	1/5	DISK OK - free space: / 8273 MB (36% inode=84%):
	Ping	OK	07-03-2024 20:20:06	9d 0h 36m 12s	1/5	PING OK - Packet loss = 0%, RTA = 0.05 ms
	Current Users	OK	07-03-2024 20:18:48	24d 4h 24m 58s	1/4	USERS OK - 1 users currently logged in
	Current Load	OK	07-03-2024 20:18:56	3d 4h 21m 52s	1/3	OK - load average: 0.13, 0.26, 0.17

Figura 24 Servicios monitoreados.



Si se hace clic en la sección de hostgroup nos mostrará un detalle de todos los hostgroup que han sido creados tal como muestra la figura 27, adicionalmente se presentaran botones para tomar acciones de forma inmediata.

Máquinas del Departamento de Ingeniería Civil Informática (Maquinas_DICI)				Servicios Externos (Servicios_Externos)				Oracle (Servidor Oracle)			
Host	Status	Services	Actions	Host	Status	Services	Actions	Host	Status	Services	Actions
pcs9219.decom.uta.cl	UP	6 OK	[Icons]	comunidadicec.uta.cl	UP	7 OK	[Icons]	oracle.decom.uta.cl	UP	7 OK	[Icons]
pcs9220.decom.uta.cl	UP	6 OK	[Icons]	facultad-ingenieria.uta.cl	UP	7 OK	[Icons]				
pcs9221.decom.uta.cl	UP	7 OK	[Icons]	ioec.uta.cl	UP	7 OK	[Icons]				
pcs9222.decom.uta.cl	UP	7 OK	[Icons]	infor2017.uta.cl	UP	6 OK	[Icons]				
pcs9224.decom.uta.cl	UP	6 OK	[Icons]	liser.aici.uta.cl	UP	7 OK	[Icons]				
pcs9226.decom.uta.cl	UP	7 OK	[Icons]	pomerape.uta.cl	UP	7 OK	[Icons]				
pcs9229.decom.uta.cl	UP	7 OK	[Icons]	sgc.aici.uta.cl	UP	7 OK	[Icons]				
pcs9232.decom.uta.cl	UP	6 OK	[Icons]								
pcs9237.decom.uta.cl	UP	6 OK	[Icons]								
pcs9240.decom.uta.cl	UP	6 OK	[Icons]								
pcs9241.decom.uta.cl	UP	6 OK	[Icons]								
pcs9243.decom.uta.cl	UP	6 OK	[Icons]								
pcs9245.decom.uta.cl	UP	7 OK	[Icons]								

Switches Cisco (Switch_Cisco)				Switches D-Link (Switch_DLink)				Access Points (access_point)			
Host	Status	Services	Actions	Host	Status	Services	Actions	Host	Status	Services	Actions
Sw_Acceso	UP	2 OK	[Icons]	SW_Ayudantes	UP	3 OK	[Icons]	AP_Academicos	UP	2 OK	[Icons]
Sw_Azufre	UP	2 OK	[Icons]	SW_Hu2	UP	2 OK	[Icons]	AP_Auditorio	UP	2 OK	[Icons]
Sw_Core	UP	1 OK	[Icons]					AP_Azufre	UP	2 OK	[Icons]
Sw_Distribucion	UP	1 OK	[Icons]					AP_Guallatire	UP	2 OK	[Icons]
Sw_Guallatire	UP	1 OK	[Icons]					AP_Licancabur	UP	2 OK	[Icons]
Sw_Hu	UP	2 OK	[Icons]					AP_Parinacota	UP	2 OK	[Icons]
Sw_Licancabur	UP	2 OK	[Icons]					AP_Pomerape	UP	2 OK	[Icons]
Sw_Parinacota	UP	2 OK	[Icons]					AP_Sala_Consejo	UP	2 OK	[Icons]
Sw_Pomerape	UP	1 OK	[Icons]					AP_Socompa	UP	2 OK	[Icons]
Sw_Socompa	UP	1 OK	[Icons]					AP_Work_Cafe	UP	2 OK	[Icons]

Linux Servers (linux-servers)			
Host	Status	Services	Actions
localhost	UP	6 OK	[Icons]

Figura 25 Sección de hostgroup creados.



Si se desea, se pueden ver los gráficos de monitoreo en tiempo real, los cuales fueron programados usando PNP4 junto a Nagios. Para acceder a estos gráficos, se debe hacer clic en el ícono del gráfico en la sección "Perform Extra Services Performance". Esto permitirá obtener acceso a los gráficos de monitoreo en tiempo real, donde se podrán observar tanto los gráficos del dispositivo como los gráficos de cada servicio monitoreado para ese dispositivo.

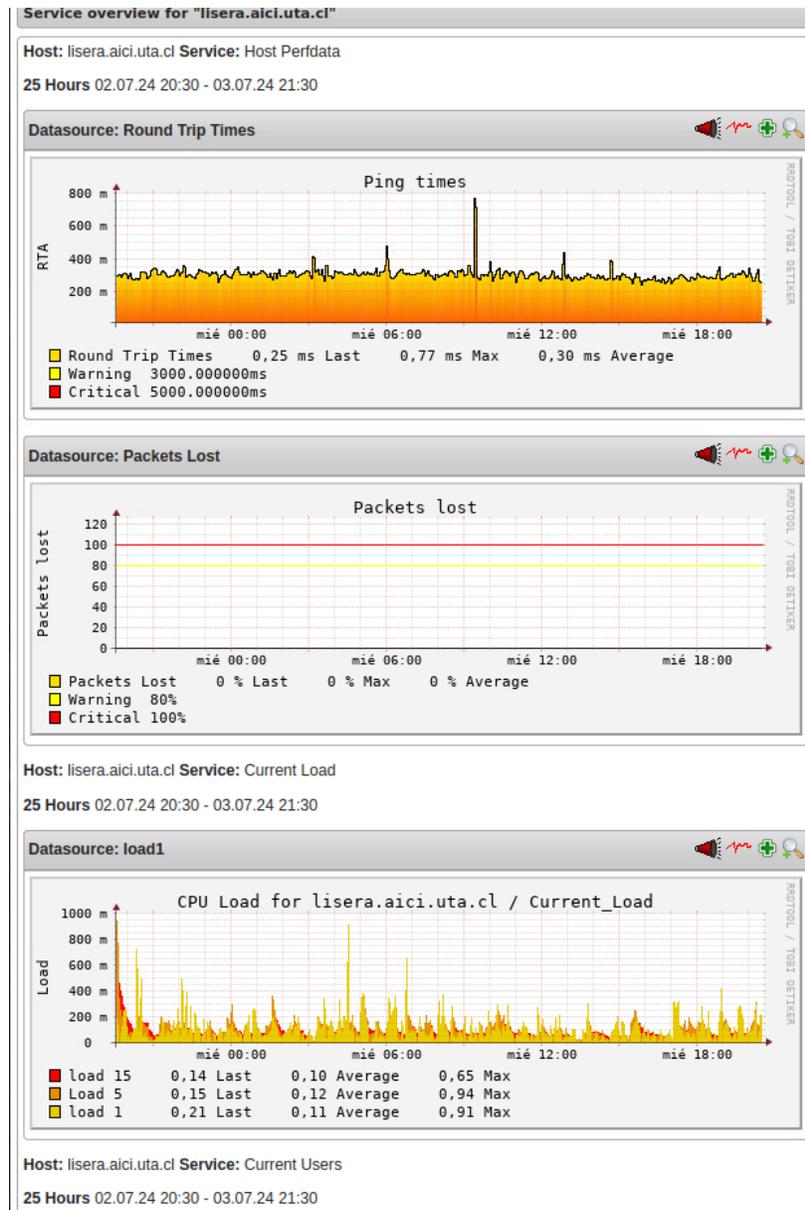


Figura 26 Gráficos parte 1 host seleccionado.

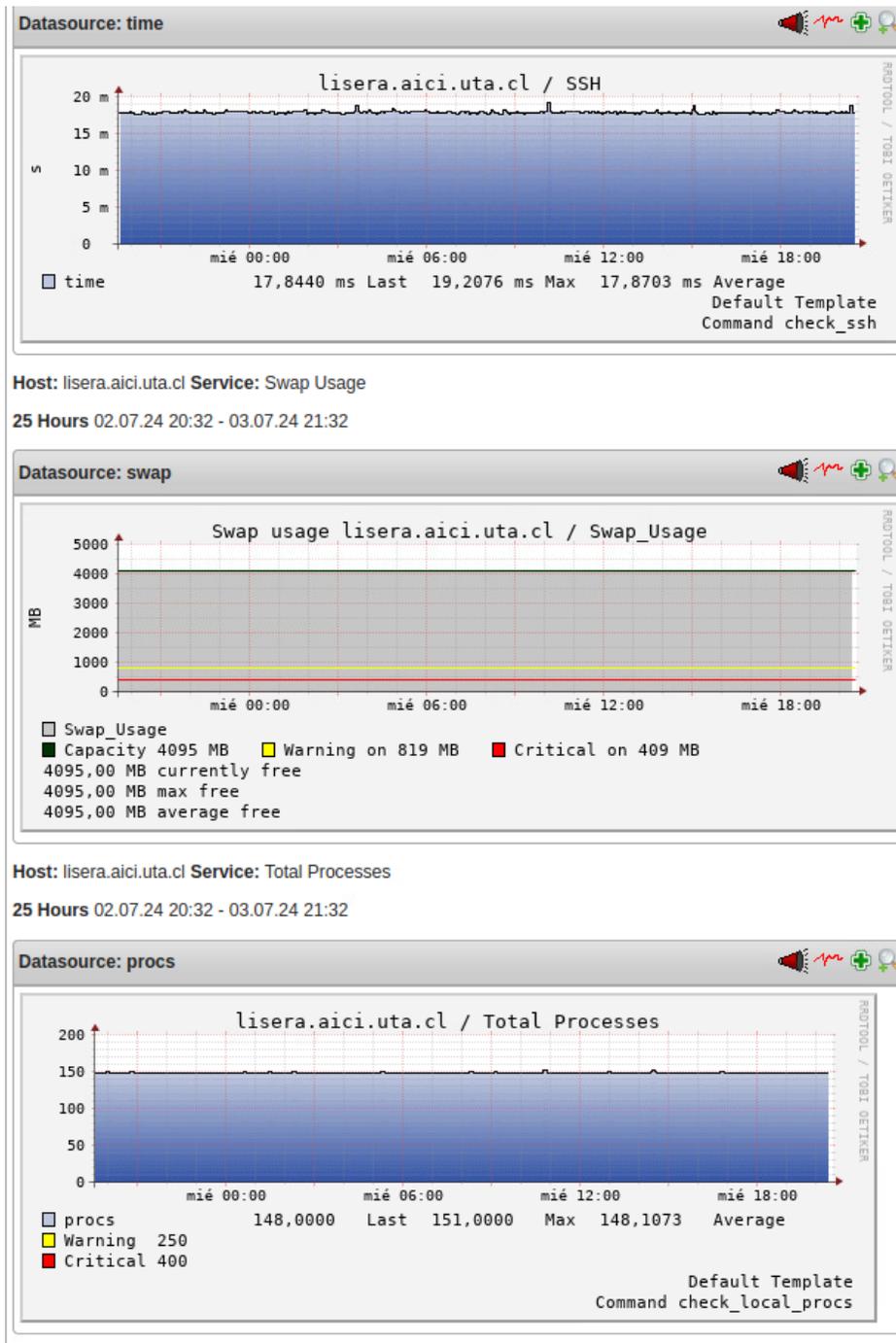


Figura 27 Gráficos parte 2 host seleccionado.

De los gráficos mostrados anteriormente, se pueden realizar interpretaciones de acuerdo con el rango de fechas seleccionado.



Adicionalmente si lo desea puede generar reportes de los mismos gráficos detallados anteriormente y guárdalos en formato PDF, solo debe hacer clic en el icono de Adobe Reader que se muestra a continuación.



Figura 28 Icono de PDF.

Y tendrá generado su reporte seleccionado según su requerimiento.

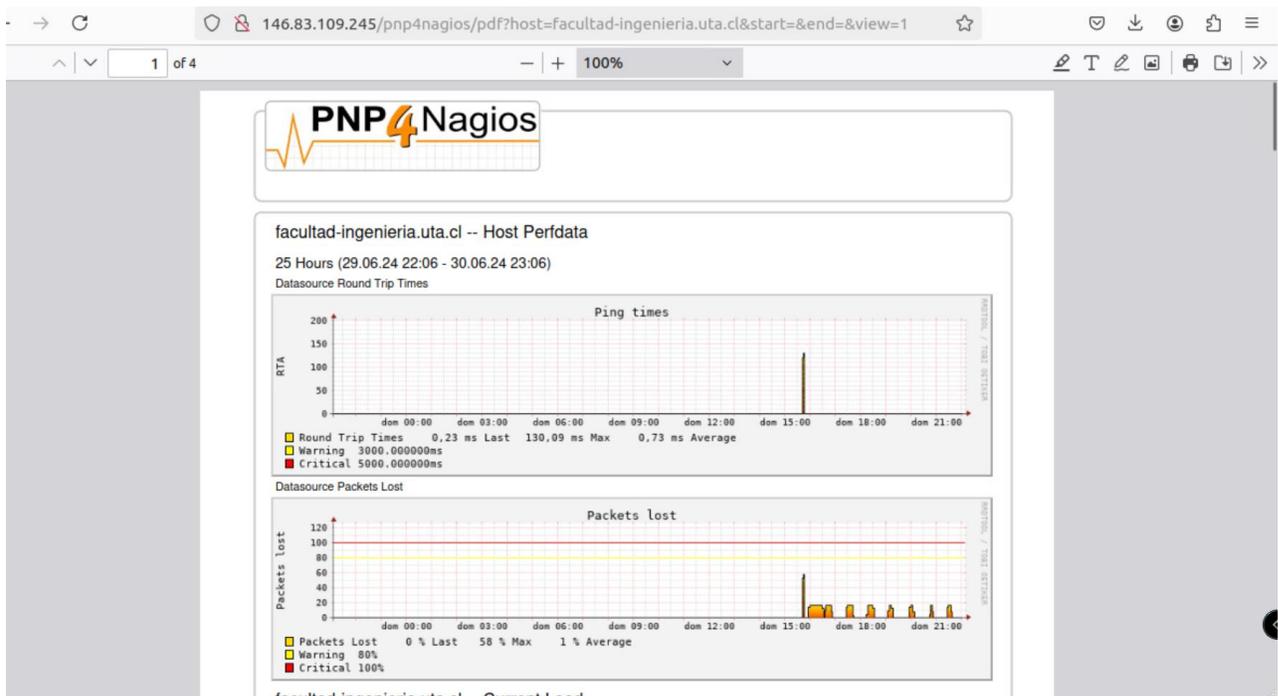


Figura 29 PDF generado por el usuario



VII Conclusiones

El proyecto ha progresado de manera significativa hasta este punto, logrando hitos importantes como la creación de hosts, servicios y hostgroups. Estas acciones representan una sólida base para el sistema de monitoreo. Además, se ha implementado el monitoreo gráfico utilizando Nagios y PNP4, lo que permite la visualización de datos en tiempo real. También se han configurado alertas para una respuesta proactiva a eventos críticos y se ha habilitado la generación de reportes en PDF, lo que facilita la documentación y análisis de la información monitoreada.

Se han creado usuarios para gestionar adecuadamente el acceso y los permisos dentro del sistema, asegurando una administración segura y eficiente. Esto garantiza que cada miembro del equipo tenga el nivel de acceso apropiado, lo cual es crucial para mantener la integridad y seguridad del sistema de monitoreo.

A pesar de estos logros, aún quedan aspectos cruciales por abordar, como la optimización continua de las gráficas y alertas para mejorar la respuesta ante eventos críticos. Sin embargo, es reconfortante contar con el respaldo y la colaboración continua del cliente, lo que indica una relación sólida y un compromiso mutuo con el éxito del proyecto.

Con el apoyo del cliente, el proyecto ha concluido con éxito y se utilizará desde un futuro cercano, asegurando un monitoreo efectivo y una gestión eficiente de los recursos de red. Esto permitirá al cliente tomar decisiones informadas y proactivas, mejorando significativamente la operatividad y el rendimiento de su infraestructura de red que forman el Departamento de Ingeniería en Computación e Informática.



REFERENCIAS

- [1] DGDT – Universidad de Tarapacá. (n.d.). <https://www.uta.cl/index.php/dgdt/>
- [2] DICI – Departamento Ingeniería en Computación e Informática. (n.d.). <https://dici.uta.cl/>
- [3] Get Ubuntu Server | Download | Ubuntu. (n.d.). Ubuntu. <https://ubuntu.com/download/server>
- [4] Nagios. (2024, May 22). Nagios XI | Nagios. https://www.nagios.com/products/nagios-xi/?utm_feeditemid=,utm_device=c,utm_term=,utm_source=google,utm_medium=p pc,utm_campaign={utmcampaign},hsa_cam=21345028299,hsa_grp=,hsa_mt=,hsa_src=x,hsa_ad=,hsa
- [5] GitHub: Let's build from here. (2024). GitHub. <https://github.com/>
- [6] Pnp4nagios. (n.d.). GitHub - pnp4nagios/pnp4nagios: PNP is an addon to NagiosCore which analyzes performance data provided by plugins and stores them automatically into RRD-databases. PNP= Pnp is Not Perfparse. Perfparse is first parsing tool in Nagios 0.x. GitHub. <https://github.com/pnp4nagios/pnp4nagios>



ANEXOS

IMPACT MAPPING DEL PROYECTO

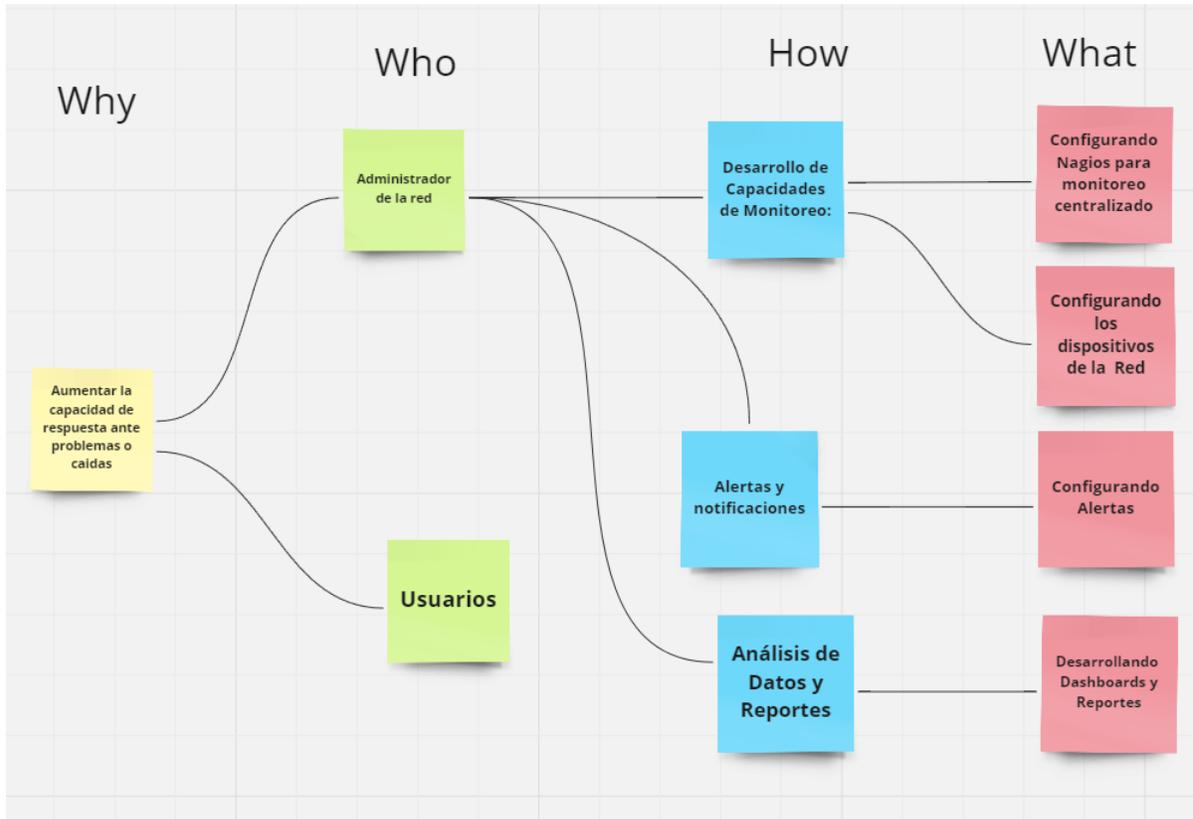


Figura 30 Impact Mapping del proyecto.

User Story Mapping

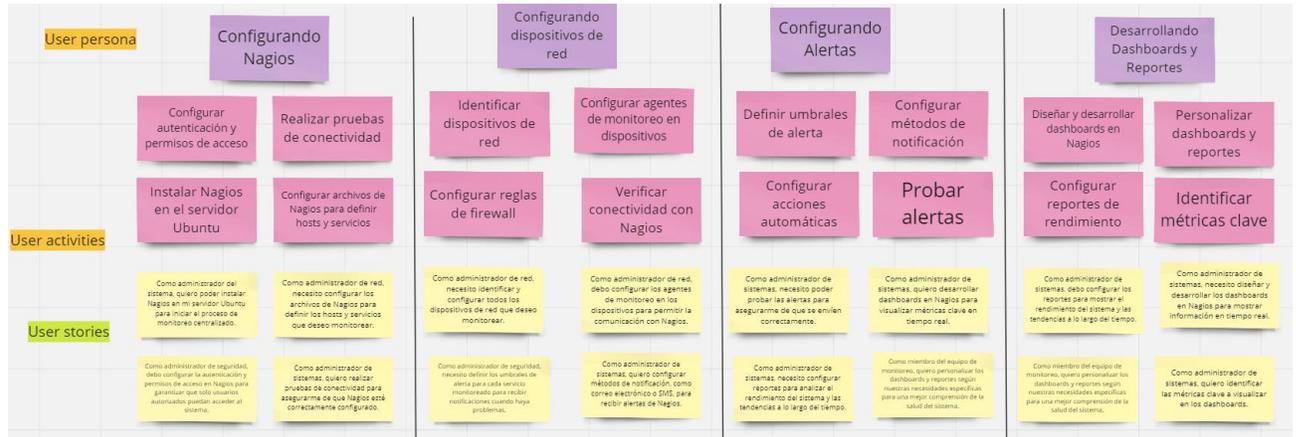


Figura 31 User story Mapping del proyecto