UNIVERSIDAD DE TARAPACÁ

FACULTAD DE INGENIERÍA

Departamento de Ingeniería en Computación e Informática

Proyecto IV

"Sistema de gestión de seguridad en un ambiente de servidores"

coloca un nickmane al proyecto

Integrantes: Scarlet Gavia Mondaca
Empresa o Unidad: DICI
Profesor: Diego Aracena Pizarro
Asignatura: Proyecto IV

Arica, Chile
2025

Índice

Índice de figuras

Índice de tablas

1. Introducción

La ciberseguridad es una rama muy importante en la actualidad, a través de ella podemos proteger nuestros datos e información importante, ya que garantiza la protección, respaldo y resguardo de los datos, por ello, es esencial que los estudiantes adquieran habilidades para defender sus dispositivos y detectar posibles ataques de agentes externos.

Este proyecto tiene como objetivo diseñar e implementar un sistema de gestión de ciberseguridad informática, para llevar a cabo este proyecto se comenzará por realizar las instalaciones de distintos sistemas operativos de distribución “Linux” en cada uno de los servidores, los cuales tendrán distintas herramientas para que los alumnos puedan aplicar ataques y defensas controladas, se liberaran los puertos señalados por el cliente, se llevará un catastro de ruta de cada proceso que se realiza semanalmente, esto se llevará a cabo con un dashboard para llevar un monitoreo de los 4 servidores en simultáneo, este dashboard permitirá reiniciar los servidores y ejecutar cualquier aplicación que el cliente quiera instalar.

Asimismo, luego de estas configuraciones, el sistema deberá ser capaz de monitorear, registrar y analizar cada una de las actividades realizadas, ya sea en el servidor físico como ataques externos, con estos datos registrados en el sistema, este debe ser capaz de realizar un análisis, identificando y registrando cada intento de intrusión, lo que permitirá al cliente ver los ataque y poder realizar un análisis de estas capturas.

2. Descripción de la empresa

El Departamento de Ingeniería en Computación e Informática ha trabajado conscientemente en el proceso de transformación de estudiantes en Ingenieros y como tales deben ser capaces de analizar y sistematizar la información, con el fin de alcanzar los objetivos organizacionales de la empresa, tanto nacional como internacional, mediante el uso de sistemas computacionales distribuidos. Darles una formación, para que sean capaces de diseñar, desarrollar e implantar sistemas para administrar información útil en la toma de decisiones usando equipo computacional, a la vez que utilice metodologías y facilidades para el desarrollo general de sistemas complejos de software base y de sistemas en particular, generando tecnología nacional.

EL DICI tiene como misión crear, difundir y hacer uso de las tecnologías de información y comunicación en beneficio de la sociedad y la formación de ingenieros con sólidas habilidades técnicas y sociales. Esta misión involucra un compromiso y una responsabilidad con la región, el país, la Universidad de Tarapacá y el DICI, ya que estos principios y valores, son los mismos que establece nuestra casa de estudios superiores.

Cuando se habla de crear, difundir y hacer uso de las tecnologías de información y comunicación en beneficio de la sociedad se quiere expresar como una unidad académica que centra su quehacer no sólo en la formación de los profesionales en el área que le compete, sino, además, en la investigación, la extensión, la formación de recursos humanos (postgrado, postítulo) y en la prestación de servicios que la región requiere.

Figura 1: Logo de la empresa.

3. Definición del proyecto

3.1. Contexto

La computación y la tecnología son parte de nuestras vidas, estudiar computación te permite formar parte del grupo de personas que desarrollan los sistemas que están dando forma a los estilos de vida del futuro, la práctica de la ciberseguridad es esencial para esta rama de estudios, ya que permite que los alumnos desarrollen habilidades en defensa de sistemas y detección de ataques, sin embargo, es necesario que estas prácticas se realicen en un entorno controlado, donde los riesgos sean mínimos y la actividad de los alumnos pueda ser supervisada adecuadamente.

3.2. Problema

Los estudiantes aplicaran ataques y defensas en sistemas reales para desarrollar habilidades efectivas, sin embargo, estas prácticas presentan riesgos si se realizan en entornos no controlados, ya que los servidores podrían dañarse o los datos podrían comprometerse, el laboratorio carece de herramientas que les permitan supervisar y registrar las actividades de estos servidores, lo que dificulta al cliente ver las actividades realizadas.

3.3. Solución

Para dar solución a esta problemática, se propone la implementación de un sistema de monitoreo para un laboratorio de ciberseguridad controlado, este sistema permitirá al cliente monitorear, registrar y analizar las actividades realizadas en los servidores, alertando sobre ataques y permitiendo realizar defensa.

4. Objetivos

4.1. Objetivo General

Realizar un sistema de monitoreo que permita ver y alertar al administrador sobre las actividades sospechosas realizadas en los servidores.

4.2. Objetivos Específicos

- Ver el estado de los servidores.
- Estudiar distintos dashboard para el sistema.
- Llevar un registro de las actividades realizadas en los servidores.
- Instalar un dashboard para análisis de las actividades en los servidores.
- Realizar pruebas del sistema.
- Realizar alertas en caso de actividad sospechosa.

rehacer hay problemas de entendimiento que es un dashboard??

5. Planificación del proyecto

5.1. Metodología ágil de prototipo descartable

Se utilizará una la metodología ágil “prototipo descartable”, ya que esta permite explorara, aclarar y validar requerimientos antes de construir la solución final, esta consiste en crear una versión preliminar, simplificada y parcialmente funcional del producto, el objetivo principal es facilitar la comunicación con el cliente, detectar errores, comprender necesidades reales y reducir la incertidumbre durante las etapas iniciales del proyecto.
Este prototipo no está destinado a evolucionar ni a formar parte del producto final, sino que se elimina una vez que se haya cumplido su función de análisis, validación y retroalimentación.

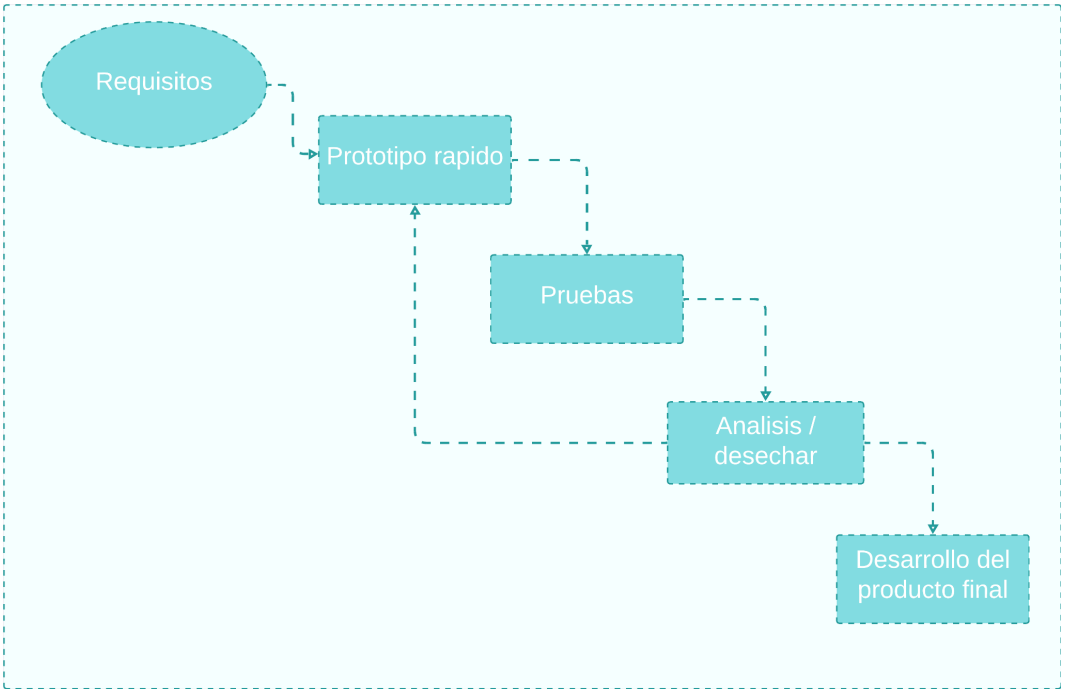

Figura 2: Metodología.

6. Carta Gantt

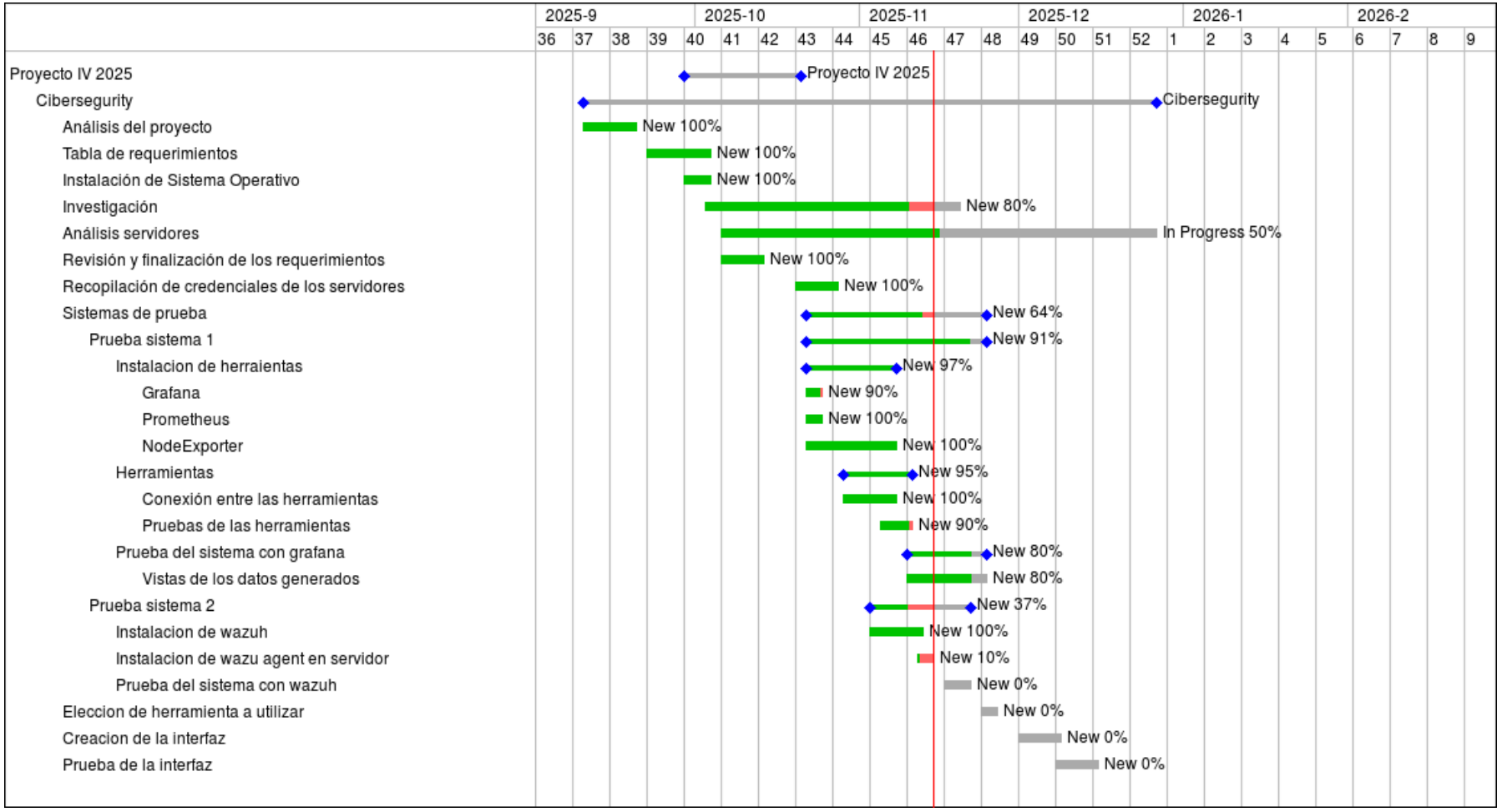

Figura 3: Carta Gantt.

7. Requisitos del sistema

7.1. Requisitos de Alto Nivel

ID	*Definición del requisito*
RAN1	Facilitar la supervisión y el análisis de las actividades realizadas.
RAN2	Garantizar servidores protegidos.
RAN3	El sistema debe contar con la tríada de ciberseguridad, pentesting, peritaje informáticos y seguridad informática en criptografía.

Tabla 1: Requisitos de alto nivel

7.2. Requisitos funcionales

ID	*Definición del requisito*	*Importancia*
RF1	El sistema debe tener 2 perfiles de acceso.	**muy alto**
RF2	El sistema debe permitir que el perfil de administrador modifique información de los servidores.	**muy alto**
RF3	El sistema debe permitir que el perfil de usuario solo pueda acceder a los datos registrados, sin opción de modificar.	**muy alto**
RF4	El sistema debe registrar todas las acciones y ataques realizados.	**alto**
RF5	El sistema debe mostrar los ataques y las vulnerabilidades detectadas.	**alto**
RF6	El sistema debe permitir la gestión de múltiples servidores.	**alto**
RF7	El sistema debe permitir un monitoreo y seguimiento de los ataques ejecutados.	**alto**
RF8	El sistema debe mostrar en pantalla el tiempo real de los eventos.	**medio**
RF9	El sistema debe mostrar los procesos de los servidores.	**medio**
RF10	El sistema debe registrar cualquier actividad realizada en los servidores (reinicio, apagado,etc).	**medio**

Tabla 2: Requisitos funcionales

7.3. Requisitos no funcionales

ID	*Definición del requisito*
RNF1	El sistema debe asegurar que los ataques realizados no afecten a otros sistemas de la empresa.
RNF2	Los servidores y el sistema deben estar siempre disponibles.
RNF3	El sistema debe ser capaz de manejar múltiples conexiones y acciones simultáneas.
RNF4	El sistema debe tener una interfaz intuitiva y permitir acceder fácilmente a la información de cada servidor.
RNF5	El sistema debe permitir agregar más servidores sin necesidad de reestructuración mayor.
RNF6	El sistema debe ser compatible con dashboard para la captura de datos.

Tabla 3: Requisitos no funcionales.

8. Análisis del sistema

8.1. Modelo de contexto

En el siguiente diagrama se explica el funcionamiento del sistema, en el cual se puede ver que los hackers o intrusos atacan los servidores, luego el sistema reconoce los ataques, analiza el servidor y finalmente el sistema alerta al administrador los ataques realizados, mientras que el usuario básico sólo puede observar las estadísticas de lo sucedido.

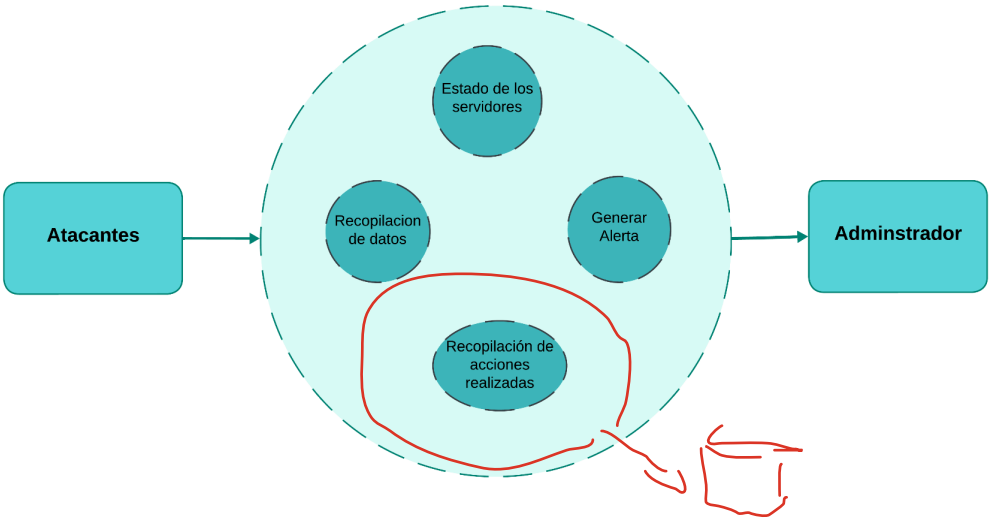

Figura 4: Modelo de contexto.

casos de usos general y su desarrollo
o desde el modelo de contexto desarrollar cada módulo, diagemas de clases
...falta

8.2. Modelo BPMN

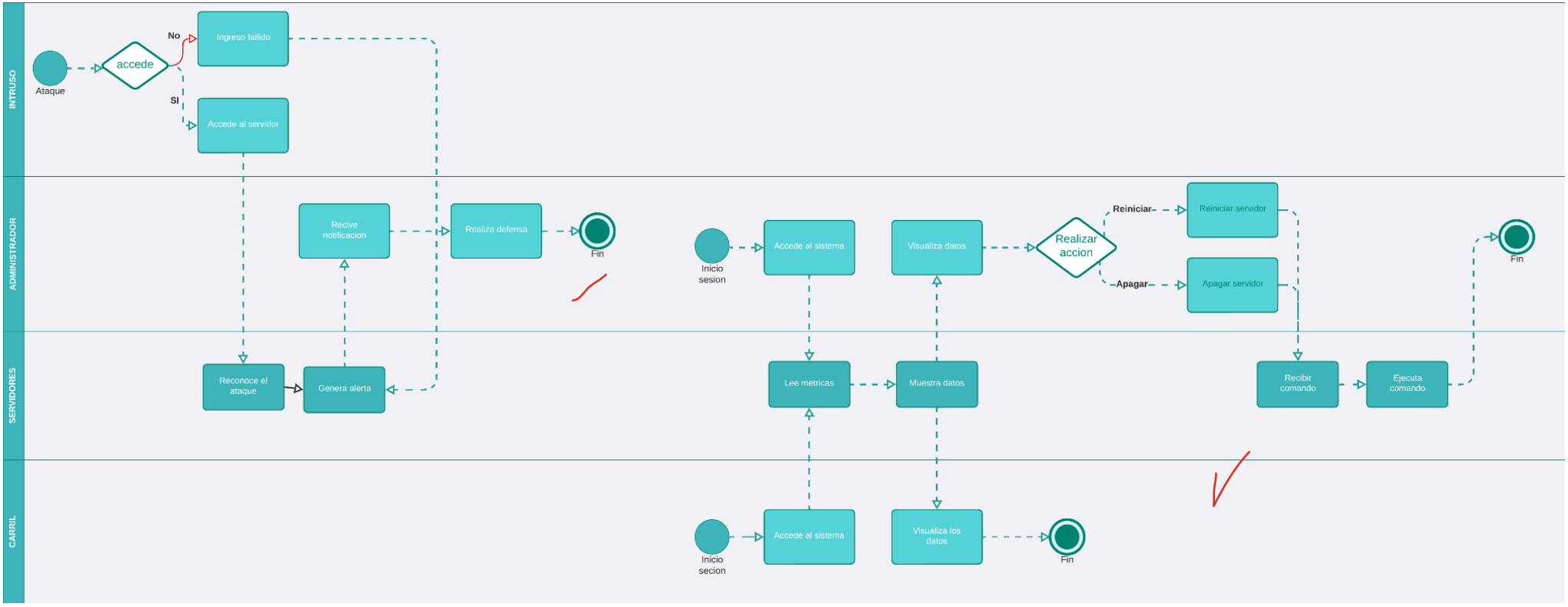

Figura 5: Modelo BPMN

9. Herramientas a utilizar

Se utilizaron distintas herramientas para el análisis de datos y alerta de ataques, para la primera prueba se utilizó:

	Nombre	**Descripción**
1	Grafana	Plataforma de código abierto que permite crear paneles de control interactivos y dinámicos que muestran métricas de rendimiento en tiempo real a través de gráficos.
2	Prometheus	Sistema de código abierto que permite recopilar y almacenar métricas de los sistemas objetivos, proporciona el lenguaje de consulta PromQL para el análisis de datos.
3	Alertmanager	Herramienta de código abierto que gestiona las alertas generadas por sistemas como Prometheus.
4	Node Exporter	Es un componente de la plataforma prometheus, recopilar métricas del sistema operativo y hardware de un servidor.

Tabla 4: Herramientas a utilizar 1ra prueba.

Para la segunda prueba se utiliza la siguiente herramienta:

	Nombre	**Descripción**
1	Wazuh	Plataforma para detectar amenazas en servidores, auditar cumplimiento, centralizar alertas y servir como capa de visibilidad en infraestructuras físicas, virtuales, en la nube y en contenedores.
2	Elasticsearch	Motor distribuido de búsqueda de logs, métricas, eventos, almacenamiento y cualquier dato indexable.
3	Kibana	Interfaz web de visualización y administración para Elasticsearch, crear dashboards, explorar datos con Discover, gestionar índices, visualizar mapas, crear visualizaciones y usar plugins
4	Filebeat	Recopila archivos de log, lee nuevos eventos en tiempo real, aplica procesadores básicos, y envía a destino configurado.

Tabla 5: Herramientas a utilizar 2da prueba.

Para la vista del cliente se utilizarán:

	Nombre	Descripción
1	Angular	Framework de desarrollo front-end basado en TypeScript, diseñado para crear aplicaciones web dinámicas, modulares y de alto rendimiento.
2	Node.js	Entorno de ejecución de JavaScript del lado del servidor, basado en el motor V8 de google, permite ejecutar código JavaScript fuera del navegador.
3	Bootstrap	Framework de diseño css orientado a la creación de interfaces web .
4	Visual Studio Code	Editor de código ligero, multiplataforma y altamente extensible, ofrece funcionalidades avanzadas como autocompletado inteligente, depuración integrada.

Tabla 6: Herramientas a utilizar framework.

10. Prototipo

Para la pantalla principal se presentará un formulario de inicio de sesión, en el cual según el nombre el sistema abrirá el usuario correspondiente, ya sea de administrador o de usuario.

Figura 6: Pantalla inicial.

Luego en la segunda pantalla se mostrará una pestaña con opciones como inicio, la cual nos llevará a una página de inicio y a la página de los paneles de control, en el final de esta pestaña se puede ver la opción de configuraciones.

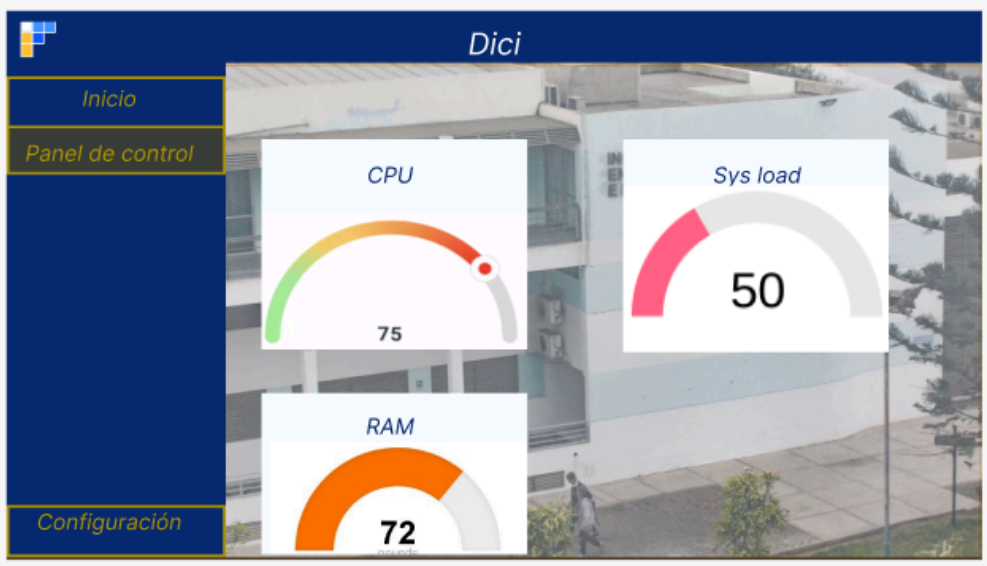

Figura 7: Panel de control.

11. Arquitectura del sistema

Para la arquitectura de este sistema, como podemos ver en la figura 8, el administrador tendrá acceso al sistema a través de una pagina creada por angular, node.js y bootstrap, esta interfaz está conectada a la API de wazuh, la cual cuenta con wazuh manager, wazuh ruleset, el motor de análisis y elasticsearch para el cuadrado de los datos capturados, esto tendrá coneccion a wazuh agent, el cual estará instalado en los servidores que se desean monitorear para obtener los datos y analizarlos.

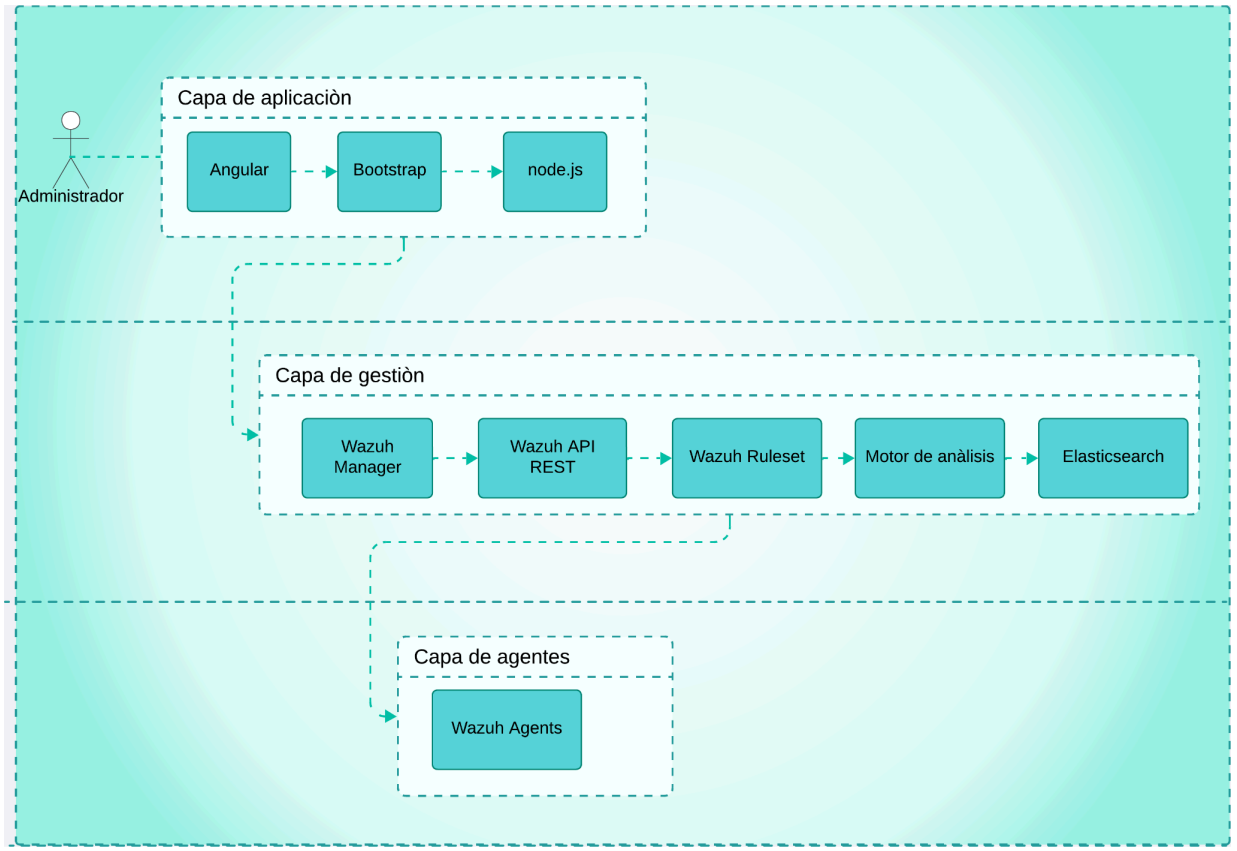

Figura 8: Arquitectura del sistema.

y el almacen de los datos históricos generados

12. Conclusión

En el presente informe se abordaron los procesos de organización y diseño del “Sistema de gestión de seguridad en un ambiente de servidores”, este sistema busca ofrecer al cliente la posibilidad de monitorear varios servidores en tiempo real, optimizando así la gestión y seguridad de la infraestructura, este sistema cuenta con un dashboard y alertas en caso de ingreso de intrusos para llevar a cabo este proyecto se analizaron diversas herramientas, se elaboró un prototipo y se desarrollaron varios diagramas que facilitaron la comprensión y planificación del sistema, en conjunto, estos elementos permitieron definir una base sólida para las futuras implementaciones y mejoras del sistema.

Ok..

Obs: Muchos faltantes, existe un mal uso de palabras técnicas.. dashboard (visualización de salida) se confunde con herramientas en algunos casos
debe reparar y colocar una buena declaración de objetivos específicos, los cuales no estan bien..

13. Referencias

1) https://documentation.wazuh.com/current/quickstart.html
2) Grafana Labs. (s. f.). *Grafana: The open and composable observability platform | Grafana Labs*. https://grafana.com/
3) *Getting started | Prometheus*. (s. f.). https://prometheus.io/docs/prometheus/latest/getting_started/
4) Wazuh. (s. f.). *Quickstart · Wazuh documentation*. https://documentation.wazuh.com/current/quickstart.html