UNIVERSIDAD DE TARAPACÁ

Facultad de ingeniería

INGENIERÍA CIVIL EN COMPUTACIÓN E INFORMÁTICA

MANUAL DE USUARIO

“Sistema de gestión de seguridad en un ambiente de servidores”

Security Control Center

Desarrollado por:
Scarlet Gavia Mondaca

Asignatura: Proyecto IV

Docente:
Diego Aracena Pizarro

Arica, Diciembre 2025

Introducción

El presente manual de usuario tiene como finalidad orientar al usuario en el uso del Sistema de Monitoreo de Seguridad basado en Wazuh, este sistema permite la visualización y gestión de información relacionada con eventos de seguridad, a través de una interfaz web intuitiva y accesible.

El sistema está compuesto por un frontend desarrollado en Angular, un backend implementado en Node.js, y una instancia de Wazuh instalada en un servidor, encargada del análisis y monitoreo de eventos; el backend actúa como intermediario entre la interfaz de usuario y la API de Wazuh, permitiendo una comunicación segura y estructurada.

Este manual describe las principales funcionalidades del sistema, así como los pasos necesarios para su correcto uso, desde el acceso a la plataforma hasta la interacción con las distintas secciones disponibles, está dirigido a usuarios finales con conocimientos básicos de informática, y no requiere experiencia previa en administración de sistemas o seguridad informática.

El contenido presentado en este documento tiene como objetivo facilitar el uso adecuado del sistema, promover una correcta interpretación de la información mostrada y servir como material de apoyo para la utilización eficiente de la plataforma de monitoreo.

Índice

Índice de tabla

Descripción general del sistema

El sistema está compuesto por tres elementos principales:

Frontend (Angular): Interfaz gráfica utilizada por el usuario.
Backend (Node.js): API intermedia que se comunica con Wazuh.
Wazuh: Plataforma de monitoreo y seguridad instalada en un servidor.

Arquitectura general

Flujo de funcionamiento:

Usuario ⟶ Interfaz Web (Angular)
⟶ Backend (Node.js)
⟶ API de Wazuh
⟶ Respuesta al usuario

Requisitos para el usuario

Requisitos de hardware:

Computador con acceso a red.
Conexión a Internet.

Requisitos de software:

Navegador web actualizado (Chrome, Firefox, Edge).
Acceso a la URL del sistema.

1.Acceso al sistema

1.1.Ingreso al sistema

Abrir el navegador web e ingresar a la URL del sistema.

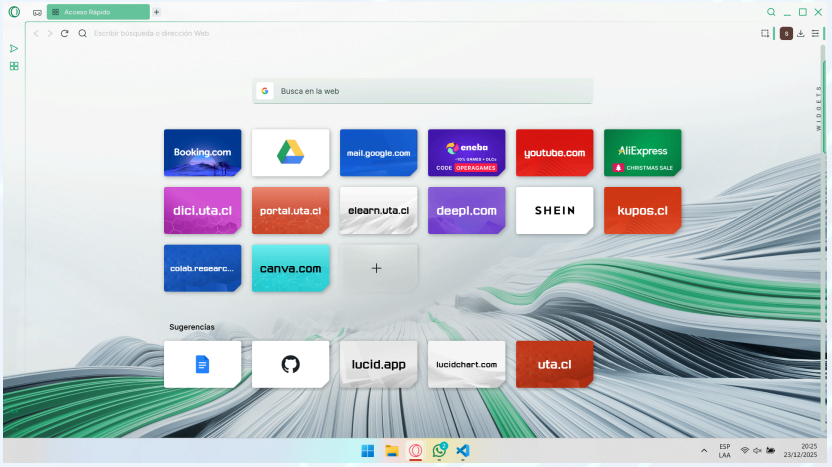

Figura 1: Navegador web

Ingresar la URL del sistema:

Para esta ocasión se ingresará con la URL “http://localhost:4200”.

El sistema mostrará la pantalla de inicio de sesión, el sistema cuenta con 2 roles para el ingreso el rol de usuario y el rol de administrador, este rol lo identificara el sistema internamente.

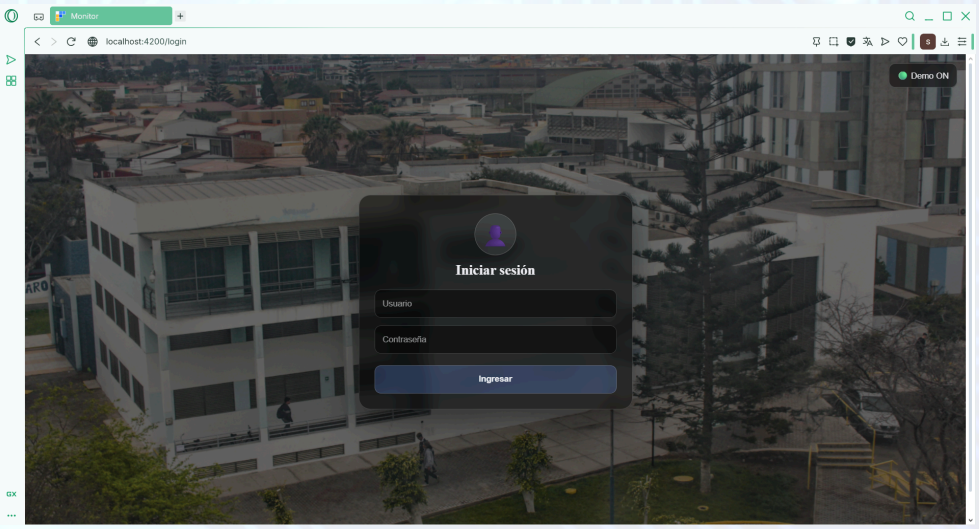

Figura 2: Ingreso al URL

2.Interfaz principal

2.1.Pantalla principal

Una vez autenticado, el usuario accede al panel principal donde puede visualizar la información general del sistema de monitoreo.
Elementos principales:

- Menú lateral:

En este menú al desplegarlo podremos ver la lista de las páginas a las cuales se puede acceder, y en la parte inferior de este menú, se encuentra el botón para cerrar la sesión como muestra la figura 3.

Figura 3: Slider.

- Área de contenido principal

Como podemos ver en la figura 4 se muestra la ventana llamada “Home”, en la cual se encontraran las distintas acciones que realiza el sistema, las cuales son:

- Datos del servidor.
- Agentes.
- Logs.
- Mitre Att&ck.
- Gestión de usuario (solo para el rol de administrador).

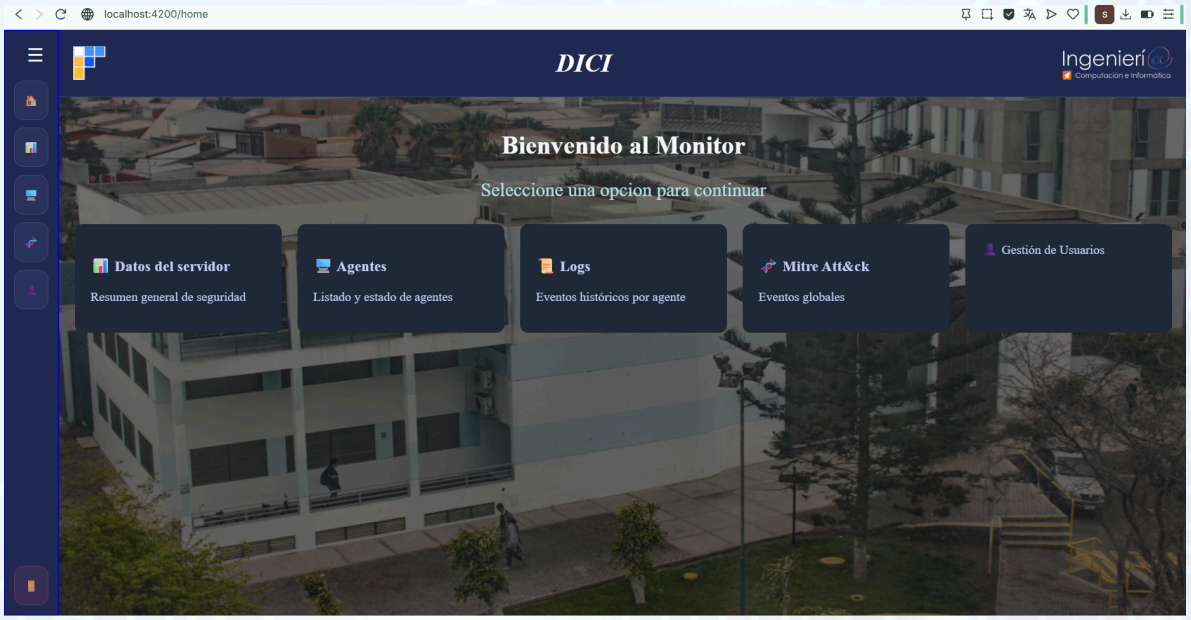

Figura 4: Ingreso al home

3.Gestión de usuarios

Esta ventana es solo para el usuario con rol de “administrador” .

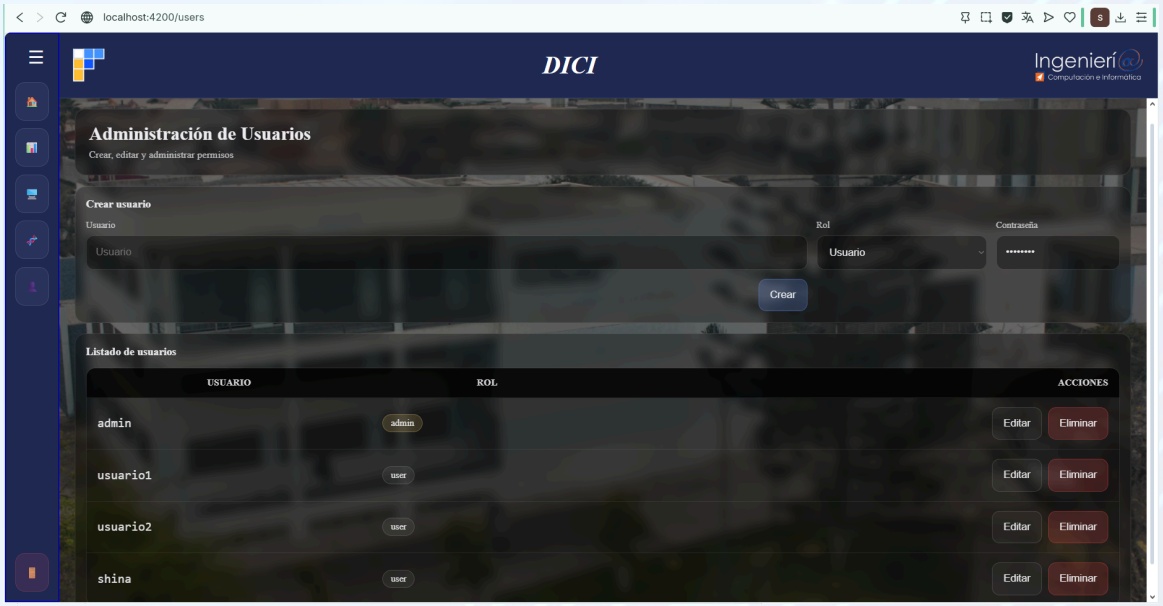

Figura 5: Gestión de usuarios.

3.1.Creación de usuarios

Como se puede ver en la figura 5 lo primero que nos muestra el sistema es un formulario para que el administrador cree usuarios.

Pasos:

1.Ingresar un nombre.
2.Seleccionar un rol (administrador o usuario).
3.Ingresar contraseña.
4.Presionar el botón crear.

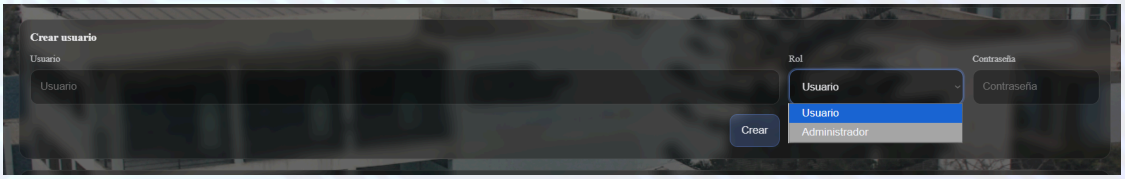

Figura 6: Formulario crear usuario.

3.2.Visualización de usuarios

Seguido del formulario para crear usuario el sistema nos muestra la lista con los usuarios del sistema, en esta lista podemos ver el nombre del usuario, el rol que posee y tenemos 2 botones por cada usuario.

Figura 7: Lista de usuarios.

- Editar:

Al presionar el botón editar, el sistema nos mostrará un formulario con los datos del usuario, hasta el momento solo se puede editar nombre y rol.

Pasos:

1. Presionar el botón editar.
2. Rellenar en el formulario los datos que requiere cambiar.
3. presionar botón guardar.

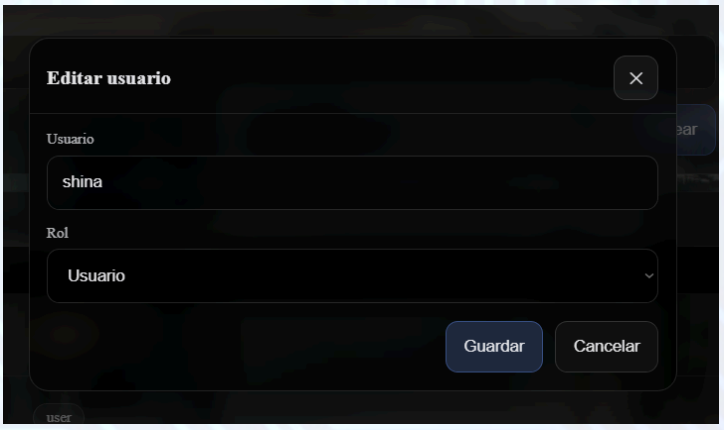

Figura 8: formulario editar usuario.

- Eliminar:

Al presionar el botón eliminar el sistema eliminará el usuario y de igual manera desaparecerá de la lista, aún no se aplica en el sistema la confirmación de eliminar usuario.

4.Datos del servidor

Al ingresar al apartado de datos del servidor como podemos ver en la figura 9 el sistema nos presenta un mensaje para seleccionar el agente del cual quiere ver los datos.

Figura 9: Dashboard wazuh.

El sistema presentará un selector con la lista de los agentes conectados al sistema.

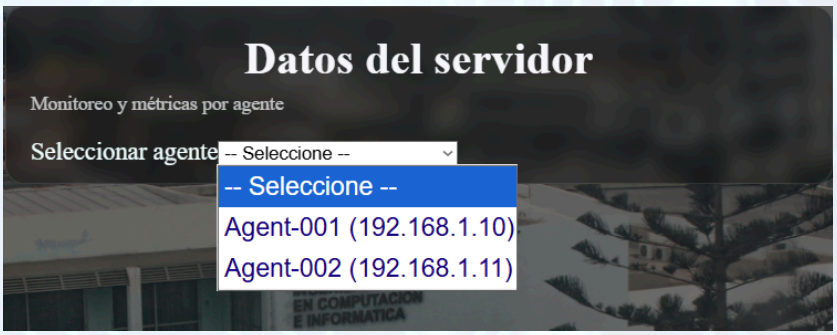

Figura 10: Lista de agentes dashboard.

Al seleccionar un agente el sistema nos mostrará las características que poseen los servidores.

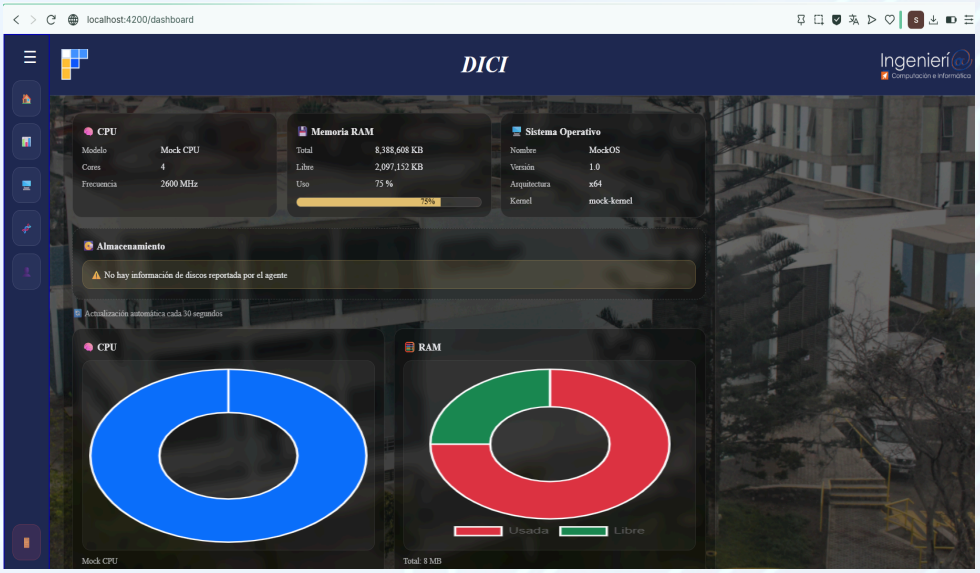

Figura 11: Características del servidor

Como podemos ver en la figura 9 el sistema nos muestra diferentes tarjetas las cuales corresponden a:

- CPU.
- Memoria Ram.
- Sistema operativo.
- Almacenamiento.

Luego de esto el sistema presenta 2 gráficos de dona, los cuales nos muestran la capacidad libre y ocupada de CPU y memoria.

5. Agentes

Al ingresar al apartado de agentes el servidor nos muestra una lista con los agentes conectados al sistema.

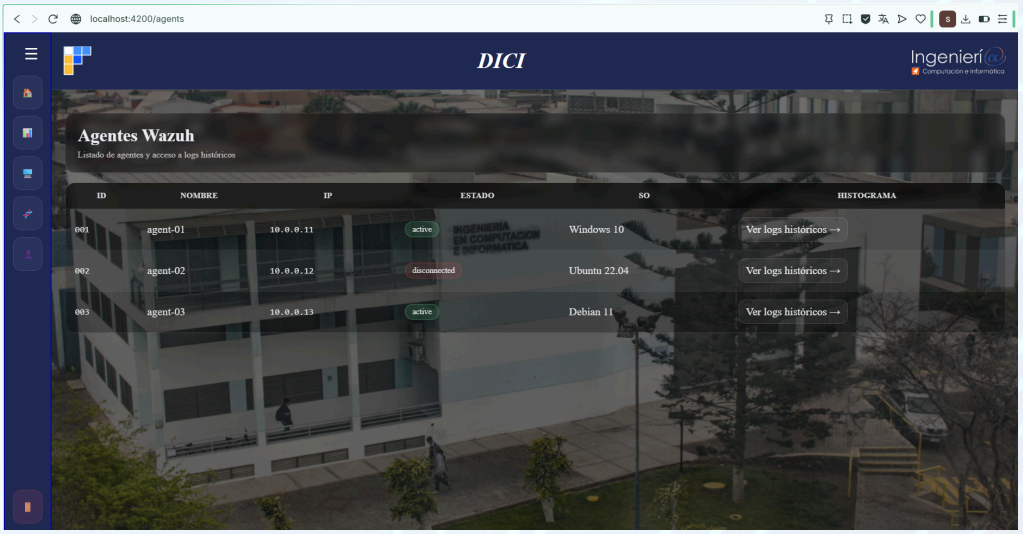

Figura 12: Agentes.

Esta lista de agentes pose datos como:

- ID: Identificador.
- IP: Dirección IP del servidor.
- Estado: activo o inactivo.
- SO: Sistema operativo.
- Histograma: Botón que nos envía a otra ventana.

Si presionamos el botón ver logs históricos, el sistema nos mostrará una lista con todos los eventos que ha capturado wazuh respecto a cada servidor.

Figura 13: Logs históricos.

Como se puede apreciar en la figura 13 el sistema nos muestra un apartado para filtrar los eventos recopilados, este se encuentra en la parte superior, estos filtros nos permiten buscar por nombre o por nivel de alerta como presenta la figura 14.

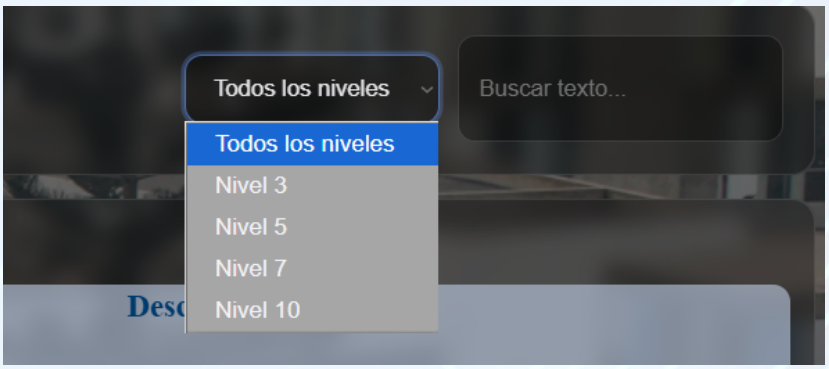

Figura 14: Filtro agentes.

Más abajo de esta lista el sistema nos muestra un gráfico de eventos, el cual irá variando por hora y nivel.

Tabla 15: Gráfico histórico de eventos.

6.MITRE ATT&CK

Al ingresar al apartado de MITRE ATT&CK el sistema nos mostrará las técnicas Globales detectadas, esto a través de distintos gráficos.

Figura 16: Gráficos de mitre

En la figura 16 podemos ver 2 gráficos correspondientes a las tácticas utilizadas en todos los servidores conectados, en el lado derecho vemos un gráfico de líneas por tiempo, mientras que en el lado izquierdo vemos un gráfico de dona con el porcentaje de cada táctica aplicada.
Al costado se encuentra una leyenda con el nombre y color correspondiente a cada táctica.

Más abajo como muestra la figura 17 podemos ver una tabla con:

- Identificador de cada técnica.
- Nombre de la técnica.
- Táctica utilizada.
- Cantidad de alertas generadas.

TÉCNICA	NOMBRE	TÁCTICA	ALERTAS
T1078	Valid Accounts	Persistence	104
T1565.001	Stored Data Manipulation	Impact	49
T1548.003	Abuse Elevation Control Mechanism: Sudo	Privilege Escalation	43
T1021	Remote Services	Lateral Movement	28
T1110.001	Password Guessing	Credential Access	19
T1021.004	SSH	Lateral Movement	8
T1110	Unknown technique	Unknown	1
T1136	Create Account	Persistence	1
T1562.001	Disable or Modify Tools	Defense Evasion	1

Figura 17: tabla de tácticas y técnicas.

Luego de esta tabla, tenemos un gráfico de distribución de técnicas según alertas, al presionar cualquiera de estos bloques, se desplegará un cuadro con la información correspondiente, los colores que poseen estos cuadros, corresponden al nivel de alerta.

Figura 18: Distribución de técnicas según alertas.

Debajo de la distribución de técnicas encontramos una tabla de top de tácticas, en el cual podemos ver de forma ordenada las tácticas capturadas, al seleccionar alguna de estas tácticas, podemos ver que el diagrama de distribución de filtra según corresponde.

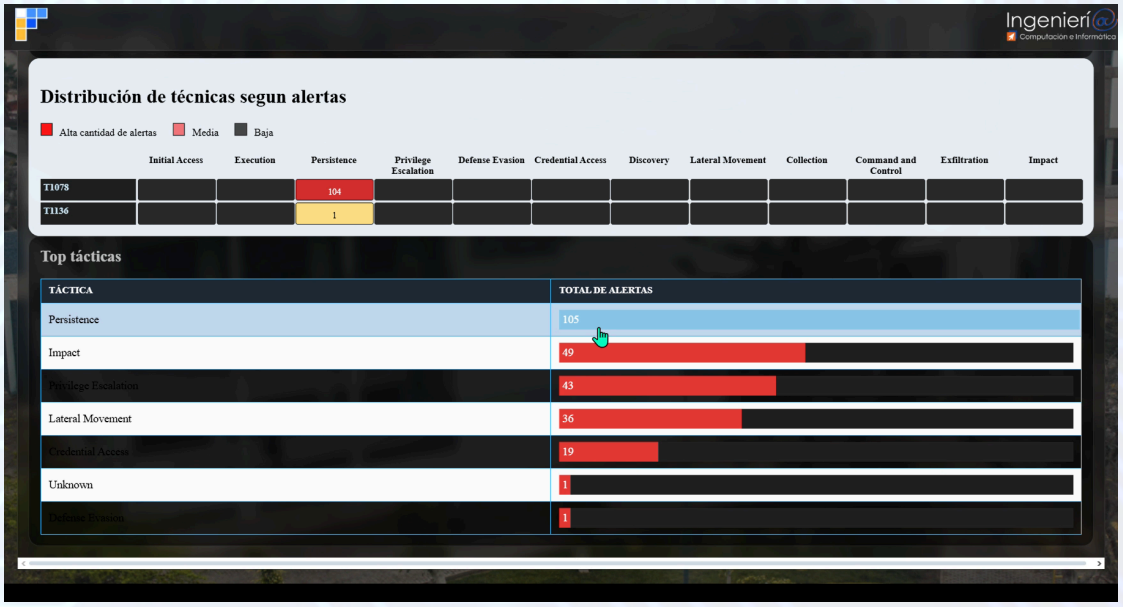

Figura 19: Top tácticas.

7. Funcionalidades adicionales

En la página principal, en la esquina superior derecha podemos ver un botón de activación llamado “demo”, este botón será el encargado de permitir que el sistema funcione con datos reales (demo off) o con datos agregados para demo (demo off).

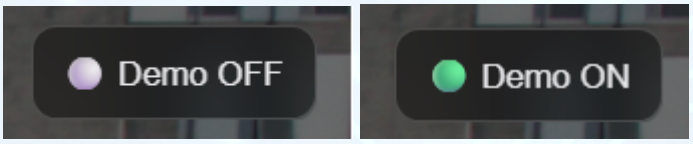

Figura 20 y 21: Botón demo

8.9. Cierre de sesión

Para cerrar sesión en la parte inferior del sidebar, se encuentra el botón de “Cerrar sesión”, al presionarlo el sistema redirigirá a la pantalla principal.

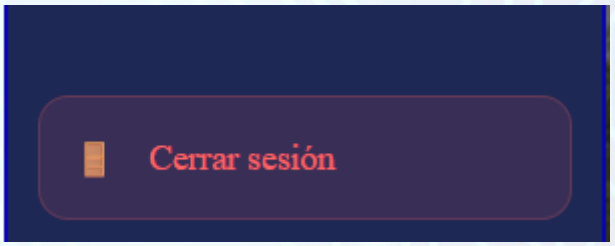

Figura 22: Botón de cerrar sesión

9. Mensajes y errores comunes

Error de conexión

Mensaje: “No se puede conectar con el servidor”
Causa: El backend no está disponible o no hay conexión con Wazuh.

Error de autenticación

Mensaje: “Credenciales incorrectas”
Causa: Usuario o contraseña inválidos.

10. Glosario

Wazuh: Plataforma de seguridad y monitoreo.

Backend: Servicio intermedio que gestiona la lógica del sistema.

Frontend: Interfaz gráfica del usuario.

API: Interfaz de comunicación entre sistemas.