

Controlador de Equipos

Documento para usuarios



Eneko Alabort

30/05/2025

1-Introducción.....	3
2 - Arquitectura y componentes principales.....	4
2.1 Script de escaneo en Python.....	4
2.2 Base de datos SQL Server.....	5
2.3 Aplicación web ASP.NET MVC.....	6
3. Acceso a la Aplicación Web.....	7
3.1 Cómo acceder.....	7
3.2 Seguridad y cifrado.....	8
3.3 ¿Qué es IIS y cómo se hospeda la aplicación?.....	8
4. Uso de la Aplicación.....	9
4.1 Dashboard dinámico.....	9
4.2 Visualización de equipos y puertos.....	10
4.3 Gestión de puertos.....	11
4.4 Historial de escaneos.....	12
4.5 Iniciar un nuevo escaneo.....	13
5. Conclusiones.....	14

1-Introducción

Este documento muestra la estructura principal y el funcionamiento básico del **Controlador de Equipos**, una aplicación web desarrollada para monitorear y gestionar los dispositivos conectados a una red empresarial. El objetivo fundamental de esta herramienta es proporcionar al administrador del sistema una visión actualizada y detallada de los equipos activos en la red, junto con los puertos abiertos en cada dispositivo en el momento del escaneo.

La importancia de esta solución radica en su capacidad para detectar posibles vulnerabilidades de seguridad, dado que la apertura de puertos en equipos conectados puede significar un punto de entrada para ataques o accesos no autorizados. Así, el Controlador de Equipos facilita la identificación temprana de riesgos, permitiendo que el personal de TI actúe rápidamente para mitigar amenazas potenciales. Esta aplicación integra varios componentes que trabajan en conjunto para lograr un monitoreo eficiente:

- Un **script**(código que se ejecuta para automatizar tareas) **de escaneo** desarrollado en Python, que utiliza la herramienta Nmap para detectar los dispositivos conectados, sus direcciones IP, nombres de host, direcciones MAC, sistema operativo y puertos abiertos.
- Una base de datos en SQL Server que almacena la información obtenida de cada escaneo, manteniendo un historial completo para análisis comparativos y auditorías.
- Una interfaz web desarrollada con ASP.NET MVC que permite a los administradores visualizar la información de manera organizada, realizar búsquedas avanzadas por equipos o puertos, y gestionar descripciones o anotaciones sobre cada puerto detectado.

Gracias a esta integración, el Controlador de Equipos no solo facilita el proceso de escaneo y registro de dispositivos, sino que también ofrece una plataforma intuitiva para la gestión y evaluación continua de la seguridad en la red corporativa.

2 - Arquitectura y componentes principales

El Controlador de Equipos está diseñado como una solución modular que combina varios componentes tecnológicos para cumplir con su función de monitoreo y gestión de la red. A continuación, se describen los principales elementos que forman parte de esta arquitectura:

2.1 Script de escaneo en Python

El corazón del sistema es un script desarrollado en Python que automatiza la exploración de la red. Utiliza la popular herramienta de código abierto **Nmap** para realizar escaneos detallados sobre los rangos de direcciones IP configurados. Este script realiza las siguientes tareas principales:

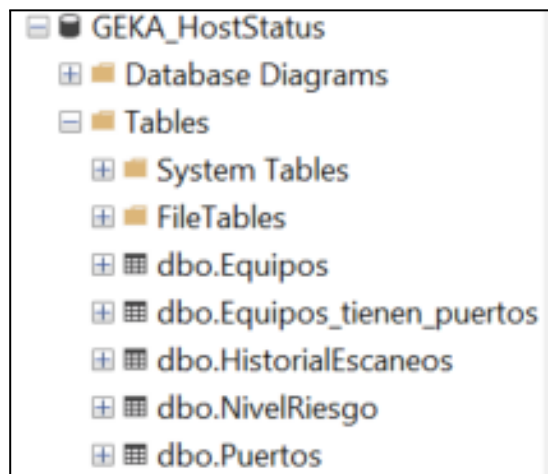
- Detecta los hosts activos en la red.
- Obtiene datos esenciales de cada equipo, como hostname, dirección IP, dirección MAC y sistema operativo.
- Identifica los puertos abiertos.
- Inserta o actualiza esta información en la base de datos central, asegurando que el historial de escaneos quede registrado.

El script está optimizado para ejecutarse en paralelo, utilizando múltiples hilos (threads) que aceleran el proceso sin saturar la red, y cuenta con manejo de errores para garantizar la estabilidad del escaneo.

2.2 Base de datos SQL Server

Toda la información recolectada por el script se almacena en una base de datos relacional SQL Server, estructurada en varias tablas que permiten organizar los datos de forma eficiente:

- **Equipos:** Almacena la información general de cada dispositivo detectado.
- **Puertos:** Contiene los puertos conocidos y sus posibles descripciones o niveles de riesgo.
- **Equipos_tienen_puertos:** Tabla intermedia que relaciona cada equipo con los puertos abiertos detectados.
- **HistorialEscaneos:** registra el detalle de cada escaneo realizado, incluyendo la fecha y los puertos abiertos en ese momento.
- **NivelRiesgo:** Guarda los valores Bajo, Medio y Alto los cuales son usados en la tabla puertos para describir su nivel de vulnerabilidad.

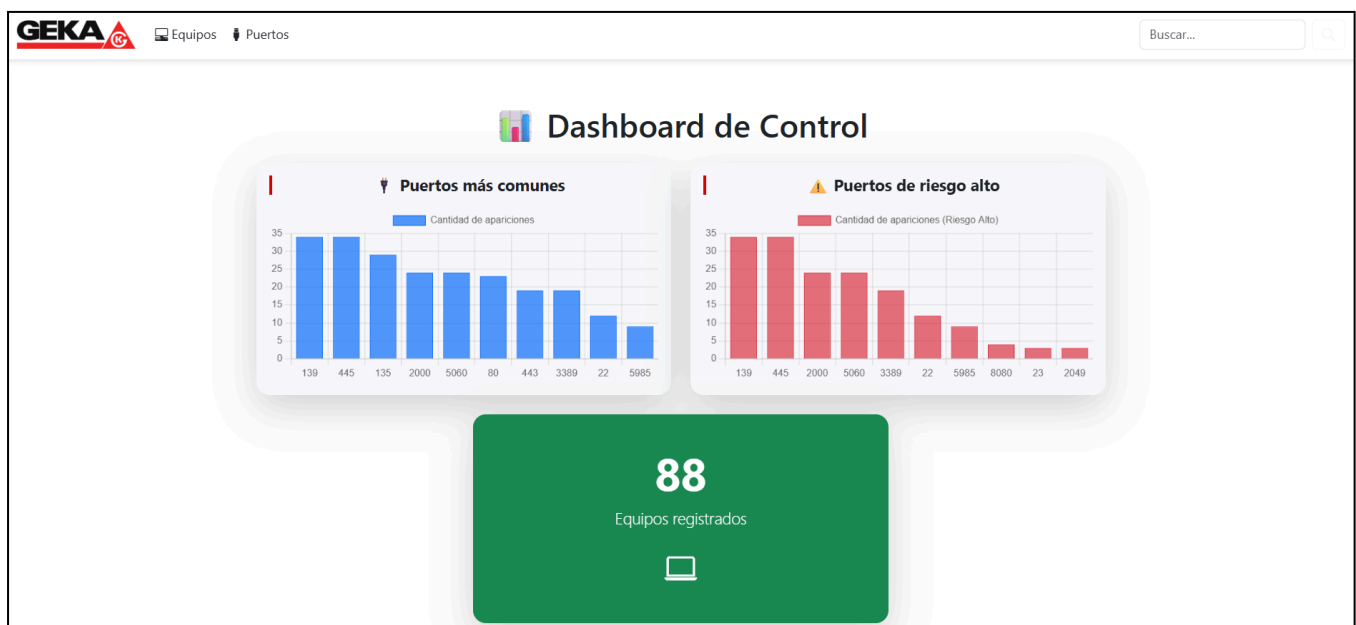


Esta estructura facilita consultas rápidas y flexibles, así como la generación de reportes históricos y alertas.

2.3 Aplicación web ASP.NET MVC

El usuario final interactúa con la plataforma a través de una aplicación web desarrollada con **ASP.NET MVC**, que se encarga de:

- Mostrar listados actualizados de los equipos y sus puertos abiertos.
- Permitir búsquedas por hostname, IP o número de puerto.
- Visualizar detalles históricos y actuales del estado de la red.
- Gestionar la información adicional, como descripciones de puertos y niveles de riesgo.
- Ejecutar comandos para iniciar el escaneo desde la interfaz y mostrar el resultado.



La aplicación web se conecta directamente a la base de datos y expone un diseño limpio y funcional para facilitar la tarea del administrador.

3. Acceso a la Aplicación Web

La aplicación Controlador de Equipos está alojada en un servidor interno de la empresa, accesible mediante un navegador web. Esta plataforma permite a los administradores de red consultar el estado de los dispositivos conectados, revisar puertos abiertos y gestionar información de forma centralizada.

3.1 Cómo acceder

- La aplicación está disponible a través de la siguiente dirección segura:
<https://gekace.geka.es:8081>
- Para acceder, es necesario estar conectado a la red corporativa, ya sea físicamente o a través de la VPN corporativa.



3.2 Seguridad y cifrado

- Para proteger la información transmitida entre el navegador y el servidor, la aplicación utiliza un certificado de seguridad que habilita HTTPS con cifrado local.
- Esto garantiza que los datos intercambiados, como nombres de usuario, contraseñas y detalles de los escaneos, estén protegidos frente a interceptaciones no autorizadas.
- La conexión segura proporciona confianza y cumple con las políticas de seguridad de la empresa para la gestión de información sensible.

3.3 ¿Qué es IIS y cómo se hospeda la aplicación?

- IIS (Internet Information Services) es un servidor web desarrollado por Microsoft que permite publicar aplicaciones web en entornos Windows.
- En nuestra empresa, IIS se utiliza para alojar la aplicación Controlador de Equipos de forma local, facilitando su acceso mediante navegadores web.
- IIS gestiona las peticiones de los usuarios, entrega las páginas web, y se encarga de la seguridad y configuración del acceso a la aplicación.
- Gracias a IIS, la aplicación está disponible de forma continua y estable para los usuarios autorizados, con soporte para protocolos seguros como HTTPS.

4. Uso de la Aplicación

Este apartado describe las funcionalidades básicas que el usuario puede realizar en la aplicación Controlador de Equipos. A continuación se explican las acciones más comunes con ejemplos visuales.

4.1 Dashboard dinámico

- Al ingresar a la aplicación, se muestra un dashboard que se actualiza automáticamente con la información más reciente de los equipos y sus puertos abiertos en la red.
- No es necesario realizar ninguna acción para refrescar la información; los datos se actualizan periódicamente para mostrar el estado actual de la red.



4.2 Visualización de equipos y puertos

- En la sección Equipos en clickando en el botón de detalles, puede ver el listado de equipos activos en la red junto con sus puertos abiertos.

GEKA

Equipos Puertos

1

Verificar y Ejecutar Script

Historial de Escaneos

Consulta el historial completo de escaneos realizados.

Ver historial

Hostname	IP	MAC	OS	Acciones
ggklap030.ggk.local	192.168.1.1			Editar Detalles Eliminar
PLANTA1-GGK-local	192.168.1.137		Microsoft Windows 11 21H2	Editar Detalles Eliminar

2

Detalles del Equipo

Información General


Hostname	
IP	192.168.1.137
MAC	
Sistema Operativo	Microsoft Windows 11 21H2



Puertos Asociados

Número de Puerto	Descripción	Nivel de Riesgo
135	RPC (Remote Procedure Call), administración de procesos y servicios en Windows.	Bajo
139	NetBIOS Session Service, compartición de archivos e impresión en redes Windows.	Alto
445	SMB (Server Message Block), compartición de archivos e impresoras en redes Windows.	Alto
1947	FlexNet License Server, gestión de licencias de software.	Alto
2000	Cisco SCCP, señalización y control de teléfonos IP en redes Cisco.	Alto
5060	SIP, señalización para sesiones de voz y video en VoIP.	Alto


4.3 Gestión de puertos

- Seleccione un puerto para ver o editar su descripción y nivel de riesgo.
- Use los botones para crear nuevos puertos, modificar los existentes o eliminarlos según sea necesario.



 Equipos  Puertos

Buscar...

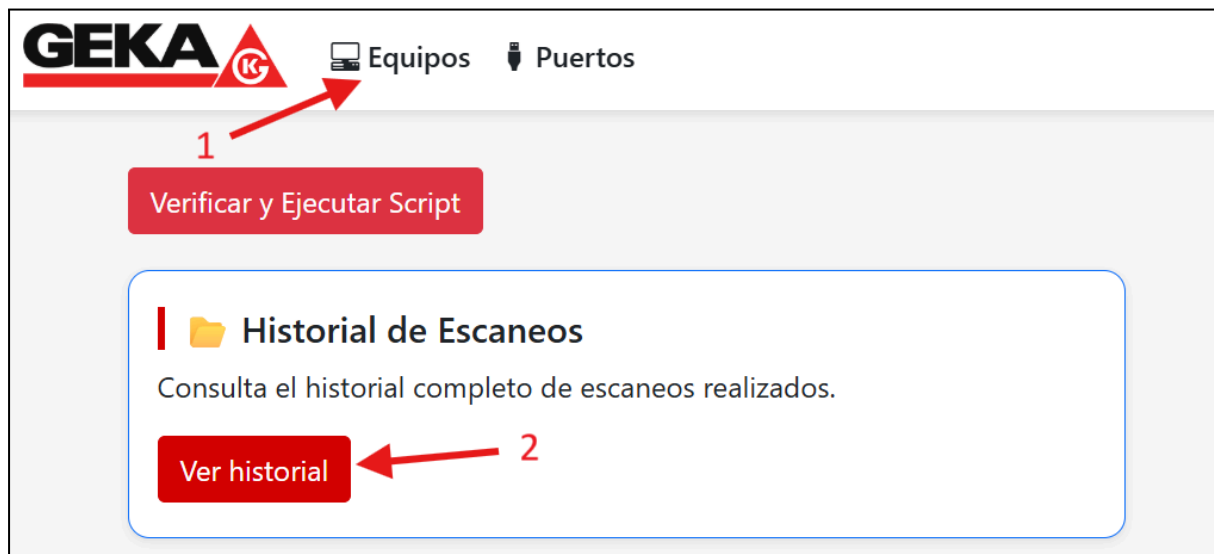


Crear Nuevo Puerto

Puerto	Descripción	Acciones
21	FTP, transferencia y gestión de archivos entre cliente y servidor.	<div>EditarDetalles</div> <div>Eliminar</div>
22	SSH, acceso seguro y administración remota de sistemas.	<div>EditarDetalles</div> <div>Eliminar</div>
23	Telnet, acceso remoto no cifrado a dispositivos y sistemas.	<div>EditarDetalles</div> <div>Eliminar</div>
53	DNS, resolución de nombres de dominio a direcciones IP.	<div>EditarDetalles</div> <div>Eliminar</div>
80	HTTP, transmisión de páginas web sin cifrado.	<div>EditarDetalles</div> <div>Eliminar</div>

4.4 Historial de escaneos

- Acceda al historial para revisar escaneos anteriores con detalles de puertos abiertos y fechas.
- Esta función permite comparar estados y detectar cambios o nuevas vulnerabilidades.

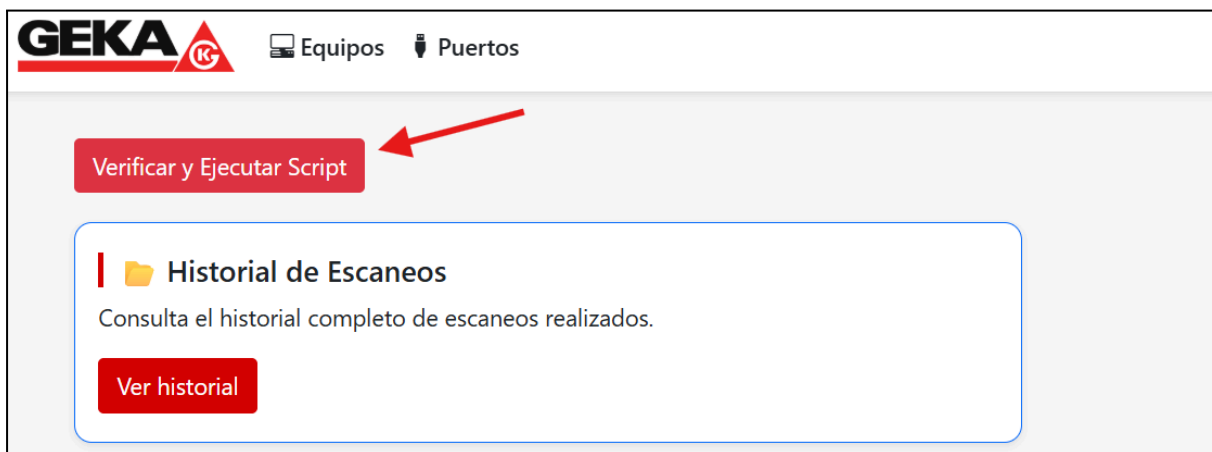


The screenshot shows the GEKA web interface with a search bar at the top right. Below the search bar, there's a section with a dropdown menu 'Buscar por Hostna' and a search input field 'Escribe para buscar...'. To the right of the search input is a red button labeled 'Buscar'. Below the search section is a table with the following data:

Hostname	IP	MAC	Sistema Operativo	Puertos Abiertos	Fecha Escaneo
ggklap030.ggk.local	192.168.1.1		Fortinet FortiOS 6.2 - 7.2	443	26/05/2025 11:30
GGKDSK003.GGK.local	192.168.1.56		Microsoft Windows Server 2008 R2 or Windows 7 SP1	135,139,2000,3389,445,49165,5060,5357,5800,5900	26/05/2025 11:31
PLANTA1.GGK.local	192.168.1.126		Microsoft Windows 11 21H2	135,139,2000,3389,445,5060	26/05/2025 11:32
PLANTA6-GK2.GGK.local	192.168.1.127		Microsoft Windows 11 21H2	135,139,2000,3389,445,5060	26/05/2025 11:32
	192.168.1.130				26/05/2025 11:33

4.5 Iniciar un nuevo escaneo

- Desde la interfaz, puede lanzar un escaneo manual para actualizar la información de la red.
- El proceso se ejecuta en segundo plano y se notificará cuando haya resultados disponibles.



5. Conclusiones

El Controlador de Equipos representa una solución integral y eficiente para la supervisión de dispositivos conectados en redes corporativas. Gracias a la combinación de tecnologías como Python, Nmap, SQL Server y ASP.NET MVC, esta herramienta proporciona a los administradores de sistemas una visión clara y actualizada del estado de la red.

Su enfoque modular permite no solo automatizar tareas de escaneo y registro, sino también gestionar información crítica sobre puertos abiertos y niveles de riesgo, lo que contribuye directamente a la seguridad informática de la empresa. La capacidad de mantener un historial de escaneos y detectar cambios en los dispositivos conectados proporciona una base sólida para auditorías y análisis forenses.

Además, la interfaz web intuitiva facilita la interacción del usuario con el sistema, mientras que el uso de HTTPS y el alojamiento en IIS garantizan un acceso seguro y confiable.

En definitiva, esta aplicación no solo agiliza el trabajo del personal de TI, sino que también fortalece la postura de ciberseguridad de la organización, anticipándose a posibles amenazas mediante una vigilancia constante y centralizada de los puntos críticos de la red.