

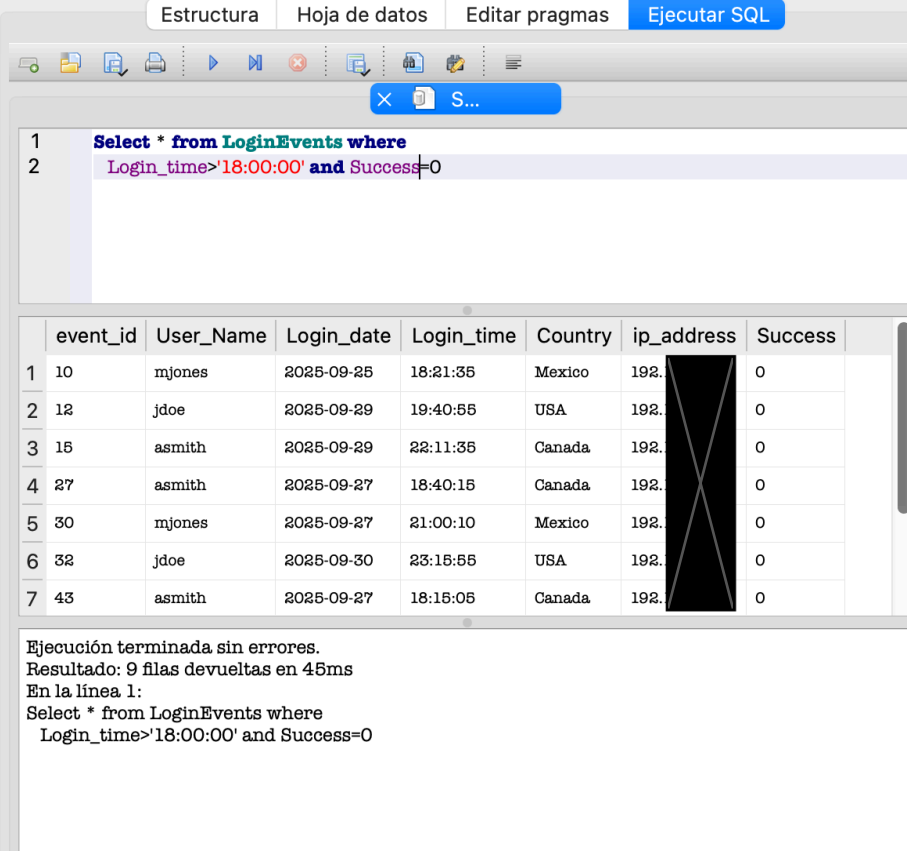
Aplicar filtros SQL a queries

Descripción

Sobre una base de datos **simulada** en SQLite, de los datos de acceso a la red una organización no existente, he aplicado algunos filtros para detectar ciertas condiciones interesantes para la seguridad de la organización.

Detectar accesos al sistema después de la hora de trabajo

Buscamos los fallos de login ocurridos después de las 18:00, que han dado como resultado un fallo en el login. Son indicativos de intento de acceso “extraño” a la red, que merecen ser investigados.



The screenshot shows a SQLite GUI with the following components:

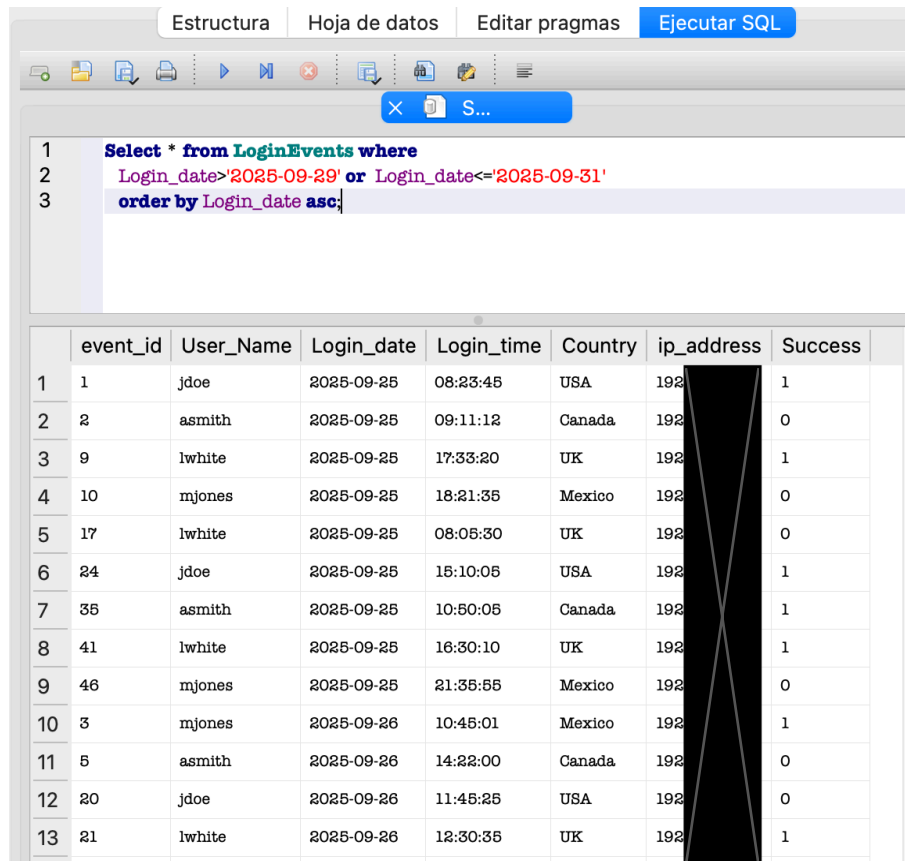
- Toolbar:** Estructura, Hoja de datos, Editar pragmas, Ejecutar SQL.
- Query Editor:** Contains the SQL query:

```
1 Select * from LoginEvents where
2 Login_time>'18:00:00' and Success=0
```
- Results Table:** A table with 9 rows and 8 columns. The columns are event_id, User_Name, Login_date, Login_time, Country, ip_address, and Success. The Success column contains the value 0 for all rows. The ip_address column is redacted with a black box.
- Status Bar:** Ejecución terminada sin errores. Resultado: 9 filas devueltas en 45ms. En la línea 1: Select * from LoginEvents where Login_time>'18:00:00' and Success=0

	event_id	User_Name	Login_date	Login_time	Country	ip_address	Success
1	10	mjones	2025-09-25	18:21:35	Mexico	192.	0
2	12	jdoe	2025-09-29	19:40:55	USA	192.	0
3	15	asmith	2025-09-29	22:11:35	Canada	192.	0
4	27	asmith	2025-09-27	18:40:15	Canada	192.	0
5	30	mjones	2025-09-27	21:00:10	Mexico	192.	0
6	32	jdoe	2025-09-30	23:15:55	USA	192.	0
7	43	asmith	2025-09-27	18:15:05	Canada	192.	0

Recuperar los intentos de login en un rango de fechas especificadas.

“Ocurrió” un incidente el 30/09/25, quiero recuperar los accesos del 20/09 y el 31/09 para comprobar lo sucedido y los antecedentes el día previo y posterior.



The screenshot shows a database management interface with a menu bar (Estructura, Hoja de datos, Editar pragmas, Ejecutar SQL) and a toolbar. A SQL query is entered in the editor:

```
1 Select * from LoginEvents where
2 Login_date>'2025-09-29' or Login_date<='2025-09-31'
3 order by Login_date asc;
```

Below the query, a table of results is displayed with 13 rows and 8 columns: event_id, User_Name, Login_date, Login_time, Country, ip_address, and Success. The ip_address column is redacted with a black box.

	event_id	User_Name	Login_date	Login_time	Country	ip_address	Success
1	1	jdoe	2025-09-25	08:23:45	USA	192	1
2	2	asmith	2025-09-25	09:11:12	Canada	192	0
3	9	lwhite	2025-09-25	17:33:20	UK	192	1
4	10	mjones	2025-09-25	18:21:35	Mexico	192	0
5	17	lwhite	2025-09-25	08:05:30	UK	192	0
6	24	jdoe	2025-09-25	15:10:05	USA	192	1
7	35	asmith	2025-09-25	10:50:05	Canada	192	1
8	41	lwhite	2025-09-25	16:30:10	UK	192	1
9	46	mjones	2025-09-25	21:35:55	Mexico	192	0
10	3	mjones	2025-09-26	10:45:01	Mexico	192	1
11	5	asmith	2025-09-26	14:22:00	Canada	192	0
12	20	jdoe	2025-09-26	11:45:25	USA	192	0
13	21	lwhite	2025-09-26	12:30:35	UK	192	1

Detectar los accesos que se han realizado desde fuera de Méjico.

En este caso hemos de modificar el condicional del selector “where” en la función SQL para incluir el país que nos interesa.

Estructura

Hoja de datos

Editar pragmas

Ejecutar SQL

Recuperar los empleados en el departamento de Ventas(Sales)

Necesito recuperar el listado de los empleados del departamento de ventas para comprobar el estado de actualización de su máquina y los parches que deben aplicarsele.

Estructura Hoja de datos Editar pragmas Ejecutar SQL					
S...					
1	select * from Employees				
2	where department ='Sales'				
3	order by username DESC;				
	employee_id	device_id	username	department	office
1	46	146	thomas_jackson	Sales	East-345
2	60	160	susan_taylor	Sales	East-360
3	23	123	ryan_moore	Sales	South-122
4	32	132	peter_miller	Sales	North-132
5	15	115	paul_jackson	Sales	South-115
6	35	135	nancy_clark	Sales	West-135
7	6	106	mary_brown	Sales	North-105
8	53	153	kevin_davis	Sales	North-153
9	28	128	katherine_smith	Sales	North-128
10	19	119	john_walker	Sales	South-119
11	56	156	jennifer_white	Sales	South-156
12	39	139	harry_jones	Sales	North-139
13	43	143	emily_taylor	Sales	North-143

Recuperar los empleados de los departamentos de finanzas o ventas

Estructura					
Hoja de datos					
Editar pragmas					
Ejecutar SQL					
S...					
1	select * from Employees				
2	where department='Finance' or department='Sales'				
3	order by department DESC;				
	employee_id	device_id	username	department	office
1	6	106	mary_brown	Sales	North-105
2	10	110	carol_lee	Sales	North-109
3	15	115	paul_jackson	Sales	South-115
4	19	119	john_walker	Sales	South-119
5	23	123	ryan_moore	Sales	South-122
6	28	128	katherine_smith	Sales	North-128
7	32	132	peter_miller	Sales	North-132
8	35	135	nancy_clark	Sales	West-135
9	39	139	harry_jones	Sales	North-139
10	43	143	emily_taylor	Sales	North-143
11	46	146	thomas_jackson	Sales	East-146
12	50	150	emily_jones	Sales	North-150
13	53	153	kevin_davis	Sales	North-153

Recuperar los empleados que no están en el departamento de IT

Estructura					
Hoja de datos					
Editar pragmas					
Ejecutar SQL					
S...					
1	select * from Employees				
2	where department not like 'IT'				
3	order by department DESC;				
	employee_id	device_id	username	department	office
1	6	106	mary_brown	Sales	North-106
2	10	110	carol_lee	Sales	North-109
3	15	116	paul_jackson	Sales	South-116
4	19	119	john_walker	Sales	South-119
5	23	123	ryan_moore	Sales	South-122
6	28	128	katherine_smith	Sales	North-128
7	32	132	peter_miller	Sales	North-132
8	36	136	nancy_clark	Sales	West-136
9	39	139	harry_jones	Sales	North-139
10	43	143	emily_taylor	Sales	North-143
11	46	146	thomas_jackson	Sales	East-146
12	50	150	emily_jones	Sales	North-150
13	53	153	kevin_davis	Sales	North-153

Recuperar los empleados de ventas de las oficinas en el ala Norte.

En este caso modificamos la cláusula 'where' y en la condición de departamento usamos el carácter '%' para seleccionar cualquier departamento que empiece por "North"

Estructura
Hoja de datos
Editar pragmas
Ejecutar SQL

S...

```

1 select * from Employees
2   where department='Sales' and office like 'North%'
3   order by department DESC;

```

	employee_id	device_id	username	department	office
1	6	106	mary_brown	Sales	North-105
2	10	110	carol_lee	Sales	North-109
3	28	128	katherine_smith	Sales	North-128
4	32	132	peter_miller	Sales	North-132
5	39	139	harry_jones	Sales	North-139
6	43	143	emily_taylor	Sales	North-143
7	50	150	emily_jones	Sales	North-150
8	53	153	kevin_davis	Sales	North-153

Resumen.

Como hemos visto a lo largo del document, he trabajado con dos tablas (employees y loginevents) y mediante la combinación distintos filtros mediante operadores lógicos (AND, OR) he extraído información para el análisis de los accesos a la infraestructura de una organización.