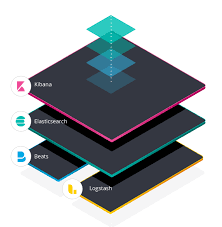
**Tutorial Stack ELK Siem**



Daniel Escaño Hernández CET Ciberseguridad

# **1. Índice:**

[**1. Índice:**](#_lmwzrhyaxgtw) **1**

[**2. Instalación de componentes necesarios**](#_g59i8ewd3ed3) **2**

[**2.1 Java y Nginx:**](#_5d38uxjyswtl) **2**

[**2.2 Elasticsearch**](#_owyw77u49jv) **3**

[**2.3 Kibana**](#_urplixozdiv8) **4**

[**2.4 Logstash**](#_ibeowhitygpl) **5**

[**2.5 Suricata**](#_jppzb7m1j2gr) **6**

[**3. Configuración LogStash**](#_tijqjyt0sqr8) **7**

[**4. Consulta de eventos y gráficas**](#_sxlbalajyea5) **8**

[**4.1 Gráfica de Barras verticales**](#_1cn4mcbbi8my) **9**

[**4.2 Gráfica de Línea**](#_4ndngguvx64h) **10**

[**4.3 Tabla**](#_ucldlrjopnh0) **10**

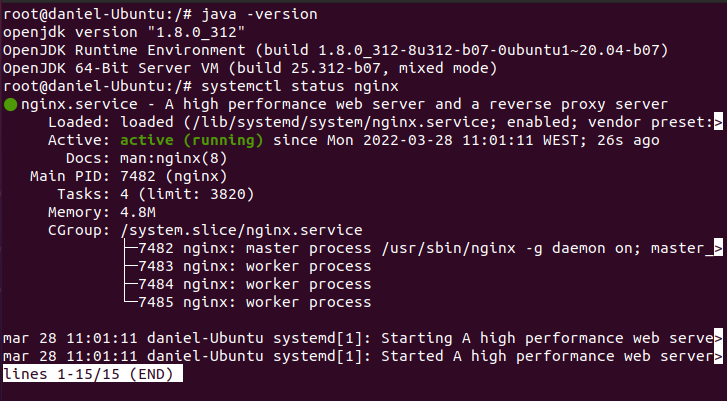
[**4.4 Métrica**](#_cqqqmwgdc1ib) **11**

[**4.5 Gráfica de Donut**](#_2w81h6i52xuk) **12**

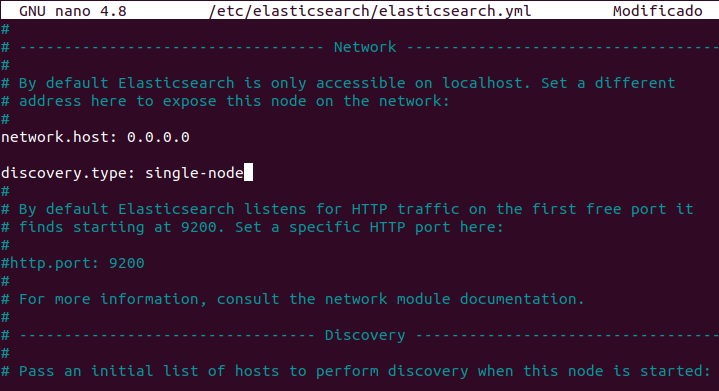
[**4.6 Panel**](#_494j2n4xgcg4) **12**

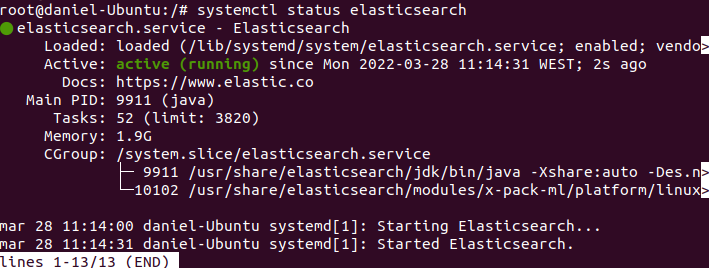
# **2. Instalación de componentes necesarios**

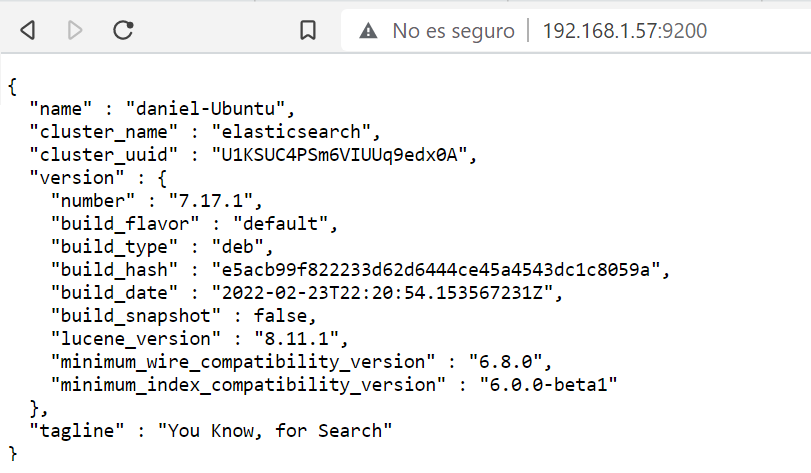
### **2.1 Java y Nginx:**



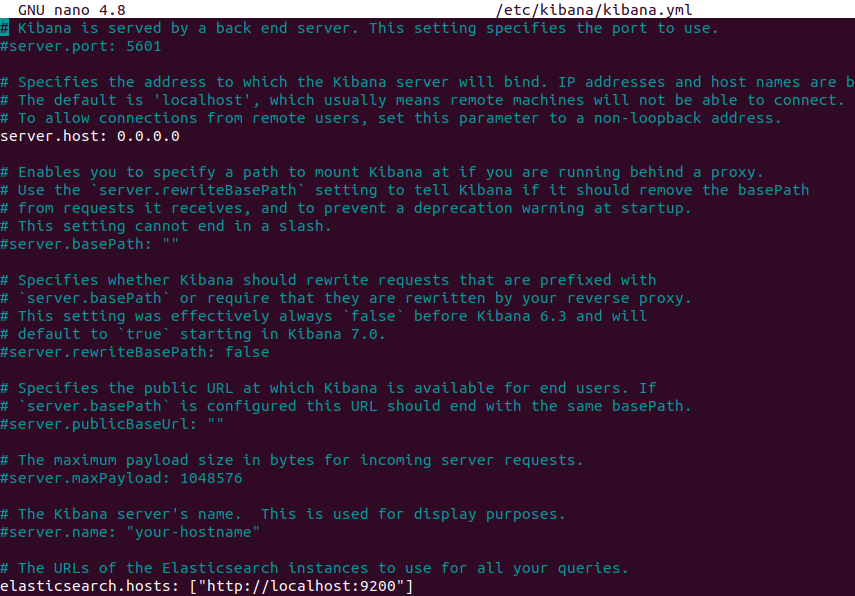
### **2.2 Elasticsearch**

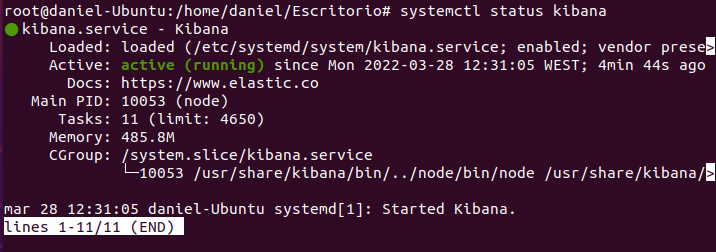


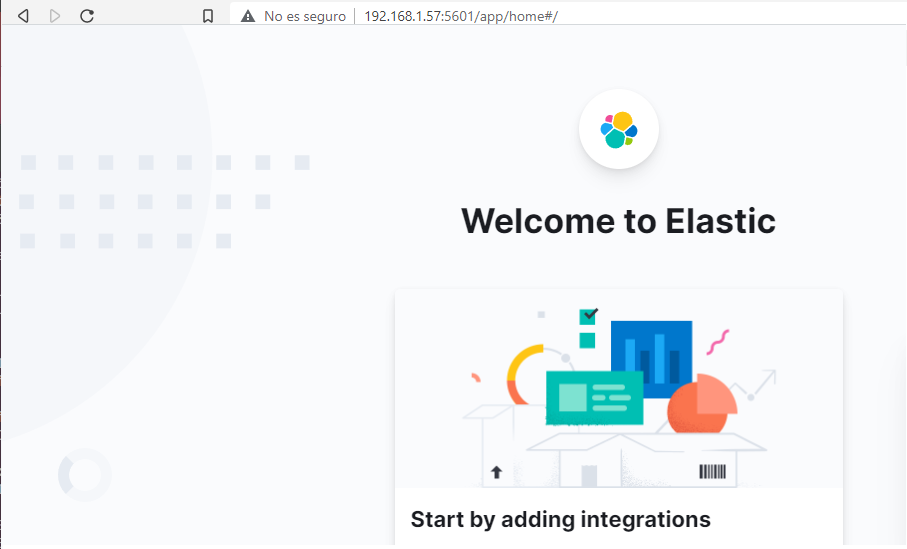




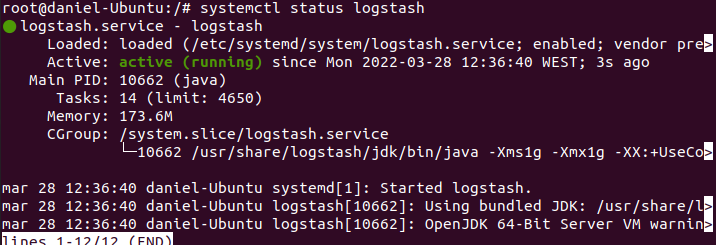
### **2.3 Kibana**



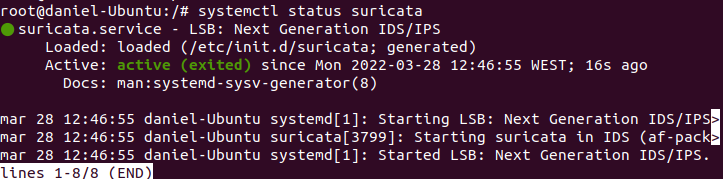


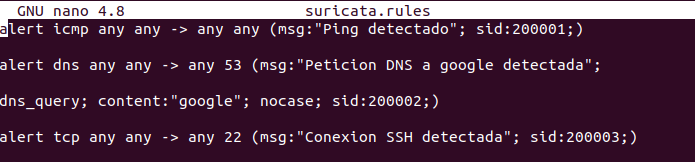


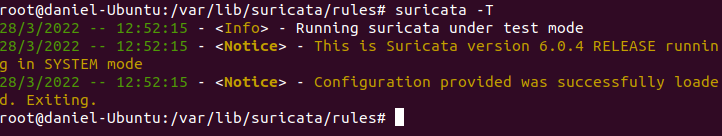
### **2.4 Logstash**

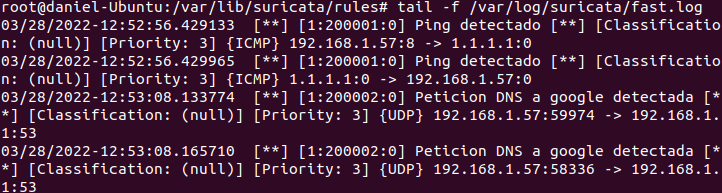


### **2.5 Suricata**

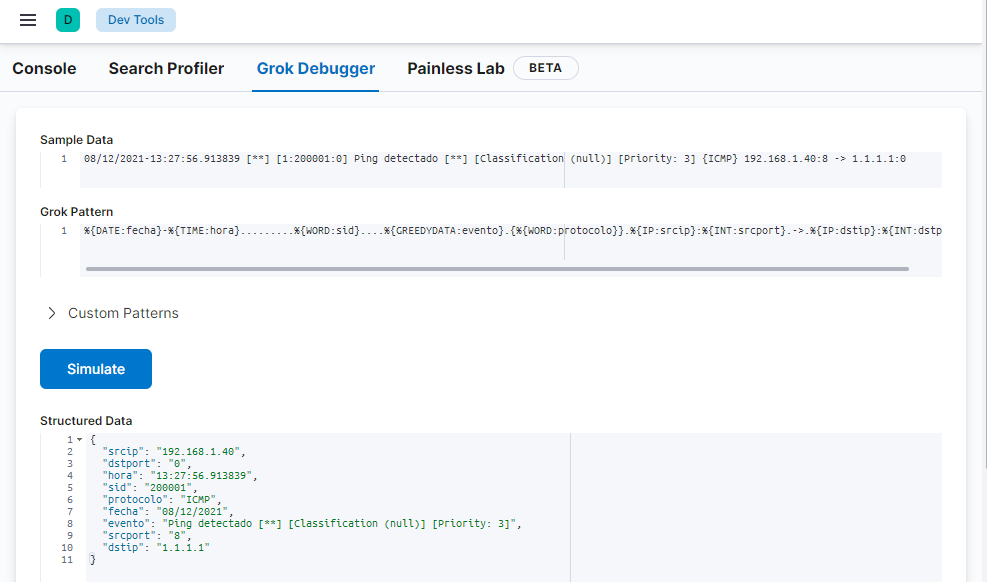


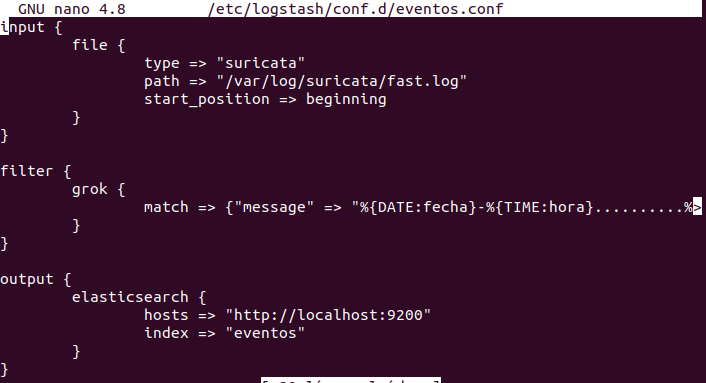




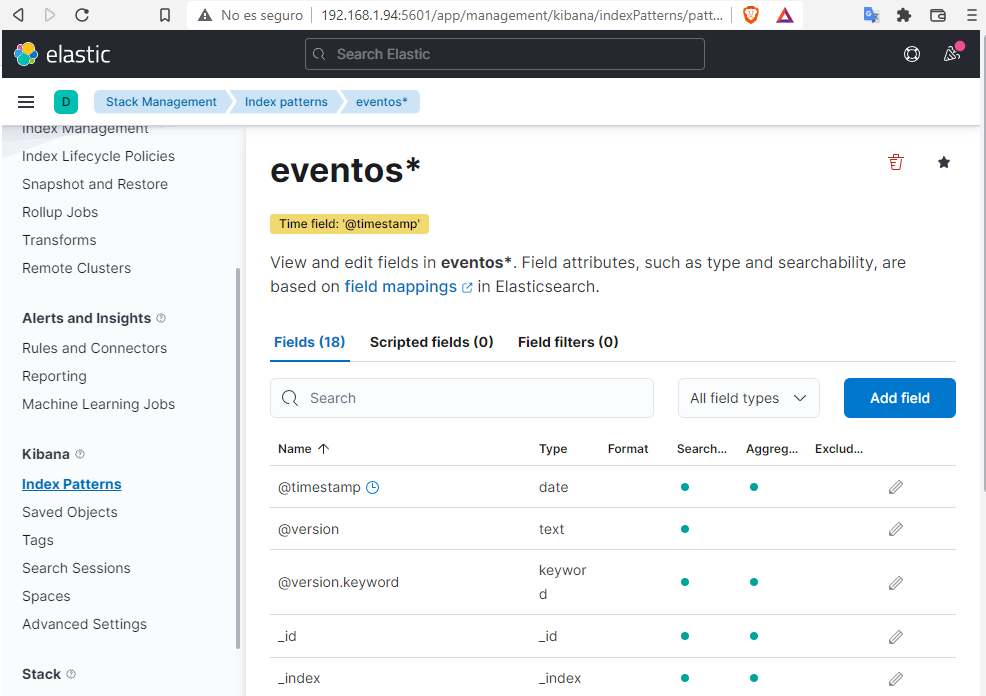


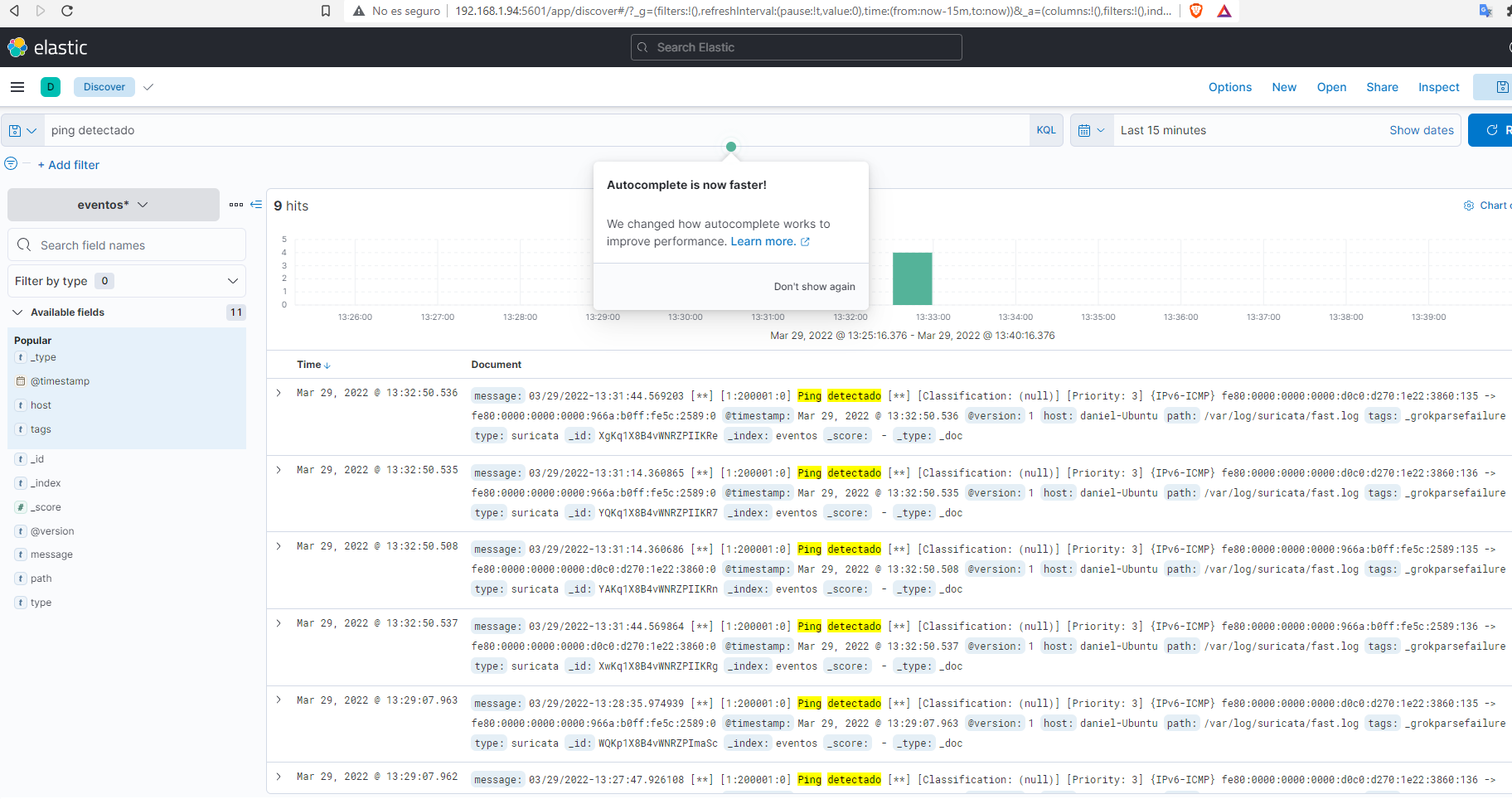
# **3. Configuración LogStash**



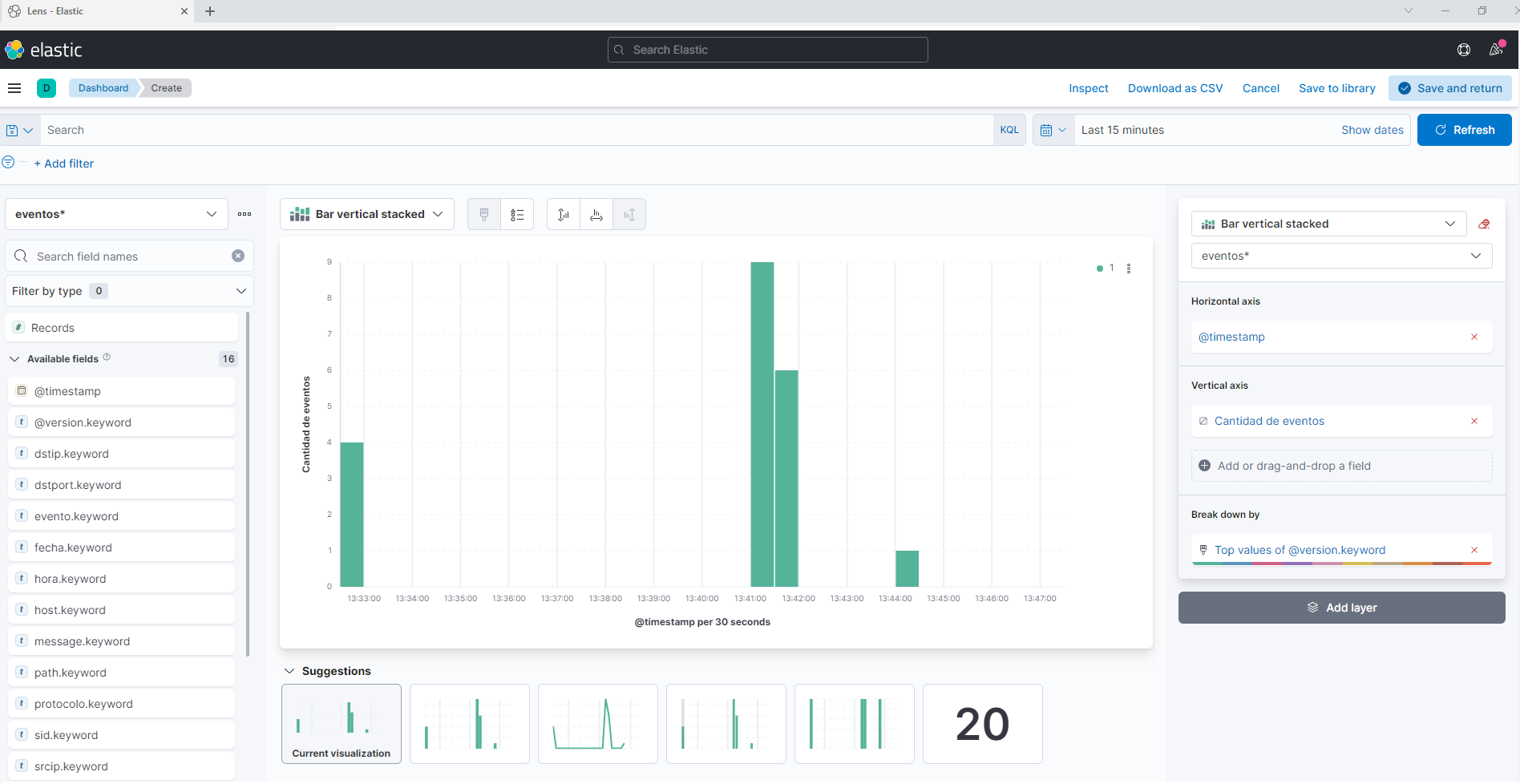


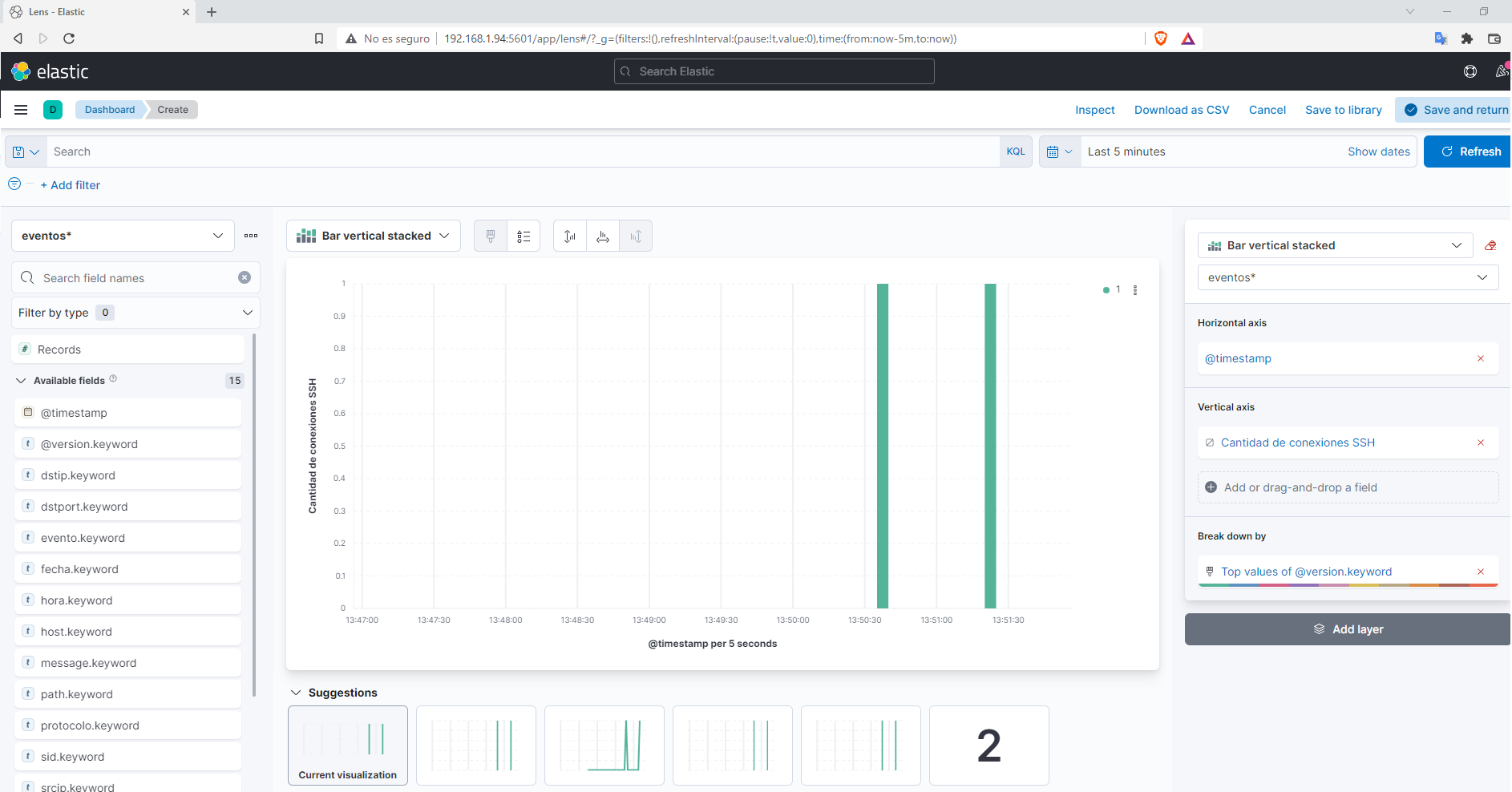
# **4. Consulta de eventos y gráficas**



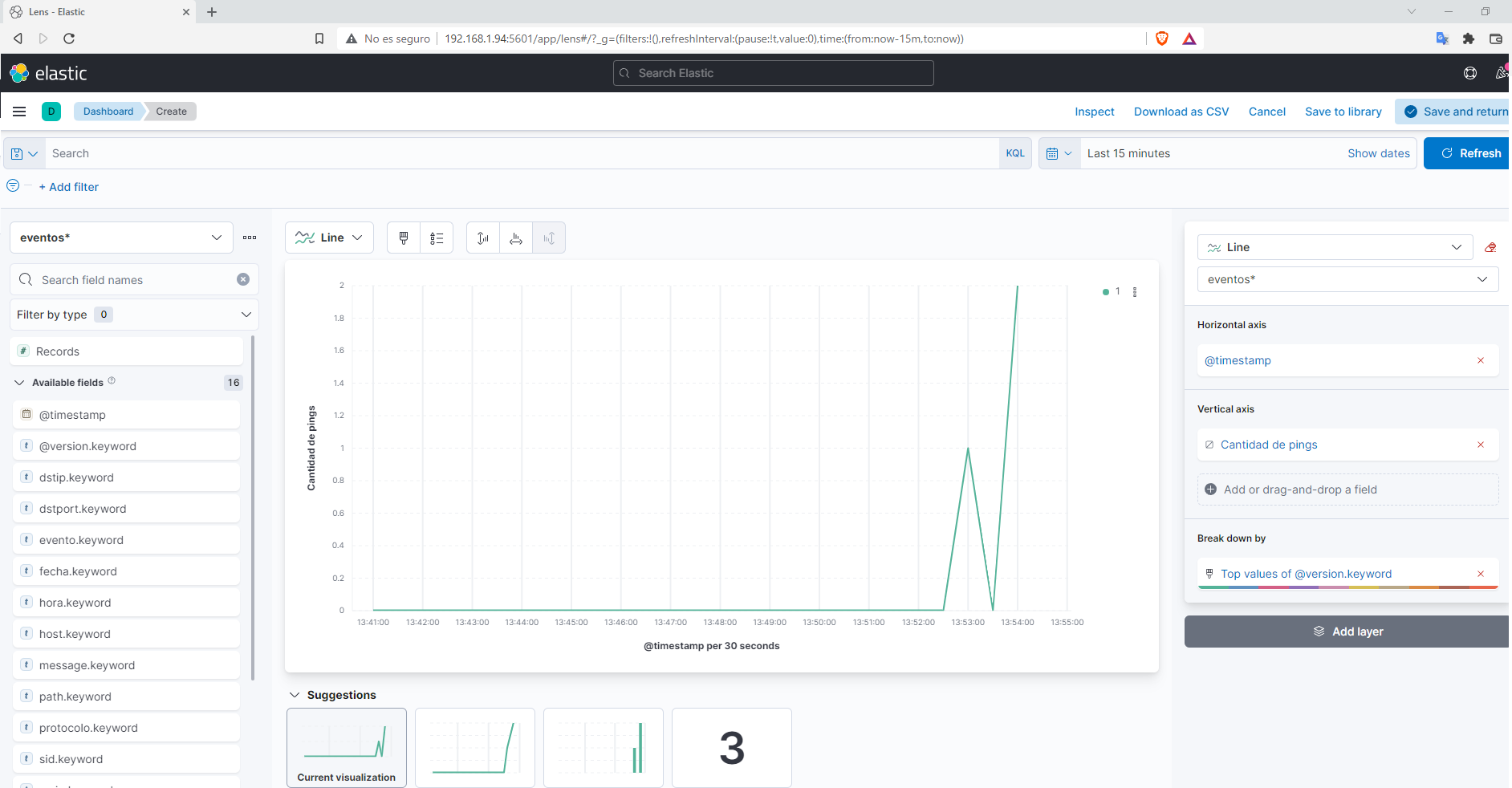


### **4.1 Gráfica de Barras verticales**

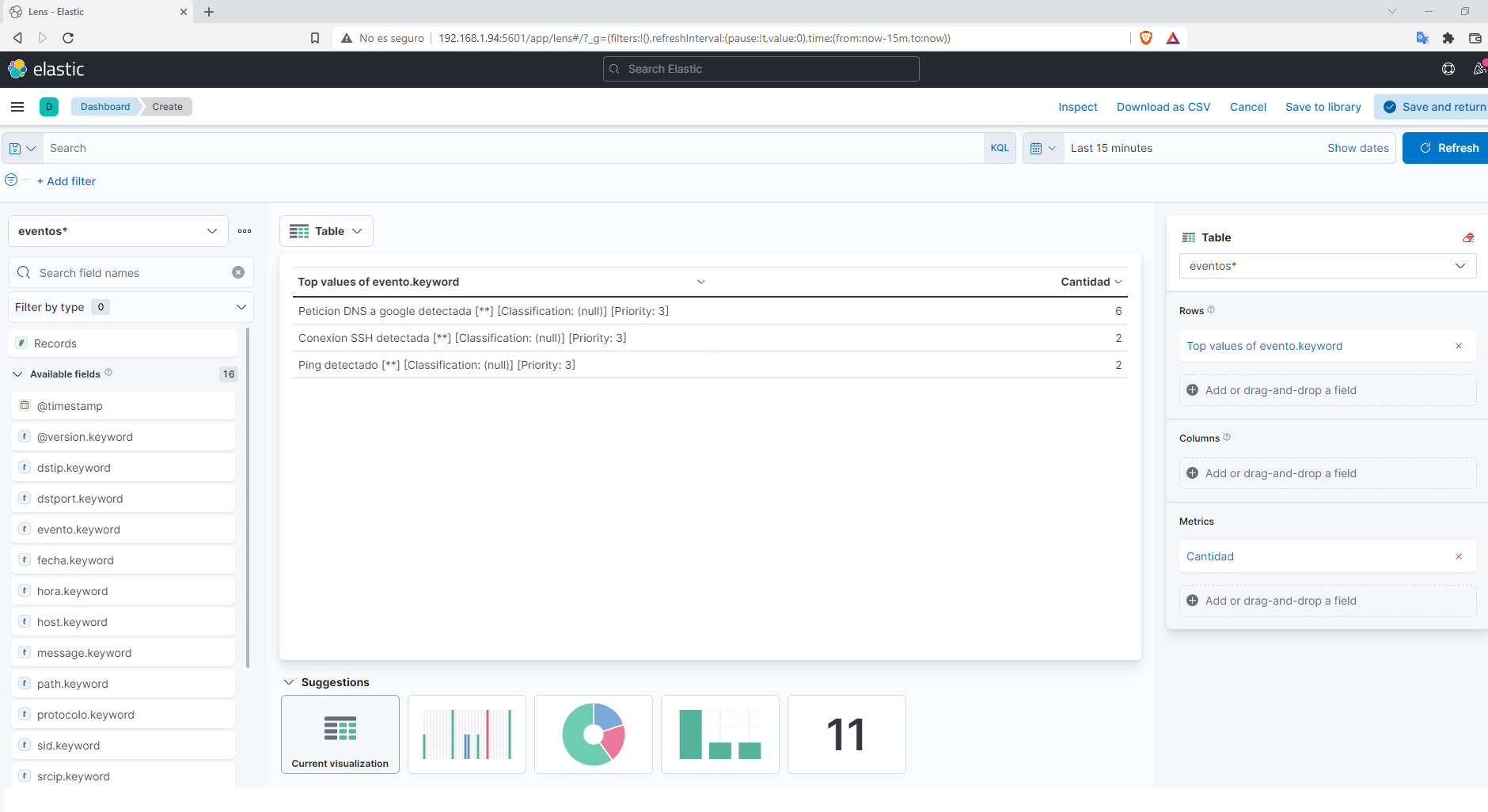




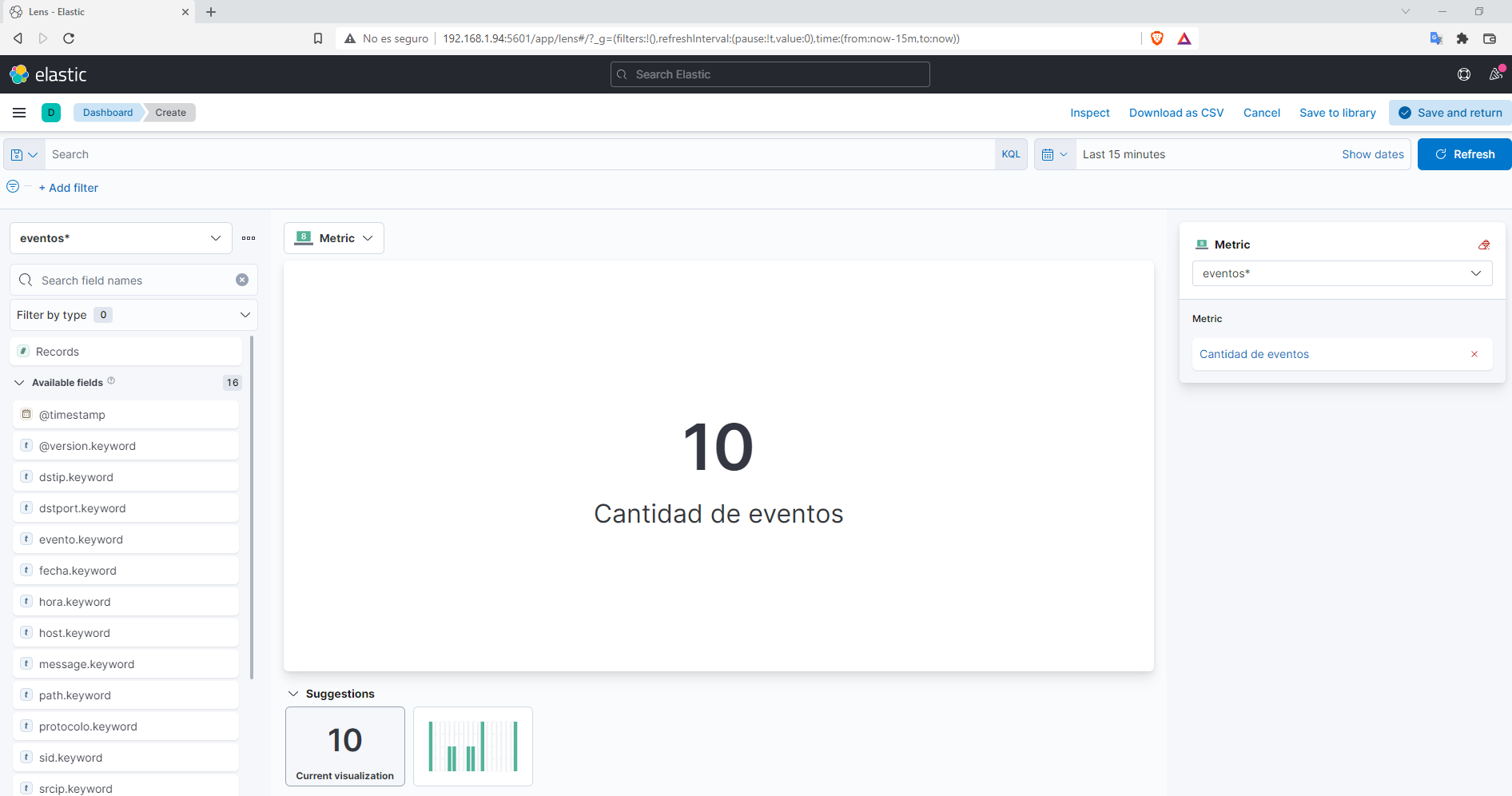
### **4.2 Gráfica de Línea**

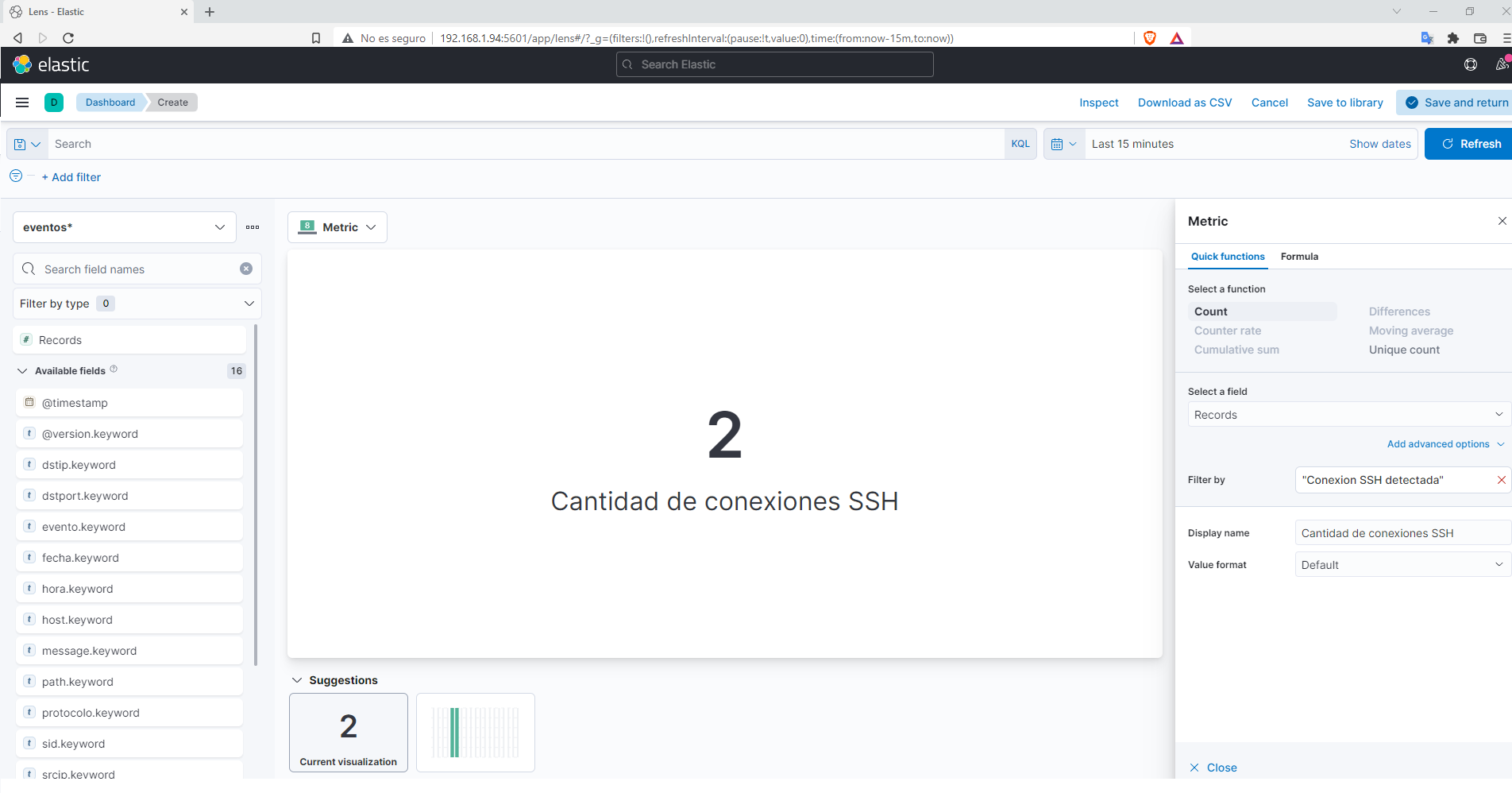


### **4.3 Tabla**

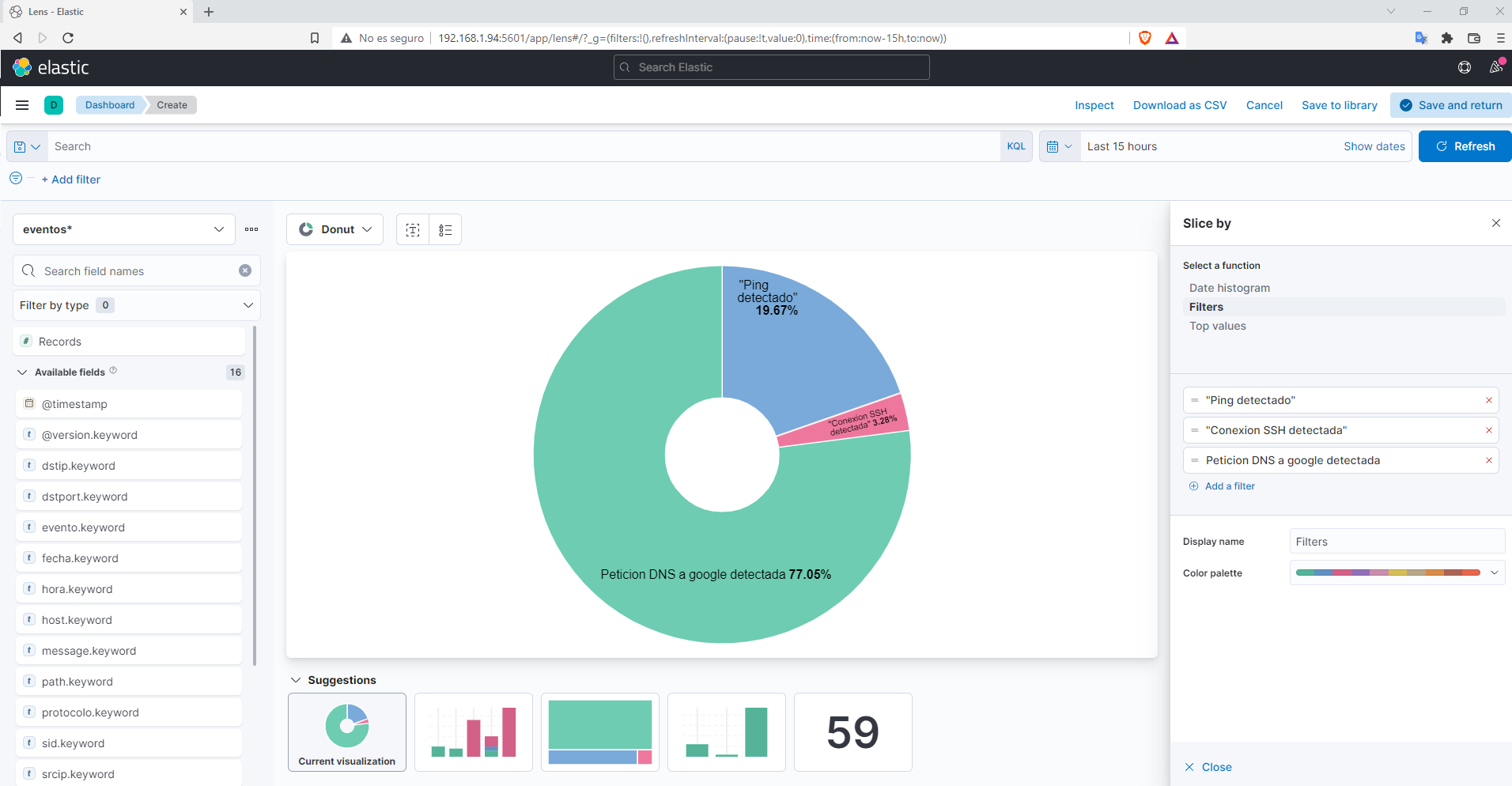


### **4.4 Métrica**





### **4.5 Gráfica de Donut**



### **4.6 Panel**

