Guía de Seguridad de las TIC
CCN-STIC 1241

Procedimiento de Empleo Seguro
BigSIEM



Noviembre 2026

Edita:

CCN
c=ES, l=MADRID, o=CCN,
ou=SELLO ELECTRONICO,
2.5.4.97=VATES-S2800155J,
serialNumber=S2800155J,
cn=CCN
2026.11.04 14:07:00 +01:00

Fecha de Edición: Noviembre de 2026

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

Esta publicación se distribuye bajo licencia CC BY-NC-ND 4.0 que permite compartir el material en cualquier medio o formato con la condición de reconocer adecuadamente la procedencia «Edita: Ministerio de Defensa. Secretaría General Técnica.» No se puede modificar. No se puede utilizar con fines comerciales.

ÍNDICE

1 INTRODUCCIÓN 3
2 OBJETO Y ALCANCE 3
3 ORGANIZACIÓN DEL DOCUMENTO 3
4 FASE PREVIA A LA INSTALACIÓN 4
4.1 ENTREGA SEGURA DEL SERVICIO 4
4.2 ENTORNO DE INSTALACIÓN SEGURO 4
4.3 REGISTRO Y LICENCIAS 4
4.4 CONSIDERACIONES PREVIAS 4
5 FASE DE INSTALACIÓN 5
5.1 ALTA DEL SERVICIO EN LA NUBE 5
6 FASE DE CONFIGURACIÓN 6
6.1 AUTENTICACIÓN 6
6.2 ADMINISTRACIÓN DEL SERVICIO 6
6.3 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS 6
6.4 ACTUALIZACIONES 6
7 FASE DE OPERACIÓN 7
8 REFERENCIAS 10
9 ABREVIATURAS 11

ILUSTRACIONES

Ilustración 1: Gráficas del Dashboard. 7
Ilustración 2: Gráficas del dashboard. 8

1 INTRODUCCIÓN

BigSIEM, del fabricante Secure&IT, consiste en un sistema de gestión y correlación de eventos de seguridad (SIEM) con capacidad de respuesta ante amenazas. Los clientes transmiten registros de auditoría de los sistemas, para que el servicio los analice conforme a una serie de reglas preestablecidas.

BigSIEM consulta periódicamente fuentes de inteligencia de amenazas y mantiene un registro actualizado de indicadores de compromiso, de manera que es capaz de detectar las últimas amenazas identificadas. Cuando se identifica una amenaza, se genera una alerta que se envía por correo electrónico al cliente que ha sufrido o está sufriendo el incidente de seguridad. Adicionalmente, cuenta con un conjunto de scripts que permiten administrar remotamente dispositivos del cliente para tomar acciones preventivas (por ejemplo, añadir una regla a un firewall para bloquear una dirección IP maliciosa).

BigSIEM incorpora una consola de administración que permite que sus administradores realicen consultas, configuren reglas para la generación de alertas o configuren la gestión de dispositivos, entre otras tareas administrativas. El acceso a dichas tareas está segregado por roles.

El servicio se encuentra desplegado en un datacenter, junto con componentes auxiliares que le permiten realizar sus funciones de seguridad.

Estos componentes se comunican entre sí mediante canales protegidos por TLS.

Cada uno de estos componentes lógicos se ejecuta en una o varias máquinas virtuales Linux, accesibles para los usuarios autorizados mediante SSH desde una VPN.

2 OBJETO Y ALCANCE

El objeto del presente documento es servir como guía para realizar una administración y operación de seguridad del servicio **BigSIEM**.

El producto BigSIEM ha sido incluido en el catálogo CPSTIC, para conocer el listado, la categoría o nivel y la familia consulte el sitio web del CPSTIC [CPSITC].

3 ORGANIZACIÓN DEL DOCUMENTO

a. Apartado 4. En este apartado se recogen aspectos y recomendaciones a considerar, antes de proceder a la instalación del servicio.

b. Apartado 5. En este apartado se recogen las recomendaciones a tener en cuenta durante la fase de instalación del servicio.

c. Apartado 6. En este apartado se recogen las recomendaciones para tener en cuenta durante la fase de configuración del servicio, para lograr una configuración segura.

d. Apartado 7. En este apartado se recogen las tareas recomendadas para la fase de operación o mantenimiento del servicio.

4 FASE PREVIA A LA INSTALACIÓN

4.1 ENTREGA SEGURA DEL SERVICIO

Dado que **BigSIEM** se trata de un servicio SaaS, Secure&IT gestiona el alta de los clientes a partir de los datos proporcionados por estos últimos.

El acceso al servicio será realizado utilizando las credenciales de alta remitidas por Secure&IT vía correo electrónico, desde el dominio @secureit.es, a través de un enlace de un solo uso.

En ese mismo mail se indica que deben cambiar esa contraseña para que solo el cliente la conozca.

4.2 ENTORNO DE INSTALACIÓN SEGURO

Secure&IT ofrece la plataforma de monitorización de eventos y alertas **BigSIEM** en formato SaaS, por lo que el entorno de despliegue es responsabilidad del proveedor de la infraestructura.

4.3 REGISTRO Y LICENCIAS

Las licencias son gestionadas directamente por Secure&IT, siendo una gestión totalmente transparente para los clientes.

4.4 CONSIDERACIONES PREVIAS

Durante la configuración, en el momento en el que se accede al servicio y, dependiendo del cliente, será necesario aplicar una configuración u otra. Por ello, es recomendable disponer de la máxima información posible sobre la infraestructura que se va a integrar, en concreto:

- VLANs que se vayan a monitorizar por la sonda. Por cada VLAN, es necesario conocer su ID, el rango de IPs y su utilidad (servidores, almacenamiento, backups, usuarios, DMZ, pública, etc).
- Identificar los direccionamientos de los principales elementos de la infraestructura.
- Adicionalmente, es muy recomendable incluir un esquema de red para poder visualizar todos los elementos, como stacks de switches, y qué redes cuelgan de cada uno de ellos.

Una vez obtengamos estos datos, el equipo de análisis del SOC evaluara las alertas que se produzcan, para intentar identificar posibles falsos positivos que se puedan generar y gestionara con los clientes reuniones periódicas de análisis para su filtrado.

5 FASE DE INSTALACIÓN

5.1 ALTA DEL SERVICIO EN LA NUBE

El servicio BigSIEM se presenta en la modalidad SaaS, siendo necesaria la instalación de las sondas en el cliente. Para la realización de dicha instalación el cliente recibe el soporte del equipo de Secure&IT.

6 FASE DE CONFIGURACIÓN

6.1 AUTENTICACIÓN

El proceso de autenticación de usuarios en la plataforma, accesible desde [CONSOLA], se realiza mediante doble factor de autenticación (2FA), requiriendo las credenciales (usuario y contraseña) que previamente habrán sido dadas de alta en la propia plataforma por personal de Secure&IT, y posteriormente la introducción de un código de un solo uso (OTP).

6.2 ADMINISTRACIÓN DEL SERVICIO

La administración del servicio, como inicio de sesión, política de contraseñas, banner, etc., es realizada de forma completa por Secure&IT y de acuerdo con la normativa del ENS.

6.3 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

Los clientes deben acordar con Secure&IT la protección a aplicar en el canal para el envío de los logs, restringiendo Secure&IT que dichos parámetros cumplan con el ENS

El acceso a KIBANA se realiza mediante el uso de HTTPS sobre TLS 1.3.

6.4 ACTUALIZACIONES

Al tratarse de un SIEM ofrecido en la modalidad SaaS, mantenido con recursos gestionados y proporcionados por Secure&IT, por lo que la gestión de actualizaciones es realizada por parte de Secure&IT, sin requerir acciones por parte del usuario.

7 FASE DE OPERACIÓN

El acceso al servicio se realiza desde [CONSOLA], donde nos deberemos identificar con nuestro usuario y contraseña facilitada durante el proceso de alta, y con OTP para completar el 2FA.

Los elementos más destacables son:

- BSC: Alertas recibidas en el SIEM BigSiemControl.
- BigProbe: Alertas recogidas por la sonda BigProbe ubicada en el cliente.
- Alertas: Evento o conjunto de eventos que cumplen unas condiciones previamente definidas y según su severidad pueden llegar a comprometer la seguridad de la organización.
- Eventos: cada línea de log recibida en el SIEM y que es generada por algún dispositivo.
- Dashboard: tablero de vigilancia, compuesto por paneles, que muestra el estado de la seguridad de la organización.
- Panel: cada una de las visualizaciones (ventanas) que conforman el dashboard.
- Cuadro de mandos: En la parte superior derecha del Dashboard se encuentra el cuadro de mandos. Desde el mismo se puede seleccionar el periodo a visualizar en los paneles inferiores.
  - Full screen: Permite ver el Dashboard en modo pantalla completa.
  - *Time range:* Permite elegir el periodo de tiempo en el que se muestran resultados, haciendo clic en el icono del calendario, podemos seleccionar el periodo. Incluye además una opción para que se actualicen automáticamente los datos en el tiempo indicado.
  - *Refresh:* Permite actualizar manualmente los datos que muestra el Dashboard.

En el Dashboard se aprecian paneles que muestran el estado de la seguridad de la organización. Unos muestran las alertas generadas por BigSIEM y otros los eventos que se han registrado en el mismo.

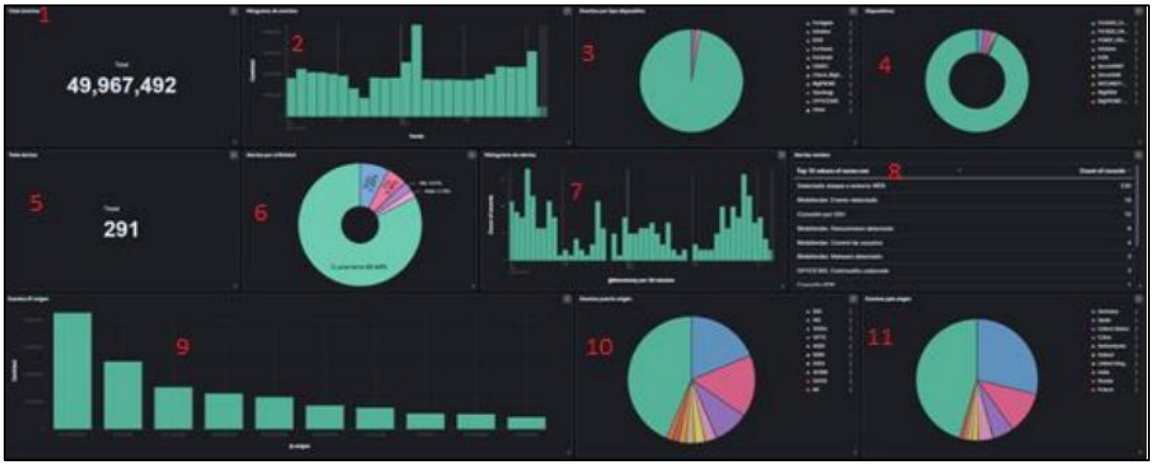


Ilustración 1: Gráficas del Dashboard.



Ilustración 2: Gráficas del dashboard.

A continuación, se muestra una breve descripción de la información identificada en las imágenes anteriores por números:

1. Número de eventos recibidos en el periodo de tiempo seleccionado.
2. Línea temporal en la que se han recibido los eventos en el periodo seleccionado.
3. Clasificación de los eventos recibido por tipo de fuente (dispositivo).
4. Clasificación de los eventos recibidos por dispositivo en el que se ha originado.
5. Número total de alertas generadas por el SIEM en el periodo de tiempo seleccionado.
6. Alertas generadas clasificadas por criticidad.
7. Línea temporal en la que se han generado las alertas.
8. Total de alertas generadas agrupadas por nombre.
9. Top 10 de los eventos recibidos agrupados por IPs origen.
10. Top 10 de los eventos recibidos agrupados por puerto origen.
11. Top 10 países desde los que se origina el tráfico cuando la IP origen es pública.
12. Top 10 de los eventos recibidos agrupados por IPs destino.
13. Top 10 de los eventos recibidos agrupados por puerto destino.
14. Top 10 países hacia los que se dirige el tráfico cuando la IP destino es pública.
15. Eventos recibidos agrupados por módulos de la fuente (tipo dispositivo) origen.
16. Eventos recibidos agrupados por tipo de tráfico.
17. Top 10 de los usuarios que más aparecen en los logs que recibimos.
18. Listado detallado de eventos recibidos.
19. Listado detallado de alertas generadas.

Los filtros de búsqueda aparecen en la parte superior derecha del dashboard y nos permiten obtener con mayor precisión la información a la que se quiere acceder.

Además, se pueden añadir filtros a los campos de dos formas diferentes:

- Desde el propio panel al hacer “click” en cualquiera de los elementos de las gráficas (barras, pie chart, etc.).
- Seleccionando los 3 puntitos que aparecen al lado de cada ítem de la leyenda, aparecerá la opción + y –, para añadir o excluir ese dato en el dashboard.

En la barra de filtrado, al hacer “click” sobre un filtro, hay posibilidad de desactivar, fijar, excluir el valor del filtro, eliminar o editar el propio filtro.

En el extremo superior derecho de cada uno de los paneles hay un botón […] que permite obtener información más detallada de los datos mostrados en el panel, así como exportar la información o ver ese panel en pantalla completa.

Los canales oficiales que nos da Secure&IT para poder comunicar una incidencia, solicitud o ponerte en contacto con el equipo técnico de soporte del SOC, son las siguientes:

- **Llamada telefónica:** al siguiente número de teléfono **911 196 995** y marcando la **opción 1**, se transferirá la llamada al equipo de soporte.
- **Correo electrónico**: enviado a la dirección de correo soporte@secureit.es. Es importante que las cuentas de correo que escriban a esta dirección de correos estén dadas de alta, en caso contrario no se abrirá incidencia en la herramienta.
- **Herramienta de soporte:** se accede a través de la página web [CONSOLA] con un usuario y contraseña previamente generado, junto con un OTP.

8 REFERENCIAS

[CONSOLA] https://accessclient.secureit.es

[CPSITC] https://cpstic.ccn.cni.es/es/catalogo-productos-servicios-stic

9 ABREVIATURAS

BSC	BigSiemControl.
CPD	Centro de Proceso de Datos.
CPSTIC	Catálogo de Productos y Servicios STIC.
ENS	Esquema Nacional de Seguridad.
HTTP	Hypertext Transfer Protocol.
HTTPS	Hypertext Transfer Protocol Secure.
OTP	One Time Password
SaaS	Software as a Service.
SIEM	Gestión de Información y Eventos de Seguridad.
SOC	Centro de operaciones de seguridad.
SSH	Secure Shell.
STIC	Seguridad de las Tecnologías de la Información y la Comunicación.
TLS	Transport Layer Security.
VLAN	Virtual LAN.
VPN	Red virtual privada.