centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1246

Procedimiento de Empleo Seguro
Elastic Platform

Junio 2026

Edita:

CCN
c=ES, l=MADRID, o=CCN,
ou=SELLO ELECTRONICO,
2.5.4.97=VATES-S2800155J,
serialNumber=S2800155J,
cn=CCN
2026.06.11 13:25:06 +02'00'

Centro Criptológico Nacional, 2026

ÍNDICE

1 INTRODUCCIÓN

1. La plataforma Elastic es un gestor de incidentes y amenazas de ciberseguridad, a través de la recolección de eventos en una infraestructura de red y la aplicación posterior de técnicas de correlación y análisis de estos eventos en tiempo real. Esta plataforma se basa en un sistema SIEM (Security Information and Event Management) gracias a las funcionalidades que ofrecen sus diferentes componentes.

1. Este producto actúa como un centro neurálgico de ciberseguridad, integrando información de toda la red para ofrecer una visión completa del estado de la seguridad y apoyar la toma de decisiones en tiempo real. Gracias a la detección temprana de amenazas se consigue una respuesta rápida ante incidentes, evitando así problemas de seguridad de un alto impacto.

2. Los componentes de la plataforma Elastic son los siguientes:

    a) Logstash: Motor de recolección de datos y análisis. Se encarga de unificar y normalizar los eventos recibidos.

    b) Elasticsearch: Base de datos centralizada donde los eventos se almacenan.

    c) Kibana: Servidor web para poder visualizar los eventos recolectados, además de las diferentes alarmas generadas cuando se detecten posibles actividades maliciosas.

    d) Elastic Agent: Agente instalado en los dispositivos monitorizados para la recolección interna de eventos y su posterior envío al motor de análisis.

    e) Fleet Server: Servidor de gestión de los agentes para aplicar diferentes políticas de forma centralizada.

3. Mediante todos sus componentes, Elastic Platform cuenta con las siguientes características principales:

    a) Recolección de datos: Centraliza logs y eventos de múltiples fuentes de la red, analizando los usuarios y dispositivos de toda la infraestructura monitorizada.

    b) Normalización: Convierte los datos en un formato común para su análisis.

    c) Correlación de eventos: Detecta patrones o comportamientos anómalos combinando información de distintas fuentes.

    d) Alertas y notificaciones: Genera avisos automáticos cuando se detectan incidentes potenciales.

    e) Dashboards: Proporciona visualizaciones para monitoreo continuo de la red analizada.

    f) Almacenamiento y auditoría: Guarda los registros históricos para análisis forense, auditorías de seguridad y cumplimiento normativo.

2 OBJETO Y ALCANCE

4. El objeto del presente documento es servir como guía para realizar una instalación, configuración y operación seguras de Elastic Platform en su versión 8.15.2, de forma que la protección y funcionamiento del producto se realice de acuerdo con unas garantías mínimas de seguridad

5. El producto Elastic Platform ha sido incluido en el catálogo de productos y servicios STIC (CPSTIC). Para para conocer el listado, categoría o nivel y familia consulte: https://cpstic.ccn.cni.es/es/catalogo-productos-servicios-stic .

3 ORGANIZACIÓN DEL DOCUMENTO

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

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

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

4 FASE PREVIA A LA INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

6. El método de entrega segura del producto queda en manos del fabricante, el cual es el encargado de ofrecer los paquetes instaladores desde su página web oficial. Dado que la plataforma Elastic se encuentra dividida en diferentes componentes, se deberán de descargar todos y cada uno de ellos. A continuación, se especifica la ruta para cada uno de los componentes del producto:
    a) Elasticsearch: [REF1]
    b) Kibana: [REF2]
    c) Logstash: [REF3]
    d) Elastic Agent y Fleet Server: [REF4]
7. En cada enlace se encontrarán disponibles los paquetes de descarga junto a un fichero llamado “sha”. Este contiene el hash SHA-512 del paquete, por lo que una vez descargado cada paquete se deberá de calcular manualmente el hash del paquete de cada componente, y compararlo con el hash del paquete “sha”.
8. De esta forma se asegura la integridad de los paquetes de instalación de los componentes.

4.2 ENTORNO DE INSTALACIÓN SEGURO

9. Acorde al despliegue cualificado, los componentes Elasticsearch, Logstash y Kibana deberán de ser instalados en un mismo servidor. Este servidor debe ubicarse en un CPD, que cuente con las medidas de seguridad adecuadas a la información que procesa, y que pueda establecer las conexiones necesarias para el desarrollo de su funcionalidad. El acceso debe estar restringido al personal autorizado para su gestión.

4.3 REGISTRO Y LICENCIAS

10. Para poder hacer uso correcto del producto según la evaluación llevada a cabo, se requiere que este sea activado mediante una licencia de tipo “Enterprise”.
11. Por defecto, una vez el producto ha sido instalado este cuenta con una licencia de tipo básico, la cual no tiene fecha de expiración. Para poder instalar una nueva licencia primeramente habrá que contactar al equipo de ventas del fabricante para su obtención. La licencia será provista en un archivo con una fecha de expiración determinada en la compra.
12. Una vez recibido este archivo se deberá de acceder a la sección *Management -> Stack Management -> Stack -> License Management*. Una vez accedido a la pantalla de gestión de las licencias, se podrá comprobar la fecha de expiración de la actual licencia. Para poder cargar el nuevo archivo de licencia se deberá pulsar el botón “*Update license*”.

4.4 CONSIDERACIONES PREVIAS

13. Los componentes de Elastic que forman el motor de recolección, almacenamiento y análisis de los eventos de seguridad deberán de ser instalados sobre un servidor con un Sistema Operativo SUSE Linux Enterprise Server en su versión 15 SP5.
14. Para asegurar un rendimiento óptimo del producto, el fabricante recomienda que este dispositivo cuente con los siguientes requisitos mínimos:
    a) CPU: 8 núcleos
    b) Memoria: 16 GB de RAM
    c) Almacenamiento: 100 GB de espacio en disco
15. Aun así, habrá que tener en cuenta el entorno de despliegue de la plataforma, y adaptar estas características a los requisitos necesarios por el entorno.

4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN

16. Para el correcto funcionamiento del producto, este establece distintas comunicaciones con los siguientes componentes en su entorno de operación, tal y como se muestra en el siguiente diagrama:

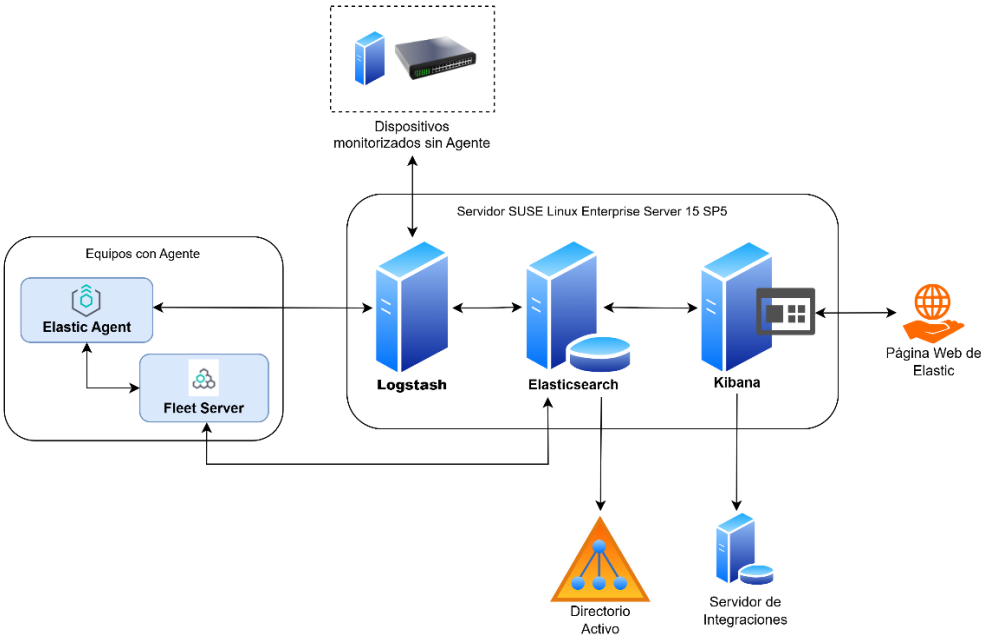

Figura 1: Componentes del entorno operacional

17. A continuación se describe cada uno de los componentes en el entorno:
    a) Dispositivos de Red Monitorizados: Fuente de datos de la propia infraestructura. Este conjunto comprende dispositivos como Cortafuegos o Enrutadores. En este caso, dado que el agente no podrá ser instalado sobre los dispositivos de red, se establecerá un canal de comunicación con ellos para solicitar y recibir los eventos de seguridad en estos.

b) Directorio Activo: Este representa a una entidad proveedora de identidades externa, encargada de la autenticación e identificación de los usuarios.

c) Servidor de Integraciones: Servidor propietario de Elastic el cual ofrece los paquetes de integración para los Elastic Agent mediante una comunicación con el componente Kibana.

d) Página Web de Elastic: Página web propietaria de Elastic, ofrecida en www.elastic.co. Kibana se comunicará con esta página para recibir noticias y mostrarlas en su interfaz web.

5 FASE DE INSTALACIÓN

18. El despliegue cualificado de Elastic debe de realizarse componente a componente, tal y como es entregado por el fabricante según lo especificado en la sección 4.1 de este documento.
19. Por un lado, los componentes Logstash, Kibana y Elasticsearch serán instalados en una misma máquina (ya sea física o virtual) de forma centralizada. Se instalarán sobre una plataforma SUSE Linux Enterprise Server 15 SP5, a la cual se recomienda aplicar la guía CCN-STIC-617.
20. Por otro lado, dada su naturaleza, los componentes Fleet Server y Elastic Agent serán desplegados según sean necesarios, de forma que se gestionen todos los equipos Windows necesarios.
21. A continuación, se especifican las guías de instalación paso a paso para cada componente:
    a) Elasticsearch: [REF5]
    b) Kibana: [REF6]
    c) Logstash: [REF7]
    d) Elastic Agent y Fleet Server: [REF8]
22. Una vez queden instalados todos los paquetes, se deberá de atender a la sección 6.1 de este documento para configurar cada uno de forma segura.

6 FASE DE CONFIGURACIÓN

6.1 MODO DE OPERACIÓN SEGURO

23. Habiendo instalado los paquetes de cada componente en su respectivo dispositivo, estos requieren de una configuración previa de forma que el producto quede instalado y desplegado en su modo de operación seguro. Para ello, a continuación, se describen las configuraciones necesarias para cada componente. Las configuraciones a continuación descritas son las cualificadas, y por tanto las recomendadas de llevar a cabo.

24. Se recomienda consultar [REF13], [REF14], [REF15] y [REF16] para obtener más detalles sobre las configuraciones realizadas en cada componente del producto.

25. **Elasticsearch**: Antes de ejecutar por primera vez este componente, se requieren de las siguientes configuraciones:

    a) Será necesario adaptar el número máximo de archivos que un usuario puede abrir a la vez y permitir al sistema acceder a un mayor número de mapas de memoria. Esto deberá de realizarse en el Sistema Operativo sobre el que se ha instalado el componente. La configuración recomendada se indica a continuación:

```
ulimit -n 65535
sysctl -w vm.max_map_count=262144
```

    b) Habiendo configurado el Sistema Operativo, se deberá de configurar el propio componente editando el archivo *elasticsearch.yml*.

Configuración inicial:

```
node.name: elasticsearch-node-1
network.host: <host_ip_address>
http.port: 9200
cluster.initial_master_nodes:
       - elasticsearch-node-1
```

Configuración de Elastic Security para mejora en la detección de amenazas:

```
xpack.security.enabled: true
```

Activación de las funciones de auditoría:

```
xpack.security.audit.enabled: true
```

Configuración segura de HTTPS:

```
xpack.security.http.ssl:
        enabled: true
        keystore.path: /path/to/http.p12
        supported_protocols: ["TLSv1.2"]
        cipher_suites:
["TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
"TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
"TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256"]
xpack.security.transport.ssl:
        enabled: true
        keystore.path: /path/to/elastic-certificates.p12
        truststore.path: /path/to/elastic-certificates.p12
       cipher_suites:
```

```
["TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
"TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
"TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256"]
```

Desactivación de autenticación local:

```
xpack.security.authc.realms.native.native1:
enabled: false
```

Activación de autenticación mediante Directorio Activo:

```
xpack:
  security:
    authc:
      realms:
        active_directory:
          my_ad:
            order: 0
            domain_name: <ad_domain>
            url: ldaps://<ad_domain>:636
           ssl:
certificate_authorities: [/path/to/ad-win-ca.pem"]
supported_protocols: ["TLSv1.2"]
cipher_suites:                ["TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
"TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
"TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256"]
files:
role_mapping: "role_mapping.yml"
```

c) Para poder mapear los roles a usuarios según el Directorio Activo, se deberá de realizar la siguiente configuración en el archivo *role_mapping.yml*:

```
<role>:
- <user1>
- <user2>
```

d) Para configurar este componente de forma que tan solo ofrezca curvas elípticas seguras se deberá de añadir la siguiente línea de comandos al archivo *config/jvm.options*:

```
-Djdk.tls.namedGroups=secp256r1,secp384r1,secp521r1,X25519
```

e) Antes de hacer uso de los usuarios por defecto *kibana_system*, *elastic* y *logstash_system*, se deberá de resetear sus credenciales mediante el siguiente comando:

```
./bin/elasticsearch-reset-password -u <USER>
```

f) Para proteger las claves privadas correctamente, se deberá de crear un *keystore* y almacenar estas claves privadas en este. Para ello, se deberán de ejecutar los siguientes comandos:

```
./path/to/elasticsearch-keystore                                    add
xpack.security.transport.ssl.keystore.secure_password

./path/to/elasticsearch-keystore                                    add
xpack.security.transport.ssl.truststore.secure_password

./path/to/elasticsearch-keystore                                    add
xpack.security.http.ssl.keystore.secure_password
```

26. **Kibana**: Habiendo configurado Elasticsearch, se requieren de las siguientes configuraciones en este componente:

    a) Se deberá de configurar el propio componente editando el archivo *kibana.yml*:

Configuración inicial:

```
server.host: "kibana-server"
server.port: 5601
server.publicBaseUrl: https://kibana-server
xpack.reporting.enabled: false
xpack.integration_assistant.enabled: false
```

Desactivación de envío de telemetría:

```
telemetry.optIn: false
```

Tiempo de inactividad configurado en 5 minutos:

```
xpack.security.session.idleTimeout: “5m”
```

Activación de las funciones de auditoría:

```
xpack.security.audit.enabled: true
```

Configuración del certificado SSL y la clave de cifrado:

```
elasticsearch.ssl.certificateAuthorities:/path/to/elasticsearch-
ca.pem
xpack.encryptedSavedObjects:
        encryptionKey: "min-32-byte-long-strong-encryption-key"
```

Activación de funcionalidades de Fleet Server:

```
xpack.fleet.agents.enabled: true
```

Reinicio de credenciales por defecto:

```
elasticsearch.username: "kibana_system"
elasticsearch.hosts: ["https://elasticsearch:9200"]
```

Prevención de X-frame:

```
server.securityResponseHeaders.disableEmbedding: true
```

Activación de política de seguridad de contenido:

```
csp.strict: true
```

Configuración de política de registro de auditoría:

```
logging.appenders.default:
        type: rolling-file
        fileName: ./logs/kibana.log
        policy:
                type: size-limit
                size: 100mb
        strategy:
                type: numeric
                max: 10
        layout:
               type: json
```

Configuración de política de rotado:

```
xpack.security.audit.appender:
type: rolling-file
fileName: ./logs/audit.log
policy:
type: size-limit
strategy:
type: numeric
max: 10
layout:
type: json # Formato JSON
xpack.security.audit.appender.policy.size: 100mb
```

b) A pesar de haber configurado anteriormente las suites de cifrado TLS cuando Kibana actúa como servidor, este componente también actúa como cliente en su despliegue, por lo que para configurar una comunicación segura mediante TLS se deberá de lanzar mediante el siguiente comando:

```
NODE_OPTIONS='--tls-min-v1.2   --tls-cipher-list=ECDHE-RSA-AES256-GCM-
SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-CHACHA20-POLY1305'
./bin/kibana
```

c) Para proteger las claves privadas correctamente, se deberá de crear un *keystore* y almacenar estas claves privadas en este. Para ello, se deberán de ejecutar los siguientes comandos:

```
./path/to/kibana-keystore create

./path/to/kibana-keystore add server.ssl.keystore.password

./path/to/kibana-keystore add server.ssl.truststore.password

./path/to/ kibana-keystore add elasticsearch.password
```

Una vez se hayan ejecutado los comando anteriores, se deberá de añadir la siguiente configuración en el archivo *kibana.yml*:

```
server.ssl.keystore.path <path to product .p12 certificate>
server.ssl.truststore.path <path to CA .p12 certificate>
```

27. **Logstash**: Antes de iniciarlo, se requieren de las siguientes configuraciones en este componente:

a) Se deberá de reiniciar las credenciales de los usuarios en el propio componente editando el archivo *logstash.yml*:

```
xpack.monitoring.elasticsearch.username: logstash_system
xpack.monitoring.elasticsearch.password: <new_password>
```

b) Se deberán de actualizar los plugins ejecutando los siguientes comandos:

```
path/to/logstash-plugin remove logstash-output-tcp

path/to/logstash-plugin install --version 7.0.1 logstash-output-tcp

path/to/logstash-plugin remove logstash-integration-kafka
```

```
path/to/logstash-plugin install --version 11.5.2 logstash-integration-
kafka
```

c) Para poder configurar los diferentes puertos en escucha, y para que se establezcan comunicaciones seguras, primeramente se deberá de configurar el archivo *pipelines.yml* como sigue:

```
- pipeline.id: elastic-agent-pipeline
path.config: "/path/to/elastic-agent-pipeline.conf"
```

Seguidamente, se deberá de crear el propio archivo llamado *elastic-agent-pipeline.conf* el cual deberá contener la siguiente información:

```
input {
elastic_agent {
    port => 5044
    ssl_enabled => true
    ssl_supported_protocols => 'TLSv1.2'
                ssl_cipher_suites =>
["TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
"TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
"TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256"]
    ssl_certificate_authorities => "/path/to/ca.crt"
    ssl_certificate => "/path/to/logstash.crt"
    ssl_key => "/path/to/logstash.key"
 ssl_client_authentication => "required"
  }

  snmp {
    hosts => [{host => " udp:<IP Address>/161" version => "3"}]
    security_name => "mySecurityName"
    auth_protocol => "hmac384sha512"
    auth_pass => "AuthPassword"
    priv_protocol => " aes256"
    priv_pass => "PrivPasword"
    security_level => "authPriv"
    get => ["<resource OID>"]
  }
  tcp {
    port => 5000
    type => syslog
    ssl_enabled => true
    ssl_supported_protocols => 'TLSv1.2'
                ssl_cipher_suites =>
['TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384',
'TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256',
'TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256',
'TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256',
'TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384',
'TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256']
    ssl_certificate_authorities => "/path/to/ca.crt"
    ssl_certificate => "/path/to/logstash.crt"
    ssl_key => "/path/to/logstash.key"
  }
}

output {
  elasticsearch {
    hosts => "https://<elasticsearch_host_ip>:9200"
```

```
    data_stream => true
    ssl_enabled => true
    ssl_supported_protocols => 'TLSv1.2'
                ssl_cipher_suites =>
['TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384',
'TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256',
'TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256',
'TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256',
'TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384',
'TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256']
    ssl_certificate_authorities => "/path/to/http_ca.crt"
    ssl_certificate => "/path/to/logstash.crt"
    ssl_key => "/path/to/logstash.key"
 api_key => "<api_key>"
  }
}
```

d) Para configurar este componente de forma que tan solo ofrezca curvas elípticas seguras se deberá de añadir la siguiente línea de comandos al archivo *config/jvm.options*:

```
-Djdk.tls.namedGroups=secp256r1,secp384r1,secp521r1,X25519
```

e) Para proteger los archivos sensibles de Logstash, como lo son el certificado o las claves privadas generados durante el proceso de instalación, o los archivos anteriormente mencionados, se deberá de permitir únicamente permisos de lectura y escritura al usuario root del Sistema Operativo mediante los siguientes comandos:

```
chmod 600 </path/to/logstash.crt>
chmod 600 </path/to/logstash.crt_folder>
chmod 600 </path/to/logstash.key>
chmod 600 </path/to/logstash.key_folder>
chmod 0600 </path/to/logstash.yml>
chmod 0600 </path/to/elastic-agent-pipeline.conf>
```

28. **Elastic Agent y Fleet Server**: Antes de iniciarlos, se requieren de las siguientes configuraciones en este componente:

a) Para sincronizar el Elastic Agent con Kibana, se deberá de crear una política en Kibana aplicada directamente al agente. Para ello, se deberá de seguir la guía de despliegue de Elastic Agent [REF9].

b) Para que el Elastic Agent sea capaz de enviar datos a Logstash, se deberá de configurar SSL/TLS tal y como se indica en la guía de configuración de comunicación segura entre Elastic Agent y Logstash [REF10]

c) Para que Elastic Agent y Fleet Server sean capaces de enviar datos a Logstash y Elasticsearch mediante canales seguros, se deberá de atender a la guía de configuración para estos componentes [REF10]. Específicamente, en el archivo *Advanced YAML configuration* se deberá de indicar la siguiente configuración:

```
ssl.supported_protocols: [TLSv1.2]
ssl.cipher_suites:  [ECDHE-RSA-AES-256-GCM-SHA384,  ECDHE-RSA-AES-128-
GCM-SHA256, ECDHE-RSA-CHACHA20-POLY1205]
```

6.2 AUTENTICACIÓN

29. Para acceder a la gestión del producto, se deberá de acceder a la interfaz gráfica ofrecida por Kibana.
30. Previo al acceso propio a las interfaces de gestión y hacer uso de las funcionalidades de gestión de eventos, el producto delegará las funciones de identificación y autenticación al Directorio Activo previamente configurado, ya que, según la versión cualificada, este será el único método aceptado.
31. Es por ello que Kibana no permitirá realizar ninguna función de administración hasta que el usuario no quede identificado y autenticado ante el AD mediante usuario y contraseña.

6.3 ADMINISTRACIÓN DEL PRODUCTO

6.3.1 ADMINISTRACIÓN REMOTA

32. Tal y como ya se ha indicado anteriormente en este documento, Kibana es el componente encargado de ofrecer la interfaz web, de forma que una vez instalado el producto y configurado en su despliegue seguro será la única forma de administración remota de producto.
33. Para ello, una vez esté listo el componente, su interfaz gráfica se ofrecerá un servicio HTTPS en el puerto 5601 por defecto. Accediendo mediante un navegador web se podrá interactuar con esta interfaz y los administradores se podrán autenticar frente al AD integrado con el producto.

6.3.2 CONFIGURACIÓN DE ADMINISTRADORES

34. Para poder llevar a cabo correctamente la administración del producto, este ofrece los siguientes roles de administración: *superuser, editor, kibana_admin, kibana_user* y *viewer*. Es importante segregar los distintos roles y permisos de acuerdo al ENS.
35. Todos estos usuarios serán gestionados a través del Directorio Activo, por lo que este deberá de ser configurado para que aplique la siguiente política de contraseñas recomendada:
    a) La contraseña debe poder contar con una longitud mínima o igual a 12 caracteres.
    b) La contraseña debe ser capaz de componerse por letras minúsculas, letras mayúsculas, números y caracteres especiales [“!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”].
36. Por parte del propio producto, Kibana a través de su interfaz web será el encargado de establecer un tiempo de inactividad a las sesiones de los administradores. Según la configuración inicial a través del Sistema Operativo, el tiempo de inactividad cualificado se ha establecido en 5 minutos.

6.4 GESTIÓN DE CERTIFICADOS

37. El producto permite la configuración del certificado digital usado por el producto para autenticarse ante los usuarios que acceden por HTTPS y para las comunicaciones

establecidas entre los propios componentes del producto, es decir, integrarse con una PKI de la organización (no deben usarse certificados autofirmados).

38. Para realizar una configuración segura de los certificados, primeramente, será necesario generar un certificado usando RSA con una longitud de clave recomendada igual o superior a 3072 bits. Este certificado deberá ser generado por los administradores del producto de forma externa a este, e importarlos al SO donde el producto está instalado.

39. Habiendo generado el certificado, se deberá de indicar la ruta a este tal y como se ha especificado en la configuración inicial de la sección 6.1 de este documento.

6.5 SERVIDORES DE AUTENTICACIÓN

40. Tal y como se ha comentado anteriormente en este documento, el producto delega sus funciones de identificación y autenticación de usuarios en un Directorio Activo.

41. Para poder configurar este servidor de autenticación, se deberán de seguir los pasos ya descritos en la sección 6.1 de este documento para ello.

6.6 SINCRONIZACIÓN

42. El producto está configurado por defecto para establecer comunicación con el Sistema Operativo sobre el que se instala, y recoger de este las marcas temporales necesarias. Por ello, es crítico que el SO cuente con un NTP integrado o esté configurado para obtener fuentes temporales fiables.

43. Por ello, el producto no ofrece la posibilidad de conectarse a ninguna fuente de sincronización por sí mismo.

6.7 ACTUALIZACIONES

44. Cuando una nueva versión de los componentes de Elastic estén disponibles, será el propio fabricante quien avise a los clientes mediante correo electrónico.

45. Elastic no ofrece un sistema de actualización directo, si no que los administradores de sistemas encargados de gestionar las instancias sobre las que los componentes están desplegados deberán de encargarse de desinstalar cada componente y posteriormente instalarlo en su nueva versión.

46. Por ello, para llevar a cabo satisfactoriamente el proceso de actualización se deberá de seguir los pasos de instalación descritos en la sección 5 de este documento.

6.8 ALTA DISPONIBILIDAD

47. A pesar de que el producto se ha cualificado en formato *standalone*, este ofrece diferentes configuraciones para que pueda ofrecer alta disponibilidad.

48. Primeramente, se recomienda contactar con el fabricante para que le ofrezca la ayuda necesaria en esto. Además, se recomienda atender a la guía de diseño resiliente del fabricante [REF12].

6.9 AUDITORÍA

6.9.1 REGISTRO DE EVENTOS

49. Dada la naturaleza del producto, el cual está encargado de registrar eventos para su posterior análisis por parte de los administradores, el producto generará una gran cantidad de eventos.

50. Por ello, principalmente en este documento se indicarán las funciones de auditoría principales referentes a las funcionalidades de SIEM que ofrece el producto. Estas funciones se indican a continuación:

    a) Inicio y cierre de sesión de los usuarios.

    b) Creación de reglas para detectar alertas

    c) Modificación y actualización de las reglas para detectar alertas previamente creadas

    d) Borrado de reglas para detectar alertas

    e) Filtro aplicado para la visualización de las alertas generadas

    f) Creación de casos

    g) Alertas generadas cuando se cumple una regla definida

51. Todos estos eventos generados en el producto contienen, al menos, la siguiente información de forma que puedan identificarse correctamente:

    a) Fecha y hora del evento.

    b) Tipo de evento identificado.

    c) Resultado del evento.

    d) Usuario que produce el evento (si aplica).

6.9.2 ALMACENAMIENTO LOCAL

52. El producto almacena todos los registros de auditoría generados de forma local. Para poder localizarlos correctamente se deberán de diferenciar, por un lado, los eventos que se generan durante la operación normal del producto, como lo son las alertas generadas cuando se cumple una regla definida, y por otro lado los eventos generados en cambios en la configuración, como la gestión de las reglas que generan alertas.

53. Por ello, el componente Elasticsearch será el encargado de almacenar todas las alarmas generadas, mientras que Kibana será el encargado de almacenar el resto de eventos relativos a cambios en la configuración.

54. Además de ello, Kibana ofrece un método de prevención de pérdida de los eventos, en el que se almacenarán como máximo 10 archivos de logs con un tamaño máximo de 100MB.

7 REFERENCIAS

REF1 Repositorio de paquetes de instalación para Elasticsearch: https://www.elastic.co/downloads/elasticsearch

REF2 Repositorio de paquetes de instalación para Kibana: https://www.elastic.co/downloads/kibana

REF3 Repositorio de paquetes de instalación para Logstash: https://www.elastic.co/downloads/logstash

REF4 Repositorio de paquetes de instalación para Elastic Agent y Fleet Server: https://www.elastic.co/es/downloads/elastic-agent

REF5 Guía de instalación de Elasticsearch, *Install Elasticsearch from archive on Linux or MacOS*: https://www.elastic.co/docs/deploy-manage/deploy/self-managed/install-elasticsearch-from-archive-on-linux-macos

REF6 Guía de instalación de Kibana, *Install Kibana from archive on Linux or macOS*: https://www.elastic.co/docs/deploy-manage/deploy/self-managed/install-kibana-from-archive-on-linux-macos

REF7 Guía de instalación de Logstash, *Installing Logstash from Logstash Reference Guide*: https://www.elastic.co/docs/reference/logstash/installing-logstash

REF8 Guía de instalación de Elastic Agent y Fleet Server, *Install Fleet-managed Elastic Agents*: https://www.elastic.co/docs/reference/logstash/installing-logstash

REF9 Guía de despliegue de Eastic Agent y Fleet Server, *Deploy on-premises and self-managed*: https://www.elastic.co/docs/reference/fleet/add-fleet-server-on-prem

REF10 Guía de comunicación segura entre Logstash y Elastic Agent, *Configure SSL/TLS for the Logstash output*: https://www.elastic.co/guide/en/fleet/8.5/secure-logstash-connections.html

REF11 Guía de configuración de Elastic Agent, Fleet Server, Logstash y Elasticsearch, *Add a Logstash output to Fleet* and *Select the Logstash output in an agent policy*: https://www.elastic.co/guide/en/fleet/8.19/ls-output-settings.html

REF12 Guía de despliegue de Elastic en Alta Disponibildiad, *Design for Resilience*: https://www.elastic.co/docs/deploy-manage/production-guidance/availability-and-resilience

REF13 Elasticsearch Guide: https://www.elastic.co/guide/en/elasticsearch/reference/8.15/index.html

REF14 Kibana Guide: https://www.elastic.co/guide/en/kibana/8.15/index.html

REF15 Logstash Introduction: https://www.elastic.co/guide/en/logstash/8.15/introduction.html

REF16 Fleet and Elastic Agent overview: https://www.elastic.co/guide/en/fleet/8.15/fleet-overview.html

8 ABREVIATURAS

AD	*Active Directory* – Directorio Activo
CCN	Centro Criptológico Nacional
CPD	Centro de Procesamiento de Datos
CPSTIC	Catálogo de Productos STIC
CPU	*Central Processing Unit* – Unidad de Procesamiento Central
ECDHE	Elliptic Curve Diffie Hellman Ephimeral
ENS	Esquema Nacional de Seguridad.
GCM	Galois-Counter Mode
HTTP	Hypertext Transfer Protocol
HTTPS	HTTP over TLS
JSON	JavaScript Object Notation
MB	Mega Bytes
NTP	Network Time Protocol
RAM	*Random Access Memory* – Memoria de Acceso Aleatorio
RSA	Protocolo Rivest, Shamir y Adleman
SHA	*Secure Hash Algorithm* – Algoritmo Seguro de Hash
SO	Sistema operativo
SIEM	*Security Information and Event Management* - Gestión de Eventos e Información de Seguridad.
SSL	Secure Sockets Layer
TLS	Transport Layer Security
YAML	YAML Ain't Markup Language