centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1206

Procedimiento de empleo seguro de *NGSIEM LogICA5*

Enero 2021

MINISTERIO DE DEFENSA

Edita:

MINISTERIO DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

CCN centro criptológico nacional

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2021.01.25 19:53:15 +01'00'

© Centro Criptológico Nacional, 2021
NIPO: 083-20-187-4

Fecha de Edición: enero de 2021
ICA Sistemas y Seguridad ha participado en la elaboración de este documento.

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.

ÍNDICE

1. INTRODUCCIÓN 4
2. OBJETO Y ALCANCE 6
3. ORGANIZACIÓN DEL DOCUMENTO 7
4. RESUMEN DE LOS MÓDULOS O SUBSISTEMAS DEL PRODUCTO 8
5. FASE DE DESPLIEGUE E INSTALACIÓN 10
5.1 ENTREGA SEGURA DEL PRODUCTO 10
5.1.1 TRANSPORTE 10
5.1.2 RECEPCIÓN 10
5.1.3 COMPROBACION DE LA VERSIÓN 11
5.1.4 PRUEBAS DE ACEPTACION 11
5.2 ENTORNO DE INSTALACIÓN SEGURO 11
5.3 REGISTRO Y LICENCIAS 11
5.4 TIPOS DE DESPLIEGUE 12
5.5 CRIPTOGRAFÍA UTILIZADA 13
5.6 INSTALACIÓN 13
5.6.1 INSTALACIÓN DEL ENTORNO OPERACIONAL 13
5.6.2 INSTALACIÓN DEL ENTORNO DE APLICACIÓN 16
5.6.3 INSTALACION DEL ENTORNO DE INTEGRACION Y COMPONENTES ADICIONALES 17
6. FASE DE CONFIGURACIÓN 18
6.1 MODO DE OPERACIÓN SEGURO 18
6.2 ENTORNO DE TRABAJO 18
6.2.1 ENTORNO OPERACIONAL 18
6.2.2 ENTORNO DE APLICACIÓN 31
6.2.3 ENTORNO DE INTEGRACIÓN 39
6.3 AUTENTICACIÓN 39
6.3.1 INTERFACES DE CONEXIÓN 41
6.4 ADMINISTRACIÓN DEL PRODUCTO 42
6.4.1 ADMINISTRACIÓN LOCAL Y REMOTA 42
6.4.2 CONFIGURACIÓN DE USUARIOS 42
6.4.3 ROLES Y PERMISOS DE ACCESOS SISTEMA OPERATIVO 42
6.4.4 ROLES Y PERMISOS DE ACCESO AL BUS 43
6.4.5 ROLES, PERMISOS Y POLITICAS DE ACCESOS *FRONTEND* 43
6.5 CONFIGURACIÓN DE PROTOCOLOS SEGUROS 44
6.6 GESTIÓN DE CERTIFICADOS 48
6.7 SERVIDORES DE AUTENTICACIÓN 49
6.8 SINCRONIZACIÓN HORARIA 50
6.9 ACTUALIZACIONES 50
6.10 AUTO-CHEQUEOS 51
6.11 AUDITORÍA 52
6.11.1 REGISTRO DE EVENTOS 52
6.12 BACKUP 53

7. FASE DE OPERACIÓN 56
7.1 MANTENIMIENTO 56
8. REFERENCIAS 58
9. ABREVIATURAS 59

1. INTRODUCCIÓN

1. **NGSIEM LogICA5** es una solución NGSIEM (gestión de eventos de seguridad e información de seguridad de nueva generación) modular que recolecta y almacena, de forma centralizada en dispositivos de alto rendimiento, líneas de logs de sistemas cedentes. Desplegable en formato appliance o formato de plataforma virtualizada, incorpora capacidad para recolectar datos de cualquier fuente cedente, correlar datos, monitorizar en tiempo real y realizar consultas avanzadas, para desarrollar analítica con objetivos de seguridad. Integra:
    - Recopilación de datos de seguridad para el cómputo de variables técnicas.
    - Inventario de activos orientado a repositorio de configuraciones CMDB (Configuration Management DataBase).
    - Mantenimiento de CMDB de activos en estructura e instancias de la propia herramienta.
    - Descubrimiento de activos y actualización de información de la CMDB.
    - Capacidades de gestión de líneas de logs con fines de auditoría forense, así como la recolección, indexación y control de la información de los dispositivos en un sistema jerárquico forense.
    - Detección y tratamiento de eventos de seguridad en tiempo real a través de la capa de agentes que se reciben por el motor de recolección.
    - Correlación centralizada con una amplia colección de reglas de correlación disponibles.
2. Y las siguientes funcionalidades.
    - Comparativa de vulnerabilidades de activos en base a BD e histórico de resultados obtenidos desde la misma plataforma.
    - Vigilancia de configuraciones de activos. Implementa funcionalidades de detección de cambios en archivos de configuración.
    - Descubrimiento de anomalías y análisis predictivo basado en patrones.
    - Descubrimiento de amenazas y vulnerabilidades sobre activos almacenados en la CMDB de activos.
    - Consulta de BD de vulnerabilidades externas con actualización de información.
    - Motor de informes expositivos y analíticos.
3. A su vez, la plataforma puede ser desplegada en modalidad de servicio, con las funcionalidades expuestas *out of the box*, o en modo *on premise* en un *appliance*.
4. Permite la integración con otras soluciones para:
    - Almacenamiento externo de incidentes.

- Centralización de usuarios de frontend por LDAP.
- Enriquecimiento de la información de seguridad mediante *feeds*.
- Consulta de *hashes*, listas de reputación, análisis de vulnerabilidades y otra información relacionada con la seguridad informática.
- Labores de threat hunting y descubrimiento de IOCs (indicadores de compromiso).
- Análisis UEBA (*User and Entity Behavior Analytics*).
- Motores de análisis predictivo mediante aprendizaje.
- Etc.

2. OBJETO Y ALCANCE

5. El objeto del presente documento es facilitar la instalación y configuración segura de la **solución NGSIEM LogICA 5 7.1**, junto con el aseguramiento del entorno en el que se despliega.
6. NGSIEM LogICA5 es un producto *software* cuya instalación inicial del entorno operacional se efectúa en un appliance compatible.
7. Este producto se sitúa dentro de la familia Sistemas de Gestión de Eventos de Seguridad (SIEM) de la taxonomía definida por el CCN para el Catálogo de Productos de Seguridad TIC (CPSTIC).

3. ORGANIZACIÓN DEL DOCUMENTO

8. Este documento está organizado en diferentes capítulos, de acuerdo a diferentes fases del ciclo de vida del producto:

   a) **Apartado 4**. En este apartado se incluye un esquema con los distintos componentes que forman el producto.

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

   c) **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.

   d) **Apartado 7**. En este apartado se recogen las tareas recomendadas para la fase de operación y mantenimiento del producto.

   e) **Apartado 8.** Incluye un listado de la documentación que ha sido referenciada a lo largo del documento.

   f) **Apartado 9.** Incluye el listado de las abreviaturas empleadas a lo largo del documento.

4. RESUMEN DE LOS MÓDULOS O SUBSISTEMAS [1] DEL PRODUCTO

9. En este apartado se enumeran los subsistemas que forman NGSIEM LogICA5, junto con los programas o aplicaciones que se emplean, si corresponde; la arquitectura detallada de NGSIEM LogICA5 puede ser consultada en el apartado correspondiente a la arquitectura en las guías *LogICA5-GuiaOperacion [REF1]*, *LogICA5-GuiaInstalacion [REF2]* y *LogICA5-GuiaUsuario [REF3]*.

- Subsistemas base del entorno operacional.
    - Sistema de almacenamiento.
        - Sistema de almacenamiento primario. Basado en *MongoDB*.
        - Sistema de almacenamiento secundario. Basado en en el sistema de archivos *XFS*.
    - Sistema distribuido de ejecución en tiempo real.
        - Componente de coordinación. Basado en *Apache Zookeeper*.
        - Componente *broker*. Basado en *Apache Kafka*.
        - Componente gestor de procesado. Basado en *Apache Storm*.
- Subsistemas base del entorno de aplicación.
    - Bus de *streaming* y procesado.
        - Componente de entrada. *Endpoints* de *syslog* y *SEPT*.
        - Componentes de recolección y procesamiento. Colectores y procesadores.
    - Servidores de frontend. Servicios REST de acceso para la configuración y gestión de la plataforma.
- Subsistemas base del entorno de integración.
    - Monitor de extracción de datos.
    - Consola.

10. A su vez NGSIEM LogICA5 se extiende funcionalmente mediante el añadido de componentes que contribuyen en modalidad *plug-in* a los diferentes subsistemas o módulos base. Se dispone de *plugins*, clasificados en *core* y *addon*. Los plugins *core* constituyen las funcionalidades principales o troncales NGSIEM de los subsistemas del entorno de aplicación, los plugins *addon* extienden las funcionalidades principales e incorporan funcionalidades complementarias:

- *Plugins core*:
    - Gestión de usuarios y roles

[1] Subsistema o módulo se emplea indistintamente, subsistema es la clasificación en fase de análisis, y módulo es la clasificación en fase de despliegue.

- Gestión de auditoría
- Inventario de activos
- Gestión de incidentes
- Análisis forense
- Análisis en tiempo real y correlación de eventos de seguridad
- Planificación de tareas

- *Plugins add-on*:
  - Gestión y ejecución de informes
  - Análisis de riesgos
  - Análisis de vulnerabilidades
  - Análisis de anomalías y predicción de patrones
  - Integración con otras soluciones
  - Configuración centralizada
  - Vigilancia de configuraciones
  - Integración de *feeds*
  - Análisis de *IOC's* mediante *threat hunting*
  - …

11. La consola, el monitor de extracción de datos y los plugins *add-on* no se encuentran dentro de la configuración evaluada y certificada *Common Criteria* y, por tanto, se encuentran fuera del alcance de este documento. Si se requiere más información sobre estos subsistemas y componentes, puede ser consultados en:
    - *LogICA5-GuiaOperación [REF 1].*
    - *LogICA5-GuiaInstalación [REF 2].*
    - *LogICA5-GuiaUsuario [REF 3].*
    - *LogICA5-GuiaUsuarioMonitor [REF 4].*

5. FASE DE DESPLIEGUE E INSTALACIÓN

5.1 ENTREGA SEGURA DEL PRODUCTO

12. La plataforma NGSIEM LogICA5 es comercializada por venta directa a clientes finales, de servicios gestionados o de implantación directa *appliance on premise*.

5.1.1 TRANSPORTE

13. NGSIEM LogICA5 y su extensión en funcionalidad se distribuyen como un archivo instalador desde un servidor de descarga *online*, cifrado y autenticado, cuyo enlace se notifica a una dirección de correo electrónico que facilita el acceso a los entregables.
14. El *appliance* de instalación de la plataforma con el entorno operacional instalado se proporciona, a través de transportistas especializados, embalado en cajas o contenedores cerrados junto con albarán de entrega.

5.1.2 RECEPCIÓN

15. Los elementos *software* de NGSIEM LogICA5 se cifran con la clave pública del destinatario. Esta clave se facilita al fabricante mediante correo electrónico u otro medio digital.
16. El destinatario, tras descifrar los elementos con su clave privada, debe verificar la firma acompañante a cada elemento con la clave pública del emisor. Esta clave se facilita al destinatario mediante un servidor de descarga *online* junto al resto de la entrega como se detalla en el apartado 4.1 de la guía *LogICA5-Distribucion [REF6]*. Esta verificación permite garantizar la integridad. Por cada elemento de la entrega se debe realizar la siguiente verificación de integridad:

    ```
    gpg --verify <nombre_fichero>.sig <nombre_fichero>
    ```

17. Junto al producto se hace entrega de documentación, que se suministra en formato electrónico firmada electrónicamente. Para acceder a la verificación de integridad se debe comprobar la validez de la integridad del fichero a través de herramientas de lectura (ofimáticos y PDF) de los formatos suministrados.
18. La recepción de los entregables electrónicos, una vez realizada la descarga de los componentes y completado el documento de recepción *LogICA5-Recepcion [REF5]*, requiere de la confirmación de recepción mediante correo electrónico, adjuntando el mencionado documento firmado electrónicamente o digitalmente escaneado.
19. El *appliance* se suministra con etiqueta de detección de apertura física. Para realizar la verificación de integridad del mismo se debe realizar lo siguiente:
    - Verificar la integridad de la etiqueta.
    - Verificar que la numeración de la etiqueta se corresponde con los datos suministrados junto a la documentación del producto.

20. La recepción del *appliance* se confirma mediante la firma, por parte del receptor de la plataforma, de un albarán de entrega en el momento de su recepción, que será entregado al transportista autorizado que realiza el suministro. En el albarán se recogen los códigos de plataforma suministrados, la orden de pedido emitida por el cliente y la referencia del proyecto asignada.

5.1.3 COMPROBACION DE LA VERSIÓN

21. La comprobación de la versión suministrada se efectúa realizando las funciones de integridad SHA-2 (256bits) de los elementos y verificando que coinciden con los que aparecen en el documento denominado *LogICA5-7.1-Resumen [REF7*], que se encuentra firmado electrónicamente por el emisor.

22. Adicionalmente, se puede realizar la verificación de versión del *software* (NGSIEM LogICA5 7.1) ejecutando el siguiente comando:

```
rpm –qpi <nombre-del-paquete>.
```

5.1.4 PRUEBAS DE ACEPTACION

23. Una vez desempaquetado y desplegado NGSIEM LogICA5 de acuerdo a las instrucciones recogidas en la guía *LogICA5-GuiaInstalacion [REF2]*, se efectúa la verificación de las funcionalidades y de configuración de acuerdo con las guías *LogICA5-GuiaOperacion [REF1]* y *LogICA5-GuiaInstalacion [REF2]* y cuyos resultados se recogen en el documento *LogICA5-Recepcion [REF5*], que forma parte de la entrega.

24. Este documento debe ser firmado por el cliente y devuelto a Grupo ICA por medios electrónicos.

5.2 ENTORNO DE INSTALACIÓN SEGURO

25. El entorno físico donde opera NGSIEM LogICA5 debe asegurar que todos los componentes estén protegidos de cualquier ataque físico, por lo que se recomienda instalar el *appliance* en un Centro de Proceso de Datos que cuente con un sistema de control de acceso limitado y restringido al conjunto de personas expresamente autorizadas y protegido contra cualquier amenaza de origen físico, ataque destructivo, incendio, inundación, robo, etc.

5.3 REGISTRO Y LICENCIAS

26. La licencia de uso de NGSIEM LogICA5 está determinado por el contrato de licencia. Dicho contrato se activa mediante la aplicación de un registro que se suministra junto a la adquisición de la licencia. La activación debe efectuarse desde la consola o desde el api REST de NGSIEM LogICA5.

27. El registro establece:

    - La fecha de caducidad de la licencia.

- El número máximo de fuentes a almacenar – líneas de log.
- El número máximo de fuentes a analizar – eventos de seguridad.
- El *hardware* de ejecución.

5.4 TIPOS DE DESPLIEGUE

28. El despliegue evaluado y certificado Common Criteria, objeto de esta guía, es un **despliegue *stand-alone* en un *appliance* compatible**, en el cual se instalan todos los módulos en un único nodo. NGSIEM LOGICA5 dispone de otros tipos de despliegue fuera del ámbito de esta guía, que se documentarán brevemente a continuación. Si se requiere más información sobre estos otros tipos de despliegue se puede obtener en las guías *LogICA5-GuiaOperacion [REF1] y LogICA5-GuiaInstalacion [REF2*].

29. Otras opciones de despliegue en caso de contar con más de un nodo o appliance son:

    - Despliegue transversal: Todos los nodos deben ser iguales de modo que cada nodo debe tener desplegado todos los subsistemas del entorno operacional y de aplicación, formando un cluster. En caso de necesidad de escalado, se encuentran las siguientes opciones:
        - Horizontal: se añaden más nodos al cluster.
        - Vertical distribuido: se incrementan los recursos *hardware* de forma homogénea en todos los nodos.
    - Despliegue dedicado: Se dedican nodos exclusivos al despliegue de los diferentes subsistemas del entorno operacional y de aplicación, formando un cluster. A los nodos que despliegan el susbsistema de almacenamiento se les denomina *backend*, y a los que despliegan el resto de subsistemas *frontend*. En caso de necesidad de escalado, éste se puede realizar de las siguientes formas:
        - Horizontal: se añaden nodos de backend o frontend, dependiendo de los requerimientos de escalado, tanto para el subsistema de almacenamiento o resto de subsistemas.
        - Vertical distribuido: se añaden más recursos *hardware* a los nodos que lo necesiten[2] de forma heterogénea.

30. Para ambos tipos de despligue:

    - En caso de necesidad de **alta disponibilidad** (no disponible en la modalidad de despliegue *stand-alone*), son necesarios componentes adicionales en los

[2] Normalmente los nodos dedicados al Sistema de Almacenamiento y Sistema distribuido de ejecución en tiempo real requieren mayores recursos *hardware* que los nodos dedicados a Servidores de *frontend*.

subsistemas del entorno operacional. Como el uso de un *proxy* de balanceo y el empleo del protocolo *vrrp*.

- Alternativamente, el almacenamiento secundario puede ser desplegado en sistemas de archivos HDFS de *Hadoop*; el envío de líneas de log desde el componente *broker* al sistema de almacenamiento secundario se efectúa mediante *Apache Flume*.

5.5 CRIPTOGRAFÍA UTILIZADA

31. NGSIEM LogICA5 ofrece las siguientes operaciones de criptografía:

    - **Cifrado asimétrico.** RSA de 3072 bits. Cumplimiento con el RFC 8017. *NGSIEM LogICA5* emplea RSA para el intercambio de certificados durante el establecimiento de la sesión TLS 1.2. Los certificados son X.509 RSA 3072, hash de SHA-256.

    - **Cifrado simétrico**. AES de 128/256 bits. Cumplimiento con el RFC 4615. *NGSIEM LogICA5* emplea AES 128/256 para el establecimiento de la sesión TLS 1.2 con clave compartida, y para el cifrado de contraseñas, AES 128, en el archivo de configuración del subsistema de servidores de *frontend* (clave accesible únicamente por los usuarios del sistema operativo). *NGSIEM LogICA5* proporciona métodos de generación y destrucción de claves AES 128/256 soportados por TLS 1.2.

32. Y las siguientes funciones de *hash*:

    - SHA3. Cumplimento con el FIPS 202. Las contraseñas de los usuarios remotos se almacenan aplicando una función resumen de *hash*. Tanto el archivo de usuarios del bus de recepción por protocolo SETP, como el de los usuarios de *frontend*, en el sistema de almacenamiento primario del entorno operacional de *NGSIEM LogICA5*. Además, se emplea para mantener la integridad de las líneas de log en el sistema de almacenamiento.

5.6 INSTALACIÓN

33. Este apartado describe la instalación de los módulos de NGSIEM LogICA5. Se puede consultar la guía *LogICA5-GuiaInstalacion [REF2]* proporcionada por el fabricante para conocer el detalle de los comandos de instalación.

5.6.1 INSTALACIÓN DEL ENTORNO OPERACIONAL

34. En este apartado se enumeran los requisitos más importantes de instalación del entorno operacional. Para conocer el detalle especifico de los componentes *software*, versiones específicas y cómo realizar la instalación de todo el entorno, consultar el documento *LogICA5-GuiaInstalacion [REF2]*.

35. El entorno operacional está formado por el sistema operativo CentOS y por software complementario perteneciente a los módulos base del entorno operacional que permite el correcto funcionamiento de la plataforma.

36. La instalación, objeto de esta guía, es en un único nodo, *stand-alone*, aunque existen otros modos de despliegue fuera del ámbito de esta guía, como se ha indicado en el apartado 5.4 Tipos de despliegue.

37. Se recomienda consultar el apartado 5.1 de la guía *LogICA5-GuiaInstalacion [***REF2***]* de NGSIEM LogICA5 para conocer el detalle de los comandos y parámetros específicos que se recomienda ejecutar en la instalación del sistema operativo.

38. Descargar e instalar la ISO correspondiente al sistema operativo de CentOS 7.x., en **el modo minimal**, es decir, sin entorno gráfico y con las librerías o paquetes por defecto.

39. Instalar el gestor de base de datos **MongoDB** del almacenamiento primario. Para el detalle completo consultar el apartado *5.4 de la guía LogICA5-GuiaInstalacion [***REF2***]*. A continuación, se indican los puntos más relevantes:

    - Emplear el usuario *root* para realizar las instalaciones.
    - Descargar e instalar la base de datos MongoDB en el único nodo en una instalación *stand-alone*. El procedimiento estándar se puede consultar en el siguiente enlace.

      https://docs.mongodb.com/v3.6/tutorial/install-mongodb-on-red-hat/

40. Instalar la plataforma de ejecución ***nodejs***. Se deben seguir los siguientes pasos:

    - Emplear el usuario *root* para realizar las instalaciones/configuraciones.
    - Descargar e instalar la plataforma de ejecución de nodejs 12.x:

      ```
      curl --silent --location https://rpm.nodesource.com/setup_12.x | bash -
      yum -y install nodejs
      ```

41. Instalar la plataforma de ejecución de ***java***:

    - Emplear el usuario *root* para realizar las instalaciones/configuraciones.
    - Descargar e instalar la plataforma de ejecución de java 1.8.0_161, en el directorio */ica/common* a partir del archivo *jdk-8u161-linux-x64.tar.gz* que puede ser descargado de la página oficial de *java*.

      ```
      mkdir /ica/common
      cd /ica/common
      tar –xzvf <ruta de descarga>/jdk-8u161-linux-x64.tar.gz
      ```

42. Instalar ***Apache Zookeeper***. Para consultar el detalle completo consultar el apartado 5.7 de la guía *LogICA5-GuiaInstalacion [***REF2***]*. A continuación, se indican los puntos más relevantes:

    - Emplear el usuario *root* para realizar las instalaciones.

- Descargar e instalar el manejador de cluster *Apache Zookeeper* en el directorio */ica/common* a partir del archivo *zookeeper-3.4.12.tar.gz* que puede ser descargado de la página oficial de *apache zookeeper*.

```
cd /ica/common
tar –xzvf <ruta de descarga>/zookeeper-3.4.12.tar.gz
```

43. Instalar el ***broker Kafka***. Para ver el detalle completo de esta instalación, se puede consultar el apartado 5.8 de la guía *LogICA5-GuiaInstalacion [***REF2***]*. A continuación, se indican los puntos más relevantes:

    - Emplear el usuario *root* para realizar las instalaciones.
    - Descargar e instalar el *broker Apache Kafka* en el directorio */ica/common* a partir del archivo *kafka_2.12-1.0.0.tgz* que puede ser descargado de la página oficial de apache kafka.

```
cd /ica/common
tar –xzvf <ruta de descarga>/kafka_2.12-1.0.0.tgz
```

44. Instalar la base de datos de *Redis*:

    - Emplear el usuario *root* para realizar las instalaciones.
    - Instalar la base de datos de Redis, empleando el administrador de paquetes de *software yum* de CentOS7.

```
yum install epel-release
yum update
yum install redis.x86_64 0:3.2.12-2.el7
```

45. Instalar la plataforma distribuida ***Apache Storm***. Para obtener el detalle completo, se puede consultar el apartado 5.10 de la guía *LogICA5-GuiaInstalacion [***REF2***]*. A continuación, se indican los puntos más relevantes:

    - Emplear el usuario *root* para realizar las instalaciones.
    - Descargar e instalar la plataforma distribuida *Apache Storm* en el directorio */ica/common* a partir del archivo *apache-storm-1.0.6.tar.gz* que puede ser descargado de la página oficial de apache storm.

```
cd /ica/common
tar –xzvf <ruta de descarga>/apache-storm-1.0.6.tar.gz
```

46. Instalar el sistema de auditoría **nmap** siguiendo los siguientes pasos:

    - Emplear el usuario *root* para realizar las instalaciones.
    - Instalar *nmap*, empleando el administrador de paquetes de *software yum* de CentOS7.

```
yum install nmap
```

47. Instalar las librerías adicionales requeridas por los diferentes componentes que constituyen el módulo de servidores de *frontend*, principalmente el *plugin* del motor de informes.

- Emplear el usuario *root* para realizar las instalaciones.
- Instalar los siguientes paquetes, empleando el administrador de paquetes de *software yum* de CentOS7.

```
yum install pango
yum install libXcomposite
yum install libXcursor
yum install libXi
yum install libXtst
yum install cups
yum install libXScrnSaver
yum install libXrandr
yum install GConf2
yum install atk
yum install gtk3
yum install pandoc
yum install pandoc-pdf
```

- Instalar las fuentes arial, descargando el paquete directamente mediante *wget*.

```
wget http://www.itzgeek.com/msttcore-fonts-2.0-3.noarch.rpm
rpm -Uvh msttcore-fonts-2.0-3.noarch.rpm
```

48. Ciertos módulos de LogICA4 son requeridos si se emplean los agentes de LogICA4 en la plataforma NGSIEM LogICA5. Estos módulos se encuentran fuera del alcance de este documento. Se puede consultar la guía *LogICA5-GuiaInstalacion [***REF2***]* para más información, los módulos que son requeridos son los siguientes:
    - *LISM* es el gestor de seguridad y licenciamiento de LogICA4. Todos los módulos de LogICA4 requieren su instalación para funcionar correctamente. Independiente del número de nodos destinados a la instalación de la plataforma de *NGSIEM LogICA5*, LISM se instala en un único nodo.
    - *LogAgent4* es el agente recolector de eventos de seguridad a partir de líneas de logs y de líneas de log de los sistemas cedentes en LogICA4. Su instalación es necesaria si se requiere emplear los analizadores de líneas de log disponibles en LogICA4. Se puede instalar *LogAgent4* en la plataforma de NGSIEM *LogICA5* o, local en una máquina de los sistemas cedentes, en la red de producción.

5.6.2 INSTALACIÓN DEL ENTORNO DE APLICACIÓN

49. Este apartado describe la instalación de los módulos de NGSIEM LogICA5 del entorno de aplicación. Se recomienda consultar la guía *LogICA5-GuiaInstalacion [***REF2***].*
50. Los módulos del entorno de aplicación de la plataforma NGSIEM LogICA5 son: el bus de streaming y procesado en tiempo real y, los servidores de *frontend*, con los componentes o *plugins* correspondientes de extensión.

51. Debe emplear el usuario *root* para realizar las instalaciones. Se parte de un entorno operacional ya instalado, o procedente del fabricante.

52. Instalar el rpm *LogICA5-core-1.1.12.-Release.x86_64.rpm* que puede ser obtenido directamente del fabricante, siguiendo el proceso descrito en el documento LogICA5-Distribución [**REF6**]. La instalación se efectúa en el directorio */ica/logica5*.

5.6.3 INSTALACION DEL ENTORNO DE INTEGRACION Y COMPONENTES ADICIONALES

53. Los modulos del entorno de integración, consola y monitor de extracción de datos, al igual que los componentes o *plugins* de extensión tipo *add-on* y, los módulos LISM y LogAgent4 en caso de requerir agentes compatibles con LogICA4, no se encuentran en la configuración evaluada y certificada Common Criteria y, por tanto, se encuentran fuera del alcance de este documento. Si se requiere más información sobre la instalación de estos módulos y componentes, puede ser consultado en la guía *LogICA5-GuiaInstalación [***REF2***]*

6. FASE DE CONFIGURACIÓN

54. El detalle del proceso de configuración de NGSIEM LogICA5, se puede consultar en las guías *LogICA5-GuiaOperación [***REF1***] y LogICA5-GuiaInstalacion [***REF2***]* proporcionadas por el fabricante.

6.1 MODO DE OPERACIÓN SEGURO

55. El modo de operación seguro de NGSIEM LOGICA5 se describe a continuación, detallando las configuraciones seguras necesarias para los difentes subsistemas que componen el producto. Para cada módulo se realiza una breve descripción de sus funcionalidades y arquitectura, centrándose en la seguridad.

6.2 ENTORNO DE TRABAJO

56. Se distinguen tres (3) entornos en los que se clasifican los módulos de NGSIEM LogICA5: el entorno operacional, el entorno de aplicación y el entorno de integración. Por lo que el entorno de trabajo de configuración también se clasifica en estos entornos.

6.2.1 ENTORNO OPERACIONAL

57. Debido a su capacidad de configuración y despliegue, existen varios elementos del entorno operacional que se agrupan como módulos de NGSIEM LogICA5:

- Sistema de Almacenamiento.
- Sistema distribuido de ejecución en tiempo real.

6.2.1.1 SISTEMA OPERATIVO

58. Como paso previo a la configuración de los módulos de NGSIEM LogICA5 del entorno operacional, es necesaria la configuración y bastionado del sistema operativo CentOS7

59. Se recomienda consultar el apartado 5.1 de la guía *LogICA5-GuiaInstalacion* [**REF2***]* de NGSIEM LogICA5 para conocer el detalle de los comandos y parámetros específicos que se recomienda ejecutar en la preparación del sistema operativo. Las principales actividades de preparación del sistema operativo son:

- Emplear el usuario *root* para realizar las configuraciones.
- Revisar los dispositivos de arranque del BIOS y eliminar dispositivos innecesarios como unidades de CDROM o DVD.
- Aplicar la configuración LVM (*Logical Volume Management*): Creación de un volumen físico PV (*Physical Volume*) asociado al dispositivo correspondiente al espacio en disco destinado al sistema operativo.
- Establecer el nombre de máquina: *logica5*

- Eliminar las cuentas de usuario innecesarias: *lp, sync, operator, games, ftp, rpc, rpcuser* y *tss.*
- Deshabilitar los servicios innecesarios: *cups, postfix, rpcbind y ctrl-alt-del.target*
- Crear el grupo para los usuarios de *NGSIEM LogICA5*.
- Crear los usuarios de sistema con grupo primario logica y directorio *home*. Usuarios con contraseña mediante algoritmo SHA512. Para esto, modificar el archivo */etc/login.defs*:

```
# Use SHA512 to encrypt password.
ENCRYPT_METHOD SHA512
```

- Establecer SELINUX en modo *permissive*.
- Realizar la configuración segura de SSH modificando el fichero *sshd_config.* Se puede consultar el punto 15 del apartado 5.1 de la guía *LogICA5-GuiaInstalacion [***REF2***]* de NGSIEM LogICA5 para más información. Se definen:
  - Los algoritmos de clave simétrica (*Ciphers*) y funciones resumen sobre la mac (*MACs*) de la máquina para su autenticación con otras máquinas o servidores.
  - Parámetros de la sesión: tiempo de sesión de 6 minutos (*ClientAliveInterval*), usuarios autorizados para iniciar sesión – ica, logica5 – (*AllowUsers*), no se permite el uso de contraseñas vacías (*PermitEmptyPasswords*), empleo del protocolo 2 de ssh (*Protocol*), número máximo de 4 intentos de autenticación (*MaxAuthTries*), y la prohibición del uso *de X11Forwarding* y de los usarios de root para iniciar sesión (*PermitRootLogin*).

```
UseDNS no
Ciphers aes128-ctr,aes192-ctr,aes256-ctr
MACs hmac-sha1,hmac-ripemd160,hmac-sha2-256,hmac-sha2-512
ClientAliveInterval 360
ClientAliveCountMax 0
PermitEmptyPasswords no
AllowUsers ica logica5
PermitRootLogin no
Protocol 2
X11Forwarding no
IgnoreRhosts yes
MaxAuthTries 4
```

- Aplicar una política de contraseñas resistentes a ataques, incluyendo IPMI (*Intelligent Platform Management Interface*), BIOS y GRUB (*GRand Unified Bootloader*).
- La política de contraseñas debe garantizar que:

- Las contraseñas poseen al menos 12 caracteres e incluyen caracteres especiales, números, masúsculas y minúsculas.
- Se evitan contraseñas poco seguras como palabras comúnmente utilizadas o cadenas de caracteres consecutivos (Ej.: “1234”).
- El periodo de caducidad de contraseñas no debe ser superior a 180 días.
- El número mínimo de intentos fallidos que darían como resultado el bloqueo de la sesión.
- El número mínimo de cambios necesarios para que una contraseña pueda repetirse. Se considera deseable que este no sea inferior a 5.
- El período mínimo durante el cual el administrador no podrá cambiar las contraseñas. Esto impedirá que el administrador la cambie en un breve período de tiempo para volver a su contraseña original. No deberá permitirse la repetición de, al menos, las 5 últimas contraseñas utilizadas.

- Definir la política de contraseñas editando el archivo */etc/login.defs*.:
  - Caducidad de las contraseñas. Se recomienda un valor de 30 días (*PASS_MAX_DAYS*).
  - Mínimo de días permitido para poder cambiar la contraseña (*PASS_MIN_DAYS*). El valor -1 indica que no se establece ningún mínimo.
  - Aviso de expiración de las contraseñas en número de días previos (*PASS_WARN_AGE*).
  - Límite de intentos de acceso al sistema. Se recomienda un valor de 3 (*LOGIN_RETRIES*).
  - Tiempo máximo para realizar el inicio de sesión en segundos (*LOGIN_TIMEOUT*).
  - Longitud mínima de las contraseñas. Se recomienda un valor de 12 caracteres (*PASS_MIN_LEN*).
  - Activación del log de nombres de usuario desconocidos en el sistema (LOG_UNKFAIL_ENAB).
  - Tiempo de latencia entre autencicaciones fallidas en segundos (FAIL_DELAY).
  - Activación del log para autenticaciones fallidas (*FAILLOG_ENAB*)

```
PASS_MAX_DAYS 30
PASS_MIN_DAYS 5
PASS_MIN_LEN  12
PASS_WARN_AGE 7
LOGIN_RETRIES 3
LOGIN_TIMEOUT 5
```

```
LOG_UNKFAIL_ENAB  yes
FAIL_DELAY    10
FAILLOG_ENAB  yes
```

- La aplicación de las políticas, para garantizar las características indicadas, se efectúa a través de los módulos PAM, modificando el fichero */etc/pam.d/password-auth*. Se puede encontrar información adicional en los puntos 21-25 y 27 del apartado 5.1 de la guía *LogICA5-GuiaInstalacion [***REF2***]* de NGSIEM LogICA5.

```
auth       required     pam_env.so
auth       required     pam_tally2.so deny=4 unlock_time=600 quiet #
auth       requisite    pam_faillock.so preauth silent audit deny=3 unlock_time=600
auth       required     pam_faildelay.so delay=2000000
auth       sufficient   pam_unix.so nullok try_first_pass
auth       [default=die] pam_faillock.so authfail audit deny=3 unlock_time=600
auth       requisite    pam_succeed_if.so uid >= 1000 quiet_success
auth       required     pam_deny.so
account    required     pam_faillock.so
account    required     pam_unix.so
account    required     pam_tally2.so #
account    sufficient   pam_localuser.so
account    sufficient   pam_succeed_if.so uid < 1000 quiet
account    required     pam_permit.so
password   requisite    pam_pwquality.so try_first_pass local_users_only retry=3 authtok_type=
password   sufficient   pam_unix.so sha512 shadow nullok try_first_pass use_authtok
password   required     pam_deny.so
session    optional     pam_keyinit.so revoke
session    required     pam_limits.so
-session   optional     pam_systemd.so
session    [success=1 default=ignore] pam_succeed_if.so service in crond quiet use_uid
session    required     pam_unix.so
# Password aging controls:
#
# PASS_MAX_DAYS Maximum number of days a password may be used.
# PASS_MIN_DAYS Minimum number of days allowed between password changes.
# PASS_MIN_LEN Minimum acceptable password length.
# PASS_WARN_AGE Number of days warning given before a password expires.
#
PASS_MAX_DAYS 180
PASS_MIN_DAYS 5
PASS_MIN_LEN  12
PASS_WARN_AGE 15
```

- Eliminar paquetes innecesarios que no pertenezcan a una distribución minimal de CentOS7.
- Realizar la configuración segura del kernel, punto 18 del apartado 5.1 de la guía *LogICA5-GuiaInstalacion [***REF2***]* de NGSIEM LogICA5.

```
#No responder a peticiones ICMP
net.ipv4.icmp_echo_ignore_all = 1
#Ignorar peticiones broadcast
net.ipv4.icmp_echo_ignore_broadcasts = 1
#Deshabilitar el source routing
net.ipv4.conf.all.accept_source_route = 0
#Protegerse antes ataques TCP-SYN
net.ipv4.tcp_syncookies = 1
#Tabla de encaminamiento
net.ipv4.conf.all.accept_redirects = 0
net.ipv4.conf.all.send_redirects = 0
net.ipv4.conf.default.accept_redirects = 0
net.ipv4.conf.default.send_redirects = 0
net.ipv4.ip_forward = 0
#Ignorar mensajes mal formados
net.ipv4.icmp_ignore_bogus_error_responses = 1
net.ipv4.conf.all.rp_filter = 2
net.ipv4.conf.default.rp_filter = 2
#Paquetes anormales o excepcionales
net.ipv4.conf.all.log_martians = 1
net.ipv4.conf.default.log_martians = 1
#Deshabilitar el source routing
net.ipv4.conf.default.accept_source_route = 0
# Proteccion contra IP Spoofing
net.ipv4.conf.all.rp_filter = 1
#Deshabilitar vulnerabilidad de marca de tiempo en TCP
net.ipv4.tcp_timestamps = 0
#Activar la proteccion Defragging
#net.ipv4.always_defrag = 1
net.core.netdev_budget = 600
net.core.rmem_max = 33554432
net.core.wmem_max = 6553600
net.ipv4.tcp_rmem = 8192 873800 8738000
net.ipv4.tcp_wmem = 4096 655360 6553600
net.ipv4.udp_mem = 6861459  9148614 12722918
net.ipv4.udp_rmem_min = 8192
net.ipv4.udp_wmem_min = 8192
net.core.somaxconn = 4096
net.ipv4.tcp_fin_timeout = 30
net.ipv4.tcp_keepalive_intvl = 30
net.ipv4.tcp_keepalive_time = 120
net.ipv4.tcp_max_syn_backlog = 4096
vm.dirty_ratio = 15
vm.dirty_background_ratio = 5
vm.zone_reclaim_mode = 0
vm.swappiness = 1
```

- Bloquear el uso CTRL-ALT-SUPR.
- Realizar la configuración del mensaje de información (*banner*) de acceso al sistema, mediante la edición del archivo */etc/motd*.
- Realizar la configuración de módulos PAM de autenticación *password-auth, system-auth* y *other.*

- Establecer la política de limitación del acceso al comando *su*.
- Realizar la configuración de arranque del sistema.
- Instalar el servicio NTP, zona horaria de la región y configuración segura del servicio. Ver apartado 6.8
- Realizar el ajuste de permisos y variables de entorno.
- Establecer la configuración de propiedad y permisos de los directorios de usuarios*:*

```
Permisos 740 directorios: /home/
Permisos 644 archivos: /etc/passwd /etc/group
Permisos especiales: chmod +t /tmp
```

- Definir el control de integridad con AIDE.
- Realizar la actualización de los paquetes instalados del sistema.
- Realizar la configuración de las interfaces de red, el detalle de los comandos y parámetros específicos se encuentran documentados en el punto 32 del apartado 5.1 de la guía LogICA5-GuiaInstalacion [**REF2***]* de NGSIEM LogICA5. Se emplea dos interfaces de red, aparte de la destinada a IPMI:
  - **Red de Gestión** para el acceso a los servicios REST del módulo de servidores de frontend, o al servicio SSH.
  - **Red de Producción** para la recepción del envío desde los sistemas cedentes: líneas de log y eventos.
- Establecer los ficheros de configuración para cada interfaz:

  /etc/sysconfig/network-scripts/ifcfg-ensXXX

```
TYPE=Ethernet
BOOTPROTO=none
IPV4_FAILURE_FATAL=yes
IPV6INIT=no
IPV6_AUTOCONF=no
IPV6_DEFROUTE=no
IPV6_FAILURE_FATAL=no
NAME=ensXXX
UUID=<UID>
DEVICE=ensXXX
ONBOOT=yes
IPADDR=<IP-DEVICE>;
PREFIX=24
GATEWAY=<IP-GATEWAY>;
```

- Configurar el DNS. Fichero: */etc/resolv.conf*

```
nameserver x.x.x.x
search localdomain
```

- Deshabilitar IPv6 y el soporte para RPC. Fichero: */etc/sysconfig/network*

```
NETWORKING_IPV6=no
IPV6INIT=no
```

- Realizar la configuración del *firewall*. El detalle de los comandos y parámetros específicos se encuentran documentados en el punto 33 del apartado 5.1 de la guía *LogICA5-GuiaInstalacion [***REF2***]* de NGSIEM LogICA5. El resto de reglas de firewall específicos para los modulos de NGSIEM LogICA5 se pueden consultar en el apartado 6.3.1
  - Puertos abiertos en la red de gestión:
    - Puerto 22, servicio SSH.
  - Tráfico saliente red de producción y gestión:
    - Se habilita todo el tráfico saliente. Servicio DNS, SMTP y NTP.

6.2.1.2 SISTEMA DE ALMACENAMIENTO

60. Este sistema es el módulo encargado del almacenamiento de los log y eventos de seguridad provenientes de los dispositivos cedentes pertenecientes a la organización y la información propia de la plataforma NGSIEM LogICA5. Se dispone de dos (2) tipos de almacenamiento (primario y secundario), con diferente ventana de retención para líneas de log y eventos de seguridad, dependiendo de los requerimientos de la instalación.
61. El sistema de almacenamiento primario está basado en un gestor de base de datos distribuido *nosql*. MongoDB.
62. Se cuenta con dos (2) bases de datos, además de las del propio sistema para:
    - el almacenamiento de colecciones de líneas de log y eventos de seguridad.
    - el almacenamiento de colecciones funcionales de la plataforma *NGSIEM LogICA5*.
63. Las colecciones son creadas por los *plugins* de análisis de eventos de seguridad y logs respectivamente. Los datos se almacenan de forma periódica, existiendo una colección por periodo, por defecto diariamente, tanto para líneas de log como para eventos. Cada línea de log se acompaña por una firma basada en hash SHA3, no configurable, calculada a partir del contenido de la línea y la firma de la línea anterior, de forma encadenada. Esta firma permite el no repudio de la información de logs.
64. La comunicación con el gestor de base de datos se efectúa sobre el protocolo TCP. Se debe habilitar la autenticación mediante usuario y contraseña, y el cifrado del canal de comunicación mediante TLS 1.2 con certificados X.509. La securización del canal se detalla en el apartado 6.5 CONFIGURACIÓN DE PROTOCOLOS SEGUROS.
65. Los sistemas de almacenamiento primario y secundario disponen de ventanas de retención para el almacenamiento de los registros de auditoría asociados a las

líneas de log y eventos de seguridad (SIEM data) procedentes de los sistemas cedentes. Se recomienda establecer un periodo de retención de al menos tres meses para el almacenamiento primario y un periodo de retecion de al menos un año para el almacenamiento secundario. Las ventanas de retención se ajustan mediante tareas planificadas por defecto, como se detalla en la guía *LogICA5-GuiaUsuario [REF3],* que se configuran teniendo en cuenta el espacio reservado disponible para el almacenamiento primario y secundario.

66. Para calcular el espacio de almacenamiento primario y secundario, se debe conocer el volumen de datos procedente de los sistemas cedentes que se integran en NGSIEM LogICA5. Es recomendable una distribución del almacenamiento disponible en una proporción 80-20 respectivamente.

67. **Se deben hacer copias de seguridad de los registros de auditoría** (apartado 6.12 BACKUP) antes de superar la ventana de retención en el almacenamiento secundario. Los registros de auditoría en el almacenamiento primario no son necesarios almacenarlos más allá de la superación de su ventana de retención, ya que las líneas de log se encuentran ya almacenadas en el almacenamento secundario. Únicamente las líneas de log se consideran en el cómputo forense por preservar la integridad y disponer de firma como se ha comentado anteriormente. Los registros de auditoría de recepción delíneas de log y eventos de seguridad son sobrescritos, tanto en el almacenamiento primario y secundario, si se supera la ventana de retención.

68. A continuación, se detalla el proceso de configuración segura del módulo de almacenamiento. Para el detalle completo consultar el apartado 5.4 de la guía *LogICA5-GuiaInstalacion [***REF2***]*. Se indican los puntos más relevantes:

    - Emplear el usuario *root* para realizar las configuraciones.
    - Aplicar la configuración LVM (*Logical Volume Management*): Creación de un volumen físico PV (*Physical Volume*) asociado al dispositivo correspondiente al espacio en disco destinado al almcenamiento primario y otro volumen físico PV al almacenamiento primario secundario.
    - Se crea el directorio de logs y de datos de la plataforma, se incluye el directorio *logroot* para el almacenamiento secundario.

```
mkdir /ica/logs
mkdir /ica/data
mkdir /ica/data/mongodb
mkdir /ica/data/mongodb/journal
mkdir /ica/data/logroot
mkdir /ica/data/backup
mkdir /ica/logica5/data
chown –R logica5:logica /ica
chmod –R 750 /ica
chmod 751 /ica
chmod 751 /ica/logs
mkdir /ica/logs/mongodb
chmod 751 /ica/data
chmod 751 /ica/data/backup
```

```
chmod 755 /ica/data/mongodb
chmod 751 /ica/data/logroot
chown –R mongod:mongod /ica/data/mongodb
chown –R mongod:mongod /ica/logs/mongodb
```

- Establecer periodos cortos de TCP *keepalive*, del orden de 120 segundos. Para ello, editar el fichero */etc/sysctl.conf* e incluir:

```
##
net.ipv4.tcp_keepalive_time  = 120
##
```

- Configurar el *sudo* para incluir el servicio de MongoDB (iniciar, parar, reiniciar y estado. Para ello, se debe añadir al fichero */etc/sudoers.d/logica5* (se debe crear el fichero si no existe previamente). En el caso de una instalación en un único nodo:

```
%logica ALL=NOPASSWD: /bin/systemctl start mongod
%logica ALL=NOPASSWD: /bin/systemctl stop mongod
%logica ALL=NOPASSWD: /bin/systemctl restart mongod
%logica ALL=NOPASSWD: /bin/systemctl status mongod
```

- Configurar la rotación de logs. Se debe crear el fichero *etc/logrotate.d/mongodb*, y añadir:

```
/ica/logs/mongodb/*.log {
      notifempty
      daily
      rotate 5
      missingok
      compress
   endscript
}
```

6.2.1.3 SISTEMA DISTRIBUIDO DE EJECUCIÓN EN TIEMPO REAL

69. El sistema distribuido de ejecución en tiempo real es el módulo *middleware* de ingesta y tratamiento de datos distribuido en tiempo real. Se basa en (3) tres componentes:

    - **Componente de coordinación** de elementos distribuidos de ejecución en tiempo real.
    - **Componente *broker*** para la publicación y subscripción asíncrona/síncrona de streaming de datos en tiempo real.
    - **Componente gestor** de procesado distribuido de streaming de datos en tiempo real.

70. Antes de comentar el proceso de configuración segura de los componentes del módulo del sistema distribuido de ejecución en tiempo real, es necesario configurar las plataformas de ejecución *nodejs* y *java*.

    Plataforma *java*:

- Emplear el usuario root para realizar las configuraciones
- Crear el enlace simbólico '*java*' en el directorio */ica/common*, y cambiar el propietario del directorio a '*logica5*':

```
ln -s /ica/common/jdk1.8.0_161 /ica/common/java
chown –R logica5:logica /ica/common
```

- Añadir al fichero */ica/home/logica5/.bash_profile*:

```
export JAVA_HOME="/ica/common/java"
export PATH=$PATH:$JAVA_HOME/bin
```

Plataforma nodejs:

- Añadir al fichero */ica/home/logica5/.bash_profile:*

```
export NODE_PATH="/usr/lib/node_modules"
export NODE_OPTIONS="--max_old_space_size=8092"
```

6.2.1.3.1 COMPONENTE DE COORDINACION

71. El componente de coordinación se encarga del control de los elementos distribuidos de ejecución en tiempo real. Los elementos se agrupan para almacenar y replicar la configuración de los elementos y la compartición de tareas para hacerlos tolerantes a fallos. Los elementos del grupo, llamados servidores, necesitan en todo momento la elección de un servidor líder. La conexión entre los servidores y los clientes se efectúa sobre el protocolo TCP.
72. En el despliegue objeto de está guía únicamente se cuenta con un nodo, por lo que únicamente hay un servidor en el cluster.
73. A continuación, se detalla el proceso de configuración segura del componente de coordinación (*Apache Zookeeper*). Para obtener el detalle completo, se puede consultar el apartado 5.7 de la guía *LogICA5-GuiaInstalacion [***REF2***]*.

- Emplear el usuario *root* para realizar las configuraciones.
- Crear el enlace simbólico '*zookeeper*' en el directorio */ica/common*:

```
ln -s /ica/common/zookeeper-3.4.12 /ica/common/zookeeper
```

- Añadir al fichero */ica/home/logica5/.bash_profile*

```
export ZOOKEEPER_HOME="/ica/common/zookeeper"
export PATH=$PATH:$ZOOKEEPER_HOME/bin
```

- Sobrescribir e incluir los siguientes archivos en las rutas indicadas:

  /ica/common/zookeeper/conf/zoo.cfg
  /ica/common/zookeeper/conf/log4j.properties
  /usr/lib/systemd/system/zookeeper.service

Los ficheros se encuentran en el directorio *etc/zookeeper* de la distribución de la plataforma. En dicho directorio se encuentran las plantillas de los ficheros de configuración y los servicios correspondientes de *Apache Zookeeper*.

- Establecer el propietario:

```
chown -R logica5:logica  /ica/common/zookeeper-3.4.12
chown logica5:logica  /ica/common/zookeeper
```

- Activar el servicio:

```
systemctl enable zookeeper
systemctl start zookeeper
```

- Configurar el *sudo* para incluir los servicios de *zookeeper* (iniciar, parar, reiniciar y estado). Añadir al fichero */etc/sudoers.d/logica5*, crear el fichero si no existe previamente:

```
%logica ALL=NOPASSWD: /bin/systemctl start zookeeper
%logica ALL=NOPASSWD: /bin/systemctl stop zookeeper
%logica ALL=NOPASSWD: /bin/systemctl restart zookeeper
%logica ALL=NOPASSWD: /bin/systemctl status zookeeper
```

- Configurar la rotación de *logs* de la salida estándar, *zookeeper.out*. Se debe crear el fichero */etc/logrotate.d/zookeeper*, y añadir:

```
/ica/logs/zookeeper/zookeeper.out {
  su logica5 logica
  notifempty
  daily
  rotate 5
  missingok
  compress
  postrotate
  endscript
}
```

6.2.1.3.2 COMPONENTE BROKER

74. El componente broker es el encargado de la subscripción y publicación de los *streams* de datos en tiempo real.

75. El canal de comunicación para la publicación y subscripción debe estar securizado mediante TLS 1.2 sobre TCP y certificados X.509. La securización del canal se detalla en el apartado 6.5 CONFIGURACIÓN DE PROTOCOLOS SEGUROS.

76. A continuación, se detalla el proceso de configuración segura del componente bróker (*Apache Kafka*). Para el detalle completo consultar el apartado 5.8 de la guía *LogICA5-GuiaInstalacion [***REF2***]*.

- Emplear el usuario *root* para realizar las configuraciones.
- Crear el enlace simbólico 'kafka' en el directorio */ica/common*:

```
ln -s /ica/common/kafka_2.12-1.0.0 /ica/common/kafka
```

- Añadir al fichero */ica/home/logica5/.bash_profile lo siguiente:*

```
export KAFKA_HOME="/ica/common/kafka"
export PATH=$PATH:$KAFKA_HOME/bin
```

- Sobrescribir e incluir los siguientes archivos en las rutas indicadas:

  /ica/common/kafka/config/server.properties
  /ica/common/kafka/config/log4j.properties
  /usr/lib/systemd/system/kafka.service

  Dichos ficheros se encuentran en el directorio *etc/kafka* de la distribución de la plataforma el cual contiene las plantillas de los ficheros de configuración y los servicios correspondientes al broker Apache Kafka.

- Establecer el propietario:

```
chown -R logica5:logica  /ica/common/kafka_2.12-1.0.0
chown logica5:logica  /ica/common/kafka
```

- La plataforma NGSIEM LogICA5 requiere dos (2) tópicos de entrada, uno para líneas de logs y otro para eventos (los tópicos de salida son creados automáticamente). Los tópicos son mecanismos que actúan a modo de cola para la publicación y consumición de información de forma asíncrona. Los dos tópicos de entrada requieren:
  - Dos (2) particiones, el tópico se divide en dos (2) descriptores para su procesamiento en paralelo.
  - Una replicación.

- Activar el servicio:

```
systemctl enable kafka
systemctl start kakfa
```

- Añadir los tópicos de entrada para líneas de log y eventos, empleando el usuario '*logica5'*:

```
/ica/common/kafka/bin/kafka-topics.sh --create --zookeeper localhost --topic loglines
--partitions 2 --replication-factor 1 --config retention.ms=86400000
/ica/common/kafka/bin/kafka-topics.sh --create --zookeeper localhost --topic events --
partitions 2 --replication-factor 1 --config retention.ms=86400000
```

- Configurar el sudo para incluir los servicios de kafka (iniciar, parar, reiniciar y estado). Se debe añadir al fichero /etc/sudoers.d/logica5 el contenido siguiente (crear el fichero si no existe previamente):

```
%logica ALL=NOPASSWD: /bin/systemctl start kafka
%logica ALL=NOPASSWD: /bin/systemctl stop kafka
%logica ALL=NOPASSWD: /bin/systemctl restart kafka
%logica ALL=NOPASSWD: /bin/systemctl status kafka
```

6.2.1.3.3 COMPONENTE GESTOR DE PROCESADO

77. El componente gestor de procesado se encarga de la gestión del procesamiento de *streams* de datos en tiempo real.

78. A continuación, se detalla el proceso de configuración segura del componente gestor de procesado (*Apache Storm)*. Para obtener el detalle completo, se puede consultar el apartado 5.10 de la guía *LogICA5-GuiaInstalacion [***REF2**].

- Emplear el usuario *root* para realizar las configuraciones.
- Crear el enlace simbólico 'storm' en el directorio /ica/common:

```
ln -s /ica/common/apache-storm-1.0.6 /ica/common/storm
```

- Añadir al fichero */ica/home/logica5/.bash_profile* el siguiente contenido:

```
export STORM_HOME="/ica/common/storm"
export STORM_PATH="/ica/common/storm"
export PATH=$PATH:$STORM_HOME/bin
```

- Sobrescribir e incluir los siguientes archivos en las rutas indicadas:

  /ica/common/storm/conf/storm.yaml

  /ica/common/storm/log4j2/cluster.xml

  /ica/common/storm/log4j2/worker.xml

  /usr/lib/systemd/system/storm-logviewer.service

  /usr/lib/systemd/system/storm-ui.service

  /usr/lib/systemd/system/storm-nimbus.service

  /usr/lib/systemd/system/storm-supervisor.service

  Los ficheros se encuentran en el directorio *etc/storm* de la distribución de la plataforma en el que están las plantillas de los ficheros de configuración y los servicios correspondientes a la plataforma distribuida Apache Storm.

- Establecer el propietario:

```
chown -R logica5:logica  /ica/common/apache-storm-1.0.6
chown logica5:logica  /ica/common/storm
```

- Activar los servicios:

```
systemctl enable storm-logviewer
systemctl start storm-logviewer
systemctl enable storm-ui
systemctl start storm-ui
systemctl enable storm-nimbus
systemctl start storm-nimbus
systemctl enable storm-supervisor
systemctl start storm-supervisor
```

- Configurar el sudo para incluir los servicios de *storm* (iniciar, parar, reiniciar y estaod). Se debe añadir al fichero */etc/sudoers.d/logica5* (crear el fichero si no existe previamente):

```
%logica ALL=NOPASSWD: /bin/systemctl start storm-logviewer
%logica ALL=NOPASSWD: /bin/systemctl stop storm-logviewer
```

```
%logica ALL=NOPASSWD: /bin/systemctl restart storm-logviewer
%logica ALL=NOPASSWD: /bin/systemctl status storm-logviewer
%logica ALL=NOPASSWD: /bin/systemctl start storm-ui
%logica ALL=NOPASSWD: /bin/systemctl stop storm-ui
%logica ALL=NOPASSWD: /bin/systemctl restart storm-ui
%logica ALL=NOPASSWD: /bin/systemctl status storm-ui
%logica ALL=NOPASSWD: /bin/systemctl start storm-nimbus
%logica ALL=NOPASSWD: /bin/systemctl stop storm-nimbus
%logica ALL=NOPASSWD: /bin/systemctl restart storm-nimbus
%logica ALL=NOPASSWD: /bin/systemctl status storm-nimbus
%logica ALL=NOPASSWD: /bin/systemctl start storm-supervisor
%logica ALL=NOPASSWD: /bin/systemctl stop storm-supervisor
%logica ALL=NOPASSWD: /bin/systemctl restart storm-supervisor
%logica ALL=NOPASSWD: /bin/systemctl status storm-supervisor
```

- Configurar la rotación de logs de la salida. Se debe crear el fichero */etc/logrotate.d/storm*, y añadir:

```
/ica/logs/storm/*.log {
  su logica5 logica
  notifempty
  daily
  rotate 5
  missingok
  compress
  postrotate
  endscript
}
```

6.2.2 ENTORNO DE APLICACIÓN

79. El entorno de aplicación está constituido por los módulos que agrupan los componentes inherentes a NGSIEM LogICA5:

    a) El bus de *streaming* y procesado

    b) Servidores de *frontend*

80. Antes de comentar el proceso de configuración segura de los módulos del entorno de aplicación, es necesario configurar la base de datos en memoria redis.

- Emplear el usuario *root* para realizar las configuraciones.
- Configurar la ruta de logs en el fichero /etc/redis.conf:

```
logfile /ica/logs/redis/redis.log
```

- Establecer la ruta de logs:

```
mkdir /ica/logs/redis
chown redis:redis /ica/logs/redis
```

- Activar el servicio:

```
systemctl enable redis
systemctl start redis
```

- Configurar el sudo para incluir los servicios de redis (iniciar, parar, reiniciar y estado). Se debe añadir al fichero */etc/sudoers.d/logica5* (crear el fichero si no existe previamente):

```
%logica ALL=NOPASSWD: /bin/systemctl start redis
%logica ALL=NOPASSWD: /bin/systemctl stop redis
%logica ALL=NOPASSWD: /bin/systemctl restart redis
%logica ALL=NOPASSWD: /bin/systemctl status redis
```

6.2.2.1 EL BUS DE STREAMING Y PROCESADO

81. El bus de streaming y procesado es el módulo encargado de establecer los procesos a ejectuar en el procesamiento distribuido. Se ejecuta sobre el sistema distribuido de ejecución en tiempo real, perteneciente al módulo del entorno operacional. Se divide en los siguientes componentes:

    - Componentes de entrada: *endpoints* de *syslog* y SETP.
    - Componentes de recolección y procesamiento.

6.2.2.1.1 COMPONENTE DE ENTRADA

82. El componente de entrada está basado en *endpoints* que actúan como servicios de entrada para la recepción de líneas de log y eventos de seguridad, para su posterior publicación en el componente *broker* del sistema distribuido de ejecución en tiempo real:

    - Servicio de recepción de líneas de logs nativos por protocolo syslog UDP, provenientes de los sistemas cedentes pertenecientes a la organización, monitores de extracción de datos o agentes externos *LogAgent LogICA4*. **Se debe securizar el canal de comunicación mediante TLS 1.2 sobre syslog TCP y certificados x509, incorporando autenticación de certificado cliente**. La configuración de la autenticación se detalla en el apartado 6.3 AUTENTICACIÓN. La securización del canal se detalla en el apartado 6.5 CONFIGURACIÓN DE PROTOCOLOS SEGUROS.
    - Servicio de recepción de eventos de seguridad por protocolo SETP sobre TCP, provenientes de los monitores de extracción de datos o agentes externos *LogAgent LogICA4*. **Se debe securizar el canal de comunicación mediante TLS 1.2 sobre TCP, el uso de certificados x509 y autenticación básica HTTPS mediante usuario y contraseña**. Incorpora validación del certificado del cliente y lista blanca de orígenes de confianza. Actúa como servicio REST de recepción de eventos, en formato JSON, sobre HTTPS, con origen en los monitores de extracción de datos. La configuración de la autenticación se detalla en el apartado 6.3 AUTENTICACIÓN. La securización del canal se detalla en el apartado 6.5 CONFIGURACIÓN DE PROTOCOLOS SEGUROS.

83. A continuación, se detalla el proceso de configuración segura del componente de entrada. Para el detalle completo consultar la guía *LogICA5-GuiaInstalacion [**REF2**]*.

- Emplear el usuario *root* para realizar las configuraciones.
- En el directorio *etc/system* de la distribución de la plataforma se encuentra los servicios de ejecución: *lsetp.service* y *lsyslog.service*. Deben incluirse en las rutas del sistema:

  /usr/lib/systemd/system/lsetp.service
  /usr/lib/systemd/system/lsyslog.service

- El archivo *lsetp.service* se encuentra pre-configurado con las opciones por defecto recomendadas:

```
ExecStart=/usr/bin/node /ica/logica5/node/resources/cep/rest/server/server.js -m kafka -o localhost:9190 -t events -h 0.0.0.0 -P 6083 -s true --ciphers AES128:!SSLv3:!TLSv1.0:!TLSv1.1 -A internal -w 4 -k /ica/logica5/data/key.pem -c /ica/logica5/data/cert.pem -u $PASS -L info -D file -F /ica/logs/lsetp.log --kafka-key /ica/logica5/data/key.pem --kafka-cer /ica/logica5/data/cert.pem --kafka-pass $PASS --kafka-allow-invalid
```

  - m: modo de salida de datos. Valor por defecto: *kafka*
  - o: host y puerto de conexión al componente *broker*. Valor por defecto: *localhost:9190*
  - t: nombre del tópico de publicación. Valor por defecto: events
  - h: dirección del servidor de conexión. Valor por defecto: 0.0.0.0
  - P: puerto seguro de escucha. Valor por defecto: 6083
  - s: establecimiento del protocolo TLS 1.2. Valor por defecto: true.
  - *ciphers*: habilitación y deshabilitación (utilizando el prefijo "!") de algoritmos de cifrado para el establecimiento del protocolo TLS 1.2. Valor por defecto: **AES128:!SSLv3:!TLSv1.0:!TLSv1.1**
  - A: modo de autenticación. Valor por defecto: internal, validación de usuario y contraseña.
  - w: número de cores de cpu de ejecución. Valor por defecto: 4
  - k: ruta de acceso al fichero de la clave privada. Valor por defecto: */ica/logica5/data/key.pem*
  - c: ruta de acceso al fichero del certificado. Valor por defecto: */ica/logica5/data/cert.pem*
  - u: contraseña de acceso al fichero de la clave privada. La contraseña se facilita en la documentación de entrega.
  - L: nivel de detalle del log. Valor por defecto: info.
  - D: modo de log. Valor por defecto: file.

- F: ruta del fichero de log. Valor por defecto: */ica/logs/lsetp.log*
- *kafka-key*: ruta de acceso al fichero de la clave privada para el servidor del broker. Valor por defecto: */ica/logica5/data/key.pem*.
- *kafka-cert*: ruta de acceso al fichero del certificado para el servidor del broker. Valor por defecto: */ica/logica5/data/cert.pem*
- *kafka-pass*: contraseña de acceso al fichero de la clave privada del broker. La contraseña se facilita en la documentación de entrega.
- *kafka-allow-invalid*: Se permiten certificados autofirmados.

La configuración de la autenticación se detalla en el apartado 6.3 y la configuración de la securización del canal se detalla en el apartado 6.5.

- El archivo *lsyslog.service* se encuentra pre-configurado con las opciones por defecto recomendadas

```
ExecStart=/usr/bin/node /ica/logica5/node/resources/logline/syslog/server.js -m kafka -o localhost:9190 -t loglines –P tls://0.0.0.0:6514 --ciphers AES128:!SSLv3:!TLSv1.0:!TLSv1.1 -A tls -w 4 -k /ica/logica5/data/key.pem -c /ica/logica5/data/cert.pem -L info -D file -F ica/logs/lsyslog.log -u $PASS --kafka-key /ica/logica5/data/key.pem --kafka-cer /ica/logica5/data/cert.pem --kafka-pass $PASS --kafka-allow-invalid
```

- m: modo de salida de datos. Valor por defecto: *kafka*
- o: host y puerto de conexión al componente broker. Valor por defecto: *localhost:9190*
- t: nombre del tópico de publicación. Valor por defecto: loglines
- h: dirección del servidor de conexión. Valor por defecto: 0.0.0.0
- P: dirección del servidor de conexión y puerto seguro de escucha. Valor por defecto: *tls://0.0.0.0:6514*
- ciphers: habilitación y deshabilitación (utilizando el prefijo "!") de algoritmos de cifrado para el estableciminto del protocolo TLS 1.2. Valor por defecto: ***AES128:!SSLv3:!TLSv1.0:!TLSv1.1***
- A: modo de autenticación. Valor por defecto: tls, validación.
- w: número de cores de cpu de ejecución. Valor por defecto: 4
- k: ruta de acceso al fichero de la clave privada. Valor por defecto: */ica/logica5/data/key.pem*
- c: ruta de acceso al fichero del certificado. Valor por defecto: */ica/logica5/data/cert.pem*
- L: nivel de detalle del log. Valor por defecto: info.
- D: modo de log. Valor por defecto: file.
- F: ruta del fichero de log. Valor por defecto: */ica/logs/lsetp.log*

- u: contraseña de acceso al fichero de la clave privada. La contraseña se facilita en la documentación de entrega.
- *kafka-key*: ruta de acceso al fichero de la clave privada para el servidor del broker. Valor por defecto: */ica/logica5/data/key.pem.*
- *kafka-cert*: ruta de acceso al fichero del certificado para el servidor del broker. Valor por defecto: */ica/logica5/data/cert.pem*
- *kafka-pass*: contraseña de acceso al fichero de la clave privada del broker. La contraseña se facilita en la documentación de entrega.
- *kafka-allow-invalid*: Se permiten certificados autofirmados.

La configuración de la autenticación se detalla en el apartado 6.3 y la configuración de la securización del canal se detalla en el apartado 6.5.

- Se debe configurar *sudo*, para incluir las operaciones de iniciar, parar, reiniciar y estado para los servicios de: *lsetp*, *lsyslog*. Se deben incluir las líneas de configuración en el fichero */etc/sudoers.d/logica5*

```
%logica ALL=NOPASSWD: /bin/systemctl start lsetp
%logica ALL=NOPASSWD: /bin/systemctl stop lsetp
%logica ALL=NOPASSWD: /bin/systemctl restart lsetp
%logica ALL=NOPASSWD: /bin/systemctl status lsetp
%logica ALL=NOPASSWD: /bin/systemctl start lsyslog
%logica ALL=NOPASSWD: /bin/systemctl stop lsyslog
%logica ALL=NOPASSWD: /bin/systemctl restart lsyslog
%logica ALL=NOPASSWD: /bin/systemctl status lsyslog
```

6.2.2.1.2 COMPONENTES DE RECOLECCIÓN Y PROCESAMIENTO

84. El componente está constituido por dos (2) tipos de elementos. El primero es denominado 'colector' y es el encargado de recoger el flujo de datos de entrada. El segundo se denomina 'procesador' y es el encargado del procesado o transformación de los datos.

85. Estos elementos se agrupan en encaminadores de *streams* de datos, en estructura de grafos, para la creación de rutas de proceso.

86. Las diferentes formas en que se van a compartir los *streams* entre los distintos procesadores a través de las rutas de proceso son:

- Aleatoria: los *streams* se envían de forma aleatoria a cualquier procesador del clúster. Se produce una distribución equitativa de carga entre los nodos.
- Por campos: los *streams* se agrupan por un determinado campo de manera que se distribuyen los valores que cumplen una determinada condición.
- Total: El *stream* se envía a todos los procesadores del clúster. Es *multicast*.
- Ninguna: Similar a la aleatoria pero donde el orden no es importante.
- Directo: Es el procesador el que decide a que otro procesador enviar los streams, indicando su ID de procesador para informar del emisor.

- Local: Se emplea el mismo procesador si tiene una o más tareas en el mismo procesador.

87. El modelo de datos que emplea el componente de recolección y procesamiento es una tupla, formada por listas de valores con un nombre específico. El valor puede ser un objeto de cualquier tipo. Se procesan, por tanto, streams de tuplas.
88. Tanto los colectores como los procesadores pueden compartir información a través de una base de datos en memoria, Redis.
89. Se disponen dos encaminadores o rutas de proceso, uno para el procesamiento de líneas de log y otro para el procesamiento de eventos de seguridad. La administración de estos encaminadores de puede consultar en las guías *LogICA5-GuiaOperacion [***REF1***] y LogICA5-GuiaUsuario [***REF3***].*

6.2.2.2 SERVIDORES DE *FRONTEND*

90. Los servidores de frontend son responsables de dar acceso a las funcionalidades de gestión y administración de NGSIEM LogICA5.
91. En el despliegue objeto de está guía únicamente se cuenta con un nodo, por lo que solamente hay un servidor de frontend.
92. El almacenamiento de recursos y el mantenimiento de estado se efectúa a través de una base de datos en memoria, Redis.
93. Los servidores de frontend exponen: recursos estáticos, servidores REST y websockets; accedidos mediante protocolo HTTP2 sobre TLS 1.2 y certificados X.509 –HTTP2S-. La securización del canal se detalla en el apartado 6.5 CONFIGURACIÓN DE PROTOCOLOS SEGUROS.
94. La autenticación está basada en usuario y contraseña. La configuración de la autenticación se detalla en el apartado 6.3 AUTENTICACIÓN. Se proporciona acceso remoto desde:
    - El módulo de la consola del entorno de integración de *NGSIEM LogICA5*.
    - Un *frontend* de servicios REST y *websockets*, con funcionalidades compatibles con el módulo de la consola.
95. A continuación, se detalla el proceso de configuración segura del componente de entrada. Para el detalle completo consultar la guía *LogICA5-GuiaInstalacion [***REF2***].*
    - Emplear el usuario *root* para realizar las configuraciones.
    - Establece la propiedad y permisos de acuerdo a las siguientes instrucciones:

```
chmod o+x   /ica/logica5/data
chmod o+x   /ica/logica5
chmod 644   /ica/logica5/data/logICA5.pem
chown –R logica5:logica /ica/logica5
```

    - En el directorio *etc/system* de la distribución de la plataforma se encuentra el servicio de ejecución: *logica.service*. Este archivo está pre-configurado

con las opciones por defecto recomendadas. Debe incluirlos en las rutas del sistema:

/usr/lib/systemd/system/logica.service

- Se debe configurar sudo, para incluir las operaciones de iniciar, parar, reiniciar y estado para los servicios de: logica, lsetp, lsyslog. Se deben incluir las líneas de configuración en el fichero */etc/sudoers.d/logica5*

```
%logica ALL=NOPASSWD: /bin/systemctl start logica
%logica ALL=NOPASSWD: /bin/systemctl stop logica
%logica ALL=NOPASSWD: /bin/systemctl restart logica
%logica ALL=NOPASSWD: /bin/systemctl status logica
```

- Configurar la rotación de logs de la salida. Se debe crear el fichero */etc/logrotate.d/logica5*, y añadir:

```
/ica/logs/logica.log
/ica/logs/logica5/*.log {
      su logica5 logica
      notifempty
      daily
      size 5M
      rotate 5
      missingok
      compress
   endscript
}
```

- Configurar las propiedades del fichero */ica/logica5/data/suite.properties*. Las propiedades que deben ser configuradas son:

  - Tiempo de expiración, en minutos, de la sesión https (propiedad ***server.session.expire***). Por defecto, está configurada en 30 minutos, se recomienda no modificarla o reducir el tiempo. Si el valor es igual a 0, la sesión no expira.
  - Nombre de usuario de conexión para la base de datos de colecciones funcionales (propiedad *mongo.db.username).*
  - Contraseña del usuario de conexión para la base de datos de colecciones funcionales *(propiedad mongo.db.password*). Debe ir cifrada con el formato *{pbe:internal2:<CYPHERED_PASSWORD>}*.
  - Nombre de usuario de conexión para la base de datos de colecciones de eventos (propiedad *mongo.db.username.data.events).*
  - Contraseña del usuario de conexión para la base de datos de colecciones de eventos *(propiedad mongo.db.password.data.events*). Debe estar cifrada con el formato:

    {pbe:internal2:<CYPHERED_PASSWORD>}.

- Nombre de usuario de conexión para la base de datos de colecciones de líneas de logs (propiedad *mongo.db.username.data.logs).*
- Contraseña del usuario de conexión para la base de datos de colecciones de líneas de logs *(propiedad mongo.db.password.data.logs*). Debe ir cifrada con el formato:

  {pbe:internal2:<CYPHERED_PASSWORD>}.
- Requerir una dirección de email válida para el usuario interno encargado de las notificaciones por smtp (propiedad mail.user).
- Requerir una contraseña para el usuario interno encargado de las notificaciones por smtp (propiedad mail.password). Debe ir cifrada con el formato:

  {pbe:internal2:<CYPHERED_PASSWORD>}.
- Dirección de email que debe aparecer en el pie en las notificaciones por smtp (propiedad mail.application.url).
- Dirección de email que debe aparecer en el remitente en las notificaciones por smtp (propiedad mail.user.from).
- Modo de acceso a los usuarios por base de datos o LDAP (propiedad security.login.type, base de datos -> *'Security', ldap -> 'SecurityLdap'*. Valor por defecto por base de datos, 'Security').
- Para cifrar y descrifrar con el formato:

  {pbe:internal2:<CYPHERED_PASSWORD>}

  Según se requiere en las propiedades indicadas, se debe emplear la clase *java EncryptedPassword* con el usuario *logica5*.

  - Cifrar:

    ```
    $JAVA_HOME/bin/java -cp
    /ica/logica5/bin:/ica/logica5/data:/ica/logica5/lib/*
    es.grupoica.suite.commons.crypto.EncryptedPassword -e  <password>
    ```

  - Descrifrar:

    ```
    $JAVA_HOME/bin/java -cp
    /ica/logica5/bin:/ica/logica5/data:/ica/logica5/lib/*
    es.grupoica.suite.commons.crypto.EncryptedPassword –d
    <cyphered_password>
    ```

96. Otras propiedades relacionadas con la seguridad son:

- Indicador para la autenticación con el servidor SMTP para el envío de notificaciones (propiedad *mail.auth.required*). Valor por defecto: *true.*
- Indicador para la notificación de contraseñas por correo electrónico en caso de alta o recuperación de acceso con el módulo de servidor de frontend (propiedad security.password.byEmail). Valor por defecto: *true*. Se recomienda cambiar el valor a *false*.

6.2.3 ENTORNO DE INTEGRACIÓN

97. El entorno de integración está formardo por los módulos que agrupan los componentes de la plataforma NGSIEM LogICA5 que se integran con otras plataformas del fabricante o sistemas externos:

    a) Monitor de extracción de datos.

    b) Consola.

98. Los modulos del entorno de integración, consola y monitor de extracción de datos, al igual que los componentes o *plugins* de extensión tipo *add-on* y, los módulos LISM y LogAgent4 en caso de requerir agentes compatibles con LogICA4, no se encuentran en la configuración evaluada y certificada Common Criteria y, por tanto, se encuentran fuera del alcance de este documento. Si se requiere más información sobre la configuración de estos módulos y componentes, puede ser consultado en la guía *LogICA5-GuiaInstalación [***REF2***].*

6.3 AUTENTICACIÓN

99. A continuación, se detalla la configuración de los mecanismos de autenticación de los módulos de NGSIEM LogICA5. Para obtener el detalle completo, se puede consultar la guía *LogICA5-GuiaOperación [***REF1***]* y el apartado 5 de la guía *LogICA5-GuiaInstalacion [***REF2***],* proporcionadas por el fabricante.

100. Para configurar la autenticación en el almacenamiento primario del módulo sistema de almacenamiento, se deben seguir los siguientes pasos:

- Emplear el usuario *root* para realizar las configuraciones.
- Conectar al cliente de base de datos:

```
mongo –host logica5
```

- Configurar la base de datos interna admin, creando un rol de administración (“lógica”, en el ejemplo) con todos los permisos, y un usuario asociado al rol.

```
use admin

db.createRole({
role:"logica",
privileges: [ {resource:{ anyResource: true }, actions:["anyAction"]} ],
roles:["root"]
})
db.createUser({
user:"admin",
pwd:"<passw>",
roles:[{role:"logica",db:"admin"}]
})
```

- Activar la autenticación. Se debe añadir al fichero */etc/mongod.conf:*

```
security:
                    authorization:enabled
```

101. Para configurar la autenticación en la recepción de líneas de log del componente de entrada del módulo bus de streaming y procesado, seguir los siguientes pasos:

- Emplear el usuario root para realizar las configuraciones.
- Modificar el fichero lsyslog.service con los parámetros necesarios para invocar el servicio con la activación de la autenticación mediante la validación del certificado del cliente. El tratamiento de certificados de confianza se detalla en el apartado 6.6 Gestión de certificados.
    - *Párametro: –A*
    - *Valor: tls.*

102. Para configurar la autenticación en la recepción de eventos de seguridad del componente de entrada del módulo bus de *streaming* y procesado, seguir los siguientes pasos:

- Emplear el usuario *root* para realizar las configuraciones.
- Crear un usuario y contraseña mediante el comando.

```
node /ica/logica5/node/resources/cep/rest/server/server.js --auth-user-add
[username:password]
```

- Modificar el fichero *lsetp.service* con los parámetros necesarios para invocar el servicio con la activación de la autenticación mediante validación de usuario y contraseña.
    - *Párametro: –A*
    - *Valor: internal.*

103. Para configurar la autenticación en el módulo de servidores de *frontend*, seguir los siguientes pasos:

- Emplear el usuario *root* para realizar las configuraciones.
- NGSIEM LogICA5 ofrece por defecto un usuario de *frontend* administrador, *superroot*, con acceso global sin restricción de acceso. Este usuario se proporciona en la documentación de entrega. Es el encargado de establecer inicialmente los roles definidos por el usuario recomendados por defecto (ver apartado 6.4.5 ROLES, PERMISOS Y POLITICAS DE ACCESOS *FRONTEND*).
- Modificar el fichero suite.properties con las propiedades necesarias para invocar la activación de la autenticación mediante validación de usuario y contraseña. Se utiliza la propiedad *security.login.type* para establecer el tipo de servidor de autenticación:
    - Interno, sistema de almacenamiento primario de NGSIEM LogICA5. Valor: *Security.* Valor por defecto.

- Externo, sistema Ldap. Valor: *SecurityLdap*. (ver apartado 6.7 SERVIDORES DE AUTENTICACIÓN).

6.3.1 INTERFACES DE CONEXIÓN

104. A continuación, se detalla la configuración segura de las interfaces de comunicación con los módulos de NGSIEM LogICA5. Para el detalle completo consultar la guía *LogICA5-GuiaInstalacion [***REF2***]* proporcionada por el fabricante.

105. Para configurar la interfaz de comunicación del componente de entrada del módulo bus de *streaming* y procesado:

- Emplear el usuario *root* para realizar las configuraciones.
- Realizar la configuración del *firewall*. Puertos abiertos, tráfico entrante de la red de producción:
  - Puerto 6080 para el acceso al endpoint SETP sobre TCP del componente de entrada del Bus de *streaming* y procesado.
  - Puerto 6083 para el acceso al endpoint SETP sobre TLS 1.2 del componente de entrada del Bus de streaming y procesado.
  - Puerto 514 para el acceso al endpoint syslog UDP/TCP del componente de entrada del Bus de streaming y procesado.
  - Puerto 6514 para el acceso al endpoint syslog TLS 1.2 sobre TCP del componente de entrada del Bus de streaming y procesado.

106. Para configurar la interfaz de comunicación con el módulo servidores de frontend:

- Emplear el usuario *root* para realizar las configuraciones.
- Realizar la configuración del *firewall*. Puertos abiertos, tráfico entrante de la red de gestión:
  - Puerto 7000 TCP

107. Para configurar la interfaz de comunicación con módulos de integración y componentes externos no contemplados en esta guía. Si se requiere más información sobre la configuración de estos módulos y componentes, puede consultarse *LogICA5-GuiaInstalación [***REF2***].*

- Emplear el usuario *root* para realizar las configuraciones.
- Realizar la configuración del *firewall*. Puertos abiertos, tráfico entrante de la red de gestión
  - Puerto 9998 para acceder al módulo Monitor de extracción de datos interno al nodo.

- Puerto 9996 para acceder al módulo LISM desde los agentes LogAgent LogICA4. Los módulos de LogICA4 que pueden integrarse con NGSIEM LogICA5 se comentan en el siguiente punto.

6.4 ADMINISTRACIÓN DEL PRODUCTO

108. Si se requiere más información sobre la administración de NGSIEM LogICA5 pueden consultar las guías *LogICA5-GuiaOperación [***REF1***]* y *LogICA5-GuiaUsuario [***REF3***]* proporcionadas por el fabricante.

6.4.1 ADMINISTRACIÓN LOCAL Y REMOTA

109. La administración se realiza a través de consola de comandos por protocolo seguro SSH, que debe configurarse de acuerdo a lo establecido en el apartado 6.2.1.1. Permite la administración local y remota del entorno operacional y de la interfaz con el sistema operativo de los módulos de servidores de *frontend* y del bus de *streaming* y procesado.

110. La interfaz de entrada con el módulo servidores de *frontend*, tanto desde el api REST o desde la consola, emplea TLS 1.2 sobre TCP y certificado X509 SHA256, RSA 3072 y cifrado AES 128/256 (la gestión de certificados se detalla en el apartado 6.6 GESTIÓN DE CERTIFICADOS y la configuración del protocolo seguro en el apartado 6.5 CONFIGURACIÓN DE PROTOCOLOS SEGUROS). Permite la administración local y remota de los servidores de *frontend*.

6.4.2 CONFIGURACIÓN DE USUARIOS

111. En este apartado se definen los diferentes usuarios de los que dispone la plataforma:

a) Usuarios del sistema operativo.

b) Usuarios de *frontend*.

c) Usuarios del bus.

112. Se recomienda seguir el **principio de mínimo privilegio** y dotar a los usuarios de unos privilegios mínimos que permitan la correcta ejecución de sus actividades e impidan la realización de acciones adicionales.

6.4.3 ROLES Y PERMISOS DE ACCESOS SISTEMA OPERATIVO

113. Los usuarios del sistema operativo son:

- Super administrador. Usuario *root* que tiene permiso completo de administración del sistema operativo del entorno operacional de *NGSIEM LogICA5*. Modifica los parámetros de instalación:
  - Arrancar, parar y comprobar el estado de los servicios *systemd* del sistema operativo, correspondientes al *endpoint* de entrada de líneas de log y al *endpoint* de entrada de eventos de seguridad.

- Gestionar los usuarios del bus (*endpoint* de entrada de eventos de seguridad), los certificados de confianza (*endpoint* de entrada de líneas de log) y cambiar los parámetros de los archivos de configuración, correspondientes al *endpoint* de entrada de líneas de log, y al *endpoint* de entrada de eventos de seguridad.

- Administrador. Usuario '*logica5*'. Dispone de permiso de escritura de todos los archivos desplegados de *NGSIEM LogICA5* y de ejecución de servicios a través de *sudo*.
- Operador. Usuario '*ica*'. Dispone de permiso de lectura de todos los archivos desplegados de *NGSIEM LogICA5*.

114. Estos usuarios se encuentran establecidos de forma predeterminada y no deben ser modificados o borrados. Los usuarios super administrador y administrador pertenecen a los usuarios administradores del sistema operativo. Únicamente se pueden crear usuarios adicionales, si es necesario, con permiso de lectura mediante la asignación del grupo primario '*logica*':

```
useradd -g logica <username>
```

6.4.4 ROLES Y PERMISOS DE ACCESO AL BUS

115. Los **usuarios del bus** son usuarios del subsistema del bus de *streaming* y procesado en tiempo real encargados de transmitir líneas de logs y eventos de seguridad. La administración de usuarios del bus se detalla en el apartado 6.1.1 del documento *LogICA5-GuiaOperacion [***REF1***]*.

116. Existe un único rol con permiso que permite la recepción de líneas de log y eventos de seguridad, inherente a todos los usuarios del bus.

6.4.5 ROLES, PERMISOS Y POLITICAS DE ACCESOS *FRONTEND*

117. Los roles o perfiles de acceso son funciones de seguridad, que se pueden asignar a los usuarios del módulo de servidores de frontend. Dichas funciones de seguridad son las siguientes:

- Secciones: identifican funcionalidades de la plataforma que sirven para autorizar el acceso. Los usuarios están autorizados a las funcionalidades de la plataforma correspondientes a las secciones asignadas a sus roles. Las secciones son funciones de seguridad.
- Control de acceso sobre la información proporcionada de los sistemas cedentes (SIEM data): colas de eventos de seguridad, consultas y patrones de filtrado sobre líneas de log y acciones sobre los eventos de seguridad.

118. La creación de roles mediante la asignación de secciones a roles y la asignación de roles a usuarios se detalla en el apartado 7 del documento *LogICA5-GuiaUsuario* (consola) o en el apartado 7.2 del documento *LogICA5-GuiaOperacion* (Servicios REST).

119. El control de acceso sobre la información proporcionada de los sistemas cedentes a los roles por defecto de administrador y operador, al igual que al resto de roles, se debe ajustar según las políticas de autorización de los sistemas cedentes.

120. Los usuarios de *frontend* administradores disponen de roles de administración: roles con secciones de acceso asignadas tipo admin/*. El asterisco denomina el nombre del componente o plugin como *admin/cep* o *admin/security*. Cada sección de acceso permite realizar acciones de administración sobre cada componente o *plugin*.

121. Los usuarios de *frontend* administradores deben realizar las siguientes funciones relativas a la seguridad:

- Gestión de usuarios de frontend.
- Gestión de roles.
- Asignación/des asignación de secciones, colas, consultas y patrones de filtrado y acciones, a roles.
- Asignación/des asignación de roles a usuarios de *frontend*.
- Gestión de políticas de seguridad.

122. Las políticas de seguridad permiten especificar los parámetros de robustez de las contraseñas utilizadas. En el apartado 5.2.1.1 se recogen ciertos requisitos que deben cumplir las contraseñas. Para los usuarios de frontend, se fija, por defecto, el número de intentos de acceso fallidos a tres (3) intentos antes de bloquear la sesión. En caso de superar dicho umbral de intentos, el bloqueo es de tres (3) minutos.

123. El resto de usuarios de *frontend* pertenecientes al rol de operador pueden consultar usuarios, roles y políticas de seguridad.

124. Para conocer el detalle de todas las secciones que se pueden gestionar a través de los roles, se debe consultar la guía LogICA5-GuiaOperacion [**REF1**].

6.5 CONFIGURACIÓN DE PROTOCOLOS SEGUROS

125. A continuación, se detalla la configuración de los protocolos seguros de comunicacion de los módulos de NGSIEM LogICA5. Para el detalle completo consultar la guía *LogICA5-GuiaInstalacion* [**REF2***]* proporcionada por el fabricante.

126. Para configurar el uso del protocolo TLS 1.2 en las comunicaciones del almacenamiento primario del módulo sistema de almacenamiento, se deben seguir los siguientes pasos:

- Emplear el usuario *root* para realizar las configuraciones.
- Crear los siguientes directorios si no están creados aún:

  mkdir /ica/logica5/

  mkdir /ica/logica5/data

- La ruta del fichero con formato pem, con la clave privada y el certificado de NGSIEM LogICA5, se encuentra en el directorio data de la distribución de la plataforma y debe copiarse en el directorio */ica/logica5/data.* Se deben establecer propietario y permisos:

```
chmod o+x   /ica/logica5/data
chmod o+x   /ica/logica5
chmod 644   /ica/logica5/data/logICA5.pem
chown –R logica5:logica /ica/logica5
```

- Añadir al *fichero /etc/mongod.conf*, en el apartado *ssl* como subapartado del apartado net, el archivo.pem con la clave privada y certificado, y la contraseña de la clave privada (*pem key password* - la contraseña se proporciona en la documentación de entrega).

```
ssl:
        mode:requireSSL
        PEMKeyFile:/ica/logica5/data/logICA5.pem
        PEMKeyPassword: <pem key password>
```

- Reiniciar el servicio: *mongod.service*

```
systemctl restart mongod
```

127. Para configurar el uso del protocolo TLS 1.2 en las comunicaciones del componente *broker* del módulo sistema distribuido de ejecución en tiempo real, seguir los siguientes pasos:

- Emplear el usuario root para realizar las configuraciones.
- Modificar el fichero */ica/common/kafka/config/server.properties*:
  - Establecer el identificador SSL, puerto 9190. Propiedad *listeners*.
  - Establecer los contenedores de claves y sus contraseñas de acceso. Las claves de la plataforma NGSIEM LogICA5 se encuentran en el directorio */ica/logica5/data*. Propiedades:
    - *ssl.keystore.location*
    - *ssl.keystore.password*
    - *ssl.key.password*
    - *ssl.truststore.location*
    - *ssl.truststore.password*
    - *ssl.client.auth*

- Establecer el identificador SSL, puerto 9190. Propiedad *advertised.listeners*.

```
listeners=SSL://localhost:9190
ssl.keystore.location=/ica/logica5/data/logICA5.p12
ssl.keystore.password= <password>
ssl.key.password= <password>
ssl.truststore.location=/ica/logica5/data/logICA5.p12
ssl.truststore.password= <password>
ssl.client.auth= required
advertised.listeners=SSL://localhost:9190
```

- Reiniciar el servicio:

```
systemctl restart kakfa
```

128. Para configurar el uso del protocolo TLS 1.2 para la recepción de líneas de log del componente de entrada del módulo bus de *streaming* y procesado, se deben seguir los siguientes pasos:

- Emplear el usuario *root* para realizar las configuraciones.
- Modificar el fichero *lsyslog.service* con los parámetros necesarios para invocar el servicio con la activación del cifrado del canal, tanto para el servidor del componente de entrada como su acceso al broker.
  - K: ruta de acceso al fichero de la clave privada. Valor por defecto: /ica/logica5/data/key.pem
  - c: ruta de acceso al fichero del certificado. Valor por defecto: /ica/logica5/data/cert.pem
  - u: contraseña de acceso al fichero de la clave privada. La contraseña se facilita en la documentación de entrega.
  - *kafka-key*: ruta de acceso al fichero de la clave privada para el servidor del broker. Valor por defecto: */ica/logica5/data/key.pem*.
  - *kafka-cert*: ruta de acceso al fichero del certificado para el servidor del broker. Valor por defecto: */ica/logica5/data/cert.pem*
  - *kafka-pass*: contraseña de acceso al fichero de la clave privada del broker. La contraseña se facilita en la documentación de entrega.
  - *kafka-allow-invalid*: Se permiten certificados autofirmados.

129. Para configurar el uso del protocolo TLS 1.2 para la recepción de eventos de seguridad del componente de entrada del módulo bus de streaming y procesado, seguir los siguientes pasos:

- Emplear el usuario root para realizar las configuraciones.
- Modificar el fichero *lsetp.service* con los parámetros necesarios para invocar el servicio con la activación del cifrado del canal, tanto para el servidor del componente de entrada como su acceso al broker.
  - K: ruta de acceso al fichero de la clave privada. Valor por defecto: */ica/logica5/data/key.pem*
  - c: ruta de acceso al fichero del certificado. Valor por defecto: */ica/logica5/data/cert.pem*
  - u: contraseña de acceso al fichero de la clave privada. La contraseña se facilita en la documentación de entrega.
  - *kafka-key*: ruta de acceso al fichero de la clave privada para el servidor del broker. Valor por defecto: */ica/logica5/data/key.pem.*
  - *kafka-cert*: ruta de acceso al fichero del certificado para el servidor del broker. Valor por defecto: */ica/logica5/data/cert.pem*
  - *kafka-pass*: contraseña de acceso al fichero de la clave privada del broker. La contraseña se facilita en la documentación de entrega.
  - *kafka-allow-invalid*: Se permiten certificados autofirmados.

130. Para configurar el uso del protoclo TLS 1.2 en las comunicaciones del módulo de servidores de frontend, seguir los siguientes pasos:

- Emplear el usuario *root* para realizar las configuraciones.
- Modificar el fichero *suite.properties* con las propiedades necesarias para invocar el servicio con la activación del cifrado del canal, tanto para el servidor de *frontend* como su acceso al almacenamiento primario, al *broker* y al servidor de correo.
  - Conexión por TLS 1.2 de la base de datos de colecciones funcionales (propiedad *mongo.db.ssl*). Debe establecerse a *true*.
  - Conexión por TLS 1.2 de la base de datos de colecciones de eventos (propiedad *mongo.db.ssl.data.events*). Debe establecerse a *true*.
  - Conexión por TLS 1.2 de la base de datos de colecciones de eventos (propiedad *mongo.db.ssl.data.logs*). Debe establecerse a *true*.
  - Conexión por TLS 1.2 para las comunicaciones con el broker (propiedad k). Debe establecers a k.
  - Clave privada para el establecimiento del protocolo TLS 1.2 en la comunicación con el *broker* (propiedad *kafka.ssl.key*) en formato PEM. Valor por defecto: */ica/logica5/data/key.pem.*
  - Certificado para el establecimiento del protocolo TLS 1.2 en la comunicación con el broker (propiedad *kafka.ssl.cer*) en formato PEM. Valor por defecto: */ica/logica5/data/cert.pem.*

- Contraseña de acceso al fichero de la clave privada para el el establecimiento del protocolo TLS 1.2 en la comunicación con el broker (propiedad *kafka.ssl.pass*).

  Valor por defecto: *{pbe:internal2:/A0YaQHp/Zgm+XYkA2MIcQ==}*

- Ruta de acceso al contenedor de clave privada y certificados para el establecimiento del protocolo TLS 1.2 en la comunicación con el módulo de servidores de *frontend* (propiedad *server.connectors.ssl.keystore*) en formato p12.

  Valor por defecto: */ica/logica5/data/logICA5.p12.*

- Contraseña de acceso al contenedor de clave privada y certificados para el establecimiento del protocolo TLS 1.2 en la comunicación con el módulo de servidores de *frontend* (propiedad *server.connectors.ssl.keystore.password*).

  Valor por defecto: *{pbe:internal2:/A0YaQHp/Zgm+XYkA2MIcQ==}.*

- Indicador para el establecimiento del protocolo TLS 1.2 en la comunicación de notificaciones por SMTP (propiedad mail.ssl.required).

  Valor por defecto: *true.*

- El mecanismo para cifrar contraseñas se ha detallado en el apartado 6.2.2.2.

6.6 GESTIÓN DE CERTIFICADOS

131. El certificado y la clave privada de la plataforma NGSIEM LogICA5 son facilitados junto con el resto del *software*. No son necesarias tareas de configuración en la gestión de certificados. La contraseña de acceso a la clave privada se proporciona en la documentación de entrega. En caso de caducidad, las claves deben ser actualizadas, por lo que es necesario ponerse en contacto con el fabricante para su actualización.

132. El certificado de la plataforma NGSIEM LogICA5 está en formato X509 con función de integridad SHA256. El certificado se basa en un conjunto de claves (pública y privada), RSA de longitud 3072.

133. Las comunicaciones seguras TLS 1.2 entre los diferentes módulos de la plataforma NGSIEM LogICA5 se establecen entre entidades que comparten los mismos certificados y claves. Se corresponden con los certificados y claves del punto anterior.

134. Las comunicaciones seguras TLS 1.2 entre los sistemas cedentes y la plataforma NGSIEM LogICA5 para la transmisión de eventos de seguridad se incluyen como parte de las comunicaciones entre módulos de la plataforma NGSIEM LogICA5 del punto anterior. En este caso los sistemas cedentes son los módulos Monitor de Extracción de datos de la plataforma NGSIEM LogICA5 y LogAgent LogICA4. Estos módulos se encuentran fuera del alcance de este documento como ya se ha

indicado en el apartado 6.2.3, pero su configuración puede ser consultada en la guía LogICA5-GuiaInstalacion *[**REF2**]*.

135. Las comunicaciones seguras TLS 1.2 entre los sistemas cedentes y la plataforma NGSIEM LogICA5 para la transmisión de líneas de log exige el intercambio de certificados entre entidades. El certificado del sistema cedente debe cumplir los requisitos de: integridad de firma SHA256 y algoritmo asimétrico RSA de 3072 bits. La interfaz de NGSIEM LogICA5 para la recepción de líneas de log, comprueba el certificado, y si no cumple los requisitos, aborta la conexión. La autenticación se efectúa por certificado, por lo que el sistema cedente debe proporcionar una CA de confianza para la plataforma NGSIEM LogICA5. Su configuración se detalla en el apartado 6.1.1.2 de la LogICA5-GuiaOperacion *[**REF1**]*. La CA suministrada por el sistema cedente se debe importar (copiar al directorio –data- configurable, por ejemplo: */ica/logica5/data*) al componente de entrada del módulo bus de *streaming* de procesado en tiempo real. De esta forma el componente de entrada puede confiar en certificados firmados por la CA importada.

6.7 SERVIDORES DE AUTENTICACIÓN

136. NGSIEM LogICA5 puede emplear un servidor LDAP de autenticación. Para ello, se debe configurar las siguientes propiedades del fichero *suite.properties* ubicado en */ica/logica5/data/suite.properties*:

- *security.login.type* → Especificar si los usuarios se almacenan por LDAP o por base de datos.
  - Interno, sistema de almacenamiento primario de NGSIEM LogICA5. Valor: *Security*. Valor por defecto.
  - Externo, sistema Ldap. Valor: *SecurityLdap*.
- *ldap.trust.manager* → Almacén de claves de confianza si LDAP por SSL.
- *ldap.vendor* → Tipo de LDAP.
- *ldap.server* → Servidor de LDAP.
- *ldap.domain* → DN del dominio de logica.
- *ldap.username* → Usuario de LDAP con permisos de administración.
- *ldap.password* → Contraseña de LDAP con permisos de administración.
- *ldap.ismultidomain* → Si el servidor de LDAP es multidominio.
- *ldap.users* → DN de la ubicación de los usuarios en LDAP.
- *ldap.users.filter* → Filtro de búsquedas de usuarios.
- *ldap.search.filter* → Filtro de búsqueda.

6.8 SINCRONIZACIÓN HORARIA

137. Todos los elementos de la plataforma deben estar sincronizados y disponer de una fuente única de tiempo. Dicha sincronización se puede establecer a través del protocolo NTP (*Network Time Protocolo*).

138. Para configurar el NTP, es necesario actualizar el fichero *ntp.conf* de acuerdo a lo especificado a continuación:

```
driftfile /var/lib/ntp/drift
restrict default kod nomodify notrap nopeer noquery
restrict -6 default kod nomodify notrap nopeer noquery
restrict 127.0.0.1
restrict -6 ::1
server <server> key 1
keys /etc/ntp.keys
trustedkey 1
controlkey 1
requestedkey 1.
disable monitor
```

139. *Se debe reemplazar la entrada <server>* con la dirección del servidor NTP que se va utilizar.

140. El servidor debe proporcionar la hora de España (o la ubicación elegida) y disponer de autenticación NTP mediante clave simétrica (la clave debe ser facilitada por parte del servidor y configurada en *ntp.keys* – se deben utilizar claves de al menos 128 bits), y este debe estar previamente configurado. Si se conecta a un *pool* de servidores, es necesario incluir la clave simétrica por cada elemento del *pool*.

141. Para configurar la clave del servidor, en el fichero */etc/ntp.keys*, se debe reemplazar *<type>* por el tipo de clave y *<key>* por la clave. En este caso al contar con un único servidor se utiliza el *id* 1.

142. Si se emplea un *pool* de servidores habría, por cada elemento del *pool,* una entrada por servidor, *trustedkey*, *controlkey* y *requestedkey* en el fichero *ntp.conf* y una entrada para cada clave correspondiente a cada elemento del *pool* en el fichero *ntp.keys*, relacionando unívocamente los elementos del *pool* por *id*.

143. Se debe asignar los permisos al fichero *ktp.keys* y reiniciar el servicio.

```
chmod 600 /etc/ntp.keys
systemctl restart ntp
```

6.9 ACTUALIZACIONES

144. El proceso de actualización del producto se desarrolla siguiendo los mismos procesos definidos para una distribución nueva (ver apartado 5.1 ENTREGA SEGURA DEL PRODUCTO). A través de esos mismos mecanismos se realiza la distribución de actualizaciones o parches de producto.

145. El fabricante se encarga de notificar de la existencia de actualizaciones. No existe un proceso de envío de notificaciones automático.

6.10 AUTO-CHEQUEOS

146. Durante el arranque de los servicios, NGSIEM LogICA5 efectúa funciones de integridad para el control de licencia. Se comprueba que la licencia facilitada en la documentación de entrega cumple con el despliegue realizado, en particular:

- Modulos instalados.
- Numero de fuentes monitorizadas, pertenecientes a los sistemas cedentes.
- La fecha no supera la fecha límite de licencia.
- La máquina empleada para desplegar NGSIEM LogICA5 es la registrada en la licencia.

147. La comprobación de las claves criptográficas se efectúa en el momento de emplear el protocolo TLS 1.2 para el envío o recepción de datos. En caso de fallo, se notifica del error en el registro (de log) destinado a ello en cada módulo. No existe un auto chequeo.

148. El proceso de inicialización de los subsistemas o módulos que forman la plataforma NGSIEM LogICA5 se produce de forma escalonada, dentro del ámbito de cada nodo.

- Primero: inicialización del sistema operativo.
- Segundo: inicialización del resto del entorno operacional y de los módulos de NGSIEM LogICA5 que forman parte de dicho entorno, sistema de almacenamiento y sistema distribuido de ejecución en tiempo real.
- Tercero: inicialización de los módulos del entorno de aplicación - Bus de *streaming* y procesado en tiempo real y servidores de *frontend*:
  - Módulo del Bus de streaming y procesado: se inicializan los servicios de *lsyslog* y *lsetp* correspondientes al componente de entrada del bus. En este momento se chequea la inicialización del servidor TLS 1.2 para la recepción de líneas de log y el servidor SETP HTTPS para la recepción de eventos de seguridad.
  - Módulo de servidores de *frontend*: se chequea la conexión con el sistema de almacenamiento, el sistema de ejecución distribuida, el bus de coordinación, el componente de gestión de procesado, el contenedor del entorno de ejecución de componentes de extensión y la inicialización del servidor HTTP2S.
- Cuarto: inicialización de los módulos de integración, monitores de extracción de datos y consola.

149. En el caso de que alguna de las comprobaciones de integridad falle, el sistema aborta su ejecución. En el registro del log destinado a cada módulo se notifica del error producido.

6.11 AUDITORÍA

6.11.1 REGISTRO DE EVENTOS

150. Los módulos del entorno de aplicación de NGSIEM LogICA5 disponen de la capacidad de generar y almacenar registros de auditoría (exitosos y fallidos). Estos registros están protegidos ante la modificación y borrado no autorizado.

151. El módulo bus de *streaming* y procesado en tiempo real almacena los registros de auditoría en archivos del sistema operativo y se encuentran, por tanto, protegidos por los permisos de acceso del propio sistema operativo. Únicamente los usuarios administradores del sistema operativo de NGSIEM LogICA5 tienen permiso de edición sobre los archivos de auditoría.

152. Se auditan los siguientes tipos de eventos:

- Arranque y parada de las funciones de auditoría.
- Mecanismo de autenticación.
- La recepción de datos de SIEM provenientes de los sistemas cedentes.

153. El arranque y parada de las funciones de auditoría y los mecanismos de autenticación se almacenan en archivos del sistema operativo, un archivo de auditoría destinado a la recepción por protocolo *syslog* y otro archivo destinado a la recepción por protocolo SETP.

154. Se dispone de un número limitado de archivos de auditoría, que puede ser ampliado por un usuario del sistema operativo administrador de NGSIEM LogICA5. NGSIEM LogICA5 se encarga de la funcionalidad de rotación, sobrescribe los archivos más antiguos por archivos nuevos cuando no hay más espacio disponible. Estos registros de auditoría pueden ser visualizados, seleccionados y ordenados por los usuarios del sistema operativo, empleando herramientas del sistema operativo del entorno operacional de NGSIEM LogICA5. Su ubicación se encuentra en los directorios */ica/logs/lsetp.log*, para la recepción de líneas de log e */ica/logs/lsyslog.log*, para la recepción de eventos de seguridad.

155. El módulo de servidores de *frontend* almacena los registros de auditoría en el módulo sistema de almacenamiento primario del entorno operacional. Estos registros de auditoría son visualizados, únicamente, por usuarios de *frontend* administradores de NGSIEM LogICA5 que dispongan de un rol con la sección de acceso *view/audit*.

156. Esta autorización permite la consulta, selección y ordenado de registros de auditoría por rango de fechas, sujeto que inició el evento y tipo de registro, y configurar, un número máximo de registros de auditoría.

157. Si se aproxima o se supera el límite de registros de auditoría, NGSIEM LogICA5 genera registros de auditoría (80%, 90% y 100% de alcance de umbrales). Si se sobrepasa el límite, se sobrescribe los registros más antiguos.

158. Se auditan los siguientes tipos de eventos:

- Arranque y parada de las funciones de auditoría.
- Mecanismos de autenticación con los usuarios de frontend.
- Mecanismos de identificación para el control de acceso por segregación en secciones o datos de seguridad.
- Modificaciones en las funciones de gestión: consulta, alta, baja y modificación de usuarios de frontend o roles.
- Expiración de la sesión por inactividad.
- Notificación: 80%, 90% y 100% de alcance de umbrales en el tamaño del espacio de memoria reservado a los registros de auditoría.
- Modificación en el tamaño máximo reservado de registros de auditoría.

159. Por cada registro de auditoría NGSIEM LogICA5 se almacena la fecha y hora, tipo de evento, entidad que inició el evento y el resultado (exitoso o fallido).

6.12 BACKUP

160. A continuación, se detalla el procedimiento de *backup* de los módulos del entorno de aplicación.

161. El almacenamiento destinado como *backup* no está incluido en el dimensionamiento del espacio de almacenamiento para la operación del producto. Se trata de un almacenamiento adicional proporcionado por el propietario de la licencia, cuyo punto de montaje será */ica/data/backup/*.

162. Para realizar la copia de seguridad del módulo bus de *streaming* y procesado, seguir los siguientes pasos. Los usuarios administradores del sistema operativo deben **realizar manualmente las siguientes configuraciones o emplear una herramienta de gestión de copias de seguridad**:

- Emplear el usuario *root* para realizar las configuraciones.
- En el servidor destinado a *NGIEM LogICA5*, guardar las salvaguardas en el directorio */ica/data/backup.*
- Se recomienda emplear compresión *gzip* estándar, u otro tipo de compresión, dependiendo del espacio de almacenamiento disponible.
- Se recomienda realizar un *backup* de los directorios de configuraciones, con una periodicidad diaria:

  /ica/logica5/node/resources/cep/rest/server/data/

  /ica/logica5/node/resources/logline/syslog/conf/

  /usr/lib/systemd/system/

  /etc/systemd/system/

  en la ubicación destino:

/ica/data/backup/daily/configurations-(yyyy-mm-dd).gz

- Se recomienda realizar un *backup* de los directorios de almacenamiento secundario, logroot, con una periodicidad diaria. Directorio correspondiente al día actual:

  /ica/data/logroot/(yyyy-mm-dd)

  en la ubicación destino:

  /ica/data/backup/daily/logroot-(yyyy-mm-dd).gz

- Adicionalmente, se recomienda realizar mensualmente y con una retención de 12 meses (12 copias), la copia de seguridad de las salvaguardas diarias del mes anterior en un único fichero, según el tipo de recurso:
  - *Backup* mensual de directorios de configuraciones en el destino */ica/data/backup/monthly/configurations-(yyyy-mm).gz*
  - *Backup* mensual de almacenamiento secundario, *logroot*, en el destino /ica/data/backup/monthly/logroot-(yyyy-mm).gz
- Realizar también, anualmente y con una retención de 5 años (5 copias), la copia de seguridad de las salvaguardas mensuales del año anterior en un único fichero, según el tipo de recurso.
  - *Backup* anual de directorios de configuraciones en el destino */ica/data/backup/yearly/configurations-(yyyy).gz*
  - *Backup* anual de almacenamiento secundario, *logroot*, en el destino */ica/data/backup/monthly/logroot-(yyyy).gz*

163. Para realizar la copia de seguridad del módulo de servidores de *frontend*, se deben seguir los siguientes pasos. Los usuarios administradores del sistema operativo deben **realizar las siguientes configuraciones manualmente o emplear una herramienta de gestión de copias de seguridad**:

- Emplear el usuario *root* para realizar las configuraciones.
- En el servidor destinado a *NGIEM LogICA5*, guardar las salvaguardas en el directorio */ica/data/backup.*
- Se recomienda emplear compresión *gzip* estándar, u otro tipo de compresión dependiendo del espacio de almacenamiento disponible.
- Se recomienda realizar un b*ackup* de los directorios de configuraciones, con una periodicidad diaria:

  /ica/logica5/data

  en la ubicación destino:

  /ica/data/backup/daily/configurations-(yyyy-mm-dd).gz

- Se recomienda realizar, con una periodicidad diaria, un *backup* de la base de datos, las colecciones funcionales y del almacenamiento primario. El

nombre de la base de datos será aquel configurado en el fichero *suite.properties* visto anteriormente (por defecto *logicacfg*).

- Utilizar el comando *mongodump*.

  mongogodump <host:puerto><datos de autenticación> <base de datos> <directorio de salida>

  ```
  mongodump –-host localhost:27017 –ssl –sslAllowInvalidCertificates –authenticationDatabase admin –u admin –p <password>---–db logicacfg
  ```

  La contraseña se corresponde al usuario de autenticación, ver apartado 6.3 Autenticación.

- La salida se almacena en el directorio por defecto, en la misma ruta *dump*. Mover la copia al directorio destino:

  /ica/data/backup/daily/ddbb-configurations-(yyyy-mm-dd).gz

- Adicionalmente, se recomienda realizar mensualmente y con una retención de 12 meses (12 copias), la copia de seguridad de las salvaguardas diarias del mes anterior en un único fichero, según el tipo de recurso:
  - *Backup* mensual de directorios de configuraciones en el destino */ica/data/backup/monthly/configurations-(yyyy-mm).gz*
  - *Backup* mensual de directorios de base de datos en el destino */ica/data/backup/monthly/ddbb-configurations(yyyy-mm).gz*
- Realizar también, anualmente y con una retención de 5 años (5 copias), la copia de seguridad de las salvaguardas mensuales del año anterior en un único fichero, según el tipo de recurso.
  - *Backup mensual de directorios de configuraciones en el destino /ica/data/backup/monthly/configurations-(yyyy-mm).gz z*
  - *Backup* mensual de directorios de base de datos en el destino */ica/data/backup/monthly/ddbb-configurations(yyyy-mm).gz*

7. FASE DE OPERACIÓN

7.1 MANTENIMIENTO

164. Los usuarios de *frontend* administradores de NGSIEM LogICA5 deben tener en cuenta las siguientes funciones y respuestas a situaciones relacionadas con los registros de auditoría:

- Administrar el tamaño de memoria reservado a los registros de auditoría (límite máximo de registros de auditoría).
- Aumentar el tamaño (por defecto de 5.000.000 de registros de auditoría) si es necesario por requisitos de retención de evidencias. El cálculo dependerá de la interacción de los usuarios con NGSIEM LogICA5 a través de los servidores de Frontend. Si se supera el umbral máximo, los registros más antiguos son sobrescritos.
- Filtrar y consultar los registros de auditoría para la detección de accesos no autorizados, y en general, situaciones que intenten vulnerar la seguridad de las funciones de seguridad.

165. Los usuarios de *frontend* administradores de NGSIEM LogICA5 deben realizar las siguientes funciones y respuestas:

- Arranque y parado de las rutas de proceso (ver apartado 6.2.2.1.2 COMPONENTES DE RECOLECCIÓN Y PROCESAMIENTO) o topologías del módulo: bus de streaming y procesado en tiempo real.
- Gestión de rutas de proceso.
- Gestión de la configuración de fuentes de *syslog*.
- Gestión de reglas de correlación y su aplicación a la ruta de proceso de eventos de seguridad.
- Gestión de activos.
- Gestión de incidentes.
- Planificación de tareas.

166. Los usuarios de *frontend* asignados al rol de operador, a su vez, deben realizar, tareas de análisis y revisión:

- Revisar el correcto funcionamiento de las rutas de proceso del subsistema: bus de *streaming* y procesado en tiempo real.
- Revisar los eventos de correlación, y posibles situaciones de seguridad comprometida dentro del entorno de monitorización de los sistemas cedentes.
- Consultar fuentes de líneas de log y eventos de seguridad.
- Consultar activos

- Consultar incidentes.

167. Los usuarios administradores del sistema operativo deben realizar las siguientes funciones:

- Ejecución, seguimiento y control de backups.
- Ejecución de actualizaciones.
- Gestión de contraseñas.
- Administración de usuarios en el módulo del bus de streaming y procesado.
- Gestión de los certificados de los sistemas cedentes.
- Actualización de configuraciones en todos los módulos.

8. REFERENCIAS[3]

REF1 *LogICA5-GuiaOperacion*

REF2 *LogICA5-GuiaInstalacion*

REF3 *LogICA5-GuiaUsuario*

REF4 *LogICA5-GuiaUsuarioMonitor*

REF5 *LogICA5-Recepcion*

REF6 *LogICA5-Distribucion*

REF7 *LogICA5-7.1-Resumen*

[3] Las guias referenciadas forman parte de la entrega de NGSIEM LogICA5, que son proporcionadas por el fabricante en la adquisición de la licencia de uso.

9. ABREVIATURAS

AES	*Advanced Encryption Standard. Sistema criptográfico de clave simétrica*
CA	*Certification Authority*
CC	*Common Criteria*
CCN	*Centro Criptológico Nacional*
CMDB	*Configuration Management Database*
GRUB	*Grand Unified Bootloader*
HDFS	*Hadoop Distributed File System*
HTTPS	*Hypertext Transfer Protocol Secure*
IOC	*Indicator of Compromise*
IPMI	*Intelligent Platform Management Interface*
JSON	*JavaScript Object Notation*
LDAP	*Lightweight Directory Access Protocol*
LVM	*Logical Volume Management*
NTP	*Network Time Protocol*
PV	*Physical Volume*
REST	*Representational State Transfer*
RSA	*Sistema criptográfico de clave pública. Sistema criptográfico asimétrico*
SETP	*Security Event Transfer Protocol*
SHA	*Secure Hash Algorithm*
TCP	*Transmission Control Policy*
TLS	*Transport Layer Security*
TOE	*Target of Evaluation*
UDP	*User Datagram Protocol*
UEBA	*User and Entity Behavior Analytics*
VRRP	*Virtual Router Redundancy Protocol*
X509	*Estándar para infraestructuras de clave pública.*