

Procedimiento de Empleo Seguro SPLUNK



Junio 2026

Edita:



Centro Criptológico Nacional, 2026



CCN
c=ES, l=MADRID, o=CCN,
ou=SELLO ELECTRONICO,
2.5.4.97=VATES-S2800155J,
serialNumber=S2800155J,
cn=CCN
2026.06.11 13:23:24 +02'00'

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	3
2 OBJETO Y ALCANCE	4
3 ORGANIZACIÓN DEL DOCUMENTO	5
4 FASE PREVIA A LA INSTALACIÓN	6
4.1 ENTREGA SEGURA DEL PRODUCTO	6
4.2 ENTORNO DE INSTALACIÓN SEGURO	6
4.3 REGISTRO Y LICENCIAS	6
4.4 CONSIDERACIONES PREVIAS.....	6
4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN	6
5 FASE DE INSTALACIÓN	8
5.1 PREREQUISITOS	8
5.2 INSTALACIÓN	9
6 FASE DE CONFIGURACIÓN.....	10
6.1 MODO DE OPERACIÓN SEGURO	10
6.1.1 PROTECCIÓN DE LA INFORMACIÓN	10
6.2 AUTENTICACIÓN	11
6.3 SERVIDORES DE AUTENTICACIÓN	11
6.4 ADMINISTRACIÓN DEL PRODUCTO.....	12
6.4.1 ADMINISTRACIÓN LOCAL Y REMOTA	12
6.4.2 CONFIGURACIÓN DE ADMINISTRADORES.....	13
6.5 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS	14
6.6 CONFIGURACIÓN DE PROTOCOLOS SEGUROS.....	15
6.7 GESTIÓN DE CERTIFICADOS	16
6.8 SINCRONIZACIÓN	16
6.9 ACTUALIZACIONES.....	16
6.10 AUTO-CHEQUEOS	17
6.11 ALTA DISPONIBILIDAD	18
6.12 AUDITORÍA	18
6.12.1 REGISTRO DE EVENTOS.....	18
6.13 BACKUP	19
6.14 FUNCIONES DE SEGURIDAD.....	19
7 FASE DE OPERACIÓN	21
8 REFERENCIAS	22
9 ABREVIATURAS	23

1 INTRODUCCIÓN

1. Splunk Enterprise es una solución de SIEM que permite gestionar el ciclo completo de seguridad en una organización, incluyendo capacidades de Detección, Monitorización, Investigación y Respuesta ante incidentes de Seguridad. Incorpora capacidades de búsqueda y generación de informes sin precedentes, análisis avanzados, inteligencia artificial integrada y contenido de seguridad predefinido y dinámico para acelerar la detección e investigación de amenazas.
2. Splunk permite clasificar por prioridad los incidentes, priorizando los incidentes que afecten a activos o identidades críticos. Permite generar alertas basadas en riesgo, identificando anomalías y amenazas tanto externas como internas. Las más de 2500 reglas de detección predefinidas por el fabricante abarcan todos los ámbitos de seguridad: IT, OT, IoT, IoMT y las nubes públicas en cualquiera de sus formatos.
3. Algunas de sus características principales son:
 - Indexación: Splunk Enterprise puede recopilar datos de dispositivos y aplicaciones como sitios web, servidores, bases de datos, sistemas operativos y más. Una vez que se recopilan los datos, el índice segmenta, almacena, comprime los datos y mantiene los metadatos de apoyo para acelerar la búsqueda.
 - Búsquedas: La búsqueda es la forma principal en que los usuarios navegan por sus datos en Splunk Enterprise. Puede guardar una búsqueda como informe y utilizarla para potenciar los dashboard panels.
 - Alertas: Las alertas le notifican cuando los resultados de búsqueda, tanto históricos como en tiempo real, cumplen las condiciones configuradas. Puede configurar alertas para desencadenar acciones.
 - Dashboards: Los paneles del tablero generalmente están conectados a búsquedas guardadas o pivotes. Muestran los resultados de búsquedas completadas y datos de búsquedas en tiempo real que se ejecutan en segundo plano.
 - Informes: Splunk Enterprise le permite guardar búsquedas y pivotes como informes y luego agregar informes a los tableros como paneles de tablero.
 - Modelo de datos: Los modelos de datos codifican conocimiento de dominio especializado sobre uno o más conjuntos de datos indexados. Permiten a los usuarios de *Pivot Editor* crear informes y paneles sin diseñar las búsquedas que los generan.

2 OBJETO Y ALCANCE

4. El objeto del presente documento es servir como guía para realizar una instalación y configuración segura de la solución Splunk Enterprise 9.4.
5. El producto Splunk Enterprise 9.4 ha sido incluido en el catálogo de productos y servicios STIC (CPSTIC) y para consultar el listado, categoría o nivel y familia consulte: <https://cpstic.ccn.cni.es/es/catalogo-productos-servicios-stic>.

3 ORGANIZACIÓN DEL DOCUMENTO

- a) Apartado 4. En este apartado se recogen aspectos y recomendaciones a considerar, antes de proceder a la instalación del producto.
- b) Apartado 5. En este apartado se recogen recomendaciones a tener en cuenta durante la fase de 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 o mantenimiento del producto.

4 FASE PREVIA A LA INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

6. Splunk Enterprise es un producto software y la descarga de este se realiza a través de la propia web de Splunk (**REF1**), se debe registrar en la web de Splunk antes de poder descargar la versión del producto.
7. Se debe comprobar la integridad de los archivos de la instalación de Splunk. Para ello, se proporciona un hash MD5 y un hash SHA-512. Sin embargo, para una verificación segura, se debe utilizar el hash SHA-512. La comprobación se debe llevar a cabo siguiendo estos pasos:
 - Descargar el archivo de instalación de Splunk.
 - Generar el hash SHA-512 del archivo.
 - Comparar el hash SHA-512 facilitado por Splunk y verificar que coinciden.

4.2 ENTORNO DE INSTALACIÓN SEGURO

8. El entorno físico donde opera el producto debe asegurar que todos los componentes estén protegidos de cualquier ataque físico, por lo que se recomienda instalar el software 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.

4.3 REGISTRO Y LICENCIAS

9. El producto requiere la instalación de licencias de uso para su correcto funcionamiento. Existen distintos tipos de licencias disponibles, el detalle de licenciamiento del producto se puede consultar en el apartado de configuración de licencias de Splunk Admin (**REF2**).

4.4 CONSIDERACIONES PREVIAS

10. Las consideraciones previas a una instalación del producto se pueden consultar en el documento de Instalación de Splunk (**REF3**).
11. Adicionalmente Splunk posee documentación que contempla todos los sistemas operativos soportados, donde se describe los elementos para tener en cuenta y sus funcionalidades. Ver documentación de System Requirements Splunk (**REF4**).

4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN

12. En la documentación de System Requirements Splunk (**REF4**) se pueden ver todos los sistemas operativos y distribuciones soportadas por la arquitectura del producto.
13. A modo general Splunk Enterprise consta de los siguientes componentes:

- Fuente de eventos: Sistemas externos al producto que generan datos (por ejemplo, registros de eventos, logs de aplicaciones, sistemas operativos, dispositivos de red o soluciones de seguridad) y que son recopilados por Splunk Enterprise para su procesamiento e indexación. Estas fuentes de datos no forman parte del producto y pueden transmitir la información mediante distintos mecanismos (ficheros, syslog, APIs, etc.), normalmente a través de canales protegidos mediante TLS, ya sea de forma directa o a través de componentes de recolección de Splunk.
- Recolector de datos (Forwarder): Componente de Splunk Enterprise encargado de la recolección y envío de datos desde las fuentes de eventos hacia los componentes de indexación del producto. Habitualmente se implementa como Splunk Universal Forwarder, una instancia ligera diseñada exclusivamente para la ingesta y el reenvío de datos. La comunicación entre el forwarder y otros componentes de Splunk Enterprise se realiza mediante canales cifrados TLS, conforme a la configuración de seguridad del producto.
- Componente de indexación (Indexer): Componente central del producto encargado del almacenamiento, indexación y gestión de los datos recopilados. Este componente permite la persistencia de los registros de auditoría y eventos de seguridad, así como su posterior consulta y correlación. En despliegues distribuidos, puede implementarse mediante clústeres de indexadores para garantizar la alta disponibilidad y la integridad de los datos.
- Plataforma Host: Un servidor de propósito general en el que está instalado el sistema operativo Linux y el producto. El producto requiere recursos de red de la plataforma host.
- Estación de trabajo de gestión: Cualquier ordenador de propósito general utilizado por un administrador de seguridad para gestionar el producto de forma remota a través de un navegador web. Tener en cuenta que la plataforma host también puede utilizarse para administrar el producto localmente.
- Servidor SMTP: Servidor de correo electrónico que puede recibir alertas del producto y enviarlas a los usuarios del entorno operativo por correo electrónico.
- Punto de distribución CRL: Servidor que proporciona listas de revocación actualizadas para la funcionalidad de validación de certificados del producto.

5 FASE DE INSTALACIÓN

14. En este apartado se describe cómo llevar a cabo la instalación de Splunk Enterprise en modo seguro.

5.1 PREREQUISITOS

15. Antes de proceder a la instalación del producto, es necesario realizar una serie de acciones previas con el fin de asegurar que el entorno cumple con los requisitos de seguridad recomendados de acuerdo con el ENS (Esquema Nacional de Seguridad) y normativa desarrollada por el CCN (Centro Criptológico Nacional).
16. Sistema operativo y arquitectura:
 - Splunk Enterprise deberá instalarse sobre un sistema operativo compatible y soportado por el fabricante, preferentemente en entornos Linux para despliegues de producción. Los sistemas operativos compatibles pueden consultarse en el documento Instalación de Splunk (**REF4**).
 - La plataforma deberá utilizar arquitectura x86_64.
 - El sistema operativo deberá encontrarse correctamente instalado y actualizado.
17. Recursos del Sistema:
 - El sistema deberá disponer de recursos suficientes de CPU, memoria, almacenamiento y red, dimensionados de acuerdo con el rol que desempeñará la instancia. La información sobre los recursos necesarios puede encontrarse en el documento Instalación de Splunk (**REF4**), en la sección *System requirements for use of Splunk Enterprise on-premises*.
 - La planificación de capacidad deberá tener en cuenta el volumen de datos a indexar y el número de usuarios concurrentes.
18. Usuario y permisos:
 - La instalación del producto requiere privilegios de administrador del sistema.
 - Una vez instalado, el servicio de Splunk Enterprise podrá ejecutarse bajo un usuario específico de servicio del sistema operativo, conforme a la configuración definida por el administrador.
19. Dependencias y entorno de ejecución:
 - Splunk Enterprise incluye y gestiona sus propias dependencias internas necesarias para su funcionamiento.
 - El sistema deberá disponer de las librerías básicas requeridas por el sistema operativo para la ejecución de aplicaciones servidor.
20. Conectividad de red:
 - El sistema deberá disponer de conectividad de red adecuada para permitir:

- El acceso a la interfaz web de administración.
- La comunicación con otras instancias de Splunk Enterprise en despliegues distribuidos.
- Los puertos necesarios deberán estar disponibles y correctamente filtrados conforme a la política de red del entorno. Esta información se puede encontrar en el documento Splunk Security (**REF6**), en la sección *Install Splunk Enterprise Securely* > *Secure Splunk Enterprise on your Network*.

5.2 INSTALACIÓN

21. Una vez verificados los prerequisites, se procederá a la instalación de Splunk Enterprise siguiendo los pasos indicados a continuación.
22. El paquete de instalación deberá descargarse desde los canales oficiales del fabricante, garantizando la integridad y autenticidad del software.
23. En sistemas Linux compatibles, se instalará utilizando el paquete RPM oficial proporcionado por el fabricante.
24. La instalación se realizará con privilegios de administrador del sistema mediante el gestor de paquetes correspondiente.
25. Durante la instalación, los binarios del producto se copiarán en la ubicación estándar definida por Splunk.
26. Tras la instalación del paquete, el servicio deberá inicializarse para completar la instalación.
27. En el primer arranque del producto:
 - Se aceptarán los términos de licencia.
 - Se creará la cuenta administrativa inicial del producto.
28. Una vez inicializado, Splunk Enterprise habilita su interfaz web de administración para la gestión del producto.
29. El acceso inicial se realiza mediante el navegador web, utilizando las credenciales del usuario administrativo configurado.
30. A partir de este momento, el producto queda listo para la configuración específica del entorno (roles, indexación, seguridad, etc.).

6 FASE DE CONFIGURACIÓN

6.1 MODO DE OPERACIÓN SEGURO

31. Se debe emplear el producto en el modo de operación seguro. Para ello se debe activar el modo seguro, antes de la conexión del sistema a la red, con el fin de evitar ventanas de exposición en configuración no endurecida. Por ello, antes del primer arranque productivo se deben incluir las siguientes modificaciones en el archivo de configuración `/etc/opt/Splunk/Splunk-launch.conf`:

```
SPLUNK_COMMON_CRITERIA=1
SPLUNK_FIPS=1
#Do not generate Python byte code
PYTHONDONTWRITEBYTECODE=1
```

6.1.1 PROTECCIÓN DE LA INFORMACIÓN

32. Se deberá configurar el entorno de ejecución del producto para proteger la información en reposo mediante el cifrado de los datos, (para más información, consultar el documento Splunk para Common Criteria (**REF5**)) Para ello, se deben seguir los siguientes pasos:

33. Iniciar el proceso dbus:

```
sudo sh /home/splunk/run_dbus.sh
```

34. Asegurar que se establezcan las variables de entorno ejecutando el siguiente comando:

```
source /home/splunk/.bashrc
```

35. Inicializar la contraseña del “almacenamiento secreto”:

```
runcon -u system_u -t splunk_t -r system_r splunk secret-storage -unlock
```

36. Ver la lista de claves disponibles:

```
runcon -u system_u -t splunk_t -r system_r splunk secret-storage --spec
```

37. Para añadir claves al almacenamiento seguro del sistema, emplear el siguiente comando:

```
runcon -u system_u -t splunk_t -r system_r splunk secret-storage --write
--no-prompt <passphrase>
```

38. El uso de GNOME Keyring y de los contextos de seguridad indicados aplica a entornos Linux compatibles con la implementación Common Criteria del fabricante (**REF5**).
39. En caso de emplear otras distribuciones Linux o configuraciones distintas del sistema operativo, se deberá consultar la documentación oficial de Splunk correspondiente al entorno específico para garantizar que el mecanismo de almacenamiento seguro cumple los requisitos de seguridad establecidos.

6.2 AUTENTICACIÓN

40. Se deberá llevar a cabo la correcta configuración de los certificados, ya que estos serán empleados para la autenticación interna de los distintos componentes del producto. Dicha configuración se puede consultar en el apartado 6.7 GESTIÓN DE CERTIFICADOS.
41. Para permitir que un usuario acceda a los servicios y recursos ofrecidos por Splunk, el producto dispone de distintos esquemas de autenticación (para más información, consultar el documento Splunk Security (**REF6**)). Cabe destacar que, para que la autenticación sea efectiva, es necesario que exista una licencia activa. A continuación, se listan los esquemas de autenticación:
 - Autenticación local de Splunk mediante usuario y contraseña. Es el esquema por defecto y tiene prioridad sobre cualquier esquema de autenticación externo.
 - LDAP. Soporta la autenticación con sus servicios de autenticación internos o con su servidor LDAP existente.
 - SAML. Soporta el contacto con un IdP que utilice SAML en su versión 2.0 y recuperar la información del usuario que puede asignarse a roles de Splunk.
 - Multi-factor. Permite el uso de dos o más servicios de autenticación e incluye la capacidad de utilizar Duo o RSA Manager.
 - Scripted Authentication API. Permite el uso de autenticación mediante script para integrar la autenticación de Splunk con un sistema de autenticación externo como RADIUS o PAM.
 - Autenticación con JWT Tokens.
 - Autenticación mediante un proxy single sign-on.
 - Autenticación mediante un reverse proxy single sign-on.
42. El método de autenticación deseado se seleccionará durante la creación de usuarios.

6.3 SERVIDORES DE AUTENTICACIÓN

43. En el documento Splunk Security (**REF6**) se puede consultar en detalle la configuración de los distintos servidores de autenticación externos soportados por Splunk.

44. Se dispone de los siguientes:

- Autenticación LDAP, descrita en la sección *Use LDAP as an authentication scheme*. En caso de emplear LDAP, se deberán activar y configurar los siguientes parámetros para asegurar el empleo de TLS en la autenticación de usuarios:
 - En el servidor, el parámetro TLSVerifyClient deberá establecerse en el valor demand de las opciones propuestas, de modo que se exija la validación obligatoria del certificado del cliente y se impida el establecimiento de conexiones sin autenticación mutua:

TLSCACertificateFile, TLSCertificateKeyFile, TLSCipherSuite, TLSRandFile, TLSEphemeralDHParamFile, TLSVerifyClient [never | allow | try | demand]

- En el cliente, el parámetro TLS_REQCERT deberá configurarse con el valor demand de las opciones propuestas, para asegurar que el certificado del servidor LDAP sea validado obligatoriamente y evitar conexiones TLS sin verificación:

TLS_KEY, TLS_RANDFILE, TLS_REQCERT [never | allow | try | demand]

- Autenticación SAML, descrita en la sección *Use SAML as an authentication scheme for single sign-on*. Se deberán seguir los pasos indicados en el apartado Secure SSO with TLS certificates on Splunk Enterprise, para asegurar las operaciones SSO mediante TLS.
- Autenticación multifactor, descrita en la sección *Use multi-factor authentication in Splunk Enterprise as an authentication scheme*.
- Autenticación usando Tokens, descrita en la sección *Authenticate into the Splunk platform with tokens*.
- Autenticación usando ProxySSO, descrita en la sección *Authenticate into the Splunk platform using proxy single sign-on*.
- Autenticación usando SSO con un reverse proxy, descrita en la sección *Authenticate into Splunk Enterprise using single sign-on with reverse proxy*.
- Autenticación usando scripts (PAM, RADIUS) descrita en la sección *Authenticate into Splunk Enterprise using scripts*.

6.4 ADMINISTRACIÓN DEL PRODUCTO

6.4.1 ADMINISTRACIÓN LOCAL Y REMOTA

45. El producto dispone de las siguientes interfaces de administración:

- Administración remota de tipo GUI, mediante acceso web. Este acceso web se realizará de forma segura mediante el uso de TLS 1.2 o superior.
- Mediante el uso de los archivos de configuración alojados en el directorio de instalación de Splunk, descritos en el apartado. Esta administración puede ser vía remota usando SSHv2 o local desde la propia consola del sistema operativo.

- Administración local y remota (empleando SSHv2) por consola de tipo CLI. La sintaxis que se debe seguir para hacer uso de la consola CLI es la siguiente:

```
/splunk <command> [<object>] [[-<parameter>] <value>]
```

46. Se recomienda emplear la administración remota de tipo GUI o la administración de tipo CLI para gestionar y configurar el producto.

6.4.2 CONFIGURACIÓN DE ADMINISTRADORES

47. El producto dispone de los siguientes roles predeterminados:
- Admin: dispone de todos los permisos.
 - Power: permite editar todos los objetos compartidos y alertas.
 - User: permite crear, editar y ejecutar búsquedas.
 - SC_admin: se emplea para crear otros usuarios y roles, pero no dispone de otros permisos administrativos.
48. Sin embargo, permite la creación de roles personalizados, pudiendo configurar así los permisos específicos de los distintos usuarios. Esto se puede realizar modificando el fichero authorize.conf desde la interfaz CLI o en la interfaz GUI desde Settings > Roles.
49. Durante la creación de usuarios se deberán especificar su rol y el método de autenticación (parámetro Authentication system). Al crear un usuario se le asigna una contraseña, por lo que se deberá activar el parámetro Require password to change on first login, de tal forma que deba modificarse la contraseña al acceder por primera vez. Todas las contraseñas deberán cumplir con la política de contraseñas definida a continuación.
50. Se deberá configurar la Política segura de contraseñas para cumplir con el ENS. Para ello desde Splunk Web ir a Settings > Password Management. Deberán configurarse los siguientes parámetros:
- *Minimum Characters*: longitud mínima de la contraseña de doce (12) caracteres.
 - *Numerals*: número de dígitos requeridos de, al menos, 1.
 - *Lowercase*: número de minúsculas requeridas de, al menos, 1.
 - *Uppercase*: número de mayúsculas requeridas de, al menos, 1.
 - *Special Character*: número de caracteres especiales requeridos de, al menos, 1.
 - Marcar la opción *Force existing users to change weak passwords* para obligar a los usuarios existentes a modificar las contraseñas en caso de no cumplir con la política definida.
 - Habilitar el campo *History* y asignar el campo *Password History Count* a un valor igual a 5 o superior, para prevenir el uso de las últimas 5 contraseñas.
 - Activar la casilla *Expiration* para forzar a los usuarios a cambiar las contraseñas tras un tiempo definido en el parámetro *Days until password expires*: asignar un valor de 60 o inferior.

- Activar la casilla Lockout para permitir el bloqueo de cuentas. Asignar el campo *Failed login attempts* a un valor de 3 o inferior. Tras el número de fallos de autenticación definidos se bloqueará la cuenta.
 - Asignar el campo *Lockout duration in minutes* a un valor de 5 o superior, para definir el tiempo de bloqueo.
51. Se deberá configurar el tiempo de inactividad de las sesiones de los usuarios en cinco (5) minutos. Para ello se debe modificar el archivo de configuración `authentication.conf` y asignar el valor `timeout` a 300.
 52. El detalle de creación y configuración de usuarios y roles se puede consultar en el apartado *Manage users and roles* de la guía Splunk Security (REF6).
 53. Por último, el administrador deberá definir de forma procedimental el número de días que deben transcurrir tras el cambio de una contraseña antes de poder modificarla de nuevo en diez (10) días.

6.5 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

54. En el documento Splunk Security (REF6) se describe la configuración de interfaces, puertos y servicios de forma segura de Splunk Enterprise en la sección *Install Splunk Enterprise Securely > Secure Splunk Enterprise on your Network*.
55. Se recomienda deshabilitar aquellos componentes de Splunk que no vayan a ser utilizados para reducir el número de ataques potenciales, se puede consultar el detalle en el apartado *Disable unnecessary Splunk Enterprise components* del documento Splunk Security (REF6). A continuación, se detallan algunos de ellos.
56. Deshabilitar componentes innecesarios de Splunk Enterprise en implementaciones de Splunk Enterprise de un solo servidor:
 - Si es posible, no ejecutar Splunk Web en Universal Forwarders de ningún tipo.
 - En las instancias configuradas como Splunk Universal Forwarder, no deberán habilitarse servicios de recepción de datos (por ejemplo, puertos TCP/UDP de escucha) salvo que la arquitectura del despliegue lo requiera expresamente. En escenarios en los que el Universal Forwarder únicamente recoja logs locales y los envíe a un indexer, no será necesario mantener puertos de entrada abiertos, pudiendo bloquearse el tráfico entrante mediante las reglas de cortafuegos del sistema operativo o de red. En caso de requerirse recepción de eventos (por ejemplo, recepción de syslog o forwarding intermedio), únicamente se habilitarán los puertos estrictamente necesarios y protegidos mediante TLS.
57. Deshabilitar componentes innecesarios de Splunk Enterprise en implementaciones de Splunk Enterprise de múltiples servidores:
 - Si es posible, deshabilitar cualquier configuración que permita que los Search heads reciban datos en puertos de red TCP o UDP o desde otras instancias de Splunk Enterprise.
 - Si los usuarios no inician sesión en Splunk Web en los indexers en un entorno distribuido, desactivar Splunk Web en esos indexers.

58. En una instalación distribuida con varios servidores, se puede deshabilitar Splunk Web en aquellos servidores donde no se emplee, siguiendo los siguientes pasos:

- En la barra del sistema, seleccionar Setting > Server Settings.
- Seleccionar General Settings.
- En la sección Splunk Web, en el botón Run Splunk Web, seleccionar No.
- Hacer clic en Save.
- Reiniciar la instancia de Splunk Enterprise.

6.6 CONFIGURACIÓN DE PROTOCOLOS SEGUROS

59. Se debe realizar una configuración segura de TLS. Este proceso es detallado en la sección *About TLS encryption and cipher suites* del documento Splunk Security (REF6):

- Acudir al directorio `/etc/opt/splunk/system/local` donde se ubican los ficheros de configuración.
- En los archivos `server.conf`, `web.conf`, `outputs.conf`, `inputs.conf` y `alerts_actions.conf` editar las siguientes líneas de código para emplear únicamente ciphersuites seguras y la versión 1.2 de TLS:

```
cipherSuite = ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-
GCM_SHA256:ECDHE-ECDSA-AES256-SHA384
sslVersions = tls1.2
```

- En el archivo `authentication.conf`, editar la siguiente línea de código:

```
[secrets]
disabled = false
```

- Guardar la configuración y cerrar los ficheros.
- Reiniciar Splunk Enterprise para que los cambios tomen efecto.

60. Se debe configurar el producto para evitar el empleo de HTTP en las comunicaciones con el servidor web y emplear únicamente el HTTPS:

- Abrir el fichero de configuración `web.conf`.
- En settings, asignar un puerto http y asignar `SplunkWebSSL` a true.

```
[settings]
httpport = <https port number>
enableSplunkWebSSL = true
```

- Reiniciar Splunk Enterprise.
- Tras reiniciar, para acceder a la instancia de Splunk Web utilizar `https://<your site name>:<port>`.

61. La configuración del protocolo SSH la lleva a cabo el sistema operativo donde reside el producto. Se deberá asegurar que únicamente se habilite SSHv2 y que se deshabiliten algoritmos criptográficos obsoletos.

6.7 GESTIÓN DE CERTIFICADOS

62. El detalle de configuración de los certificados se puede consultar en el documento Splunk Security (**REF6**) en el apéndice *Secure communications between Splunk Web and your browser*.
63. El producto emplea los certificados para asegurar las comunicaciones entre los siguientes componentes:
 - Comunicaciones entre el navegador web y el servidor web de Splunk para la gestión remota.
 - Comunicaciones entre los componentes internos del producto (forwarder e indexer).
 - Comunicaciones entre el producto y el servidor SMTP.
64. Se deberán seguir los siguientes pasos generales:
 - Importar el certificado de la CA que se utilizará para generar el certificado de servidor.
 - Crear un CSR (Certificate Signing Request). Se deberá utilizar uno de los siguientes parámetros para la creación del certificado:
 - Tipo de clave ECDSA, con un tamaño de 256 o 384 bits y algoritmo de firma SHA-384 o SHA-256
 - Importar el certificado de servidor una vez recibido.

6.8 SINCRONIZACIÓN

65. Se recomienda que todos los sistemas utilizados por la organización se encuentren sincronizados por medio de un mecanismo de tiempo NTP para permitir una alta fiabilidad en los sistemas de auditoría y logging. El producto recibe la hora del sistema operativo sobre el que se encuentre desplegado.

6.9 ACTUALIZACIONES

66. Las actualizaciones del producto deberán llevarse a cabo manualmente por un usuario administrador. Para ello, se deberán seguir los siguientes pasos:
 - Hacer clic en Update URL en la consola de gestión web.
 - Autenticarse en el portal de descargas y descargar manualmente el paquete .rpm.
 - Con permisos de administrador, ejecutar el comando `rpm -K` para verificar la autenticidad de la descarga empleando la clave pública de Splunk.

- Realizar la instalación del paquete con el comando `rpm -i fichero_descargado - nodeps`.

6.10 AUTO-CHEQUEOS

67. En el apartado Check the integrity of your Splunk Software files en el documento Splunk Admin (**REF2**) se describen los distintos procedimientos para verificar la integridad del producto.
68. Splunk ofrece la capacidad validar los archivos y detectar si ha habido alguna modificación no válida en el software de la plataforma. Esta comprobación se realiza automáticamente en el arranque y también puede llevarse a cabo de forma manual. Se mostrarán los resultados en la consola de monitorización, el detalle se puede consultar en Access and customize health checky en el documento de Splunk Admin (**REF2**).
69. Para llevar a cabo una validación manual, emplear el siguiente comando desde el directorio de instalación:

```
./splunk validate files
```

70. Esta comprobación manual se puede ejecutar con dos controles adicionales:
 - Es posible especificar al archivo mediante la descripción del archivo correcto utilizando la opción `-manifest` (es válido cualquier archivo manifest que se encuentre disponible).
 - Se puede limitar el test a archivos que terminen con `.conf` utilizando la opción `-type conf`.
71. En cuanto a la validación automática, esta se lleva a cabo en dos etapas:
 - Antes de iniciar el servicio `splunkd`, se lleva a cabo una validación preliminar. Esta validación solamente abarca los archivos de configuración por defecto y se muestra un mensaje en la terminal como resultado.
 - Una vez iniciado `splunkd`, la prueba de validación verifica todos los archivos proporcionados por Splunk Enterprise, incluyendo archivos de configuración, librerías, binarios, y archivos de datos. Los resultados se guardan en el archivo `splunkd.log`, y también se muestran los mensajes del boletín del sistema en la interfaz web de Splunk. La segunda etapa de la validación puede ser configurada en el archivo `limits.conf`.
72. La lectura de todos los archivos proporcionados con la instalación tiene un efecto moderado en el rendimiento de E/S. Si necesita reiniciar Splunk varias veces en un corto periodo de tiempo, es posible que sea necesario desactivar esta comprobación temporalmente para mejorar el rendimiento de E/S
73. Los archivos se validan contra el archivo manifest en el directorio de instalación. Si este archivo se elimina o altera, la comprobación puede no funcionar correctamente.

74. En caso de fallo en la validación de los archivos, el servicio no se iniciará indicando el error en el archivo Splunkd.log.

6.11 ALTA DISPONIBILIDAD

75. Splunk Enterprise emplea clusterización para proporcionar alta disponibilidad, esta puede ser aplicada no solo a la capa de indexado sino también a la capa de gestión y búsqueda. El detalle se puede consultar en el documento Splunk Deployment Manual (**REF77**).
76. En el documento Splunk Deployment Manual (**REF77**) en la sección High availability deployment: Indexer cluster se describe la instalación de un entorno de alta disponibilidad. Los pasos para implementarlo son los siguientes:
- Instalar las instancias necesarias de Splunk Enterprise siguiendo el procedimiento de instalación seguro de esta guía.
 - Desplegar el clúster de indexadores según lo indicado en el apartado *Indexer cluster deployment overview* del documento Manage Indexers and Indexer Clusters (**REF9**). No ha de aplicarse ningún parámetro específico de seguridad.
 - Si se desea, implementar un clúster de servidores de búsqueda consultar el apartado *Integrate the search head cluster with an indexer cluster* de Splunk Distributed Search (**REF88**).
 - Configurar la licencia de Splunk Enterprise.
 - Conectar los nodos pares a las fuentes de datos.

6.12 AUDITORÍA

6.12.1 REGISTRO DE EVENTOS

77. En el documento de Splunk Security (**REF6**) en la sección Audit activity in Splunk Enterprise se describe cómo se realiza el registro de las actividades del producto. El producto registra todos los eventos de seguridad relevantes.
78. Dentro de un evento de auditoría se encuentra la siguiente información:
- Marca de tiempo. Fecha y hora en la que sucedió el evento
 - Información de usuario. Quien generó el evento (si no tiene información de usuario, Splunk asigna el usuario a quien esté logueado en ese momento).
 - Información adicional. Detalles del evento, éxito/denegado, etc.
79. El producto almacena los registros de auditoría en el fichero \$SPLUNK_HOME/var/log/Splunk/Audit.log
80. Es posible realizar el envío de los registros a un servidor externo empleando TLSv1.2 como puede ser otro indexer dentro de una arquitectura distribuida, un clúster dedicado a la custodia de logs, un repositorio con retención inmutable o un SIEM jerárquico superior. Para ello es necesario configurar el producto como

un forwarder, de tal forma que reenviará los registros de auditoría junto al resto de eventos a la ubicación configurada.

81. Se recomienda configurar el reenvío de los registros a un servidor externo. Aunque los eventos locales deben indexarse y monitorizarse dentro del propio SIEM, la copia externa aporta una capa adicional de protección conforme a los principios de separación de funciones e integridad de los registros.

6.13 BACKUP

82. Se recomienda establecer copias de seguridad periódicas. El producto no dispone de un mecanismo de copias de seguridad, si no que se deberán copiar los archivos y directorios con la configuración del producto. Estos son los siguientes:
 - El directorio `$SPLUNK_HOME/etc/` y sus subdirectorios contiene toda la configuración para la instalación de Splunk, incluidas las búsquedas guardadas, las cuentas de usuario, las etiquetas y los nombres de tipo de origen personalizados, y todas las aplicaciones.
83. Se recomienda almacenar la copia de seguridad en una ubicación independiente, distinta al dispositivo en el que se despliega el producto.
84. En los siguientes documentos se pueden consultar los procedimientos técnicos detallados para la realización de copias de seguridad de los diferentes componentes de Splunk:
 - En el documento de Splunk Admin (**REF2**) sección *Splunk platform administration* se describen las copias recomendadas de los distintos componentes del producto. En la sección *Back up and restore KV store* se describe cómo hacer la copia de seguridad del componente KVStore.
 - En el documento Splunk Distributed Search (**REF8**) sección *Back up and archive your indexes* indica cómo realizar las copias de seguridad de los datos indexes.
 - En el documento Splunk Distributed Search (**REF8**) sección *Back up and restore search head cluster settings* indica cómo realizar las copias de los datos de *cluster*.

6.14 FUNCIONES DE SEGURIDAD

85. El documento Splunk Security (**REF6**) describe las capacidades de Splunk, así como las consideraciones a tener en cuenta en un despliegue para mantener la plataforma segura.
86. En el documento Forward and Process Data (**REF10**), en el apartado Deploy a heavy forwarder, se describe como configurar un Heavy Forwarder. Entre sus funcionalidades se encuentra el envío de eventos a un servidor remoto syslog mediante la funcionalidad de forwarding.
87. El reenvío de eventos desde un Heavy Forwarder intermedio se emplea en arquitecturas jerárquicas o federadas, donde un nodo local envía la información a un SIEM corporativo central, así como en escenarios de integración con terceros,

cumplimiento de requisitos regulatorios o contractuales, segmentación de red y necesidades de filtrado o normalización previa. El objetivo de este mecanismo es centralizar la monitorización y correlación, optimizar el volumen de datos mediante selección previa, garantizar interoperabilidad con infraestructuras basadas en syslog estándar y facilitar el cumplimiento normativo y la separación de responsabilidades en entornos multi-organización, aplicando controles de transformación antes del envío para mejorar la gobernanza del flujo de eventos.

88. Este ejemplo muestra cómo configurar un Heavy Forwarder para enviar datos desde hosts cuyos nombres comienzan con "nyc" a un servidor syslog llamado loghost.example.com a través del puerto 514:

- Editar props.conf y transforms.conf para especificar los criterios de filtrado.
- En props.conf, aplicar la transformación send_to_syslog a todos los nombres de host que comienzan con nyc:

```
[host::nyc*]  
TRANSFORMS-nyc = send_to_syslog
```

- En transforms.conf, configurar la transformación send_to_syslog para especificar _SYSLOG_ROUTING como DEST_KEY y el grupo de destino my_syslog_group como FORMAT:

```
[send_to_syslog]  
REGEX = .  
DEST_KEY = _SYSLOG_ROUTING  
FORMAT = my_syslog_group
```

- En outputs.conf, definir el grupo de destino my_syslog_group para el servidor noSplunk:

```
[syslog:my_syslog_group]  
server = loghost.example.com:514
```

- En las configuraciones indicadas en el apartado de CONFIGURACIÓN DE PROTOCOLOS SEGUROS, se exige el empleo de TLSv1.2 en todas las comunicaciones en las que Splunk actúe como forwarder, mediante el fichero outputs.conf.

7 FASE DE OPERACIÓN

89. El correcto funcionamiento del producto requiere de unas características que deben estar presentes en el entorno operacional:
- El producto debe contar con las últimas actualizaciones de seguridad para preservar al mismo de amenazas y vulnerabilidades conocidas.
 - Se deben mantener y analizar los registros de auditoría. Estos registros estarán protegidos de borrados y modificaciones no autorizadas, y solamente el personal de seguridad autorizado podrá acceder a ellos.
 - Se deben gestionar correctamente los certificados utilizados, actualizándolos cuando sea necesario, por ejemplo, al expirar.
 - Se deben realizar copias de seguridad de manera periódica.
90. Por otra parte, Splunk Enterprise ofrece dos modelos de monitorización para controlar el correcto uso del producto en fase de operación. La información sobre ambos modelos se puede encontrar en el documento Monitor (**REF11**):
- Consola de monitorización. Herramienta basada en búsqueda, diseñada para brindar a los usuarios información detallada sobre la topología y el rendimiento de su implementación. Incluye una serie de paneles preconstruidos que ofrecen visibilidad en áreas clave, como el rendimiento de búsqueda e indexación, el uso de recursos, el uso de licencias, etc. Los usuarios pueden aprovechar la Consola de Monitorización para hacer un seguimiento del estado de su implementación, independientemente del tipo de topología utilizada, desde implementaciones de una sola instancia hasta complejos clústeres de indexadores de varios sitios
 - Componente de monitorización pro-activa. Esta herramienta basada en REST de Splunk permite supervisar el estado de salud de las funcionalidades de una implementación de Splunk Enterprise. La monitorización se lleva a cabo a través de la salida de un punto de conexión REST API. Cada funcionalidad informa su estado de salud mediante una estructura de árbol que proporciona una vista continua y de alto nivel del estado de salud de la implementación. Hay dos opciones para acceder a la información del estado de salud de las funcionalidades. La primera opción es utilizar el informe de salud de splunkd disponible en Splunk Web. La segunda opción es acceder a la información del estado de salud directamente desde el punto de conexión `/server/health/splunkd`.

8 REFERENCIAS

- REF1** Descarga Splunk Enterprise
https://www.splunk.com/en_us/download.html
- REF2** Splunk Admin
<https://help.splunk.com/en/splunk-enterprise/administer/admin-manual/9.4>
- REF3** Instalación de Splunk
<https://help.splunk.com/en/splunk-enterprise/get-started/install-and-upgrade/9.4>
- REF4** System Requirements
<https://help.splunk.com/en/splunk-enterprise/get-started/install-and-upgrade/9.4/plan-your-splunk-enterprise-installation/system-requirements-for-use-of-splunk-enterprise-on-premises>
- REF5** Splunk para Common Criteria
<https://help.splunk.com/en/splunk-enterprise/administer/manage-users-and-security/9.4/establish-and-maintain-compliance-with-fips-and-common-criteria-in-splunk-enterprise/best-practice-for-maintaining-compliance-with-fips-and-common-criteria-in-your-splunk-enterprise-environment>
- REF6** Splunk Security
<https://docs.splunk.com/Documentation/Splunk/9.4.0/Security/>
- REF7** Splunk Deployment Manual
<https://docs.splunk.com/Documentation/Splunk/9.4.0/Deploy/>
- REF8** Splunk Distributed Search
<https://docs.splunk.com/Documentation/Splunk/9.4.0/DistSearch/Whatisdistributedsearch>
- REF9** Manage Indexers and Indexer Clusters
<https://help.splunk.com/en/splunk-enterprise/administer/manage-indexers-and-indexer-clusters/9.4>
- REF10** Forward and Process Data
<https://help.splunk.com/en/splunk-enterprise/forward-and-process-data/forwarding-and-receiving-data/9.4/>
- REF11** Monitor
<https://help.splunk.com/en/splunk-enterprise/administer/monitor/9.4/>

9 ABREVIATURAS

CCN	Centro Criptológico Nacional
CLI	Command Line Interface
CPSTIC	Catálogo de Productos y Servicios TIC
CPU	Central Processing Unit
CRL	Certificate Revocation List
ECDSA	Elliptic Curve Digital Signature Algorithm
ENS	Esquema Nacional de Seguridad
FTP	File Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IKE	Internet Key Exchange
IoMT	Internet of Medical Things
IoT	Internet of Things
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
NTP	Network Time Protocol
OT	Operational Technology
PAM	Privileged Access Manager
RSS	Really Simple Syndication
SAML	Security Assertions Markup Language
SHA	Secure Hash Algorithm
SIEM	Security Information and Event Management
SMTP	Simple Mail Transfer Protocol
SPL	Search Processing Language
SSH	Secure Shell
SSO	Single Sign On
STIC	Sistemas y Tecnologías de la Información y las Comunicaciones
TLS	Transport Layer Security
URL	Uniform Resource Locator
XSRF	Cross-Site Request Forgery
XSS	Cross-Site Scripting

