Guía de Seguridad de las TIC
CCN-STIC 1242

Procedimiento de Empleo Seguro
LogPoint SIEM

Marzo 2026

Edita:

centro criptológico nacional

Fecha de Edición: Marzo de 2026

CCN
c=ES, l=MADRID, o=CCN, ou=SELLO ELECTRONICO, 2.5.4.97=VATES-S2800155J, serialNumber=S2800155J, cn=CCN
2026.04.06 08:56:35 +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

ÍNDICE

1 INTRODUCCIÓN

1. Logpoint SIEM es un sistema de gestión de eventos de seguridad (SIEM). Logpoint SIEM actúa como el núcleo central para los datos de eventos de seguridad dentro de una organización. Recopila, correlaciona, analiza y visualiza información proveniente de diversas fuentes mediante distintos "Collectors" y "Fetchers", lo que permite a los equipos de seguridad detectar e investigar incidentes con rapidez y eficacia.

2. Sus funciones avanzadas de generación de informes y análisis de datos históricos garantizan el cumplimiento de la normativa y apoyan la mejora continua de la seguridad de una organización.

3. Un usuario autorizado puede acceder al producto a través de su interfaz web mediante un navegador web estándar. La autenticación basada en roles se implementa para restringir el acceso, asegurando que sólo los usuarios autorizados puedan interactuar con funcionalidades específicas del producto.

4. A continuación, se enumeran las principales funciones de Logpoint SIEM:

    - **Gestión de registros:** Los registros en bruto se recopilan u obtienen de diversas fuentes de registro y se descomponen en mensajes individuales. Logpoint SIEM enriquece estos mensajes normalizándolos, etiquetándolos y añadiendo información contextual del dominio.
    - **Inteligencia sobre amenazas:** Los registros se mejoran aún más con la inteligencia sobre amenazas recopilada de una amplia gama de proveedores, lo que proporciona a los equipos de seguridad el contexto necesario para hacer frente a las amenazas emergentes.
    - **Monitorización:** Los paneles y widgets personalizables permiten la supervisión de registros históricos y en tiempo real, con visualizaciones que proporcionan información valiosa sobre los eventos de seguridad. Los usuarios pueden realizar búsquedas en tiempo real y retrospectivas para un análisis más profundo.
    - **Alertas y gestión de incidentes:** Se aplican reglas de alerta para identificar posibles amenazas mediante la correlación de los datos de registro con consultas y condiciones predefinidas. Cuando se cumplen estas condiciones, se activan las alertas y se generan los incidentes correspondientes para su investigación. Estos incidentes ayudan a los equipos de seguridad a determinar si existe una amenaza legítima.
    - **Informes:** Los informes se componen de consultas de búsqueda que presentan los datos en diversos formatos. Las plantillas de informes contienen estas consultas, mientras que los diseños dictan la presentación visual del informe. Logpoint ofrece varios informes predefinidos, que pueden utilizarse tal cual o personalizarse. Los informes pueden programarse para que se ejecuten automáticamente en diversos formatos y distribuirse a los usuarios designados.
    - **Análisis forense:** Logpoint SIEM ofrece sólidas capacidades forenses, lo que permite a los usuarios autorizados buscar vulnerabilidades en toda la red mediante el análisis de los datos de registro recopilados. Esta funcionalidad ayuda a identificar actividades sospechosas y a mitigar los riesgos en tiempo real.

2 OBJETO Y ALCANCE

5. El presente documento tiene como objeto detallar la integración segura del producto Logpoint SIEM, versión 7.4.0.4, en la infraestructura del cliente. Además, especifica la configuración necesaria para que el producto cumpla con los requisitos de la taxonomía en la que se ha cualificado: CCN-STIC-140 B6 [REF1].
6. Logpoint SIEM es una solución de software que puede instalarse en una sola máquina o en varias máquinas en una configuración distribuida. Las configuraciones del producto incluyen las siguientes:
    - Un único dispositivo Logpoint.
    - Varios dispositivos Logpoint trabajando juntos en una configuración distribuida.
7. Logpoint SIEM, puede configurarse como un colector, ofreciendo un subconjunto de los componentes completos de Logpoint. Sin embargo, el Logpoint Collector y el uso de varios dispositivos Logpoint en una configuración distribuida no se incluyen como parte de las configuraciones evaluadas.
8. El despliegue de Logpoint SIEM se lleva a cabo en un entorno virtual mediante un fichero OVA.
9. Logpoint SIEM versión 7.4.0.4 ha sido cualificado e incluido dentro del Catálogo de Productos y Servicios de Seguridad TIC (CPSTIC) del Centro Criptológico Nacional (CCN) en la familia “Sistemas de gestión de eventos de seguridad (SIEM)” para categoría ENS ALTA.

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.

4 FASE PREVIA A LA INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

10. Tras la formalización contractual entre la parte interesada y Logpoint, se podrá acceder al software del producto en formato OVA descargándolo desde el enlace indicado en [REF5]. Para ello, es necesario contar con un usuario autenticado en la plataforma "Service desk" de Logpoint, cuyas credenciales son proporcionadas directamente por el fabricante a través de correo electrónico.
11. Una vez completada la descarga, el cliente deberá comprobar que el hash SHA256 del OVA descargado coincide con el hash indicado en la página de descarga del producto [REF7]. Para realizar la comprobación, se puede ejecutar el siguiente comando en una consola de powershell:

```
Get-FileHash -Algorithm sha256 .\<ruta del fichero> | Format-List.
```

12. Además del fichero en formato OVA, se requiere el parche del producto en formato PAK, disponible para su descarga en el enlace indicado en [REF6]. Este parche actualizará el producto de la versión 7.4.0 a la 7.4.0.4. El cliente deberá comprobar que el hash SHA256 del PAK descargado coincide con el hash indicado en la página de descarga del producto [REF7]. Para realizar la comprobación, se puede ejecutar el siguiente comando en una consola de powershell:

```
Get-FileHash -Algorithm sha256 .\<ruta del fichero> | Format-List.
```

13. Los manuales y la documentación técnica están disponibles a través del enlace indicado en [REF4].
14. Logpoint se comunicará con el cliente exclusivamente mediante direcciones de correo electrónico bajo el dominio "@logpoint.com", garantizando así una comunicación segura y confiable.

4.2 ENTORNO DE INSTALACIÓN SEGURO

15. Se recomienda llevar a cabo la instalación de Logpoint SIEM en el CPD de la organización con el fin de limitar el acceso físico al equipo. El acceso físico al producto deberá realizarse únicamente por administradores previamente autorizados.

4.3 REGISTRO Y LICENCIAS

16. Para cualquier gestión relacionada con el registro de licencias, consulte la sección "*Logpoint → Deploy → Install and Upgrade Logpoint → Logpoint License*" del enlace indicado en [REF4].

4.4 CONSIDERACIONES PREVIAS

17. La OVA del producto ha sido desplegada y evaluada usando *VMWare Workstation Pro 17*.
18. En caso de que se requiera desplegar la OVA del producto en *VMWare ESXi server*, este deberá ser versión 7.0.3 o superior.
19. Debe garantizarse la conexión entre Logpoint SIEM y el host desde el cual se administra.

4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN

20. A continuación, se describe el entorno operativo recomendado por el fabricante para garantizar el correcto funcionamiento del producto:

21. La plataforma de hardware en la que se instala Logpoint SIEM debe estar dedicada exclusivamente a su funcionamiento, sin desempeñar funciones secundarias. Asimismo, el producto puede instalarse en una máquina virtual, siempre que esta se utilice únicamente para ejecutar el producto.

22. Navegador compatible para acceder a la interfaz web del producto: Google Chrome 68.x o posterior, Mozilla Firefox 62.x o posterior, Microsoft Internet Explorer 11 o posterior, Apple Safari 12.x o posterior.

23. La fuente de registro desde la que se generan los registros y se envían a Logpoint SIEM. Estos registros proveen información crítica para monitorizar, auditar y detectar eventos de seguridad dentro de la red.

24. La siguiente imagen muestra todos los componentes y comunicaciones de Logpoint SIEM:

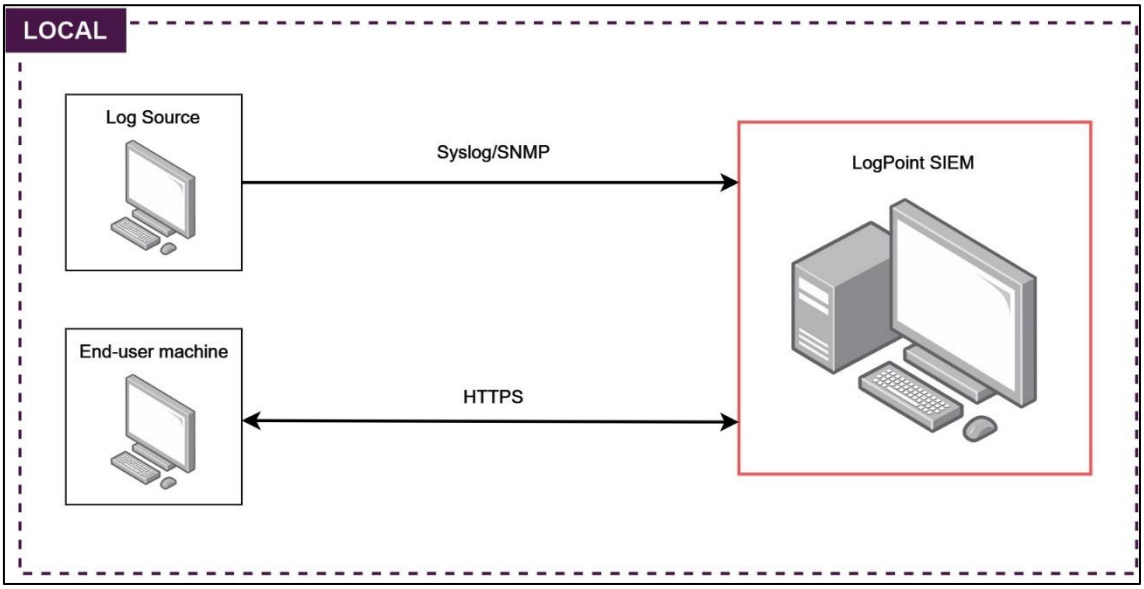

Ilustración 1. Componentes y comunicaciones

25. A continuación, se detallan los requisitos mínimos de hardware necesarios para el correcto funcionamiento de Logpoint SIEM:

Item	Identification	Description
Operating System	Ubuntu 20.04.6 LTS	N/A
Hardware	Intel-compatible quad core CPU, 2GHz Minimum memory: 8GB or more recommended. Disk Space 150GB (RAID-1 protected) recommended. Network adapter: 1GB network adapter	N/A

Tabla 1. Requisitos mínimos

26. Si se utiliza LDAP para la autenticación de usuarios, será necesario contar con un servidor LDAP adecuado. OpenLDAP está disponible en los repositorios predeterminados de Ubuntu bajo el paquete «slapd».

27. Se implementarán medidas de seguridad apropiadas para proteger las credenciales de usuario transmitidas desde Logpoint SIEM al servidor LDAP.

5 FASE DE INSTALACIÓN

28. Tras la preinstalación del producto, se procede a su instalación de manera segura. Para ello, se siguen los siguientes pasos:

    a) Abrir VMware Workstation Pro 17.

    b) Hacer click en “Open a Virtual Machine” y seleccionar el fichero en formato OVA previamente descargado en [REF5].

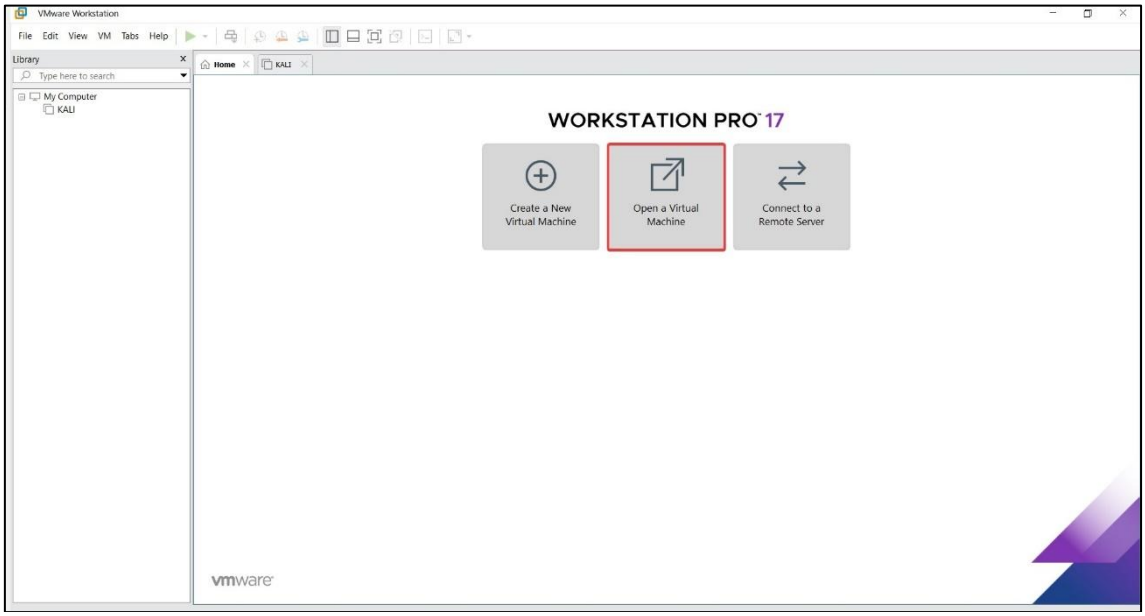

Ilustración 2. Open Virtual Machine

c) Escribe un valor para “Name for the new virtual machine” y hacer click en “Import”.

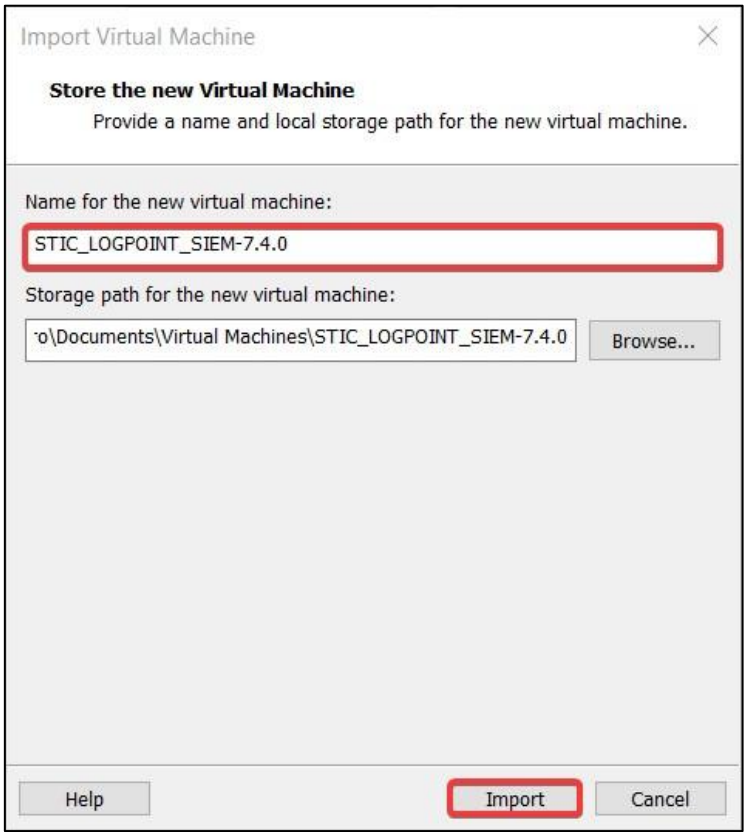

Ilustración 3. Nombrar la máquina virtual

d) Esperar hasta que la importación se haga efectiva.

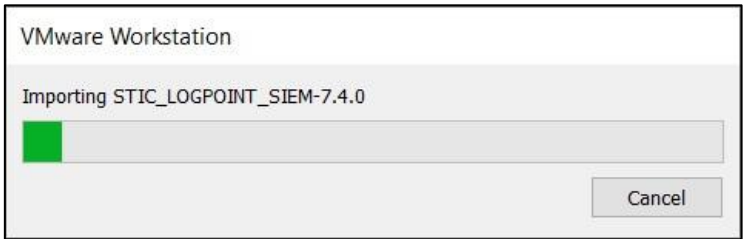

Ilustración 4. Progreso de la importación

e) Para iniciar la máquina virtual, hacer click en “Power on this virtual machine”.

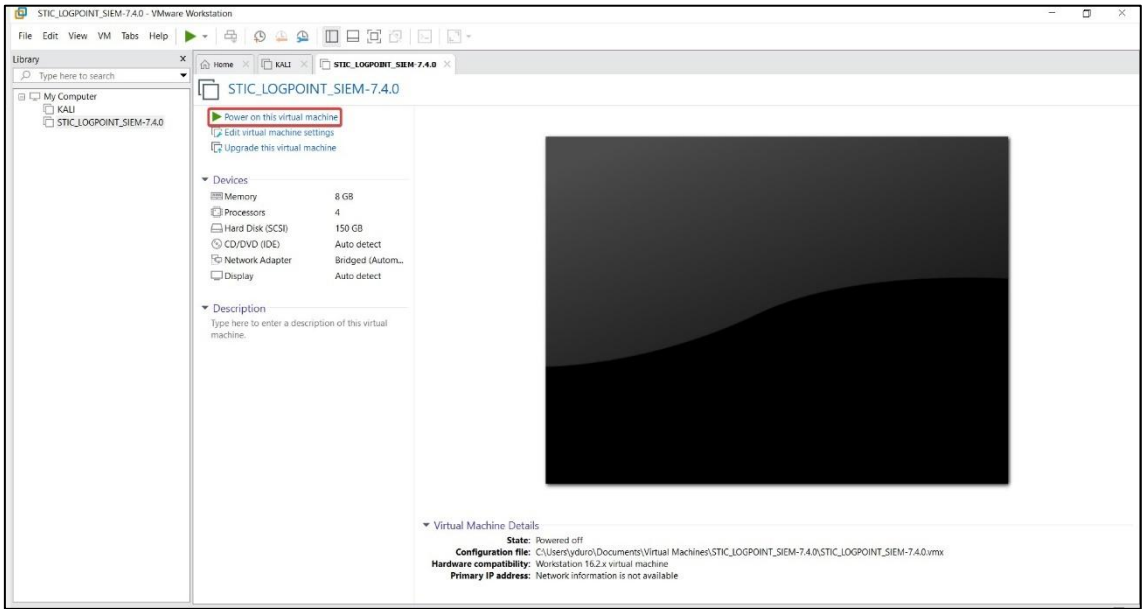

Ilustración 5. Inicialización de la máquina virtual

f) Hacer login en la CLI del producto usando las siguientes credenciales.

```
Username: li-admin

Password: changeme
```

```
Ubuntu 20.04.6 LTS logpoint tty1

logpoint login: li-admin
Password:
Welcome to LogPoint v7.4.0 (GNU/Linux 5.4.0-170-generic x86_64)

Welcome to the LogPoint Server!
             (o)  system delivered by
                  _          ___      ____      ____      ___     ___    _    _    _____
                 | |        / _ \    / ___|   |  _ \    / _ \   |_ _|  | \ | |  |_   _|
                 | |       | | | |  | |  _    | |_) |  | | | |   | |   |  \| |    | |
                 | |___    | |_| |  | |_| |   |  __/   | |_| |   | |   | |\  |    | |
                 |_____|    \___/    \____|   |_|       \___/   |___|  |_| \_|    |_|
oooOOOoooOOOoooOOOoooOOOoooOOOoooOOOoooOOOoooOOOoooOOOoooOOOoooOOOoooOOOoooOOOoooOOOo

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
```

Ilustración 6. Login mediante CLI

g) Para acceder a la interfaz web del producto, abra un navegador y diríjase a (https://<LOGPOINT-IP>). Al hacerlo, aparecerá la advertencia "Warning: Potential Security Risk Ahead". Para continuar, haga clic en "Advanced…" y luego en "Accept the Risk and Continue".

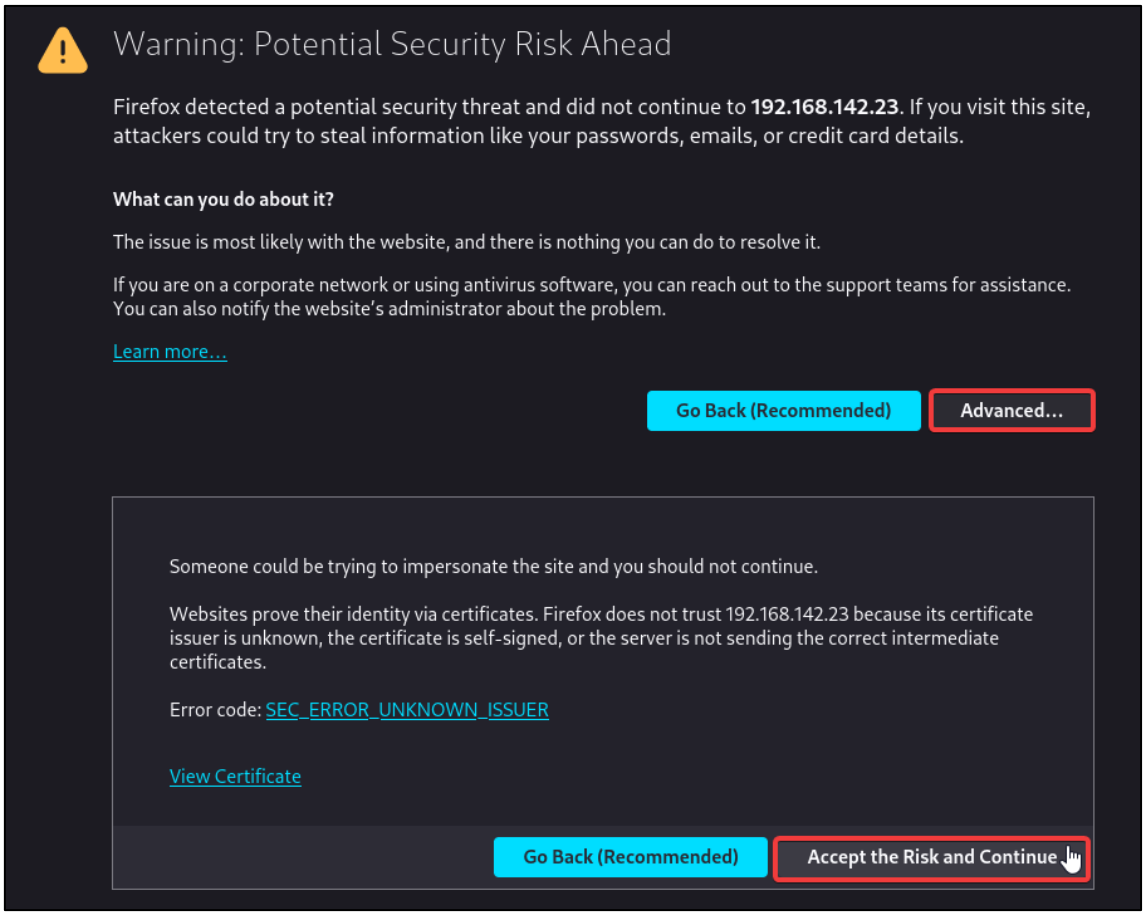

Ilustración 7. Aceptación de certificado

h) Inicie sesión en (https://<LOGPOINT-IP>) utilizando las siguientes credenciales.

```
Username: admin

Password: changeme
```

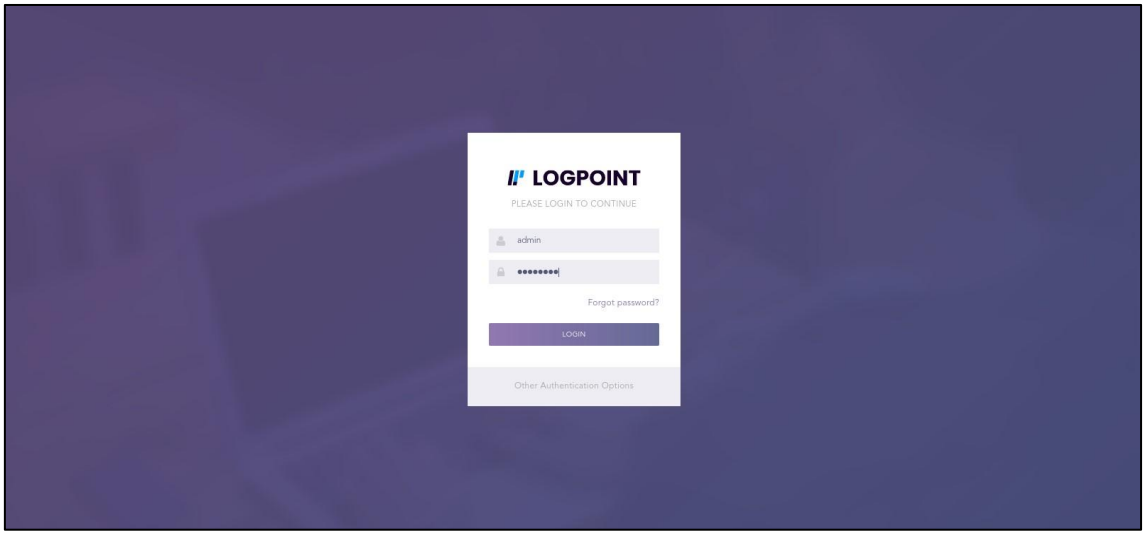

Ilustración 8. Login mediante interfaz web

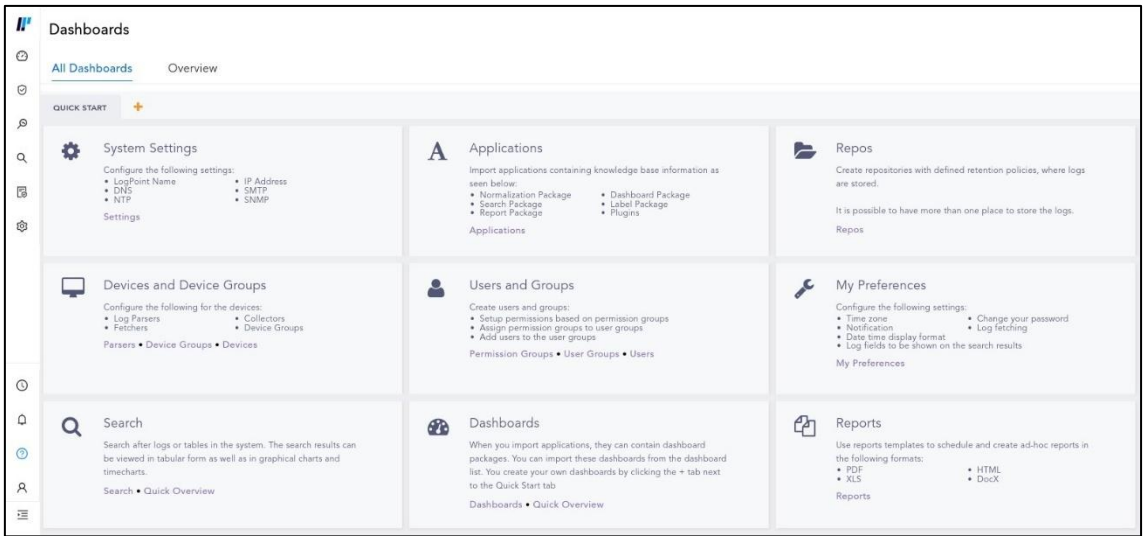

Ilustración 9. Dashboards

i) Expandir el menú ubicado a la izquierda de la pantalla y hacer click en "Settings → System Settings".

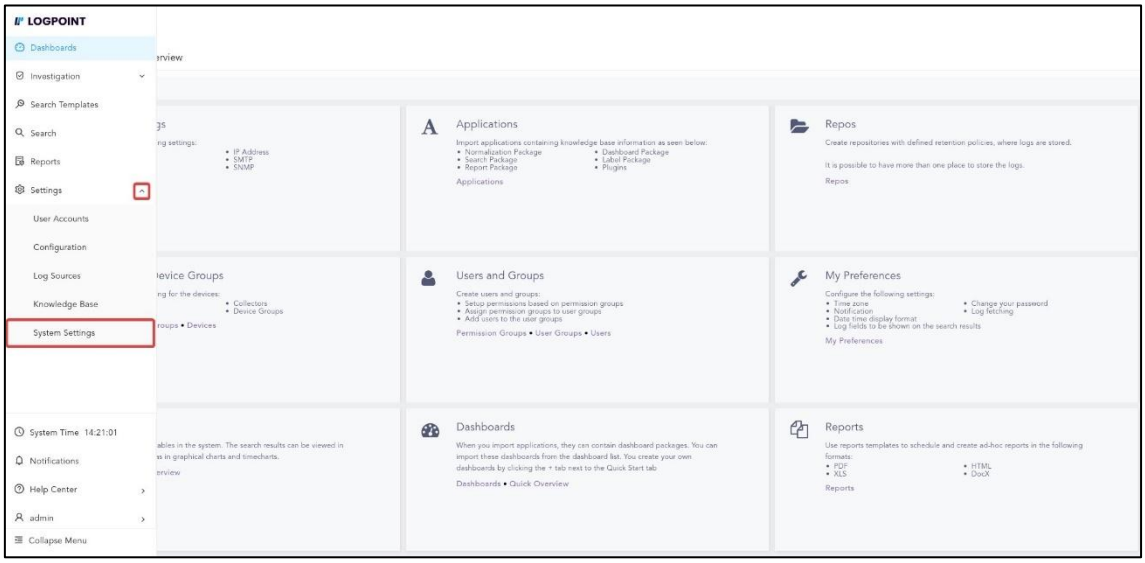

Ilustración 10. Menú System Settings

j) Cerrar el menú y hacer click en "Updates".

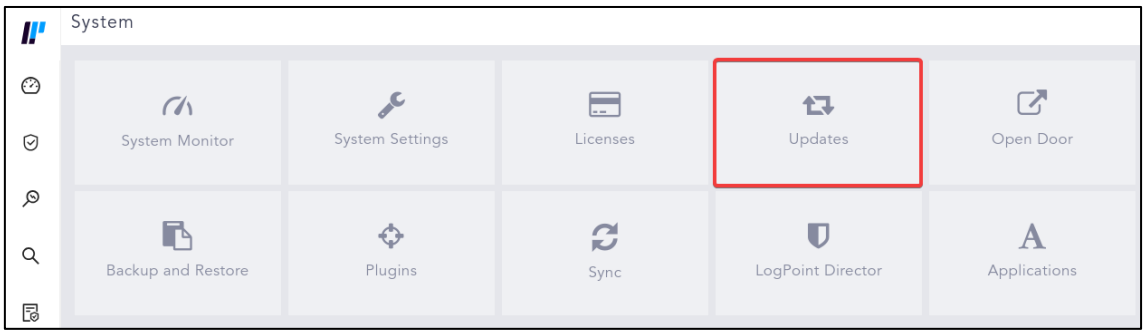

Ilustración 11. Menú Updates

k) Hacer click en “Upload Patch”.

Ilustración 12. Botón de actualización de parche

l) Aparecerá la ventana “IMPORT UPDATE PATCH”, hacer click en “Browse”, seleccionar el fichero PAK descargado en [REF6] y luego hacer click en “Upload”.

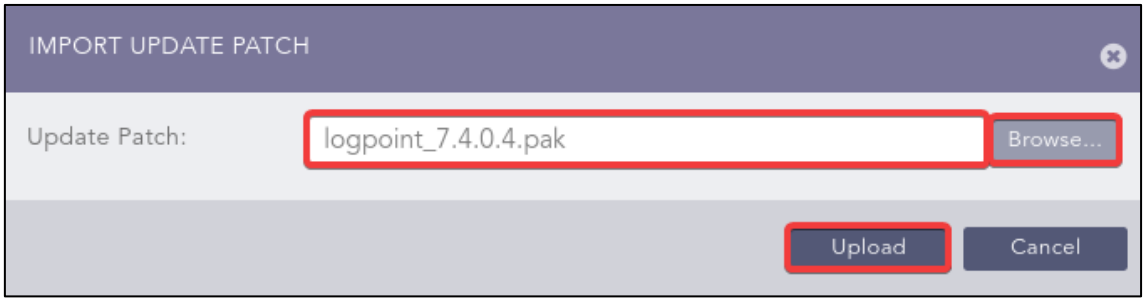

Ilustración 13. Ventana de selección de parche

m) Bajo la columna “Action”, hacer click en el icono “Install Update”.

n) Esperar hasta que la instalación del parche haya finalizado.

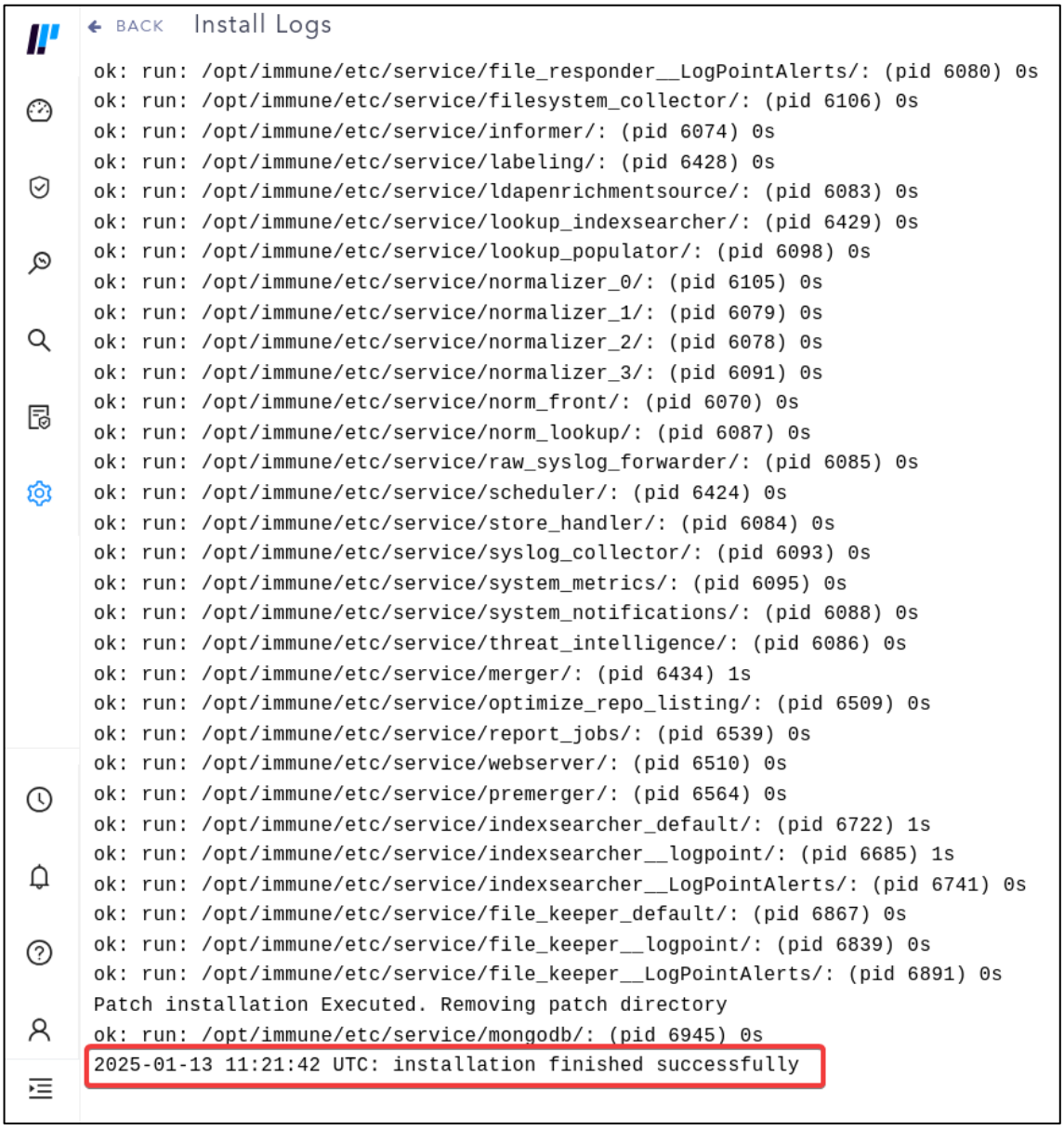

Ilustración 14. Log de instalación

o) Para cumplir con los requisitos mínimos de seguridad, se debe cambiar la contraseña de los usuarios “li-admin” y “admin”, conforme a lo establecido en el apartado 6.2.2 CONFIGURACIÓN DE ADMINISTRADORES.

6 FASE DE CONFIGURACIÓN

6.1 AUTENTICACIÓN

29. El acceso a la interfaz web de Logpoint SIEM se realiza desde un navegador utilizando HTTPS sobre TLSv1.2 o TLSv1.3 y está controlado mediante el uso de una pareja de valores usuario y contraseña.
30. El inicio de sesión en Logpoint SIEM requiere introducir el nombre de usuario y su contraseña de acceso con el fin de validar la identidad de la persona que desea autenticarse en el sistema.
31. Si estos datos son incorrectos, Logpoint SIEM notificará el motivo del rechazo e invitará al usuario a introducir los datos nuevamente; si, por el contrario, son correctos, se autorizará el acceso.
32. Estas credenciales se almacenan en la base de datos local cifradas mediante un algoritmo hash. Este algoritmo no es configurable por parte del usuario.
33. Las claves de los componentes internos que requieren autenticación (BBDD) por defecto están almacenadas en el sistema de ficheros y protegidas por el sistema operativo en el que se ejecuta Logpoint SIEM.
34. Se recomienda utilizar el acceso por SSH con el usuario configurador del SO para la configuración del producto. Dicho acceso se realiza también mediante usuario/contraseña. El usuario root (superusuario) del sistema operativo no puede acceder vía SSH directamente, lo hará escalando desde un usuario sin privilegios.

6.2 ADMINISTRACIÓN DEL PRODUCTO

6.2.1 ADMINISTRACIÓN LOCAL Y REMOTA

35. El producto dispone de las siguientes interfaces para la administración de este:
    - Administración local por terminal de comandos.
    - Administración remota por terminal de comandos mediante SSH (puerto 22 por defecto).
    - Administración remota por interfaz web mediante HTTPS (puerto 443 por defecto) sobre TLSv1.2 o TLSv1.3. Esta interfaz proporciona las siguientes suites de cifrado:
        - TLS_CHACHA20_POLY1305_SHA256
        - TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
        - TLS_AES_256_GCM_SHA384
        - TLS_AES_128_CCM_8_SHA256
        - TLS_AES_128_CCM_SHA256
        - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
        - TLS_AES_128_GCM_SHA256
        - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
36. Además, se utiliza la curva elíptica “secp384r1” para el intercambio de claves y el certificado dispone de una longitud de clave de 3072 bits. De esta forma, las comunicaciones de la interfaz cumplen con la guía CCN-STIC-807 [REF2].

6.2.2 CONFIGURACIÓN DE ADMINISTRADORES

37. El detalle de configuración de administradores se puede consultar la sección *"Logpoint → Configure → User Account Management*" del enlace indicado en [REF4].

38. Los privilegios de acceso de los administradores se definen a través de grupos de permisos. Por defecto, el producto proporciona dos (2) grupos de permisos con diferentes niveles acceso:

    - **Admin:** Tiene permisos de lectura, creación y eliminación.
    - **Operator**: Solo tiene permisos de lectura.

39. Adicionalmente se pueden crear perfiles de administración nuevos en los que se pueden determinar los permisos específicos.

40. La contraseña predeterminada de los usuarios "li-admin" y "admin" es "changeme" y deberá modificarse manualmente en el primer inicio de sesión. Dado que el producto no dispone de una política predefinida de contraseñas, todas las contraseñas asignadas al crear nuevos usuarios, incluida la de los usuarios "li-admin" y "admin", deberán cumplir con los siguientes requisitos mínimos de seguridad establecidos en la guía CCN-STIC-807 [REF2]:

    - Longitud mínima de la contraseña: doce (12) caracteres.
    - Composición de la contraseña: letras mayúsculas, letras minúsculas, números y símbolos especiales.

41. Para configurar el tiempo de inactividad de las sesiones con un máximo de cinco (5) minutos, consulte la sección "Logpoint → Configure → System Configuration → System Settings → General" del enlace indicado en [REF4].

42. Para configurar el número de intentos fallidos de inicio de sesión con un máximo de tres (3) intentos y el tiempo de bloqueo tras los intentos fallidos con un mínimo de cinco (5) minutos, consulte la sección "*Logpoint → Configure → System Configuration → System Settings → Lockout Policy*" del enlace indicado en [REF4].

6.3 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

43. Las interfaces, puertos y servicios requeridos por Logpoint SIEM están detalladamente especificados en la sección "Logpoint → Deploy → Install and Upgrade Logpoint → Connections Required By Logpoint" del enlace indicado en [REF4].

6.4 GESTIÓN DE CERTIFICADOS

44. La configuración y gestión de certificados se puede consultar en la sección "*Logpoint → Configure → System Configuration → System Settings*" del enlace indicado en [REF4]. Pese a que las guías referencian que la longitud de clave RSA son de un mínimo de 2048 bits, hay que tener en cuenta que la versión 7.4.0.4 del producto aumenta la longitud de clave RSA a 3072 bits con el objetivo de cumplir con las especificaciones de la guía CCN-STIC-807 [REF2].

45. El producto emplea certificados de servidor para las 3 siguientes comunicaciones:

    - HTTPS
    - Syslog

- SSH

6.5 SERVIDORES DE AUTENTICACIÓN

46. Si la organización interesada hace uso de LDAP con el fin de autenticar usuarios. Logpoint SIEM puede configurarse para que extraiga las credenciales de usuario y las reglas de control de acceso basadas en funciones del directorio LDAP existente.

47. En caso de requerir la configuración de un servidor externo de autenticación LDAP, consulte la sección *"Logpoint → Configure → User Account Management → Authentication → LDAP Authentication*" del enlace indicado en [REF4].

48. Además de LDAP, los usuarios pueden autenticarse mediante los siguientes protocolos de autenticación. Sin embargo, es importante señalar que estos protocolos no forman parte de la configuración cualificada:

    - RADIUS
    - ADFS
    - SAML
    - OAuth

6.6 SINCRONIZACIÓN

49. Se recomienda que todos los sistemas utilizados por la organización se encuentren sincronizados para permitir la alta fiabilidad en los sistemas de auditoría y logging.

50. Para realizar la sincronización segura del producto, consulte la sección "*Logpoint → Configure → System Configuration → System Settings → NTP*" del enlace indicado en [REF4].

6.7 ACTUALIZACIONES

51. Para cualquier gestión relacionada con las actualizaciones del producto, consulte la sección "*Logpoint → Deploy → Install and Upgrade Logpoint → Patch Installation*" del enlace indicado en [REF4].

6.8 ALTA DISPONIBILIDAD

52. En el caso de desplegar el producto a partir de un OVA, se recomienda que la máquina forme parte de un clúster de VMware.

6.9 AUDITORÍA

6.9.1 REGISTRO DE EVENTOS

53. A continuación, se detallan los registros de eventos generados por Logpoint SIEM en su configuración evaluada:

    - Configuración de notificación de alertas.
    - Tamaño del registro en Syslog Collector superior a 12 KB.
    - Gestión de usuarios, grupos de usuarios y grupos de permisos.
    - Inicios de sesión correctos/incorrectos.

- Bloqueo/desbloqueo de usuarios.
- Cambios en los parámetros de bloqueo.
- Administrador desbloquea a un usuario antes del periodo de bloqueo.
- Cierre de un incidente desde la API de incidentes.
- Gestión de elementos de la base de conocimientos tales como macros.
- Generación y eliminación de Informes.
- Gestión de Dashboards.
- Gestión de incidentes.
- Reinicio/apagado del sistema.
- Uso del disco.
- Cuando Logpoint SIEM se conecta/desconecta de otro Logpoint SIEM vía Open Door.

54. Logpoint SIEM incluirá los campos “previous_config” y “updated_config” en sus registros de auditoría al modificar los siguientes componentes:

- Normas de alerta.
- Dispositivos y sus “Collectors” y “Fetchers”.
- Paquetes de normalización y políticas de normalización.
- Usuarios, grupos de usuarios y permisos de objetos.
- Repositorios, políticas de enrutamiento y políticas de procesamiento.
- Configuración general, políticas de bloqueo y configuraciones NTP.
- Macros.

55. Logpoint SIEM genera registros de auditoría para todos los eventos relevantes relacionados con la seguridad. A continuación, se indica el formato de los logs que se registran:

FIELD	DESCRIPTION
log_ts	Fecha y hora de cuando sucedió el evento.
type	Tipo de evento.
action	Resultado del log.
user	Nombre del usuario del log.
previous_config	Configuración previa del componente.
updated_config	Configuración del componente tras su modificación.

Tabla 2. Campos de los logs de auditoría

56. Logpoint SIEM registra la información de auditoría en un formato legible y accesible solo para usuarios con los permisos adecuados. Además, protege los registros almacenados contra modificaciones y eliminaciones.

6.9.2 ALMACENAMIENTO LOCAL

57. Los registros de auditoría se almacenan en archivos de log en distintos directorios según el repositorio (/opt/makalu/storage/logs/).

58. El producto debe notificar a los usuarios cuando el uso del disco alcance un umbral predefinido y, en caso de alcanzar la capacidad máxima de almacenamiento, ignorar los nuevos datos de eventos SIEM. Por defecto, el producto incluye dos umbrales predefinidos que generan notificaciones cuando el uso del espacio en disco alcanza el 80 % y el 90 %. Estos valores pueden personalizarse según lo indicado en la sección "Logpoint → Configure → System Notifications → Configure Custom Disk Usage Notification" del enlace indicado en [REF4].

6.9.3 ALMACENAMIENTO REMOTO

59. El producto permite enviar los registros de alertas e incidentes a un servicio remoto mediante e-mail, SSH, SNMP, HTTP o Syslog, Estas alertas e incidentes pueden configurarse según lo indicado en la sección "Logpoint → Search and Analytics → Alerts and Incidents" del enlace indicado en [REF4].

60. Para configurar Syslog consulte la sección *"Logpoint → Configure → Log Sources → Creating Log Sources → Syslog Collector*" del enlace indicado en [REF4].

6.10 BACKUP

61. Para cualquier gestión relacionada con las copias de seguridad del producto, consulte la sección "*Logpoint → Configure → Backup and Restore*" del enlace indicado en [REF4].

7 REFERENCIAS

[REF1] CCN-STIC-140-B.6: Taxonomía de Sistemas de gestión de eventos de seguridad

[REF2] Guía CCN-STIC-807

[REF3] Web oficial del fabricante

[REF4] Documentación oficial del fabricante

[REF5] LogpointSIEM v7.4.0 OVA

[REF6] Logpoint SIEM v7.4.0.4 PAK

[REF7] Releases de Logpoint SIEM

8 ABREVIATURAS

CCN	Centro Criptológico Nacional
CPD	Centro de Procesamiento de Datos
CPSTIC	Catálogo de Productos y Servicios TIC
ENS	Esquema Nacional de Seguridad.
HTTPS	Hypertext Transfer Protocol Secure
LDAP	Lightweight Directory Access Protocol
NTP	Network Time Protocol
OVA	Open Virtual Appliance
SIEM	Sistemas de gestión de eventos de seguridad
SSH	Secure Shell
TLS	Transport Layer Security
URL	Uniform Resource Locator
VM	Virtual Machine