Guía de Seguridad de las TIC
CCN-STIC 1479

Procedimiento de Empleo Seguro
VoyagerVM4.0 KlasOS Keel

Marzo 2026

Edita:

CCN
c=ES, l=MADRID, o=CCN,
ou=SELLO ELECTRONICO,
2.5.4.97=VATES-S2800155J,
serialNumber=S2800155J,
cn=CCN
2026.04.06 09:37:54 +02'00'

Fecha de Edición: Marzo de 2026

LIMITACIÓN DE RESPONSABILIDAD

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

AVISO LEGAL

ÍNDICE

1 INTRODUCCIÓN

1. KlasOS Keel es un sistema operativo orientado a entornos de computación perimetral, que combina un núcleo Linux reforzado con servicios de virtualización mediante KVM. Su arquitectura permite ejecutar máquinas virtuales y contenedores de forma aislada, lo que facilita el despliegue de funciones de red, aplicaciones de seguridad y análisis de datos en un único equipo físico.
2. El sistema gestiona de forma centralizada las interfaces de red disponibles —25Gbps/10Gbps/2.5Gbbps/1Gbps Ethernet— y permite configurar políticas de enrutamiento y priorización del tráfico. Esta capacidad resulta especialmente útil en escenarios con múltiples enlaces WAN, en los que es necesario conmutar automáticamente en caso de fallo y seleccionar la mejor ruta disponible para mantener la conectividad.
3. KlasOS Keel incorpora un cortafuegos con filtrado con estado y compatibilidad con túneles cifrados, lo que permite proteger las comunicaciones entre nodos remotos y redes centrales. También ofrece mecanismos de autenticación de usuarios y gestión de certificados, facilitando su integración en infraestructuras de seguridad existentes.

2 OBJETO Y ALCANCE

4. El objetivo es poner en conocimiento del administrador del VoyagerVM4.0 los mecanismos de seguridad necesarios para proteger los sistemas de información y comunicaciones conectados al VoyagerVM4.0. Con este conocimiento, es posible establecer un marco de referencia para las recomendaciones STIC en el despliegue y uso de dicho equipo.
5. Generalmente, este documento no aporta ajustes de configuración relacionados con la operación del equipo. Principalmente las configuraciones mostradas se centran en su operación en modo seguro. Otros aspectos como las políticas de flujo de información y el control de acceso deben ser implementados de acuerdo con las políticas vigentes en cada organización.
6. El producto VoyagerVM4.0 KlasOS Keel ha sido cualificado en el catálogo CPSTIC para categoría ENS ALTA en las familias “Cortafuegos” y “Enrutadores”.

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

7. La entrega segura del producto es un paso fundamental para garantizar la integridad y autenticidad del equipo antes de su puesta en servicio. Este procedimiento describe las verificaciones que deben realizarse desde la recepción del paquete hasta la inspección física del dispositivo, con el fin de confirmar que no ha sido manipulado, que procede de un proveedor autorizado y que el número de serie coincide con el indicado en la documentación de compra. Seguir estas comprobaciones permite asegurar que el switch recibido es el solicitado y que no ha sufrido alteraciones durante el transporte o el proceso de entrega.

    a) Antes de abrir el paquete en el que fue entregado el VoyagerVM4.0, compruebe que el paquete contenga la serigrafía y el logotipo de Klas/Voyager. Si no es así, contacte con el proveedor del equipo (Klas o un distribuidor autorizado)

    b) Compruebe que el paquete no ha sido abierto y vuelto a sellar, fijándose en la cinta que lo cierra. Si el paquete parece haber sido abierto y vuelto a sellar, contacte con el proveedor del equipo (Klas o un distribuidor autorizado).

    c) Preste atención al número de serie del equipo especificado en la documentación del pedido. El número de serie que figura en la etiqueta blanca de la caja se debe corresponder con el número de serie del dispositivo. Por tanto, compruebe que este número concuerda con el número de serie en la factura enviada por correo. Si no es así, contacte con el proveedor del equipo (Klas o un distribuidor autorizado).

    d) Compruebe que el pedido fue enviado por el proveedor esperado (Klas o un distribuidor autorizado). Este proceso puede llevarse a cabo verificando el código de envío/paquete junto con la empresa de transporte.

    e) Una vez que el paquete ha sido abierto, inspeccione el dispositivo. Compruebe que el número de serie mostrado en él concuerda con el número de serie que aparece en la documentación del envío y la factura. Si no es así, contacte con el proveedor del equipo (Klas o un distribuidor autorizado).

8. El equipo se entrega con un software instalado. No obstante, puede que no sea la versión del software más reciente, en cuyo caso el VoyagerVM4.0 deberá actualizarse, siguiendo el procedimiento definido en la sección 97 Si el servidor NTP remoto requiere autenticación, primero habría que configurar la clave y luego vincularla al servidor NTP configurado. Toda la configuración a aplicar sería la siguiente:

```
ntp authenticate
ntp authentication-key 1 sha1 <shared-secret>
ntp trusted-key 1
ntp server <ntp_server_IP or FQDN> key 1
```

9. ACTUALIZACIONES.

4.2 ENTORNO DE INSTALACIÓN SEGURO

10. Se recomienda instalar en un entorno físico seguro que cuente con un sistema de control de acceso limitado únicamente a las personas autorizadas.

4.3 REGISTRO Y LICENCIAS

11. No es necesaria la aplicación de ninguna licencia para acceder a la funcionalidad requerida para la configuración segura del equipo.

4.4 CONSIDERACIONES PREVIAS

12. El VoyagerVM4.0 requiere de los siguientes componentes (incluidos con el equipo) para su puesta en marcha inicial a través del puerto de consola:
    - Cable Rollover RS232-RJ45.
    - Convertidor de USB a RS232 (Si el puesto de gestión no dispone de puerto RS232 pero dispone de USB).
13. La configuración del cliente de consola está definida en la sección 5 FASE DE INSTALACIÓN.

4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN

14. El VoyagerVM4.0 puede interconectarse con los siguientes componentes en el entorno operativo:
    - Puesto de gestión por consola: Este puesto hace referencia a cualquier estación de trabajo que permita una conexión por consola (puerto serie) en el VoyagerVM4.0.
    - Puesto de gestión con cliente SSH: Este puesto hace referencia a cualquier estación de trabajo con un cliente SSHv2 instalado que se emplea para la configuración y administración del VoyagerVM4.0.
    - Servidor RADIUS AAA (Opcional)
    - Servidor de monitorización por SNMP/ICMP (Opcional)

5 FASE DE INSTALACIÓN

Para su instalación hay que seguir la “VoyagerVM4.0 Hardware Guide” (guía de hardware correspondiente al VoyagerVM4.0), que se puede descargar directamente desde el “helpdesk” de Klas. [REF7].

15. Para acceder al puerto de consola del equipo, se debe usar un cable de consola con los siguientes parámetros:
    - 9600 baudios
    - 8 bits de datos
    - Sin paridad
    - 1 bit de parada
    - Sin control de flujo
16. Una vez conectado el cable de red y cuando el equipo haya arrancado completamente, el equipo mostrará el siguiente mensaje: “Press RETURN to get started.” Presione ENTER para acceder a la consola del equipo.

6 FASE DE CONFIGURACIÓN

17. El VoyagerVM4.0 necesita una configuración inicial realizada mediante el cable de consola entregado con el equipo. Esta configuración inicial permite la configuración de la conexión por SSHv2 usando cualquiera de los puertos Ethernet del equipo.
18. La documentación que incluye la configuración inicial del dispositivo se encuentra disponible en [REF3].
19. En general, toda la configuración se realiza usando la línea de comandos. Hay tres modos de operación distintos:
    - **EXEC Usuario:** Modo por defecto cuando se enciende el equipo por primera vez. Es un modo de usuario sin permisos de administración donde solamente hay disponibles unos pocos comandos de solo lectura. El prompt es:

```
KlasOS>
```

    - **EXEC Usuario Privilegiado:** Usando el comando "enable" accedemos al modo de usuario privilegiado (administrador). Este modo es solamente para administradores del equipo y se debe crearse contraseñas para evitar que otros usuarios no autorizados accedan a este modo (ver sección 6.3.2 CONFIGURACIÓN DE ADMINISTRADORES). En este modo podemos acceder a todos los comandos del sistema. El prompt es el nombre del dispositivo seguido de un signo de almohadilla #. Por ejemplo:

```
KlasOS#
```

    - **Modo de configuración global:** En este modo es donde se realiza la mayoría de la configuración necesaria. Para entrar en este modo, introduciremos el comando "configure terminal" desde el modo EXEC privilegiado y el prompt cambiará a:

```
KlasOS(config)#
```

    NOTA: Se pueden ejecutar comandos del modo privilegiado desde el modo de configuración usando el comando "do" delante del comando privilegiado que se quiera ejecutar.
20. Cuando se están introduciendo comandos en la línea de comandos, el usuario puede ver qué opciones hay disponibles usando la tecla del signo de interrogación (?) o pulsando el tabulador (TAB).
21. El comando `exit` nos permite ir a modos de usuario con menos privilegios:
    - Para salir del modo de configuración al modo privilegiado se usa el comando "`exit`".
    - Igualmente, para salir del modo privilegiado al modo usuario se usa el comando "`exit`".
    - De nuevo para salir de la sesión del modo usuario se usa el comando "`exit`".
22. Para verificar la configuración del equipo, se pueden emplear comandos que muestren tanto la configuración en ejecución como la configuración de arranque. Estos comandos deben ejecutarse desde el modo de usuario privilegiado, tal y como se indica a continuación.
    - Para mostrar la configuración actual del dispositivo, desde el modo de usuario privilegiado hay que usar el comando "`show running-config`".

- Para mostrar la configuración de arranque del equipo, desde el modo de usuario privilegiado hay que usar el comando "`show startup-config`".

6.1 MODO DE OPERACIÓN SEGURO

23. Cuando el equipo arranca por primera vez, no hay ninguna configuración aplicada y todos los puertos permiten el paso de tráfico sin restricción alguna.
24. Es obligatorio realizar una configuración completa antes de exponer el equipo a una red externa.
25. La configuración segura implica seguir este documento junto con los manuales generales del dispositivo en los siguientes aspectos:
    - Contraseña de administrador. Sección 6.2
    - Usuario(s) y contraseña(s). Sección 6.2
    - Banner de acceso. Sección 6.2.1
    - Temporizador de inactividad. Sección 6.2.2
    - Bloqueo de cuentas. Sección 6.2.3
    - Fecha y hora. Sección 6.8
    - Claves públicas y privadas. Sección 6.6
    - SSH para acceso remoto. Sección 6.3
    - Túnel SSH para "trusted path". Sección 6.5.3
    - Servidor de syslog. Sección 6.5.2
    - Servidor HTTP seguro (HTTPS). Sección 6.5.2

6.2 AUTENTICACIÓN

26. Los usuarios se identificarán y autenticarán con un usuario y contraseña. Por seguridad, y aunque la longitud mínima de una contraseña son 12 caracteres para el cumplimiento del ENS, se recomiendan contraseñas con una longitud mínima de 15 caracteres, incluyendo soporte para los siguientes caracteres especiales: "`!#$%&()*+,-./[]^_{|}~=<>@;:`".
27. La política de contraseñas y la creación de usuarios se gestionan mediante comandos específicos en el modo de configuración global. A continuación, se indican los comandos para ajustar la longitud mínima de las contraseñas y para configurar cuentas de usuario no administrativas de forma segura.
    - El administrador puede requerir una longitud mayor, de hasta 128 caracteres, usando el comando "`security passwords min-length <longitud_minima>`".
      NOTA: Obligatorio usar un mínimo de 12 caracteres cumplir con requisitos del ENS.
    - Los usuarios se crean con el comando "`username <username> algorithm-type sha512 secret <password>`"

28. Por defecto, no hay ningún usuario ni contraseña preconfigurados. Esto significa que hay que crear usuarios y contraseñas antes de usarlo. Siguiendo las buenas prácticas, se recomienda crear usuarios nominales.

29. Una vez creados, los usuarios pueden iniciar sesión en el equipo. Se registrará un mensaje de error en el log si un usuario falla la autenticación:

```
2024-04-30T20:21:51.914014+00:00 KlasOS login: %SYS-5-PRIV_AUTH_FAIL:
Authentication Failed by klas on ttyS0
```

30. Para que el sistema requiera la autenticación de usuarios, las siguientes líneas de configuración deben ser introducidas de manera obligatoria:

```
aaa new-model
aaa authentication login default local
```

6.2.1 BANNER DE ACCESO

31. El equipo puede configurarse con un banner que incluya un aviso con las condiciones de conexión a dicho equipo. Este mensaje se mostrará antes del login. Para configurar dicho banner, desde el modo de configuración se debe introducir el siguiente comando:

```
banner login "Ejemplo de banner"
```

32. Si se desean añadir líneas adicionales al banner, se debe usar la cadena de caracteres "///" como retorno de carro para cada línea:

```
banner login "Primera línea del banner///Segunda línea del banner"
```

6.2.2 TEMPORIZACIÓN DE INACTIVIDAD

33. Cada usuario puede terminar su propia sesión introduciendo el comando "exit" en la línea de comandos.

34. Si el usuario está en el modo EXEC de usuario (solo lectura), introducir el comando "exit" terminará la sesión para dicho usuario.

35. Si el usuario está en el modo PRIV EXEC (administrador), introducir el comando "exit" le devolverá al modo EXEC de usuario (solo lectura), donde deberá volver a introducir el comando "exit" y así terminará la sesión para dicho usuario.

36. Un temporizador de inactividad se debe configurar para la consola local o bien para sesiones remotas. Una vez este temporizador ha expirado, se cerrará la sesión y el usuario será desconectado. Se aconseja establecer el temporizador en 5 minutos.

37. Para configurar un timer de inactividad para la consola, utilizar la siguiente configuración:

```
line console 0
exec-timeout <mins> <secs>
```

38. Para configurar un timer de inactividad para una sesión remota (SSH), utilizar la siguiente configuración:

```
line vty 0 4
exec-timeout <mins> <secs>
```

39. Cuando estos temporizadores están activos y un usuario es desconectado por inactividad, el log del sistema registrará el evento.

6.2.3 BLOQUEO DE CUENTAS

40. El equipo se debe configurar de manera que un usuario remoto sea bloqueado tras un número determinado de fallos en su intento de acceso al sistema. Para desbloquear a dicho usuario, se requerirá la intervención manual de un administrador.

    NOTA: El equipo siempre permitirá a un usuario autenticarse en el puerto de consola, incluso si su cuenta está bloqueada. Este comportamiento no puede ser configurado de ninguna otra manera.

41. El siguiente comando de configuración se puede utilizar para establecer el número máximo de intentos de autenticación posibles de acceso de un usuario remoto. Se aconseja establecer el número de intentos en 3:

```
aaa authentication attempts max-fail <number of failures>
```

6.3 ADMINISTRACIÓN DEL PRODUCTO

6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA

42. El dispositivo se puede gestionar de manera local usando un cable de consola (ver sección 5 FASE DE INSTALACIÓN).

43. Una vez configurada la autenticación de usuarios (sección 6.2 Autenticación), generadas las claves criptográficas (sección 6.5.3 Túnel SSH) y configurado el servidor de nombres de dominio (sección 6.5.2 Configuración de Servicios), el acceso SSH estará habilitado, y el dispositivo se puede gestionar de manera remota.

6.3.2 CONFIGURACIÓN DE ADMINISTRADORES

44. La contraseña de administrador se configura usando el comando "`enable secret <password_administrador>`" y debe ser de al menos 15 caracteres y contener al menos un número y uno de los caracteres especiales mencionados anteriormente (ver sección 6.2 AUTENTICACIÓN).

6.4 GESTIÓN DE CERTIFICADOS

45. Los certificados en el equipo VoyagerVM4.0 se usan para autenticar la identidad del sistema local al conectar de manera segura con otros dispositivos. A su vez, se permite importar certificados de terceros dispositivos servirá para autenticar dichos dispositivos ante el dispositivo local.
    NOTA: No hay una limitación específica que impida usar certificados autofirmados.

46. Ejemplos de uso de dichos certificados incluye añadir un certificado para el servidor https (Sección 6.5.2) o el uso de SDWAN en modo "pki-DTLS" [REF10].

47. KlasOS permite crear solicitudes de firma de certificados (certificate signing request – CSR), almacenar y gestionar certificados a través de "trustpoints".

48. Para generar un trustpoint, el dispositivo pasa por las siguientes fases:

    a) Configuración de las claves: El dispositivo debe tener las claves RSA generadas

    b) Información del dispositivo: La información "subj" debe ser configurada.

c) Generación de la solicitud de firma de certificado: El dispositivo genera una CSR para ser firmada por una autoridad de certificados (certificate authority - CA)

6.4.1.1 GENERACIÓN E INCLUSIÓN DE CERTIFICADOS

1. **Creación de claves:** Para crear una clave nueva se utiliza el comando:

```
crypto key generate [ec|rsa] general-keys modulus [2048|3072|4096]
label <mylabel>
```

2. **Creación de trustpoint:** Para configurar un trustpoint, usar la siguiente configuración:

```
certmgr trustpoint <trustpoint name> RSA
```

3. **Hacer referencia a la clave:** Para ello usar la "label" previamente configurada:

```
key-id <mylabel>
```

4. **Asignar al trustpoint un valor correcto de "subj":** Usar la configuración:

```
subj "/CN=yourdomain.com"
```

5. **Generar la solicitud de firma de certificado:** Usar el siguiente comando:

```
certmgr generate CSR trustpoint <trustpoint name> flash: <CSR filename>
```

NOTA: El archivo se generará en la flash:

6. **Obtener el certificado de una CA a partir del archivo CSR:** Usar la CA preferida para firmar el archivo CSR y obtener el certificado para el dispositivo. El archivo CSR puede ser mostrado usando el comando:

```
more flash: <CSR filename>
```

7. También es posible exportar via SCP el fichero con el comando:

```
copy flash: scp:
```

NOTA: Los parámetros necesarios como la IP del servidor, el usuario o el nombre del fichero a transferir se solicitarán al usuario una vez ejecutado el comando.

8. **Copiar el certificado de la CA y del dispositivo a la flash:** Copiar ambos certificados al equipo usando el comando:

```
copy scp: flash:
```

9. **Hacer referencia a los certificados en el trustpoint:** Usar la siguiente configuración:

```
certmgr trustpoint mytruspoint RSA
device-cert flash: device_cert.pem
ca-cert-chain flash: CA_cert_chain.pem
```

10. **Configurar un identificador de referencia para un trustpoint:** Usar la siguiente configuración:

```
certmgr trustpoint mytruspoint RSA
reference-id <FQDN or IPv4/IPv6]
validation identifier-check strict
```

11. **Comprobar el estado del trustpoint/certificado:** Se puede usar los comandos:

```
show certmgr trustpoints
show certmgr trustpoints servertp
```

6.5 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

6.5.1 CONFIGURACIÓN DE INTERFACES

49. Para configurar una interface del VoyagerVM4.0 habilite el modo privilegiado (enable) primero y luego acceda al modo de configuración (configure terminal).

50. El artículo [REF3] contiene información adicional sobre las configuraciones básicas de una interface (IP, máscara de red…).

51. El VoyagerVM4.0 dispone de las siguientes interfaces:

    - 2 interfaces 2.5Gigabit Ethernet RJ45. Para acceder al modo de configuración de estas interfaces utilice uno de los siguientes comandos (cada comando configura una interfaz):

```
interface Ethernet 0/0
interface Ethernet 0/1
```

    - 4 interfaces 25Gigabit SFP28. Para acceder al modo de configuración de estas interfaces utilice uno de los siguientes comandos (cada comando configura una interfaz):

```
interface Ethernet 1/0
interface Ethernet 1/1
interface Ethernet 1/2
interface Ethernet 1/3
```

52. Interfaces virtuales de switching (vSwitch). Para acceder al modo de configuración de estas interfaces introduzca el siguiente comando (Siendo X el identificador deseado para la interfaz virtual):

```
interface vSwitch X
```

53. Interfaces virtuales de túneles SDWAN (software defined wide area network). Para acceder al modo de configuración de estas interfaces introduzca el siguiente comando (Siendo X el identificador deseado para la interfaz de túnel SDWAN):

```
interface sdwan X
```

6.5.2 CONFIGURACIÓN DE SERVICIOS

54. El dispositivo permite habilitar o deshabilitar diversos servicios de red y administración que deben configurarse de forma controlada para garantizar el cumplimiento de los requisitos de seguridad. A continuación, se detallan los comandos que el administrador puede utilizar desde el modo de configuración para gestionar cada uno de estos servicios.

55. El servicio DNS integrado en el dispositivo puede habilitarse o deshabilitarse según las necesidades de la red. A continuación, se muestran los comandos para iniciar o detener el servidor DNS desde el modo de configuración global.

    - Servidor DNS. Para iniciar el servicio local de servidor DNS y que el VoyagerVM4.0 actúe como servidor DNS hay que usar el comando:

```
ip dns server
```

- Para detener el servicio local de servidor DNS usar el comando:

```
no ip dns server
```

56. El servicio de servidor NTP está deshabilitado por defecto, y debe permanecer deshabilitado para asegurar la configuración segura de Common Criteria (CC) y el cumplimiento con el ENS alto. Si por alguna razón se hubiera habilitado el servicio por el cual el VoyagerVM4.0 actúa como servidor NTP, se debe usar el siguiente comando para deshabilitarlo:

```
no ntp master
```

57. El equipo permite habilitar un servidor HTTPS para la acceder a una interfaz web para monitorizar el estado de las interfaces del equipo. Esta funcionalidad se controla desde el modo de configuración global y permite iniciar, detener o asociar un certificado concreto al servicio. Los siguientes comandos muestran cómo gestionar el servidor HTTPS.

58. Servidor HTTPS. Para iniciar el servidor HTTPS usar el comando:

```
ip http secure-server
```

59. Si se desea especificar un certificado específico, se puede usar el comando:

```
ip http secure-server certmgr <trustpoint>
```

60. Para más información sobre trustpoints, ver la sección 6.4.

61. Para detener el servidor HTTPS usar el comando:

```
no ip http secure-server
```

NOTA: Es posible limitar el acceso a los servicios del VoyagerVM4.0 usando listas de control de acceso (ACL). Para acceder a la documentación sobre la configuración de ACL ver [REF11]

62. El dispositivo permite redirigir los registros de eventos a un servidor de syslog remoto para su centralización y análisis. Esta práctica es recomendable para cumplir con requisitos de auditoría y trazabilidad.

63. Para configurar que los logs sean enviados a un servidor de syslog, usar el comando:

```
logging host <IP or hostname> [transport <udp or tcp> port <portid>]
```

64. Para habilitar el acceso seguro por línea de comandos mediante SSH, es necesario generar previamente las claves criptográficas del dispositivo (ver sección 6.5.3 Túnel SSH). Antes de crear dichas claves, se debe definir un nombre de dominio en el equipo, requisito indispensable para el proceso de generación.

NOTA: Este nombre de dominio no tiene porque ser un dominio interno de la organización, a menos que el equipo vaya a usarse como el servidor DNS del dominio. En este caso, el nombre del dominio será usado para resolución DNS y debe estar en línea con el dominio de la organización para manterner la coherencia en la resolución de nombres.

A continuación, se indica el comando para configurar el nombre de dominio:

```
ip domain-name <domain>
```

6.5.3 TÚNEL SSH (PARA "TRUSTED CHANNEL")

65. El VoyagerVM4.0 utiliza SSH para enviar los mensajes syslog desde el propio equipo hasta el servidor remoto de syslog.

66. El cliente SSH del sistema operativo KlasOS Keel solamente soporta SSH v2. Otras versiones no están soportadas (ejemplo: v1).

67. Además, el cliente está restringido a los siguientes algoritmos:

    - Encriptación: AES-CTR-128, AES-CTR-256, AES-CBC-256 o AES-CBC-128
    - Autenticación: SSH-RSA, ECDSA-SHA2-NISTP256 o ECDSA-SHA2-NISTP384
    - Integridad: HMAC-SHA1, HMAC-SHA2-256, o HMAC-SHA2-512
    - Intercambio de claves: DIFFIE-HELLMAN-GROUP14-SHA1, ECDH sobre NIST P256 con SHA2 o ECDH sobre NIST P384 con SHA2.

    NOTA: Estos algoritmos no son configurables por un administrador. Por el contrario, estos algoritmos serán usados dependiendo del algoritmo que use el servidor SSH remoto y el tipo de clave generada en el VoyagerVM4.0 (limitada a los algoritmos anteriormente citados).

6.5.3.1 AÑADIR CLAVE PÚBLICA PARA SERVIDOR SSH/SYSLOG REMOTO

68. Para generar una clave en el VoyagerVM4.0, ir a la Sección 6.6 Gestión de claves criptográficas. Una vez generada la clave criptográfica, exportar la clave pública del VoyagerVM4.0 al servidor de syslog.

69. Dicha clave se encuentra en: `/home/<user>/.ssh/authorized_keys`

70. Si se desea obtener la clave en formato SECSH, se puede utilizar el comando:

```
show ip ssh
```

71. Y la tercera línea será la clave (terminada en ==). Ejemplo de salida del comando:

```
SSH Enabled - version 2
Keys in SECSH format:
ecdsa-sha2-nistp384 AAAAE2VjZHNhLXNoYTItbmlzdHAzODQAAAAIbmlzdHAzODQAAABhBDmTldLQ
TazBRPog7uKtSoAryCtyb73YZCOPZcVAZ4+JAbvfIsicvzWZ+9APv3XvWwpEClau2U/CAXqfYpuD+EqT
Y/chx3Hvo22UeKDwyHa4Va4fgCMuEEhoKz/ai9wiRA== ec-key-384
```

72. Así pues, en el ejemplo anterior, la clave en formato SECSH sería:

```
ecdsa-sha2-nistp384
AAAAE2VjZHNhLXNoYTItbmlzdHAzODQAAAAIbmlzdHAzODQAAABhBDmTldLQTazBRPog7
uKtSoAryCtyb73YZCOPZcVAZ4+JAbvfIsicvzWZ+9APv3XvWwpEClau2U/CAXqfYpuD+E
qTY/chx3Hvo22UeKDwyHa4Va4fgCMuEEhoKz/ai9wiRA==
```

6.5.3.2 AÑADIR CLAVE DEL SERVIDOR SSH/SYSLOG REMOTO

73. Lo primero es asegurarse que está habilitada la comprobación estricta de las claves criptográficas de cada dispositivo. Para configurar este parámetro, un administrador debe introducir esta línea de configuración desde el modo de configuración:

```
ip ssh strict hostkey checking
```

74. Después hay que añadir la clave pública del servidor de SSH/Syslog remoto a la lista de dispositivos conocidos. Para ello, usaremos las siguientes líneas de configuración:

```
ip ssh known-hosts
key-string <server ip address> <public key algorithm> <key data>
```

75. Comando de ejemplo:

```
key-string                          192.168.1.9                          ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQCg3EmANUfJ+yWMq3ZLdCetmujs24f6xpeXI7VQe
ocmvDaZwy+qPJoxQ8szSHKlKBCoMd9eUgw0NM4aH6927Ba8P2tnxXZhXoSHp9ZKE4zmK/
+nHVU9QfdefYBH/YOGx4qum0KbXNHICDEtIw9df41Sanfqn2KXG/sHWLRb8N08CiO9+5/
JQWYVMkNqDo46e2T8Ie08Rr9+VljvpkhGc7p0P3TYfs2I21rLYpRKXCje1uIr612zEh0e
dnuzgsRilXsn09ckaSSxECoeRptoim5Xsui6JqRpX5hc8j3u+U9ROY2XJhzCJ6zD97qPB
YRhKYiN1LrfMNA4XEnvRwh96WQr
```

76. Para asegurarse que la clave ha sido importada correctamente, podemos usar el siguiente comando:

```
show ip ssh known-hosts
```

77. Para eliminar una entrada específica de la lista de dispositivos conocidos, hay que usar las siguientes líneas de configuración:

```
ip ssh known-hosts
no key-string <server ip address> <public key algorithm>
```

78. También es posible eliminar todas las entradas de dispositivos conocidos de una sola vez usando el comando:

```
clear ip ssh known-hosts
```

79. Eliminar entradas de dispositivos conocidos generará una entrada en el log del sistema.

6.5.3.3 CONFIGURAR EL TÚNEL SSH

80. Para configurar el túnel SSH en el VoyagerVM4.0 hay que configurar la siguiente línea:

```
ssh tunnel username <username> host <syslog server IP> localport 50514
remoteport 514
```

81. El puerto local (local port) puede ser cualquier puerto que no esté en uso en el VoyagerVM4.0.

82. El puerto remoto (remote port) debe el ser el puerto en el que está escuchando el servidor syslog remoto.

83. El intento de conexión del túnel SSH será registrado en el log del sistema. De igual manera, una autenticación correcta o un fallo en autenticarse con el dispositivo remoto también causarán una entrada en el log del sistema.

84. Para terminar el túnel SSH, se debe configurar lo siguiente:

```
no ssh tunnel username <username> host <syslog server IP> localport
50514 remoteport 514
```

85. Los parámetros deben coincidir con el túnel anteriormente creado para terminarlo. La finalización del túnel generará una entrada en el log del sistema.

86. Mientras el túnel está activo, se procederá a renegociar las claves cada hora, o antes si el tráfico del túnel ha llegado a 1GB, lo que ocurra primero.

6.6 GESTIÓN DE CLAVES CRIPTOGRÁFICAS

87. Las claves criptográficas son necesarias para iniciar la funcionalidad de SSH (cliente y servidor). Dichas claves también pueden ser usadas en trustpoints como se indica en la sección 6.4 Gestión de Certificados.

88. Para crear una pareja de claves RSA, desde el modo EXEC privilegiado usar el siguiente comando:

```
crypto key generate rsa general-keys modulus <2048|3072|4096> label
<label name>
```

89. También se pueden generar claves ECDSA con el comando:

```
crypto key generate ec keysize <256|384> label <label name>
```

90. Las claves privadas no son visibles, pero para ver las claves públicas disponibles use el comando:

```
show crypto key mypubkey <all|rsa|ec>
```

91. Para eliminar una clave almacenada en la flash del equipo usar el siguiente comando:

```
crypto key zeroize <ec|rsa> <label name>
```

92. Para eliminar todas las claves del sistema usar el comando:

```
crypto key zeroize
```

NOTA: Se recomienda usar este comando durante un reseteo del sistema a un estado por defecto (salido de fábrica). Eliminar las claves desactivará los servicios asociados a dichas claves (como SSH).

6.7 SERVIDORES DE AUTENTICACIÓN

93. KlasOS Keel permite integrar el dispositivo con servidores de autenticación externos para centralizar la gestión de credenciales y políticas de acceso. Actualmente se soportan los protocolos TACACS+ y RADIUS, cuyas guías de configuración están disponibles en los enlaces que se indican a continuación.

    - Para realizar la configuración de TACACS+ seguir el procedimiento definido en [REF4].

94. Para realizar la configuración de RADIUS seguir el procedimiento definido en [REF5].

6.8 SINCRONIZACIÓN

95. Aunque el VoyagerVM4.0 tiene un reloj interno que puede ser utilizado como origen para la fecha y hora del equipo, esta funcionalidad no debe ser utilizada y solamente se usará un servidor NTP para sincronizar fecha y hora del equipo.

96. Una modificación de la fecha/hora del sistema generaría un mensaje en el log del sistema.

6.8.1 USO DE SERVIDOR NTP EXTERNO

97. El sistema debe sincronizarse con un servidor NTP (network time protocol) externo usando NTPv3 con el comando:

```
ntp server <ntp server IP or FQDN>
```

98. Si el servidor NTP remoto requiere autenticación, primero habría que configurar la clave y luego vincularla al servidor NTP configurado. Toda la configuración a aplicar sería la siguiente:

```
ntp authenticate
ntp authentication-key 1 sha1 <shared-secret>
ntp trusted-key 1
ntp server <ntp_server_IP or FQDN> key 1
```

6.9 ACTUALIZACIONES

99. Las instrucciones detalladas para la actualización de la imagen del sistema de forma segura se encuentran en [REF8].

100. Al descargar el software, por favor, tomar nota del checksum. Ejemplo para KlasOS v5.4.0:

Latest Common Criteria Certified release

KlasOS.keel.v5.4.0rc7.bin	**md5:** 25041e36f6b19b4ded60bbd71f025a43
KlasOS.keel.v5.4.3rc2.bin	**md5:** 90dc89a92d510c5d3adaa9dd1909330d

101. Una vez descargado, compruebe el checksum para asegurarse de que coincide. Si no coincide, ha habido algún tipo de corrupción o fallo en la transferencia y hay que volver a descargar la imagen de nuevo.

6.10 AUTO-CHEQUEOS

102. El sistema operativo KlasOS dispone de comprobación de la integridad de la imagen del sistema operativo al arranque. Intentar arrancar una imagen no firmada o corrupta provocará un fallo en ese arranque y el sistema procederá al arranque de una imagen interna que se cargará para que el equipo arranque y se le pueda volver a actualizar a una imagen correcta usando el procedimiento disponible en [REF8].

103. Para comprobar la integridad de las imágenes antes de su uso, se puede usar el comando:

```
verify /md5 flash: <image name>
```

6.11 ALTA DISPONIBILIDAD

104. Para garantizar la continuidad del servicio y minimizar el impacto de fallos en la red, KlasOS Keel ofrece compatibilidad con distintos protocolos y mecanismos de alta disponibilidad. Estos permiten implementar redundancia y balanceo de carga de forma eficiente. A continuación, se enumeran los principales protocolos soportados y la referencia a su documentación de configuración.

105. KlasOS Keel soporta varios protocolos para alta disponibilidad tales como:

- VRRP es un protocolo de redundancia de routers definido en la RFC 5798 que permite asignar dinámicamente un router virtual a un grupo de routers físicos en la misma red. La documentación para configurar VRRP en KlasOS se puede encontrar en [REF9].
- SD-WAN es una arquitectura de red que separa el plano de control del plano de datos para gestionar de forma centralizada las conexiones WAN. La documentación para entender y configurar KlasOS Keel SDWAN se puede encontrar en [REF6].

6.12 AUDITORÍA

6.12.1 REGISTRO DE EVENTOS

106. Los siguientes logs se usan para depuración, auditoría, filtrado de paquetes y resolución de problemas.

6.12.1.1 AUDIT LOG

107. Aquí se registran todos los comandos que el usuario introduce en la línea de comandos, incluyendo:

- Cambios relacionados con la seguridad.
- Generación/importación, modificación o eliminación de claves criptográficas.
- Restablecimientos de contraseñas.
- Inicio y parada de servicios.

108. Los mensajes del log usan el siguiente formato:

```
[Date and Time] [IP address or Hostname] CLI[process id]:
(admin) [user] [Origin of CLI command] [CLI command] : [success|failure]
```

109. Si un comando se introduce con privilegios de administrador, el log añade la etiqueta (admin) antes del nombre del usuario que lo ejecutó. Ejemplo:

```
2024-04-30T20:31:44.176220+00:00 KlasOS CLI[10476]: (admin) (klas)
(KlasOS) exit : Success
```

110. Si el comando se ejecuta desde el modo usuario, el mensaje solamente contendrá el nombre de usuario. Ejemplo:

```
2024-04-30T20:31:44.176220+00:00 KlasOS CLI[10457]: (klas)
(KlasOS) show clock : Success
```

111. Este log no se puede parar o desactivar ni por el administrador, está siempre activo.

112. Para mostrar el Audit log del equipo se necesitan permisos de administrador y se pueden usar los comandos:

- Para mostrar el contenido más reciente del log:

```
show logging audit
```

- Para mostrar el contenido del log en tiempo real use el siguiente comando (Use Ctrl+C para volver a la consola):

```
show logging audit continuous
```

- Para mostrar el contenido completo del log:

```
show logging audit full
```

- La redirección de los mensajes del Audit logging a la consola local está desactivada por defecto, pero puede activarse por un administrador en el modo EXEC priv usando el comando:

```
logging audit local
```

- Para volver a desactivarlo se puede usar el comando:

```
no logging audit local
```

6.12.1.2 SYSTEM LOG

113. Aquí se registran todos los mensajes generales del sistema, incluyendo:

- Eventos de autenticación de usuarios y administradores tanto para sesiones remotas como locales.
- Mensaje de fallo o éxito del auto-chequeo de la integridad del firmware.
- Modificaciones del reloj del sistema.

114. Sigue los formatos:

```
[Date and Time] [Hostname or IP address]:[tag]: [log message][Date and
Time] [Hostname or IP address] process[process id]: [tag]: [log message]
```

115. Este log no se puede parar o desactivar ni por el administrador, está siempre activo.

116. Todos los logs incluyen fecha y hora del evento, el tipo de evento, el usuario y si se procesó correctamente o falló.

117. Además, hay una entrada en el log si algún sistema de almacenamiento local llega al 75% de su capacidad. Dicho umbral no es configurable. Se recomienda que, en este umbral, el administrador borre archivos innecesarios de manera manual para evitar que el sistema de almacenamiento se llene por completo. El espacio restante de cada sistema de almacenamiento puede ser consultado en cualquier momento con el comando EXEC priv:

```
dir <disk0: or flash: or nvram:>
```

118. Cada log se rota aproximadamente cada 10MB aunque nunca superará los 20MB por fichero. El administrador debe asegurarse de que el sistema almacenamiento nunca se llene por completo para evitar inestabilidad en el sistema.

    NOTA: El sistema no borra ningún log, si se llega al límite del almacenamiento simplemente no puede escribir más por falta de espacio.

119. Para comprobar el nombre y el tamaño actual del log, se puede usar el comando:

```
show log files
```

120. Para borrar archivos, se debe utilizar el comando:

```
delete <disk0: or flash: or nvram:> filename
```

121. Para mostrar el System log del equipo se necesitan permisos de administrador y se pueden usar los comandos:

```
show logging
```

122. Nos mostrará el contenido más reciente del log

```
show logging continuous
```

123. Nos mostrará el contenido del log en tiempo real. Use Ctrl+C para volver a la consola.

```
show logging full
```

124. Nos mostrará el contenido completo del log.

125. Todos los eventos de autenticación se muestran con el siguiente formato:

```
[Date and Time] [IP address of ToE] [process]: [tag]: [authentication message detailing the user name and the location of the authentication attempt]
```

126. Se puede modificar la prioridad de los mensajes que se muestran en la consola local. Por defecto la prioridad es “critical”, pero se puede cambiar con el comando:

```
logging console debugging
```

127. Para desactivar el logging en la consola por completo se puede usar el comando:

```
no logging console
```

6.12.2 ALMACENAMIENTO LOCAL

128. El equipo VoyagerVM4.0 dispone de un disco local de arranque (NVMe de 1TB) con varias particiones:

- nvram: Principalmente utilizada para almacenar la configuración de arranque (startup-config).
- flash: Usada principalmente para las imágenes de arranque del sistema operativo KlasOS Keel, la configuración actual del sistema (running-config) y las claves criptográficas.
- disk0: Partición del disco de arranque para almacenar los discos virtuales de las máquinas virtuales (QCOW2, ISO, etc).

Aparte, el equipo también dispone de dos discos (NVMe E1.S) para almacenamiento de gran capcidad (hasta 15.36TB cada uno) con las siguientes particiones:

- disk1: Partición principal del primer disco de capacidad para almacenar los discos virtuales de las máquinas virtuales (QCOW2, ISO, etc).
- disk2: Partición principal del segundo disco de capacidad para almacenar los discos virtuales de las máquinas virtuales (QCOW2, ISO, etc).

6.12.3 ALMACENAMIENTO REMOTO

129. Todos los logs se pueden enviar a un servidor de syslog remoto, pero esta configuración debe hacerse sobre un canal seguro a través de SSH (ver Sección 6.5.3 Túnel SSH). Si se ha configurado un servidor de syslog remoto, los mensajes son enviados de forma simultánea al log local y al remoto.

130. Para transferir archivos de manera segura usando SCP desde un servidor remoto a la partición flash local, use el comando:

```
copy scp: flash:
```

131. Para transferir la partición principal del disco local, use el comando:

```
copy scp: disk0:
```

132. Remote syslog: Para configurar que los logs sean enviados a un servidor de syslog remoto, use el comando:

```
logging host <IP or hostname> [transport <udp or tcp> port <portid>]
```

6.13 BACKUP

133. Para cumplir con los requisitos del ENS es necesario guardar y respaldar la configuración del equipo de forma periódica para garantizar la recuperación ante fallos o cambios no deseados. KlasOS Keel permite tanto almacenar la configuración en la memoria de inicio como exportarla o restaurarla de manera segura mediante SCP hacia/desde un servidor remoto de copias de seguridad.

134. Para guardar la configuración actual del equipo, en el modo PRIV EXEC, se usa el comando:

```
copy running-config startup-config
```

135. Para exportar la configuración del equipo de manera segura a un servidor remoto de copias de seguridad, en el modo PRIV EXEC, se usa el comando:

```
copy startup-config scp:
```

NOTA: Tras introducir este comando, el sistema preguntará por la IP del sistema remoto, el usuario y el nombre de fichero para intentar la conexión y posterior transferencia.

136. Para restaurar la configuración del equipo localizada en un servidor seguro con una copia de seguridad, desde el modo PRIV EXEC, se usa el comando:

```
copy scp: startup-config
```

NOTA: Tras introducir este comando, el sistema preguntará por la IP del sistema remoto, el usuario y el nombre de fichero para intentar la conexión y posterior transferencia.

7 REFERENCIAS

[REF1] Helpdesk de Klas:
https://helpdesk.klasgov.com

[REF2] RFC5798:
https://datatracker.ietf.org/doc/html/rfc5798

[REF3] Keel Guide: KlasOS Getting Started Guide
https://helpdesk.klasgov.com/s/article/klasos-initial-configuration1

[REF4] Keel Cybersecurity: Configuring TACACS+ Authentication
https://helpdesk.klasgov.com/s/article/configuring-tacacs-authentication-in-klasos-on-trx1

[REF5] Configuring 802.1x Authentication
https://helpdesk.klasgov.com/s/article/configuring-voyageresr-for-8021x-authentication

[REF6] Keel SD-WAN: Introduction to SD-WAN
https://helpdesk.klasgov.com/s/article/introduction-to-sdwan1

[REF7] VoyagerVM4.0 Hardware Guide
https://helpdesk.klasgov.com/s/article/VoyagerVM-4-0-Hardware-Guide

[REF8] Keel Guide: Upgrading Keel Firmware
https://helpdesk.klasgov.com/s/article/upgrading-klasos-keel-x86-baremetal-software-on-trx-r1

[REF9] VRRP Configuration Guide
https://helpdesk.klasgov.com/s/article/Keel-Networking-VRRP-Configuration-in-KlasOS-Keel

[REF10] Keel SD-WAN: SD-WAN Encryption and Encryption-Mode
https://helpdesk.klasgov.com/s/article/sdwan-encryption1

[REF11] Keel Firewall: ACL Guide
https://helpdesk.klasgov.com/s/article/ACL-Guide-For-KlasOS-Firewall

8 ABREVIATURAS

5G	Fifth Generation
AAA	Authentication Authorization Accounting
ACL	Access Control List
CC	Common Criteria
CLI	Command Line Interface
DNS	Domain Name System
ECDSA	Elliptic Curve Digital Signature Algorithm
ENS	Esquema Nacional de Seguridad.
EXEC	Executive
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICMP	Internet Control Message Protocol
IP	Internet Protocol
ISO	International Organization for Standardization
KVM	Kernel-based Virtual Machine
LTE	Long Term Evolution
MD5	Message Digest 5
NTP	Network Time Protocol
NVMe	Non-Volatile Memory Express
PRIV_AUTH_FAIL	Privilege Authentication Fail
QCOW2	QEMU Copy On Write version 2
R2	Revision 2
RADIUS	Remote Authentication Dial-In User Service
RFC	Request for Comments
RJ45	Registered Jack 45
RSA	Rivest Shamir Adleman
SCP	Secure Copy Protocol
SDWAN	Software Defined Wide Area Network
SFP+	Small Form-factor Pluggable Plus
SHA512	Secure Hash Algorithm 512
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSHv2	Secure Shell version 2

STIC	Seguridad de las Tecnologías de la Información y las Comunicaciones
SYS	System
Syslog	System Logging
TACACS+	Terminal Access Controller Access Control System Plus
ToE	Target of Evaluation
TRX	Transceiver
TTY	Teletypewriter
VRRP	Virtual Router Redundancy Protocol
vSwitch	Virtual Switch
WAN	Wide Area Network
x86	Extended 86