centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1304

Procedimiento de empleo seguro
CARMEN 7.2.4

Marzo 2022

MINISTERIO DE DEFENSA

Catálogo de Publicaciones de la Administración General del Estado
https://cpage.mpr.gob.es

cpage.mpr.gob.es

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

CCN centro criptológico nacional

CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2022.03.17 13:29:33 +01'00'

Pº de la Castellana 109, 28046 Madrid
© Centro Criptológico Nacional, 2022
NIPO: 083-22-065-0
Fecha de Edición: marzo de 2022

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 DE DESPLIEGUE E INSTALACIÓN 6
4.1 ENTREGA SEGURA DEL PRODUCTO 6
4.2 ENTORNO DE INSTALACIÓN SEGURO 7
4.3 REGISTRO Y LICENCIAS 7
4.4 CONSIDERACIONES PREVIAS 7
4.5 INSTALACIÓN 7
5. FASE DE CONFIGURACIÓN 10
5.1 AUTENTICACIÓN 10
5.2 ADMINISTRACIÓN DEL PRODUCTO 10
5.2.1 ADMINISTRACIÓN LOCAL Y REMOTA 10
5.2.2 CONFIGURACIÓN DE ADMINISTRADORES 11
5.2.3 POLÍTICA DE CONTRASEÑAS Y PARÁMETROS DE SESIÓN 12
5.3 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS 13
5.4 CONFIGURACIÓN DE PROTOCOLOS SEGUROS 13
5.5 GESTIÓN DE CERTIFICADOS 13
5.6 SINCRONIZACIÓN HORARIA 14
5.7 ACTUALIZACIONES 14
5.8 SNMP 15
5.9 ALTA DISPONIBILIDAD 15
5.10 AUDITORÍA 15
5.10.1 REGISTRO DE EVENTOS 15
5.10.2 ALMACENAMIENTO LOCAL 16
5.10.3 ALMACENAMIENTO REMOTO 16
5.11 BACKUP 16
5.12 SERVICIOS DE SEGURIDAD 16
6. FASE DE OPERACIÓN 18
7. CHECKLIST 19
8. REFERENCIAS 20
9. ABREVIATURAS 21

1. INTRODUCCIÓN

1. **CARMEN**, Centro de Análisis de Registros y Minería de EveNtos, es un desarrollo de S2 Grupo en colaboración con el Centro Criptológico Nacional para la identificación del compromiso por parte de amenazas persistentes avanzadas (APT), constituyendo la primera capacidad española, basada en conocimiento y tecnología nacionales, en este sentido.
2. El proceso de identificación de una amenaza de este tipo (APT) depende de las aptitudes de un analista y de la información de la que dispone. CARMEN permite adquirir información de diferentes protocolos de red (http/s, tls, smtp, dns, netbios, icmp, netflows y la información del endpoint Claudia).
3. La información adquirida se analiza dando indicios al analista para poder investigar si esas pistas constituyen una amenaza real. Cada analista tiene asignados unos roles concretos en la aplicación que le permiten ver sólo las pantallas asociadas a este, con lo que sólo verá la información asociada a dichas pantallas
4. **CARMEN** es una solución software de adquisición, procesamiento y análisis de información para soportar el proceso de identificación de amenazas a partir de los tráficos de una red.

2. OBJETO Y ALCANCE

5. El presente documento tiene como objetivo detallar las configuraciones de seguridad del producto **CARMEN 7.2.4**, de forma que la protección y funcionamiento del producto se realice de acuerdo a unas garantías mínimas de seguridad.
6. Carmen se distribuye en un *appliance* físico con las siguientes características: 2 CPU de 8 núcleos cada uno, 64 GB RAM, 2 HDD en RAID10 de 300GB cada uno y 2 HDD de 600GB para el almacenamiento. Tiene además una fuente de alimentación redundante y 8 interfaces de red en dos tarjetas de cuatro interfaces cada una.
7. Adicionalmente **CARMEN** se ejecuta sobre el sistema Operativo CentOS 7.5.1804 y de usa los siguientes softwares de terceros: Gestor de colas RabbitMQ 3.5.1, gestor de base de datos PostgreSQL 9.2.24, gestor de almacenamiento de logs ElasticSearch 6.3.0, máquina virtual de JAVA 1.8.0_191, interprete Python, versión 2.7.5 y servidor de aplicaciones Apache Tomcat, versión 8.5.35.

3. ORGANIZACIÓN DEL DOCUMENTO

8. El presente documento se estructura en las secciones indicadas a continuación:

- **Apartado 4.** En este apartado se recogen recomendaciones a tener en cuenta durante la fase de despliegue e instalación del producto.
- **Apartado 5**. En este apartado se recogen las recomendaciones a tener en cuenta durante la fase de configuración del producto, para lograr una configuración segura.
- **Apartado 6.** En este apartado se recogen las tareas recomendadas para la fase de operación o mantenimiento del producto.
- **Apartado 7:** En este apartado se recoge la lista de elementos que deben revisarse.
- **Apartado 8:** Referencias.
- **Apartado 9**: Abreviaturas.

4. FASE DE DESPLIEGUE E INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

9. Cuando una organización formaliza la adquisición de **CARMEN**, se solicita al distribuidor de hardware un equipo (*appliance* físico) de las características identificadas para su distribución. Esta configuración es mantenida por un largo periodo de tiempo, minimizando de esta forma los problemas derivados de las modificaciones en las configuraciones hardware.

10. En el momento en el que el equipo es recogido en las instalaciones de S2 Grupo por parte de la empresa de transporte, se comunica a la organización en la que va a realizarse el despliegue los siguientes dos aspectos: la fecha en la que entregará el *appliance* físico por parte del transportista para su recepción en las instalaciones de la organización destinataria; la fecha en la que se desplazará un técnico de S2 Grupo a sus instalaciones para realizar las acciones de despliegue, configuración, y validación final.

11. Además, se facilitará acceso mediante una contraseña al repositorio de distribución albergado en https://minube.s2grupo.es para su posterior distribución.

12. En el repositorio se encontrarán las guías del producto:

    - Guía de usuario del producto (llamada u7.3_ccn.pdf).
    - Guía de administrador del producto (llamada a7.3_ccn.pdf).

13. Se deberá comprobar su integridad realizando el hash SHA-256 de los documentos y verificando que coincide con los indicados posteriormente. De esta manera, durante la instalación y configuración del *appliance,* la organización puede seguir a través de las guías el procedimiento que el técnico está llevando a cabo. Los hashes de los dos documentos entregados son:

    - La guía de usuario llamada “u7.3_ccn.pdf”, en formato “.pdf”. Esta guía también puede ser descargada tras una autenticación exitosa en la aplicación web de CARMEN y hace referencia a CARMEN_AGD_OPE_v7.3. Su hash sha-256 es:

      43fa1256a1c9ee773961ab6887b5a39bcf90e2354b076b42b4d945834006878f

    - La guía de administrador llamada “a7.3_ccn.pdf” en formato “.pdf” Esta guía también puede ser descargada tras una autenticación exitosa en la aplicación web de CARMEN y hace referencia a CARMEN_AGD_PRE_v7.3. Su hash sha-256 es:

      1d46393a4624bfa032355342cb0285ae4449489996b963b56a195bdf6f61cb3c

14. El técnico encargado debe asegurarse de que el equipo instalado coincide con el número de serie asociado a la organización, y validar mediante un agente que este se encuentre con la configuración definida en el momento de su instalación.

4.2 ENTORNO DE INSTALACIÓN SEGURO

15. El producto debe ubicarse en un CPD, que cuente con las medidas de seguridad adecuadas a la información que procesa, y que pueda establecer las conexiones necesarias para el desarrollo de su funcionalidad. El acceso debe estar restringido al personal autorizado para su gestión.

4.3 REGISTRO Y LICENCIAS

16. El *appliance* se entrega instalado desde S2 al cliente que lo ha comprado. El cliente puede verificar que lo que se le ha entregado corresponde con las firmas de los elementos instalados, así como el número de serie del *appliance* físico dado que quedan registrados en la plataforma EMAS de S2 Grupo, para poder ser verificados en el cliente final, quedando así registro de versión y paquetería. La plataforma es accesible desde internet en: https://emas.s2grupo.es

4.4 CONSIDERACIONES PREVIAS

17. Se recomienda facilitar a S2 la información de configuración de red (IP, direccionamiento, Gateway y DNS). De esta forma dicha información se parametrizará en el producto durante la instalación inicial. En dicho caso se generará un certificado auto firmado para la IP/DOMINIO.
18. Este certificado deberá ser sustituido en la instalación del cliente por el instalador de S2 Grupo, por uno autorizado y reconocido por el cliente.
19. Las contraseñas de los usuarios por defecto se generan en cada instalación de forma única y se almacenan de forma segura en un gestor de contraseñas de S2.

4.5 INSTALACIÓN

20. El administrador del producto deberá validar la versión entregada de CARMEN mediante el agente *checker.py*. Dicho agente se puede obtener del repositorio facilitado por S2, bajo el nombre de *checker.py*. Se deberá descargarlo y ejecutarlo en caso de querer realizar la verificación posteriormente.
21. Deberá ejecutarse mediante el siguiente comando:

    python /usr/local/carmen/agents/checker/checker.py -c /usr/local/carmen/agents/checker/spec.json

22. Para obtener el siguiente mensaje.

```
Comprobando CARMEN 7.2.4
Total de errores: 0
```

Ilustración 1. Verificación de la instalación.

23. Es posible realizar posteriormente la configuración de la red siguiendo los siguientes pasos:

- Acceder al dispositivo mediante SSH.
- Utilizar el siguiente comando:

  Nano /etc/sysconfig/network-scripts/ifcg-eth0

- Tras hacer clic en Enter, se mostrará la información de red configurada. Se deben editar los parámetros *DEVICE, IPADDR, PREFIX y GATEWAT*.
  - DEVICE: es independiente de la configuración de red y se debe introducir el valor *em1.*
  - IPADDR: dirección IP que se asigna a la máquina.
  - PREFIX: mascara de red en formato corto, por ejemplo, *22*.
  - GATEWAY: puerta de enlace de la red, en formato IP.
- Una vez realizados los cambios, pulsar *CTRL+O* para guardar, *Enter* para mantener el mismo nombre de fichero y *CTRL+X* para salir de la edición del fichero.

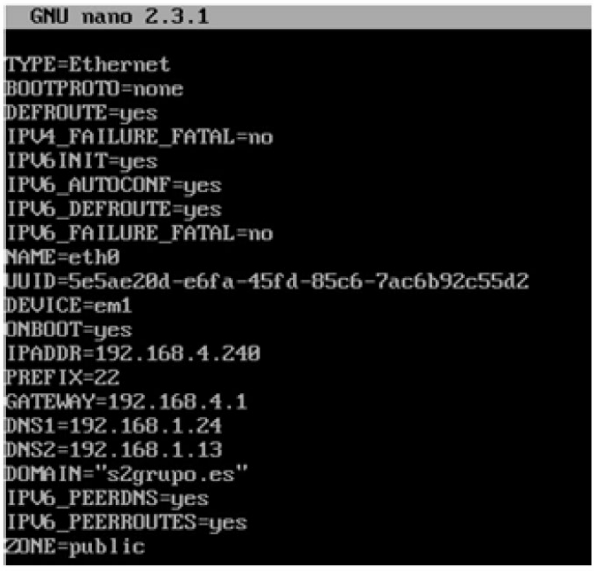

Ilustración 2. Configuración de red.

24. Una vez configurada la dirección IP del dispositivo, se debe editar el fichero hosts mediante el comando *nano /etc/hosts* y se debe cambiar la dirección IP correspondiente a *carmen carmen.s2grupo.es*, por la dirección configurada en IPADDR. Por último, ejecutar el comando *Reboot* para reiniciar el servidor y aplicar los cambios.

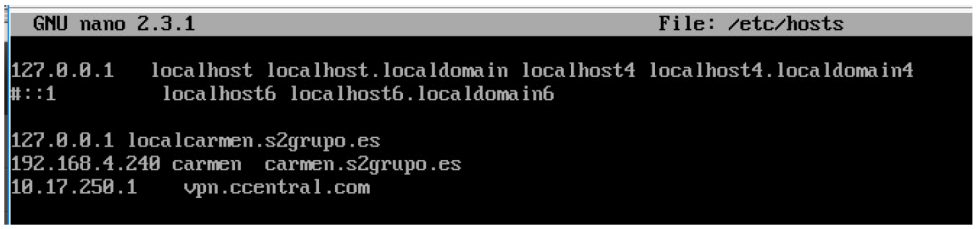

Ilustración 3. Edición del fichero hosts.

5. FASE DE CONFIGURACIÓN

5.1 AUTENTICACIÓN

25. El acceso a CARMEN mediante GUI se realiza utilizando HTTPS sobre TLSv1.2 y está controlado mediante el uso de una pareja de valores usuario y contraseña. Todo usuario que interactúe con el sistema debe haber sido dado de alta previamente por un usuario con permisos de administración (ver apartado 5.2.2 CONFIGURACIÓN DE ADMINISTRADORES).
26. El inicio de sesión en CARMEN 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.
27. Si estos datos son incorrectos, CARMEN notificará el motivo del rechazo e invitará al usuario a introducir los datos nuevamente; si, por el contrario, son correctos, se autorizará el acceso.
28. Estas credenciales se almacenan en la base de datos local cifradas mediante un algoritmo hash. Este algoritmo no es configurable.
29. Las claves de los componentes internos que requieren autenticación (BBDD, gestor de colas…) por defecto están almacenadas en el sistema de ficheros y protegidas por el sistema operativo en el que se ejecuta CARMEN.
30. 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.
31. Las claves de SSH se generan en el momento de la instalación y son únicas para cada instalación.

5.2 ADMINISTRACIÓN DEL PRODUCTO

5.2.1 ADMINISTRACIÓN LOCAL Y REMOTA

32. Se utilizará la interfaz web para la operación del producto y para algunas labores de configuración, como los usuarios y roles. La conexión a esta interfaz se realiza mediante HTTPS sobre TLSv1.2 por defecto.
33. Es desde la interfaz web dónde se gestionan los usuarios de CARMEN y sus roles. Los roles permiten/ocultan las pantallas a las que puede acceder un usuario.
34. Se utilizará para configurar parámetros como la información de red o las comunicaciones del producto la interfaz CLI accesible desde SSH o directamente de forma local desde el propio CPD si fuera necesario. Esta conexión se realiza mediante SSHv2 por defecto. Para este acceso se dispone de los usuarios Carmen y Root del Sistema Operativo.

35. Las restricciones de acceso remoto (SSH o HTTPS) quedan delegadas en la seguridad de redes de la organización.
36. Tan solo se puede acceder al producto remotamente mediante HTTPS o SSH. No existe otro tipo de acceso no seguro como HTTP, Telnet, etc.

5.2.2 CONFIGURACIÓN DE ADMINISTRADORES

37. La aplicación web de CARMEN dispone de cuatro roles preestablecidos, éstos son Administrador, Trabajador, Civil y Analista de Malware. En el caso de los dos primeros, no es posible borrarlos de la aplicación, aunque si se permite su modificación.
38. En función del rol asignado al usuario, éste dispondrá de diferentes capacidades. A continuación, se describen las funciones disponibles para cada rol de la interfaz web configurados por defecto:
    - **Administrador**: Tiene acceso a toda la interfaz web, sin ningún tipo de restricción.
    - **Trabajador**: Tiene limitadas algunas funciones de configuración como pueden ser los roles, los usuarios, las unidades organizativas… Además, en función de la organización, es posible limitar el acceso a algunos eventos a este rol.
    - **Civil**: Tiene más limitadas sus funciones que el rol trabajador. Además de no tener acceso a funciones de configuración, no puede realizar análisis.
    - **Analista Malware**: Es un rol meramente analista, solo tiene visibilidad sobre las pantallas destinadas al análisis de malware.
39. La aplicación permite mediante la pantalla de roles, crear y modificar las visibilidades de estos. Para ello, seguir los siguientes pasos:
    - Desde el menú principal, ir a *Configuración > Roles*.
    - Aparecerá un listado de Roles. Situando el ratón sobre un rol, se podrá borrar o visualizar haciendo clic en los iconos y respectivamente. Tras visualizar un rol, se puede editar el mismo pulsando el icono .
    - Para la creación de un nuevo rol, se deberá hacer clic sobre el icono "+" y seleccionar la opción *Nuevo rol*.

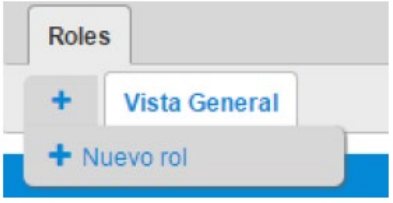

Ilustración 4. Creación de roles

- Se mostrará un formulario donde se debe introducir el *Nombre* que tendrá el nuevo rol y se deberá seleccionar las pantallas a las que tendrá acceso dicho rol haciendo uso de los botones “>” y “<”.
- Finalmente hacer clic en *Guardar*.

40. El producto permite también la gestión y creación de usuarios. Para ello seguir los siguientes pasos:
    - Desde el menú principal, ir a *Configuración > Usuarios*.
    - Se mostrará un listado con los usuarios dados de alta en el sistema. Situando el ratón sobre un usuario, se podrá borrar o visualizar haciendo clic en los iconos y respectivamente. Tras visualizar un usuario, se puede editar el mismo pulsando el icono .
    - Para la creación de un nuevo usuario, se deberá hacer clic sobre el icono “+” y seleccionar la opción *Crear un usuario*.

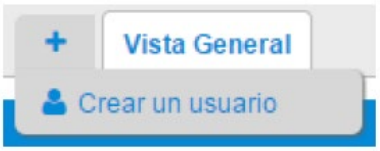

Ilustración 5. Creación de usuarios.

- Se mostrará un formulario donde se debe introducir la información del usuario. En las casillas *Contraseña* y *Confirmar Contraseña* se debe introducir la contraseña de dicho usuario. En el apartado *Roles seleccionados* se añadirá el rol o roles que tendrá el usuario.
- Por último, seleccionar la casilla *Habilitado* para permitir el uso del usuario y hacer clic en *Guardar*.

41. Los usuarios pueden modificar sus contraseñas en cualquier momento en la GUI desde el menú desplegable situado en la esquina superior derecha. Haciendo clic en *Cambio de contraseña*.

5.2.3 POLÍTICA DE CONTRASEÑAS Y PARÁMETROS DE SESIÓN

42. Tras un tiempo de inactividad, se mostrará una ventana indicando que ha caducado la sesión, permitiendo al usuario volver a autenticarse o cerrar la sesión.
43. El tiempo de inactividad es posible configurarlo accediendo a través del menú a la opción *configuración > unidad organizativa*, y editando el campo que indica “caducar sesión”. Por defecto, el tiempo de inactividad está marcado en 25 minutos. Se recomienda configurar un valor máximo de 5 minutos.
44. Para generar contraseñas de los usuarios de la interfaz web y la interfaz de gestión el producto hace uso de la siguiente política de seguridad (no modificable):
    - La contraseña debe tener entre 8 y 64 caracteres.

- La contraseña debe contener al menos una letra, un número y alguno de los siguientes símbolos: !@#$%^&.
- La contraseña nueva y la repetición de contraseña deben ser iguales.

45. El configurador (ssh) puede establecer el periodo de validez de las contraseñas para cumplir con ENS editando el fichero */etc/carmen/carmen-web/config.groovy*, seteando la línea "*carmen.weektime.expired.pass=N*" dónde N es el número de semanas. Se recomienda un valor de dos meses aproximadamente (10 semanas).
46. El configurador (ssh) puede establecer el periodo de validez de una sesión editando el fichero */etc/carmen/carmen-web/config.groovy*, seteando la línea "*carmen.timeout.minutes=N*" dónde N es el número de minutos (por defecto 25).

5.3 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

47. Los únicos puertos (y servicios) abiertos son HTTPS, SSH y, si se configura, recepción de tráfico por syslog (ver apartado 5.12.3 Almacenamiento remoto). El resto de los servicios/puertos son de uso interno y no se exponen.
48. La configuración de los puertos abiertos del sistema se encuentra en /etc/firewall/zones/public.xml, dónde se establecen puertos/servicios expuestos. Se deben mantener todos los puertos cerrados a excepción de los servicios en uso.

5.4 CONFIGURACIÓN DE PROTOCOLOS SEGUROS

49. El acceso a GUI mediante HTTPS está configurado con un certificado firmado por una CA autofirmada en el mismo *appliance*. Se recomienda que este sea actualizado por uno firmado por un CA válida por la organización, para ello deberá informar al configurador de S2Grupo.
50. El producto utiliza por defecto el protocolo TLS versión 1.2 o superior. La configuración de dicho protocolo corresponde al servicio NGINX del *appliance*.
51. El producto utiliza por defecto el protocolo SSHv2. La configuración de dicho protocolo corresponde al Sistema Operativo del *appliance*.

5.5 GESTIÓN DE CERTIFICADOS

52. El *appliance* dispone de un servicio (script) que genera una CA autofirmada y un certificado temporal firmado con dicha CA. Esa creación se realiza con claves suficientemente seguras siguiendo las recomendaciones de CCN-STIC-807 (tamaño de bits de la clave 4096, RSA).
53. El cliente deberá ponerse en contacto con el proveedor S2Grupo para sustituir el certificado autofirmado por uno firmado por una CA válida y reconocida por el organismo.

5.6 SINCRONIZACIÓN HORARIA

54. El producto hace uso del NTP del Sistema Operativo (CentOS 7). Para la configuración del servicio de sincronización horaria (NTP) se deben realizar las siguientes acciones:

    - `$vi /etc/ntp.conf`
    - Añadir/modificar: `server <IP_SERVER_NTP> iburst`
    - `systemctl restart ntpd` [Arrancamos servicio]

55. Se deberá hacer uso de autenticación NTP. Para ello se debe en el archivo `/etc/ntp.conf` del Sistema Operativo.

5.7 ACTUALIZACIONES

56. El proceso de actualización de CARMEN siempre es llevado a cabo por un técnico de S2 Grupo, para ello obtiene la versión a instalar del sistema de registro y configuración para realizar la intervención en las instalaciones de la organización, bien física o remotamente.

57. Este paquete de instalación es accesible para la organización a través de la compartición del repositorio de S2 Grupo albergado en *https://minube.s2grupo.es*. Se denomina <X.Y.Z>.tgz, siendo <X.Y.Z> valores numéricos que permiten identificar de forma unívoca la versión a la que CARMEN va a ser actualizada, incluye el ejecutable update.sh junto con el fichero de instalación y todos los elementos que se van a actualizar, ya sea paquetería o funcionalidad, además del nuevo *spec.json* del que dispone el técnico para validar que la instalación ha sido realizada de manera correcta.

58. Antes de realizar la actualización del sistema de Carmen, el técnico de S2 Grupo debe validar que el hash SHA-256 del paquete que va a instalar corresponde con el que se ha indicado en el gestor de eventos de la organización, comprobando de este modo que no se ha realizado ninguna modificación del paquete.

59. Para consultar el hash del paquete a actualizar se debe ejecutar la siguiente directiva: *sha256sum <X.Y.Z>.tar.gz*

60. Tras asegurarse de que todo es correcto, realiza la actualización ejecutando el *update.sh*.

61. Para validar que la actualización de Carmen ha sido realizada de forma satisfactoria y garantizar la integridad del sistema, se debe ejecutar el agente checker. Para ello se debe copiar en la ruta adecuada el fichero y seguir las siguientes directivas *$python /../checker.py -c /../spec.json*

62. Cabe resaltar que el técnico de S2 Grupo realizará la validación con el fichero *spec.json* específico de la versión instalada que lleva consigo mismo.

63. Tras finalizar su ejecución, el resultado mostrado por el agente confirma que tanto los elementos de control definidos en el sistema, como los permisos asociados a

cada uno de ellos, son los correspondientes a la versión que ha sido actualizada e instalada, mostrando el siguiente mensaje esperado:

Total de errores: 0

64. Si aparecieran errores o discrepancias, se debe asegurar que la directiva ha sido ejecutada con un usuario con los suficientes permisos antes de considerarlo como una posible incidencia en la instalación.
65. Además, el técnico se conecta a la interfaz web y accede al menú ayuda, la opción *acerca de*, y comprueba que, tras la actualización, el *popup* de la aplicación web muestra la versión correcta.

5.8 SNMP

66. La configuración SNMP se realiza desde el fichero */etc/carmen/carmen-web/config.groovy*, añadiendo las siguientes líneas:

```
carmen.snmp.enabled=true
carmen.snmp.OID=<OID>
carmen.snmp.address=<SNMP-IP-address/server-name>
carmen.snmp.adressType=<udp/tcp>
carmen.snmp.community=<SNMP-Community>
```

67. El SNMP se puede usar para enviar las alertas generadas en CARMEN a otro dispositivo externo. No es posible especificar la versión de SNMP que utilizará el producto.

5.9 ALTA DISPONIBILIDAD

68. El producto dispone por defecto de alta disponibilidad en los datos mediante la réplica de la información en dos discos. Sin embargo, estos discos se encuentran en el mismo *appliance*, por lo que no dispondrá de alta disponibilidad en caso de que el servidor de error, se apague o sufra alguna otra avería.

5.10 AUDITORÍA

5.10.1 REGISTRO DE EVENTOS

69. Los eventos que genera CARMEN son las alertas (ejecuciones exitosas de IOC, o analizadores con resultados). Estos se pueden enviar a sistemas externos, aparte de quedar almacenados en base de datos.
70. Los accesos al sistema quedan registrados en la base de datos y un administrador los puede ver desde la interfaz. En ella se ve el usuario, la hora en la que se ha intentado conectar, la IP y si ha sido éxito o no.
71. Además en los registros de tomcat (/var/log/tomcat/catalina.yyy-MM-dd.log se muestra la información de los accesos del usuario por la plataforma: *User: <usuario> acess to <pantalla>*

5.10.2 ALMACENAMIENTO LOCAL

72. Todos los registros de acceso al sistema se almacenan en base de datos y logs. Estos logs rotan periódicamente para garantizar que la máquina no se quede sin espacio.
73. La periodicidad de rotación por defecto es de 30 días. Se puede modificar accediendo al fichero */etc/carmen/agents/config.properties* y modificando la siguiente información por el número de días deseado:

```
[di]
days=NUM_DIAS
```

5.10.3 ALMACENAMIENTO REMOTO

74. El servidor permite enviar los registros de alerta (y sólo esos) a un servicio remoto vía syslog o snmp.
75. La configuración de estos servicios ha de realizarse por un usuario configurador de la máquina (acceso root). Sin embargo, el envío mediante Syslog o SNMP se realiza en texto claro, por lo tanto, no se recomienda su uso.
76. Es por esto que, para el almacenamiento de logs, se recomienda salvar manualmente y de forma periódica los ficheros ubicados en */var/log* en una ubicación externa.

5.11 BACKUP

77. No existe un método de backup de la máquina. Si existen directorios de configuración (/etc) que se pueden salvar si el usuario lo requiere, pero no está integrado en el funcionamiento del *appliance*.
78. Se deberán salvar para poder recuperar el estado del *appliance* (que no el estado de los datos ingestados):

    /etc/carmen

    /usr/local/Carmen

    dump de base de datos */etc/nginx*

5.12 SERVICIOS DE SEGURIDAD

79. CARMEN es una herramienta de *Threat Hunting*, y no proporciona ningún servicio de seguridad más allá de notificar cuando cree encontrar un patrón de algún comportamiento potencialmente malicioso.
80. Desde la interfaz web, en *Configuración > Fuentes*, se pueden configurar los orígenes de datos de los que se nutre el producto. Permite activar y desactivar estos orígenes o modificarlos.

81. Las fuentes disponibles en el producto son: HTTP, DNS Pasivo, SMTP Pasivo, NetBios. Si se quiere cambiar la configuración de una fuente seguir los siguientes pasos:

    - Desde el menú principal, ir a *Configuración > Fuentes*.
    - Seleccionar la fuente deseada e ir a la pestaña *Configuración*.
    - Editar la información deseada y seleccionar *Guardar*.

6. FASE DE OPERACIÓN

82. Durante la fase de operación se pueden detectar y prevenir malfuncionamientos, para ello es recomendable revisar de forma periódica:

- Comprobaciones periódicas del hardware y software del producto para comprobar que no se han introducido elementos no autorizados.
- Pantalla de status que da información del estado de los discos, RAM, procesos y CPU.
- No hace falta mirar el estado de los parches de seguridad del sistema, pues en cada liberación de versión se hace una actualización de paquetería.
- Consultar a proveedor si existen versiones nuevas del producto.
- Revisar periódicamente los registros de auditoría.
- Realizar copias de seguridad de forma periódica.

7. CHECKLIST

ACCIONES	SÍ	NO	OBSERVACIONES
DESPLIEGUE E INSTALACIÓN			
Verificación de la entrega segura del producto	☐	☐	
Instalación en un entorno seguro	☐	☐	
CONFIGURACIÓN			
Creación de los usuarios y roles necesarios para la operación del producto	☐	☐	
Configuración de los parámetros de sesión	☐	☐	
Cierre delos puertos no utilizados	☐	☐	
Configuración de NTP	☐	☐	
Guardado de los logs en una ubicación externa	☐	☐	
Guardado de la copia de seguridad	☐	☐	

8. REFERENCIAS

83.

REF1 Guía de administrador del producto CARMEN_AGD_OPE_v7.2

REF2 CCN-STIC-807
https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/513-ccn-stic-807-criptologia-de-empleo-en-el-ens/file.html

9. ABREVIATURAS

CLI	*Command Line Interface*
CPD	Centro de Procesamiento de Datos
CPU	*Central Processing Unit*
DNS	*Domain Name System*
ENS	Esquema Nacional de Seguridad.
GUI	*Graphical User Interface*
HDD	*Hard Drive Disk*
RAM	*Random Access Memory*
RFID	*Radio Frequency Identification*
SO	Sistema Operativo

PUBLICACIONES DE DEFENSA

GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA
SUBDIRECCIÓN GENERAL DE PUBLICACIONES Y PATRIMONIO CULTURAL