

Guía de Seguridad de las TIC

CCN-STIC 1117

Procedimiento de Empleo Seguro

COSMIKAL ENDURANCE



Octubre 2025



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

cpage.mpr.gob.es

Edita:



Pº de la Castellana 109, 28046 Madrid
© Centro Criptológico Nacional, 2025
NIPO: 083-26-120-2



Fecha de Edición: Octubre de 2025

CCN
c=ES, l=MADRID, o=CCN,
ou=SELLO ELECTRONICO,
2.5.4.97=VATES-
S2800155J,
serialNumber=S2800155J
, cn=CCN
2026.05.05 09:40:03
+02'00'

LIMITACIÓN DE RESPONSABILIDAD

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

AVISO LEGAL

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

ÍNDICE

1 INTRODUCCIÓN	3
2 OBJETO Y ALCANCE	4
3 ORGANIZACIÓN DEL DOCUMENTO	5
4 FASE PREVIA A LA INSTALACIÓN	6
4.1 ENTREGA SEGURA DEL PRODUCTO	6
4.2 ENTORNO DE INSTALACIÓN SEGURO	6
4.3 REGISTRO Y LICENCIAS	6
4.4 CONSIDERACIONES PREVIAS	6
4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN	7
5 FASE DE INSTALACIÓN	8
6 FASE DE CONFIGURACIÓN	10
6.1 AUTENTICACIÓN	10
6.2 ADMINISTRACIÓN DEL PRODUCTO	10
6.2.1 ADMINISTRACIÓN LOCAL Y REMOTA	10
6.2.2 CONFIGURACIÓN DE ADMINISTRADORES	11
6.3 GESTIÓN DE CERTIFICADOS	11
6.4 SERVIDORES DE AUTENTICACIÓN	12
6.5 SINCRONIZACIÓN	12
6.6 ACTUALIZACIONES	12
6.7 ALTA DISPONIBILIDAD	13
6.8 AUDITORÍA	13
6.8.1 REGISTRO DE EVENTOS	13
6.8.2 ALMACENAMIENTO LOCAL	13
6.9 BACKUP	14
7 REFERENCIAS	15
8 ABREVIATURAS	16

1 INTRODUCCIÓN

1. El producto se trata de un gestor de acceso privilegiado (*Privileged Access Management, PAM*) diseñado para gestionar de forma segura accesos privilegiados a información crítica. Consiste en un escritorio remoto que permite a los usuarios acceder a recursos IT y OT de los que dispone la organización, siempre y cuando estos tengan permisos para ello.

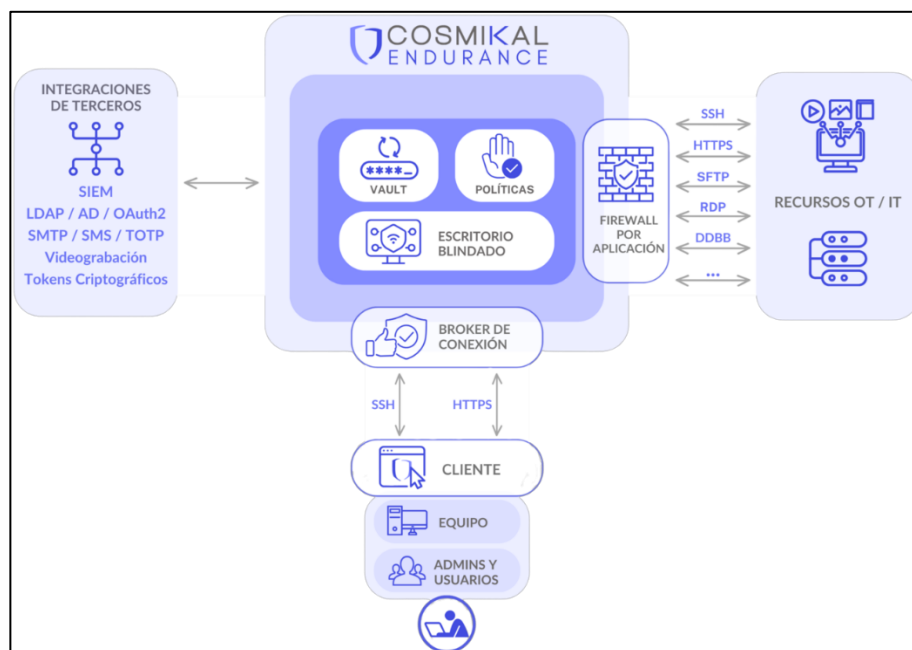


Figura 1. Arquitectura del producto.

2. El TOE se compone de varios componentes con distintas funcionalidades:
 - **Manager.** Es una aplicación interna que permite al administrador (*PAM admin*) gestionar usuarios, recursos IT y OT y credenciales. Este consta de una interfaz gráfica de usuario la cual solamente es accesible por el administrador una vez este haya accedido al ENDURANCE Desktop, y de un *backend* que se encarga de procesar las peticiones realizadas por la interfaz gráfica de usuario.
 - **Interfaz local.** Interfaz que permite al *PAM Admin* gestionar el producto de forma local.
 - **ENDURANCE Desktop.** Escritorio remoto el cual permite a los usuarios acceder a los recursos IT y OT de la organización, además permite al *PAM Admin* acceder al componente Manager.
 - **Vault.** Base de datos empleada para almacenar las credenciales de los usuarios para acceder a los activos de la organización.
 - **Servidor Syslog.** Servidor integrado de forma local que recolecta y almacena los registros de auditoría generados en el producto.
 - **Broker de conexión (HTTPS y SSH).** Interfaces remotas a través de las cuales el PAM admin y usuarios no administradores pueden acceder a ENDURANCE Desktop.
3. Con el fin de controlar los recursos a los que los usuarios pueden acceder, el producto implementa publicaciones, las cuales consisten en reglas o políticas que asocian usuarios a recursos IT y OT específicos, detallando el modo de acceso y las credenciales requeridas.

2 OBJETO Y ALCANCE

4. El objeto del presente documento es servir como guía para realizar una instalación, configuración y operación segura de Cosmikal Endurance v1.1.2.
5. Este producto ha sido cualificado e incluido en el Catálogo de Productos y Servicios STIC (CPSTIC) del Centro Criptológico Nacional para categoría ENS MEDIA en la familia “Gestión de acceso privilegiado (PAM)”. Se recomienda consultar la versión cualificada en cada momento.

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

6. Una vez se adquiere el producto, Cosmikal enviará un correo electrónico al cliente cuando se confirme la orden de compra.
7. En este correo electrónico se incluye la siguiente información:
 - Enlace al repositorio del fabricante donde se encuentra la imagen del producto para su descarga.
 - Usuario y contraseña para acceder al repositorio de descargas del fabricante.
 - Junto con la imagen del producto, se provee el hash SHA-256 de esta. El hash deberá ser comprobado manualmente una vez se descargue la imagen.

4.2 ENTORNO DE INSTALACIÓN SEGURO

8. Se deberán cumplir las medidas de seguridad físicas y lógicas de aplicación a los sistemas donde se desea desplegar la imagen.
9. Estas medidas de seguridad deberán garantizar que los sistemas donde se despliega el software se encuentren de forma protegida, permitiendo el acceso solamente a personal autorizado (considerando únicamente al administrador como confiable).

4.3 REGISTRO Y LICENCIAS

10. Durante la fase de instalación, tras el paso de solicitud de sobreescritura y previo a la opción de recuperación de datos existentes, aparecerá un código QR en la pantalla. Este código QR redirige al servicio de licenciamiento de Cosmikal.
11. En el servicio de licenciamiento aparecerá un código el cual tiene que ser introducido en el producto de forma correcta para poder continuar con la instalación. En caso de que el código sea erróneo, el producto notificará el error.
12. Este proceso de licenciamiento puede consultarse en la sección 3.1 del manual de instalación de Cosmikal Endurance [REF1].

4.4 CONSIDERACIONES PREVIAS

13. El producto se distribuye en formato IMG. Para llevar a cabo su instalación, es necesario de disponer de un hipervisor para poder alojar el producto y aplicar una conversión al formato soportado por el hipervisor usado.
14. Para asegurar un rendimiento óptimo del producto, el fabricante recomienda que la máquina en la que este se ejecute cumpla con las siguientes características mínimas:
 - **CPU:** 4 núcleos.
 - **Memoria:** 8 GB de RAM.
 - **Almacenamiento:** 64 GB de espacio en disco.
15. Estos requisitos pueden consultarse en la sección 2.2.2 del manual de instalación de Cosmikal Endurance [REF1].

4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN

16. Para el correcto funcionamiento del producto, este establece conexiones hacia internet de la siguiente forma:
 - **Servidor de actualizaciones.** Empleado para poder actualizar el producto, este realizará una conexión con el servidor de actualizaciones del fabricante.
 - **Repositorio de Ubuntu.** El producto se comunicará con los repositorios oficiales de Ubuntu para obtener una lista de los paquetes que tienen que ser actualizados.
 - **Entidades de Google.** Cuando se hace uso del navegador Google Chrome para conectarse a la interfaz de gestión del manager o a los activos de la organización mediante HTTPS, el producto establecerá comunicaciones con los siguientes *endpoints* de Google con el fin de transmitir estadísticas de telemetría:
 - clientservices.googleapis.com
 - accounts.google.com
 - update.googleapis.com
 - dl.google.com
 - safebrowsing.googleapis.com
 - www.googleapis.com
 - www.gstatic.com
 - edgedl.me.gvt1.com (HTTP)
 - chromewebstore.googleapis.com
 - clients2.google.com
 - clientservices.googleapis.com
 - Redirector.gvt1.com
 - safebrowsinghttpgateway.googleapis.com
 - r1---sn-h5qzen7d.gvt1.com
17. Por otra parte, dado que se puede acceder al ENDURANCE Desktop del producto mediante HTTPS o a través de SSH, será necesario disponer de alguna de las siguientes herramientas:
 - Cliente HTTPS, como puede serlo un navegador web (Microsoft Edge, Firefox, Google Chrome o Safari).
 - Cliente SSH mediante el cliente nativo de ThinLinc.
18. Para obtener más información acerca de ThinLinc, se deberá consultar la sección 3.1 del manual de administración de Cosmikal Endurance [REF2].
19. Para obtener más información acerca de cómo conectarse al producto usando un navegador, se deberá consultar la sección 3.2 del manual de administración de Cosmikal Endurance [REF2].

5 FASE DE INSTALACIÓN

20. El despliegue cualificado ha sido realizado en modo *standalone*, donde todos los componentes del producto se encuentran en la misma máquina. En caso de requerir de otro tipo de despliegue, se deberá contactar con el fabricante (Cosmikal).
21. El producto se puede instalar en una máquina física o en una máquina virtual.
22. En caso de usar una máquina virtual, será necesario disponer de un hipervisor para poder alojar el producto.
23. Una vez se disponga de una máquina física o de un hipervisor para alojar el producto, se seleccionará como medio de arranque del sistema o bien un dispositivo externo, en caso de máquina física, o bien la imagen en formato IMG en caso de máquina virtual.
24. Los pasos a seguir para completar la instalación son los siguientes:
 - a) Una vez arranque, aparecerá el logo de Cosmikal Endurance.
 - b) Seguidamente, se debe pulsar cualquier tecla para continuar con la instalación.
 - c) Aparecerán los posibles dispositivos donde instalar el producto, se seleccionará el deseado por el usuario (normalmente solo aparecerá uno).
 - d) El producto solicitará confirmación para llevar a cabo este proceso.
 - e) Una vez se acepta esta confirmación, aparecerá un código QR para activar la licencia. Para más información acerca del licenciamiento del producto, se deberá consultar la sección 4.3.
 - f) Cuando ya se encuentre el producto activado, se solicitará la confirmación para expandir el tamaño del disco o mantenerlo en 16 GB (por defecto). Se recomienda expandir para utilizar todo el tamaño del disco. Esta decisión no es reversible.
 - g) Una vez tomada la decisión, el producto mostrará una barra con el porcentaje de instalación.
 - h) Cuando finalice la instalación, se deberá pulsar cualquier tecla para finalizar el proceso de instalación.
 - i) El producto se reiniciará.
25. En el primer arranque de la máquina, se accederá a la configuración inicial, donde el producto solicitará el establecimiento para el primer usuario (*PAM Admin*):
 - a) Se deberá establecer la contraseña de este usuario. La contraseña debe tener una longitud mínima de 12 caracteres, y contar con, al menos, una letra minúscula, una letra mayúscula, un número y un carácter especial. En caso de que la contraseña introducida no cumpla con la política, el producto devolverá un error y se deberá de volver a incluir la contraseña.
 - b) Se deberá volver a introducir la contraseña para realizar una confirmación de que esta es correcta.
 - c) Tras esto, la máquina se reiniciará.
 - d) Tras el reinicio, el producto queda listo para su uso.

- e) Tras el reinicio, el producto queda listo para su configuración, permitiendo la conexión del usuario PAM Admin usando como credenciales el usuario “pam_admin” (sin comillas) y la contraseña establecida previamente.

6 FASE DE CONFIGURACIÓN

6.1 AUTENTICACIÓN

26. Para acceder al producto se puede utilizar el cliente SSH ThinLinc o un cliente HTTPS.
27. En caso de acceder al producto haciendo uso de un cliente SSH, el producto ofrecerá los siguientes mecanismos de autenticación:
 - Contraseña, siendo este el mecanismo cualificado y el que debe usarse.
 - Clave pública.
 - Tarjeta inteligente.
 - Ticket Kerberos.
28. En caso de acceder al producto haciendo uso de un cliente HTTPS, solamente se podrá acceder mediante usuario y contraseña.
29. Para más información acerca de la gestión de usuarios, se deberá consultar la sección 5.3.1 del manual de administración de Cosmikal Endurance [REF2].
30. Además, es posible configurar el producto para que este emplee un segundo factor de autenticación (2FA). Para más información acerca del segundo factor de autenticación, se deberá consultar la sección 4.0.5 del manual de instalación de Cosmikal Endurance [REF1].

6.2 ADMINISTRACIÓN DEL PRODUCTO

6.2.1 ADMINISTRACIÓN LOCAL Y REMOTA

31. El producto dispone de administración tanto local como remota.
32. Para acceder a la interfaz local de administración, se necesitará tener acceso a la máquina donde se encuentra instalado el producto. A la interfaz local solamente podrá acceder el usuario administrador (*PAM Admin*).
33. Para acceder al producto de forma remota, se podrá realizar a través de HTTPS haciendo uso de un cliente como un navegador web, y a través de SSH mediante un cliente SSH, tal como se define en 4.5.
34. A las interfaces remotas HTTPS y SSH podrán acceder tanto los usuarios no administradores como el usuario administrador (*PAM Admin*). Sin embargo, solo el PAM admin podrá acceder a la interfaz ofrecida por el Manager.
35. El producto, debido a su funcionalidad, es capaz de establecer conexiones con los recursos IT y OT mediante diversos protocolos. Se recomienda encarecidamente que solamente se empleen los protocolos HTTPS (sobre TLS v1.2 o TLS v1.3) y SSHv2 para establecer conexiones con los recursos de la organización.
36. En cuanto a estos protocolos, no es necesario realizar ninguna configuración dado que estos implementan algoritmos categorizados como recomendados por la guía CCN-STIC-807 [REF4].
37. Para obtener más información acerca de los protocolos que soporta el producto, se deberá consultar la sección 5.4 del manual de administración de Cosmikal Endurance [REF2].
38. En cuanto a los activos IT y OT de la organización, se recomienda usar protocolos de comunicación y algoritmos criptográficos aprobados por la guía CCN-STIC-807 [REF4].

6.2.2 CONFIGURACIÓN DE ADMINISTRADORES

39. El producto define un usuario de administración, conocido como *PAM Admin*. Este usuario es el encargado de realizar todas las funciones de administración del producto.
40. A la hora de crear usuarios, el administrador *PAM Admin* tendrá que establecer un periodo de inactividad. Para ello, en el proceso de creación de un usuario, se deberá acceder a la ruta *Inicio/Configuración/Sesiones* (o *Home/Settings/Sessions*) en la interfaz gráfica de usuario del Manager, seleccionar la opción de *close* e indicar 10 minutos en la casilla de *Inactivity period*.
41. A la hora de crear credenciales asociadas a activos IT y OT, se deberá establecer el parámetro *Modo de acceso* (o *Access mode*) a *Fijo* (o *Fixed*) en los campos *Dominio*, *Usuario* y *Autenticación* (o *Domain*, *User* y *Authentication*). De este modo, la configuración permitirá un proceso de autenticación transparente a los usuarios que desean acceder a los recursos IT y OT.
42. Además, el producto por defecto no establece un periodo de validez de las credenciales asociadas a los activos IT y OT. Para ello, será necesario establecer un periodo de validez, el cual solamente podrá ser configurado para credenciales creadas con el modo *Fijo* (o *Fixed*). La configuración se debe realizar durante el proceso de creación de credenciales, seleccionando el periodo deseado en el desplegable *Días de expiración* (o *expiry time*). Esta configuración hará que las contraseñas de los activos de IT y OT introducidas tengan un periodo de caducidad y dejen de ser válidas después de este periodo.
43. El producto incorpora un mecanismo para establecer una conexión SSH con el fabricante, de modo que el equipo de soporte fabricante pueda acceder al producto para llevar a cabo tareas de mantenimiento o de solución de errores. Por defecto, esta funcionalidad se encuentra deshabilitada (y no debe habilitarse salvo causa de fuerza mayor).
44. Para habilitar esta funcionalidad será necesario contactar previamente con el fabricante a través de cualquiera de sus canales oficiales para poder llevar a cabo el mantenimiento necesario. Luego de contactar con el fabricante, se habilitará esta funcionalidad con el usuario *PAM Admin*, accediendo a la ruta *Inicio/Configuración/Soporte* (o *Home/Settings/Support*) y habilitando la opción *Habilitar acceso del equipo de soporte* (o *Enable access for support team*).
45. Internamente, cuando el *PAM Admin* habilita esta opción, se activa el usuario de soporte y se establece una conexión SSH a los servidores del fabricante.
46. Cuando se deshabilita esta funcionalidad, se cierra la conexión establecida y se desactiva el usuario de soporte.
47. Para obtener más información acerca del usuario administrador y de las funciones que este puede llevar a cabo, se deberá consultar el manual de administración de Cosmikal Endurance [REF2].

6.3 GESTIÓN DE CERTIFICADOS

48. El producto permite la configuración del certificado digital usado por el producto para autenticarse ante los usuarios que acceden por HTTPS. Para realizar esta configuración se deben seguir los siguientes pasos:

- a) En primer lugar, será necesario generar un certificado usando RSA con una longitud de clave igual o superior a 3072 bits.
 - b) Una vez se disponga del certificado, se deberá crear en el dispositivo del cliente una carpeta llamada **endurance** y ubicar en ella el certificado completo con el nombre **endurance.crt** y la clave asociada **endurance.key**.
 - c) Usando el cliente SSH mencionado en la sección 4.5, se deberá acceder al producto con la carpeta **endurance** compartida en modo lectura.
 - d) Se deberá acceder a la herramienta de gestión de certificados y pulsar el botón de **Update certificates**. Tras esto, el certificado se habrá actualizado correctamente y será el presentado por el producto a los clientes en las conexiones HTTPS.
49. Para obtener más información acerca de cómo actualizar los certificados, se deberá consultar la sección 4.1.2 del manual de administración de Cosmikal Endurance [REF2].

6.4 SERVIDORES DE AUTENTICACIÓN

50. Aunque el producto ofrezca autenticación local y esta sea la que debe usarse, el producto es compatible con servidores externos de autenticación LDAP.
51. Para obtener más información acerca de cómo integrar un servidor de autenticación LDAP, se deberá consultar la sección 5.7.5 del manual de administración de Cosmikal Endurance [REF2].

6.5 SINCRONIZACIÓN

52. El producto es compatible con servidores NTP para configurar la fecha y hora del sistema. La configuración de la fecha y hora solo puede ser llevada a cabo por el *PAM Admin*. La configuración se realizará de la siguiente manera:
- a) Hacer click al icono en la barra de tareas de la interfaz gráfica del manager que permite acceder a la configuración de fecha y hora.
 - b) Una vez accedida a dicha configuración, se deberá seleccionar la opción *Manual*. Esta opción sincroniza la fecha y hora del producto con la fecha y hora del sistema operativo.
53. Para obtener más información acerca de servidores NTP, deberá consultarse la sección 4.1.3 del manual de administración de Cosmikal Endurance [REF2].

6.6 ACTUALIZACIONES

54. Las actualizaciones del producto se encuentran en un repositorio del fabricante, accesible a través de internet.
- a) En la ruta *Inicio/Configuración/Actualizaciones* (o *Home/Settings/Updates*) se encuentra un botón mediante el cual se puede consultar si existen actualizaciones disponibles.
 - b) En caso de que haya una actualización disponible, aparecerá una pantalla donde se preguntará si se desea actualizar el producto.
 - c) En caso afirmativo, el producto descargará la actualización.

- d) Una vez descargada la actualización, se mostrará de nuevo una pantalla para confirmar si se desea instalar la actualización.
 - e) En caso afirmativo, el producto se reiniciará, aplicándose la actualización.
55. Para obtener más información acerca del proceso de actualización del producto, se deberá consultar la sección 5.7.2 el manual de administración de Cosmikal Endurance [REF2].

6.7 ALTA DISPONIBILIDAD

56. A pesar de que el producto se ha cualificado en formato *standalone*, este ofrece la posibilidad de separar sus componentes e instalarlos en varias máquinas o instalarlo en múltiples máquinas con alta disponibilidad y balanceo de carga.
57. Para obtener más información acerca de cómo desplegar el producto de forma que se obtenga alta disponibilidad, se deberá consultar la sección 2.2.3 del manual de instalación de Cosmikal Endurance [REF1], además de contactar con el fabricante.

6.8 AUDITORÍA

6.8.1 REGISTRO DE EVENTOS

58. El producto registra los siguientes eventos:
- Inicio de sesión.
 - Cierre de sesión.
 - Cambios en credenciales de usuarios.
 - Cambios en la configuración de terminación de sesión cuando se detecta inactividad.
 - Creación y borrado de usuarios.
 - Creación de activos nuevos.
 - Asignación de acceso a recursos a través de publicaciones.
 - Creación, modificación o borrado de credenciales en el Vault.
59. Los eventos registrados contienen la siguiente información:
- Fecha y hora del evento.
 - Tipo de evento identificado.
 - Resultado del evento.
 - Usuario que produce el evento (si aplica).

Para obtener más información acerca de los registros de auditoría del producto, deberá consultarse el manual de Auditoría de Cosmikal Endurance [REF3].

6.8.2 ALMACENAMIENTO LOCAL

60. El producto almacena todos los registros de auditoría generados de forma local.
61. Además, permite configurar un periodo de retención mediante el cual se mantienen los registros de auditoría generados durante el tiempo establecido, por ejemplo, durante 180 días.
62. Para obtener más información acerca del periodo de retención de los registros de auditoría, se deberá consultar la sección 5.7.6 del manual de administración de Cosmikal Endurance [REF2].

6.9 BACKUP

63. El producto permite la generación de copias de seguridad de los datos del sistema. Por defecto, esta funcionalidad se encuentra deshabilitada.
64. Para habilitar la realización de copias de seguridad, es necesario disponer de un servidor SFTP externo.
65. Una vez se disponga de un servidor SFTP externo, en la ruta *Inicio/Configuración/Backup* (o *Home/Settings/Backup*) deberán configurarse los parámetros SFTP:
 - Servidor.
 - Usuario.
 - Contraseña.
 - Ruta.
66. Además, deberá configurarse cada cuanto tiempo se realizan las copias de seguridad y cuanto tiempo permanecen en el servidor. Se recomienda encarecidamente que se realicen copias de seguridad de forma periódica.
67. Para obtener más información acerca de la realización de copias de seguridad, deberá consultarse la sección 5.7.7 del manual de administración de Cosmikal Endurance [REF2].

7 REFERENCIAS

- [REF1] Installation Manual, Endurance, 1.1.2, COSMIKAL, 02/12/2024
- [REF2] Administration Manual, Endurance, 1.1.2, COSMIKAL, 02/12/2024
- [REF3] Audit, Endurance, 1.1.2, Cosmikal, 02/12/2024
- [REF4] Guía de Seguridad de las TIC CCN-STIC 807, Criptología de empleo en el Esquema Nacional de Seguridad

8 ABREVIATURAS

2FA	Two-Factor Authentication
CCN	Centro Criptológico Nacional
CPSTIC	Catálogo de Productos y Servicios STIC
CPU	Central Processing Unit
ENS	Esquema Nacional de Seguridad
GB	Gigabyte
HTTPS	HyperText Transfer Protocol Secure
IMG	Image
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
NTP	Network Time Protocol
OT	Operational Technology
PAM	Privileged Access Management
QR	Quick Response
RAM	Random Access Memory
RSA	Rivest-Shamir-Adleman (algoritmo de cifrado)
SFTP	Secure File Transfer Protocol
SHA	Secure Hash Algorithm
SHA-256	Secure Hash Algorithm 256-bit
SSH	Secure Shell
SSL	Secure Sockets Layer
STIC	Seguridad de las Tecnologías de la Información
TLS	Transport Layer Security
TOE	Target of Evaluation

