

MINISTERIO DE DEFENSA



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: 083-26-135-1



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 13:07:31 +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 CONSIDERACIONES PREVIAS.....	6
5 INSTALACIÓN.....	7
6 FASE DE CONFIGURACIÓN	8
6.1 AUTENTICACIÓN	8
6.2 ADMINISTRACIÓN DEL PRODUCTO.....	8
6.2.1 ADMINISTRACIÓN LOCAL Y REMOTA	8
6.2.2 CONFIGURACIÓN DE ADMINISTRADORES	8
6.3 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS	9
6.4 CONFIGURACIÓN DE PROTOCOLOS SEGUROS	10
6.5 GESTIÓN DE CERTIFICADOS	11
6.6 ACTUALIZACIONES	11
6.7 AUTO-CHEQUEOS.....	11
6.8 AUDITORÍA	11
6.8.1 REGISTRO DE EVENTOS.....	11
6.8.2 ALMACENAMIENTO LOCAL.....	12
6.9 BACKUP	12
6.10 SERVICIOS DE SEGURIDAD	13
7 FASE DE OPERACIÓN	14
8 CHECKLIST	15
9 REFERENCIAS	16
10 ABREVIATURAS.....	17

1 INTRODUCCIÓN

1. *Katua SDI Platform* es la solución hiperconvergente de KRC ESPAÑOLA que ofrece múltiples capacidades en una plataforma unificada:
 - Despliegues de CPD virtuales.
 - Despliegue de servicios *cloud*.
 - Almacenamiento unificado.
 - Escalabilidad.
 - SDN.
 - Capacidad *multi-tenant* en contextos de seguridad diferenciados.
2. La solución se entrega en formato *appliance*, instalada en un *hardware* especialmente optimizado para este propósito.
3. Los requisitos mínimos del hardware son:
 - Procesador Intel Xeon
 - Memoria RAM 32GB RAM
 - Almacenamiento de base 750GB
 - Dos interfaces de red.
4. Al estar diseñada siguiendo el principio de “**Security by Design**”, la solución está securizada desde fábrica por lo que las actuaciones para una puesta en marcha segura son mínimas.

2 OBJETO Y ALCANCE

5. La presente guía recoge el procedimiento de puesta en marcha inicial del producto, primeros pasos, así como recomendaciones generales de configuración para garantizar el uso seguro del mismo.
6. Los procedimientos indicados en este documento se circunscriben a la **versión 2.0** del producto.
7. Determinadas operaciones por su complejidad y longitud sólo se referencian, remitiendo a los siguientes documentos para ver con detalle la operación:
 - Manual del usuario del dashboard [REF1].
 - Manual del usuario CLI [REF2].
8. Esta solución ha sido cualificada e incluida en el Catálogo de Productos y Servicios de Seguridad TIC (CPSTIC) en la familia de *“Herramientas de hiperconvergencia”* para categoría ENS Alta.

3 ORGANIZACIÓN DEL DOCUMENTO

- a) Apartado c). En este apartado se recogen aspectos y recomendaciones a considerar, antes de proceder a la instalación del producto.
- b) Apartado **¡Error! No se encuentra el origen de la referencia..** En este apartado se recogen recomendaciones a tener en cuenta durante la fase de instalación del producto.
- c) Apartado 7. En este apartado se recogen las recomendaciones a tener en cuenta durante la fase de configuración del producto, para lograr una configuración segura.
- d) Apartado 7. En este apartado se recogen las recomendaciones a tener en cuenta durante la fase de operación del producto.

4 FASE PREVIA A LA INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

9. *KATUA SDI Platform* se entrega en formato *appliance*, por lo que en el momento de recibir el producto se deberá verificar que:
 - El embalaje está perfectamente cerrado, sin roturas en las cintas de precinto marcadas con el anagrama de KRC Española.
 - El producto no presenta signos de manipulación o deterioro de algún tipo.
 - El etiquetado no ha sido manipulado ni presenta roturas, especialmente el sello de garantía identificado como tal en el equipo.
 - El número de serie del producto a través del código de barras o QR de la misma.
 - Los discos que conforman la solución están bloqueados y no se pueden extraer.

4.2 ENTORNO DE INSTALACIÓN SEGURO

10. La plataforma está diseñada para ser instalada en un Centro de Proceso de Datos (CPD), con acceso restringido y controlado. Es responsabilidad del cliente final garantizar esta seguridad física.

4.3 CONSIDERACIONES PREVIAS

11. La plataforma se ha diseñado para permitir su puesta en marcha de dos (2) formas diferentes:
 - Sin conexión de red, para lo que será necesario conectar un monitor y teclado a la plataforma. En este modo la configuración inicial se puede llevar a cabo a través de la interfaz CLI disponible (ver Manual de Usuario CLI [REF2]).
 - Con conexión de red, modo *headless*, para lo que será necesario conectar la plataforma a una infraestructura de red existente y acceder a través de un equipo con navegador web compatible HTML5. Para garantizar la máxima seguridad en la puesta en marcha, tanto la red existente como el equipo utilizado deberían estar convenientemente bastionados.

5 INSTALACIÓN

12. El producto viene preinstalado de fábrica, por lo que no se requieren actuaciones especiales para su instalación inicial. En el primer arranque, se debe cambiar la password de root y del usuario krcadmin:

```
#passwd krcadmin
```

```
#passwd root
```

6 FASE DE CONFIGURACIÓN

6.1 AUTENTICACIÓN

13. En lo concerniente a la autenticación de los usuarios, la plataforma implementa su propio modelo de autenticación basado en credenciales locales.
14. Todos los componentes internos se comunican haciendo uso de certificados. La plataforma implementa su propia PKI para la generación y gestión de certificados de los diferentes componentes. Para más información, consultar 6.5 GESTIÓN DE CERTIFICADOS.
15. La conexión de usuarios a través de CLI requiere autenticación en dos pasos: acceso local al sistema operativo (por consola o *ssh*), y autenticación adicional para el acceso a la gestión de la plataforma. Esto permite distinguir el usuario administrador de la plataforma, del usuario con acceso *root* del sistema operativo.
16. El proceso de conexión y autenticación está descrito en el Manual de Usuario del Dashboard [REF1], apartado 3.

6.2 ADMINISTRACIÓN DEL PRODUCTO

6.2.1 ADMINISTRACIÓN LOCAL Y REMOTA

17. La plataforma admite la administración de forma local, a través del uso de la consola, o de forma remota a través de conexión *ssh* o *https*.
18. Para realizar la **administración local** es necesario una autenticación en dos (2) fases:
 - Identificación del usuario del sistema operativo (cuenta local)
 - Identificación ante la plataforma que ofrece su propia línea de comandos (ver Manual de Usuario CLI)
19. La **administración remota** se puede realizar de dos (2) formas, utilizando siempre y de forma obligatoria canales seguros. Sólo se admite el uso de *SSH* y *HTTPS*.
 - CLI: Conexión vía *SSH* y autenticación del usuario del sistema operativo (cuenta local), y posteriormente autenticación ante la plataforma.
 - DASHBOARD: Conexión vía *HTTPS* y autenticación ante la plataforma.
20. El sistema NO permite el uso de canales o servicios no seguros, como telnet.
21. La plataforma no permite la transferencia de archivos a/desde la misma utilizando el servicio *FTP*. Sólo es posible realizar transferencia mediante el uso de *SCP*. El proceso de transferencia mediante scp está descrito en el Manual de Usuario del Dashboard [REF1], apartado 2.6

6.2.2 CONFIGURACIÓN DE ADMINISTRADORES

22. Los usuarios administradores pueden crear y asociar permisos a usuarios definiendo los privilegios de actuación sobre los diferentes aspectos de la plataforma. Los tipos de permisos son agrupados en los siguientes bloques:
 - Permisos globales de la plataforma.

- Permisos sobre *tenants*.
 - Permisos delegados de administración sobre el *tenant*.
 - Permisos “*readonly*” para monitorización.
 - Permisos sobre APIs.
23. Dichos permisos quedan descritos en el Apartado 3 del Manual de Usuario Katua SDI Platform [REF1].
 24. Los usuarios y roles existentes, así como su asociación se puede consultar a través del *dashboard*, en la opción *Identity*.
 25. La plataforma controla la política de contraseñas, así como los parámetros de *timeout* y sesiones. Los valores de estos parámetros están establecidos desde fábrica por defecto. El usuario *root* tiene la capacidad de cambiar los mismos mediante la edición de los ficheros de configuración correspondientes.
 26. Los ajustes en relación con la política segura de contraseñas se pueden efectuar modificando los ficheros */etc/login.defs* y */etc/security/pwquality.conf* para la configuración de acceso vía *ssh/console* y el fichero */etc/keystone/keystone.conf* para la configuración de acceso vía *dashboard*.
 27. Los ajustes en relación con la configuración de *timeouts* y bloqueos se pueden efectuar modificando los ficheros */etc/ssh/sshd_config* y */etc/pam.d/password-auth* para accesos vía *ssh/console* y el fichero */etc/keystone/keystone.conf* para accesos vía *dashboard*.
 28. Los valores por defecto para la política segura de contraseñas y sesiones se han establecido de la siguiente forma:
 - Configuración de la política segura de contraseñas:
 - Longitud mínima de 11 caracteres para el servicio *SSH* y 12 para el *dashboard*.
 - Se debe incluir al menos una letra minúscula
 - Se debe incluir al menos una letra mayúscula
 - Se debe incluir al menos un número
 - Se debe incluir al menos un carácter especial
 - Configuración de parámetros de sesión:
 - *Timeout* de sesión para la CLI de 300 segundos y para el *dashboard* 1800.
 - El sistema bloquea la interfaz web durante 1800 segundos tras 6 intentos fallidos.
 - Los usuarios del sistema operativo se bloquean indefinidamente tras 8 intentos (no *root*).
 - El usuario *root* será el encargado de realizar el desbloqueo de las cuentas de forma manual.
 - Los accesos por *SSH* bloquean la IP de los clientes que realicen 6 intentos en un corto periodo de tiempo durante 1 hora.

6.3 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

29. La plataforma se entrega con una de las interfaces configurada para la administración y gestión de la plataforma a través de *CLI* o *dashboard*.
30. El *appliance* dispone de una interfaz de red *IPMI 2* para la conexión remota a la consola. Por seguridad, desde fábrica se entrega desactivada, siendo responsabilidad del cliente su activación posterior. Para habilitar la funcionalidad *IPMI*, se recomienda seguir las instrucciones específicas proporcionadas en el manual de la placa base del fabricante.

31. Generalmente, el procedimiento consiste en acceder a la configuración del sistema (BIOS/UEFI), localizar la sección correspondiente al BMC o IPMI, y habilitar la interfaz. A continuación, se debe configurar la red del controlador de gestión, ya sea mediante DHCP o mediante una dirección IP estática, asegurándose de que la interfaz esté operativa y accesible desde la red de administración. Es importante verificar que los parámetros de red se hayan aplicado correctamente, así como cambiar las credenciales por defecto para garantizar la seguridad del acceso remoto. Todos estos pasos pueden variar en función del modelo de placa base, por lo que es imprescindible consultar el manual técnico correspondiente para una correcta implementación.
32. En la ilustración 1 se identifican las diferentes interfaces de red en la configuración *hardware* predeterminada:

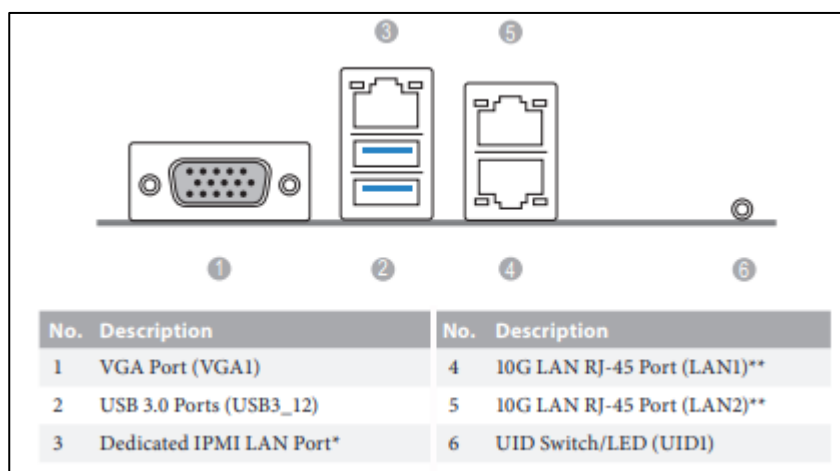


Ilustración 1. Interfaces de red del producto

6.4 CONFIGURACIÓN DE PROTOCOLOS SEGUROS

33. Todos los protocolos de red en la plataforma se entregan preconfigurados para garantizar la seguridad desde el primer instante.
34. Por motivos de seguridad y conforme a las recomendaciones de los organismos oficiales, no se debe habilitar ninguna versión de SSL ni versiones de TLS distintas de TLSv1.2. **Esta versión está configurada por defecto y proporciona un nivel de cifrado suficientemente robusto y compatible con los estándares actuales.** La activación de versiones anteriores (como SSLv2, SSLv3, TLSv1.0 o TLSv1.1) representa un riesgo de seguridad conocido y puede exponer el sistema a vulnerabilidades críticas.
35. El servicio *HTTP* está deshabilitado en el portal de administración y así debe permanecer, debiendo hacer uso de *HTTPS*. El navegador debe soportar el uso de *TLSv1.2* o superior. En caso contrario se rechazará la conexión.
36. Las conexiones a través de *SSH* se realizan utilizando el protocolo *SSHv2*.
37. La plataforma se entrega configurada para hacer uso exclusivamente de *Ciphers* admitidos en la guía CCN-STIC-807 [REF4]. **No se recomienda alterar esta configuración**, pero en caso necesario, se puede realizar editando los ficheros */etc/ssh/sshd_config* para las conexiones *SSH* y */etc/httpd/conf.d/ssl.conf* para las conexiones *HTTPS*.

6.5 GESTIÓN DE CERTIFICADOS

38. La plataforma implementa su propia infraestructura PKI para la generación de certificados digitales de uso interno. En el Manual de Usuario del dashboard [REF1], apartado 2.4 se describe el procedimiento para regenerar todos los certificados.
39. Recomendamos la generación de certificados usando longitudes de bits lo más amplias posibles con una duración en general no superior a 4 años.

6.6 ACTUALIZACIONES

40. La plataforma hace uso del sistema de gestión de paquetes *deb* del sistema operativo para las actualizaciones.
41. Los paquetes se deberán descargar desde la web de soporte de KRC Española para el producto.
42. Se recomienda el uso de un equipo seguro tipo aduana para la descarga de los paquetes, evitando la conexión directa de la plataforma a Internet.
43. Los paquetes descargados en el equipo seguro se podrán subir a la plataforma haciendo uso de *scp*.
44. Los paquetes de actualización se entregan firmados digitalmente y el usuario deberá verificar si la firma es correcta. Esta verificación se puede realizar desde la consola CLI ejecutar el comando *sha256sum <NombrePaquete>*.
45. Una vez verificada la firma, se podrá realizar la instalación de los paquetes con Nombre Paquete *dpkg -i <NombrePaquete>*.
46. Esta operación sólo está disponible para el usuario *root* del sistema.

6.7 AUTO-CHEQUEOS

47. La plataforma no realiza auto chequeos programados. Al reiniciar, se realiza un *check* de integridad de almacenamiento, memoria, CPU, como parte del *POST* del equipo y del sistema operativo.
48. Todos los paquetes están firmados, tanto los correspondientes al sistema operativo de base, como los propios de la plataforma. Se puede verificar la integridad de los paquetes utilizando “*debsums -s*”, una vez identificado como *root* en el sistema operativo.

6.8 AUDITORÍA

6.8.1 REGISTRO DE EVENTOS

49. La plataforma define dos (2) niveles de log:
 - Nivel de sistema operativo: Registra información del sistema operativo, tales como inicios/cierres de sesión, servicios propios necesarios para el funcionamiento de la plataforma, mensajes de componentes del sistema, etc.
 - Nivel de componentes HCI: Registra los logs de los diferentes componentes de la plataforma HCI: mensajes de la capa de computación, *storage*, *images*, etc.
50. De forma general, se auditan eventos de:

- Conexión/Desconexión.
 - Cambios de contraseñas y permisos de usuarios.
 - Cambios en la configuración del sistema.
 - Eventos que afecten a la funcionalidad del sistema, como son creación de volúmenes, conexión/desconexión de interfaces de red, eventos de *kernel* y escalado de privilegios.
51. El formato de los logs y eventos se almacenan en texto, dentro de la carpeta del sistema operativo */var/log*.
52. Es posible modificar los eventos objeto de auditoría, así como las políticas de retención de los ficheros de log generados. Para efectuar estos cambios es necesario editar el fichero */etc/audit/rules.d/audit.rules*.
53. Los registros de auditoría se protegen mediante mecanismos técnicos que impiden su modificación o eliminación, incluso por usuarios privilegiados. Los ficheros activos están marcados como solo-apéndice (+a) para permitir escritura segura y los archivos rotados se marcan como inmutables (+i). Se recomienda que los usuarios privilegiados nunca alteren estos atributos. Únicamente *audit.log* no dispone de este atributo +a ya que su rotado lo realiza el propio servicio *auditd* y su control y acceso es exclusivo del usuario privilegiado. Se recomienda igualmente que el usuario privilegiado no altere dicho log. La verificación de integridad está reforzada mediante *AIDE* y *auditd*, permitiendo trazabilidad y detección de accesos no autorizados.

6.8.2 ALMACENAMIENTO LOCAL

54. Todo el almacenamiento de los logs se realiza de forma local.
55. Las políticas definidas de contención de los logs son las siguientes:
- Sistema *Audit* del sistema operativo:
 - Máximo 12 archivos de logs.
 - Tamaño del log generado: 12MB.
 - Rotación automática al alcanzar estos límites.
 - Resto de componentes:
 - Rotación semanal.
 - Mantiene 4 (14 en el caso de algunos componentes de la capa hiperconvergente) archivos de log.
 - Los archivos de log se sobrescriben para evitar el llenado del espacio de almacenamiento.
56. Las políticas se pueden modificar editando, una vez autenticado en el sistema como *root* mediante la edición de los ficheros */etc/audit/auditd.conf* y */etc/logrotate.conf*

6.9 BACKUP

57. El sistema permite la generación de *snapshots* que pueden ser exportados para su extracción a través de canal seguro vía *scp*. En el Manual de Usuario del dashboard [REF1], apartado 9, se describe el procedimiento para la generación de instantáneas.
58. Se recomienda el uso de *scp* para la extracción como método óptimo, dado el tamaño que pueden ocupar los *snapshots* de las instancias.

59. Para realizar un *backup* de la configuración existente, basta con realizar una copia del directorio */etc* del sistema, donde se almacena la configuración para su posterior restauración en otro *appliance*.
60. La periodicidad de la realización de *snapshots* y *backups* dependerá en gran medida de la volatilidad de la información almacenada y de los cambios en la configuración de la plataforma.
61. De forma general se recomienda realizar un *snapshot* previo a cambios en la configuración de las instancias y posteriormente, una vez verificada su funcionalidad.
62. Para el *backup* de la configuración existente, dado que no es una operación habitual realizar cambios a este nivel, se recomienda realizar un *backup* previo a cualquier cambio en los ficheros de configuración, y una vez verificado el funcionamiento correcto realizar un nuevo *backup*.

6.10 SERVICIOS DE SEGURIDAD

63. El sistema implementa herramientas para prevenir posibles ataques. Los servicios asociados a las herramientas de prevención se entregan habilitados y configurados por lo que no es necesaria ninguna actuación sobre los mismos.
64. Los servicios implementados son:
 - Implementación de *firewall* de sistema operativo.
 - Implementación de políticas de contraseña fuerte con detección de ataques de fuerza bruta.
 - Implementación de políticas contra ataques *DoS* o *DDoS*.
 - Implementación de contextos de seguridad SELinux por cada instancia.

7 FASE DE OPERACIÓN

65. Se recomienda realizar mensualmente una revisión de la plataforma para verificar el correcto funcionamiento y el nivel de vulnerabilidad siguiendo esta guía:
66. Con un usuario identificado a nivel de sistema operativo como *root* comprobar:
 - Ficheros de log de la auditoría con el objetivo de localizar cambios en ficheros del sistema o en los servicios activos. Los ficheros de auditoría están ubicados en */var/log/audit*.
 - Fichero de registro de mensajes del sistema. Localizar posibles errores con *cat /var/log/messages | grep -i error*.
 - Ficheros log de la plataforma. Verificar los diferentes ficheros de log en busca de posibles errores de la plataforma HCI. Dentro del directorio */var/log* se encuentran las carpetas correspondientes a cada uno de los componentes del sistema (*nova*, *cinder*, etc.).
 - Comprobar la integridad de ficheros revisando el log: */var/log/aide/aide-check.log*
 - Comprobar la integridad de los paquetes instalados con *rpm -qaV*.
 - Comprobar la versión y *hash* de la instalación desde el *dashboard* accediendo a la opción *KatuaSDI->About*.
 - Actualizar la BIOS del sistema a la última versión disponible en la web de soporte del producto.
<https://www.asrockrack.com/general/productdetail.asp?Model=D2163D4I2-2T#Download>
Si el producto se ha entregado instalado en un servidor con otro hardware compatible, se proporcionará información del fabricante relativo a la actualización de la BIOS.
 - Actualizar los paquetes del sistema a la última versión disponible en la web de soporte del producto. Las actualizaciones del producto podrán ser entregadas a través de un link de empresa, que estará comprimido y con contraseña.
 - Revisar la caducidad de certificados de la PKI integrada. En caso necesario, regenerar e instalar los certificados.
67. En la sección 2 del Manual de Usuario del dashboard [REF1] se describen los procedimientos de actualización y regeneración de certificados.

8 CHECKLIST

ACCIONES	SÍ	NO	OBSERVACIONES
DESPLIEGUE E INSTALACIÓN			
Verificación de la entrega segura del producto	☐	☐	
Instalación en un entorno seguro	☐	☐	
CONFIGURACIÓN			
MODO DE OPERACIÓN SEGURO			
Autenticación	☐	☐	
Configuración de administradores	☐	☐	
Configuración de interfaces de red	☐	☐	
CONFIGURACIÓN DE PROTOCOLOS SEGUROS			
Gestión de certificados	☐	☐	
OPERACIÓN			
AUDITORIA			
Activación auditoría	☐	☐	
Registro de mensajes del sistema	☐	☐	
Logs de componentes de la plataforma HCI	☐	☐	
Verificación de paquetes	☐	☐	
Comprobación de versión y hash de producto	☐	☐	

9 REFERENCIAS

- [REF1] «Manual de usuario del dashboard de Katua SDI Platform,» [Se entrega junto con el producto].
- [REF2] «Manual de usuario de línea de comando de Katua SDI Platform,» [Se entrega junto con el producto].
- [REF3] CCN-STIC-104 Catálogo de productos con clasificación ZONING.
- [REF4] Guía CCN-STIC-807 - Criptografía de empleo en el Esquema Nacional de Seguridad.

10 ABREVIATURAS

CCN	Centro Criptológico Nacional
CLI	Command Line Interface
CPD	Centro de Procesamiento de Datos
CPSTIC	Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y la Comunicación
DDoS	Distributed Denial of Service
DoS	Denial of Service
ENS	Esquema Nacional de Seguridad.
FTP	File Transfer Protocol
HCI	Hyper-Converged Infrastructure
HTML	HyperText Markup Language
HTTPS	Hypertext Transfer Protocol Secure
IPMI	Intelligent Platform Management Interface
PKI	Public Key Infrastructure
POST	Power-on Self-Test
SCP	Secure Copy Protocol
SDI	Software Defined Infrastructure
SDN	Software Defined Networking
SELinux	Security-Enhanced Linux
SSH	Secure Shell
SSL	Secure Sockets Layer
STIC	Seguridad de las Tecnologías de la Información y Comunicación
TLS	Transport Layer Security

