

Guía de Seguridad de las TIC

CCN-STIC 1656

Procedimiento de Empleo Seguro

UDS Enterprise



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: 083-26-138-8



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 13:16:35 +02'00'

LIMITACIÓN DE RESPONSABILIDAD

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

AVISO LEGAL

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	8
5 FASE DE INSTALACIÓN	11
6 FASE DE CONFIGURACIÓN	12
6.1 MODO DE OPERACIÓN SEGURO	12
6.2 AUTENTICACIÓN	12
6.3 ADMINISTRACIÓN DEL PRODUCTO	13
6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA	13
6.3.2 CONFIGURACIÓN DE ADMINISTRADORES	13
6.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS	14
6.5 GESTIÓN DE CERTIFICADOS	14
6.6 SERVIDORES DE AUTENTICACIÓN	14
6.7 SINCRONIZACIÓN	15
6.8 ACTUALIZACIONES	15
6.9 AUTO-CHEQUEOS	15
6.10 ALTA DISPONIBILIDAD	16
6.11 AUDITORÍA	16
6.11.1 REGISTRO DE EVENTOS	16
6.11.2 ALMACENAMIENTO LOCAL	17
6.11.3 ALMACENAMIENTO REMOTO	17
6.12 BACKUP	17
7 REFERENCIAS	18
8 ABREVIATURAS	19

1 INTRODUCCIÓN

1. UDS Enterprise es una plataforma diseñada para gestionar el acceso y la administración centralizada de recursos informáticos en entornos de Data Center. Funciona como un bróker de conexiones multiplataforma, permitiendo a los usuarios acceder de forma segura y sencilla a escritorios virtuales, aplicaciones virtualizadas y equipos físicos desde cualquier dispositivo y ubicación.
2. La solución destaca por su flexibilidad y escalabilidad, ya que puede integrarse con múltiples hipervisores y sistemas de virtualización.
3. UDS Enterprise facilita la creación de entornos de “digital workplace” personalizados, permitiendo a los administradores TI gestionar toda la infraestructura desde una única consola, una de sus principales ventajas es la simplificación de la administración: los administradores pueden asignar escritorios o aplicaciones virtuales a usuarios de manera dinámica y personalizada, según los requerimientos de cada grupo.
4. Ofrece un acceso seguro y autenticación desdoblada, incrementando la seguridad de la plataforma y permitiendo el acceso seguro desde cualquier navegador web actual y sistema operativo, sin necesidad de software adicional, gracias a plugins de conexión integrados.
5. Entre sus funcionalidades avanzadas destacan la gestión automática del ciclo de vida de los servicios, la programación de tareas, el control de sesiones de usuario y la generación de informes de uso.

2 OBJETO Y ALCANCE

6. El presente documento recoge el Procedimiento de Empleo Seguro de la solución **UDS Enterprise**, incluyendo los siguientes componentes:
 - UDS Server 3.6.0 Build 20241216
 - UDS Actor 3.6.0.18850
 - UDS Tunnel 3.6.0 Build 20240620
7. Esta solución ha sido incluida en el Catálogo de Productos STIC bajo la familia correspondiente al **Anexo F.12 Infraestructura de escritorio virtual (VDI)** en la categoría MEDIA de ENS.
8. El alcance de este documento cubre las recomendaciones de seguridad necesarias para el despliegue y configuración segura del producto en entornos empresariales y organismos públicos.

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

9. **UDS Enterprise** se entrega mediante un modelo de suscripción que incluye el suministro del software paquetizado junto con sus módulos principales y servicios asociados. La entrega se realiza como un Virtual Appliance, es decir, una máquina virtual preconfigurada que se despliega en la plataforma hipervisora elegida (como VMware, KVM, Hyper-V, entre otros).
10. Solo se tendrá acceso a la URL de descarga del software cuando se haya adquirido una suscripción y será proporcionada por el fabricante mediante correo electrónico.

4.2 ENTORNO DE INSTALACIÓN SEGURO

11. Los componentes del producto deben instalarse en un Centro de Proceso de Datos (CPD), cuyo acceso estará limitado a un conjunto de personas que posean una autorización expresa.
12. La instalación también se podrá realizar en entorno virtualizado donde el acceso también estará limitado a un conjunto de personas que posean una autorización expresa.

4.3 REGISTRO Y LICENCIAS

13. El manual de instalación y administración de UDS Enterprise, sección 3.2 *Instalación componentes UDS Enterprise* de [REF1], detalla paso a paso el proceso de registro, activación y gestión de licencias.
14. El registro en UDS Enterprise se realiza durante la instalación mediante la introducción de un código de activación, que puede validarse online u offline según la conectividad del servidor. Las licencias se gestionan por suscripción y se aplican directamente al servidor UDS sin necesidad de componentes adicionales.
15. El código de la licencia es enviado vía correo electrónico incluido en un certificado adjunto. Este es posteriormente recibido únicamente por el cliente final que ha efectuado la compra de la suscripción.

4.4 CONSIDERACIONES PREVIAS

16. Antes de proceder a la instalación y configuración de UDS Enterprise, es necesario disponer de un entorno de virtualización con una arquitectura aplicada que cumpla todos los estándares de seguridad que garanticen el cumplimiento de un entorno seguro certificado en el ENS. Este entorno estará protegido y no será accesible por terceros.
17. Se debe tener preparado un entorno con sistema operativo **Debian 11** para que se ejecuten los componentes **UDS Server** y **UDS Tunnel**.
18. Los componentes de la solución **UDS Enterprise** requieren una infraestructura de clave pública (PKI) para autenticarse frente a los componentes del entorno de operación definidos en la sección 4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN.
19. Respecto a los componentes del entorno de operación, es preciso tener en cuenta las siguientes consideraciones:

- Disponer de una **plataforma de virtualización** con permisos administrativos. La configuración cualificada tuvo en cuenta el uso de un hipervisor VMWARE vSphere 6.5.
 - Se deben establecer dos subredes separadas para prevenir que los usuarios accedan directamente a los escritorios virtuales. La comunicación entre estas dos redes se realizará a través del **UDS Tunnel**.
 - La primera subred contendrá los servicios de gestión: UDS Tunnel, UDS Server, UDS Actor, base de datos MariaDB, Virtual Desktops, vCenter y Windows Server 2019.
 - La segunda subred contiene los usuarios y, de nuevo, UDS Tunnel y UDS Server, para que estos usuarios puedan interactuar a través de la interfaz web. Esta configuración tiene, por tanto, el UDS Tunnel y el UDS Server en ambas subredes de forma que los usuarios estarán en un segmento de red diferente que el resto de las entidades.
20. Para que las plantillas de Windows utilicen TLS de forma segura en RDP, es necesario desactivar las suites y versiones de cifrado TLS. Para ello, con un usuario con privilegios de administrador, ejecute los siguientes comandos:

21. Para deshabilitar TLSv1.0 y TLS v1.1:

```
New-Item
'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Pr
otocols\TLS 1.0\Server' -Force
New-ItemProperty                                     -Path
'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Pr
otocols\TLS 1.0\Server' -PropertyType 'DWORD' -Name 'Enabled' -Value
'0'
New-ItemProperty                                     -Path
'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Pr
otocols\TLS 1.0\Server' -PropertyType 'DWORD' -Name 'DisabledByDefault'
-Value '1'
New-Item
'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Pr
otocols\TLS 1.0\Client' -Force
New-ItemProperty                                     -Path
'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Pr
otocols\TLS 1.0\Client' -PropertyType 'DWORD' -Name 'Enabled' -Value
'0'
New-ItemProperty                                     -Path
'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Pr
otocols\TLS 1.0\Client' -PropertyType 'DWORD' -Name 'DisabledByDefault'
-Value '1'
New-Item
'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Pr
otocols\TLS 1.1\Server' -Force
New-ItemProperty                                     -Path
'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Pr
otocols\TLS 1.1\Server' -PropertyType 'DWORD' -Name 'Enabled' -Value
'0'
New-ItemProperty                                     -Path
'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Pr
otocols\TLS 1.1\Server' -PropertyType 'DWORD' -Name 'DisabledByDefault'
-Value '1'
New-Item
'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Pr
otocols\TLS 1.1\Client' -Force
```

```
New-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Client' -PropertyType 'DWORD' -Name 'Enabled' -Value '0'
New-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Client' -PropertyType 'DWORD' -Name 'DisabledByDefault' -Value '1'
```

22. Para desactivar cipher suites inseguras, para cada una no permitida de acuerdo con las guías CCN-STIC-807 (categoría ALTA de ENS):

```
Disable-TlsCipherSuite -Name "INSECURE_CIPHER_SUITE_HERE"
```

4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN

23. Pueden coexistir diversos componentes externos que no forman parte del núcleo de UDS Enterprise pero que son necesarios o habituales para el correcto funcionamiento de la infraestructura. Los principales componentes externos que pueden aparecer son:
- Plataformas de virtualización.
 - Servidores de autenticación externos.
 - Servidores de base de datos externos.
 - Servidores DNS y DHCP.
 - Servidores de aplicaciones RDS (Remote Desktop Services).
 - Clientes de acceso.
 - Servidores de almacenamiento externo.
 - Equipos de red y seguridad.
24. Estos componentes externos interactúan con UDS Enterprise para conformar una infraestructura VDI completa y funcional.
25. El entorno de operación definido en la cualificación de esta solución está formado por los siguientes componentes:
- **Base de datos MariaDB.** Componente responsable de almacenar los datos de proveedores de servicio, autenticadores, conectividad, eventos de auditoría e información de generación de estadísticas. Para la configuración cualificada, se tuvo en cuenta la versión 10.5.12 de MariaDB instalada en un sistema operativo Debian 11. Se localiza esta base de datos en la misma máquina que el componente **UDS Server**.
 - **Windows Server 2019**, que integra los siguientes componentes:
 - **Servidor LDAP.** Este servidor de directorio debe estar instalado en el entorno de operación y con las características necesarias para proporcionar una correcta autenticación a los usuarios de la organización.
 - Para **habilitar la autenticación y autorización vía LDAP**, es necesario configurar el producto como viene especificado en la sección “4.2 Administrando UDS - Authenticators” del Manual de Instalación, Administración y Usuario de UDS Enterprise 3.6 de [REF1].
 - Este LDAP debe configurarse con las credenciales tanto de los administradores como de los grupos. Por lo tanto, la solución certificada no almacena credenciales de usuario.

- Para garantizar una autenticación correcta de los usuarios, los administradores y los miembros del personal deben autenticarse de la siguiente manera:
 - Autenticación de todos los usuarios directamente en el servidor LDAP.
 - Establecimiento de políticas de complejidad de contraseña con los requerimientos de CCN.
 - Establecimiento de una política para imponer un tiempo de espera de 5 minutos a los usuarios que tengan más de 3 intentos de inicio de sesión fallidos, para evitar ataques de fuerza bruta.
 - **Servidor DNS.** Este servidor es necesario para la operación de la plataforma virtual y los servicios UDS.
 - **Servidor DHCP.** Este servidor es necesario para asignar direcciones IP a los grupos de escritorios virtuales creados por **UDS Enterprise**.
 - **vCenter.** Es un software de gestión de servidores que proporciona una plataforma centralizada para controlar los entornos vSphere.
 - **Virtual Desktop.** Es el escritorio virtual donde está instalado el **UDS Actor**. Este escritorio virtual es el que el **UDS Actor** configura en función de los recursos, almacenamiento y redes necesarios y clona a petición del usuario.
26. En la siguiente figura se detalla la arquitectura de la configuración cualificada en relación con el entorno de operación:

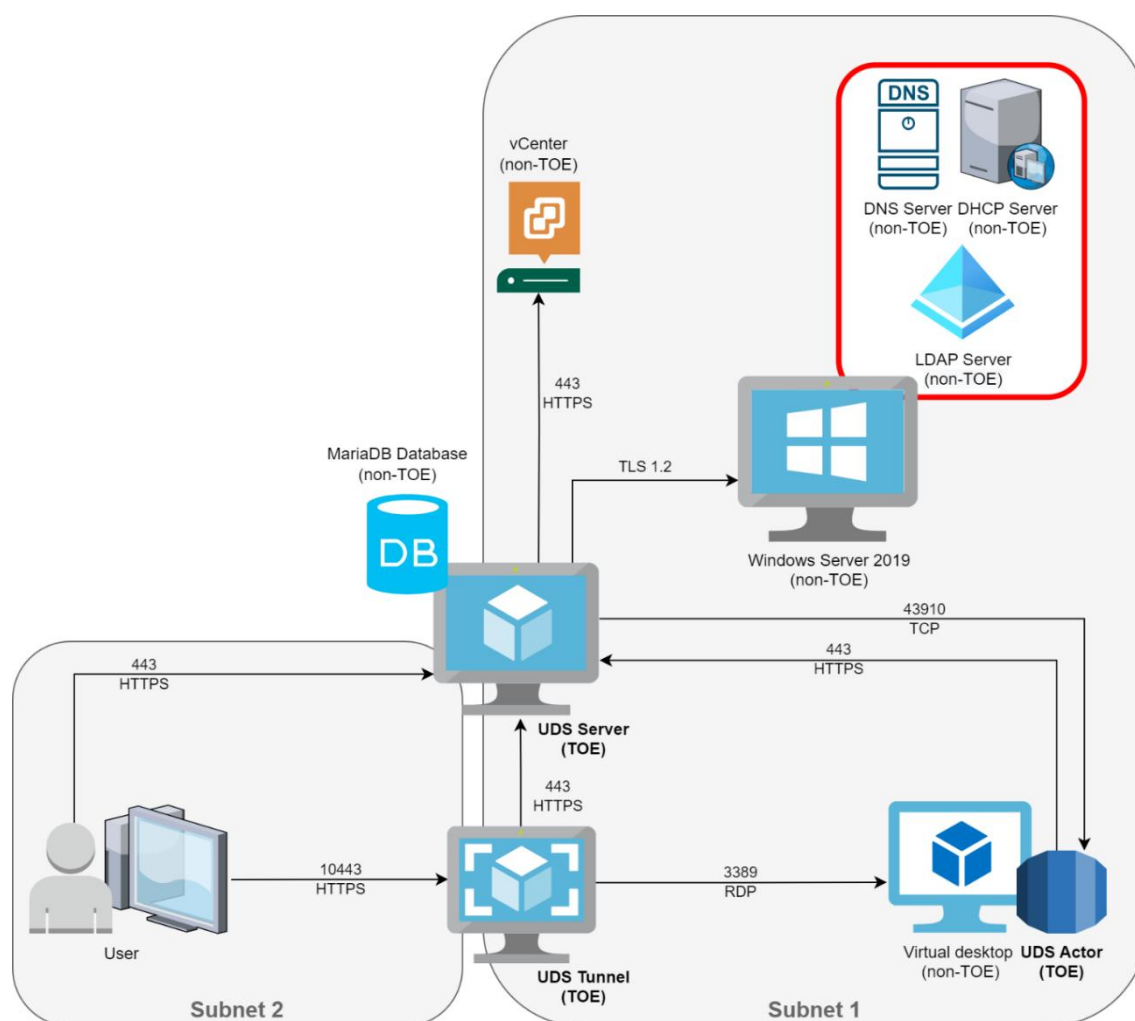


Ilustración 1 Entorno de operación de UDS Enterprise

27. Los usuarios se comunican con el **UDS Server** y con el **UDS Tunnel** a través del protocolo HTTPS (HTTP sobre TLS v1.2 o v1.3), así como el **UDS Tunnel** se comunica con el UDS Server a través del mismo protocolo. Por otro lado, el **UDS Tunnel** se comunica con los Virtual Desktops a través del protocolo RDP (sobre TLS v1.2 o v1.3).

5 FASE DE INSTALACIÓN

28. En el manual de instalación, configuración y administración de UDS Enterprise [REF1], y específicamente en la subsección “3.2.2 Instalando UDS Enterprise – Instalación componentes UDS Enterprise - UDS Server”, se detalla todo el proceso necesario para la instalación del appliance UDS Server.
29. Para realizar una instalación segura, se recomienda seguir las siguientes consideraciones:
 - **Plataforma de virtualización segura** y soportada (VMware vSphere, Microsoft Hyper-V, XenServer, etc.). Solamente los usuarios autorizados tienen acceso administrativo a esta plataforma.
 - **Contraseñas robustas:** Todas las contraseñas (del gestor de la plataforma de virtualización, de la base de datos, del usuario administrador de UDS, etc.) deben cumplir con los requerimientos de las guías CCN.
 - Configuración de red:
 - Asignación de direcciones IP estáticas a los principales componentes de la solución UDS Enterprise.
 - Configurar la máscara de red, pasarela y servidores DNS.
 - Evitar el uso de DHCP para los servidores principales.
 - **Base de datos externa:** Utilizar una base de datos externa y modificar la contraseña por defecto de la base de datos proporcionada por UDS.
 - **Acceso restringido:** Limitar el acceso al panel de administración de UDS Enterprise solo a usuarios autorizados.
30. Estas recomendaciones están detalladas en los manuales oficiales, especialmente en los apartados de “Procedimiento de empleo seguro” incluidos en diversas secciones dentro del manual de instalación, configuración y administración de UDS Enterprise [REF1].

6 FASE DE CONFIGURACIÓN

31. Adicionalmente, es preciso partir de las siguientes configuraciones para lograr la configuración segura cualificada:
- Para el **UDS Server** es necesario que el dispositivo virtual tenga las características y requisitos especificados en la sección “1.4.1 Introducción – Componentes de UDS Enterprise - UDS Server” del Manual de Instalación, Administración y Usuario de UDS Enterprise 3.6 [REF1].
 - Para el **UDS Tunnel** se requiere que el dispositivo virtual tenga las características y requisitos especificados en la sección “1.4.2 Introducción – Componentes de UDS Enterprise - UDS Tunnel” del Manual de Instalación, Administración y Usuario de UDS Enterprise 3.6 [REF1].
 - Para el **UDS Actor** se precisan los requisitos definidos en la sección “1.4.4 Introducción – Componentes de UDS Enterprise - UDS Actor” del Manual de Instalación, Administración y Usuario de UDS Enterprise 3.6 [REF1]. Adicionalmente, El sistema operativo soportado para la generación de escritorios virtuales es Windows 11..
 - Para la **base de datos MariaDB** se requiere que el dispositivo virtual tenga las características y requisitos especificados en la sección “1.4.3 Introducción – Componentes de UDS Enterprise - UDS DBServer” del Manual de Instalación, Administración y Usuario de UDS Enterprise 3.6 [REF1].

6.1 MODO DE OPERACIÓN SEGURO

32. La configuración aplicada en el asistente de configuración del componente UDS Server garantiza el cumplimiento de la versión certificada. El resto de los componentes del entorno VDI, también deberán tener aplicadas una serie de configuraciones para el cumplimiento de la certificación. A continuación, se indican algunas de las más importantes:
- HTTPS obligatorio y certificados válidos.
 - Arquitectura de red segura (DMZ, firewalls, mínimos puertos abiertos).
 - Autenticación robusta y control de acceso.
 - Actualizaciones y monitorización activas.
 - Alta disponibilidad y redundancia.
 - Cifrado de datos y timeout de sesiones automático.

6.2 AUTENTICACIÓN

33. UDS Enterprise utiliza una variedad de mecanismos de autenticación tanto para la instalación y configuración inicial de sus componentes como para el acceso de usuarios y administradores a la plataforma. Estos mecanismos están diseñados para ser flexibles y adaptarse a diferentes entornos y requisitos de seguridad.
34. Durante la instalación y configuración inicial, se utiliza un usuario y contraseña de administrador local para acceder al panel de gestión de UDS Enterprise. Este usuario permite realizar la configuración inicial del sistema y añadir otros métodos de autenticación externos. Para más información sobre los usuarios administradores, revisar el apartado 6.3 ADMINISTRACIÓN DEL PRODUCTO.

35. Una vez configurados otros métodos de autenticación, el usuario local puede ser deshabilitado.
36. UDS Enterprise permite integrar diferentes sistemas de **autenticación externos** que garanticen un acceso seguro de los usuarios. Para más información, ir a la sección 6.6 SERVIDORES DE AUTENTICACIÓN.
37. El acceso al portal web y la comunicación entre componentes se realiza siempre mediante conexiones cifradas con certificados SSL/TLS, lo que refuerza la seguridad de la autenticación.
38. Esta solución acepta el uso de certificados digitales (RSA 3072) para garantizar la autenticación de sus componentes.

6.3 ADMINISTRACIÓN DEL PRODUCTO

6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA

39. La administración de UDS Enterprise se realiza a través de una consola web centralizada, accesible únicamente para usuarios con permisos administrativos, y está diseñada para garantizar la máxima seguridad, integridad y confidencialidad de la gestión del entorno VDI.
40. Todo el acceso administrativo y la gestión de servicios se realiza a través de conexiones cifradas utilizando HTTPS, asegurando la confidencialidad e integridad de los datos transmitidos.

6.3.2 CONFIGURACIÓN DE ADMINISTRADORES

41. Los usuarios administradores en UDS Enterprise tienen roles específicos y configuraciones detalladas para garantizar una administración segura y eficiente del entorno VDI.
42. A continuación, se describen los aspectos clave relacionados con los roles, configuración y políticas de contraseñas para usuarios administradores en UDS Enterprise. Toda esta información está accesible en el manual de instalación, configuración y administración de UDS Enterprise [REF1], y específicamente en la sección “4.4 Administrando UDS - Usuarios, grupos y metagrupos”.
 - **Superusuario Inicial:** Tras la instalación del servidor UDS, existe un superusuario configurado por defecto en el asistente de instalación al cual se le aplicarán políticas de complejidad de contraseña, tiempos de inactividad, etc. Este usuario no se valida contra ningún autenticador externo y está siempre disponible salvo que sea deshabilitado explícitamente en configuraciones avanzadas. Se recomienda deshabilitarlo una vez que se hayan creado usuarios con permisos administrativos adecuados.
 - **Usuarios Administradores Personalizados:** Se deben crear usuarios específicos con permisos justos y necesarios para la administración, evitando el uso del usuario “Administrador”. Esto permite un control granular y seguro sobre las funciones administrativas. Se deben aplicar todas las políticas necesarias para garantizar la seguridad de estos usuarios, estas políticas se habilitarán en los sistemas de autenticación externos conectados a UDS.
 - **Permisos y Accesos:** Los usuarios administradores pueden acceder al panel de control de UDS Enterprise mediante un navegador web con credenciales válidas.

Desde allí, pueden configurar y gestionar escritorios virtuales, aplicaciones, accesos remotos, políticas de seguridad, y recursos asignados a usuarios.

6.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

43. Para poder llevar a cabo las comunicaciones necesarias con los componentes de la solución UDS Enterprise y resto de componentes del entorno operacional, es preciso asegurarse de que los siguientes puertos están accesibles:
- Puerto **443**: comunicaciones entre el usuario y el componente UDS Server, entre el UDS Tunnel y el UDS Server, entre el UDS Actor y el UDS Server y entre el UDS Tunnel y el vCenter.
 - Puerto **10443**: comunicaciones entre el usuario y el UDS Tunnel.
 - Puerto **3389**: comunicaciones entre el UDS Tunnel y el Virtual Desktop.
 - Puerto **43910**: comunicaciones entre el UDS Actor y el UDS Server.

6.5 GESTIÓN DE CERTIFICADOS

44. UDS Enterprise utiliza certificados digitales principalmente para asegurar las comunicaciones entre clientes y servidores, garantizando la autenticidad, integridad y confidencialidad de los datos transmitidos.
45. UDS Enterprise emplea certificados SSL/TLS, en formato PEM, para cifrar y proteger las comunicaciones web y entre servicios. Estos certificados permiten que el acceso al panel administrativo, así como la conexión a escritorios virtuales y aplicaciones, se realice de forma segura, evitando ataques de interceptación o manipulación de datos.
46. Se recomienda utilizar claves privadas de al menos **3072 bits para RSA o 256 bits para ECDSA**, ya que proporcionan un nivel de seguridad adecuado y equilibran rendimiento y protección. El acceso a las claves debe estar restringido y las claves deben renovarse periódicamente.
47. Los certificados se instalan en el directorio */etc/certs*, donde se deben colocar tanto el archivo del certificado del servidor como el archivo de la clave privada, ambos en formato PEM.
48. UDS Enterprise incluye la herramienta *uds cert* para facilitar la instalación de certificados. En el manual oficial del fabricante [REF1] se explica el funcionamiento de esta herramienta.

6.6 SERVIDORES DE AUTENTICACIÓN

49. En el manual de instalación, configuración y administración de UDS Enterprise, sección 4.2 *Authenticators* de [REF1], se indican todas las configuraciones necesarias para integrar un sistema de autenticación externa. A continuación, se detallan los principales requisitos y parámetros de seguridad:
- **LDAPS (LDAP sobre SSL/TLS)**: Es obligatorio que la comunicación entre UDS Enterprise y el servidor de autenticación esté cifrada mediante SSL/TLS. Esto se consigue configurando el servidor AD para que acepte conexiones LDAPS (puerto 636 por defecto).

- **Certificados válidos:** El servidor AD debe disponer de un certificado SSL válido y reconocido, instalado y configurado correctamente para evitar errores de validación y posibles ataques. En la administración de UDS, active la validación SSL en la configuración del autenticador para asegurar que todas las comunicaciones sean cifradas y validadas.
- **Usuario con permisos delegados:** Se requiere un usuario que tenga permisos suficientes para realizar consultas y, si procede, modificar contraseñas en el Active Directory. No es necesario utilizar un usuario administrador completo; se puede delegar el permiso para modificar contraseñas sobre las unidades organizativas necesarias.

6.7 SINCRONIZACIÓN

50. La sincronización NTP en UDS Enterprise se habilita durante la instalación o actualización desde el asistente de configuración, donde se introduce el servidor NTP deseado. También puede configurarse posteriormente desde la consola del servidor, editando la configuración del servicio NTP o utilizando herramientas de gestión de tiempo del sistema operativo.
51. Este proceso de configuración de servidores NTP está indicado y detallado en el manual de instalación, configuración y administración de UDS Enterprise [REF1], específicamente en el paso 4 de la sección “3.2.2 – Instalación UDS Enterprise – Instalación Componentes UDS Enterprise - UDS Server”.

6.8 ACTUALIZACIONES

52. En el documento: Actualización de UDS Enterprise, se detalla todo el proceso para la actualización del software [REF2].
53. A continuación, se detallan los puntos más importantes:
 - a) Realizar una copia de seguridad (backup o snapshot) de la base de datos antes de iniciar la actualización de la solución.
 - b) A la hora de desplegar nuevos Virtual Appliances, subir los nuevos de UDS Server a la plataforma hipervisora soportada y apagar los servidores antiguos una vez iniciado el proceso de actualización.
 - c) Para nuevos servidores, iniciar y configurar el nuevo UDS Server con los mismos datos de red y configuración que la versión anterior, conectándolo a la base de datos existente. Acceder a la dirección IP del nuevo servidor (normalmente por el puerto 9900) vía HTTPS para completar la configuración inicial.
 - d) Activar la suscripción de la nueva versión, preferiblemente con salida directa a internet para este proceso.

6.9 AUTO-CHEQUEOS

54. La solución certificada no incorpora mecanismos automáticos de auto-chequeo (self-test) de integridad del software ni de verificación del funcionamiento de algoritmos criptográficos.

55. Se considera que el control de integridad y funcionamiento se realiza mediante otros mecanismos complementarios, como la monitorización continua, los registros de actividad y las actualizaciones.

6.10 ALTA DISPONIBILIDAD

56. Los componentes de UDS Enterprise pueden configurarse en alta disponibilidad mediante balanceadores de carga, asegurando la continuidad del servicio ante posibles fallos.
57. Esta solución soporta una configuración en alta disponibilidad, todos los requisitos y proceso de configuración están indicados en la guía: Configurar UDS Enterprise en Alta disponibilidad [REF3].

6.11 AUDITORÍA

6.11.1 REGISTRO DE EVENTOS

58. En el documento [REF4] se especifican todos los ficheros de logs del servidor UDS que contienen los eventos sucedidos en el software, estos ficheros están en formato texto y pueden ser tratados para su filtrado y mejor visualización [REF4].
59. Adicionalmente también existe el informe “registro de auditoría” en la sección “informes disponibles” en la administración de UDS. A través de este es posible visualizar cualquier evento realizado en el panel de administración.
60. Como ejemplo de los principales ficheros de logs:

Componente	Fichero de Log	Tipo de Eventos registrados
UDS Server	auth.log	Validación de usuarios, IP, máquina origen
UDS Server	sql.log	Cambios en la base de datos
UDS Server	trace.log	Acceso a servicios, usuario, transporte, IP
UDS Server	uds.log	Conexiones y errores del servidor
UDS Server	use.log	Accesos a servicios, login/logout, cliente, autenticador, servicio, pool
UDS Server	workers.log	Tareas internas (autolimpieza, programadas, caché)
Web Server (NGINX)	access.log	Accesos web, terceros, interfaz de administración
Asistente de configuración	setup.log	Eventos y errores de configuración del servidor/tunneler
Asistente de configuración	trace.log, run.log	Información adicional sobre configuración (BD, zona horaria)

Tabla 1 Ejemplos de logs de la solución UDS Enterprise

6.11.2 ALMACENAMIENTO LOCAL

61. Los ficheros de logs del servidor UDS se almacenan por defecto en el almacenamiento local del servidor, en el documento “Logs UDS Enterprise” [REF4], y específicamente en la sección “*UDS-Server*” se informa de las políticas de retención de estos ficheros para lograr una rotación y tamaño óptimo de estos ficheros con el fin de dotar al entorno de unos ficheros de logs con información suficiente y evitar que un tamaño excesivo de los ficheros afecte al rendimiento del servidor.

6.11.3 ALMACENAMIENTO REMOTO

62. Para la solución certificada no se ha hecho uso de un servidor remoto Syslog. Toda la auditoría queda almacenada de la siguiente manera:
 - En el UDS Server, se almacenan los registros de auditoría relacionados con los cambios en la configuración del UDS Server y las conexiones de usuario del túnel HTML5 RDP.
 - En la base de datos MariaDB se almacenan los registros de auditoría de las funcionalidades de seguridad certificadas.
 - En los directorios del sistema operativo de los escritorios virtuales con el UDS Actor instalado.

6.12 BACKUP

63. En el documento: Backup y restore de la base de datos de UDS Enterprise [REF5], y en específico la sección “*Backup de la Base de datos de UDS Enterprise*” se muestran ejemplos de cómo realizar backup de todas las configuraciones realizadas en UDS Enterprise, este documento se centra en el componente Base de datos, ya que el propio servidor de UDS no almacena ningún dato de la configuración de la administración del entorno o de usuarios.
64. En dicho documento se especifica que la configuración de backup realizada debe ser como mínimo diaria y alojada en un almacenamiento seguro y siempre disponible para que en caso de desastre y pérdida pueda ser restaurado lo antes posible.
65. En el componente UDS Server, únicamente se almacenarán los ficheros de log, los cuales se recomienda su configuración a través de una herramienta syslog para que, en caso de desastre, estos ficheros no se pierdan.

7 REFERENCIAS

- [REF1] Manual de Instalación, Administración y Usuario de UDS Enterprise 3.6
- [REF2] Manual “Actualización de UDS Enterprise”
- [REF3] Manual “Configurar UDS Enterprise en Alta disponibilidad”
- [REF4] Manual “Logs UDS Enterprise”
- [REF5] Manual “Backup y Restore de la base de datos de UDS Enterprise”

8 ABREVIATURAS

AD	Active Directory
CCN	Centro Criptológico Nacional
CPD	Centro de Procesamiento de Datos
DB	Database
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
DNS	Domain Name System
ECDSA	Elliptic Curve Digital Signature Algorithm
ENS	Esquema Nacional de Seguridad
HTML5	HyperText Markup Language version 5
HTTPS	HTTP over TLS
IP	Internet Protocol
KVM	Kernel-based Virtual Machine
LDAP	Lightweight Directory Access Protocol
LDAPS	LDAP over SSL/TLS
NTP	Network Time Protocol
OS	Operating System
PEM	Privacy Enhanced Mail
PKI	Public Key Infrastructure
RDP	Remote Desktop Protocol
RDS	Remote Desktop Services
RSA	Rivest-Shamir-Adleman
SSL	Secure Sockets Layer
STIC	Seguridad de las Tecnologías de la Información y las Comunicaciones
Syslog	System Logging Protocol
TI	Tecnologías de la Información
TLS	Transport Layer Security
UDS	Universal Desktop Services
URL	Uniform Resource Locator
VDI	Virtual Desktop Infrastructure

