# Guía de Seguridad de las TIC
# CCN-STIC 1658

# Procedimiento de Empleo Seguro
# Red Hat Enterprise Linux


Junio 2026

Edita:

CCN
c=ES, l=MADRID, o=CCN,
ou=SELLO ELECTRONICO,
2.5.4.97=VATES-S2800155J,
serialNumber=S2800155J,
cn=CCN
2026.06.11 13:32:29 +02'00'

Centro Criptológico Nacional, 2026

# ÍNDICE

# 1 INTRODUCCIÓN

1. Red Hat Enterprise Linux 9.0 Extended Update Support es un sistema operativo de código abierto que soporta un entorno informático de uso general para múltiples usuarios y aplicaciones. Construido sobre una base de código abierto, Red Hat Enterprise Linux 9.0 Extended Update Support ofrece un sistema operativo robusto, con soporte y actualizaciones a largo plazo, orientado a servidores y máquinas virtuales. Su diseño está orientado a facilitar la implementación, administración y escalabilidad en infraestructuras tanto físicas como virtuales, y responde a las necesidades de compañías que buscan fiabilidad y soporte técnico de nivel empresarial.

2. Como principales características se incluyen la generación de auditoría, implementación de algoritmos criptográficos considerados como recomendados por [REF4], canales de comunicación seguros, protección contra ataques de autenticación por fuerza bruta, control de accesos a información sensible y verificación de la integridad del arranque.

3. Principalmente, la configuración y gestión de sus funcionalidades se realizan de forma intuitiva mediante una consola de línea de comandos (CLI). Esta interfaz permite acceder y administrar el dispositivo tanto localmente como de manera remota, mediante el protocolo SSHv2, garantizando así el cumplimiento de los estándares de seguridad establecidos por la normativa LINCE.

# 2 OBJETO Y ALCANCE

4. El objeto del presente documento es servir como guía para realizar la instalación, configuración y operación segura de Red Hat Enterprise Linux 9.0 Extended Update Support.
5. El alcance del producto evaluado comprende todo el sistema operativo, instalado sobre las plataformas PowerEdge R440, z16 3931-A01 y POWER10 9080-HEX.
6. El producto Red Hat Enterprise Linux 9.0 Extended Update Support ha sido incluido en el catálogo de productos y servicios STIC (CPSTIC). Para conocer el listado, categoría o nivel y familia de éste, consulte: https://cpstic.ccn.cni.es/es/catalogo-productos-servicios-stic.

# 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.

Apartado 5. En este apartado se recogen recomendaciones a tener en cuenta durante la fase de instalación del producto.

Apartado 6. En este apartado se recogen las recomendaciones a tener en cuenta durante la fase de configuración del producto para lograr una configuración segura.

# 4 FASE PREVIA A LA INSTALACIÓN

## 4.1 ENTREGA SEGURA DEL PRODUCTO

7. El producto está formado por distintos paquetes, que deben ser descargados de https://access.redhat.com/. En concreto, los paquetes que forman parte del producto son:
   - Imagen de instalación ISO de Red Hat Enterprise Linux 9.0.
   - El paquete cc-config RPM (contiene archivos de instalación adicionales).
   - Paquetes adicionales RPM (contienen versiones actualizadas de algunos paquetes incluidos en la imagen ISO).
8. A continuación, se detallan los pasos para obtener de forma segura cada uno de los componentes.
9. Realice los siguientes pasos para obtener la imagen de instalación ISO de Red Hat Enterprise Linux 9.0:
   a) Inicie sesión en https://access.redhat.com/.
   b) Haga clic en ‘Descargas’ en la esquina superior izquierda.
   c) Haga clic en el enlace 'Red Hat Enterprise Linux' bajo 'Product' y luego haga clic en 'All Red Hat Enterprise Linux Downloads'.
   d) Para la instalación en Dell PowerEdge, seleccione ‘Red Hat Enterprise Linux for x86_64’ como variante del producto y ‘9.0’ como versión.
   e) Para la instalación en IBM Z, busque 'Red Hat Enterprise Linux for IBM z Systems' como variante de producto y '9.0' como versión.
   f) Para la instalación en IBM Power, busque ‘Red Hat Enterprise Linux for Power, little endian’ como variante de producto y ‘9.0’ como versión.
   g) A continuación, bajo 'Product Software' debería ver una sección llamada 'Full installation image' y una línea con 'Red Hat Enterprise Linux 9.0 Binary DVD'.
   h) Haga clic en ‘Download Now’ a la derecha de esa línea.

   **NOTA**: Es posible que tenga que seguir instrucciones adicionales para grabar un DVD o grabar en una unidad USB de arranque o adjuntar la ISO como medio virtual al hardware. Consulte [REF5] para obtener instrucciones para su entorno.
10. El paquete RPM cc-config es la forma que tiene Red Hat de enviar archivos de instalación adicionales a los clientes a través de canales de confianza, que requieren una suscripción RHEL Extended Update Support (EUS) para acceder. Realice los siguientes pasos para obtener el **paquete RPM cc-config**:
    a) Inicie sesión en https://access.redhat.com/.
    b) Haga clic en ‘Downloads’ en la esquina superior izquierda.
    c) Haga clic en el enlace 'Red Hat Enterprise Linux' bajo ‘Product’.
    d) Seleccione 'Red Hat Enterprise Linux for x86_64 - Extended Update Support' como variante del producto y '9.0' como versión.

e) Haga clic en la pestaña 'Packages'.

f) En el campo 'Search', introduzca "cc-config".

g) En la lista de resultados filtrados, haga clic en el elemento 'cc-config'.

h) Seleccione la versión 9.0 en la pestaña 'Version'.

i) En la sección de descarga de RPM de la parte inferior, haga clic en el botón 'Download Now' situado junto al nombre del paquete.

j) Después de transferir el archivo descargado a un sistema RHEL-9.0, puede instalarlo ejecutando el comando: `rpm -ivh cc-config-9.0-*.rpm`

11. Realice los siguientes pasos para obtener los **paquetes RPM adicionales**:

    a) Abra el archivo kickstart ospp.ks ubicado en /usr/share/cc-config con un editor de texto y busque una sección llamada sanity_check_nvrs, que contiene una lista de paquetes RPM descritos en varias columnas tituladas:

        - Source RPM
        - Name
        - Version
        - Release
        - Architectures

    b) Descargue cada uno de los RPMs listados siguiendo el mismo procedimiento que para la descarga de cc-config, utilizando el nombre para la búsqueda inicial, y concatenando versión y release con un guion (-), seleccionándolo en el desplegable 'Versión' de la web.

12. Por defecto, todos los paquetes proporcionados para la instalación están firmados con RSA-4096. Para que el producto compruebe automáticamente dichas firmas antes de llevar a cabo la instalación, se debe seguir la sección 3.2.2.1 de [REF1].

## 4.2 REGISTRO Y LICENCIAS

13. Siga el capítulo 2 (CHAPTER 2. REGISTERING THE SYSTEM AND MANAGING SUBSCRIPTIONS) de [REF2] para el registro del software y de la licencia.

## 4.3 CONSIDERACIONES PREVIAS

14. Para instalar el producto, se necesitarán los siguientes sistemas:

    - Un host para acceder a https://access.redhat.com/ y descargar la imagen de instalación.
    - Un host donde previamente se ha instalado Red Hat Enterprise Linux 9.0 EUS y que dispone de la suscripción Extended Update Support (EUS), para extraer y configurar el paquete cc-config.

    **Nota**: este host con RHEL 9.0 EUS no es el producto, es un host auxiliar.

- Un servidor web para almacenar temporalmente los archivos necesarios para la instalación del producto. Las instrucciones para configurar el servidor web pueden encontrarse en [REF6].
- Un servidor FTP para la instalación de los sistemas LPAR IBM Z. Las instrucciones para configurar el servidor FTP pueden encontrarse en [REF7].

15. **Nota**: el servidor web y el servidor FTP pueden ser instalados en el mismo host si es necesario.

- Una plataforma hardware sobre la que instalar el producto. Puede ser una de las siguientes plataformas:
    - **Dell PowerEdge Systems**. Las plataformas Dell PowerEdge deben configurarse para utilizar el arranque UEFI, con la comprobación de firmas de Secure Boot activada antes de la instalación del sistema operativo.

a) Inicie el equipo y acceda al software de configuración del sistema (BIOS), utilizando la consola virtual iDRAC o pulsando F2 durante el arranque inicial.

b) Navegue hasta la BIOS del sistema.

c) En Boot Settings, establezca Boot Mode en UEFI.

d) En System Security, configure:

- Secure Boot a “Enabled”.
- Secure Boot Policy a “Standard”.
- Secure Boot Mode a “Deployed”.

e) A continuación, pulse varias veces la tecla Esc y, cuando se le pregunte, guarde la configuración modificada y reinicie.

16. Para habilitar la consola serie local en los sistemas Dell PowerEdge, se debe ejecutar el siguiente proceso:

a) Modificar el archivo */etc/default/grub* para habilitar las conexiones de consola de la siguiente forma:

```
vim /etc/default/grub
GRUB_CMDLINE_LINUX_DEFAULT="console=tty0 console=ttyS0,9600n8"
GRUB_TERMINAL="console serial"
GRUB_SERIAL_COMMAND="serial --speed=9600 --unit=0 --word=8 --parity=no
--stop=1"
```

**Nota**: La velocidad en baudios debe coincidir con la del terminal y la del sistema Dell PowerEdge.

b) Reconstruya el archivo de configuración de grub ejecutando el siguiente comando:

```
grub2-mkconfig -o /boot/efi/EFI/redhat/grub.cfg
```

c) Reinicie el producto.

- **IBM Z Systems**. No se necesita ningún prerrequisito adicional.
- **IBM Power10 Systems**. Deben configurarse con la comprobación de firmas de Secure Boot desactivada antes de la instalación del sistema operativo; de lo contrario no será posible arrancar desde el archivo ISO del DVD montado. El Secure Boot debe habilitarse sólo después de la instalación. Cambiar la

configuración de Secure Boot sólo es posible para una LPAR que esté apagada, así que asegúrese de hacerlo primero. A continuación, ejecute los siguientes pasos en la Consola de Gestión de Hardware (HMC):

a) En Particiones, haga clic en “LPAR”.

b) Navegue a Propiedades, Propiedades Generales y luego a Configuración Avanzada.

c) Configure Secure Boot como “Disabled” o “Enabled and Log only”.

d) Guarde la configuración.

## 4.4 COMPONENTES DEL ENTORNO DE OPERACIÓN

17. Los componentes que deben estar presentes en el entorno operacional para que el producto opere de acuerdo a la configuración evaluada son los siguientes:

- **Servidor de actualizaciones**. El producto recibe actualizaciones del repositorio local de una organización a través de TLS.
- **Servidor SSH**. El producto es capaz de comunicarse de forma segura con un servidor SSHv2.
- **Cliente SSH**. El producto es capaz de comunicarse de forma segura con un cliente SSHv2.
- **Plataforma hardware**. El producto requiere una plataforma hardware sobre la que instalarse, que cumpla las siguientes especificaciones:
  - Plataformas Intel Xeon Silver x86-64 UEFI (de microarquitectura Cascade Lake).
  - Plataformas IBM z16 (LPAR) con UEFI 2.3.1 o posterior.
  - Plataformas Power10, PowerVM (LPAR) con UEFI 2.3.1 o posterior.

# 5 FASE DE INSTALACIÓN

## 5.1 PREREQUISITOS

18. Para preparar el entorno de instalación y garantizar que el sistema cumpla con los requisitos, es necesario configurar previamente la infraestructura de software y repositorios:

    a) Se deberá desplegar una máquina Red Hat Enterprise Linux 9.0 EUS con la suscripción activada creando un repositorio local para conseguir la configuración evaluada. En él se deberá descargar e instalar el paquete cc-config, el cual es el encargado de definir los paquetes necesarios para cumplir con la CC.

    b) Estos paquetes se pueden descargar desde el RHEL-9.0 EUS subscribed system o desde la web de Red Hat. Siga la sección 3.1.2 y 3.1.3 de [REF1].

    c) Una vez descargados dichos paquetes, se deberá crear un repositorio YUM (sección 4.1.1 de [REF1]) y habilitar Apache (sección 2.1.1 de [REF1]).

    d) También será necesario modificar el archivo ospp.ks en la máquina con el repositorio para apuntar al repositorio YUM creado con los paquetes que se necesitan para la instalación. Siga la sección 4.1.2 de [REF1].

    e) El repositorio deberá estar configurado para obtener paquetes de actualización desde los canales EUS.

## 5.2 INSTALACIÓN

19. Siga la sección 4 de [REF1] para llevar a cabo la instalación del producto.

20. Es importante tener en cuenta que el producto debe instalarse con el modo FIPS habilitado, ya que las claves públicas/privadas generadas en el proceso de instalación se generarán con algoritmos aprobados por FIPS.

21. En función de la plataforma hardware elegida para la instalación del producto, se deberá seguir una de las siguientes secciones:

    - Instalación en Dell PowerEdge. Siga la sección 4.2.1 de [REF1].
    - Instalación en IBM Z LPAR. Siga la sección 4.2.2 de [REF1].
    - Instalación en IBM PowerVM LPAR. Siga la sección 4.2.3 de [REF1].

# 6 FASE DE CONFIGURACIÓN

## 6.1 AUTENTICACIÓN

22. El producto permite dos tipos de autenticación para los usuarios: a través de credenciales locales (usuario y contraseña) y a través de clave pública.

23. Cuando los usuarios se autentican mediante credenciales locales (usuario y contraseña), deberá tenerse en cuenta lo siguiente:

    - Cada usuario establecerá su propia contraseña siguiendo la política de contraseñas definida por el administrador en la sección 6.2.2.
    - Cada usuario contará con un máximo de 3 intentos de inicio de sesión fallidos, tras los cuales se bloqueará al usuario y solamente podrá ser desbloqueado por un administrador. El número máximo de intentos fallidos será establecido por el administrador como se indica en la sección 6.2.2.

## 6.2 ADMINISTRACIÓN DEL PRODUCTO

### 6.2.1 ADMINISTRACIÓN LOCAL Y REMOTA

24. El producto se administrará tanto de forma local (a través de consola, con acceso físico al producto) como remota (a través de CLI) por medio de SSHv2.

25. Para acceder localmente, el usuario deberá contar con acceso físico a la plataforma sobe la que se instala el producto. Una vez arranque la plataforma, se le mostrará una ventana de *login*, en la que deberá de introducir sus credenciales.

26. Para acceder remotamente, el usuario deberá de ejecutar el siguiente comando desde una interfaz de línea de comandos en su dispositivo (distinto al usado para instalar el producto): `ssh` *`username@direcciónIP del producto`* e introducir su contraseña una vez le sea solicitada.

### 6.2.2 CONFIGURACIÓN DE ADMINISTRADORES

27. Tal y como se define en [REF3] (sección 6.5.1), existe un rol de usuario “Administrator” (entre los que se incluye el usuario root), cuyos miembros son del grupo “wheel”. Por otra parte, existe otro grupo de usuarios llamado “Users”, que no cuentan con privilegios de administración (no pueden ejecutar comandos con sudo). Para más detalles, consulte la sección 9 de [REF2].

28. Por otra parte, el administrador realizará las siguientes configuraciones:

    - Configuración de la política segura de contraseñas. Ejecute el comando `pam_pwquality` con las siguientes opciones para habilitar una política de contraseñas con longitud mínima de 12 caracteres y al menos una letra mayúscula, una minúscula, un número y un carácter especial:
        - minlen=12
        - ucredit=-1
        - lcredit=-1

- dcredit=-1
- ocredit=-1

- Configuración del tiempo de inactividad de las sesiones. Lleve a cabo las siguientes configuraciones para cerrar la sesión del usuario tras 5 minutos de inactividad:
  - Para sesiones locales, edite el fichero */etc/profile.d/timeout.sh* estableciendo el valor "300" en la variable *TMOUT*. Guarde el fichero y aplique los cambios ejecutando el comando `source /etc/profile`.
  - Para sesiones remotas por SSH, edite el fichero */etc/ssh/sshd_config* estableciendo el valor "300" en la variable *ClientAliveInterval*, y el valor "0" en la variable *ClientAliveCountMax*. Guarde el fichero y reinicie el servicio SSH con el comando sudo `systemctl restart sshd`.
- Configuración del número de intentos fallidos de inicio de sesión. Configure el archivo `/etc/security/faillock.conf` de la siguiente forma para bloquear a los usuarios tras 3 intentos de inicio de sesión fallidos:
  - Añada la línea deny = 3
  - El administrador puede desbloquear un usuario bloqueado ejecutando el siguiente comando: `faillock --user <user> --reset`
- Configuración del mensaje de aviso y consentimiento en el inicio de sesión (login banner).
  - Para sesiones locales, configure el archivo /etc/issue indicando el contenido del banner.
  - Para sesiones remotas por SSH, configure el archivo /etc/issue.net indicando el contenido del banner. Tras esto, configure el fichero /etc/ssh/sshd_config añadiendo o verificando la presencia de la línea "Banner /etc/issue.net". Por último, reinicie el servicio SSH con el comando sudo `systemctl restart sshd`.

## 6.3 CONFIGURACIÓN DE CRIPTOGRAFÍA

29. La criptografía en Red Hat se maneja de forma centralizada mediante unos archivos llamados crypto-policies. Estos permiten manejar la criptografía a nivel general (group/mac/cipher/…), a nivel de protocolo (TLS/SSH/Kerberos/…) o a nivel de implementación (libssl/GnuTLS/…). Además, no permiten especificar explícitamente qué suites de cifrado utilizar, sino que especifican las diferentes partes de estas, como se ha mencionado previamente a nivel general.
30. Para configurar los protocolos de comunicación (en este caso, TLS y SSH), será necesario crear una nueva política. Para ello, copie el fichero FIPS.pol del directorio */usr/share/crypto-policies/policies/* y péguelo con un nuevo nombre dentro de */etc/crypto-policies/policies/*.
31. Una vez copiado, modifíquelo para cumplir con ENS ALTO de la siguiente forma:

```
(update group with)
group = SECP256R1 SECP384R1 SECP521R1 \
    FFDHE-3072 FFDHE-4096 FFDHE-6144 FFDHE-8192 X25519
```

```
(left only the following ones)
sign = ECDSA-SHA3-256 ECDSA-SHA2-256 \
       ECDSA-SHA3-384 ECDSA-SHA2-384 \
       ECDSA-SHA3-512 ECDSA-SHA2-512
(remove both ciphers fields and use the next one)
cipher = AES-256-GCM AES-256-CTR \
         AES-128-GCM AES-128-CTR

(left only the ECDHE)
key_exchange=ECDHE
(Modify the sizes)
min_dh_size = 3072
min_dsa_size = 3072
min_rsa_size = 3072
```

32. Las claves SSH (SSH HostKeys) a usar no se declaran en la crypto-policy, sino que se deberán referenciar en el archivo /etc/ssh/sshd_config para funcionar. Se deben usar claves generadas con RSA-3072 bits o superior, o ECDSA usando las curvas P-384 o P-521:
    a) HostKey /etc/ssh/ssh_host_rsa3072_key
    b) HostKey /etc/ssh/ssh_host_rsa4096_key
    c) HostKey /etc/ssh/ssh_host_ecdsa384_key
    d) HostKey /etc/ssh/ssh_host_ecdsa521_key
33. Tras esta configuración, guarde el fichero y reinicie el servicio SSH con el comando sudo systemctl restart sshd.
34. Establezca la política configurada como la política criptográfica a usar a través del siguiente comando:

```
update-crypto-policies --set <Nombre de la política configurada>
```

35. Reinicie el dispositivo.

## 6.4 GESTIÓN DE CERTIFICADOS

36. Por defecto, la instalación del producto genera una hostkey SSH con ECDSA y P-256. Ejecute el siguiente comando con privilegios de administrador para generar una hostkey ECDSA con P-384 o P-521:

```
sudo ssh-keygen -t ecdsa -b <384|521> -f
/etc/ssh/ssh_host_ecdsa_nistp<384|521>_key -N ''
```

## 6.5 SINCRONIZACIÓN

37. Configure el fichero `/etc/chrony.conf` para sincronizar el producto con un servidor NTP externo añadiendo la siguiente línea: "server <FQDN/dirección IP> iburst".
38. Tras esta configuración, ejecute el siguiente comando para reiniciar el servicio chrony:

```
service chronyd restart
```

## 6.6 ACTUALIZACIONES

39. El producto se encuentra configurado para llevar a cabo actualizaciones de forma automática. Consulte la sección 3.2.2.3 de [REF1] para más detalles.

40. Por otra parte, el producto permite consultar si existen actualizaciones disponibles e instalarlas de forma manual. Consulte la sección 3.2.2.2 de [REF1] para más detalles.

## 6.7 AUTO-CHEQUEOS

41. El producto verifica la integridad del *boot chain* a través de la comprobación de firmas digitales. Consulte la sección 6.6.5 de [REF3] para más detalles.

## 6.8 CLAVES SECURE BOOT

42. Como se declara en [REF3], el proceso de secure boot implementado por el producto (*second stage boot loader*) se basa en la comprobación de firmas digitales RSA-2048 con SHA-256.

43. No obstante, las claves usadas para la verificación (en este caso, de 2048 bits) no depende del producto, sino que está condicionado por el firmware UEFI de la placa base sobre la que se instala, donde se almacenan las claves públicas utilizadas en el secure boot y donde se realiza la primera fase del arranque seguro (*first stage boot loader*). UEFI permite claves de 2048 a 4096 bits, y actualmente no hay placas base en el mercado que restrinjan la longitud mínima a 3072 bits. El firmware UEFI es cargado directamente por el fabricante de la placa base y no depende del producto.

44. Ya que el algoritmo RSA-2048 se considera Legacy de acuerdo a [REF4], se recomienda sustituir la plataforma hardware sobre la que corre el producto por una cuya placa base restrinja la longitud mínima de las claves públicas almacenadas en el firmware UEFI a 3072 bits, cuando estas estén disponibles en el mercado.

## 6.9 AUDITORÍA

### 6.9.1 ALMACENAMIENTO LOCAL

45. Los registros de auditoría se almacenan en `/var/log/Audit/Audit.log`. Consulte la sección 10.1 de [REF1] para comprobar el formato de dichos registros.

46. Consulte la sección 10.2 de [REF1] para verificar todos los eventos para los cuales el producto genera un registro de auditoría.

# 7 REFERENCIAS

[REF1] Red Hat Enterprise Linux 9.0 EUS Common Criteria Guide, version 1.1 January 2024 (https://www.niap-ccevs.org/MMO/Product/st_vid11379-agd1.pdf)

[REF2] Red Hat Enterprise Linux 9 Configuring basic system settings Set up the essential functions of your system and customize your system environment, 2024-09-06 (https://docs.redhat.com/en-us/documentation/red_hat_enterprise_linux/9/pdf/configuring_basic_system_settings/Red_Hat_Enterprise_Linux-9-Configuring_basic_system_settings-en-US.pdf)

[REF3] Red Hat Enterprise Linux 9.0 EUS Security Target, version 1.1, 04 January 2024 (https://www.commoncriteriaportal.org/nfs/ccpfiles/files/epfiles/st_vid11379-st.pdf)

[REF4] Guía de Seguridad de las TIC CCN-STIC 807 - Criptología de empleo en el Esquema Nacional de Seguridad, Mayo 2022 (https://www.ccn-cert.cni.es/es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/513-ccn-stic-807-criptologia-de-empleo-en-el-ens/file?format=html)

[REF5] Red Hat Enterprise Linux 9 https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/9/html/performing_a_standard_rhel_9_installation/assembly_preparing-for-your-installation_installing-rhel#assembly_creating-a-bootable-installation-medium_assembly_preparing-for-your-installation

[REF6] Setting up a single-instance Apache HTTP Server https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/9/html/deploying_web_servers_and_reverse_proxies/setting-apache-http-server_deploying-web-servers-and-reverse-proxies#setting-up-a-single-instance-apache-http-server_setting-apache-http-server

[REF7] How to configure FTP Server on Red Hat Enterprise Linux ?
https://access.redhat.com/solutions/1421563

# 8 ABREVIATURAS

| | |
|---|---|
| AES | Advanced Encryption Standard |
| BIOS | Basic Input Output System |
| CC | Common Criteria |
| CLI | Command Line Interface |
| CPSTIC | Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y las Comunicaciones |
| CTR | Counter |
| DH | Diffie-Hellman |
| DSA | Digital Signature Algorithm |
| DVD | Digital Versatile Disc |
| ECDHE | Elliptic Curve Diffie-Hellman Ephemeral |
| ECDSA | Elliptic Curve Digital Signature Algorithm |
| ENS | Esquema Nacional de Seguridad. |
| EUS | Extended Update Support |
| FFDHE | Finite Field Diffie-Hellman Ephemeral |
| FIPS | Federal Information Processing Standards |
| FQDN | Fully Qualified Domain Name |
| FTP | File Transfer Protocol |
| GCM | Galois Counter Mode |
| HMC | Hardware Management Console |
| IBM | International Business Machines |
| iDRAC | Integrated Dell Remote Access Controller |
| IP | Internet Protocol |
| ISO | International Organization for Standardization |
| LPAR | Logical Partition |
| NTP | Network Time Protocol |
| pam_pwquality | Pluggable Authentication Module Password Quality |
| RHEL | Red Hat Enterprise Linux |
| RPM | Red Hat Package Manager |
| RSA | Rivest Shamir Adleman |
| SECP256R1 | Standards for Efficient Cryptography Prime256v1 |

| | |
|---|---|
| SECP384R1 | Standards for Efficient Cryptography Prime384v1 |
| SECP521R1 | Standards for Efficient Cryptography Prime521v1 |
| SHA | Secure Hash Algorithm |
| SHA2 | Secure Hash Algorithm 2 |
| SHA3 | Secure Hash Algorithm 3 |
| SSH | Secure Shell |
| SSHv2 | Secure Shell version 2 |
| STIC | Seguridad de las Tecnologías de la Información y las Comunicaciones |
| TLS | Transport Layer Security |
| UEFI | Unified Extensible Firmware Interface |
| VM | Virtual Machine |
| x86-64 | Extended 86 64-bit |
| YUM | Yellowdog Updater Modified |