centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1623

Procedimiento de empleo seguro
Cisco Email Security Appliance

Agosto 2023

MINISTERIO DE DEFENSA

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

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

centro criptológico nacional

CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2024.01.15 12:04:29 +01'00'

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-23-287-6.
Fecha de Edición: enero de 2024.

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

ÍNDICE

1. INTRODUCCIÓN

1. El objetivo de este documento es proporcionar las directrices de seguridad que deben ser tenidas en cuenta para la configuración de los equipos de *Cisco Email Security Appliance (ESA)*, con sistema operativo AsyncOS versión 13.X.
2. Esta guía incluye el detalle asociado a la configuración de seguridad cuando es necesario y referencias a la documentación de Cisco.
3. Los siguientes modelos han sido cualificados e incluidos en el Catálogo de Productos y Servicios de Seguridad TIC (CPSTIC) del Centro Criptológico Nacional en la familia "Protección de Correo Electrónico":
    - C190
    - C195
    - C390
    - C395
    - C690
    - C690X
    - C695
    - C695F
    - Dispositivos virtuales C100v, C300v y C600v ejecutados sobre UCS-C220-M4 y UCS-C220-M5.
4. La estructura del documento y sus contenidos no exigen una lectura lineal del mismo. Se recomienda al lector utilizar el índice de contenidos para localizar el capítulo que trate el aspecto concreto sobre el que se desee obtener información.

2. OBJETO Y ALCANCE

5. El objeto de la presente guía es detallar la configuración del producto para utilizarlo de forma segura. De esta forma, es posible establecer un marco de referencia que contemple las recomendaciones STIC en el despliegue y utilización de estos productos.
6. Este documento, salvo menciones especiales, no aporta ajustes de configuración para la operación del producto, fuera de las directamente relacionadas con su operación en modo seguro. Aspectos como las políticas de flujo de información y el control de acceso, deben ser implementadas de acuerdo a las políticas vigentes en la organización.
7. Las autoridades responsables de la aplicación de la política de seguridad de las TIC (STIC) determinarán el análisis y aplicación de este documento a los equipos Cisco WLC bajo su responsabilidad.

3. ORGANIZACIÓN DEL DOCUMENTO

8. Este documento se compone de los siguientes apartados:

   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.

   d) Apartado **7**. En este apartado se recogen las tareas recomendadas para la fase de operación o mantenimiento del producto.

4. FASE PREVIA A LA INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

9. El equipo debe ser examinado para comprobar que no ha sido manipulado durante su entrega confirmando los siguientes pasos:

   a) Antes de abrir el paquete donde fue entregado el producto, se debe comprobar que el paquete contenga la serigrafía y logo de *Cisco Systems*. Si no es así, se recomienda contactar con el proveedor del equipo (*Cisco Systems* o un distribuidor autorizado).

   b) Es necesario comprobar que el paquete no ha sido abierto y sellado de nuevo, mediante inspección de la cinta que lo cierra. Si el paquete parece haber sido abierto y después sellado de nuevo, es recomendable contactar con el proveedor del equipo (*Cisco Systems* o un distribuidor autorizado).

   c) Se debe verificar que el paquete contiene la impresión resistente a manipulaciones de Cisco en la cara externa de la caja de cartón. Si no es así, se deberá contactar con el proveedor del equipo (*Cisco Systems* o un distribuidor autorizado). Esta impresión contiene el número de producto de Cisco, su número de serie e información adicional sobre el contenido de la caja.

   d) Es importante chequear el número de serie del producto especificado en la documentación del pedido. El número de serie que figura en la etiqueta blanca de la caja se debe corresponder con el número de serie del dispositivo. Por tanto, es necesario verificar que este número concuerda con el número de serie en la factura enviada por correo. Si no es así, se debe contactar con el proveedor del equipo (*Cisco Systems* o un distribuidor autorizado).

   e) En la recepción de la unidad, es necesario comprobar que el pedido fue enviado por el proveedor esperado (*Cisco Systems* o un distribuidor autorizado). Este proceso puede llevarse a cabo verificando el código de envío/paquete junto con la empresa de transporte. También es recomendable comprobar que los números de serie de los productos enviados concuerdan con los números de serie de los productos recibidos. Esta verificación debe ser llevada a cabo por algún mecanismo externo que no pertenezca al proceso de envío. Por ejemplo, teléfono, fax o un servicio online de rastreo de paquetes.

10. Una vez que el paquete ha sido abierto, es recomendable inspeccionar el dispositivo. Aquí es necesario comprobar que el número de serie mostrado en él concuerda con el número de serie que aparece en la documentación del envío y la factura. Si no es así, se debe contactar con el proveedor del equipo (*Cisco Systems* o un distribuidor autorizado).

4.2 ENTREGA SEGURA DEL *SOFTWARE*

11. El equipo se entrega con *software* instalado, pero puede ocurrir que no sea la versión recomendada. En este caso, el *software* deberá actualizarse.
12. El software está disponible para su descarga en el "*Software Center*" de Cisco: https://software.cisco.com/download/home . Se ha de referir a [1] en el apartado "*Download the Cisco Content Security Virtual Appliance Image*" para la descarga de la imagen.
13. El *software* para descargar contiene un *checksum* para su comprobación. Por lo que previo a la descarga se debe copiar el *checksum*.
14. En la ilustración 1, se puede ver un ejemplo de la página de descarga del *software* para equipos virtuales. En ella se puede ver como el último campo del menú emergente contiene un campo denominado SHA512 Checksum.

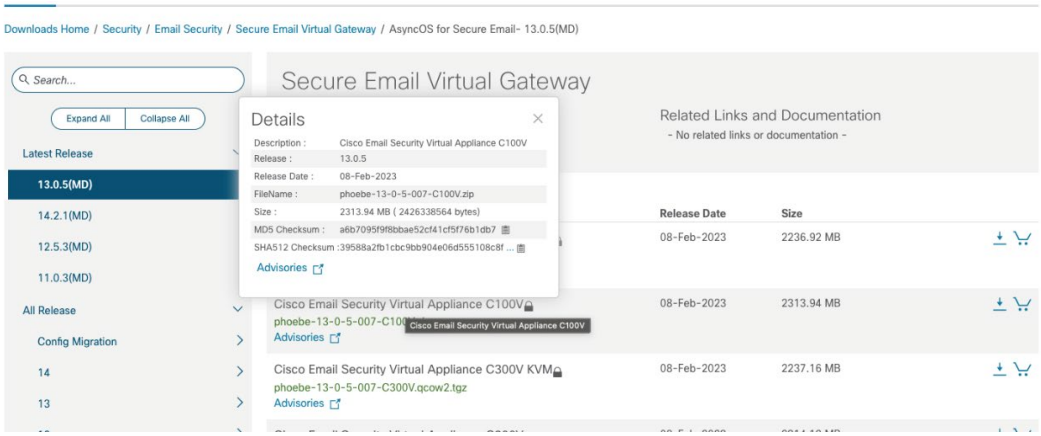

Ilustración 1 – Captura de pantalla de la página de descarga del software

15. Una vez completada la descarga, **el administrador debe chequear los *upgrade_logs*** que se han generado por el ESA dado que contienen los archivos descargados y **permiten comparar el hash publicado** (ver Ilustración 1) con el hash que aparece en dichos logs. Si ambos coinciden se puede proseguir con la instalación. Si no es así, contacte con el proveedor del equipo (Cisco o un distribuidor autorizado).

4.3 ENTORNO DE INSTALACIÓN SEGURO

16. El equipo debe instalarse en una ubicación físicamente segura donde **solo se permita acceso físico al personal autorizado.**

4.4 REGISTRO Y LICENCIAS

17. El sistema de licencias se denomina *Smart Software Licensing*.
18. Cada cliente tiene una cuenta propia en *Smart Licensing* en el portal de Cisco: *https://software.cisco.com/*
19. Haciendo uso de esta cuenta, se dispone del *Cisco Smart Software Manager (CSSM).* La información referente al CSSM se puede encontrar en la guía [2].

20. En el CSSM se pueden ver las licencias adquiridas. Cuando el CSMM recibe las informaciones sobre el uso de las licencias modificando el contador de las licencias usadas.

21. El procedimiento de registro a seguir se encuentra en *"System Administration > Email Security Appliance Licensing" y "System Administration > Cisco Email Security Virtual Appliance Virtual Email Gateway License"* de la guía [3].

4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN

22. El equipo requiere los siguientes componentes en el entorno operacional:

    a) Servidor de monitorización.

    b) Este punto hace referencia a un servidor que permita una conexión SCP en un servidor de *syslog* remoto.

    c) Puesto de gestión por consola.

    d) Este puesto hace referencia a cualquier estación de trabajo que permita una conexión por consola al equipo.

    e) Puesto de gestión con cliente SSH.

    f) Este puesto hace referencia a cualquier estación de trabajo con un cliente SSHv2 instalado, que se emplea para la configuración y administración del equipo.

5. FASE DE INSTALACIÓN

23. Para la instalación del equipo siga la guía Cisco Hardware *Installation Guide* [4] o [5] dependiendo del modelo.
24. En el caso de tratarse de un equipo virtual, para la instalación del equipo siga la guía *Cisco Content Security Virtual Appliance Installation Guide* [1] en el apartado *"Set Up the Virtual Appliance".*

6. FASE DE CONFIGURACIÓN

25. El equipo necesita de una configuración básica mediante cable de consola conectado directamente previo a ser conectado a una red.
26. Un administrador autorizado debe hacer uso del *System Wizard Setup* para asegurar una configuración inicial completa. El acceso al *System Wizard Setup* se realiza mediante GUI y viene descrito en el apartado *"Setup and Installation > Using the System Setup Wizard"* de la guía [3].
27. Durante el proceso de configuración inicial realizado con el *System Setup Wizard* se debe cambiar la contraseña usada por defecto por el equipo siguiendo el procedimiento. Esta acción se realiza en el segundo paso de configuración básica haciendo uso del *System Setup Wizard* vía GUI. Se puede seguir el procedimiento en "*Setup and Installation > Defining Basic Configuration using the Web-based System Setup Wizard*" de la guía [3].
28. Además, la contraseña seleccionada debe cumplir los requerimientos de complejidad para ser catalogada como segura. Esta contraseña debe ser una contraseña con seis o más caracteres y debe almacenarse en una localización segura. Se puede consular esta información en el procedimiento en *"Setup and Installation > Defining Basic Configuration using the Web-based System Setup Wizard > Step 2: System > Setting the Passphrase"* de la guía [3].
29. Los cambios mencionados anteriormente, se deben realizar siguiendo el procedimiento del apartado "*Setup and Installation"* de la guía [3].

6.1 MODO DE OPERACIÓN SEGURO

30. **El producto debe utilizarse en el denominado modo de operación seguro. Para ello, el equipo debe ejecutarse en modo de operación FIPS.**
31. El comando *fipsconfig* configura automáticamente los algoritmos y los tamaños de llave necesarios para poder realizar una ejecución de ESA en modo FIPS. Además, todas las contraseñas almacenadas y las llaves se encriptarán.
32. El procedimiento de uso de este comando se debe seguir mediante la guía [3] en el apartado "*FIPS Management*".
33. Durante el proceso mencionado anteriormente es necesario que el administrador autorizado seleccione "*y*" a la pregunta: "*Do you want to enable encryption to sensitive data in configuration file when FIPS mode is enable?".* Esto permite que todas las contraseñas y claves se encripten. El procedimiento se encuentra en la guía [3] en el apartado "*FIPS Management > Switching the Appliance fo FIPS Mode".*

6.2 ADMINISTRACIÓN DEL PRODUCTO

6.2.1 DESHABILITACIÓN TELNET

34. Por defecto telnet viene deshabilitado, pero para realizar dicha comprobación en [3] en el apartado "*Set Up and Installation*" se encuentran el comando "*interfaceconfig*"**. Se debe seleccionar cada una de las interfaces y comprobar que telnet está deshabilitado.**

6.2.2 CONFIGURACIÓN SSHV2

35. SSHv2 se encuentra habilitado por defecto. Para poder acceder de forma remota, el administrador debe seleccionar un cliente SSH que soporte SSHv2 haciendo uso de alguno de los siguientes mecanismos de intercambio de claves: **ecdh-sha2-nistp256, ecdh-sha2- nistp384 y ecdh-sha2-nistp521**.
36. Para la configuración SSHv2 se debe seguir la guía [6] en el apartado *"The Commands: Reference Examples > sshconfig".*
37. El administrador autorizado para poder acceder por CLI vía SSH se puede autenticar haciendo uso de una llave pública criptográfica. Para ello, en el procedimiento anterior debe hacer uso del comando "*userkey"* para insertar la llave pública. En caso de no realizar esta configuración, la autenticación será mediante usuario y contraseña.
38. **Para la configuración SSH, se debe usar:**
    - Algoritmos de cifrado: aes256-ctr y aes128-ctr.
    - MAC: hmac-sha1
    - Autenticación de algoritmos de llave pública:
        - cliente SSH: ecdh-sha2-nistp256, ecdh-sha2-nistp384 and ecdh-sha2-nistp512
        - servidor SSH: rsa-sha2-256 and, rsa-sha2-512
        - Algoritmos KEX: ecdh-sha2-nistp256 y ecdh-sha2-nistp521
        - Mínimo tamaño de la llave del servidor: 3072
39. Durante el proceso de configuración, aparecerá la pregunta "*Do you want to enable host key checking?*". **Se debe responder con "*y*" para habilitar el chequeo de la llave.**
40. Para asegurar una conexión remota segura, el administrador autorizado debe mantener una base de datos local que asocie la llave pública con el equipo remoto a la que pertenece.
41. Además, se debe solicitar un refresco de la llave pasada una hora o/y 1GB de datos.

6.2.3 CONFIGURACIÓN TLS

42. El protocolo **TLS** para la administración del producto mediante GUI **no debe** utilizarse y debe quedar deshabilitado, dado que no cumple con los requisitos para el establecimiento de claves (Diffie-Hellman 14 y RSA de longitud 2048).

6.2.4 AUTOCHEQUEOS

43. El propio equipo contiene *tests* criptográficos propios para chequear que las siguientes funcionalidades están correctas:
    - Prueba de respuesta conocida AES
    - Prueba de respuesta conocida de firma RSA
    - Prueba de respuesta conocida HMAC
    - Prueba de respuesta conocida SHA-1/256/512
    - Prueba de integridad del software
44. Durante el proceso de arranque del sistema (encendido o reinicio), todos los *test* POST comprobarán que los algoritmos criptográficos funcionan correctamente.
45. En caso de que algún error ocurra durante este proceso se podrá ver en los logs del sistema el siguiente mensaje:

    _FIPS-2-SELF_TEST_WAS_FAILURE: "WAS crypto FIPS self test failed at %s.
46. En caso de que esto ocurra, contactad con el soporte de Cisco vía http://www.cisco.com/techsupport or 1 800 553-2447
47. Estas comprobaciones son suficientes para verificar que las operaciones criptográficas se están realizando de una manera correcta.

6.2.4.1 PUESTA A CERO DE LAS LLAVES

48. Aunque la puesta a cero de las llaves se gestiona desde el módulo criptográfico, existe un comando *wipe* para confirmar que esto ocurre. Se debe seguir la guía [6] en el apartado "*The Commands: Reference Examples > wipedata*" para lanzar el comando.

6.2.5 SINCRONIZACIÓN

49. **El producto debe estar configurado de acuerdo a una fuente de tiempo fiable**. La sincronización del reloj es tarea del administrador autorizado.
50. Para realizar la configuración el procedimiento viene descrito en el apartado *"System Administration > System Time"* de la guía [3].

6.2.6 CONFIGURACIÓN DE PUERTOS Y SERVICIOS

51. En la siguiente tabla se puede encontrar la lista de servicios y protocolos permitidos en ESA como cliente (siendo el iniciante) o como servidor (como terminador) ejecutándose a nivel de procesos *system-level*.

Servicio o protocolo	Cliente (iniciante)	Permitido	Servidor (terminador)	Permitido	Uso permitido con configuración certificada
DHCP	Sí	Sí	Sí	Sí	Sin restricción
DNS	Sí	Sí	No	n/a	Sin restricción
FTP	Sí	No	No	n/a	Usar SCP o HTTPS
HTTP	Sí	No	Sí	No	Para funciones HTTP de "copia", pero se recomienda el uso de HTTPS
HTTPS	Sí	Sí	Sí	Sí	Sin restricción
ICMP	Sí	Sí	Sí	Sí	Sin restricción
IMAP4S	Sí	Sobre TLS	No	n/a	Sin restricción
LDAP	Sí	No	No	n/a	Si se usa para autenticación, configurar TLS
LDAP-over-SSL	Sí	No	No	n/a	Si se usa para autenticación, configurar TLS
NTP	Sí	Sí, pero no se ha testeado la configuración	No	n/a	Cualquier configuración. Se recomienda autenticación key-based .
RADIUS	Sí	No	No	n/a	Si se usa para autenticación, usar TLS para securizar.
SCP	Sí	Sí	Sí	Sí	Configurar SSH
SMTP	Sí	No	No	n/a	
SMTPS	Sí	No	No	n/a	

Servicio o protocolo	Cliente (iniciante)	Permitido	Servidor (terminador)	Permitido	Uso permitido con configuración certificada
SNMP	Sí (traps)	No se ha testeado la configuración	Sí	No	Sólo traps y recomendado sobre túnel en TLS
SSH	Sí	Sí	Sí	Sí	
SSL (no TLS)	Sí	No	Sí	No	Usar TLS
Telnet	Sí	No	Sí	No	Usar SSH
TLS	Sí	No se ha testeado la configuración	Sí	No	
TFTP	Sí	No	No	n/a	Se recomienda usar SCP o HTTPS.

Tabla 1 - Lista de servicios y protocolos permitidos

6.3 GESTIÓN SEGURA

6.3.1 ADMINISTRADORES AUTORIZADOS

52. Para realizar la configuración administradores autorizados se ha descrito en el apartado el procedimiento "*Distributing Administrative Tasks > User Roles*" de la guía [3]. En ella se encuentran descritas las descripciones de cada uno de los roles.

6.3.2 COMPLEJIDAD DE LA CONTRASEÑA

53. **La contraseña que se genere para cada uno de los roles debe tener de un mínimo de 15 caracteres**, haciendo uso de mayúsculas, minúsculas, números y al menos un carácter especial.

54. Los requerimientos se pueden encontrar *en "Distributing Administrative Tasks > PassPhrase > Configuring Restrictive User Account and Passphrase Settings"* de la guía [3].

6.3.3 GENERACIÓN DE UN *BANNER*

55. El administrador autorizado debe **crear un *banner* para mostrar a los usuarios antes de acceder**. Se pueden encontrar *"Distributing Administrative Tasks > Dislpaying Messages to Administrative Users"* de la guía [3].

6.3.4 CIERRE Y TERMINACIÓN DE SESIÓN

6.3.4.1 BLOQUEO DE USUARIO

56. **Las cuentas de usuario deben bloquearse tras un número de autenticaciones fallidas concretas. El número por defecto es de 5 intentos, pero deberá fijarse a 3.** Para realizar el cambio, el procedimiento se encuentra en *"Distributing Administrative Tasks > PassPhrase > Locking and Unlocking a User Account "* de la guía [3].

6.3.5 CIERRE DE SESIÓN INACTIVA

57. Las sesiones deben tener una configuración de inactividad para que estas se cierren al cabo de un lapso de tiempo determinado. **El tiempo por defecto es de 30 minutos, pero deberá fijarse a 10 minutos.** Para realizar el cambio, el procedimiento se encuentra en "*Distributing Administrative Tasks > Configuring Access to the Email Security Appliance > Configuring Session Timeouts"* de la guía [3].

6.3.6 CIERRE DE SESIÓN

58. El usuario debe realizar el cierre de sesión mediante el "*logout*" si está en GUI y mediante un "*exit*" si se encuentra en CLI.

6.4 AUDITORÍA

6.4.1 CONFIGURACIÓN DE LOGGING

59. **Los ficheros de log generados se deben guardar realizando una copia de seguridad a un servidor SCP o a un servidor de *syslogs* remoto**. Para realizar la configuración de los logs viene descrito en el apartado "*Using Message Filters to Enforce Email Policies > Configuring Filter Log Subscriptions > logconfig"* de la guía [3].
60. El administrador autorizado debe asegurarse de que al menos los siguientes logs están incluidos:
    - *Status Logs*
    - *System Logs*
    - *CLI Audit Logs*
    - *HTTP Logs*
    - *Authentication Logs*
    - *Configuration History Logs*

6.5 *BACKUP*

61. **Se deben realizar copias de la configuración del producto**. El procedimiento para la realización de dichsa copias viene descrito en el apartado "*System administration managing configuration files > saving and exporting the current configuration* file" de la guía [3].

7. FASE DE OPERACIÓN

62. Durante la fase de operación del equipo, el administrador debe llevar a cabo las siguientes tareas:

    - Mantenimiento del **control de acceso** al equipo.
    - **Comprobaciones periódicas del *hardware* y *software*** para asegurar que no se ha introducido hardware o software no autorizado.
    - **Seguimiento de las alertas de seguridad de Cisco** (*Security Advisories*) y, si es necesario, aplicar un *patch*.
    - **Mantenimiento de los registros de auditoría**. Estos registros estarán protegidos contra borrados y modificaciones no autorizados, y solamente el personal de seguridad autorizado podrá acceder a ellos.

8. REFERENCIAS

[1] «Cisco Secure Email and Web Virtual Appliance Installation Guide,» [En línea]. Available: https://www.cisco.com/c/dam/en/us/td/docs/security/content_security/virtual_appliances/Cisco_Content_Security_Virtual_Appliance_Install_Guide.pdf.

[2] «Smart Licensing Deployment Guide,» [En línea]. Available: https://www.cisco.com/c/en/us/td/docs/wireless/technology/mesh/8-2/b_Smart_Licensing_Deployment_Guide.html.

[3] «User Guide for AsyncOS 13.0 for Cisco Email Security Appliances - GD (General Deployment),» [En línea]. Available: https://www.cisco.com/c/en/us/td/docs/security/esa/esa13-0/user_guide/b_ESA_Admin_Guide_13-0.html.

[4] «Cisco 170 Series Hardware Installation Guide,» [En línea]. Available: https://www.cisco.com/c/dam/en/us/td/docs/security/esa/hw/170Series_HW_Install.pdf.

[5] «Cisco Email Security Appliance C195, C395, C695, and C695F Getting Started Guide,» [En línea]. Available: https://www.cisco.com/c/dam/en/us/td/docs/security/content_security/hardware/x95_series/Cx95_GSG.pdf.

[6] «CLI Reference Guide for AsyncOS 13.0 for Cisco Email Security Appliances - GD(General Deployment),» [En línea]. Available: https://www.cisco.com/c/en/us/td/docs/security/esa/esa13-0/cli_reference_guide/b_CLI_Reference_Guide_13_0.html.

9. ABREVIATURAS

AES	*Advanced Encryption Standard*
CLI	*Command Line Interface*
CSR	*Certificate Signing Request*
CSSM	*Cisco Smart Software Manager*
DHCP	*Dynamic Host Configuration Protocol*
DNS	*Domain Name Service*
ESA	*Email Security Appliance*
FIPS	*Federal Information Processing Standard*
FTP	*File Transfer Protocol*
GUI	*Graphical User Interface*
HTTP	*Hypertext Trasfer Protocol*
HTTPS	*Hypertext Trasfer Protocol Secure*
ICMP	*Internet Control Message Protocol*
IMAP4S	*Internet Message Protocol Secure version 4*
IP	*Internet Protocol*
LDAP	*Lightweight Directory Access Protocol*
NTP	*Network Time Protocol*
POST	*Power On Self Test*
RADIUS	*Remote Authenticatio Dial in User Service*
RSA	*Rivest, Shamir and Adleman*
SCP	*Secure Copy Protocol*
SMTP	*Simple Mail Transfer Protocol*
SMTPS	*Simple Mail Transfer Protocol over TLS*
SNMP	*Simple Network Management Protocol*
SSH	*Secure Shell*
SSL	*Secure Socket Layer*
TCP	*Transport Control Protocol*
TCP/IP	*Transport Control Protocol/ Internet Protocol*
TLS	*Transport Layer Security*
TFTP	*Trivial File Transfer Protocol*
UCS	*Unified Computing System*

PUBLICACIONES DE DEFENSA

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