Guía de Seguridad de las TIC
CCN-STIC 140

Taxonomía de productos STIC -
Anexo A.1 M: Dispositivos de Control de Acceso a Red

Febrero de 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
2023.03.01 11:10:43 +01'00'

Pº de la Castellana 109, 28046 Madrid
Centro Criptológico Nacional, 2023

NIPO: 083-23-071-5.
Fecha de Edición: febrero de 2023

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 Y OBJETO

1. El presente documento describe los Requisitos Fundamentales de Seguridad (RFS) exigidos a un producto de la familia Control de acceso a red para ser incluido en el apartado de Productos Cualificados del Catálogo de Productos y Servicios STIC (CPSTIC), publicado por el CCN.
2. Estos requisitos representan las capacidades de seguridad mínimas que cualquier producto dentro de esta familia debe implementar para un determinado caso de uso, independientemente del fabricante y la tecnología, con el fin de proporcionar un nivel mínimo de confianza y considerarse objetivamente cualificado desde el punto de vista de la seguridad para ser empleado en los sistemas de información del sector público a los que sea de aplicación el **Esquema Nacional de Seguridad (ENS) Categoría MEDIA**. Estos requisitos aportan mecanismos enfocados a reducir vulnerabilidades y contrarrestar amenazas, fundamentalmente de carácter técnico, aunque también pueden ser de naturaleza física o procedimental.
3. Además, la aplicación de estos criterios permitirá:
    - Que se establezcan unas características mínimas de seguridad que sirvan de referencia a los **fabricantes** a la hora de desarrollar nuevos productos STIC.
    - Que los **organismos responsables de la adquisición** dispongan de evaluaciones completas, consistentes y técnicamente adecuadas, que permitan contrastar la eficacia y proporcionar información no sesgada acerca de los servicios de seguridad que ofrecen dichos productos.
    - Que los **usuarios finales** posean una guía que facilite el despliegue y garantice el uso apropiado del producto desde el punto de vista de la seguridad.
4. Por lo tanto, los productos catalogados dentro de la familia **Control de acceso a red** conforme a la taxonomía definida por el Centro Criptológico Nacional, serán susceptibles de ser evaluados usando como referencia este documento.
5. En el caso de productos multipropósito, queda fuera del alcance de este documento cualquier otra funcionalidad de seguridad proporcionada, más allá de la especificada para esta familia en la sección siguiente. Dichos productos podrían optar a ser incluidos de manera adicional como Productos Cualificados en otra(s) familia(s) del CPSTIC si cumpliesen los RFS correspondientes.

2. DESCRIPCIÓN DE LA FAMILIA DE PRODUCTOS

2.1 FUNCIONALIDAD

6. El objetivo del control de acceso a red es asegurar que todos los dispositivos que se conectan a las redes corporativas de una organización cumplen con las políticas de seguridad establecidas, incluyendo las de pre-admisión, el cumplimiento de las políticas de seguridad implementadas por el usuario final y los controles post-admisión sobre los recursos de red a los que pueden acceder los usuarios y dispositivos, de cara a reducir el riesgo de entrada de virus, fuga de información sensible, etc.
7. En este contexto, las funciones básicas de seguridad que proporciona esta familia de productos son las siguientes:
    - Impedir aquellos accesos a la red a entidades que no estén autorizadas o no implementen las políticas de seguridad exigidas.
    - Administrar el acceso a los recursos de la red, en base a permisos o roles definidos conforme a la política de seguridad establecida.

2.2 CASOS DE USO

8. Para esta familia de productos se contempla un solo caso de uso que admitirá múltiples configuraciones, ya que serán las políticas de seguridad con las que se configure el dispositivo las que puedan variar e incluir más o menos restricciones.

2.2.1. CASO DE USO 1– GESTIÓN DEL CONTROL DE ACCESO A LA RED

9. El dispositivo de control de acceso se encuentra ubicado, dentro de la arquitectura de red, en una capa anterior a los servicios o redes de la organización para los cuales se requiere un control de acceso.
10. Las fases en las que se divide el proceso de control de acceso a red son:
    - Autenticación de la entidad en función de las políticas establecidas por la organización. Esta tarea podría ser realizada por el propio dispositivo o tratarse de un servicio externo.
    - Si el resultado del proceso de autenticación es positivo, el producto realiza una verificación de que esa entidad cumple los requisitos de seguridad establecidos para la protección de los servicios de la red.
    - Por último, en caso de que se hayan verificado con éxito los requisitos indicados anteriormente, se permitiría el acceso a los recursos de la red en función de los privilegios asignados al perfil de usuario, que residen en un servicio de directorio.
11. Por lo tanto, los datos que maneja el sistema de control de accesos a red son:
    - Los archivos de configuración en base a las políticas de seguridad definidas.

- Los objetos de archivos con los que opera, que podrían ser de granularidad diferente a los utilizados por el sistema operativo. Así, mientras el sistema operativo se enfoca a trabajar con objetos fundamentales como ficheros o interfaces de comunicación entre procesos, este tipo de productos tiene la capacidad de trabajar con abstracciones de más alto nivel que pueden ser implementadas como una combinación de objetos fundamentales.
- Los eventos de auditoría registrados.

12. La Figura 1 muestra un esquema de la arquitectura del sistema, que podrá ser implementada por un solo producto con múltiples capacidades o por un conjunto de productos.

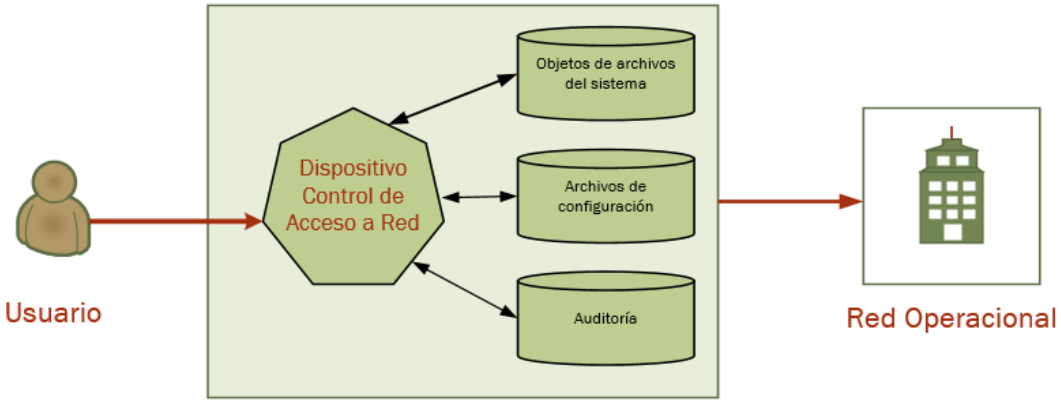

Figura 1 Ejemplo de caso de uso de Control de acceso a red

2.3 HIPÓTESIS SOBRE EL ENTORNO DE EJECUCIÓN

13. Por lo general estos dispositivos se utilizan en grandes o medianas empresas y en redes del sector público, junto con otras medidas de seguridad complementarias, formando parte de una arquitectura de defensa en profundidad que busca asegurar el entorno de comunicación.
14. Para la utilización en condiciones óptimas de seguridad de estos productos, es necesaria su integración en un entorno operacional que cumpla las siguientes condiciones:

- **Protección física**. El producto debe estar protegido físicamente por su entorno operacional y no sujeto a ataques físicos que puedan comprometer su seguridad o interferir en su correcta operación. En caso de productos software, esta hipótesis aplica a la plataforma física sobre la que se ejecuta el producto.
- **Administración confiable**. Los administradores son miembros de plena confianza y velan por los mejores intereses en materia de seguridad de la organización. Dichas personas deben estar debidamente capacitadas y carecer de cualquier intención maliciosa o conflicto de intereses al administrar el producto.

- **Actualizaciones periódicas**. El firmware/software del producto es actualizado conforme aparezcan actualizaciones que corrijan vulnerabilidades conocidas.
- **Funcionalidad limitada**. El producto solo debe proporcionar la funcionalidad de *control de acceso a red* como función principal y no debe proporcionar ninguna otra funcionalidad o servicio.
- **Protección de las credenciales**. Todas las credenciales, en especial la del administrador, deberán estar correctamente protegidas por parte de la organización que utilice el producto.

2.4 DELIMITACIÓN DEL ALCANCE DEL DISPOSITIVO

15. Este tipo de productos se presentan en formato de equipo dedicado (*Appliance*: *hardware* provisto de *firmware*[1] dedicado) con las funcionalidades estrictamente necesarias para cumplir su finalidad y acotadas al servicio específico que presten.
16. Adicionalmente, suele ser habitual que en las máquinas y dispositivos que protegen se incluya un software instalable (agente) que ejerce un papel de control de las entidades conectadas en la red.
17. Por último, para realizar las funciones de control y administración del dispositivo es normal incluir con el producto un software específico para instalarlo en un equipo informático estándar.
18. En caso de ofrecer funcionalidades adicionales a las definidas en la sección 2.1, éstas quedan fuera del alcance analizado, y deberán ser evaluadas conforme a los RFS específicos aplicables a tales funcionalidades complementarias.

2.5 CERTIFICACIÓN LINCE

19. Para que un producto de esta familia pueda ser incluido en el CPSTIC bajo la categorización de ENS Medio, deberá disponer de una Certificación Nacional Esencial de Seguridad (LINCE)[2] que incluya los RFS reflejados en el apartado 4, que deberán ser evaluados considerando el problema de seguridad definido en el presente documento.

[1] *Firmware* funciona como el nexo de unión entre las instrucciones (*software*) que llegan al dispositivo desde el exterior y las diversas partes electrónicas (*hardware*).
[2] Toda la información relativa a esta metodología se encuentra disponible en la web del Organismo de Certificación (https://oc.ccn.cni.es)

3. ANÁLISIS DE AMENAZAS

3.1 ACTIVOS SENSIBLES A PROTEGER

20. Los recursos que deben protegerse mediante el uso de estos productos incluyen:

- **AC.Administración.** Interfaces de gestión del producto y la información transmitida a través de ellas, en ambos sentidos, que debe ser protegida en Confidencialidad, Trazabilidad, Autenticidad e Integridad.
- **AC.PSS.** Datos de configuración, registros auditoría y [***asignación****: listado de datos definidos por el fabricante*] que deben ser protegidos en Integridad.
- **AC.PSC.** [**selección**: credenciales; claves; [**asignación**: *listado de datos definidos por el fabricante*] que deben ser protegidos en Confidencialidad e Integridad.
- **AC.Actualizaciones.** Actualizaciones del producto susceptibles de afectar a su configuración y funcionalidad, que deben ser protegidos en Integridad y Autenticidad.
- **AC.Comunicaciones.** Comunicaciones del producto, establecidas entre sus propios componentes y con [**asignación**: *listado de entidades autorizadas*] que deben ser protegidas en Confidencialidad, Integridad y Autenticidad.

3.2 AMENAZAS

21. Las principales amenazas a las que el uso de esta familia de productos pretende hacer frente serían:

- **A.NOAUT Acceso no autorizado de administrador:** Un atacante puede obtener un acceso de administración no autorizado haciéndose pasar por un administrador ante el producto, haciéndose pasar por el producto ante un administrador, reproduciendo una sesión de administración, o realizando ataques del hombre en medio.
- **A.CRYPTO Mecanismos criptográficos débiles:** Utilización en el producto de mecanismos criptográficos o longitudes de clave débiles que permitan a un atacante comprometerlo, fundamentalmente mediante ataques de fuerza bruta.
- **A.COM Protocolos de comunicación no autorizados:** Utilización de protocolos no autorizados que permiten a un atacante comprometer la integridad y confidencialidad de las comunicaciones críticas del producto.
- **A.ACT Actualización maliciosa:** un atacante puede realizar una actualización maliciosa que comprometa las funcionalidades del producto.

- **A.AUD Actividades no detectadas:** Un atacante puede intentar acceder, cambiar o modificar las funcionalidades de seguridad del producto sin el conocimiento del administrador.
- **A.PSC Compromiso de parámetros de seguridad críticos:** un atacante puede comprometer los parámetros de seguridad críticos y acceder de forma continuada al producto y a sus datos críticos.
- **A.FUN Fallo de las funcionalidades de seguridad:** Un atacante externo puede aprovechar fallos en las funcionalidades de seguridad declaradas del producto y podría acceder, cambiar o modificar información, funcionalidades de seguridad o tráfico de red en el producto.
- **A.NOAUTUSR Acceso no autorizado de usuario:** Un atacante puede obtener un acceso no autorizado haciéndose pasar por un usuario ante el producto, haciéndose pasar por el producto ante un usuario, reproduciendo una sesión de usuario, o realizando ataques del hombre en medio.
- **A.CRE Compromiso de credenciales:** Un atacante puede aprovecharse del uso de credenciales débiles o desprotegidas, para ganar acceso privilegiado al producto.
- **A.RED Ataque a la red:** Un atacante consigue acceder a la red pudiendo realizar mapeos de las máquinas que residen en ella y obtener datos de dirección IP, servicios o cualquier otra información que le permita lanzar ataques a dichas máquinas y servicios.

3.3 TRAZABILIDAD AMENAZAS/REQUISITOS DE SEGURIDAD

22. En la siguiente tabla se trazan que Requisitos Fundamentales de Seguridad definidos en el apartado 4 cubren las amenazas definidas:

	A.NOAUT	A.CRYPTO	A.COM	A.ACT	A.AUD	A.PSC	A.FUN	A.NOAUTUSR	A.CRE	A.RED
ADM.1	X									
ADM2	X									
ADM.3	X									
IAU.1	X							X		
IAU.2									X	
IAU.3									X	
IAU.4	X									
COM.1		X	X							
COM.2			X							
COM.3			X							
COM.4		X	X							
ACT.1				X						
ACT.2				X						
ACT.3				X						
AUD.1					X					
AUD.2					X					
AUD.3					X					
AUD.4					X					
AUD.5					X					
PSC.1						X				
PRO.1										
CIF.1		X	X							
NAC.1										X
NAC.2										X

4. REQUISITOS DE SEGURIDAD

23. A continuación, se recogen los requisitos fundamentales de seguridad que deben cumplir los productos que quieran optar a la inclusión en el CPSTIC en esta familia.

24. La convención utilizada en las descripciones de los RFS es la siguiente:

    - Selección**:** se deberá seleccionar al menos una opción de las indicadas en el RFS y se incluirá en la declaración de seguridad. Ejemplo:

      RFS: Administración del producto [**selección***: local; remota*]

      DS: Administración del producto local y remota

    - Asignación: se deberá especificar el listado de opciones que sean de aplicación al TOE (podría no haber ninguna). Ejemplo:

      RFS: El TOE deberá identificar y autenticar a cada usuario administrador y [**asignación:** otros usuarios del producto] antes de otorgar acceso.

      DS: El TOE deberá identificar y autenticar a cada usuario administrador, auditor y usuario avanzado antes de otorgar acceso.

4.1 ADMINISTRACIÓN CONFIABLE

25. Estas funcionalidades podrán ser cubiertas por el producto o por su entorno operacional.

26. **ADM.1** El TOE debe definir, al menos, el rol de administrador y ser capaz de asociar usuarios a roles.

27. **ADM.2** El TOE debe ser capaz de realizar la gestión de las siguientes funcionalidades:

    - Administración del producto [**selección**: *local; remota*].
    - Configuración del tiempo de terminación de sesión o bloqueo al detectar inactividad.
    - [**asignación**: otras funcionalidades administrables del producto].

28. **ADM.3** El TOE deberá asegurar que solamente un usuario con permisos de administrador será capaz de realizar las funciones descritas en **ADM.2**.

> Nota de aplicación: en el caso de que existan distintos tipos de administrador, cada uno de ellos con distintos permisos, deberá probarse que únicamente pueden realizar aquellas funcionalidades para las que tengan permiso.

4.2 IDENTIFICACIÓN Y AUTENTICACIÓN

29. Estas funcionalidades podrán ser cubiertas por el producto o por su entorno operacional.

30. **IAU.1** El TOE deberá identificar y autenticar a cada usuario administrador y [**asignación**: *otros usuarios del producto*] antes de otorgar acceso, salvo para las siguientes funcionalidades [**asignación**: *listado funcionalidades*].

31. **IAU.2** El TOE deberá implementar mecanismos que impidan ataques de autenticación por fuerza bruta.

32. **IAU.3** El TOE debe disponer de la capacidad de gestión de las contraseñas:

    - La contraseña debe poder configurarse con una longitud mínima o igual a 12 caracteres.
    - La contraseña debe ser capaz de componerse por letras minúsculas, letras mayúsculas, números y caracteres especiales [“!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “].

> Nota de aplicación: este requisito podría ser modificado en el caso de que el TOE implemente otros mecanismos de autenticación.

33. **IAU.4** El TOE debe [**selección***: bloquear; cerrar*] la sesión de un usuario después de [***asignación****: tiempo de inactividad*] de inactividad.

4.3 CANALES SEGUROS

34. Estas funcionalidades podrán ser cubiertas por el producto o por su entorno operacional.

35. **COM.1** Protección de la información en tránsito. El TOE deberá establecer canales seguros cuando intercambie información sensible con entidades autorizadas: [**selección***: servidor de auditoría;* [***asignación****: otras entidades*]] o entre distintas partes del producto, usando [**selección***: IPSec; SSHv2 o superior; TLS 1.2 o superior; DTLS; HTTPS/TLS 1.2 o superior*] con los siguientes mecanismos criptográficos [***asignación****: listado de mecanismos o suites autorizadas de acuerdo a lo establecido en la guía CCN-STIC-807 para cada protocolo*].

36. **COM.2** El TOE debe permitir que los canales de comunicación definidos en **COM.1** sean iniciados por él mismo o por las entidades autorizadas.

37. **COM.3** El TOE hará uso de certificados digitales para la autenticación cuando utilice cualquiera de los protocolos definidos en **COM.1**.

38. **COM.4** Protección de la información del canal de administración. El TOE deberá establecer canales seguros cuando intercambie información con el administrador remoto, usando [**selección**: *IPsec; SSHv2 o superior; TLS 1.2 o superior; DTLS; HTTPS/TLS 1.2 o superior*] con los siguientes mecanismos criptográficos [***asignación****:*

listado de mecanismos o suites autorizadas de acuerdo a lo establecido en la guía CCN-STIC-807 para cada protocolo].

4.4 CRIPTOGRAFÍA

39. Estas funcionalidades podrán ser cubiertas por el producto o por su entorno operacional.
40. **CIF.1** El TOE permitirá exclusivamente el empleo de mecanismos criptográficos: [***asignación**: listado de mecanismos*] autorizados de acuerdo a lo establecido en la guía CCN-STIC-807. La fortaleza de clave empleada será la indicada en esa guía para Categoría MEDIA del ENS, y de acuerdo al nivel de amenaza establecido.

4.5 INSTALACIÓN Y ACTUALIZACIÓN CONFIABLES

41. **ACT.1** El TOE ofrecerá la posibilidad de consultar la versión actual del firmware/software y podrá [**selección**: actualizarse automáticamente; iniciar actualizaciones manualmente] y [**selección**: comprobar si existen nuevas actualizaciones disponibles; ningún otro].
42. **ACT.2** El TOE deberá utilizar [**selección***: hashes publicados; firma digital*] que estén autorizados en la guía CCN-STIC-807 para autenticar las actualizaciones *firmware/software* antes de instalarlas.
43. **ACT.3** La actualización del *firmware/software* se permitirá únicamente a usuarios con rol de administrador.

4.6 AUDITORÍA

44. Estas funcionalidades podrán ser cubiertas por el producto o por su entorno operacional.
45. **AUD.1** El producto debe generar registros de auditoría cuando se produzca alguno de los siguientes eventos:
    - Al inicio y finalización de las funciones de auditoría.
    - *Login* y *logout* de usuarios registrados.
    - Cambios en las credenciales de usuarios.
    - Cambios en la configuración del producto [**asignación**: *listado de cambios*].
    - Eventos relativos a la funcionalidad del producto [**asignación:** *listado de eventos*].
    - Si el TOE gestiona claves criptográficas, [**selección:** generación; importación; cambio; eliminación de claves criptográficas; ningún otro].

46. **AUD.2** Los registros de auditoría contendrán al menos la siguiente información: fecha y hora del evento, tipo de evento identificado, resultado del evento, usuario que produce el evento.
47. **AUD.3** A los registros de auditoría se aplicará la siguiente política de acceso:
    - Lectura: usuarios autorizados.
    - Modificación: ningún usuario.
    - Borrado: [**selección**: solo administradores; ningún usuario]
48. **AUD.4** El TOE debe ser capaz de almacenar en sí mismo la información de auditoría generada y [**selección**: transmitir la información de auditoría generada a una entidad externa utilizando un canal seguro COM.1; no transmitir la información de auditoría generada].
49. **AUD.5** El TOE deberá [**selección**: sobreescribir los registros siguiendo el criterio de mayor antigüedad; enviar a una entidad externa y eliminar; otra opción validada por el CPSTIC] en el caso de que el espacio para almacenamiento de los registros alcance su límite.

4.7 PROTECCIÓN DE CREDENCIALES Y DATOS SENSIBLES

50. **PSC.1** En el caso en que el TOE almacene [***selección**: credenciales; claves privadas; [**asignación**: otros parámetros de seguridad críticos*] estos no deberán almacenarse en claro, sino que se utilizarán mecanismos de protección criptológica que cumplan con **CIF.1**.

4.8 PROTECCIÓN DEL PRODUCTO Y SUS SERVICIOS

51. **PRO.1** El TOE deberá ser capaz de realizar un test durante el arranque o encendido del producto, [**selección***: periódicamente durante la operación normal del producto; a petición de un usuario autorizado; ninguna*] para verificar la integridad del software/firmware, [***selección**: el correcto funcionamiento de los mecanismos criptográficos; [**asignación**: otros]; ninguno*].

4.9 CONTROL DE ACCESO A RED

52. **NAC.1** El TOE aplicará las políticas de control de acceso definidas por el usuario. En ellas, se definirán permisos de acceso a [**selección***: usuarios; roles de usuario*] que realicen sobre objetos [***selección**: programas; ficheros; configuraciones; urls; [**asignación**: otros]*] determinadas operaciones [***selección**: creación; lectura; modificación; ejecución; [**asignación**: otras]*] y determinados parámetros condicionales adicionales: *[**asignación**: parámetros]*.
53. **NAC.2** El producto aplicará las últimas políticas configuradas cuando se restaure su funcionamiento después de algún problema en su funcionamiento.
54. **NAC.3** El producto deberá aplicar políticas de denegación por defecto y notificar al administrador en caso de detectar un malfuncionamiento.

4.10 NOTAS DE APLICACIÓN

55. En caso de que el producto no implemente la funcionalidad a la que aplica alguno de los requisitos anteriores (o algunas partes de ellos), y ésta sea proporcionada por el entorno operacional, el fabricante deberá indicarlo en la declaración de seguridad o justificarlo debidamente. En este caso, se evaluará si dada la misión y capacidades del producto, se puede considerar que el requisito ***no aplica***.

56. Lo anterior no es válido en caso de que tal funcionalidad solicitada en un requisito, sea proporcionada por un componente del producto que no forma parte de la configuración evaluada. En este caso ***sí aplica***, y el fabricante deberá demostrar el correcto cumplimiento del requisito por parte del producto.

5. ABREVIATURAS

CCN	Centro Criptológico Nacional
CPSTIC	Catálogo de Productos y Servicios de Seguridad de las Tecnologías de Información y las Comunicaciones
ENS	Esquema Nacional de Seguridad
RFS	Requisitos Fundamentales de Seguridad
TLS	*Transport Layer Security*

PUBLICACIONES DE DEFENSA

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