centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 140

Taxonomía de productos STIC-
Anexo D.10: Web Application Firewall (WAF)

Marzo 2020

MINISTERIO DE DEFENSA

Edita:

MINISTERIO DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

centro criptológico nacional

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2020.03.13 17:13:36 +01'00'

NIPO: 083-19-053-9.

Fecha de Edición: marzo de 2020

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 ***Web Application Firewall (WAF)*** para ser incluido en el apartado de Productos Cualificados del Catálogo de Productos de Seguridad de las Tecnologías de la Información y la Comunicación (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 para los que sea de aplicación el **Esquema Nacional de Seguridad (ENS)**. 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 ***Web Application Firewall (WAF)*** 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. Los Firewalls de Aplicaciones Web o, más comúnmente conocidos por sus siglas en inglés: WAF (*Web Application Firewall*) son productos que se centran en analizar y filtrar el tráfico dirigido a aplicaciones web específicas. La protección tiene lugar dentro de la capa 7 del modelo OSI (Capa de Aplicación).
7. Los WAF son, por lo tanto, un tipo especializado de cortafuegos o *firewall* que se instalan por delante de los servidores web, para proteger las aplicaciones web contra ataques internos y externos. Analizan el tráfico bidireccional HTTP/HTTPS para detectar y bloquear el tráfico dañino. Son capaces de detectar ataques como inyección SQL, *cross-site scripting* (XSS), ataques automatizados (*bots*), DoS a nivel de aplicación, etc.
8. Los WAF emplean diferentes técnicas de protección: basadas en firmas (*signature-based*), modelos de seguridad positiva/negativa, detección de anomalías, etc.
9. Además de monitorizar y controlar el acceso a las aplicaciones web, los WAF también recolectan *logs* destinados a cumplimiento de normativas (*compliance*), auditoría y análisis.

2.2 CASOS DE USO

10. Dependiendo de las funcionalidades del producto explotadas, y de la finalidad o el contexto en que se utilicen, se contemplan diferentes casos de uso para esta familia de productos tal y como se indica a continuación.

2.2.1. CASO DE USO 1– DESPLIEGUE EN RED

11. El WAF se despliega como un dispositivo de red más, ya sea en formato *hardware* (*appliance*) o virtualizado.

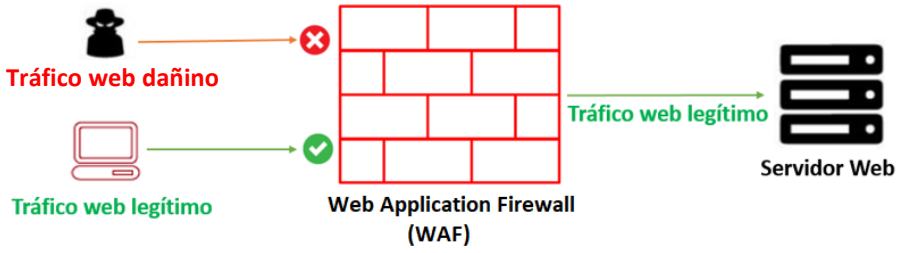

Figura 1: Despliegue de WAF en red.

2.2.2. CASO DE USO 2 – DESPLIEGUE EN ENDPOINT

12. El WAF se despliega como un módulo *software* en el servidor en el que se encuentra alojada la aplicación o servicio web. Puede ser implementado de diferentes formas:

    - Instalado como una herramienta o programa independiente.
    - Instalado como un complemento del servidor web.
    - Instalado como un *plugin*.

Figura 2: Despliegue de WAF en *endpoint*.

2.3 ENTORNO DE USO

13. Para la utilización en condiciones óptimas de seguridad de las herramientas WAF, es necesario que se integren en un entorno de trabajo que cumpla una serie de condiciones mínimas de protección:

    - **Protección física:** El producto deberá instalarse en un área donde el acceso sólo sea posible para el personal autorizado y con condiciones ambientales adecuadas.
    - **Plataforma segura:** En caso de tratarse de un producto *software*, este se ejecutará sobre una plataforma confiable, incluyendo el sistema operativo o cualquier entorno de ejecución sobre el que se utilice.
    - **Administración confiable**: El Administrador será un miembro de plena confianza y que vela por los mejores intereses en materia de seguridad de la empresa/administración. Por ello se asume que dicha persona estará capacitada, formada y carecerá de cualquier intención dañina al administrar el producto.
    - **Actualizaciones periódicas:** El firmware (si aplica) y software del producto será actualizado conforme aparezcan actualizaciones que corrijan vulnerabilidades conocidas.
    - **Protección de las credenciales:** Todas las credenciales, en especial las del administrador, deberán estar correctamente protegidas por parte de la organización que utilice el producto.

2.4 DELIMITACIÓN DEL ALCANCE DEL DISPOSITIVO

14. Este tipo de productos suelen presentarse en formato **Equipo dedicado o *Appliance*** (*hardware* provisto de *firmware* y *software* dedicado), formato **máquina virtual** o formato ***software*** (que se instala en un sistema de ficheros proporcionado por un Sistema Operativo).

2.5 ALINEAMIENTO CON CRITERIOS COMUNES (*COMMON CRITERIA*)

15. El estándar *Common Criteria* (CC) proporciona un conjunto común de requisitos funcionales y de aseguramiento para la evaluación de los productos TIC (Tecnologías de la Información y de las Comunicaciones).
16. En el ámbito de CC se definen un conjunto de objetivos y requisitos de seguridad, tanto funcionales (*SFR, Security Functional Requirements*) como de evaluación (*SAR, Security Assurance Requirements*), independientes de la implantación, que cada producto incluirá dentro de su declaración de seguridad (*ST, Security Target*).
17. **Los productos dentro de esta familia, deberán disponer de una declaración de seguridad (ST) certificada con un nivel de confianza EAL2 o superior (*Evaluation Assurance Level*), que contenga los RFS indicados en el apartado 4.**
18. En caso de que alguno de los requisitos definidos en el apartado 4 no se encuentre recogido en la declaración de seguridad del producto, pero este sí implemente esa función de seguridad, se podrá llevar a cabo una *evaluación STIC complementaria*, cuyo objetivo será verificar el cumplimiento de esos requisitos.

3. ANÁLISIS DE AMENAZAS

3.1 RECURSOS QUE ES NECESARIO PROTEGER

19. Los recursos que es necesario proteger mediante el uso de estos productos incluyen:

- Interfaces de gestión del producto e información transmitida a través de ellas, en ambos sentidos.
- Toda la información que tenga que hacer uso del producto para ser transmitida (como contraseñas, parámetros de configuración, actualizaciones críticas).
- Datos de configuración del producto y de auditoría generados por éste.
- Actualizaciones del dispositivo susceptibles de afectar a su configuración y funcionalidad.
- Aplicaciones y servicios web de la organización, susceptibles de ser objeto de ataques a través de tráfico, principalmente, HTTP.

3.2 AMENAZAS

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

- **A.RED. Ataque a la red.** Un atacante desde dentro o desde fuera de la red, consigue acceder a información intercambiada a través de la red, entre el producto y otras entidades autorizadas o modificar sus comunicaciones.
- **A.LOCAL. Ataque local.** Un atacante puede actuar a través de software no privilegiado ejecutado en la misma plataforma de computación donde se ejecuta el producto. Los atacantes podrían modificar de forma maliciosa los ficheros o comunicaciones que utiliza el producto.
- **A.REST. Acceso a información almacenada.** Un atacante podría acceder a información sensible almacenada en la plataforma en la que se instala y ejecuta el producto.
- **A.SEG. Acceso a las funciones de seguridad.** Un atacante podría acceder y modificar las funciones y datos de seguridad del producto.
- **A.NODET. Actividad no detectada.** Un atacante consigue acceder, cambiar o modificar la funcionalidad de seguridad del producto o los datos recopilados por este, sin que esto sea apreciado por el administrador.
- **A.EXT**. **Contenido externo potencialmente dañino**. Un atacante puede enviar información no permitida o dañina a través del producto, que resulta en la explotación de aplicaciones o servicios web en la red interna.

4. REQUISITOS FUNDAMENTALES DE SEGURIDAD (RFS)

21. 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.

4.1 ADMINISTRACIÓN CONFIABLE

1. Estas funcionalidades de seguridad mitigan la amenaza (A.SEG). **Podrán ser cubiertas por el producto o por su entorno operacional.**
2. **ADM.1** El producto debe definir, al menos, el rol de administrador y ser capaz de asociar usuarios a roles.
3. **ADM.2** El producto debe ser capaz de realizar la gestión de las siguientes funcionalidades:
   - Administración del producto de forma local y remota.
   - Configuración del tiempo de terminación de sesión o bloqueo al detectar inactividad.
   - Otros parámetros de configuración del producto.
4. **ADM.3** El producto deberá asegurar que solamente un usuario con permisos de administrador será capaz de realizar las funciones anteriormente descritas (ADM.2).

4.2 IDENTIFICACIÓN Y AUTENTICACIÓN

5. Estas funcionalidades de seguridad mitigan la amenaza (A.REST, A.SEG). **Podrán ser cubiertas por el producto o por su entorno operacional.**
6. **IAU.1** El producto deberá identificar y autenticar a cada usuario antes de otorgar acceso.
7. **IAU.2**. El producto deberá implementar mecanismos que impidan ataques de autenticación por fuerza bruta.
8. **IAU.3.** El producto deberá proteger de lectura y modificación no autorizada las credenciales de autenticación.
9. **IAU.4**. El producto deberá 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 [“!”, “@”, “#”, “$”,“%”, “^”, “&”, “*”, “(“, “]

10. **IAU.5** El producto debe bloquear o cerrar la sesión de un usuario después de un determinado periodo de tiempo de inactividad.

4.3 AUDITORÍA

11. Estas funcionalidades de seguridad mitigan la amenaza (A.NODET).
12. **AUD.1** El producto deberá generar información de auditoría al comienzo y finalización de las funciones de auditoría y cuando se produzca alguno de los siguientes eventos:
    - *Login* y *logout* de personal autorizado.
    - Cambio en las credenciales de usuarios.
    - Cambios en la configuración del producto.
    - Eventos relativos a la funcionalidad del producto.
13. **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 (si aplica).
14. **AUD.3** A los registros de auditoría se aplicará la siguiente política de acceso:

    a) Lectura: usuarios autorizados.

    b) Modificación: ningún usuario.

    c) Borrado: administradores.
15. **AUD.4** Si se trata de un producto *appliance*, debe ser capaz de almacenar la información de auditoría generada en sí mismo o en una entidad externa.
16. **AUD.5** Si se trata de un producto *appliance*, este debe ser capaz de eliminar o sobrescribir registros de auditoría anteriores cuando el espacio de almacenamiento esté lleno.

4.4 CANAL SEGURO

17. Estas funcionalidades de seguridad mitigan la amenaza (A.RED).
18. **COM.1** El TOE deberá establecer canales seguros (HTTPS/TLS 1.2, TLS 1.2 o superior, IPSec, SSHv2, etc.) cuando intercambie información sensible con entidades autorizadas, o entre las distintas partes del producto, empleando funciones, algoritmos y protocolos que estén de acuerdo a lo establecido en la guía CCN-STIC-807 (p.ej.: HTTPS/TLS 1.2, TLS 1.2 o superior, IPSec, etc.).

4.5 INSTALACIÓN Y ACTUALIZACIÓN CONFIABLES

19. Estas funcionalidades de seguridad mitigan la amenaza (A.LOCAL, A.SEG).

20. **ACT.1** El producto ofrecerá la posibilidad de consultar la versión actual del *firmware/software*, iniciar actualizaciones manualmente y comprobar si existen nuevas actualizaciones disponibles.
21. **ACT.2** El producto deberá ofrecer mecanismos, conforme a la criptografía de empleo en el ENS, a través de hashes o firma digital para autenticar las actualizaciones de *firmware/software* antes de instalarlas.
22. **ACT.3.** La actualización del *firmware/software* se permitirá únicamente a usuarios con rol de administrador.
23. **ACT.5** En caso de tratarse de un producto *software*, este deberá estar empaquetado de forma que, si se elimina, no deje rastro de su instalación (excepto por configuraciones y ficheros de salida o auditoría).
24. **ACT.6** En caso de tratarse de un producto *software*, este no descargará ni modificará su propio código binario.
25. **ACT.7** En caso de tratarse de un producto *software*, solamente utilizará las bibliotecas de terceras partes declaradas por el fabricante.

4.6 PROTECCIÓN DE CREDENCIALES Y DATOS SENSIBLES

26. Estas funcionalidades de seguridad mitigan la amenaza (A.REST). **Podrán ser cubiertas por el producto o por su entorno operacional.**
27. **CRD.1** En el caso en que el producto almacene credenciales y/o datos sensibles, éstos no deberán almacenarse en claro.

4.7 REQUISITOS CRIPTOGRÁFICOS

28. Estas funcionalidades de seguridad mitigan las amenazas (A.RED, A.REST).
29. **CIF.1** El TOE permitirá exclusivamente el empleo de funciones, algoritmos y protocolos criptográficos que estén incluidas entre las autorizadas para Categoría ALTA del ENS, de acuerdo a lo establecido en la guía CCN-STIC-807.
30. **CIF.2** El producto deberá impedir el acceso en claro a los parámetros de seguridad críticos del sistema (claves simétricas y claves privadas).
31. **CIF.3** Generador de bits aleatorios. En caso de suministrar un servicio de generación de bits aleatorios (RBG1) determinísticos, el producto deberá:
    - Utilizar Hash_DRBG (any), HMAC_DRBG (any) o CTR_DRBG (AES).
    - Usar una semilla de al menos una fuente de entropía que acumule entropía de varias fuentes o disponer de una fuente de entropía estudiada, con un mínimo de bits de entropía al menos igual a la mayor fortaleza de seguridad de las claves y hashes que generará, de acuerdo a la ISO/IEC 18031:2011.
32. **CIF. 4** Generación de claves asimétricas. En caso de generar claves asimétricas, el producto podrá utilizar los siguientes algoritmos:

- ECC con una longitud de clave de 256 o superior.
- FFC con una longitud de clave de 3072 o superior.
- RSA con una longitud de clave de 3072 o superior.

33. **CIF.5** Establecimiento de claves. Para el establecimiento de claves, el producto podrá utilizar los siguientes algoritmos:
    - Esquemas basados en RSA con una longitud de clave de 3072 o superior.
    - Esquemas basados en FFC con una longitud de clave de 3072 o superior.
    - Esquemas basados en ECC con una longitud de clave de 256 o superior.
    - Esquemas basados en DH grupos 15, 19, 20, 21, 28, 29 o 30.
34. **CIF.6** Algoritmos HASH. Las funciones resumen o HASH que utilice el producto deberán utilizar los algoritmos SHA-22 y SHA-3 de longitud mayor o igual a 256.
35. **CIF.7** Firma digital. Para los servicios de verificación de firma digital, el producto deberá utilizar uno de los siguientes algoritmos:
    - *Digital Signature Algorithm* (DSA) con una longitud de clave de 3072 bits o superior.
    - *Elliptic Curve Digital Signature Algorithm* (ECDSA) con una longitud de clave de 256 o superior.
    - RSA con una longitud de clave de 3072 o superior.
36. **CIF.8** Cifrado de datos y claves con AES. El producto implementará cifrado de datos de acuerdo con el algoritmo AES los modos CBC, GCM y longitud de claves 128 bits o superior.
37. **CIF.9** Autenticación de mensajes. Para los servicios de autenticación de mensajes, el producto podrá utilizar HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA512.
38. **CIF.10** El producto deberá implementar los siguientes métodos de borrado de claves:
    - Para memoria volátil, la destrucción podrá ser realizada utilizando los siguientes métodos:
        i. Una pasada de sobrescritura utilizando alguno de los siguientes:
            1. Un patrón pseudoaleatorio generado por el RBG.
            2. Todo ceros o unos.
            3. Algún valor que no contenga ningún parámetro de seguridad crítico (PSC).
        ii. Destrucción de la referencia a la clave directamente seguida por una llamada al “recolector de basura” de la memoria.

- Para memoria no volátil, la destrucción deberá ejecutarse por la invocación de un interfaz que:
    i. Apunte lógicamente a la ubicación de almacenamiento de la clave y realice una o más pasadas de sobrescritura utilizando:
        1. Un patrón pseudoaleatorio generado por el RBG del producto.
        2. Todo ceros o unos.
        3. Algún valor que no contenga ningún parámetro de seguridad crítico (PSC).
    ii. Ordene a otra parte del producto que destruya la abstracción que representa la clave.

4.8 POLÍTICA DE SEGURIDAD WAF

39. Esta funcionalidad de seguridad mitiga la amenaza (A.EXT).
40. **WAF.1** El producto debe proporcionar una *política de seguridad WAF* para gobernar el tráfico dirigido a las aplicaciones y servicios web que protege. La política permitirá la configuración de reglas por parte de los administradores.
41. **WAF.2** En función de las reglas configuradas, se podrán lanzar las acciones especificadas por el administrador. Dentro de las acciones posibles, se podrá alertar y/o bloquear el tráfico sospechoso.
42. **WAF.3** El producto permitirá la creación de listas blancas (explícitamente autorizadas) y negras (explícitamente denegadas). Estas listas podrán basarse en direcciones IP, protocolo, servicio, etc.
43. **WAF.4** El producto deberá detectar y protegerse frente a, al menos, los siguientes tipos de ataques:

TOP	TIPOS DE ATAQUES	DESCRIPCIÓN
A1	*Inyección (Injection)*	Consiste en el envío a un intérprete, de ciertos datos maliciosos como parte de un comando o consulta. El tipo de datos que se suelen utilizar son SQL, NoSQL, OS y LDAP. El objetivo es que el intérprete ejecute comandos no deseados o proporcione información sin la autorización adecuada.
A2	*Debilidad de Autenticación (Broken Authentication)*	Un atacante se aprovecha de mecanismos de autenticación y control de sesión débiles, en la aplicación o servicio web. De esta forma, puede comprometer credenciales o tokens de sesión para asumir la identidad de usuarios legítimos, de forma temporal o permanente.

TOP	TIPOS DE ATAQUES	DESCRIPCIÓN
A3	*Exposición de datos sensibles (Sensitive Data Exposure)*	Un atacante se aprovecha de mecanismos débiles de protección de datos sensibles (en reposo y en tránsito), en las aplicaciones y servicios web. De esta forma, un atacante podría robar estos datos débilmente protegidos, para realizar fraudes con tarjetas de crédito, robo de identidad u otros delitos.
A4	*Entidades Externas XML (XXE)*	Un atacante puede utilizar entidades externas dentro de documentos XML, para revelar archivos internos, escaneo de puertos internos, ejecución remota de código y ataques de denegación de servicio.
A5	*Debilidad de Control de Acceso (Broken Access Control)*	Un atacante se aprovecha de mecanismos de control de acceso débiles en la aplicación o servicio web. De esta forma, puede acceder a funcionalidades o datos no autorizados.
A6	*Configuración de Seguridad incorrecta (Security Misconfiguration)*	Un atacante se aprovecha de una configuración de seguridad incompleta o incorrecta en la aplicación o servicio web. No solo la configuración incorrecta de opciones, funciones y parámetros, sino la falta de parcheado y actualización regular.
A7	*Cross-Site Scripting (XSS)*	Un atacante se aprovecha de debilidades en aplicaciones o servicios web, que recogen datos no confiables y los envían al navegador web sin una validación previa o codificación adecuada. De esta forma, un atacante puede ejecutar comandos en el navegador de la víctima, secuestrar una sesión, modificar (*defacement*) los sitios web, o redireccionar al usuario hacia un sitio malicioso.
A8	*Deserialización insegura (Insecure Deserialization)*	Un atacante se aprovecha de la debilidad de algunas aplicaciones y servicios web, que aceptan objetos serializados dañinos, los cuales pueden ser manipulados o borrados por el atacante, para realizar ataques de repetición (*replay*), inyección o escalado de privilegios. En el peor de los casos, la desacralización insegura puede conducir a la ejecución remota de código en el servidor.
A9	*Uso de componentes con vulnerabilidades conocidas*	Un atacante se aprovecha de componentes como librerías, *frameworks*, y otros módulos software, que se ejecutan con los mismos privilegios que la aplicación. De esta forma, si alguno de los componentes es vulnerable, el atacante puede lanzar ataques que provoquen pérdida de datos o tomar el control del servidor.

TOP	TIPOS DE ATAQUES	DESCRIPCIÓN
A10	*Insuficiente monitorización y logging*	Un atacante se aprovecha de una insuficiente monitorización de las aplicaciones y servicios web, junto con la falta de un mecanismo de respuesta a incidentes adecuado. De esta forma, el atacante puede lanzar ataques al sistema de forma persistente y mantenida en el tiempo, saltar a otros sistemas, y manipular, extraer o destruir datos.
A11	*Otros ataques*	Se podrán declarar otro tipo de ataques que sean mitigados por el producto.

Tabla 1.- Top 10 Web Application Security Risks de OWASP

NOTA: Se ha tomado como referencia el *Top 10 Web Application Security Risks de OWASP*[1] (*Open Web Application Security Project*) a fecha de publicación de este Anexo. Este listado está sujeto a actualizaciones y deberá tenerse en cuenta la última lista publicada en el momento de realización de la evaluación.

[1] https://owasp.org/www-project-top-ten/

5. ABREVIATURAS

CC	*Common Criteria*
CCN	Centro Criptológico Nacional
CPSTIC	Catálogo de Productos de Seguridad de las Tecnologías de Información y las Comunicaciones
EAL	*Evaluation Assurance Level*
ENS	Esquema Nacional de Seguridad
LDAP	*Lightweight Directory Access*
NIAP	*National Information Assurance Partnership*
OWASP	*Open Web Application Security Project*
RFS	Requisitos Fundamentales de Seguridad
SFR	*Security Functional Requirements*
SQL	*Structured Query Language*
ST	*Security Target*
TOE	*Target of Evaluation*
WAF	*Web Application Firewall*