centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 140

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

Noviembre de 2022

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
2023.01.03 14:55:54 +01'00'

Pº de la Castellana 109, 28046 Madrid
Centro Criptológico Nacional, 2022
NIPO: 083-22-102-1

Fecha de Edición: noviembre de 2022

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 y Servicios 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), 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 ***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.

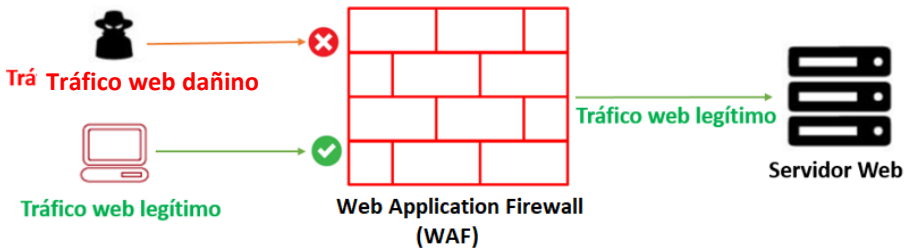

Figura 1: Despliegue de WAF en red

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 HIPÓTESIS SOBRE EL ENTORNO DE EJECUCIÓN

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 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.
    - **Funcionalidad limitada**: El producto solo deberá proporcionar la funcionalidad de análisis y filtrado de tráfico dirigido a aplicaciones web como su función principal y no debe proporcionar ninguna otra funcionalidad o servicio que puedan considerarse de propósito general.
    - **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.
    - **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.

- **Plataforma confiable**. En caso de tratarse de un producto software, este se ejecutará sobre una plataforma confiable, incluyendo el sistema operativo o cualquier entorno de ejecución que la plataforma proporcione.

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). En caso de ofrecer funcionalidades adicionales a las definidas en la sección 2.1, éstas quedan fuera del alcance analizado, debiendo ser evaluadas conforme a los RFS específicos aplicables a tales funcionalidades complementarias.

2.5 CERTIFICACIÓN LINCE

15. 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)[1] que incluya los RFS reflejados en el apartado 4, que deberán ser evaluados considerando el problema de seguridad definido en el presente documento.
16. El alcance de la evaluación deberá incluir el módulo de evaluación básico de 25 días de esfuerzo y el Módulo de Evaluación Criptográfica (MEC). El Módulo de Revisión de Código Fuente (MCF) será opcional.

[1] Toda la información relativa a esta metodología se encuentra disponible en la web del Organismo de Certificación (https://oc.ccn.cni.eshttps://oc.ccn.cni.es)

3. ANÁLISIS DE AMENAZAS

3.1 ACTIVOS SENSIBLES A PROTEGER

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

    18. **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.

    19. **AC.PSS.** Datos de configuración, registros auditoría y [***asignación**: listado de datos definidos por el fabricante*] que deben ser protegidos en Integridad.

    20. **AC.PSC.** [**selección**: credenciales; claves; [**asignación**: *listado de datos definidos por el fabricante*] que deben ser protegidos en Confidencialidad e Integridad.

    21. **AC.Actualizaciones.** Actualizaciones del producto susceptibles de afectar a su configuración y funcionalidad, que deben ser protegidos en Integridad y Autenticidad.

    22. **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

23. 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.INT Compromiso de la integridad del *software/firmware*:** Un atacante puede intentar comprometer la integridad del producto a través de un software sin privilegios ejecutado en la misma plataforma en la que se ejecuta el producto
- **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.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

24. 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.NOAUTUSR	A.CRE	A.INT	A.RED
ADM.1	X									
ADM2	X									
ADM.3	X									
IAU.1	X						X			
IAU.2								X		
IAU.3								X		
IAU.4	X									
IAU.5								X		
COM.1		X	X							
COM.2			X							
COM.3			X							

	A.NOAUT	A.CRYPTO	A.COM	A.ACT	A.AUD	A.PSC	A.NOAUTUSR	A.CRE	A.INT	A.RED
COM.4		X	X							
ACT.1				X						
ACT.2				X						
ACT.3				X						
ACT.4				X						
ACT.5				X						
AUD.1					X					
AUD.2					X					
AUD.3					X					
AUD.4					X					
AUD.5					X					
EXP.1									X	
EXP.2									X	
EXP.3									X	
PSC.1						X				
CIF.1		X	X							
WAF.1										X
WAF.2										X
WAF.3										X
WAF.4										X

4. REQUISITOS DE SEGURIDAD

25. 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.

26. 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.

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

4.1 ADMINISTRACIÓN CONFIABLE

28. Podrán ser cubiertas por el producto o por su entorno operacional.

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

30. **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].

31. **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

32. Podrán ser cubiertas por el producto o por su entorno operacional.

33. **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*].
34. **IAU.2** El TOE deberá implementar mecanismos que impidan ataques de autenticación por fuerza bruta.
35. **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.
36. **IAU.4** El TOE debe [**selección***: bloquear; cerrar*] la sesión de un usuario después de [***asignación****: tiempo de inactividad*] de inactividad.
37. **IAU.5** Cuando el acceso se realice utilizando credenciales por defecto o el usuario no tenga asignadas credenciales, el TOE obligará al [**selección***: cambio; establecimiento*] de credenciales en el siguiente acceso.

4.3 CANALES SEGUROS

38. Podrán ser cubiertas por el producto o por su entorno operacional.
39. **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*].
40. **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.
41. **COM.3** El TOE hará uso de certificados digitales para la autenticación cuando utilice cualquiera de los protocolos definidos en **COM.1**.
42. **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

43. Podrán ser cubiertas por el producto o por su entorno operacional.
44. **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

45. **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].
46. **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.
47. **ACT.3** La actualización del *firmware/software* se permitirá únicamente a usuarios con rol de administrador.
48. **ACT.4** En el caso de que el TOE sea una aplicación software, esta deberá estar empaquetada de forma que, si se elimina, no deje rastro de su instalación (excepto por configuraciones y ficheros de salida o auditoría).
49. **ACT.5** En el caso de que el TOE sea una aplicación software, este no descargará ni modificará su propio código binario.

4.6 AUDITORÍA

50. Podrán ser cubiertas por el producto o por su entorno operacional.
51. **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].

52. **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.
53. **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]
54. **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].
55. **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 CAPACIDADES ANTI-EXPLOTACIÓN

56. Los requisitos de la presente familia serán de aplicación únicamente cuando el producto se presente en formato *software*.
57. **EXP.1** Cuando el TOE se encuentre en ejecución, este no solicitará la asignación de ninguna dirección explícita de memoria del sistema, ni asignará memoria con permisos simultáneos de escritura y ejecución.
58. **EXP.2** El TOE está configurado por defecto con permisos de ficheros que lo protejan de accesos no autorizados.
59. **EXP.3** En el caso de que el TOE sea una aplicación *software*, este solamente utilizará las bibliotecas de terceras partes declaradas [asignación: *listado de librerías*].

4.8 PROTECCIÓN DE CREDENCIALES Y DATOS SENSIBLES

60. **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**.

4.9 POLÍTICA DE SEGURIDAD WAF

61. **WAF.1** El TOE 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.

62. **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.

63. **WAF.3** El TOE permitirá la creación de listas blancas (explícitamente autorizadas) y negras (explícitamente denegadas). Estas listas podrán basarse en direcciones IP, protocolo, servicio, etc.

64. **WAF.4** El TOE 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.
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.

TOP	TIPOS DE ATAQUES	DESCRIPCIÓN
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.
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.

TOP	TIPOS DE ATAQUES	DESCRIPCIÓN
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*[2] (*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.

4.10 NOTAS DE APLICACIÓN GENERAL

65. 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***.
66. 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.

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

5. ABREVIATURAS

CC	*Common Criteria*
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
LDAP	*Lightweight Directory Access*
OWASP	*Open Web Application Security Project*
RFS	Requisitos Fundamentales de Seguridad
SQL	*Structured Query Language*
TOE	*Target of Evaluation*
WAF	*Web Application Firewall*

PUBLICACIONES DE DEFENSA

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