

Edita:



© Centro Criptológico Nacional, 2020
NIPO: 083-19-053-9

Fecha de Edición: Agosto 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

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

ÍNDICE

1. INTRODUCCIÓN Y OBJETO	4
2. DESCRIPCIÓN DE LA FAMILIA DE PRODUCTOS	5
2.1 FUNCIONALIDAD	5
2.2 CASOS DE USO.....	5
2.2.1. CASO DE USO 1 – BALANCEADOR	5
2.3 ENTORNO DE USO.....	6
2.4 DELIMITACIÓN DEL ALCANCE DEL DISPOSITIVO	7
2.5 ALINEAMIENTO CON CRITERIOS COMUNES (COMMON CRITERIA)	7
3. ANÁLISIS DE AMENAZAS	8
3.1 RECURSOS QUE ES NECESARIO PROTEGER.....	8
3.2 AMENAZAS	8
4. REQUISITOS FUNDAMENTALES DE SEGURIDAD (RFS).....	10
4.1 PERFIL DE PROTECCIÓN	10
4.2 REQUISITOS CRIPTOGRÁFICOS.....	10
4.3 CONTROL DE LOS FLUJOS DE INFORMACIÓN	10
4.4 REQUISITOS DE BALANCEADOR	11
5. ABREVIATURAS.....	12

1. INTRODUCCIÓN Y OBJETO

1. El presente documento describe los Requisitos Fundamentales de Seguridad (RFS) exigidos a un producto de la familia de **Balanceadores de Carga** 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 a las 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 de **Balanceadores de Carga** 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 productos asociados a esta familia están orientados al control del ancho de banda entre diferentes elementos del sistema. En concreto, buscan optimizar los tiempos de respuesta y evitar la saturación de los servidores que atienden peticiones remitidas por equipos cliente.
7. Un ejemplo sería el escenario en el que equipos clientes, dentro de una red interna o externa (como Internet), solicitan recursos a los servidores del sistema que actúan como *back-end*. Dichas solicitudes pasan a través del balanceador de carga, ubicado en algún punto de la frontera entre ambas redes, quién a su vez analizará las solicitudes y distribuirá las peticiones, trasladándolas a los servidores destino.
8. En este contexto proporcionan las siguientes funciones básicas de seguridad asociadas a la disponibilidad del sistema:
 - Asignar o balancear las solicitudes de equipos cliente a servidores mediante el uso de un algoritmo dedicado.
9. El balanceo de carga puede tener lugar a diferentes niveles dentro de las capas definidas por el modelo de interconexión de sistemas abiertos (ISO/IEC 7498-1)¹, fundamentalmente a nivel de capa 4 (de transporte) y/o 7 (de aplicación).
10. Los productos incluidos en esta familia pueden ofrecer otras funcionalidades complementarias (p.ej. cortafuegos, *proxies* o WAF²) recogidas en otras familias de productos.

2.2 CASOS DE USO

11. Se contempla 1 caso de uso.

2.2.1. CASO DE USO 1 – BALANCEADOR

12. El dispositivo se encuentra desplegado como elemento del sistema al que los clientes remiten peticiones para ser analizadas y remitidas al servidor de destino elegido, garantizando el balanceo de carga entre un conjunto de servidores.

¹ Modelo de interconexión de sistemas abiertos (ISO/IEC 7498-1) es un modelo de referencia para los protocolos de la red de arquitectura en capas creado por la Organización Internacional de Normalización (ISO) y la Comisión electrotécnica Internacional (IEC).

² *Web Application Firewall*

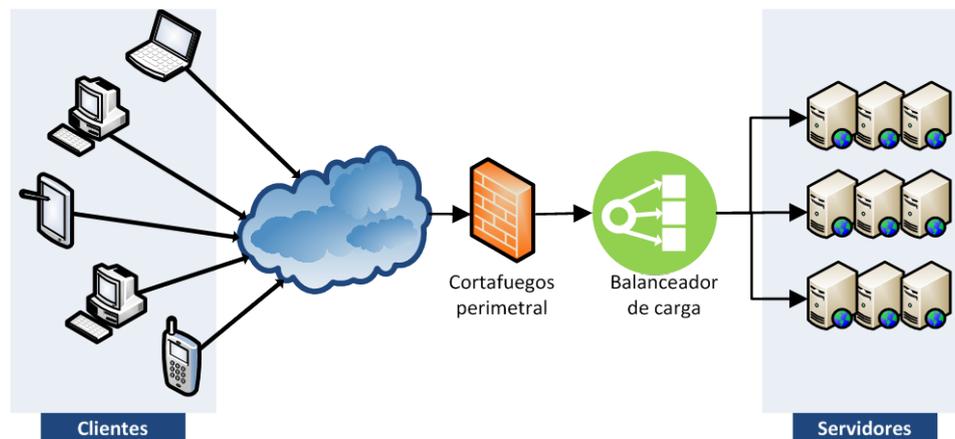


Figura 1 – Ejemplo de Caso de Uso: Balanceador de carga

2.3 ENTORNO DE USO

13. Este tipo de dispositivos son de uso generalizado en grandes o medianas empresas, así como en redes del sector público, en las que se busca optimizar el uso de los recursos para garantizar la disponibilidad del servicio suministrado al ciudadano.
14. Para la utilización en condiciones óptimas de seguridad de estos dispositivos, es necesaria su integración 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.
 - **Administración confiable:** El usuario 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 altamente capacitada y carecerá de cualquier intención dañina al administrar los dispositivos. El producto no será capaz de defenderse contra un usuario administrador con malas intenciones.
 - **Actualizaciones periódicas:** El *firmware* y el *software* del producto será actualizado conforme aparezcan actualizaciones que corrijan vulnerabilidades conocidas.
 - **Política de seguridad de la información:** Deberá existir una política de seguridad que recoja el conjunto de principios, organización y procedimientos impuestos por una organización para hacer frente a sus necesidades de seguridad de la información, incluyendo el uso de las TIC.

2.4 DELIMITACIÓN DEL ALCANCE DEL DISPOSITIVO

15. Este tipo de productos se presentan en formato **equipo dedicado o *Appliance*** (*hardware* provisto de *firmware*³ dedicado) con las funcionalidades estrictamente necesarias para cumplir su finalidad y acotadas al servicio específico que presten.
16. En caso de ofrecer funcionalidades adicionales a las definidas en la [sección 2](#), éstas quedan fuera del alcance analizado, y deberán ser evaluadas conforme a los RFS específicos aplicables a tales funcionalidades complementarias.

2.5 ALINEAMIENTO CON CRITERIOS COMUNES (COMMON CRITERIA)

17. El estándar *Common Criteria* (CC) proporciona un conjunto común de requisitos funcionales y de aseguramiento para la evaluación de los productos de TI (Tecnologías de la Información).
18. En el ámbito de CC se elaboran unos perfiles de seguridad que definen, para un dominio o categoría de productos, un conjunto de objetivos y requisitos de seguridad, tanto funcionales como de evaluación, independientes de la implantación.
19. Los productos dentro de esta familia deberán estar certificados de acuerdo a la norma *Common Criteria*. Dicha certificación deberá evidenciar el problema de seguridad definido en el presente documento e incluir los requisitos fundamentales de seguridad recogidos en el apartado 4.
20. El nivel de confianza EAL (*Evaluation Assurance Level*) con el que deben ser evaluados los requisitos exigidos para esta familia será:
 - **El determinado por el perfil de protección** para aquellos SFR incluidos en los perfiles exigidos cuando los productos se encuentren certificados contra alguno de los perfiles anteriormente descritos.
 - **EAL2 o superior** en el caso en el que el producto no se encuentre certificado contra ningún perfil.
21. En caso de que alguno de los requisitos indicados 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*Firmware* funciona como el nexo de unión entre las instrucciones (*software*) que llegan al dispositivo desde el exterior y las diversas partes electrónicas (*hardware*)

3. ANÁLISIS DE AMENAZAS

3.1 RECURSOS QUE ES NECESARIO PROTEGER

22. Los recursos que deben protegerse mediante el uso de estos productos son:
- Información que atraviese el producto, que provenga de los equipos y dispositivos para los cuales se realiza la función de balanceador, en ambos sentidos.
 - Interfaces de gestión del producto e información transmitida a través de ellas, en ambos sentidos.
 - Datos de configuración del producto y de auditoría generados por éste.
 - Actualizaciones del dispositivo susceptibles de afectar a su configuración y funcionalidad.

3.2 AMENAZAS

23. Las principales amenazas a las que el uso de esta familia de productos pretende hacer frente serían:
- **Divulgación de información no autorizada:** Un atacante ya sea desde dentro de la red o desde fuera consigue enviar información no autorizada de la red interna al exterior a través del dispositivo (p.ej.: direccionamiento IP de la red protegida o mapa de dispositivos de la red).
 - **Acceso no autorizado:** Un atacante ya sea desde dentro de la red o desde fuera consigue acceder a información intercambiada a través del dispositivo para la que no estaba autorizado (p.ej.: recibir información transmitida a través del dispositivo, pero no destinada a él) o utilizar el dispositivo como mecanismo de acceso a la red protegida.
 - **Envío de tráfico dañino:** Un atacante ya sea desde dentro de la red o desde fuera consigue eludir o inhabilitar las políticas de balanceo configuradas y/o enviar información no autorizada desde el exterior a la red interna a través del dispositivo (p.ej.: introducir información maliciosa de manera encubierta proveniente de la red externa).
 - **Cifrado débil:** Utilización en el dispositivo de algoritmos criptográficos débiles que permitan a un atacante comprometerlo, fundamentalmente mediante ataques de fuerza bruta.
 - **Uso de canales de comunicación inseguros:** Mala implementación de protocolos estándar o utilización de protocolos no estandarizados que permiten a un atacante comprometer la integridad y confidencialidad de las comunicaciones del dispositivo.
 - **Compromiso de la funcionalidad del dispositivo:** Un atacante o un fallo en el dispositivo compromete la funcionalidad de seguridad, incluyendo el

balanceo de carga y registro de actividad, permitiendo modificarla o desactivarla de manera no conforme a las políticas de seguridad (p.ej. instalación de actualizaciones maliciosas o administración no autorizada del dispositivo).

4. REQUISITOS FUNDAMENTALES DE SEGURIDAD (RFS)

24. 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 PERFIL DE PROTECCIÓN

25. **REQ. 1** Los productos deberán estar certificados con uno de los siguientes perfiles de protección certificados de acuerdo a la norma *Common Criteria*:

PERFILES DE PROTECCIÓN			
Perfil de protección	Versión	Fecha	Organismo responsable
<i>Collaborative Protection Profile for Network Devices v2.0 + Errata 20180314</i>	2.0	14/03/2018	CCDB
<i>Collaborative Protection Profile for Network Devices v2.1</i>	2.1	24/09/2018	CCDB

Tabla 2. Perfiles de protección

26. **REQ. 2** En caso de que el producto no esté certificado contra ningún perfil de los anteriores, la declaración de seguridad deberá contener al menos los SFR (Security Functional Requirements) del perfil *Collaborative Protection Profile for Network Devices. Version 2.1* con un nivel de confianza EAL (*Evaluation Assurance Level*) **EAL2 o superior**.

4.2 REQUISITOS CRIPTOGRÁFICOS

27. **REQ. 3** Todos los algoritmos de cifrado simétrico, asimétrico, protocolos de acuerdo de clave y funciones resumen que utilice el producto deberán encontrarse dentro de los acreditados por el CCN para su uso por sistemas de **categoría ALTA** bajo el alcance del ENS. El listado de dichos algoritmos se encuentra recogido en la *CCN-STIC-807 Criptología de empleo en el ENS*.

4.3 CONTROL DE LOS FLUJOS DE INFORMACIÓN

28. **REQ. 4** El producto debe tener la capacidad de conectarse a dos interfaces de red entre las que debe transmitir la información, identificando claramente, física y lógicamente, cada una de las redes.
29. **REQ. 6** El producto debe asegurar que el contenido de los datos (*payload*) del paquete no se modifica desde que entra por una interfaz hasta que sale por la otra.

30. **REQ. 7** El producto debe asegurar que el contenido de los datos (*payload*), una vez utilizados para su transmisión o recepción, deja de estar disponible y no se reutiliza.
31. **REQ.8** El producto debe ser capaz de mantener la coherencia en las comunicaciones para los flujos de información de entrada en la red protegida, recomponiendo las cabeceras del protocolo con los datos necesarios para que la comunicación sea viable y alcance al destinatario correcto dentro de la red interna.
32. **REQ.9** El producto debe permitir aplicar políticas de seguridad o restricciones aplicables a los flujos de información (p.ej.: volumen máximo de datos admitidos).

4.4 REQUISITOS DE BALANCEADOR

33. **REQ.10** El producto redistribuirá la carga (peticiones o conexiones) de acuerdo a un algoritmo definido (*Round Robin, Least Connection* u otro).
34. **REQ.11** El producto deberá ser capaz de procesar, sin pérdida de información, un ancho de banda mínimo declarado por el fabricante.
35. **REQ.12** El producto tendrá en cuenta criterios de salud de los servidores o de su canal de comunicación a la hora de asignar una petición al servidor que la recibirá y atenderá, para garantizar el buen funcionamiento de los servidores evitando su sobrecarga.

5. ABREVIATURAS

CC	<i>Common Criteria</i>
CCDB	<i>Common Criteria Development Board</i>
CCN	<i>Centro Criptológico Nacional</i>
CPSTIC	<i>Catálogo de Productos de Seguridad de las Tecnologías de Información y las Comunicaciones</i>
EAL	<i>Evaluation Assurance Level</i>
ENS	<i>Esquema Nacional de Seguridad</i>
HTTPS	<i>Hypertext Transfer Protocol Secure</i>
IEC	<i>International Electrotechnical Commission</i>
IP	<i>Internet Protocol</i>
ISO	<i>International Organization for Standardization</i>
NIAP	<i>National Information Assurance Partnership</i>
OSI	<i>Open System Interconnection</i>
RFS	<i>Requisitos Fundamentales de Seguridad</i>
SFR	<i>Security Functional Requirements</i>
WAF	<i>Web Application Firewall</i>