centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 140

Taxonomía de productos STIC Anexo C.2: Sistemas Honeypot/Honeynet

Agosto 2020

MINISTERIO DE DEFENSA

Edita:

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2020.08.10 10:10:03 +02'00'

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

ÍNDICE

1. INTRODUCCIÓN Y OBJETO

1. El presente documento describe los Requisitos Fundamentales de Seguridad (RFS) exigidos a un producto de la familia **Sistemas Honeypot/Honeynet** 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 **Sistemas Honeypot/Honeynet** 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 a ser el objetivo de ataques informáticos, de modo que la actividad desarrollada por un atacante sea monitorizada en un entorno preparado para ello, que permita recoger información de los patrones de ataque y de los atacantes y que resulte de utilidad para la protección de la organización que lo despliega.
7. Este tipo de herramientas cumplen una doble función, ya que permiten investigar el modus operandi de los ataques para así poder proteger los servicios de la organización de manera más efectiva, a la vez que sirven como un señuelo verosímil al atacante que desvíen su atención de otros sistemas realmente críticos de la organización, lo que ofrece la posibilidad de detectar y mitigar la amenaza antes de que progrese hasta ellos.
8. Los ***honeypot*** son sistemas informáticos que simulan una cierta funcionalidad (p.ej.: servicios web, bases de datos, servicios de red, etc.), preparados para registrar y alertar de la existencia de un ataque y, en ocasiones, para mantener algún tipo de interacción con el atacante que permita reunir mayor cantidad de información o ralentizar su avance logrando más tiempo de reacción.
9. Cuando el producto desplegado consiste en un sistema que, física o virtualmente, integra una red de herramientas y computadoras dedicadas en exclusiva a esta tarea se le denomina ***honeynet*.**
10. En este contexto las funciones básicas de seguridad que proporcionan esta familia de productos son las siguientes:

    - **Investigación de nuevas vulnerabilidades.** Los sistemas de protección se basan en medidas ya conocidas, pero resultan inútiles frente a las desconocidas. Gracias a los *honeypots*, es posible detectar nuevos vectores de ataque y vulnerabilidades y poder plantear medidas preventivas contra ellas (p. ej.: Detección de vulnerabilidades de tipo 0-days[1], nuevos *malwares*[2], etc.).

    - **Detección de atacantes y patrones de ataque.** Estos productos se exponen en un punto de la arquitectura de red de la organización para que puedan recibir ataques y así poder estudiar el comportamiento de los atacantes. El producto se puede asemejar a la configuración y/o topología de red de los servicios de la organización para permitir la monitorización y rastreo de los atacantes.

11. Estos productos no deben facilitar o contar con información relevante o sensible para la organización. De otro modo, el atacante podría extraer alguna

[1]Son aquellas que no disponen de soluciones que las neutralicen al desconocerse por el fabricante.
[2]Todo tipo de programas dañino como por ejemplo virus, gusanos, troyanos, etc.

información útil para sus fines o que le proporcione inteligencia de cara al reconocimiento e intrusión en las redes protegidas.

12. Los productos incluidos en esta familia pueden ofrecer otras funcionalidades complementarias no específicamente contempladas en este documento.

2.2 CASOS DE USO

13. En el caso de los productos de esta familia se contemplan tres casos de uso, todos ellos enfocados a recopilar información sobre ataques y atacantes. A continuación, se exponen brevemente cada uno de los casos contemplados.

2.2.1. CASO DE USO 1 – CREACIÓN DE LISTAS NEGRAS DE ACCESO

14. El producto se sitúa detrás o delante de la primera barrera de protección de la organización y en un rango de red donde no se espera tráfico corporativo. De este modo, todo el tráfico que llega al producto se puede considerar sospechoso. Posteriormente, una vez analizadas, las direcciones de red capturadas se introducen en los dispositivos de protección para que éstos filtren automáticamente cualquier tráfico con ese origen, impidiendo su progresión.

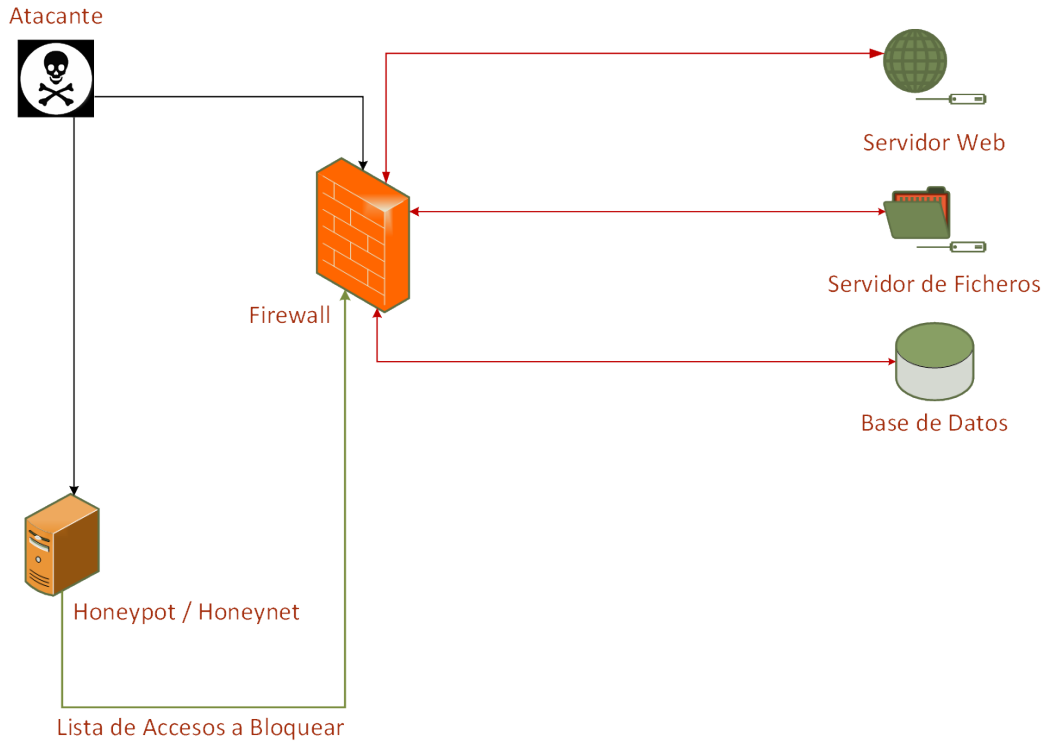

Figura 1. Ejemplo de Caso de Uso 1: Creación de Listas Negras de Accesos

2.2.2. CASO DE USO 2 – COMPLEMENTO DE IDS/IPS

15. La utilización de este producto en conjunto con un IDS/IPS (Dispositivos de prevención y detección de intrusiones) permite conseguir información más

relevante sobre los incidentes, lo que facilita descartar falsos positivos y hacer llegar a los analistas sólo información relevante.

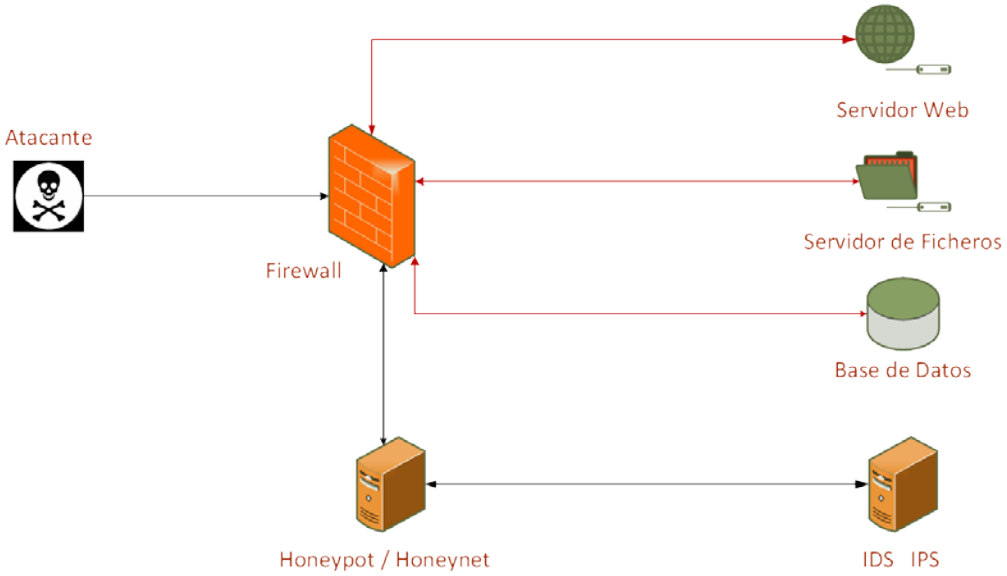

Figura 2. Ejemplo de Caso de Uso 2: Complemento de IDS/IPS

2.2.3. CASO DE USO 3 – REPLICACIÓN DE SERVICIO

16. Se utiliza un producto honeypot para replicar un servicio concreto de la arquitectura de red de la organización. Si el producto es atacado, comprometido y utilizado para realizar un mapeo y reconocimiento de la arquitectura de red y los servicios de la organización, la detección es mucho más fácil que mediante el uso de otros dispositivos (p. ej.: Firewalls) que pueden identificar erróneamente el tráfico generado por el equipo comprometido como tráfico de red.

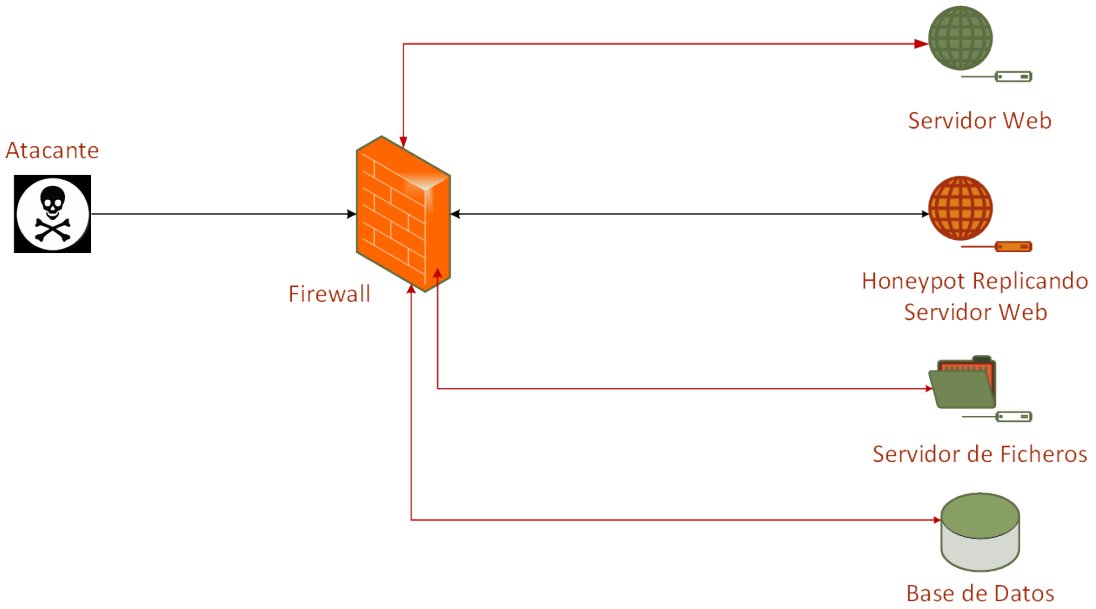

Figura 3. Ejemplo de Caso de Uso 3: Replicación de Servicio

2.3 ENTORNO DE USO

17. Esta familia de productos es utilizada en grandes organizaciones como parte de una arquitectura de defensa en profundidad, coexistiendo por tanto con otros sistemas de seguridad, con la finalidad de proteger los sistemas TIC y la información de la organización manejada en ellos, fundamentalmente frente a atacantes externos.

18. Para la utilización en condiciones óptimas de seguridad de estos productos, es necesaria su integración en un entorno operacional que cumpla las siguientes condiciones mínimas de protección:

    - **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.
    - **Actualizaciones periódicas**. El producto será puesto al día conforme aparezcan actualizaciones que corrijan vulnerabilidades conocidas.
    - **Protección de las comunicaciones.** Deberán habilitarse los mecanismos necesarios que permitan una comunicación segura entre los productos y las redes bajo control de la organización a las que estos se conecten (p.ej.: terminadores VPN[3], puntos de acceso WLAN[4] seguros, etc.). Esta medida es fundamental si el producto necesita administración remota debido a su naturaleza de producto destinado a permitir ataques.
    - **Segregación de red**. La red en la que se despliegue el producto debería estar segregada de otras redes que contengan información sensible o servicios protegidos de la organización, de modo que un posible incidente de seguridad en el producto quede contenido dentro del segmento en el que se encuentra ubicado.
    - **Política de seguridad de la información.** La política de seguridad deberá recoger 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. Esta política debería recoger las restricciones de uso de estos productos dentro del marco legal y los límites en la información organizativa que exponen.

2.4 DELIMITACIÓN DEL ALCANCE DEL DISPOSITIVO

19. Este tipo de productos se presentan en formato de paquete Software, generalmente instalado sobre equipamiento Hardware en forma de servidor dedicado a proporcionar esta funcionalidad, debiendo tener la capacidad de soportar y manejar multitud de conexiones simultáneas ya que actúan como

[3] *Virtual Private Network*. Red Privada Virtual
[4] *Wireless Local Area Network*. Red de área local inalámbrica

señuelos frente a los atacantes y se pretende recabar la máxima información de ellos, estudiando su comportamiento dentro del sistema.

20. Los entornos o servicios emulados por el producto, así como cualquier otra funcionalidad adicional a las definidas en la sección 2.1 quedan fuera del alcance analizado, debiendo ser evaluados conforme a los RFS específicos aplicables en caso de considerarse oportuno.

2.5 ALINEAMIENTO CON CRITERIOS COMUNES (COMMON CRITERIA)

21. El estándar *Common Criteria* (CC) proporciona un conjunto común de requisitos funcionales y de aseguramiento para la evaluación de los productos de TIC (Tecnologías de la Información y de las Comunicaciones).

22. 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.

23. 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.

24. 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.

25. 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. ANÁLISIS DE AMENAZAS

3.1 RECURSOS QUE ES NECESARIO PROTEGER

26. Aunque estos productos no representan un recurso de protección real en sí mismos, si no que se utilizan como señuelos para estudiar ataques y a sus actores, tienen el propósito final de proteger los usuarios y servicios reales de las redes de la organización, a partir de la información descubierta mediante su uso.

27. Debe tenerse en consideración que los mecanismos de protección y los recursos a proteger dentro del alcance de este documento se centran en la funcionalidad y administración del propio producto, no de los entornos o servicios que emulen para lograr su finalidad, e incluyen:

    - Información sensible que pueda almacenar el producto en su configuración o en el dispositivo hardware donde haya sido desplegado.
    - Interfaces de gestión del producto y la 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

28. Como se menciona en el punto anterior, un producto de esta familia se concibe con la premisa de estar expuesto a ataques, pero esto no implica que el producto en su conjunto no deba protegerse frente a determinadas amenazas como las definidas a continuación. En particular, el producto contará con funcionalidades o interfaces relacionadas con su administración y configuración que podrían ser explotadas por una amenaza, provocando un incidente que vaya más allá del caso de uso para el que se concibe el producto y que ponga en riesgo otros sistemas a proteger dentro de la organización. Las principales amenazas deliberadas serían:

    - **Divulgación de información no autorizada:** Un atacante consigue recopilar información no autorizada del producto o de los servicios/redes a los que emula, resultando útil para comprometer las redes protegidas de la organización (p.ej. servicios reales de la organización, configuraciones de red interna, etc.).
    - **Escucha de red:** Un atacante consigue infiltrarse hasta un punto de conexión de la infraestructura de red. El atacante puede supervisar y obtener acceso a la comunicación y/o los datos intercambiados (p.ej. credenciales de usuarios) entre el producto y otros puntos finales de la red corporativa que no son los escogidos de forma deliberada para el estudio de los ataques.

- **Acceso no autorizado**: Un atacante consigue acceder a información en el producto para la que no estaba autorizado, más allá de la expuesta intencionadamente como señuelo (p.ej.: información sobre credenciales de administración del producto o registros generados).
- **Cifrado débil**: Utilización en el producto de algoritmos criptográficos débiles que permitan a un atacante comprometerlo, más allá de los expuestos intencionadamente como señuelo, fundamentalmente mediante ataques de fuerza bruta (p.ej. contra sus interfaces de administración).
- **Uso de canales de comunicación inseguros**: Mala implementación de protocolos estándar o utilización de protocolos no estandarizados, más allá de los expuestos intencionadamente como señuelo, que permiten a un atacante comprometer la integridad y confidencialidad de las comunicaciones del producto.
- **Compromiso de la funcionalidad del producto**: Un atacante o un fallo en la herramienta compromete la funcionalidad de seguridad, permitiendo modificarla o desactivarla de manera no conforme a las políticas de seguridad (p.ej.: instalación de actualizaciones dañinas o administración no autorizada de la herramienta).

4. REQUISITOS FUNDAMENTALES DE SEGURIDAD (RFS)

29. 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

30. **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**
Collaborative Protection Profile for Network Devices[5]	2.2e	27/03/2020	CCDB
Collaborative Protection Profile for Network Devices[6]	2.1	24/09/2018	CCDB
Collaborative Protection Profile for Network Devices[7]	2.0 + Errata 20180314	14/03/2018	CCDB
Collaborative Protection Profile for Network Devices.[8]	1.0	27/02/2015	CCDB

Tabla 1. Perfiles de protección

31. **REQ. 2** En caso de que el producto no esté certificado contra ninguno de los perfiles anteriores, la declaración de seguridad deberá contener al menos los SFR (*Security Functional Requirements*) de *Collaborative Protection Profile for Network Devices V.2.2e* con un nivel de confianza EAL (*Evaluation Assurance Level*) **EAL2 o superior.**

4.2 PROTECCIÓN DE LOS DATOS DE USUARIO

32. **REQ. 3** El producto permitirá anonimizar o desvirtuar la información expuesta cuando ésta sea clonada o importada, ya sea de servicios como de configuraciones de red reales de la organización (p.ej. direccionamiento IP, usuarios, contenidos, etc.).

[5] https://www.commoncriteriaportal.org/files/ppfiles/CPP_ND_V2.2E.pdf
[6] https://www.commoncriteriaportal.org/files/ppfiles/CPP_ND_V2.1.pdf
[7] https://www.commoncriteriaportal.org/files/ppfiles/CPP_ND_V2.0E.pdf
[8] https://www.commoncriteriaportal.org/files/ppfiles/CPP_ND_V1.0.pdf

33. **REQ. 4** El producto no requerirá de interfaces con servicios ubicados en redes protegidas de la organización (p.ej. acceso a bases de datos en producción) para desempeñar su funcionalidad.

34. **REQ. 5** El producto debe ser capaz de aportar evidencias de la integridad de todos los datos recopilados (intentos de acceso, ficheros de registro de eventos, etc.).

4.3 AUDITORÍA Y REGISTROS DE SEGURIDAD

35. **REQ. 6** El producto debe proporcionar una forma de acceso legible a los registros de auditoría para facilitar su revisión a los usuarios autorizados.

36. **REQ. 7** El producto debe generar un informe de error en caso de un problema acaecido, que incluya la máxima información posible.

4.4 PROTECCIÓN DEL DISPOSITIVO Y SUS SERVICIOS

37. **REQ. 8** El producto no facilitará ningún tipo de información comercial o publicitaria accesible a un atacante que permita identificar su condición como producto *honeypot/ honeynet*.

5. ABREVIATURAS

CC	*Common Criteria*
CCDB	*Common Criteria Development Board*
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*
HTTPS	*Hypertext Transfer Protocol Secure*
RFS	*Requisitos Fundamentales de Seguridad*
VPN	*Virtual Private Network*
WLAN	*Wireless Local Area Network*