GOBIERNO DE ESPAÑA
MINISTERIO DE LA PRESIDENCIA Y PARA LAS ADMINISTRACIONES TERRITORIALES

CCN Centro Criptológico Nacional

Guía de Seguridad de las TIC
CCN-STIC 140

Taxonomía de referencia para productos de seguridad TIC - Anexo C.1: Dispositivos de Prevención/Detección de Intrusiones

Noviembre 2017

Edita:

GOBIERNO DE ESPAÑA
MINISTERIO DE LA PRESIDENCIA Y PARA LAS ADMINISTRACIONES TERRITORIALES

CCN Centro Criptológico Nacional

CENTRO CRIPTOLOGICO NACIONAL
2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, cn=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2017.11.27 11:18:26 +01'00'

NIPO: 785-17-037-2.

Fecha de Edición: noviembre 2017

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 4

2. DESCRIPCIÓN DE LA FAMILIA DE PRODUCTOS 5

2.1 FUNCIONALIDAD 5

2.2 CASO DE USO 6

2.2.1. CASO DE USO 1 6

2.2.2. CASO DE USO 2 6

2.2.3. CASO DE USO 3 7

2.3 ENTORNO DE USO 7

2.4 DELIMITACIÓN DEL ALCANCE DEL DISPOSITIVO 8

2.5 ALINEAMIENTO CON CRITERIOS COMUNES (COMMON CRITERIA) 9

3. 3ANÁLISIS DE AMENAZAS 10

3.1 RECURSOS QUE ES NECESARIO PROTEGER 10

3.2 AMENAZAS 10

4. REQUISITOS FUNDAMENTALES DE SEGURIDAD (RFS) 12

4.1 PERFIL DE PROTECCIÓN 12

4.2 REQUISITOS CRIPTOGRÁFICOS 12

4.3 AUDITORÍA Y REGISTROS DE SEGURIDAD 12

4.4 PREVENCIÓN DE INTRUSIÓN 13

4.4.1. DETECCIÓN Y ANÁLISIS 13

4.4.2. REACCIÓN 14

5. ABREVIATURAS 15

1. INTRODUCCIÓN Y OBJETO

1. El presente documento describe los Requisitos Fundamentales de Seguridad (RFS) exigidos a un producto de la familia **Dispositivos de prevención de intrusiones** 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 **Dispositivos de prevención de intrusiones** 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 dispositivos de prevención de intrusiones (*IPS*[1]) son productos cuya funcionalidad principal es la de monitorizar a una o más redes con objeto de detectar el tráfico potencialmente dañino y reaccionar ante estos ataques. Esta funcionalidad pueden implementarla de manera independiente y/o en conjunción con otros componentes de red que formen parte de soluciones empresariales mayores.

7. Por ejemplo, aunque todos los IPS deben tener capacidad de monitorizar, analizar y reaccionar a tráfico de red, también podrán:

   - Monitorizar todo el tráfico de red detectado pasivamente por uno o más interfaces, y/o monitorizar solo determinados flujos de tráfico que pasan a través del IPS para ser inspeccionados.
   - Transmitir datos del IPS a un servidor de auditoría externo y (opcionalmente) almacenar datos internamente.
   - Analizar tráfico de red basado en reglas que el administrador puede configurar localmente y (opcionalmente) basado en reglas importadas/aplicadas desde un sistema externo.
   - Reaccionar de forma independiente a tráfico potencialmente malicioso (bloqueando flujos de tráfico o transmitiendo reinicios de sesión a los puntos finales o *endpoints*), y (opcionalmente) reaccionar en colaboración con componentes externos incluidos en la solución global de la empresa.

8. El análisis de tráfico podría estar basado en identificación de amenazas conocidas o desconocidas. La identificación conocida puede ser implementada mediante la comparación de patrones, comparando cadenas de caracteres dentro de un paquete *IP*[2], mediante reconocimiento de patrones de tráfico comunes o detectando ataques de denegación de servicio.

9. La identificación de amenazas desconocidas puede ser desarrollada mediante uso de varias formas de detección anormal que consisten en dotar al IPS con patrones de tráfico típicos o esperados con objeto de que sea capaz de detectar y reaccionar ante patrones de tráfico anómalos (no esperados o atípicos).

10. Por último, es importante destacar que, aunque existen numerosas similitudes entre los IPS y los sistemas de detección de intrusión (*IDS*[3]), también existen notables diferencias. La más importante de ellas es que el IDS se limita a generar un evento de auditoría u otra alerta cuando detecta un flujo de tráfico malicioso, mientras que el IPS debe ser capaz de iniciar una respuesta proactiva

[1] *IPS Intrusion Prevention System*
[2] *IP*: *Internet Protocol*
[3] *IDS: Intrusion Detection System*

para terminar/interrumpir una amenaza potencial, así como causar la interrupción en tiempo real de los flujos de tráfico sospechosos.

2.2 CASO DE USO

11. Aunque el administrador del dispositivo pueda configurarlo de manera que las respuestas proactivas no estén activadas y desplegarlo solo con las funcionalidades de IDS, estos RFS aplicarán siempre a los casos en los que actúe como IPS.
12. Dependiendo de las funcionalidades del producto explotadas y de la finalidad o el contexto en que se utilicen, se contemplan tres casos de uso para esta familia de productos tal como se definen a continuación.

2.2.1. CASO DE USO 1

13. El IPS está operando en **modo promiscuo**[4]. Captura datos de dos redes separadas, los analiza y envía actualizaciones de filtros de tráfico a los dispositivos de protección de perímetro (enrutador y cortafuegos o *firewall*) para que bloqueen el tráfico no deseado en tiempo real.

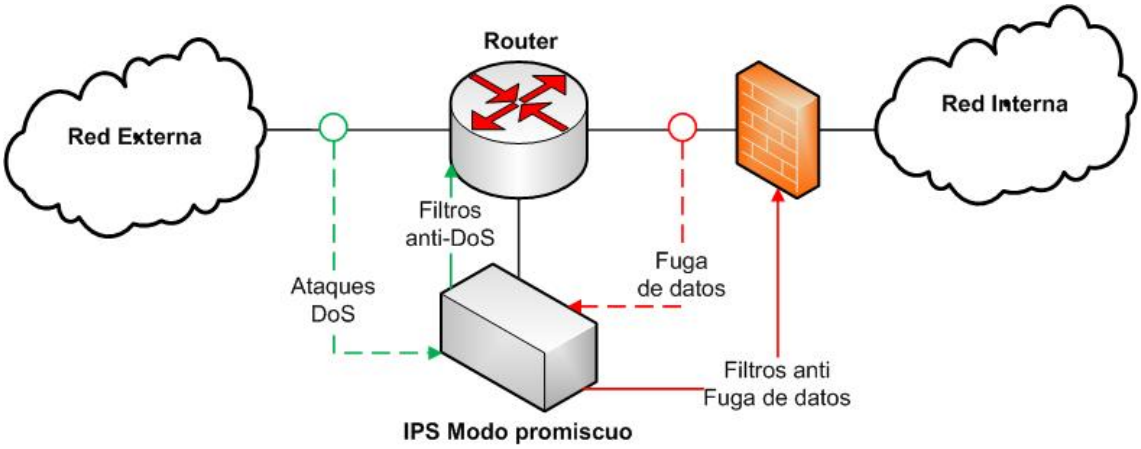

Figura 1-IPS trabajando en modo promiscuo

2.2.2. CASO DE USO 2

14. El IPS opera en **modo en línea**. Analiza tráfico desde o hacia una red inalámbrica y bloquea en tiempo real el tráfico que viole las políticas definidas por el administrador del IPS.

[4] Un interfaz de red que captura todos los paquetes que pasan por la red a la que está conectada, aunque no estén dirigidos a él.

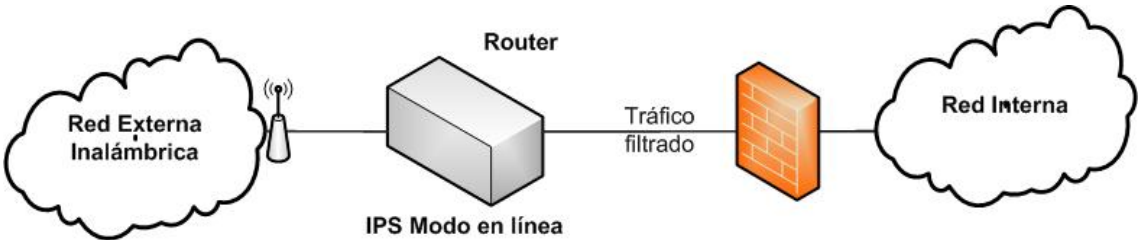

Figura 1 IPS trabajando en modo en línea

2.2.3. CASO DE USO 3

15. El IPS está operando en una **combinación de modo promiscuo y modo en línea**. Tiene al menos un par de interfaces que crean un puente *(bridge)* o enrutador que analiza y filtra en tiempo real el tráfico que lo atraviesa. Además, el mismo IPS tiene uno o más interfaces promiscuos recogiendo y analizando tráfico que circula por cada red separada y reaccionando a actividad anormal, gusanos u otra actividad no aprobada.

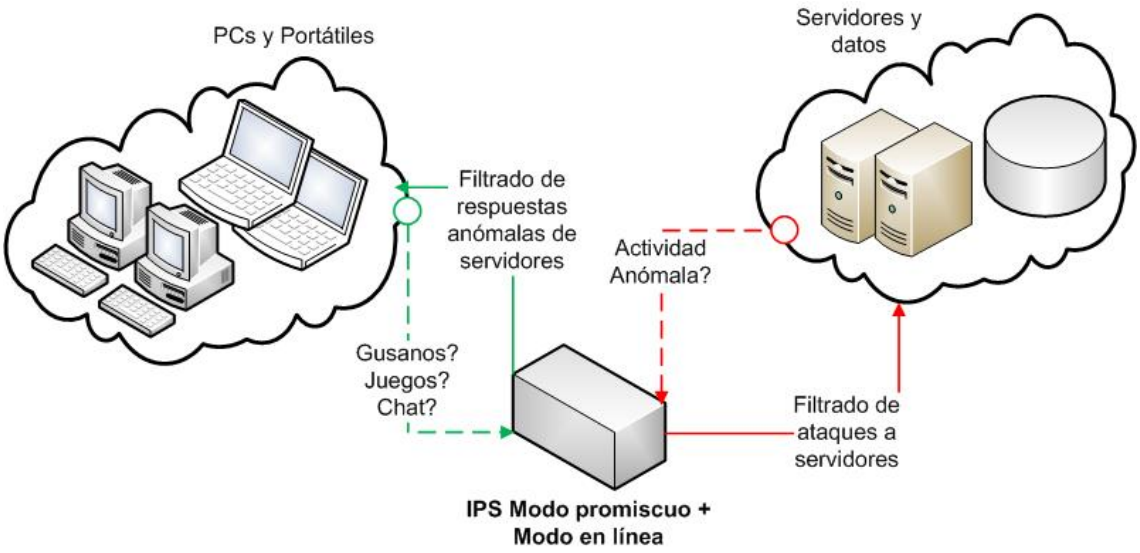

Figura 2 IPS trabajando en modo promiscuo y en línea

2.3 ENTORNO DE USO

16. Este tipo de dispositivos son de uso generalizado, tanto en el ámbito del sector público como en el privado, debido a su importancia en la mejora de la seguridad de redes, en combinación con otras medidas complementarias.
17. Para la utilización en condiciones óptimas de seguridad de los IPS, es necesario que se integre 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 software del producto será 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.
- **Política de seguridad de la información:** Una 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.

2.4 DELIMITACIÓN DEL ALCANCE DEL DISPOSITIVO

18. Los productos para los que serían de aplicación estos RFS son aquellos que inspeccionan tráfico IP (TCP[5], UDP[6], ICMP[7], etc.) y protocolos basados en IP (GRE[8], ESP[9], AH[10]).
19. No se incluyen dentro del alcance otros IPS que incluyan escáner, analizadores, sensores, etc. Ni la evaluación de otros protocolos no-IP incluyendo protocolos nivel 2 (enlace de datos) o Ethernet.
20. Además, los RFS definidos son aquellos que se consideran necesarios para un producto de prevención de intrusión, al margen de aquellas funcionalidades que pueda dar en conjunción con otros dispositivos de soluciones empresariales mayores.
21. En caso de que el IPS sea un producto distribuido a lo largo de toda la red IP el perímetro del dispositivo deberá dibujarse como la suma de todos sus componentes.

[5] *Transmission Control Protocol*. Protocolo de Control de Transmisión
[6] *User Datagram Procotol.* Protocolo de nivel de transporte de datagramas
[7] *Internet Control Message Protocol.* Protocolo de mensajes de control de Internet
[8] *Generic Routing Encapsulation* es un protocolo para el establecimiento de túneles a través de Internet
[9] *Encapsulating Security Payload*. Carga de seguridad encapsulada. Proporciona autenticidad de origen, integridad y confidencialidad de un paquete
[10] *Authentication Header*. Encabezamiento de autenticación

2.5 ALINEAMIENTO CON CRITERIOS COMUNES (COMMON CRITERIA)

22. 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).

23. 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.

24. Los productos dentro de esta familia deberán cumplir con los requisitos Fundamentales de Seguridad reflejados en el apartado 4 y con los SFR (*Security Functional Requirements*) que se especifican en alguno 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.[11]	1.0	27/02/2015	CCDB
Protection Profile for Network Devices.[12]	1.1	08/06/2012	NIAP

Tabla 1. Perfiles de protección

25. 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** para los RFS adicionales que no encuentren incluidos dentro de un perfil.
- **EAL2 o superior** en el caso en el que el producto no se encuentre certificado contra ningún perfil.

[11] https://www.commoncriteriaportal.org/files/ppfiles/CPP_ND_V1.0.pdf
[12] https://www.commoncriteriaportal.org/files/ppfiles/PP_ND_V1.1.pdf

3. ANÁLISIS DE AMENAZAS

3.1 RECURSOS QUE ES NECESARIO PROTEGER

26. Los recursos que es necesario proteger mediante el uso de esta familia de productos, incluyen:

- Información que atraviese el producto entre sus interfaces de red.
- 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.
- Información almacenada en el dispositivo.
- Actualizaciones del dispositivo susceptibles de afectar a su configuración y funcionalidad.

3.2 AMENAZAS

27. Las principales amenazas a las que el uso de esta familia de productos pretende hacer frente, atendiendo a los casos de uso expuestos en la sección **¡Error! No se encuentra el origen de la referencia.**, serían:

- **Ataques de denegación de servicio.** Lo que implicaría obstruir el funcionamiento normal de la red monitorizada por el dispositivo.
- **Divulgación de información no autorizada**. Un atacante consigue recopilar:
  - Información relativa a la configuración de la red. Sondeando la información sobre la red monitorizada o sus puntos finales o *endpoints,* mediante el uso de escaneados o técnicas de mapeo.
  - Datos de usuario que circulen por la red o que se encuentren almacenados en el dispositivo.
- **Acceso no autorizado.** Un atacante consigue, a través de ataques de fuerza bruta o de código dañino, el acceso no autorizado a información intercambiada a través del dispositivo o a los recursos y servicios de la red(es) monitorizada(s).
- **Envío de tráfico malicioso.** Un atacante consigue enviar información a través del dispositivo de manera malintencionada, con el fin de poner en riesgo la seguridad de éste o de aquellos otros recursos a los que protege.
- **Compromiso de la funcionalidad del dispositivo.** Un atacante o un fallo en el dispositivo compromete la funcionalidad de seguridad, influyendo en su 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).

28. Un atacante que quisiera comprometer estos dispositivos, atendiendo al entorno de uso en el que se concibe su implementación conforme a la sección **¡Error! No se encuentra el origen de la referencia.**, requeriría:

- Una cantidad arbitraria de tiempo para analizar los flujos de información intercambiados a través del dispositivo.
- Acceso a unidades del dispositivo donde llevar a cabo pruebas/intentos de ataque, o al propio dispositivo una vez instalado.
- Equipamiento comercial/abierto y conocimiento de su uso (p.ej. herramientas de análisis de red, de explotación de vulnerabilidades, etc.).

4. REQUISITOS FUNDAMENTALES DE SEGURIDAD (RFS)

4.1 PERFIL DE PROTECCIÓN

29. **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.[13]	1.0	27/02/2015	CCDB
Protection Profile for Network Devices.[14]	1.1	08/06/2012	NIAP

Tabla 2. Perfiles de protección

30. **REQ. 2** En caso de que 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.1.0* con un nivel de confianza EAL (Evaluation Assurance Level) **EAL2 o superior**.

4.2 REQUISITOS CRIPTOGRÁFICOS

31. **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 en el ENS. El listado de dichos algoritmos se encuentra recogido en la CCN-STIC-807 (Categoría ALTA).

4.3 AUDITORÍA Y REGISTROS DE SEGURIDAD

32. **REQ. 4** El IPS generará un evento de auditoría, como mínimo, en los siguientes casos:

    - Inicio y finalización de las funciones de IPS.
    - Cuando se produzca un evento diferenciado con respecto al resto. Se guardará junto con un sello temporal.
    - Cuando se produzca una reacción del IPS diferenciada con respecto al resto. Se guardará junto con un sello temporal.

[13] https://www.commoncriteriaportal.org/files/ppfiles/CPP_ND_V1.0.pdf
[14] https://www.commoncriteriaportal.org/files/ppfiles/PP_ND_V1.1.pdf

- Cuando se produzcan un conjunto de eventos similares. Se guardará la descripción del evento junto con el número de ocurrencias y el período de tiempo en el que ocurrieron.
- Cuando se produzcan un conjunto de reacciones similares. Se guardará la descripción de la reacción junto con el número de ocurrencias y el período de tiempo en el que ocurrieron.

33. **REQ. 5** Entre los eventos considerados como auditables estarán, entre otros:
    - Modificación de política de IPS.
    - Tráfico inspeccionado que coincida con la política basada en anomalías del IPS.
    - Trafico inspeccionado que coincida con listas blancas y negras de direcciones IP.
    - Modificación de los interfaces asociados a cada política.
    - Tráfico inspeccionado que coincida con la política basada en firma.
34. **REQ. 6** Deberá permitir el filtrado y ordenación de los registros de auditoría.
35. **REQ. 7** Los datos de auditoría deberán presentarse en un formato legible para el administrador.

4.4 PREVENCIÓN DE INTRUSIÓN

4.4.1. DETECCIÓN Y ANÁLISIS

36. **REQ. 8** El producto deberá soportar la definición de patrones de tráfico esperados y aprobados, anomalías, así como la descripción de la actividad de cada anomalía.
37. **REQ. 9** El producto deberá permitir la descripción de la actividad de las anomalías.
38. **REQ. 10** Permitirá la creación de listas blancas y negras de direcciones IP.
39. **REQ. 11** Permitirá a los administradores configurar elementos de la política de IPS como listas blancas y negras de direcciones, de reglas, etc.
40. **REQ. 12** El producto desarrollará un análisis del tráfico de red basado en IP y detectará violaciones de las políticas definidas por el administrador del IPS. Este tráfico podrá implementar los siguientes protocolos: IPv4, IPv6, ICMPv4, ICMPv6, TCP, UDP.
41. **REQ. 13** Tendrá la capacidad de inspeccionar el contenido de las cabeceras de paquetes/unidades de datos IPv4, IPv6, ICMPv4, ICMPv6, TCP, UDP.

4.4.2. REACCIÓN

42. **REQ. 14** Ante la detección de un tráfico potencialmente dañino, el IPS deberá reaccionar permitiendo las siguientes operaciones, asociadas a una política IPS basada en anomalías:

    - Permitir el tráfico.
    - Enviar una instrucción de reinicio (*reset*) de la conexión TCP a la dirección origen del tráfico detectado.
    - Enviar una instrucción de reinicio de la conexión TCP a la dirección destino.
    - Enviar un mensaje ICMP de “destino no alcanzable”.
    - Enviar un mensaje a otro dispositivo de red para que bloquee el tráfico dañino.

5. ABREVIATURAS

AH	*Authentication Header*
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*
ESP	*Encapsulating Security Payload*
GRE	*Generic Routing Encapsulation*
ICMP	*Internet Control Message Protocol*
IDS	*Intrusion Detection System*
IP	*Internet Protocol*
IPS	*Intrusion Prevention System*
NIAP	*National Information Assurance Partnership*
RFS	*Requisitos Fundamentales de Seguridad*
TCP	*Transmission Control Protocol*
UDP	*User Datagram Procotol*
VPN	*Virtual Private Network*