

Guía de Seguridad de las TIC

CCN-STIC 811

Interconexión en el ENS



Octubre 2017

Edita:



© Centro Criptológico Nacional, 2017

NIPO: 785-17-052-9

Fecha de Edición: octubre de 2017

José Antonio Mañas ha participado en la realización y modificación del presente documento y sus anexos.

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.

PRÓLOGO

El uso masivo de las tecnologías de la información y la comunicación (TIC), en todos los ámbitos de la sociedad, ha creado un nuevo espacio, el ciberespacio, donde se producirán conflictos y agresiones, y donde existen ciberamenazas que atentarán contra la seguridad nacional, el estado de derecho, la prosperidad económica, el estado de bienestar y el normal funcionamiento de la sociedad y de las administraciones públicas.

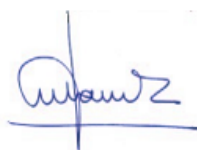
La Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia (CNI), encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información en su artículo 4.e), y de protección de la información clasificada en su artículo 4.f), a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional (CCN) en su artículo 9.2.f).

Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través de su Centro Criptológico Nacional, regulado por el Real Decreto 421/2004, de 12 de marzo, diversas actividades directamente relacionadas con la seguridad de las TIC, orientadas a la formación de personal experto, a la aplicación de políticas y procedimientos de seguridad, y al empleo de tecnologías de seguridad adecuadas.

El Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (ENS, en adelante), al que se refiere el apartado segundo del artículo 156 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, establece la política de seguridad en la utilización de medios electrónicos que permita una protección adecuada de la información.

Precisamente el Real Decreto 3/2010 de 8 de Enero, modificado por el Real Decreto 951/2015, de 23 de octubre, fija los principios básicos y requisitos mínimos así como las medidas de protección a implantar en los sistemas de la Administración, y promueve la elaboración y difusión de guías de seguridad de las tecnologías de la información y la comunicación (STIC) por parte de CCN para facilitar un mejor cumplimiento de dichos requisitos mínimos.

En definitiva, la serie de documentos CCN-STIC se elabora para dar cumplimiento a los cometidos del Centro Criptológico Nacional y a lo reflejado en el Esquema Nacional de Seguridad, conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo su difícil, y en ocasiones, ingrata tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.



Octubre de 2017

Félix Sanz Roldán
Secretario de Estado
Director del Centro Criptológico Nacional

ÍNDICE

1. INTRODUCCIÓN.....	5
2. OBJETO	6
3. ALCANCE	6
4. ASPECTOS GENERALES.....	6
5. PRINCIPIOS BÁSICOS	7
6. ACUERDO DE SEGURIDAD DE LA INTERCONEXIÓN	7
7. ARQUITECTURA DE PROTECCIÓN PERIMETRAL (APP)	8
7.1. CAPAS OSI.....	8
7.2. ENRUTADORES (<i>ROUTERS</i>)	9
7.3. CORTAFUEGOS (<i>FIREWALLS</i>).....	9
7.4. INTERMEDIARIOS (<i>PROXIES</i>)	10
7.5. PASARELAS DE INTERCAMBIO SEGURO	11
7.6. DIODOS DE DATOS	12
8. TIPOS DE ARQUITECTURAS DE PROTECCIÓN DE PERÍMETRO	13
8.1. ARQUITECTURA DE PROTECCIÓN DE PERÍMETRO DE TIPO 1 (APP-1).....	13
8.2. ARQUITECTURA DE PROTECCIÓN DE PERÍMETRO DE TIPO 2 (APP-2).....	14
8.3. ARQUITECTURA DE PROTECCIÓN DE PERÍMETRO DE TIPO 3 (APP-3).....	14
8.4. ARQUITECTURA DE PROTECCIÓN DE PERÍMETRO DE TIPO 4 (APP-4).....	15
8.5. ARQUITECTURA DE PROTECCIÓN DE PERÍMETRO DE TIPO 5 (APP-5).....	16
8.6. ARQUITECTURA DE PROTECCIÓN DE PERÍMETRO DE TIPO 6 (APP-6).....	17
8.7. ARQUITECTURA DE PROTECCIÓN DE PERÍMETRO DE TIPO 7 (APP-7).....	17
9. DESPLIEGUE	18
9.1. SERVIDORES Y SERVICIOS EN LA FRONTERA.....	18
9.2. GARANTÍAS DE DISPONIBILIDAD.....	19
9.3. FRONTERA COMPARTIDA.....	19
9.4. REDES PRIVADAS VIRTUALES	20
9.5. EQUIPOS REMOTOS	21
10. REQUISITOS DEL ENS SOBRE ARQUITECTURAS DE PROTECCIÓN DE PERÍMETRO	22
11. HERRAMIENTAS DE SEGURIDAD	22
11.1. DETECCIÓN DE CÓDIGO DAÑINO.....	22
11.2. ANÁLISIS DE VULNERABILIDADES	23
11.3. ANÁLISIS DE REGISTROS DE ACTIVIDAD	23
11.4. DETECCIÓN Y PREVENCIÓN DE INTRUSIÓN (IDS/IPS)	23
11.5. MONITORIZACIÓN DE TRÁFICO	23
11.6. PREVENCIÓN DE FUGA DE DATOS (DLP).....	24
11.7. VERIFICACIÓN DE LA CONFIGURACIÓN	24
12. REQUISITOS DEL ENS SOBRE HERRAMIENTAS DE SEGURIDAD	24
ANEXO A. GLOSARIO DE TERMINOS Y ABREVIATURAS	27
ANEXO B. BIBLIOGRAFÍA DE REFERENCIA.....	28

1. INTRODUCCIÓN

1. En los últimos años hemos asistido a un desarrollo sin precedentes en la sociedad de la información, la generalización de las conexiones de banda ancha y la cada vez mayor alfabetización digital han contribuido a un nuevo escenario donde el ciudadano demanda facilidad y flexibilidad de acceso a los servicios prestados por el sector público.
2. Esta guía se encuadra dentro de los requisitos del artículo 22 (Prevención ante otros sistemas de información interconectados), del Real Decreto 3/2010 de 8 de enero, por el que se regula el Esquema Nacional de Seguridad (ENS) en el ámbito de la Administración Electrónica, y su modificación mediante el Real Decreto 951/2015, de 23 de octubre según lo previsto en el apartado segundo del artículo 156 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público y la Instrucción Técnica de Seguridad de Interconexión de Sistemas de Información¹.
3. Esta guía será de uso para los sistemas de información comprendidos en los ámbitos subjetivo y objetivo de aplicación según dispone el artículo 3 del Real Decreto 3/2010 de 8 de enero, del ENS, así como al resto de las entidades que forman parte de los ámbitos subjetivos de aplicación de la Ley 39/2015, de 1 de octubre, de Procedimiento Administrativo Común de las Administraciones Públicas, y la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
4. Estas leyes reconocen el derecho de los ciudadanos a relacionarse con las administraciones públicas electrónicamente y la obligación de las mismas de garantizar este derecho, planteando a su vez un importante desafío a nivel tecnológico para los diferentes organismos, que han visto aumentar la complejidad de sus sistemas a la par que las interrelaciones y conexiones con otras entidades.
5. La finalidad del Esquema Nacional de Seguridad es la creación de las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos, que permita a los ciudadanos y a las Administraciones públicas, el ejercicio de derechos y el cumplimiento de deberes a través de estos medios. La manera y forma en que los sistemas de los diferentes organismos del sector público se interconectan debe adecuarse a este nuevo marco de trabajo y es en esta función en la que esperamos esta guía sirva de ayuda.
6. Precisamente el artículo 22 del ENS, establece la obligatoriedad de proteger el perímetro de los sistemas a interconectar, en particular si se utilizan redes públicas, total o parcialmente, y de analizar los riesgos derivados de la interconexión de los sistemas, controlando además su punto de unión.
7. Esta guía pretende ayudar a los responsables involucrados en la interconexión de sistemas a los que sea de aplicación el Esquema Nacional de Seguridad.

¹ Por Resolución del Secretario de Estado de Función Pública (pendiente de publicación)

2. OBJETO

8. El objeto de esta guía es analizar los elementos disponibles para interconectar sistemas afectados por el Esquema Nacional de Seguridad a otros sistemas, adscritos o no al ENS, con referencia a la Instrucción Técnica de Seguridad de Interconexión de sistema de información.
9. El objetivo de establecer un perímetro de seguridad es siempre proteger los flujos de información entre el sistema de información propio y el sistema al que queremos conectarnos. En base a unas reglas que determinen qué flujos son permisibles y cuáles deben ser bloqueados, se decide permitir el paso o detener dicho flujo.
10. Estos controles deben proteger tanto la información de usuario, como los datos de configuración y administración que regulan los flujos de información.
11. Para poder llevar a cabo de una manera efectiva esta protección, se debe tener en cuenta el control de los flujos de información, determinando qué comunicaciones se permiten o se deniegan, en la interconexión de sistemas.
12. Los elementos del perímetro son tanto elementos de protección, como activos del sistema que hay que proteger con igual o más diligencia que cualquier otro elemento del sistema.

3. ALCANCE

13. Esta guía tratará las interconexiones basadas en protocolos estándares de comunicaciones cuando uno de los sistemas esté afectado por el Esquema Nacional de Seguridad.
14. En el caso de que alguna interconexión de sistemas utilizase protocolos no estándares o propietarios, se recomienda su estudio caso por caso.
15. Los requisitos establecidos en el perímetro han de cumplir con el ENS, que es de aplicación a todos los componentes del sistema.

4. ASPECTOS GENERALES

16. Dos o más sistemas de información pueden comunicarse entre sí para intercambiar información o servicios. Se produce una conexión cuando se proveen los medios físicos y lógicos de transmisión adecuados y susceptibles de ser empleados para el intercambio de información.
17. Se produce una interconexión de sistemas cuando
 - existe una conexión,
 - se habilitan flujos de comunicación entre los sistemas conectados y
 - esa conexión se produce entre sistemas con diferente responsable de seguridad o de diferente categoría (de acuerdo con el anexo I del ENS).
18. Cuando una red se segrega en subredes pero todas las partes tienen la misma categoría y el responsable de seguridad es único, no se considera interconexión. A veces se dice que las diferentes subredes son extensiones. Aunque esta guía no sea estrictamente de aplicación en esos casos, hay que tener en cuenta lo

requerido por la medida de seguridad “[mp.com.4] Segregación de redes”.

19. Desde el punto de vista de seguridad se debe proteger la información almacenada estáticamente en cada sistema, además de información viajando dinámicamente por la interconexión.

5. PRINCIPIOS BÁSICOS

20. Mínimo privilegio. Los usuarios y procesos autorizados a atravesar el perímetro solo disfrutarán de los derechos mínimos imprescindibles para ello.
21. Nodo auto protegido. Cuando un nodo se interconecta a otro, debe partir de la base de que el otro nodo no es fiable y por tanto hay que defenderse. Cada nodo debe protegerse a sí mismo como si los demás estuvieran comprometidos. Este principio impide la propagación de incidentes, accidentales o deliberados, entre nodos.
22. Despliegue mínimo. En el perímetro solamente se desplegarán, configurarán y usarán los equipos, cuentas de usuarios y administradores, aplicaciones, protocolos, servicios y flujos de información, estrictamente imprescindibles para el cumplimiento de la misión de la interconexión. En otras palabras, en el perímetro no habrá nada que no sea imprescindible. El objeto último es reducir la superficie de exposición a un ataque.

6. ACUERDO DE SEGURIDAD DE LA INTERCONEXIÓN

23. Antes de interconectar dos sistemas, se requiere un Acuerdo de Seguridad de la Interconexión² que es un documento formal, aprobado por los responsables de seguridad de los sistemas cuando estos sean diferentes, y que incluirá, al menos, los siguientes puntos:
 - Identificación de roles, funciones y personas designadas para los mismos.
 - Requisitos de negocio – la funcionalidad que se quiere proveer.
 - Comunidad(es) de usuario(s), incluyendo sus niveles de habilitación, en su caso.
 - Información que se va a intercambiar, incluyendo su clasificación y reglas de marcado, en su caso.
 - Servicios (incluyendo el detalle de los protocolos que se van a emplear, directa o indirectamente).
 - Topología del sistema de protección (nivel lógico y físico).
 - Controles que se han desplegado para proteger los intercambios de información.
 - Análisis de riesgos que concrete riesgos potenciales y residuales.
 - Procedimientos operativos de seguridad; al menos los relativos a autorización, configuración, gestión de incidencias y gestión de cambios.
 - Registros de actividad y sus procedimientos asociados.

² ISA – Interconnection Security Agreement, en inglés.

24. Cuando la conexión se realice con una red pública (por ejemplo, Internet), el Acuerdo de Seguridad de la Interconexión vendrá aprobado únicamente por el Responsable de la Seguridad del sistema de información adscrito al ENS.

7. ARQUITECTURA DE PROTECCIÓN PERIMETRAL (APP)

25. Se deberá constituir una arquitectura de protección perimetral, utilizando para ello dispositivos que permitan proteger los flujos de información.
26. Dentro de las posibilidades tecnológicas que podemos adquirir, para cumplir ese objetivo, nos centraremos en los siguientes dispositivos.
- Enrutadores (*routers*)
 - Cortafuegos (*firewalls*)
 - Intermediarios (*proxies*)
 - Pasarelas de intercambio seguro
 - Diodos de datos
27. A continuación, se describe la funcionalidad de cada dispositivo, explicando brevemente el modelo de comunicación de interconexión de sistemas abiertos (modelo OSI).

7.1. CAPAS OSI

28. El modelo de interconexión de sistemas abiertos (OSI³) es un modelo conceptual desarrollado en los años 70 y publicado como norma ISO⁴/IEC 7498. Buscaba una referencia independiente de los fabricantes de productos para que estos pudieran interoperar.
29. Es un modelo prácticamente paralelo al desarrollo del modelo TCP⁵/IP⁶, sobre el que se sustenta Internet.
30. Ambos modelos (OSI y TCP/IP) se basan en el concepto de agrupación de protocolos en capas. Así los protocolos de las capas inferiores realizan tareas que proporcionan servicios a las capas superiores. La siguiente figura muestra las 7 capas de la pila de protocolos OSI, así como varios protocolos y elementos que operan en cada capa.

aplicación	POP-SMTP, HTTP, HTTPS
presentación	HTML, DOC, PDF
sesión	RPC, SCP
transporte	TCP, UDP, SSL
red	IPv4, IPv6
enlace	ETHERNET, VLAN
físico	cobre, fibra, radio

³ OSI: Open System Interconnection

⁴ ISO: International Organization for Standardization

⁵ TCP: Transmission Control Protocol. Protocolo de control de la transmisión. Es un protocolo de red que permite las comunicaciones a través de Internet

⁶ IP: Internet Protocol. Protocolo Internet

Figura 1. Modelo OSI.

7.2. ENRUTADORES (ROUTERS)

31. Son elementos que trabajan a nivel de red. En este nivel se inician, mantienen y terminan las conexiones que transmiten paquetes IP, permitiendo que estos paquetes pasen de una red a otra. Se trata por tanto de un elemento imprescindible para conectar dos redes, entendiendo por red el conjunto de equipos que se pueden conectar directamente entre sí sin necesidad de un enrutador. Permiten interconectar redes LAN⁷ y WAN⁸.
32. Los enrutadores o encaminadores o routers filtran los paquetes IP en función de las direcciones IP, servicios y puertos a los que se quiere acceder. Además, proporcionan control de tráfico y funciones de filtrado a nivel de red. Permiten también reencaminar (enrutar) dinámicamente para dirigir los paquetes IP.
33. Los *routers* tienen la capacidad de controlar los flujos de información tanto entrante como saliente. Se trata por tanto de dispositivos que requieren de una configuración adecuada para proteger nuestro sistema.

7.3. CORTAFUEGOS (FIREWALLS)

34. Un cortafuegos es un dispositivo de seguridad fundamental para proteger el perímetro. Puede actuar en varias capas del modelo OSI (principalmente de red y transporte, aunque también pueden ser de aplicación). Puede ser una aplicación, un dispositivo o una combinación de ambos. Su función principal consiste en aislar redes internas y bloquear redes externas según las políticas de cada organización.
35. Hay cortafuegos de red, que controlan el tráfico en tránsito de la red.
36. Hay cortafuegos de equipo que controlan la conexión de un equipo a una red. Por ejemplo, en equipos personales, son frecuentes los cortafuegos personales que determinan qué paquetes pueden entrar y qué paquetes pueden salir.
37. Los cortafuegos analizan paquetes IP, y teniendo en cuenta dirección origen, dirección destino, protocolo y puerto de destino, deciden permitir o bloquear su paso.

⁷ LAN: Local Area Network (Red de Área Local)

⁸ WAN: Wide Area Network (Red de Área Extensa)

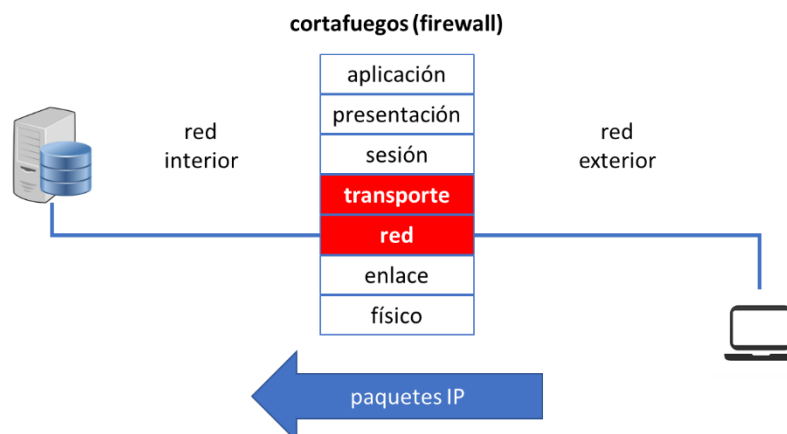


Figura 2. Capas en las que pueden actuar los cortafuegos

7.4. INTERMEDIARIOS (PROXIES)

38. Se trata de un dispositivo que se sitúa en la red actuando de intermediario para prestar un servicio determinado. Su función es recibir todas las peticiones de los usuarios de una organización, a un determinado protocolo, y distribuir las entradas y salidas de información de acuerdo con unos filtros.
39. Los intermediarios o proxies trabajan a nivel de aplicación. Existen proxies para diferentes protocolos, por ejemplo, mensajería electrónica (POP⁹, SMTP¹⁰), navegación web (HTTP¹¹), transferencia de ficheros (FTP¹²) etc.

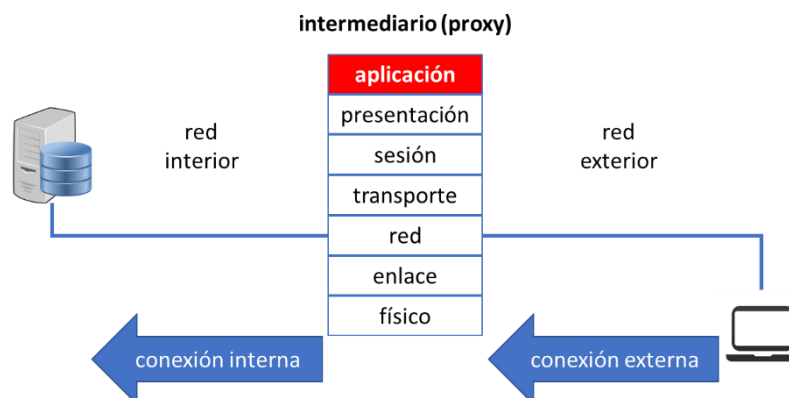


Figura 3. El intermediario o proxy en el modelo OSI

⁹ POP: Post Office Protocol, Protocolo de Oficina de Correo en clientes locales de correo para obtener los mensajes de correo electrónico almacenados en un servidor remoto, denominado Servidor POP. Es un protocolo de nivel de aplicación en el Modelo OSI

¹⁰ SMTP: Simple Mail Transfer Protocol, protocolo para transferencia simple de correo

¹¹ HTTP: Hypertext Transfer Protocol, y el HTTPS Hypertext Transfer Protocol Secure, Protocolo seguro de transferencia de hipertexto, es un protocolo de aplicación basado en el protocolo HTTP, destinado a la transferencia segura de datos de Hipertexto, es decir, es la versión segura de HTTP.

¹² FTP: File Transfer Protocol, Protocolo de Transferencia de Archivos: es un protocolo de red para la transferencia de archivos entre sistemas conectados a una red TCP (Transmission Control Protocol), basado en la arquitectura cliente-servidor

40. Los *proxies* no trabajan con paquetes IP o, para ser más precisos, reciben paquetes TCP/IP por la entrada, examinan y extraen su contenido y crean nuevos paquetes TCP/IP en la salida. Esta operación desactiva los paquetes como mecanismos para trasladar carga maliciosa.
41. La ventaja de los *proxies* es que examinan el contenido del paquete, comprenden el protocolo y pueden detectar un uso anómalo del mismo.

7.5. PASARELAS DE INTERCAMBIO SEGURO

42. Las pasarelas de intercambio seguro de información son dispositivos de protección de perímetro más complejos que un cortafuegos o un proxy. Están orientadas a la protección de interconexiones entre redes que manejan información con diferentes categorías o políticas de seguridad, con el fin de evitar la entrada o salida de información no autorizada.
43. Para ello, aportan las siguientes funcionalidades de seguridad:
 - Separación de redes. Ruptura de la continuidad de los protocolos de comunicaciones entre dos redes interconectadas en todas las capas del modelo OSI. Así, las pasarelas suelen estar formadas por dos unidades, una que se conecta a la red interna (la que se protege) y otra a la externa, unidas por un dispositivo pasivo de lectura y escritura. Ambas unidades se comunican mediante un protocolo desarrollado ad-hoc, que impide que utilicen simultáneamente los mismos recursos. De esta forma se asegura que nunca se establece una conexión TCP/IP entre las entidades origen y destino, independientemente de la configuración software del dispositivo, ni que a la red externa lleguen paquetes con información de la red interna.
 - Filtrado de contenidos. Las pasarelas analizan el contenido del paquete y permiten el paso de información siempre que cumpla las reglas de filtrado definidas, tanto para la entrada como para la salida. También posibilitan la utilización de mecanismos de firma digital para el control de flujo de información, de tal manera que solo aquello que se encuentre firmado pueda salir de la red interna. Este control basado en firma digital está enfocado a sistemas que manejan información a la que se le exige un nivel muy alto de confidencialidad.
 - Las pasarelas son especialmente útiles para implementar mecanismos de defensa en profundidad y neutralizar o minimizar el efecto de las Amenazas Persistentes Avanzadas al no permitir la fuga de información sensible desde la red interna.
44. Las pasarelas de intercambio seguro no se exigen en el Esquema Nacional de Seguridad, no obstante, pudieran ser una opción recomendable para algunos organismos dependiendo de los entornos y activos esenciales a proteger.
45. Existen pasarelas de intercambio seguro para correo electrónico, servicios web o para transferencia de ficheros. Ver guía CCN-STIC 105 Catálogo de productos de la seguridad de las tecnologías de la Información y la Comunicación.
46. La siguiente figura muestra un esquema de interconexión con pasarela:

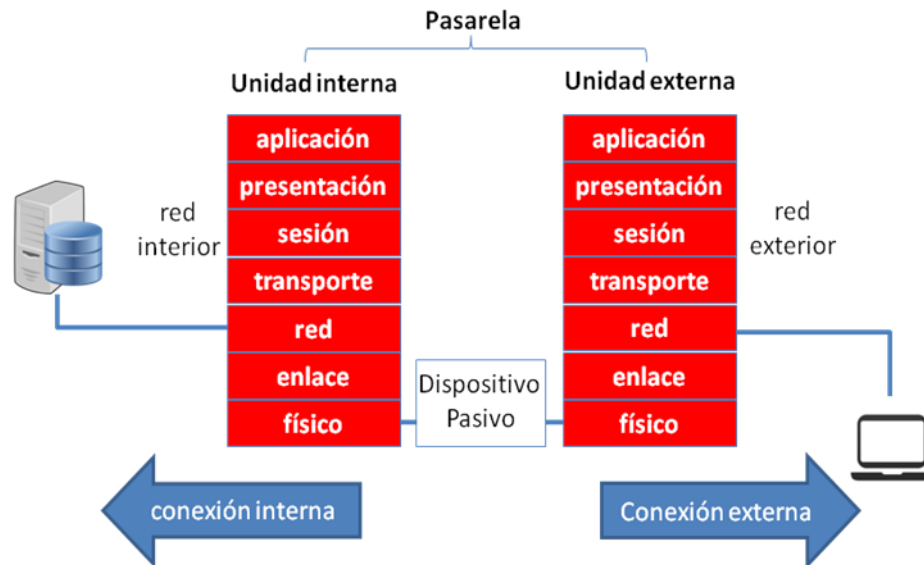


Figura 4. Pasarela de intercambio seguro

7.6. DIODOS DE DATOS

47. Los diodos de datos son los dispositivos de protección de perímetro que aportan una mayor seguridad frente a la fuga de información sensible, dado que garantizan el flujo unidireccional de la información mediante hardware, al no existir un canal de retorno físico.
48. Están orientados a la protección de interconexiones entre redes que manejan información con diferentes categorías o políticas de seguridad, con el fin de evitar la salida de cualquier tipo de información del sistema que protegen.
49. Dado que no existe este canal de retorno, en el caso en que ambos sistemas utilicen protocolos de comunicaciones orientados a conexión (p.ej.: TCP) o arquitecturas cliente/servidor que por definición exijan una bidireccionalidad, estos dispositivos requerirán de una lógica adicional a ambos lados del dispositivo hardware unidireccional en el que la lógica externa actúe como receptor frente a la red exterior y la lógica interna como emisor frente a la red interior y así permitir que la comunicación se realice con éxito. Esta imposibilidad de comunicación bidireccional extremo a extremo hace que el emisor nunca pueda disponer de un acuse de recibo real (*acknowledge*) del resultado de la transmisión.
50. Esta lógica podrá estar integrada o no dentro del propio dispositivo hardware unidireccional.
51. Los diodos tampoco se exigen en el Esquema Nacional de Seguridad y sirven para implementar políticas muy restrictivas. Por ejemplo, en un sistema se permite que entre información; pero no que salga, impidiendo las fugas de información.
52. La siguiente figura muestra un esquema de interconexión con diodo:



Figura 5. Diodo de datos; bloquea toda salida de datos

8. TIPOS DE ARQUITECTURAS DE PROTECCIÓN DE PERÍMETRO

53. Se describen a continuación 7 arquitecturas típicas de protección de perímetro, combinando los dispositivos previamente mencionados. En todos los casos se describen los elementos que proporcionan seguridad considerando que la función de enrutador o *router* está contemplada en ellos.

8.1. ARQUITECTURA DE PROTECCIÓN DE PERÍMETRO DE TIPO 1 (APP-1)

54. Se despliega, un cortafuegos entre nuestra red y el exterior. Como se ha comentado el cortafuegos aún las funciones de encaminamiento y filtro de paquetes o de circuito.

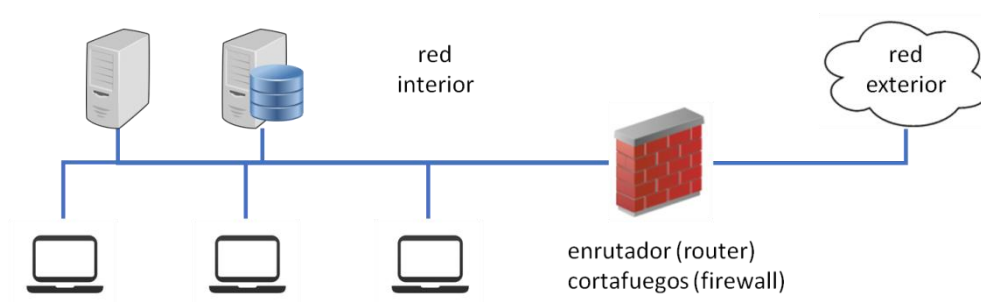


Figura 6. Arquitectura de protección de perímetro tipo -1 (APP-1)

55. Esta arquitectura no controla contenidos, solamente controla el tráfico permitido.
56. El cortafuegos está expuesto a ataques desde el exterior y desde el interior.
57. Un fallo (vulnerabilidad) en el cortafuegos, tiene como consecuencia directa la posibilidad de acceso al interior de nuestro sistema, o la fuga de datos.

8.2. ARQUITECTURA DE PROTECCIÓN DE PERÍMETRO DE TIPO 2 (APP-2)

58. Simplemente se despliega un intermediario (proxy) entre nuestra red y el exterior. El mismo intermediario aúna las funciones de encaminador (router).

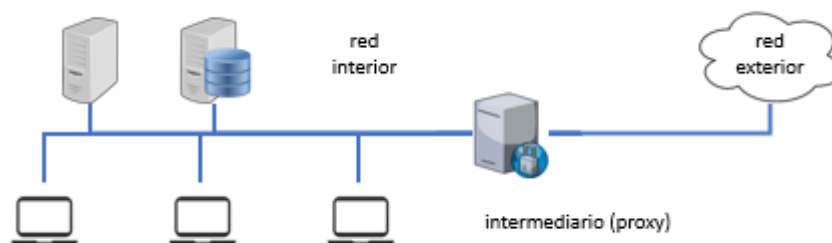


Figura 7. Arquitectura de protección de perímetro tipo -2 (APP-2)

59. Esta arquitectura permite monitorizar y controlar los intercambios de datos y los contenidos, pudiendo establecer reglas precisas de autorización y registro de actividad.
60. El intermediario o proxy está expuesto directamente a ataques desde el exterior y desde el interior.
61. Un fallo (vulnerabilidad) en el intermediario tiene como consecuencia directa el acceso al interior o la fuga de datos.

8.3. ARQUITECTURA DE PROTECCIÓN DE PERÍMETRO DE TIPO 3 (APP-3)

62. Combinamos un cortafuegos con un intermediario.

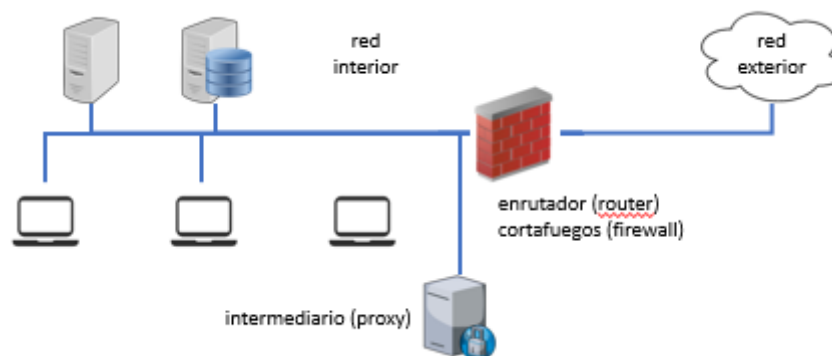


Figura 8. Arquitectura de protección de perímetro tipo -3 (APP-3)

63. Esta arquitectura permite monitorizar y controlar los intercambios de datos y los contenidos, pudiendo establecer reglas precisas de autorización y registro de actividad.
64. El elemento que hace de cortafuegos está expuesto directamente a ataques desde el exterior; pero el elemento que hace de intermediario ve reducida su superficie de ataque a lo que permita el cortafuegos, además de los ataques procedentes del

interior.

65. Un fallo (vulnerabilidad) en el cortafuegos tiene como consecuencia directa el acceso al interior, o la fuga de datos.
66. Si el intermediario se viera comprometido, el atacante tendría acceso a la red interior.

8.4. ARQUITECTURA DE PROTECCIÓN DE PERÍMETRO DE TIPO 4 (APP-4)

67. Similar a la arquitectura APP-3; pero el cortafuegos tendrá configurados 3 puertos, uno para la red interior, otro para la red exterior y un tercero para el proxy. De este modo conseguimos que el proxy no esté ni en la red interior ni en la exterior, sino en un tramo de red intermedio, que se denomina zona desmilitarizada (DMZ¹³). La diferencia funcional radica en que todo el tráfico de entrada y de salida a nuestra red es filtrado a través del proxy y todos los accesos al proxy deben ser autorizados en los cortafuegos.
68. La zona DMZ es un tramo de acceso controlado, filtrado por el cortafuegos que protege sus conexiones interna y externa. Es habitual desplegar en esta zona servicios como pasarelas de correo electrónico o de páginas web, de forma que es sencillo filtrar el contenido de los intercambios. También es frecuente desplegar en esta zona servidores DNS que limitan la visibilidad exterior a lo estrictamente necesario.
69. Esta arquitectura controla entre qué elementos pueden circular paquetes IP, limitando el tráfico permitido:
- entre la red interior y el intermediario o proxy.
 - entre el intermediario (proxy) y la red exterior
 - no debe autorizarse el paso de paquetes directamente de la red exterior a la interior sin atravesar el intermediario o proxy.

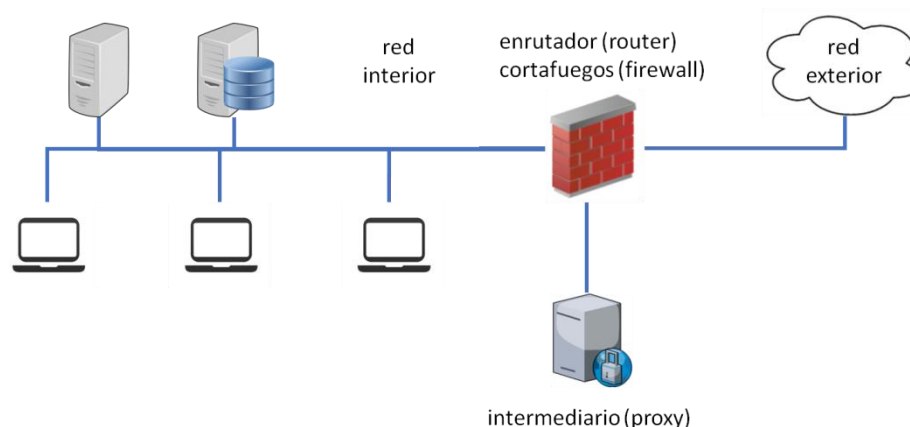


Figura 9. Arquitectura de protección de perímetro tipo -4 (APP-4)

¹³ Demilitarized Zone. Zona desmilitarizada.

70. Esta arquitectura permite reducir la exposición de nuestro sistema ante ataques externos o errores internos, ya que el tráfico es filtrado por el cortafuegos. Se controla qué flujos de información se permiten entre el interior y el intermediario. Esto reduce la exposición a ataques o errores internos que puedan llevar flujos no autorizados al intermediario. Así mismo, si el intermediario se viera comprometido, se limita su accesibilidad a la red interior.
71. Un fallo (vulnerabilidad) en el cortafuegos, tiene como consecuencia directa la posibilidad de acceso al interior, o la fuga de datos.

8.5. ARQUITECTURA DE PROTECCIÓN DE PERÍMETRO DE TIPO 5 (APP-5)

72. Se despliegan, un intermediario (*proxy*) y dos cortafuegos, dejando un tramo de red intermedio. Esta red intermedia se denomina coloquialmente zona desmilitarizada (DMZ) y no se autoriza que circulen paquetes, directamente entre los cortafuegos.

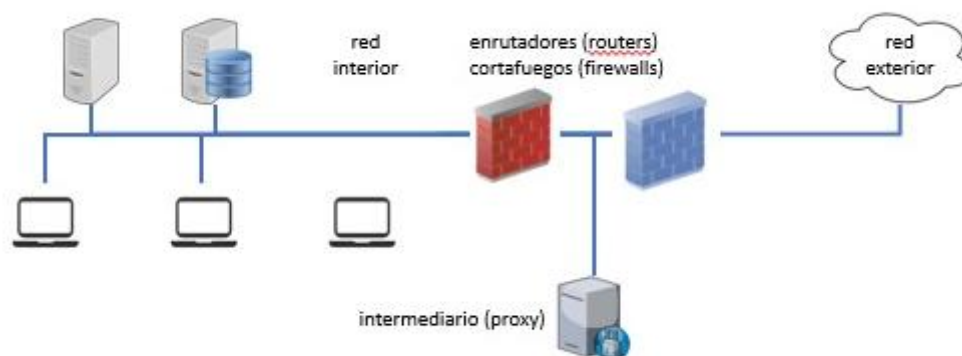


Figura 10. Arquitectura de protección de perímetro tipo -5 (APP-5)

73. Un cortafuegos permite la entrada de datos al proxy, mientras que el otro cortafuegos permite la salida de datos del proxy. En ambas direcciones, según requieran los flujos autorizados.
74. Funcionalmente, esta arquitectura funciona de forma similar a la APP-4; pero dificultamos los ataques al cortafuegos: ahora deben comprometerse 2 cortafuegos para atravesar el perímetro sin ser interceptados por el proxy. Para potenciar esta característica se evita que ambos cortafuegos puedan sucumbir como consecuencia de un único vector de ataque, forzando a que sean diferentes: diferente fabricante, diferente software, diferente configuración, diferentes administradores de seguridad, etc.
75. Esta arquitectura controla entre qué elementos pueden circular paquetes IP, limitando el tráfico permitido:
- entre la red interior y el intermediario (proxy).
 - entre el intermediario (proxy) y la red exterior.
 - no debe autorizarse el paso de paquetes directamente de la red exterior a la

interior sin atravesar el intermediario o proxy.

76. Comparado con APP-4 se ha eliminado el riesgo de que una vulnerabilidad en un solo cortafuegos se traduzca en una posibilidad de acceso directo a la red interna.

8.6. ARQUITECTURA DE PROTECCIÓN DE PERÍMETRO DE TIPO 6 (APP-6)

77. Se despliegan, un intermediario (proxy) y dos cortafuegos, pero, a diferencia de la arquitectura APP-5, no existe un tramo de red directo entre los cortafuegos.

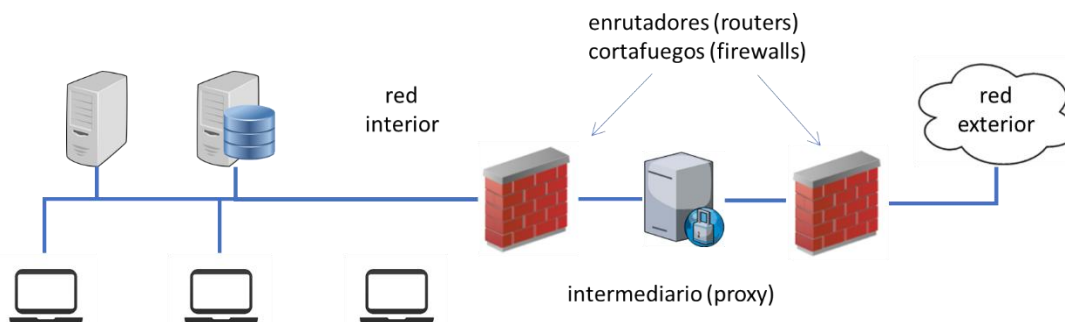


Figura 11. Arquitecturas de protección de perímetro tipo 6 (APP-6)

78. Comparado con APP5, eliminamos el requisito de que los cortafuegos deban ser diferentes, al no existir conexión directa entre ellos. El razonamiento tras el requisito de que los cortafuegos sean diferentes es reducir la posibilidad de que una vulnerabilidad en uno de ellos se reproduzca automáticamente en el otro, bien sea una vulnerabilidad hardware, software o de la configuración. Si la vulnerabilidad afecta al encaminamiento de paquetes, en APP-5 sería posible pasar de la red exterior a la red interior directamente. Al no existir la red física en APP-6, ese peligro desaparece.

8.7. ARQUITECTURA DE PROTECCIÓN DE PERÍMETRO DE TIPO 7 (APP-7)

79. Como se ha indicado anteriormente puede haber casos en los que el organismo tenga unos requisitos de confidencialidad superiores a los que marca el Esquema Nacional de Seguridad, para los que sea recomendable sustituir el intermediario o proxy por una pasarela de intercambio seguro o incluso un diodo.

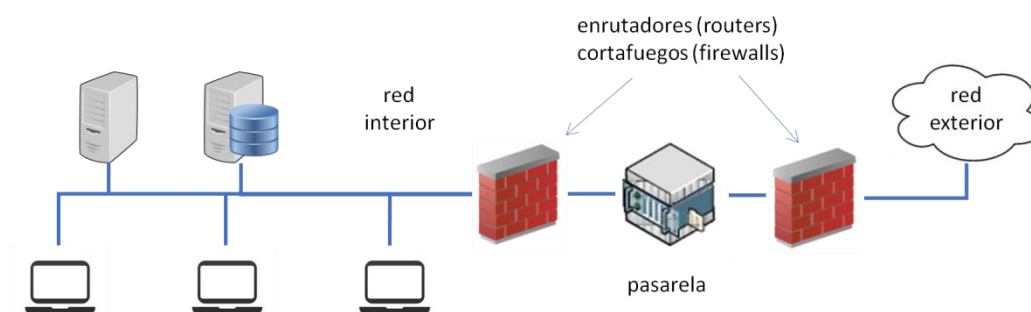


Figura 12. Arquitectura de protección de perímetro tipo 7 (APP-7) con pasarela de intercambio seguro

9. DESPLIEGUE

80. Las arquitecturas descritas pueden ser desplegadas en diferentes esquemas de red para atender a las necesidades concretas del servicio. Dependiendo de cuales sean los flujos de información requeridos, la frontera debe adaptarse a las necesidades concretas sin mermar su capacidad de protección de la red interna.
81. El acceso a los equipos de la frontera para su administración solo se podrá realizar desde dentro de la frontera, nunca desde el exterior

9.1. SERVIDORES Y SERVICIOS EN LA FRONTERA

82. Es habitual que elementos como servidores web se dispongan en la frontera para facilitar el acceso de usuarios internos sin necesidad de que penetren en la red interna. Son habituales: servidores HTTP y HTTPS de páginas web, servidores FTP de transferencia de ficheros, servidores DNS de resolución de nombres, etc. Todos ellos configurados de forma autónoma sin necesidad de establecer conexiones con la red interior para responder a las demandas de los usuarios externos. Si necesitaran establecer conexiones internas, pasarían a la categoría de servicios intermediados (proxies).

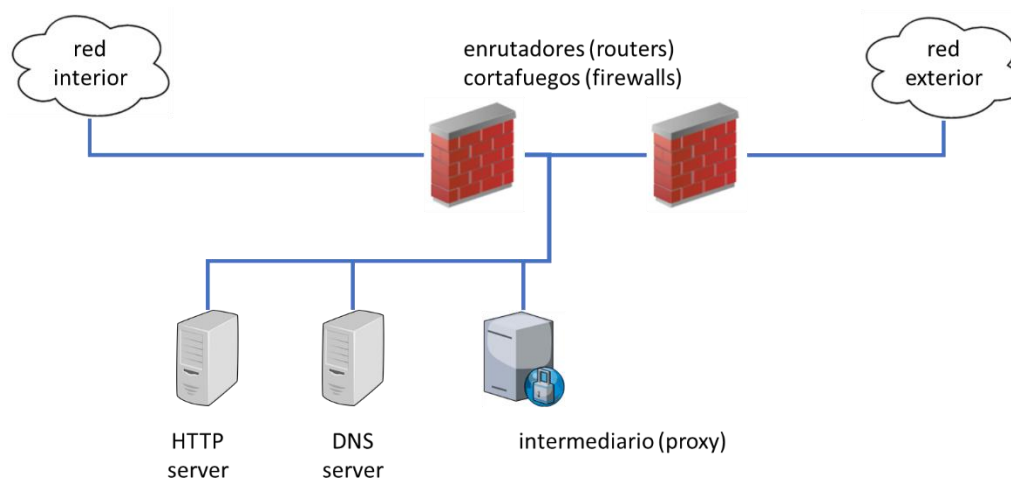


Figura 13. Servidores y servicios en frontera

83. Estos servicios deben configurarse de forma que los flujos de información desde el exterior atravesasen un cortafuegos y el intermediario. Debe considerarse la oportunidad de desplegar un proxy separado para estos servicios que no entran en la red interna.
84. Siempre atendiendo a los principios establecidos en la sección 5 (mínimo privilegio, nodo auto-protegido y despliegue mínimo), se deberán implantar suficientes herramientas de seguridad según lo establecido en la sección 11.
85. Por motivos de economía de recursos de operación, las conexiones a estos servicios pueden compartir herramientas de seguridad con otros elementos de la

frontera.

9.2. GARANTÍAS DE DISPONIBILIDAD

86. A fin de garantizar los niveles de seguridad requeridos por los servicios prestados a través de la interconexión, la frontera puede estar redundada. Varios cortafuegos, intermediadores (*proxies*) y servidores en la frontera pueden estar trabajando en paralelo para repartir carga y para evitar que el fallo de uno de ellos interrumpa el servicio. Incluso puede llegar a replicarse la frontera entera para evitar puntos únicos de fallo en equipamiento de red, elementos físicos y proveedores de servicio de Internet.
87. Desde el punto de vista de seguridad, el control de los flujos de información deberá ser igual en todos los elementos redundados, concretamente en lo que respecta a flujos permitidos y herramientas de seguridad.

9.3. FRONTERA COMPARTIDA

88. Es relativamente frecuente el caso de que haya varias redes internas compartiendo una conexión al exterior. Bien sea por una segregación interna de la red, bien porque varios sistemas de información llegan a un acuerdo para compartir recursos.

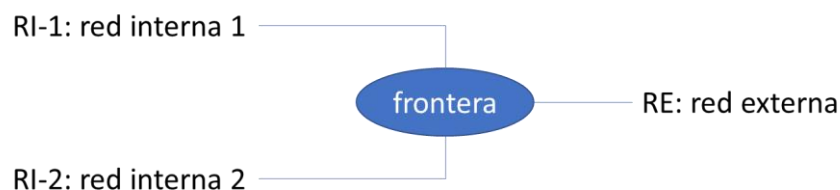


Figura 14. Frontera compartida

89. En estos casos, se considera que hay tantas interconexiones como pares de redes conectados a la frontera compartida. En el ejemplo de la figura anterior, hay 3 interconexiones:
- Red Interna-1 con Red Externa
 - Red Interna-2 con Red Externa
 - Red Interna-1 con Red Interna-2
90. Y en cada una de las interconexiones se deben aplicar los principios básicos de la sección 5, la arquitectura de seguridad apropiada de entre las descritas en la sección 8 y las medidas de seguridad de la sección 11.
91. A modo de ejemplo, se muestra un esquema que combina 2 redes internas compartiendo una salida al exterior, donde defendemos los flujos con el exterior, así como los flujos entre redes internas.

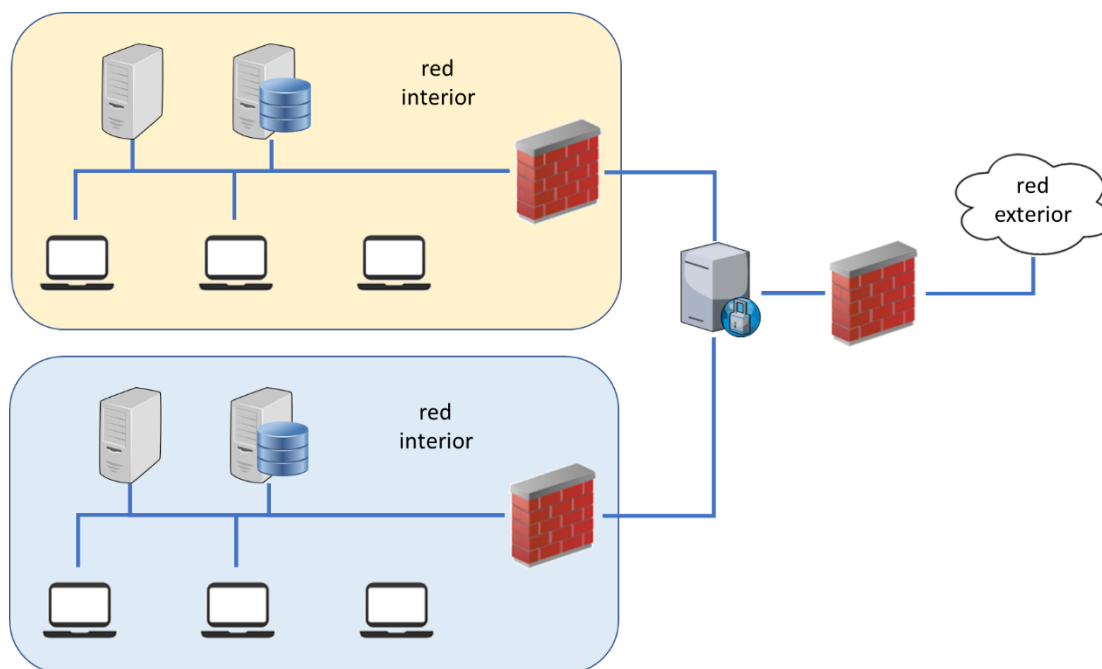


Figura 15. Ejemplo de frontera compartida

9.4. REDES PRIVADAS VIRTUALES

92. Las redes privadas virtuales (VPN, *Virtual Private Networks*) aparecen como un medio de comunicarse de forma segura a través de medios que no ofrecen garantías de seguridad.
93. Por seguridad nos referimos a garantías de confidencialidad, integridad y autenticidad, según se recoge en las medidas de seguridad [mp.com.2] protección de la confidencialidad y [mp.com.3] protección de la autenticidad y de la integridad del ENS. Estas garantías son en buena parte criptográficas y se ajustarán a lo previsto en la guía CCN-STIC 807 Criptología de Empleo en el Esquema Nacional de Seguridad.
94. Las características y requisitos de las redes privadas virtuales se tratan en detalle en la guía CCN-STIC 836 Seguridad en VPN en el marco del ENS.
95. Las redes privadas virtuales conectan la red interior con otra red remota o con un nodo individual remoto, conexión vehiculada a través de una red externa. Esta conexión se convierte en una interconexión cuando se cumple lo previsto en la sección 4: diferente responsable de la seguridad o diferente categoría al otro extremo de la red virtual.
96. El concentrador de redes privadas virtuales (donde terminan las VPN) debe instalarse preferentemente en la zona desmilitarizada (DMZ) y todos los flujos de información, entrantes y salientes, deben pasar por el intermediador (*proxy*).
97. Cuando sea necesario establecer la red privada desde un equipo interior y los datos aparezcan cifrados (negros) en la frontera, el equipo interior deberá disponer de un agente intermediador (*proxy*) que revise toda la información enviada o recibida a través de la red virtual.

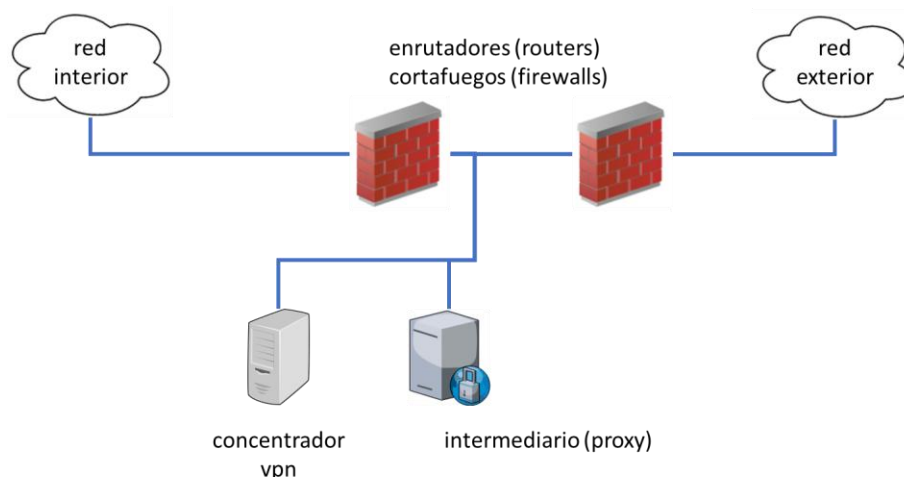


Figura 16. Concentrador de Redes Privadas Virtuales se situará junto a los servidores DNS, HTTPS

98. Se debe estudiar la oportunidad de desplegar un cortafuegos entre la terminación VPN y el proxy, a fin de limitar los paquetes que pueden atravesar esta interfaz.

9.5. EQUIPOS REMOTOS

99. Se consideran equipos remotos aquellos equipos de usuario que se conectan a la red interior desde el otro lado de la frontera. Típicamente se utilizarán redes privadas virtuales para el acceso a través de redes públicas o de terceros.

100. Los escenarios más típicos son:

- teletrabajadores, que acceden a información y servicios proporcionados en la red interna; donde el equipo cliente puede ser propiedad del organismo o ser propiedad del usuario (BYOD – Bring Your Own Device)
- empresas de mantenimiento remoto que proporcionan servicios de mantenimiento de software y de configuración a distancia

101. A estos equipos remotos les serán de aplicación las medidas de seguridad del ENS que correspondan a la información que pueda estar o quedar almacenada en ellos. Se debe prestar atención, prioritariamente, a los requisitos de confidencialidad.

102. Todos los equipos remotos deberán:

- Disponer de un cortafuegos individual.
- Atravesar el servicio proxy de la frontera en todos los accesos a la red interior.
- Limitar al administrador de seguridad la instalación de software y la configuración de seguridad del equipo. La administración de la seguridad se realizará bajo la responsabilidad del Responsable de la Seguridad de la red interior, bien por personal propio o por delegación en administradores de seguridad específicamente autorizados.

103. Si el sistema es de categoría MEDIA o superior,

- El equipo remoto solamente podrá conectarse a sitios explícitamente autorizados (lista blanca)

104. Si el sistema es de categoría ALTA,

- Todas las comunicaciones entre el equipo y redes diferentes a la interior deberán ser a través del servicio proxy establecido en la frontera.

10. REQUISITOS DEL ENS SOBRE ARQUITECTURAS DE PROTECCIÓN DE PERÍMETRO

105. Para sistemas de las tecnologías de la información sujetos al Esquema Nacional de Seguridad, se autorizan las siguientes arquitecturas de protección del perímetro.

Categoría del sistema	Arquitectura de Protección de Perímetro
Básica	APP-3 o superior
Media	APP-4 o superior
Alta	APP-5 o superior

Tabla 1. Arquitectura de protección de perímetro mínima a implantar por categoría del sistema

11. HERRAMIENTAS DE SEGURIDAD

106. Las herramientas de seguridad se describen funcional y operativamente en la guía CCN-STIC 818 Herramientas de seguridad en el ENS.

107. Un sistema de protección perimetral debe contemplar el uso de herramientas de seguridad, bien para tratar los flujos de información, bien para analizar y proteger los componentes hardware y software que forman parte del perímetro de seguridad.

11.1. DETECCIÓN DE CÓDIGO DAÑINO

108. Son herramientas que analizan el código y el comportamiento de software detectando actividades [potencialmente] peligrosas. Normalmente se analiza el código que se ejecuta y, sobre todo, los elementos del sistema a los que accede: registro, sistema de ficheros, software instalado, configuración del sistema, manejadores de dispositivos (*drivers*), etc. También es importante analizar conexiones a equipos remotos que puedan ser empleadas como canales para descargar más código o para exfiltrar datos.

109. Al trabajar sobre patrones conocidos, su actualización es crítica.

110. Hay que trabajar también sobre código móvil (tipo *applets*¹⁴, *flashplayer*¹⁵, macros, o similares) que a fin de cuentas es software ajeno que se ejecuta en nuestro

¹⁴ Un *applet* es un componente de una aplicación que se ejecuta en el contexto de otro programa, por ejemplo, en un navegador web.

sistema. En estos casos lo más importante es revisar a qué recursos accede. Una aproximación preventiva frecuente consiste en trabajar en una zona aislada (*sandbox*¹⁶) donde un ataque no tiene recorrido efectivo.

11.2. ANÁLISIS DE VULNERABILIDADES

- 111. Son herramientas que buscan defectos en el software. Normalmente trabajan con bibliotecas de defectos reportados por los fabricantes y se centran en detectar su presencia en software en operación.
- 112. Pueden ir más lejos y apoyar actividades de penetración para auditar hasta dónde podría llegar un atacante.
- 113. Al trabajar sobre patrones conocidos, su actualización es crítica.

11.3. ANÁLISIS DE REGISTROS DE ACTIVIDAD

- 114. Son herramientas que analizan a posteriori las actividades de los usuarios en general y, especialmente, la de los usuarios con privilegios como los administradores. Buscan por una parte comportamientos anómalos, aunque también se utilizan para análisis forense posterior a un incidente de seguridad.
- 115. Los registros de actividad se almacenarán en la red interior.
- 116. Ver guía CCN-STIC 434 Herramientas para el análisis de ficheros de logs.

11.4. DETECCIÓN Y PREVENCIÓN DE INTRUSIÓN (IDS/IPS¹⁷)

- 117. Son herramientas que buscan, en tiempo real, comportamientos típicos de maniobras de intrusión, o cruce no autorizado de la frontera. Pueden ser meramente observadores pasivos (IDS) o reaccionar activamente (IPS).
- 118. A veces se despliegan en paralelo a una función de cortafuegos (*firewall*) o intermediario (*proxy*).
- 119. A veces se despliegan sobre la red, monitorizando el tráfico por la misma.
- 120. Al trabajar sobre patrones conocidos, su actualización es crítica.
- 121. Ver guía CCN-CERT 432 Seguridad perimetral (detección de intrusos)

11.5. MONITORIZACIÓN DE TRÁFICO

- 122. Son herramientas que permiten registrar el tráfico IP¹⁸ en la red. Normalmente se procesa el registro a posteriori, bien para detectar comunicaciones anómalas o para realizar un análisis forense de un incidente de seguridad.

¹⁵ Es una aplicación informática del género reproductor multimedia.

¹⁶ Palabra inglesa que significa cajón de arena. Es un entorno de pruebas separado del entorno de producción. como un sistema de aislamiento de procesos, a menudo usado como medida de seguridad. Por extensión, una máquina virtual que emula el comportamiento de un ordenador completo.

¹⁷ *Intrusion Detection System/ Intrusion Prevention System*. Sistemas de detección de intrusos / Sistemas de prevención de intrusos.

123. También se utilizan para analizar estadísticamente el uso de la red y tomar decisiones de dimensionamiento y configuración.

124. Ver guía CCN-STIC 435 Herramientas de monitorización de tráfico.

11.6. PREVENCIÓN DE FUGA DE DATOS (DLP¹⁹)

125. Son herramientas frecuentemente utilizadas en combinación con funciones de cortafuegos (*firewall*) o intermediación (*proxy*). Analizan el contenido de la información que fluye y toman decisiones a partir de reglas que determinan si la información puede circular, si debe ser detenida o si debe suspenderse su flujo hasta tomar una decisión manual.

126. Estas herramientas trabajan sobre patrones para caracterizar la información a partir de los datos observados. Son muy eficaces (prácticamente infalibles) cuando la información está clasificada y marcada adecuadamente y la herramienta es capaz de analizar los metadatos²⁰.

11.7. VERIFICACIÓN DE LA CONFIGURACIÓN

127. Son herramientas que permiten analizar remotamente la configuración de seguridad de un equipo (por ejemplo, servidores, puestos de usuario, equipos de red, impresoras, etc.), revisar su configuración y levantar alarmas ante situaciones potencialmente peligrosas o, simplemente, disconformes con la política aprobada.

128. CLARA es una herramienta del CCN-CERT para analizar equipos cliente Windows.

129. ROCÍO es una herramienta del CCN-CERT para analizar configuraciones de encaminadores (*router*), cortafuegos (*firewalls*).

12. REQUISITOS DEL ENS SOBRE HERRAMIENTAS DE SEGURIDAD

130. El despliegue de herramientas de seguridad en el sistema de protección del perímetro se atenderá a los siguientes parámetros no funcionales en función de la categoría del sistema protegido por dicho perímetro.

131. En concreto se precisan los tiempos máximos admisibles de comprobación de actualizaciones de herramientas de detección de código dañino, de análisis de vulnerabilidades, de detección y prevención de intrusos y de prevención de fuga de datos, se determinan los plazos máximos entre el anuncio del proveedor y el despliegue de las actualizaciones de seguridad, y por último se fijan las frecuencias mínimas de escaneo de vulnerabilidades o revisión de los registros de actividad.

132. El CCN-CERT mantendrá permanentemente actualizados estos parámetros en cumplimiento de la Instrucción Técnica de Seguridad de Interconexión de sistemas de información.

¹⁸ *Internet Protocol*, protocolo internet.

¹⁹ *Data Loss Prevention*, Prevención de fuga de datos.

²⁰ Son datos que describen otros datos. En general, un grupo de metadatos se refiere a un grupo de datos que describen el contenido informativo de un objeto al que se denomina recurso

Categoría del sistema	Básica	Media	Alta
Detección de código dañino	Aplica	=	+
• La base de datos se mantiene actualizada	< 4 días	< 48 horas	< 24 horas
• Se aplican las actualizaciones (parches) de seguridad	< 7 días	< 7 días	< 4 días
Análisis de vulnerabilidades	Aplica	=	=
• El software se mantiene actualizado	< 7 días	< 7 días	< 7 días
• Frecuencia mínima de escaneo	3meses	1mes	1semana
Análisis de registros de actividad	Recomendado	Aplica	=
• Frecuencia mínima de revisión	1 mes-	1semana	3 día
Detección y prevención de intrusos	Opcional	Aplica	+
• El software se mantiene actualizado	< 7 días	< 7 días	< 7 días
Monitorización de tráfico	Opcional	Recomendado	Aplica
Verificación de la configuración	Opcional	Recomendado	Aplica
• Frecuencia mínima de verificación	1 año	6 meses	2 meses
Prevención de fuga de datos (DLP)	Opcional	Opcional	Recomendado
• El software se mantiene actualizado	< 7días	< 7días	< 7días

Tabla 2. Requisitos del ENS sobre herramientas de seguridad

133.Sin perjuicio de lo establecido en el ENS para estas herramientas, se cumplirán los siguientes puntos:

134.Detección de código dañino, antivirus.

- La base de datos se mantiene actualizada.
- Se aplican las actualizaciones de seguridad (parches).
- En el arranque se revisan los programas y los servicios.
- Se escanean los datos transferidos.
- Además, para categoría Alta: Se activan alarmas en tiempo real.

135.Análisis de vulnerabilidades.

- El software se mantiene actualizado.
- Se analiza el sistema de forma regular.

136.Análisis de registro de actividad (log) (aplica en categorías Media y Alta).

- Se analizan los registros regularmente.

137.Detección y prevención de intrusión (IDS/IPS – Intrusion Detection/Prevention System) – (aplica para categorías Media y Alta).

- El software se mantiene actualizado.
- Se escanean los datos transferidos.
- Además, para categoría Alta se activan alarmas en tiempo real.

138.Monitorización de tráfico (aplica en categoría Alta).

- Descubrimiento de equipos, protocolos y servicios activos.
- Comprobación, al menos una vez al día, de que los servicios están disponibles.
- Registro de tráfico entre equipos y protocolos que se emplean.
- Se activan alarmas en tiempo real.

139.Verificación de la configuración (aplica en categoría Alta).

- Se verifica la configuración de los equipos para comprobar que coincide con la política aprobada.

140.Prevencción de fuga de datos (DLP – Data Loss Prevention) (recomendado para categoría Alta).

- El software se mantiene actualizado.
- Se escanean los datos transferidos.
- Se activan alarmas en tiempo real.

ANEXO A. GLOSARIO DE TERMINOS Y ABREVIATURAS

141.Ver guía CCN-STIC-800 Glosario de Términos y Abreviaturas del ENS.

ANEXO B. BIBLIOGRAFÍA DE REFERENCIA

- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos
- Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal
- Real Decreto 3/2010 del 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica
- Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica
- Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica
- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal
- Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional
- Instrucción técnica de seguridad de Conformidad con el Esquema Nacional de Seguridad por Resolución de 13 de octubre de 2016, del Secretario de Estado de Administraciones Públicas
- Instrucción Técnica de Seguridad de Informe del Estado de la Seguridad por Resolución de 7 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas
- Guía de seguridad de las TIC (CCN-STIC 105)- Catálogo de productos de la seguridad de las Tecnologías de la Información y la Comunicación (pendiente de publicación).
- Guía de seguridad de las TIC - (CCN-STIC-430) – Herramientas de seguridad
- Guía de seguridad de las TIC - (CCN-STIC-432) – Seguridad perimetral (detección de intrusos)
- Guía de seguridad de las TIC - (CCN-STIC-434) – Herramientas para el análisis de ficheros de logs
- Guía de seguridad de las TIC - (CCN-STIC-435) – Herramientas de monitorización de tráfico
- Guía de seguridad de las TIC – (CCN-STIC 807) - Criptología de Empleo en el ENS.
- Guía de seguridad de las TIC - (CCN-STIC-808) - Verificación del cumplimiento de las medidas en el ENS
- Guía de seguridad de las TIC - (CCN-STIC 818) - Herramientas de seguridad en el ENS.

- Guía de seguridad de las TIC - (CCN-STIC-830) - Ámbito de aplicación del Esquema Nacional de Seguridad
- Guía de seguridad de las TIC - (CCN-STIC 836) - Seguridad en VPN en el marco del ENS
- MAGERIT – versión 3. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Consejo Superior de Administración Electrónica, 2012.