GOBIERNO DE ESPAÑA
MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS

CCN
CENTRO CRIPTOLÓGICO NACIONAL

GUÍA DE SEGURIDAD (CCN-STIC-818)

HERRAMIENTAS DE SEGURIDAD EN EL ENS

(BORRADOR)

ens
Esquema Nacional de Seguridad

OCTUBRE 2012

SIN CLASIFICAR

Edita:

GOBIERNO DE ESPAÑA MINISTERIO DE LA PRESIDENCIA

NIPO: 002-12-062-7

Tirada: 1000 ejemplares
Fecha de Edición: octubre 2012
Andrés Méndez Barco y Raúl Gámez Gámez han elaborado el presente documento.

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

PRÓLOGO

El uso masivo de las tecnologías de la información y las telecomunicaciones (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, 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 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.

Una de las funciones más destacables del Centro Criptológico Nacional es la de elaborar y difundir normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los sistemas de las tecnologías de la información y las comunicaciones de la Administración, materializada en la existencia de la serie de documentos CCN-STIC.

Disponer de un marco de referencia que establezca las condiciones necesarias de confianza en el uso de los medios electrónicos es, además, uno de los principios que establece la ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, en su artículo 42.2 sobre el Esquema Nacional de Seguridad (ENS).

Precisamente el Real Decreto 3/2010 de 8 de Enero de desarrollo del Esquema Nacional de Seguridad 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 las comunicaciones 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 2012

Félix Sanz Roldán
Secretario de Estado
Director del Centro Criptológico Nacional

INDICE

1. ANTECEDENTES

1. El Esquema Nacional de Seguridad (Real Decreto 3/2010 de 8 de enero) en sus artículos 18, 20, 21 y sobre todo 22 establece una serie de requisitos para cuyo cumplimento resulta de gran importancia contar con las herramientas adecuadas.

2. Esta guía pretende ayudar en la elección de aquellas herramientas que faciliten el cumplimiento del Esquema Nacional de Seguridad.

2. INTRODUCCIÓN

3. La dependencia de las Administraciones Públicas de los sistemas de Tecnologías de la Información y Comunicaciones se ha incrementado en los últimos años, siendo por tanto plenamente justificada la dedicación de esfuerzo adicional a la securización de los mismos a fin de preservarlos de las posibles amenazas.

4. En general las herramientas de seguridad pueden describirse como el conjunto de hardware o software que proporcionan servicios orientados a reforzar y dar soporte a la seguridad de los sistemas.

5. Estas herramientas se utilizan además para aumentar la confianza en que las medidas de seguridad, establecidas en los Sistemas para satisfacer los objetivos de seguridad (confidencialidad, integridad y disponibilidad), están siendo correctamente implementadas y mantenidas (Art. 11, 20 y 25 del ENS).

6. El Esquema Nacional de Seguridad indica la tipología de herramientas a usar en la interconexión de sistemas en función de la clasificación de los mismos (ver guía CCN-STIC-811).

7. Las herramientas que encontrará mencionadas en la presente guía se ofrecen a modo orientativo, no conformando una lista exhaustiva ni exclusiva de herramientas autorizadas por el CCN.

3. OBJETO

8. La presente guía persigue el doble objetivo de describir y clasificar las diferentes herramientas de seguridad existentes, así como establecer los requisitos relativos a la selección, aprobación, implementación, uso y mantenimiento de dichas herramientas de seguridad en los Sistemas.

4. ALCANCE

9. El Responsable de Seguridad, determinará el alcance de su aplicación, considerando la Política de Seguridad de la Organización y los requisitos de obligado cumplimiento definidos por el Esquema Nacional de Seguridad.

10. Este documento describe alguna de las responsabilidades y criterios a emplear durante el ciclo de vida de las herramientas de seguridad.

11. Los dispositivos de protección de perímetro (enrutador, cortafuegos, proxy, etc.), a pesar de que proporcionan protección a los sistemas, no se consideran en el ámbito de esta guía, ya que son tratados en las guías CCN-STIC-408 y CCN-STIC-811.

5. REQUISITOS GENERALES

12. Las herramientas de seguridad deben implementar funcionalidades que permitan facilitar y reforzar al menos los siguientes aspectos:

    a. Identificación y autenticación.
    b. Control de acceso (protección de datos de usuario en terminología Common Criteria).
    c. Registro de los eventos y auditoría.
    d. Integridad.
    e. Disponibilidad.
    f. Gestión de la configuración.
    g. Gestión de la seguridad.
    h. Garantía1.

13. Dada la naturaleza de su funcionalidad, las herramientas de seguridad pueden constituirse en punto de acceso a información de carácter sensible, es por ello que deben cumplir los siguientes requisitos:

    a. Control de acceso a la información/recursos granular y basado en perfiles: de manera que cada usuario sólo pueda acceder a aquellos que esté autorizado y siempre con el nivel de acceso adecuado, para aquellas herramientas que sean utilizadas por varios usuarios.
    Exploración de la información: las herramientas dispondrán de la capacidad de elaborar informes en múltiples formatos y en base a distintos criterios, los cuales permitirán facilitar la correcta interpretación de la información y su posterior tratamiento.
    Trazabilidad: las herramientas deben generar registros (logs) de su actividad y la de sus usuarios, de manera que pueda identificarse de manera inequívoca las acciones de los mismos. Para aquellas herramientas que por su simplicidad no dispongan de esta funcionalidad, deberá establecerse un método alternativo de registro de actividad mediante el sistema operativo, por ejemplo.

6. CLASIFICACIÓN

14. Las herramientas que serán expuestas en los apartados siguientes se clasificarán en base a su funcionalidad principal en las siguientes categorías:

    a. Auditoría
    b. Protección
    c. Detección
    d. Reacción

[1] La garantía aquí indicada se refiere a la garantía que se proporciona respecto al cumplimiento de las medidas de seguridad de un producto, demostrada mediante la certificación del mismo por parte de la Autoridad Nacional de Evaluación y Certificación, o conforme a Criterios Comunes (CC), etc.

15. Los niveles en que una herramienta puede operar son básicamente: red, sistema, usuario, aplicación o datos, si bien y dependiendo de la complejidad de la herramienta puede que trabaje en varios niveles.

16. Las herramientas de seguridad pueden agruparse en las siguientes áreas principales de actividad:

    a) Gestión de la seguridad: estas herramientas serán utilizadas habitualmente para labores de certificación y acreditación, fundamentalmente en el ámbito del análisis y gestión de riesgos, análisis de vulnerabilidades, inspecciones periódicas o respuesta a incidentes.
    Administración de la seguridad del Sistema: Las herramientas enmarcadas dentro de esta clasificación cubrirán aspectos como comprobaciones de integridad de sistemas de ficheros, filtrado o supervisión de recursos, revisión automática de logs y comprobaciones de configuración.

17. Hay que tener presente que la tecnología en general y de manera especialmente acentuada en lo referente a la seguridad, evoluciona a gran velocidad, por lo que la clasificación dada pretende ser más una guía de referencia que una foto exacta del estado del arte actual.

7. SELECCIÓN, CONTROL DE LA CONFIGURACIÓN Y OPERACIÓN

18. En el mercado podemos encontrar gran cantidad de herramientas con diferentes funcionalidades y licencias de uso, a continuación describiremos los criterios que nos ayudarán a seleccionar la adecuada para la necesidad que debamos cubrir.

7.1. SELECCIÓN

19. Es condición indispensable que las herramientas de seguridad que se utilicen sean aprobadas por el Responsable de Seguridad y cumplan la Política de Seguridad TIC de la Organización.

20. Se valorará positivamente, como garantía, que las herramientas de seguridad dispongan, o estén en proceso de hacerlo, de certificaciones según Criterios Comunes (Common Criteria, CC) o equivalente (ITSEC, TCSEC, etc.).

21. Las certificaciones deberían ser emitidas por un organismo de certificación nacional o internacional reconocido. Se recomienda, como mínimo, un nivel de garantía de evaluación 3 en la certificación CC. En cualquier caso, el nivel de certificación mínimo dependerá del resultado del análisis de riesgos que se lleve a cabo y de la categoría del sistema conforme al ENS.

22. La aprobación de una herramienta de seguridad por parte de la Autoridad correspondiente para un sistema de nivel de protección Alto, cuando no esté certificada o en proceso de certificación, debería basarse en un Plan de Evaluación y Pruebas de Seguridad aprobado por ésta.

23. Un Plan de Evaluación y Pruebas debe contemplar como mínimo lo siguiente:

    a. Ventajas que se obtienen al usar dicha herramienta.

b. Vulnerabilidades o riesgos, si existen, derivados de su uso.

c. Limitaciones de uso.

d. Recursos hardware y software necesarios para su funcionamiento.

e. Experiencia, soporte y formación necesarios para su correcto despliegue y operación.

24. La autorización de uso dependerá de la criticidad del Sistema y de la ausencia de herramientas con este tipo de certificación en el mercado.

25. Las herramientas de cifrado software constituyen un grupo especial, ya que pueden requerir, según la categoría del Sistema, de certificación criptológica adicional.

7.2. CONTROL DE LA CONFIGURACIÓN

26. El control de la configuración de las herramientas de seguridad instaladas con carácter permanente, debe realizarse conforme a los procedimientos de control de la configuración aplicables a los Sistemas de Producción, los cuales a su vez dependerán de la categoría asignada a los mismos conforme a los criterios del ENS.

27. El control de la configuración de las herramientas de seguridad instaladas con carácter temporal, debería realizarse de acuerdo con la correspondiente documentación de seguridad aprobada.

28. A la hora de aplicar cambios en la configuración, requeridos por actualizaciones del proveedor, deberemos tener en cuenta la necesidad o no de nuevas funcionalidades y, en cualquier caso, debe acordarse con el Responsable de Seguridad la idoneidad del cambio en la configuración, ya que se debe a una situación creada por el proveedor y no por una necesidad del organismo y que por tanto no tiene por qué derivar en un cambio. En caso de que se realice el cambio, se deben documentar los requisitos de actualización y la motivación de la misma.

7.3. OPERACIÓN

29. Las herramientas de seguridad deben ser operadas conforme a los procedimientos definidos en la documentación de seguridad aprobada para el sistema. Recordemos que el Esquema Nacional de Seguridad define la necesidad de documentar y aprobar estos procedimientos de operación.

30. Como mínimo los procedimientos definidos para los sistemas deberían cubrir los siguientes aspectos:

a) Control de la configuración y gestión de la herramienta: Definiendo roles y perfiles a implementar, a fin de garantizar que los usuarios tienen el nivel de acceso adecuado a su labor y responsabilidad.

b) Análisis y protección de datos: Se deberá indicar cómo manejar los datos que se obtengan a partir de la operación de la herramienta, así como las maneras de protegerlos frente a modificación, revelación, destrucción, etc. no autorizadas.

c) Definición de operación básica, la cual debe cubrir la mayor parte del día a día de la operación de la herramienta.

d) Gestión de incidentes derivados del uso de la herramienta, indicando las

Autoridades que deben ser informadas y que estarán identificadas en los Procedimientos Operativos de Seguridad del Sistema (POS).

31. El Responsable de Seguridad podrá delegar la gestión de los aspectos anteriores si lo considera oportuno.

32. En el caso de herramientas capaces de explotar vulnerabilidades del sistema, solo podrán ser utilizadas por personal autorizado y en las condiciones definidas para ello. En cualquier caso el uso de herramientas de seguridad debe ser consecuente con la legislación vigente y normas aplicables.

33. Información adicional puede encontrarse en la URL: https://www.gdt.guardiacivil.es/webgdt/legislacion.php

34. La documentación generada por las herramientas de seguridad debe calificarse conforme al procedimiento establecido conforme al ENS (medida de seguridad [mp.info.2]). Conforme a dicho nivel de calificación, se aplicarán las medidas pertinentes para su protección y distribución.

8. RESPONSABILIDADES

35. A continuación definiremos de manera genérica las diferentes responsabilidades y funciones que se deberían considerar durante el ciclo de vida de las herramientas de seguridad, que deben estar alineadas con lo especificado para el cumplimiento con el ENS (medidas de seguridad [mp.per.1] y [mp.per.2]).

8.1. PLANIFICACIÓN Y ADQUISICIÓN

36. Los organismos, a través de las personas responsables de la planificación y adquisición de las herramientas de seguridad y conforme a lo establecido en el organismo para el cumplimiento con el ENS (medidas de seguridad [op.pl.3], [op.pl.4] y [op.pl.5]), deben tener en cuenta al menos lo siguiente:

a) Los Pliegos de Prescripciones Técnicas (PPT) deben contemplar los requisitos obligatorios definidos en esta guía para las herramientas de seguridad.

b) Los PPT deben especificar de manera detallada los requisitos hardware y software de las herramientas de seguridad correspondientes.

c) Los recursos adicionales que se consideren necesarios para la adecuada explotación de las herramientas de seguridad, deben estar reflejados y tenidos en cuenta.

8.2. RESPONSABLE DE SEGURIDAD DEL SISTEMA

37. El Responsable de Seguridad del Sistema es aquella persona designada para desempeñar los roles de responsables del empleo y protección de la información generada por las herramientas.

38. Todas las actividades a realizar por el Responsable de Seguridad del Sistema deben estar reflejadas en la documentación de seguridad del Sistema.

39. El Responsable de Seguridad puede delegar funciones en cuantos Responsables de Seguridad Delegados estime necesario (ver “CCN-STIC-801 ENS responsabilidades y

funciones").

9. HERRAMIENTAS DE AUDITORÍA

40. Son aquellas herramientas cuyo objetivo es el análisis del estado en materia de seguridad de los sistemas en un determinado momento.

41. Los requisitos específicos a considerar para herramientas de seguridad cuya finalidad sea la auditoría se describen a continuación.

9.1. NIVEL DE RED

42. En este grupo se englobaran herramientas que, haciendo uso del nivel de red, obtienen información de los sistemas. Un ejemplo típico de este tipo de herramientas son los escáners de red, los cuales son capaces de identificar servicios (por los puertos TCP o UDP abiertos) y sistemas (por el contenido de los paquetes).

9.2. NIVEL DE SISTEMA

9.2.1. REVISIÓN DE LA CONFIGURACIÓN

43. Existe una familia de herramientas destinadas a realizar auditorías de la configuración del sistema.

44. El valor de este tipo de herramientas reside en la capacidad de poder comparar la configuración de un sistema en diferentes momentos de tiempo. Para poder realizar esta labor es imprescindible contar con una línea base de configuración, considerada "limpia" o de referencia y que estará aprobada por el Responsable de Seguridad del Sistema.

45. Una auditoría es, en esencia, un proceso de recopilación de información para su posterior comparación frente a un estado anterior conocido u objetivo, por tanto una modificación o acción (por ejemplo una intrusión) que no se ajuste a la política de la organización, producirá cambios en los parámetros básicos del Sistema que serán detectados por este tipo de herramientas.

46. Este tipo de herramientas permitirán también facilitar nuestra tarea de ajustarnos a un determinado estándar o nivel de seguridad.

47. La recogida de información para las auditorías puede realizarse de dos maneras:

    a) Local: el componente software que realiza las comparaciones reside en el sistema y contrasta los cambios según una base de datos local.

    b) Remota: se realiza un acceso remoto para recoger la información y se contrastan los cambios en un lugar centralizado.

9.2.2. REVISIÓN DE CONSUMO DE RECURSOS

48. Aunque este tipo de herramientas podría englobarse dentro del conjunto de las dedicadas a la monitorización de los sistemas, pueden resultar de utilidad en caso de no contar con las anteriores. Recopilar información acerca del uso de los recursos es una buena práctica de seguridad. Por ejemplo: un consumo anómalo de ancho de banda o de CPU puede ponernos sobre la pista de un compromiso y uso no autorizado

de un sistema.

9.3. NIVEL DE USUARIO

9.3.1. AUDITORÍA DE CONTRASEÑAS

49. Su principal finalidad es comprobar la robustez de las contraseñas empleadas por los usuarios para acceder a los Sistemas afectados por el ENS, identificando aquellas que no se ajusten a la política de seguridad de la Organización.

50. Para realizar esta labor estas herramientas pueden seguir varios modos de funcionamiento, siendo los más comunes la búsqueda en diccionarios o la comparación de patrones. Finalmente, y en caso de no haber obtenido éxito con otros métodos, se puede verificar la robustez de una contraseña mediante el uso de fuerza bruta.

51. Si la herramienta, una vez averiguada una contraseña, es capaz de mostrarla, debe disponerse de un procedimiento de actuación, ya que de lo contrario se podría estar violando la política de confidencialidad establecida para el cumplimiento de la medida de seguridad [op.acc.1] del ENS.

52. Como funcionalidad adicional, algunas de estas herramientas, además de verificar la robustez de las contraseñas empleadas, permiten generar contraseñas seguras conforme a la política de seguridad establecida.

53. Se recomienda consultar la guía "CCN-STIC-436 Herramientas de análisis de contraseñas".

9.4. NIVEL DE APLICACIÓN

9.4.1. CONTROL Y CALIDAD EN EL DESARROLLO

54. El uso de herramientas de control de versiones (CVS, Concurrent Versions System) nos permiten conocer quién ha modificado cierta parte del código fuente de una aplicación y en qué momento, lo que es fundamental a la hora de auditar cambios en el software. Este tipo de herramientas, además, facilitan el desarrollo, evitan que personal no autorizado tenga acceso o modifique el código, y reducen por lo tanto los errores que se pueden producir a la hora de integrar diferentes partes de código.

55. Existen también herramientas más propias de la mejora en el desarrollo software que de su auditoría, como son las herramientas de integración continua, que dentro de un procedimiento de desarrollo seguro pueden ayudar al auditor a conocer si el software pasó las pruebas de funcionamiento correspondientes.

9.4.2. AUDITORÍA DE CÓDIGO

56. Las herramientas de auditoría de código ayudan en la detección automatizada de errores habituales en la programación. Dichos errores, constituyen en muchas ocasiones la causa última de un problema de seguridad o malfuncionamiento de los sistemas.

57. El uso de herramientas automatizadas de revisión de código, no sustituyen en ningún caso a la auditoría manual realizada por un experto, ya que existen multitud de errores

difíciles de tipificar para su detección automática, además de los relativos a la lógica de negocio propia de la aplicación.

58. El requisito lógico que debe tenerse en cuenta a la hora de elegir una herramienta de este tipo, es que se adapte al entorno utilizado (sistema operativo y lenguaje de programación).

9.4.3. ANÁLISIS DE METADATOS

59. Muchas de las aplicaciones que se emplean, como por ejemplo las herramientas de ofimática para la redacción de documentos o de edición de imágenes, almacenan información en los archivos resultantes que va más allá de almacenar el propio contenido del documento, dado que estas aplicaciones pueden almacenar el nombre del redactor del mismo, datos identificativos de su ordenador (la dirección MAC de la tarjeta de red), ubicación donde se realizó la fotografía, etc.

60. Existen aplicaciones que no permiten controlar o limitar la cantidad de información que añaden al archivo, por lo que es necesario utilizar en dichas circunstancias herramientas que permitan identificar la información adicional añadida al archivo y su eliminación.

9.5. MULTINIVEL

61. Las herramientas referenciadas a continuación requieren para desempeñar su labor el acceso a distintos niveles del entorno (red, sistema, aplicación, usuario y datos).

9.5.1. ANÁLISIS DE VULNERABILIDADES

62. Estas herramientas, que pueden cubrir múltiples niveles (red, sistema, aplicación, usuario y datos), proporcionan información sobre deficiencias de configuración o vulnerabilidades en los distintos componentes software que conforman un Sistema (sistemas operativos, bases de datos, aplicaciones, equipos de comunicaciones, dispositivos de protección de perímetro y otros componentes del sistema).

63. Esta clase de herramientas suele contar con una base de datos de vulnerabilidades conocidas, las cuales utilizan para identificar posibles problemas, aportando además información acerca de las mismas.

64. Este tipo de herramientas debe reunir las siguientes características:

    a) Actualización regular, tanto de la herramienta como de la bases de datos de vulnerabilidades por parte del proveedor.

    b) Posibilidad de realizar análisis específico de una vulnerabilidad o conjunto de vulnerabilidades específico sobre un componente concreto del sistema.

    c) Posibilidad de establecer controles de acceso a la herramienta, a fin de que la misma sólo pueda ser utilizada por personal autorizado.

    d) Generación de informes (reporting) a partir de los análisis realizados. Estos informes deberán poder generarse en varios formatos (HTML, PDF, etc.) y en base a diferentes criterios.

65. Se recomienda ver la guía "CCN-STIC-431 Herramientas de análisis de vulnerabilidades" que recoge en detalle las recomendaciones para la selección,

aprobación y uso de este tipo de herramientas.

10. HERRAMIENTAS DE PROTECCIÓN

10.1. NIVEL DE RED

66. Hoy en día prácticamente cualquier dispositivo de red gestionable ofrece funcionalidades de control y aumento de la seguridad, desde los más sencillos switches con control de acceso y VLANS a complejos sistemas IDS /IPS.

10.1.1. DISPOSITIVOS DE PROTECCIÓN PERIMETRAL

67. Tal y como se comentaba anteriormente existen guías editadas por el CCN como la "CCN-STIC-408 Seguridad Perimetral – Cortafuegos" y "CCN-STIC-811 Interconexión en el ENS" (centrada esta última en el ENS) que tratan en profundidad los dispositivos de protección perimetral. No obstante y en aras de la completitud de esta guía, mencionaremos las herramientas más comunes dentro de este apartado:

a) Routers: Su principal misión es el enrutado del tráfico de una red a otra, aunque es habitual que implementen listas de control de acceso implementado un filtrado de tipo básico.

b) Cortafuegos: Su principal función es establecer controles de acceso entre los distintos segmentos de red que interconecta. Es habitual que cada vez incorporen mayor número de funcionalidades e inteligencia incorporando funcionalidades propias de otros dispositivos.

c) Proxys: dispositivos diseñados específicamente para un protocolo, que se sitúan en medio de la comunicación, ofreciendo posibilidad de establecer controles de acceso, verificar la sanidad del protocolo o añadir funcionalidades adicionales como el cacheo.

d) Dispositivos de sentido único: dispositivos cuya funcionalidad es permitir el tránsito de información en un único sentido.

10.1.2. DETECCIÓN Y PREVENCIÓN DE INTRUSIONES

68. En los últimos tiempos la prevención de intrusiones es una de las áreas que viene experimentando un mayor crecimiento e innovación en el número de herramientas y servicios disponibles. La inmensa mayoría de las herramientas disponibles para estas funciones se pueden agrupar en tres categorías:

a) Detección de intrusiones (IDS): herramientas cuya funcionalidad es la detección de intrusiones en curso o ya logradas, así como la generación de algún tipo de alarma o notificación. Son herramientas con carácter pasivo, su función es detectar y notificar a otras herramientas o personas para que puedan tomar las acciones correctivas necesarias.

b) Prevención de intrusiones (IPS): herramientas cuya funcionalidad es la

prevención de intrusiones, así como la generación de algún tipo de alarma o notificación. Son herramientas con carácter activo, su función es prevenir las intrusiones antes de que se materialicen para lo cual disponen de capacidad de acción bien directa, bien mediante notificación a herramientas de terceros. Un ejemplo de acción de este tipo de herramientas sería la ejecución de un script para introducir una regla en un cortafuegos y así bloquear a un atacante.

c) IDS/IPS: herramientas que integran las funcionalidades de los dos conjuntos anteriores, pudiendo realizar la detección y prevención.

69. Este tipo de herramientas trabajan normalmente analizando el tráfico de red y comparándolo con bases de datos de patrones de ataque conocidos, es por ello que la frecuencia de actualización de este tipo de herramientas, es uno de los factores importantes a tener en cuenta.

70. Se recomienda consultar la guía "CCN-STIC-432 Seguridad perimetral IDS".

10.1.3. GESTIÓN DE RED

71. Su objetivo es facilitar la correcta configuración de los dispositivos de red, facilitando su gestión y permitiendo monitorizar el estado de los mismos.

72. Para realizar la gestión de los dispositivos las herramientas hacen uso de protocolos estándar como SNMP y si disponen de ellos, agentes de monitorización y configuración. La gestión de los dispositivos se realizará desde una consola central.

73. Suelen incluir capacidades de gestión de seguridad de la red para dispositivos que hagan uso de protocolos estándar y en gran parte de los casos incluir características específicas destinadas a un rango limitado de productos propietarios o comerciales.

74. Suelen contar con interfaces, que permiten a los administradores interactuar con la herramienta de manera gráfica.

10.2. NIVEL DE SISTEMA

10.2.1. CONFIGURACIONES DE SEGURIDAD

75. Por configuraciones de seguridad (bastionado) entendemos el conjunto de técnicas que buscan mejorar el nivel de seguridad de un sistema sin alterar la capacidad para desempeñar su labor (aunque en ocasiones afectará a la manera en la que lo hace). Las técnicas empleadas para bastionar un Sistema son diversas, aunque puede establecerse la siguiente categorización básica:

a) Aplicación de parches/extensiones de seguridad.

b) Configuración segura de servicios.

c) Configuración de cortafuegos de Sistema.

d) Fortalecimiento de permisos y contraseñas.

e) Eliminación de cuentas de usuario innecesarias.

f) etc.

76. Existen diversas guías del CCN respecto a la configuración segura de diferentes soluciones, como es el caso por ejemplo de "CCN-STIC-441 Configuración segura de VMware", "CCN-STIC-503A Seguridad en Windows 2003 Server (controlador de dominio)", "CCN-STIC-504 Seguridad en Internet Information Server", "CCN-STIC-610 Seguridad Red Hat Linux 7", "CCN-STIC-636 Seguridad en BD Oracle 10gR2 sobre Red Hat 3 y 4", "CCN-STIC-671 Seguridad de servidor web Apache", etc., por lo que se recomienda su consulta y aplicación.

10.2.2. ACTUALIZACIONES

77. Son herramientas que permiten actualizar los componentes de software de un sistema a su versión más reciente, de manera que a la vez que se incorporan nuevas funcionalidades, se pueden corregir fallos o vulnerabilidades existentes.

78. Aunque este tipo de herramientas suele ser especifico de cada fabricante, cada vez más están surgiendo herramientas centralizadas de gestión, que permiten interactuar con las herramientas propias de cada fabricante de manera única y con herramientas gráficas o web que facilitan su uso, además de ofrecer funcionalidades avanzadas como generación de informes, despliegues de software, control de acceso, etc.

79. Solemos encontrar dos aproximaciones al respecto:

    a) Basadas en agente: los sistemas tienen instalado una componente software (agente) que atiende las peticiones de actualización lanzadas por parte de un servidor. Este determina qué acciones se realizarán en el sistema.

    b) Basada en clientes: suelen conectarse periódicamente a un servidor centralizado para ver si existen nuevas actualizaciones y en caso afirmativo las descarga. Dependiendo de la configuración del sistema es posible que ofrezca o no al usuario la posibilidad de elegir el momento de la actualización.

10.2.3. DETECCIÓN Y PREVENCIÓN DE INTRUSIONES

80. Al igual que existen herramientas para analizar el tráfico de red para identificar y bloquear intentos de ataque a través de la red (10.1.2 Detección y prevención de intrusiones), existen este tipo de herramientas a nivel de sistema, como siguiente línea de defensa para identificar si un usuario autorizado está intentando aumentar su nivel de acceso, intentando realizar modificaciones no autorizadas, etc.

81. Este tipo de herramientas se conocen como HIDS (Host-based Intrusion Detection System, Sistema de Detección de Intrusos basado en Host).

10.3. NIVEL DE APLICACIÓN

10.3.1. CORTAFUEGOS DE APLICACIÓN

82. El cortafuegos de aplicación funciona de una forma muy parecida a los proxys tradicionales, situándose por tanto en medio del flujo de comunicación y añadiendo la posibilidad de realizar reglas de filtrado en base a características avanzadas de los protocolos utilizados.

83. Los cortafuegos de aplicación ha de estar por tanto adaptados a la aplicación que se desea proteger y ser suficientemente flexibles para trabajar con los distintos tipos de contenido que la aplicación pueda aceptar, pudiendo establecer controles sobre la aceptación o no de los mismos.

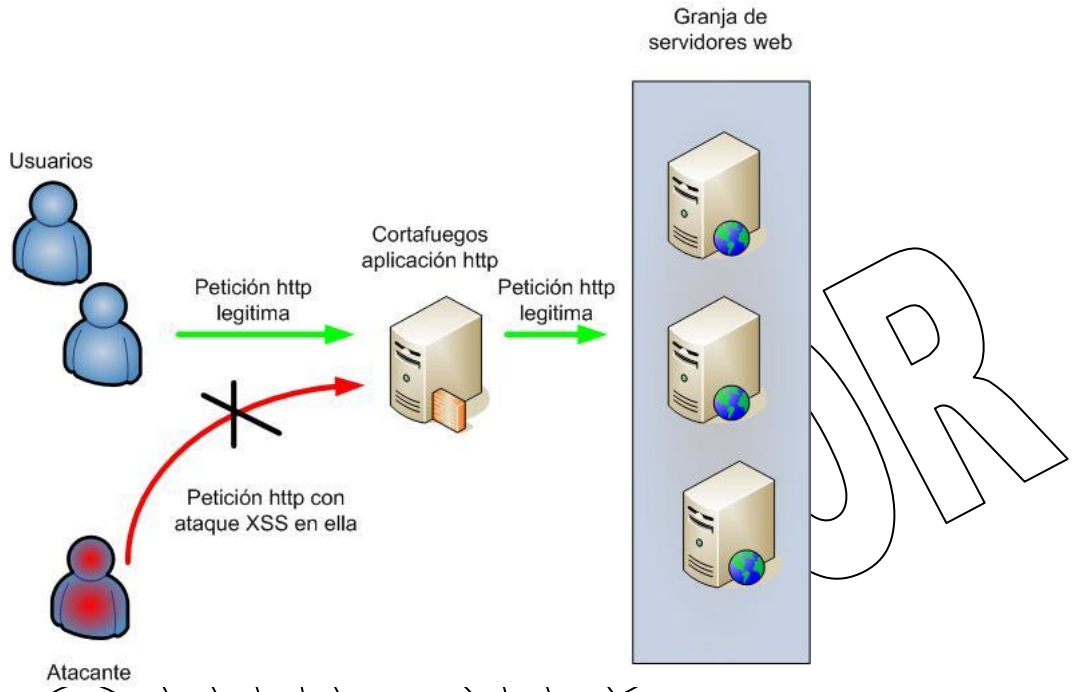

Figura 1. Ejemplo de cortafuegos de aplicación web

84. Es habitual encontrar este tipo de herramientas con posibilidad de incluir diversos módulos para servidores web que protejan frente a XSS, inyecciones SQL, etc.

85. Para más información sobre cortafuegos de aplicación y el despliegue de Modsecurity consulte la guía "CCN-STIC-661 Seguridad en firewalls de aplicación web (Modsecurity)".

10.3.2. LIMPIEZA DE METADATOS

86. Para evitar que se publiquen en una página web documentos que contengan metadatos con información que no debe hacerse pública, existen herramientas que analizan los metadatos de los ficheros que vayan a ser publicados y les eliminan los metadatos no autorizados.

87. Este tipo de soluciones también están disponibles como pasarelas de correo electrónico para eliminar los metadatos existentes en ficheros adjuntos a correos electrónicos.

10.4. NIVEL DE USUARIO

10.4.1. CONTRASEÑAS

88. Existen herramientas que ayudan a los usuarios a la gestión y manejo de contraseñas,

cubriendo aspectos tan dispares como la generación de las mismas (para que cumplan con la política establecida) o su custodia segura, en cuyo caso tienen que cumplir los requisitos establecidos tanto para la robustez de la contraseña como para su almacenamiento cifrado conforme a lo establecido en la medida de seguridad [mp.info.3] del ENS.

89. En caso de que la categoría del sistema no permita el uso de contraseñas, el uso de este tipo de herramientas para la gestión de claves no estará autorizado.

10.4.2. ANTIVIRUS

90. Los puestos de usuario deberán contar con software antivirus operativo, siendo de vital importancia mantener actualizadas conforme a la política establecida las definiciones de virus del mismo.

91. El antivirus deberá estar configurado para identificar amenazas antes de su ejecución en memoria, protegiendo así fuentes de infección como el correo electrónico, la navegación web, el intercambio de ficheros por red o mediante dispositivos, etc.

92. En aquellos entornos de nivel medio y bajo en que no se gestione el software de manera centralizada, se deberá concienciar al usuario sobre la importancia de mantener el software antivirus actualizado y operativo, además de la necesidad de realizar análisis periódicos del equipo. En sistemas de nivel alto se deberá bloquear el acceso a la consola del antivirus (para evitar que el usuario lo desactive). En cualquier caso es recomendable programar escaneos y actualizaciones de manera periódica.

10.4.3. FILTROS ANTISPAM

93. Esta tipo de herramientas centrada específicamente en el correo electrónico, incrementa el nivel de protección del usuario frente a la recepción de correo no deseados (SPAM), los cuales pueden constituir un importante riesgo de entrada de virus, troyanos, phishing y similares.

10.4.4. CIFRADO

94. Dentro de esta categoría se englobarían aquellas herramientas que permiten cifrar información bien para su almacenaje, bien para su transmisión.

95. Al igual que para el cifrado en servidores, es importante comprobar que el método de cifrado usado por la herramienta cumple con los requisitos especificados en la documentación de seguridad.

96. Se recomienda consultar la guía “CCN-STIC-437 Herramientas de cifrado software”.

10.4.5. BORRADO SEGURO

97. En el intercambio de información mediante dispositivos extraíbles de almacenamiento (lápices USB, discos duros externos, etc.), o al desechar ordenadores, puede quedar información sensible accesible a personas no autorizadas, siendo por ello necesario contar con herramientas de borrado seguro que garanticen que no es posible recuperar información que hemos eliminado previamente.

98. Existen varias herramientas de este tipo, pero nos centraremos en aquellas que no destruyen el soporte físico, sino la información y que además lo hace mediante el uso

de software, sin necesidad de contar con aparto alguno. Este tipo de herramientas normalmente borran la información sobrescribiéndola en numerosas ocasiones con caracteres sin valor (por ejemplo 0).

99. Las herramientas que se usen deberán cumplir con la política de borrado seguro, la cual puede exigir un número determinado de sobre escrituras.

11. HERRAMIENTAS DE DETECCIÓN

11.1. NIVEL DE RED

100. A continuación se describen los requisitos específicos a considerar para las herramientas de seguridad cuyo objetivo es la detección.

11.1.1. CAPTURA, MONITORIZACIÓN Y ANÁLISIS DE TRÁFICO

101. Son herramientas cuya funcionalidad es la de la captura del tráfico de red, para su monitorización y posterior análisis.

102. Este tipo de herramientas pueden ser de gran utilidad a la hora de establecer patrones y estadísticas de uso, que a su vez permitirán detectar anomalías.

103. Es recomendable realizar análisis esporádicos del tráfico del Sistema, principalmente en sistemas desplegados con carácter temporal o con tecnologías inalámbricas.

104. Otra de las utilidades de este tipo de herramientas es la verificación de que el tráfico de red que debiera ser cifrado, realmente va cifrado, o la verificación de que no llegan comunicaciones desde redes que no deberían tener acceso.

105. Para utilizar este tipo de herramientas es necesario que la red lo permita, esto es, que los mecanismos de interconexión permitan capturar el tráfico de la red a analizar. En este caso, los hubs (concentradores) permiten la captura del tráfico, mientras que los switches (conmutadores) no lo permiten. No obstante, existen switches que permiten su configuración para habilitar un puerto para la captura del tráfico.

106. Si se usan este tipo de herramientas, es deseable que cuenten con capacidad y posibilidad de analizar todo el flujo de datos existente en la red, de lo contrario la información obtenida será incompleta y se verá mermada la efectividad de las mismas.

107. Cabe recordar que acceder al contenido de las comunicaciones podría suponer una vulneración del artículo 18.3 de la Constitución Española que reza “Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial”. Y también podría suponer una vulneración de la Ley General de Telecomunicaciones (Ley 32/2003, de 3 de noviembre) en su artículo 33 bajo la rúbrica del “Secreto de las comunicaciones”.

108. Por lo tanto, si la herramienta es capaz de mostrar no sólo información sobre el tráfico sino el propio contenido también, debe disponerse de un procedimiento de actuación, ya que de lo contrario se podría estar violando además la política de confidencialidad establecida para el cumplimiento de la medida de seguridad [mp.info.1], [mp.info.2] y [mp.info.3] del ENS.

109. Se recomienda consultar la guía "CCN-STIC-435 Herramientas de monitorización de tráfico".

11.1.2. MONITORIZACIÓN Y SUPERVISIÓN DE DISPOSITIVOS DE RED

110. Este tipo de herramientas que se pueden desplegar también como medida de protección, constituyen una excelente fuente de información sobre el estado y modo de uso de nuestra red.

111. Contar con información sobre el comportamiento normal de nuestra infraestructura es uno de los primeros pasos para detectar una anomalía.

112. La monitorización a menudo se realizara desde una consola central, la cual se conectara a los distintos dispositivos, mediante agentes o protocolos estándar (SNMP, etc.) para recabar la información y generar el reporting y alarmas ante eventos no deseados.

113. Este tipo de herramientas, también suele ofrecer la posibilidad de recibir notificaciones desde los dispositivos, vía protocolos estándar (traps SNMP por ejemplo).

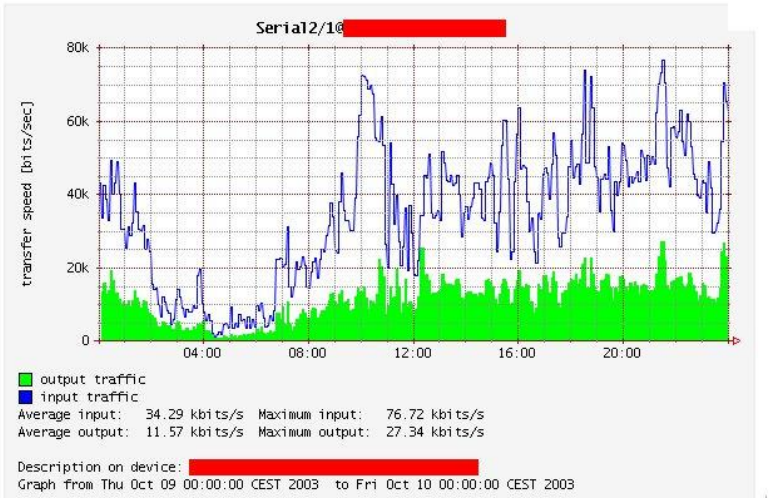

Figura 2. Ejemplo de gráfica de tráfico de red proporcionada por de una herramienta de monitorización

11.2. MULTINIVEL

11.2.1. MONITORIZACIÓN Y ANÁLISIS DE REGISTROS DEL SISTEMA

114. Para poder identificar situaciones que pongan en riesgo la seguridad del Sistema, y para poder conocer quién ha hecho qué y cuándo y con qué resultado, es necesario que los elementos que componen el Sistema generen registros (logs) como mínimo de las operaciones que deseamos monitorizar.

115. De nada sirve contar con muchas herramientas que generan registros, como firewalls, antivirus, aplicaciones, sistemas operativos, etc. si luego dichos registros no son analizados por el Responsable de Seguridad del Sistema (o sus delegados) y se aplican los procedimientos oportunos.

116. Pero la gran cantidad de registros que se generan convierte en una necesidad el contar

con una herramienta que permita:

a) Recopilar todos los logs de los sistemas.
b) Establecer unos permisos de acceso a los logs con independencia de los permisos existentes en el sistema que los ha generado.
c) Evitar que puedan ser alterados o eliminados.
d) Poder realizar búsquedas en dichos logs.
e) Poder ver lo que ha ido ocurriendo como una secuencia de registros.
f) Y, llegados al caso, generar alarmas cuando se identifiquen sucesos fuera de lo común o no autorizados gracias a la correlación de eventos (observando lo que ocurre en varios sistemas como un todo y no con la visión parcial que cada sistema tiene).

117. Todas estas funcionalidades convierten a una herramienta de gestión de logs en una herramienta tanto de auditoría (por su capacidad de recopilar evidencias) como de detección (por su capacidad de análisis y generación de alertas en tiempo real). Esto es lo que se conoce como una herramienta SIEM: Security Information and Event Management.

118. Es importante, a la hora de diseñar una solución de gestión de logs, identificar previamente de qué sistemas vamos a recopilar los logs (aquellos necesarios para identificar un ataque o realizar un análisis forense adecuado) y la cantidad de logs que vamos a almacenar, tanto por consumo de almacenamiento como de transmisión en la red.

119. Por lo tanto, contar con una solución SIEM se convierte en algo fundamental en la protección de la seguridad del Sistema.

120. Se recomienda consultar la guía "CCN-STIC-434 Herramientas para el análisis de ficheros de logs".

12. HERRAMIENTAS DE REACCIÓN

12.1. MULTINIVEL

12.1.1. ANÁLISIS FORENSE

121. En determinadas ocasiones, por ejemplo una vez tengamos constancia de que un sistema ha sido comprometido, o dañado (de manera accidental o premeditada), puede ser necesario determinar la secuencia de acciones que llevaron a esa situación, quién las realizo, desde dónde y qué información ha estado expuesta debido a ella.

122. Es en este tipo de escenarios en el que cobran sentido las herramientas de análisis forense, las cuales mediante técnicas no intrusivas (sin afectar al contenido original de los sistemas) y mediante el análisis de logs, buffers de sistema, contenido de memoria, recuperación de ficheros borrados, etc., etc. permitirán reconstruir la secuencia de eventos que condujeron a la situación actual de seguridad comprometida.

123. La información obtenida por personal cualificado con este tipo de herramientas, constituye un gran valor a la hora de determinar porque se ha producido un problema de seguridad y como solucionarlo en el futuro, además y siempre en las condiciones adecuadas puede ser usada en procesos legales como prueba.

124. Como es lógico, una vez que se ha producido una incidencia de seguridad, es tarde para activar los mecanismos de registro, por lo que éstos deberán ser configurados previamente conforme se indica en la medida de seguridad [op.exp.8] y para los sistemas que sean necesarios conforme a [op.pl.1] del ENS.

125. Es importante recordar que las herramientas de análisis forense deben ser operadas por personal autorizado por el Responsable de Seguridad del Sistema y con los conocimientos técnicos y legales necesarios, ya que cualquier alteración de los sistemas por parte de estas herramientas, puede invalidar la información obtenida como prueba con valor legal.

126. Para llevar a cabo este tipo de actividad, el organismo puede apoyarse en los servicios que presta el CCN-CERT o en otro organismo que le proporcione esta capacidad.

12.1.2. ANÁLISIS DE CÓDIGO DAÑINO

127. Las herramientas de análisis de código, entre las que encontramos descompiladores, desensambladores, etc. permitirán analizar los programas en busca de código malicioso.

128. Este tipo de herramientas se suele basar en la ejecución instrucción a instrucción del código, a la vez que se analizan registros, ficheros accedidos, etc. en busca de un comportamiento malicioso.

129. Este tipo de análisis de bajo nivel es necesario ya que a menudo no se tiene acceso al código fuente de la aplicación sospechosa, además de que es habitual la ocultación del mismo dentro de rutinas aparentemente no dañino y el uso de técnicas de ofuscación de binarios para dificultar su detección.

12.1.3. GESTIÓN DE INCIDENCIAS

130. Una vez identificada una incidencia o incidente, es necesario contar con una herramienta de ticketing que facilite la comunicación por parte de la persona o del sistema que ha identificado la incidencia con las personas con capacidad de respuesta para su análisis y resolución.

131. Para su adecuada resolución y aprendizaje de la misma, es necesario que dicha herramienta proporcione funcionalidades que permitan:

    a) Identificar quién notifica la incidencia.
    b) Identificar cuándo se produce o se notifica.
    c) Identificar el servicio o sistema afectado.
    d) Registrar el detalle de la incidencia.
    e) Registrar las actuaciones que se lleven a cabo.

12.2. NIVEL DE DATOS

12.2.1. BACKUP

132. Las herramientas para gestionar e implementar una política de copias de seguridad (backup) y recuperación adecuada al sistema a proteger, son una de las medidas proactivas más importantes a implementar, ya que nos permitirá recuperar nuestros sistemas al momento anterior (o próximo) a la aparición de un problema.

133. Disponer de una política de backup adecuada es por tanto una de las mejores garantías ante un fallo físico, accidental o de seguridad.

13. CRITERIOS PARA EL EMPLEO DE HERRAMIENTAS DE SEGURIDAD SEGÚN LA CLASIFICACIÓN DEL SISTEMA

Tipo de herramienta	Nivel al que usar	Categoría		
		Básica	Media	Alta
Auditoría	Nivel de red	N.A.	N.A.	Aplica
	Nivel de sistema	N.A.	Aplica	Aplica
	Nivel de usuario	Aplica	Aplica	Aplica
	Nivel de aplicación	Aplica	Aplica	Aplica
	Multinivel	N.A.	N.A.	Aplica
Protección	Nivel de red	Aplica	Aplica	Aplica
	Nivel de sistema	Aplica	Aplica	Aplica
	Nivel de usuario	Aplica	Aplica	Aplica
	Nivel de aplicación	N.A.	Aplica	Aplica
Detección	Nivel de red	N.A.	Recomendado	Aplica
Reacción	Multinivel	N.A.	Aplica	Aplica
	Nivel de datos	Recomendado	Aplica	Aplica

Tabla 1. Criterios de empleo según clasificación del sistema.

14. ANEXO A. RELACIÓN DE HERRAMIENTAS ORIENTATIVAS

134. A continuación se exponen algunas de las herramientas existentes más significativas que cubren parte de las soluciones técnicas que un organismo podría necesitar en el ámbito del ENS.

Tipo de herramienta	Herramienta orientativa	Fabricante	Plataforma	Licenciamiento
Control y calidad en el desarrollo	Subversion	Apache Software Foundation	Multiplataforma	Gratuita
	Git	Software Freedom Conservancy, Inc. (Software libre)	Multiplataforma	Gratuita
	Rational ClearCase	IBM	Multiplataforma	Comercial
	Jenkins	Jenkins CI	Multiplataforma	Gratuita
Auditoría de código	Sonar	SonarSource	Multiplataforma	Gratuita
	Checkstyle	Software libre	Multiplataforma	Gratuita
	FindBugs	University of Maryland	Multiplataforma	Gratuita
Análisis y/o limpieza de metadatos	Libextractor	Gnu.org	Multiplataforma	Gratuita
	Doc Scrubber	Brightfort	Windows	Gratuita
	MetaStripper	PhotoThumb.com	Windows	Gratuita
	OOMetaExtractor	Informática64	Windows	Gratuita
	FOCA	Informática64	Windows	Gratuita y Comercial
	Metaviewer	Pinpoint Laboratories	Windows	Gratuita
	BatchPurifier	Digital Confidence	Windows	Comercial
Detección y prevención de intrusiones (HIDS)	OSSEC	Trend Micro, Inc.	Multiplataforma	Gratuita
	Tripwire	Tripwire, Inc.	Multiplataforma	Comercial
Limpieza de metadatos	MetaShield Protector	Informática64	Windows	Comercial
	MailValve GX	Digital Confidence	Windows	Comercial
	Metadact-e	Litéra	Windows	Comercial

Tipo de herramienta	Herramienta orientativa	Fabricante	Plataforma	Licenciamiento
Cifrado	TrueCrypt	TrueCrypt Foundation	Multiplataforma	Gratuita
	GnuPG[2]	Free Software Foundation, Inc.	Multiplataforma	Gratuita
Captura, monitorización y análisis de tráfico	Snort	Sourcefire, Inc.	Multiplataforma	Gratuita
	Wireshark	Wireshark Foundation	Multiplataforma	Gratuita
Monitorización y análisis de logs	OSSIM	AlienVault	Linux	Gratuita y Comercial
	Bitacora	S21Sec	Linux	Comercial
	LogICA	Grupo ICA	Linux	Comercial
	iView	Cyberoam	Multiplataforma	Gratuita
	ArcSight	HP	Multiplataforma	Comercial
	NetIQ	Novell	Máquina virtual	Comercial
	QRadar	IBM	Appliance	Comercial
	NitroSecurity	McAfee	Appliance	Comercial
	LogLogic	LogLogic Inc.	Máquina virtual	Comercial
	Splunk	Splunk Inc.	Multiplataforma	Comercial
Análisis de código dañino	IOC Finder	Mandiant	Windows	Gratuita
	IOC Editor	Mandiant	Windows	Gratuita
	Redline	Mandiant	Windows	Gratuita
	IDA	Hex-Rays	Multiplataforma	Gratuita y Comercial
	OllyDbg	Oleh Yuschuk	Windows	Gratuita
	HijackThis	Trend Micro	Windows	Gratuita
	IceSword	pjf	Windows	Gratuita
	GMER	GMER	Windows	Gratuita
	Process Monitor	Microsoft (Sysinternals)	Windows	Gratuita
Gestión de incidencias	GLPI	Asociación Indepnet	Multiplataforma	Gratuita
	MantisBT	MantisBT Group	Multiplataforma	Gratuita

[2] Se recomienda consultar la guía "CCN-STIC-955 Recomendaciones de empleo de GnuPG".

Tipo de herramienta	Herramienta orientativa	Fabricante	Plataforma	Licenciamiento
	OTRS Help Desk	OTRS Inc.	Multiplataforma	Gratuita
	Redmine	Jean-Philippe Lang	Multiplataforma	Gratuita
	Request Tracker	Best Practical Solutions LLC.	Linux	Gratuita
	Request Tracker for Incident Response	Best Practical Solutions LLC.	Linux	Gratuita
	Jira	Atlassian	Multiplataforma	Comercial

15. ANEXO B. PLANTILLA AUDITORÍA USO DE HERRAMIENTAS

Tarea			Clasificación del Sistema según el ENS			Medida de Seguridad según el ENS	Observaciones
			Bajo	Medio	Alto		
Designación del Responsable de Seguridad del Sistema			Aplica	Aplica	Aplica		
Existencia documentación de seguridad del Sistema			Aplica	Aplica	Aplica		
Herramientas de Auditoría	Nivel de red		N/A	Aplica	Aplica		
	Nivel de Sistema	Revisión de la configuración	N/A	Aplica	Aplica	op.exp.3	
		Revisión del consumo de recursos	N/A	N/A	Aplica	op.pl.4 mp.s.8	
	Nivel de Usuario	Auditoría de contraseñas	N/A	Aplica	Aplica	op.acc.5	
	Nivel de Aplicación	Herramientas de control y calidad en el desarrollo	N/A	Aplica	Aplica	mp.sw.1	
		Herramientas de auditoría de código	N/A	Aplica	Aplica	mp.sw.2	
		Herramientas de análisis de metadatos	Aplica	Aplica	Aplica	mp.info.6	

Tarea			Clasificación del Sistema según el ENS			Medida de Seguridad según el ENS	Observaciones
			Bajo	Medio	Alto		
	Multi-Nivel	Herramientas de análisis de vulnerabilidades	N/A	Aplica	Aplica	mp.sw.2	
Herramientas de Protección	Nivel de Red	Dispositivos de protección perimetral	Aplica	Aplica	Aplica	mp.com.1 mp.com.2 mp.com.3 mp.com.4	
		Herramientas IDS / IPS	N/A	N/A	Aplica	op.mon.1 mp.s.2 mp.s.8	
		Herramientas de gestión de red	N/A	N/A	Aplica	mp.s.8	
	Nivel de Sistema	Configuraciones de seguridad	N/A	Aplica	Aplica	op.exp.2	
		Herramientas de gestión de actualizaciones	N/A	Aplica	Aplica	op.exp.4	
		Herramientas HIDS	N/A	N/A	Aplica	op.mon.1	
	Nivel de Aplicación	Cortafuegos de aplicación	Aplica	Aplica	Aplica	mp.s.2	
		Limpieza de metadatos	Aplica	Aplica	Aplica	mp.info.6	

Tarea			Clasificación del Sistema según el ENS			Medida de Seguridad según el ENS	Observaciones
			Bajo	Medio	Alto		
	Nivel de Usuario	Herramientas de gestión de contraseñas	N/A	N/A	N/A	op.acc.5	
		Antivirus	Aplica	Aplica	Aplica	op.exp.6 mp.s.1	
		Filtros antispam	Aplica	Aplica	Aplica	mp.s.1	
		Cifrado	N/A	N/A	Aplica	mp.si.2	
		Borrado seguro	N/A	Aplica	Aplica	mp.si.5	
Herramientas de Detección	Nivel de Red	Captura, monitorización y análisis de tráfico	N/A	Recomendado	Aplica	op.pl.4 mp.com.2 mp.com.4	
		Monitorización y supervisión de dispositivos de red	N/A	Recomendado	Aplica	op.pl.4 mp.s.8	
	Multinivel	Monitorización y análisis de registros del sistema	N/A	N/A	Aplica	op.exp.10	
Herramientas de Reacción	Multinivel	Análisis forense	N/A	N/A	Aplica	op.exp.7 op.exp.9	
		Análisis de código dañino	N/A	N/A	Aplica	op.exp.7 op.exp.9	
		Gestión de incidencias	N/A	Aplica	Aplica	op.exp.9	

Tarea			Clasificación del Sistema según el ENS			Medida de Seguridad según el ENS	Observaciones
			Bajo	Medio	Alto		
	Nivel de Datos	Backup	Recomendado	Aplica	Aplica	mp.info.9	

16. ANEXO C. GLOSARIO DE TÉRMINOS Y ABREVIATURAS

Término	Significado
Common Criteria	Estándar internacional para la certificación de la seguridad en computadoras que pretende garantizar que el software se comporta conforme a las especificaciones.
CVS	Herramienta de control de versiones de gran utilidad en entornos de desarrollo software.
Escáner de red	Herramienta de seguridad cuyo objetivo es la detección de los sistemas conectados a la red, así como los servicios que estos puedan estar prestando.
IDS	Sistema de detección de intrusiones.
IPS	Sistema de prevención de intrusiones.
Ofuscación	Proceso de ocultar o dificultar el acceso a la información mediante técnicas de camuflaje, encriptación, compresión, etc.
Phishing	Delito informático consistente en obtener información confidencial de forma fraudulenta y haciendo uso de la ingeniería social.
POS	Procedimientos Operativos de Seguridad del Sistema
PPT	Pliego de prescripciones técnicas
SNMP	Protocolo estándar de Gestión de Red
SQL Injection	Técnica de ataque, cuyo objetivo es hacer uso de alguna vulnerabilidad en la validación de entradas en una aplicación para pasar código SQL no autorizado a una base de datos no accesible a priori para el atacante.
Troyano	Software malicioso que simula habitualmente ser software legitimo y que puede tener como misión ser una puerta trasera de entrada al sistema o recolectar/enviar información.
VLAN	Técnica consistente en crear redes lógicas dentro de una misma red física.
Vulnerabilidad	Error de programación o diseño que permite explotar el sistema de una manera diferente a la original.
XSS	Ataque informático que hace uso de vulnerabilidades en el sistema de validación de HTML.

17. ANEXO D. EJEMPLO USO DE HERRAMIENTAS

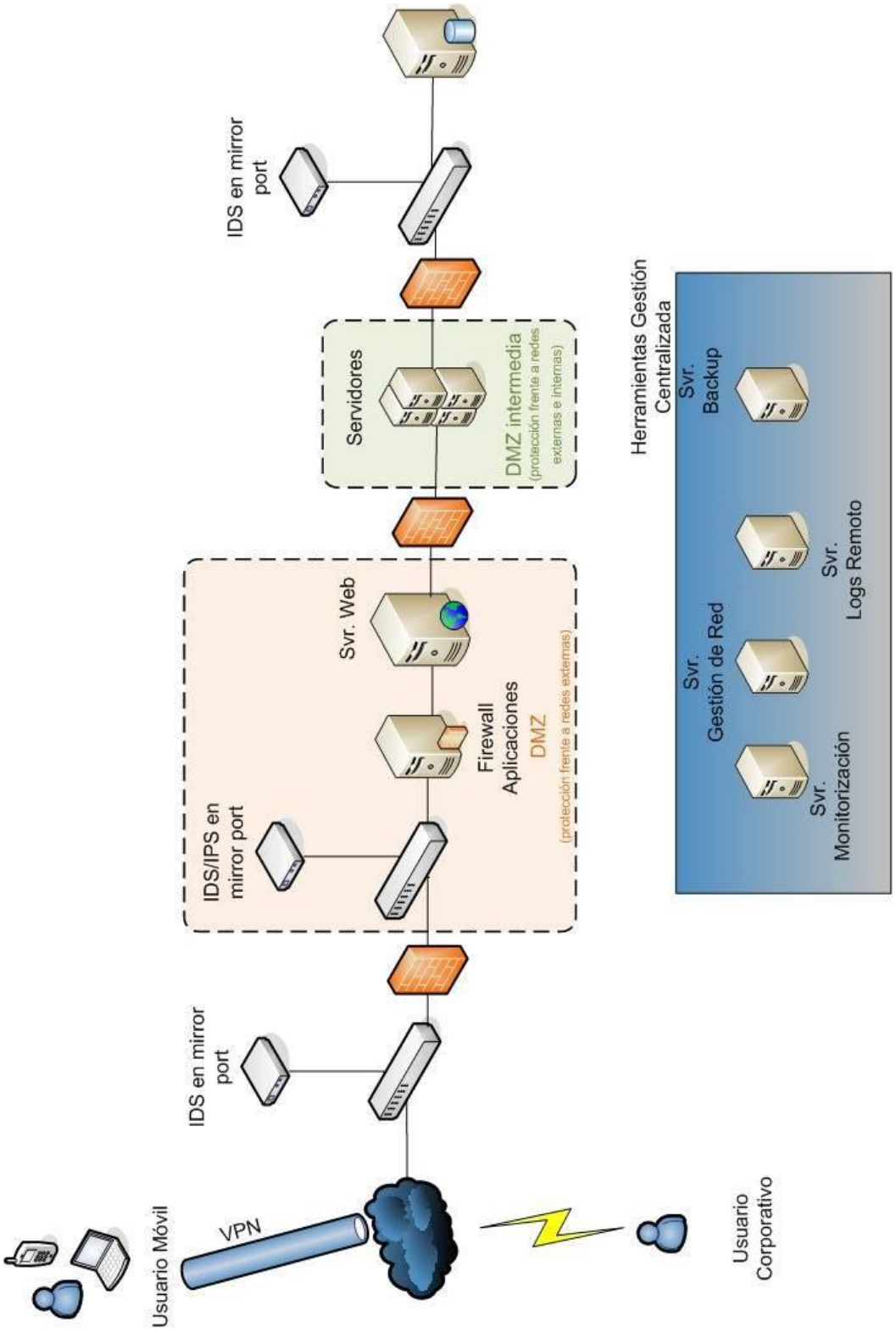

Figura 3. Ejemplo de esquema de red en que muestra el uso de herramientas de seguridad

18. ANEXO E. REFERENCIAS

CCN-STIC-408 Seguridad Perimetral – Cortafuegos

CCN-STIC-412 Requisitos de Seguridad de Entornos y Aplicaciones Web

CCN-STIC-430 Herramientas de Seguridad

CCN-STIC-431 Herramientas de Análisis de Vulnerabilidades

CCN-STIC-432 Seguridad Perimetral – IDS

CCN-STIC-434 Herramientas para el Análisis de ficheros de logs

CCN-STIC-435 Herramientas de Monitorización de Tráfico

CCN-STIC-436 Herramientas de Análisis de Contraseñas

CCN-STIC-437 Herramientas de Cifrado Software

CCN-STIC-441 Configuración segura de VMware

CCN-STIC-503A Seguridad en Windows 2003 Server (controlador de dominio)

CCN-STIC-504 Seguridad en Internet Information Server

CCN-STIC-610 Seguridad Red Hat Linux 7

CCN-STIC-636 Seguridad en BD Oracle 10gR2 sobre Red Hat 3 y 4

CCN-STIC-661 Seguridad en firewalls de aplicación web (Modsecurity)

CCN-STIC-671 Seguridad de servidor web Apache

CCN-STIC-801 ENS responsabilidades y funciones

CCN-STIC-803 Valoración de sistemas en el Esquema Nacional de Seguridad

CCN-STIC-811 Interconexión en el ENS

CCN-STIC-955 Recomendaciones de empleo de GnuPG