ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA DE SISTEMAS

ANÁLISIS DE RIESGOS Y VULNERABILIDADES DE LA INFRAESTRUCTURA TECNOLÓGICA DE LA SECRETARÍA NACIONAL DE GESTIÓN DE RIESGOS UTILIZANDO METODOLOGÍAS DE ETHICAL HACKING

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS INFORMÁTICOS Y DE COMPUTACIÓN

OSWALDO ANDRÉS ACOSTA NARANJO

andresacosta.sn@gmail.com

DIRECTOR: ING. CESAR GUSTAVO SAMANIEGO BURBANO

gustavo.samaniego@epn.edu.ec

Quito, Marzo 2013

DECLARACIÓN

Yo, Oswaldo Andrés Acosta Naranjo, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

_____

Oswaldo Andrés Acosta Naranjo

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Oswaldo Andrés Acosta Naranjo, bajo mi supervisión.

_____

Ing. Gustavo Samaniego
DIRECTOR DE PROYECTO

AGRADECIMIENTOS

Agradezco a Dios, por haberme guiado desde el principio de mi vida personal y académica, quien me permitió llegar a concluir esta etapa de mi carrera.

Agradezco principalmente a mi padre Oswaldo Acosta y a mi madre Teresa Naranjo, por estar presentes durante todos los años de estudio, por su incansable apoyo y por enseñarme que las metas se cumplen con esfuerzo y sacrificio propio.

Agradezco profundamente a mis hermanas Catalina, Silvia, Evelin, Ivon y Mariatere, por el apoyo incondicional que me brindaron para la culminación de mi carrera .

Agradezco a mis cuñados y a mis sobrinas, que me brindaron su total apoyo y que de una u otra forma han contribuido a la culminación de mis estudios.

Agradezco especialmente a mi novia Andreita, por su amistad, cariño e incondicional amor, por el apoyo durante la realización de este proyecto y porque siempre creyó en mí.

A los amigos, Edgar, Sociedad y a todos aquellos y aquellas con los cuales he compartido momentos agradables durante mis estudios y que siempre han estado allí.

Andrés Acosta

DEDICATORIA

Dedico especialmente este trabajo a mis padres que siempre me apoyaron, y por haberme dado las bases de sacrificio y honestidad para culminar mis estudios.

A mis hermanas, cuñados y sobrinas que siempre estuvieron presentes con su apoyo y consejos en cada momento de mi vida estudiantil.

A mi novia que siempre me apoyo desde el inicio hasta el fin de este proyecto.

Andrés Acosta

CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

El presente proyecto permite realizar un Análisis de Riesgos y Vulnerabilidades de la Infraestructura Tecnológica de la Secretaría Nacional de Gestión de Riesgos, con el propósito de determinar si existe un entorno seguro para los sistemas y servicios que ofrece la Institución, así como planes de mitigación de riesgos tecnológicos.

El Primer Capítulo, presenta información de la Secretaría Nacional de Gestión de Riesgos y de la dirección de Tecnologías de la Información y Comunicación.

El Capítulo Dos, contiene la descripción de las metodologías de Ethical Hacking a utilizar, con las respectivas justificaciones comparativas de su elección. Una vez seleccionada la metodología ISSAF draft 0.2.1, se realiza la identificación de riesgos la cual se divide en identificación de activos o puntos de acceso e identificación y búsqueda de vulnerabilidades, esta última es la fase en la cual se realizan las pruebas de testeo de seguridad, en las cuales se identifican las vulnerabilidades presentes en cada una de las entidades de evaluación definidas por la metodología. Luego se realiza el análisis de riesgos, en segunda instancia la evaluación y valoración de riesgo, y finalmente se procede con el análisis de impacto técnico e impacto de negocio.

El Tercer Capítulo, presenta el desarrollo del plan de mitigación de riesgos basado en el análisis de impacto, en el cual se describen las contramedidas recomendadas por la metodología; además, se presentan conclusiones y recomendaciones las mismas que permitirán mitigar los riesgos detectados.

Finalmente en el Cuarto Capítulo, se exponen las conclusiones y recomendaciones formuladas al finalizar el presente proyecto.

PRESENTACIÓN

El presente documento muestra un Análisis de Riesgos y Vulnerabilidades para la Infraestructura Tecnológica de la Secretaría Nacional de Gestión de Riesgos, utilizando la Metodología de Ethical Hacking ISSAF draft 0.2.1, con el cual se pretende transformar entornos informáticos inseguros en entornos protegidos, logrando una clara evaluación de los mismos, planificando las medidas oportunas para mantener los riesgos bajo control, y teniendo en cuenta los procesos del negocio para así mantener la información a salvo, garantizando su confidencialidad, integridad y disponibilidad.

El motivo por el cual se realiza el análisis de riesgos y vulnerabilidades, es por problemas de seguridad presentados constantemente en los sistemas y servicios que ofrece la Secretaría Nacional de Gestión de Riesgos, además de la inexistencia de planes de mitigación de riesgos, lo que provoca que los problemas de seguridad sean solucionados por el personal de TIC a medida que ocurren.

La utilización de la metodología ISSAF y del conjunto de herramientas libres recomendadas para cada una de las pruebas de evaluación, permite realizar una identificación completa de las vulnerabilidades y una evaluación de los riesgos a medida que se realizan las pruebas; además, cada prueba de evaluación contempla su conjunto de contramedidas y recomendaciones que permitirán reducir el riesgo a un nivel aceptable.

CAPÍTULO 1

1. CARACTERIZACIÓN DE LA INSTITUCIÓN

1.1 INFORMACIÓN DE LA SECRETARIA NACIONAL DE GESTIÓN DE RIESGOS

"El Gobierno Nacional ha expresado en reiteradas ocasiones su decisión de trabajar sostenidamente a fin de que la Gestión integral para la reducción de riesgos y manejo de emergencias y desastres se convierta en una Política de Estado, con la finalidad del buen vivir de la población, asegurado los logros del desarrollo y bienestar social en el largo plazo.

Bajo estas premisas surge la reciente iniciativa de crear una organización sistémica para la reducción de riesgos y manejo de emergencias y desastres. Por ello con fecha 26 de abril del 2008, mediante Decreto Ejecutivo 1046-A, se creó la Secretaría Técnica de Gestión de Riesgos, como entidad adscrita al Ministerio Coordinador de Seguridad Interna y Externa. Asumió todas las competencias, atribuciones, funciones, representaciones y delegaciones que eran ejercidas por la Dirección Nacional de Defensa Civil.

Con fecha 10 de Septiembre de 2009, mediante Decreto Ejecutivo 42, se eleva de Secretaría Técnica de Gestión de Riesgos a Secretaría Nacional de Gestión de Riesgos, la cual ejercerá sus competencias de manera independiente, Descentralizada y Desconcentrada."[1]

1 Fuente, http://www.snriesgos.gob.ec/quienes-somos.html, (marzo 2012)

Misión Institucional[2]

Construir y liderar el Sistema Nacional Descentralizado de Gestión de Riesgos (SNDGR) para garantizar la protección de personas, colectividades y la naturaleza de los efectos negativos de emergencias o desastres de origen natural o antrópico, generando políticas, estrategias y normas que permitan gestionar técnicamente los riesgos para la identificación, análisis, prevención y mitigación de los mismos; construir capacidades en la ciudadanía que le permitan enfrentar y manejar eventos de emergencia o desastre; recuperar y reconstruir las condiciones sociales, económicas y ambientales afectadas por dichos eventos, así como contar con todas las capacidades humanas, técnicas y de recursos para la respuesta eficiente a situaciones de emergencia.

Visión Institucional[3]

En un lapso de cinco años, ser reconocida en el ámbito nacional e internacional por la implementación, consolidación y administración del Sistema Nacional Descentralizado de Gestión de Riesgos del Ecuador a través del cumplimiento efectivo de la misión institucional.

1.1.1 ESTRUCTURA ORGÁNICA POR PROCESOS

"El organigrama de la Secretaría Nacional de Gestión de Riesgos, se utiliza invariante para los dos regímenes existentes: uno permanente, para situaciones de normalidad; y otro, para estados de emergencia oficialmente declarados.

En situaciones declaradas formalmente como de emergencia, las necesidades coyunturales podrían provocar cambios en las relaciones entre las diferentes unidades administrativas o que se articulen de manera diversa, sin que esto signifique cambios a la estructura organizativa."[4]

---

2 Fuente, Estatuto Orgánico de Gestión Organizacional por Procesos de la SNGR, Articulo 7
3 Fuente, Estatuto Orgánico de Gestión Organizacional por Procesos de la SNGR, Articulo 7
4 Fuente, Estatuto Orgánico de Gestión Organizacional por Procesos de la SNGR, Articulo 8

En la figura 1-1 se indica la Estructura Orgánica de la Secretaría Nacional de Gestión de Riesgos, resaltando la Dirección de Tecnologías de Información y Comunicación.

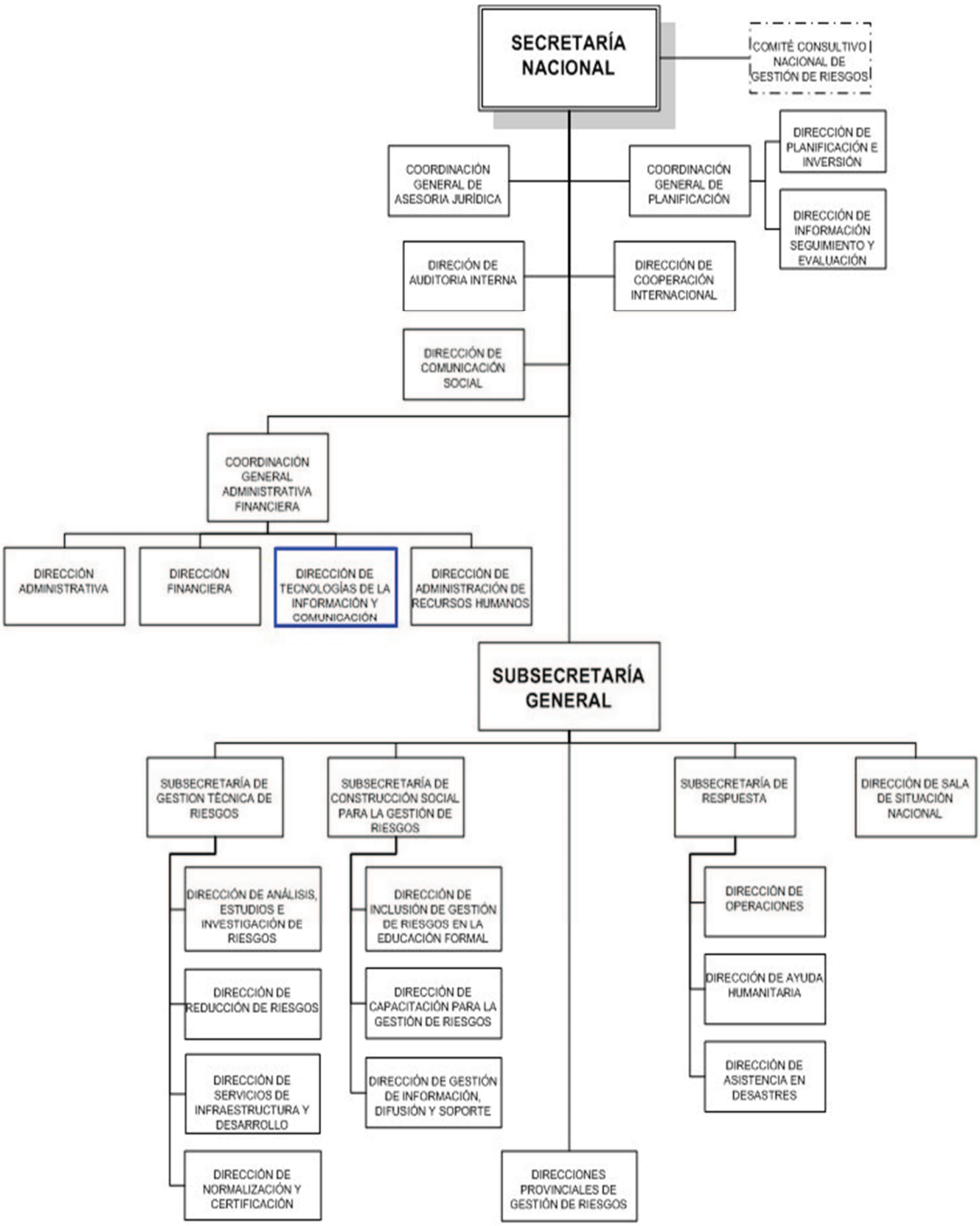


Figura 1-1: Estructura Orgánica por Procesos[5]

5 Fuente, Estatuto Orgánico de Gestión Organizacional por Procesos de la SNGR, Articulo 8

1.2 DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES

La Dirección de TIC[6] de la SNGR[7], tiene alcance a nivel nacional en cuanto a sus funciones, razón por la cual mantiene los recursos informáticos y de comunicaciones actualizados y funcionando de manera correcta para así poder dar respuestas rápidas y oportunas a los desastres o emergencias que se presenten.

Misión[8]

Ejecutar las políticas, estrategias, normas, planes, programas y proyectos con la finalidad de definir y ejecutar la planificación informática institucional con el fin de investigar, proporcionar y administrar nuevas tecnologías de información y comunicaciones que faciliten y optimicen la gestión. Contará con tres oficinas de Centro de Datos (Data Center), establecidos en Quito, Guayaquil y Coca, para mantenimiento de datos y sistemas en casos de emergencia.

1.2.1 PROCESOS Y SERVICIOS DE TIC

Administración de los Servicios de Producción

Es la administración del centro de datos, definida por planes de servicios de producción, de requerimientos tecnológicos de sistemas informáticos y licencias de uso; además, contempla planes de mantenimiento preventivo y correctivo de las aplicaciones y sistemas informáticos, políticas de seguridad de la información, y la elaboración de procedimientos e instructivos para respaldo y recuperación de información institucional, así como el plan de implementación.

---

6 TIC, Tecnologías de Información y Comunicaciones
7 SNGR, Secretaría Nacional de Gestión de Riesgos
8 Fuente, Estatuto Orgánico de Gestión Organizacional por Procesos de la SNGR, Articulo 3.2.1.3

Administración de los Servicios de TIC

Son los servicios en el portal institucional, el correo institucional, el SNIGR[9], la Intranet, y la ayuda y soporte técnico a usuarios finales; además, contempla la actualización continua de inventarios informáticos, para posteriores planes de mantenimiento preventivo y correctivo de hardware y software instalado.

Gestión de la Investigación y Gestión de Proyectos de TIC

Son planes y programas de integración e interoperabilidad interinstitucional con sistemas similares de otras instituciones públicas o privadas, especialmente con los actores del SNDGR[10]; también contempla la investigación de nuevos proyectos de tecnología, desarrollados e implementados para atender situaciones de emergencia.

Administración de Comunicaciones

Es la operación y supervisión de los servicios de voz, con planes y programas de contingencia para mantener la disponibilidad y la operación de la infraestructura de telecomunicaciones.

9 SNIGR, Sistema Nacional de Información para la Gestión de Riesgos
10 SNDGR, Sistema Nacional Descentralizado de Gestión de Riesgos

CAPÍTULO 2

2. ANÁLISIS DE RIESGOS Y VULNERABILIDADES

2.1 DETERMINACIÓN DE LA METODOLOGÍA DE ETHICAL HACKING A UTILIZARSE

El Ethical Hacking, consiste en pruebas de penetración controladas que no incluyen obligatoriamente ganar acceso privilegiado de los sistemas informáticos y/o de comunicaciones, permitiendo descubrir deficiencias de seguridad y vulnerabilidades, para su posterior análisis, determinación del grado de riesgo y sus posibles soluciones.

OSSTMM[11] e ISAFF[12], utilizan ethical hacking en sus metodologías, razón por la cual es necesario describir cada una de ellas y determinar cuál es la más adecuada a utilizarse.

2.1.1 DESCRIPCIÓN DE LA METODOLOGÍA OSSTMM

OSSTMM versión 2.2, es un manual con metodologías que permiten realizar pruebas y análisis de seguridad utilizando la metodología OML[13], y es publicado bajo “Licencia Creative Commons”[14] 3.0, lo que permite su uso y libre distribución.

---

11 OSSTMM, Open Sourse Security Testing Methodology Manual, (Manual de la Metodología Abierta de Testeo de Seguridad)

12 ISSAF, Information Systems Security Assessment Framework, (Marco de Evaluación de Seguridad de Sistemas de Información)

13 OML, Open Methodology License, (Licencia de Metodología Abierta), http://www.isecom.org/oml.html, (abril 2012)

14 Licencia Creative Commons, (Licencia de Bienes Comunes Creativos), http://creativecommons.org/licenses/by-nc-sa/3.0/es/, (abril 2012)

"ISECOM[15] exige que un testeo de seguridad solamente sea considerado por OSSTMM cuando sea:

- Cuantificable.
- Consistente y que se pueda repetir.
- Válido más allá del período de tiempo "actual".
- Basado en el mérito del testeador y analista, y no en marcas comerciales.
- Exhaustivo.
- Concordante con leyes individuales y locales y el derecho humano a la privacidad."[16]

Mapa de Seguridad

El mapa de seguridad es una imagen del ambiente de análisis de seguridad y está compuesta por seis secciones equivalentes que se superponen entre si y contienen elementos de todas las otras secciones; en la figura 2-1, se observa el mapa de seguridad con los diferentes puntos de revisión de la metodología.

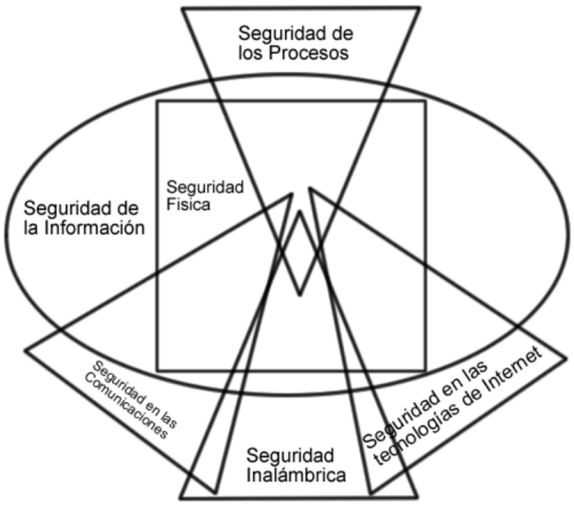


Figura 2-1: Mapa de Seguridad[17]

15 ISECOM, The Institute for Security and Open Methodologies, (Instituto de Seguridad y Metodologías Libres)
16 Objetivos ISECOM, Fuente: OSSTMM versión 2.1, página 11
17 Fuente: OSSTMM versión 2.1, página 23

La lista de módulos se encuentra en el *Anexo 1*; y de acuerdo al mapa de seguridad son los elementos primarios de cada sección, e incluyen todas las Dimensiones de Seguridad que están integradas con tareas a ser desarrolladas.

2.1.1.1 Metodología OSSTMM

"La metodología de OSSTMM fluye desde el módulo inicial hasta completar el módulo final permitiendo la separación entre recolección de datos y pruebas de verificación de los datos recolectados; también determina los puntos precisos de cuando extraer e insertar estos datos."[18]

En la figura 2-2, se muestra el flujo de la metodología desde un punto de presencia de seguridad y cada módulo tiene una entrada y una salida; la entrada es la información usada en el desarrollo de cada tarea y la salida es el resultado de las tareas completadas.

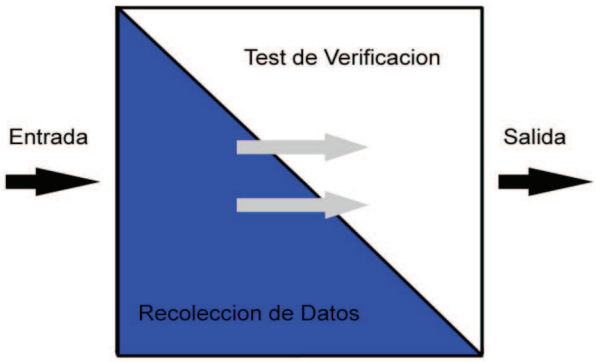


Figura 2-2: Metodología OSSTMM[19]

La salida puede o no ser datos analizados que sirven como entrada para otro módulo o incluso puede ocurrir que la misma salida sirva como entrada para más de un módulo o sección; y las tareas son las pruebas de seguridad a ejecutarse dependiendo de la entrada del módulo, los resultados de las tareas son considerados la salida del módulo y pueden ser analizados inmediatamente para actuar como un resultado procesado o se pueden dejar sin analizar.

18 Metodología OSSTMM, Fuente: OSSTMM versión 2.1, página 32
19 Fuente: OSSTMM versión 2.1, página 32

OSSTMM tiene un conjunto de reglas, lineamientos y métodos para realizar un testeo de seguridad de cada sección con presencia de seguridad, en la que se incluyen plantillas de datos de pruebas de seguridad con los módulos y tareas, pero con la desventaja de que son solamente para algunos módulos específicos de determinadas secciones; en la figura 2-3, se observa la estructura de las pruebas y tareas.

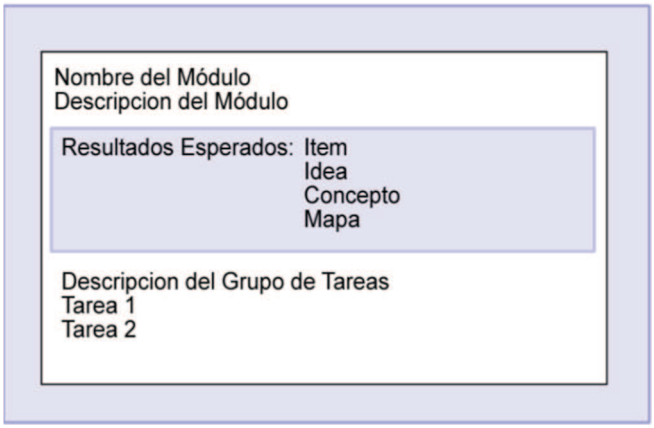


Figura 2-3: Estructura de las Pruebas y Tareas[20]

2.1.1.2 Análisis y Evaluación de Riesgos con OSSTMM

El proceso de un análisis de seguridad, se concentra en evaluar las áreas que reflejan los niveles de seguridad presentes, siendo estos las Dimensiones de Seguridad; y la evaluación de riesgo recopila todos los datos que sirven de soporte para una evaluación válida por medio de testeos no privilegiados.

Las dimensiones de seguridad definidas por OSSTMM son:

- Visibilidad
- Acceso
- Confianza
- Autenticación
- Confidencialidad
- Privacidad
- Autorización
- Integridad
- Seguridad

20 Fuente: OSSTMM versión 2.1, página 31

"Integrados a cada módulo, se encuentran los Valores de la Evaluación de Riesgo (RAVs). Estos se definen como la degradación de la seguridad (o elevación del riesgo) sobre un ciclo de vida específico, basándose en mejores prácticas para tests periódicos.

El tipo de riesgo tal y como se designa por OSSTMM, está definido por:

- Identificado, pero no investigado o con resultados no concluyentes.
- Verificado, con un positivo absoluto o una vulnerabilidad explotada, o
- No aplicable, debido a que no existe porque la infraestructura o mecanismo de seguridad no se encuentra presente."[21]

Para determinar los valores de evaluación de riesgos (RAVs) se establece una tabla con los tipos de riesgos definidos por OSSTMM como son vulnerabilidad, debilidad, preocupación, filtrado de información, y desconocidos; y para los parámetros de evaluación se definen valores de verificado, identificado y no aplicable; y de acuerdo a como se muestra en la tabla 2-1.

	Verificado	***Identificado***	***No Aplicable***
Vulnerabilidad	3.2	1.6	0.8
Debilidad	1.6	0.8	0.4
Preocupación	0.8	0.4	0.2
Filtrado de Información	0.4	0.2	0.1
Desconocidos	0.2	0.1	-

Tabla 2-1: Valores de la Evaluación de Riesgos de OSSTMM[22]

21 Valores de Evaluación del Riesgo, Fuente: OSSTMM versión 2.1, página 28
22 Tabla elaborada por el autor, Fuente: OSSTMM versión 2.1, página 29

2.1.2 DESCRIPCIÓN DE LA METODOLOGÍA ISSAF

ISSAF versión 0.2.1, es una metodología estructurada con procedimientos muy detallados para pruebas y análisis de seguridad en varios dominios, contempla detalles de criterios de evaluación con objetivos específicos para cada una de las pruebas de tal modo que reflejen situaciones de la vida real, y es publicado bajo licencia GNU[23] GPL[24].

"La información contenida en ISSAF se organiza en los criterios de evaluación definidos por:

- Sus objetivos y su descripción.
- Los pre-requisitos para la realización de las evaluaciones
- El proceso para la evaluación
- Muestra los resultados esperados
- Las medidas recomendadas
- Y las referencias a documentos externos"[25]

2.1.2.1 Metodología ISSAF

ISSAF, enfoca su metodología alrededor de lo que son los Criterios de Evaluación; en la figura 2-4, se observan las tres fases de la metodología.

23 GNU, GNU is Not Unix, (GNU No es Unix acrónimo recursivo)
24 GPL, General Public Licence, (Licencia Publica General)
25 Criterios de evaluación, Fuente: ISSAF versión 0.2.1, página 18

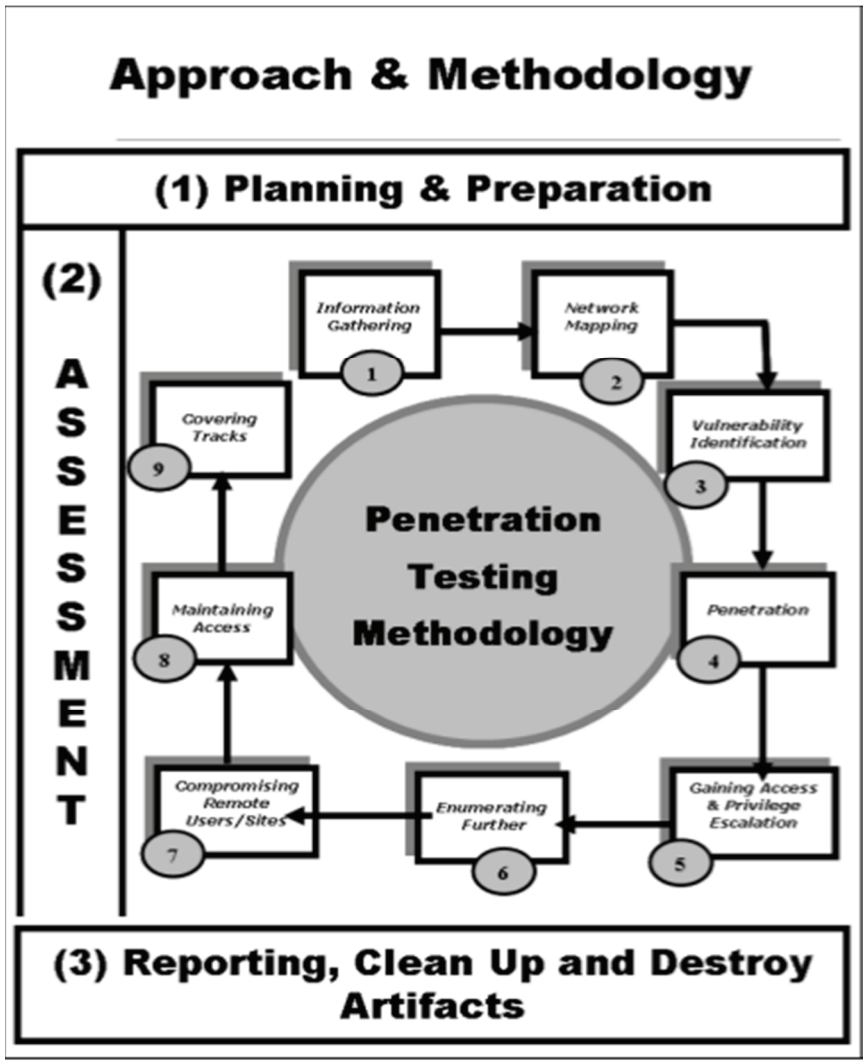


Figura 2-4: Metodología ISSAF[26]

Pre – evaluación: planificación y preparación

"En este punto se definen las áreas de alcance, que pueden incluir:

- Organización completa.
- Ubicación específica.
- División específica (s) / Sub-división (s)
- Limitaciones y condiciones para las evaluaciones.
- La naturaleza de las pruebas (intrusiva / no intrusiva)
- Pruebas desde el exterior, interior o ambas.

26 Fuente: ISSAF versión 0.2.1, página 137

- Las direcciones IP o rangos que se debe evaluar.
- La dirección IP específica o subred, host, dominio que se debe restringir.
- Dirección IP de origen de la máquina donde la evaluación y las pruebas serán llevadas a cabo.
- En el contexto de presencia en la web
  - Nombres de servidor (interno)
  - Nombres de Dominio (DNS)
  - Direccionamiento IP
- En el contexto de la Infraestructura permitir el acceso remoto."[27]

La fase también consta de plantillas para la identificación de los puntos de acceso basados en la arquitectura de diseño para cada nivel de la red, lo que permite armar un cuadro completo de la infraestructura tecnológica de la Institución, y que puede servir como base para la siguiente fase.

Evaluación

Es la fase en la que se llevan a cabo las pruebas, e involucran los procesos de recolección de información, mapeo de red, identificación de vulnerabilidades, penetración, obtención de acceso y escalada de privilegios, enumeración de usuarios, comprometer sitios y usuarios remotos, mantenimiento del acceso, y cubrimiento de huellas.

ISSAF, presenta plantillas que utilizan controles para realizar una evaluación técnica; en la figura 2-5, se muestra la plantilla para pruebas de penetración con los objetivos, pre-requisitos, procesos, descripción detallada de la técnica a utilizar, ejemplos y resultados, herramientas recomendadas, contramedidas, referencias a documentos, enlaces externos, y comentarios globales.

27 Áreas de Alcance, Fuente: ISSAF versión 0.2.1, página 67

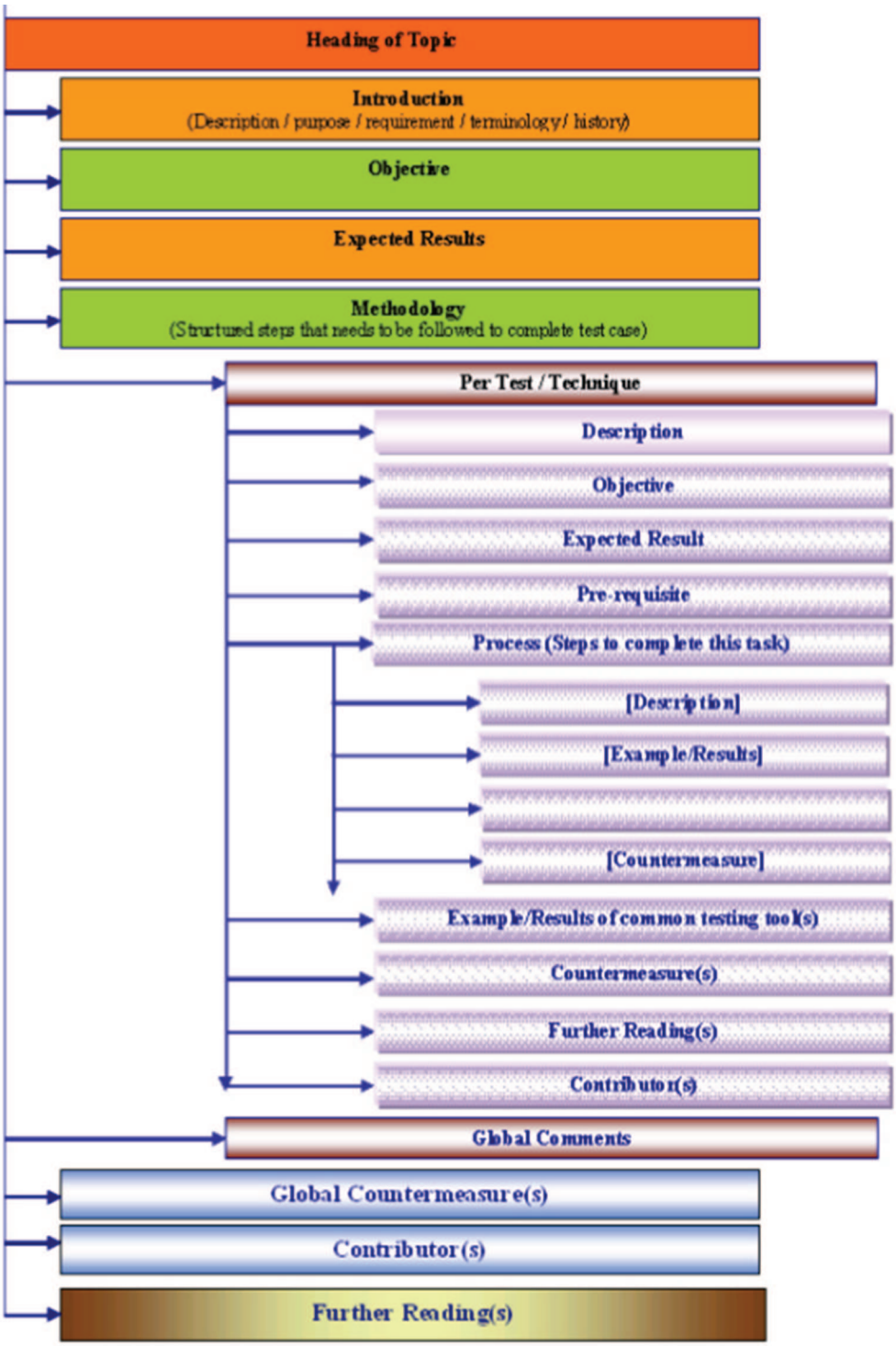


Figura 2-5: Estructura para las Pruebas[28]

28 Fuente: ISSAF versión 0.2.1, página 23

“Luego de identificar los puntos de acceso específicos, se realiza la identificación de puntos débiles explotables con actividades que incluyen:

- Recolección de información.
- Realizar un mapeo de red.
- Identificar los servicios vulnerables en puertos abiertos o filtrados.
- Realizar un análisis de vulnerabilidad para buscar vulnerabilidades conocidas.
- Realizar verificación de falsos positivos y falsos negativos.
- Enumerar las vulnerabilidades descubiertas.
- Estimar el impacto probable (clasificando las vulnerabilidades encontradas)
- Identificar las rutas de ataque y escenarios para la explotación.”[29]

Pos – evaluación: reportes, limpieza y destrucción de artefactos

Esta fase contempla la generación de reportes, uno verbal para informar que se ha identificado asuntos críticos en la seguridad; y otro escrito, con detalles como alcances, objetivos, tiempos de prueba, evaluaciones realizadas, informe de vulnerabilidades con el nombre, su descripción, su nivel de riesgo, contramedidas, y un plan de acción con recomendaciones, observaciones y conclusiones presentadas en una tabla con prioridades de acuerdo al nivel de impacto en la seguridad; también en esta fase, se procede con la limpieza de información y/o artefactos utilizados en las pruebas de penetración.

2.1.2.2 Análisis y Evaluación de Riesgos con ISSAF

El análisis de los resultados de las pruebas establece como objetivo identificar y posteriormente verificar vulnerabilidades detectadas en la evaluación, para luego establecer contramedidas y recomendaciones.

29 Identificación de vulnerabilidades, Fuente: ISSAF versión 0.2.1, página 139

“Riesgo puede ser definido como la pérdida potencial sufrida para el negocio como un resultado de un evento no deseado que se traduce en la pérdida ya sea de negocios o provocada por la interrupción de las operaciones comerciales.”[30]

“El objetivo principal de la evaluación de riesgos es identificar los riesgos y las acciones a ser implementadas para mitigar esos riesgos y hacerlas descender a un nivel aceptable. La salida se puede detallar en un documento que comúnmente se denomina Registro de Riesgos.

El registro de riesgos es una lista de elementos que comprenden lo siguiente:

- Las entidades clasificadas por importancia para el negocio.
- Sus amenazas afines, clasificadas por su probabilidad de ocurrencia.
- Vulnerabilidades clasificadas por su criticidad.

Y lo ideal, para que el registro de riesgos sea eficaz, debe incluir también información con respecto a:

- Los pasos que se deben tomar para mitigar esos riesgos.
- Las responsabilidades asignadas.
- Cronograma para la aplicación de los controles.”[31]

ISAFF, también establece controles de evaluación de riesgos que permiten mitigar o reducir el riesgo, asignando valores o niveles de riesgo tanto para el análisis de impacto técnico como para el análisis de impacto de negocio.

Los valores definidos para el impacto técnico se clasifican según su severidad en vulnerabilidades de riesgo muy alto, alto, medio, bajo, muy bajo y asignándoles valores de 1 a 0.2 respectivamente; y para los valores de impacto de negocio se realiza en función de las amenazas asignándoles valores de riesgo alto, medio y bajo.

En el *Anexo 2,* se encuentra las entidades de evaluación consideradas por ISSAF.

---

30 Definición de Riesgo, Fuente: ISSAF versión 0.2.1, página 89
31 Objetivo de la Evaluación de Riesgos, Fuente: ISSAF versión 0.2.1, página 94

2.1.3 SELECCIÓN DE LA METODOLOGÍA

Para determinar la metodología a utilizarse; en la tabla 2-2, se comparan aspectos fundamentales de las metodologías OSSTMM e ISSAF.

ASPECTOS	ISSAF	OSSTMM
Permite realizar pruebas y análisis de seguridad	Si	Si
Establece requisitos previos para la evaluación	Si	No
La metodología define un proceso detallado para la realización de pruebas	Si	Si
Define áreas de alcance	Si	No
Contiene plantillas para realizar las pruebas	Si	Si
Detalla técnicas para cada prueba	Si	No
Contiene ejemplos de pruebas y resultados	Si	No
Recomienda herramientas para cada prueba	Si	No
Presenta procesos de análisis y evaluación de riesgos	Si	Si
Define dimensiones de seguridad a evaluar	No	Si
Establece valores o niveles de evaluación de riesgos	Si	Si
Enumera y clasifica las vulnerabilidades encontradas	Si	No
Realiza estimación de impacto	Si	Si
Genera reportes e informes	Si	No
Presenta contramedidas y recomendaciones	Si	No
Contiene referencias a documentos y enlaces externos	Si	No

Tabla 2-2: Comparación de Metodologías[32]

Del análisis comparativo se determina que ISSAF versión 0.2.1, es una metodología que reúne los aspectos más importantes para identificar riesgos, analizarlos, evaluarlos y posteriormente establece medidas para reducir su impacto.

32 Tabla elaborada por el autor, Fuente: OSSTMM versión 2.1, ISSAF versión 0.2.1

2.2 IDENTIFICACIÓN DE RIESGOS

El presente capítulo tiene como objetivo identificar activos y vulnerabilidades de la infraestructura tecnológica de la Secretaria Nacional de Gestión de Riesgos, utilizando la metodología ISSAF versión 0.2.1; en la tabla 2-3, se muestra las áreas de alcance y los parámetros iniciales definidos en conjunto con la Dirección de TIC, para las siguientes fases de la metodología y posteriores capítulos.

Áreas de Alcance	***Parámetros***
Organización completa	Solamente la dirección de TIC
Ubicación especifica	Centro de Datos Quito
División especifica	TIC
Limitaciones y condiciones	No provocar interrupción en los sistemas y servicios
Naturaleza de las pruebas	No intrusivas
Origen de las pruebas	Internas
Direcciones IP o rangos a evaluar	Direcciones IP de los servidores del Centro de Datos
Dirección IP, subred o dominio restringido	Bases de datos del SNIGR
Dirección IP origen de las evaluaciones y pruebas	Dirección IP signada por el servidor DHCP[33]
Información de servidores y direccionamiento IP	Proporcionada por el área de Infraestructura y telecomunicaciones
Permitir el acceso remoto	Si

Tabla 2-3: Áreas de Alcance[34]

2.2.1 IDENTIFICACIÓN DE ACTIVOS

ISSAF, no establece parámetros ni procesos para la identificación de activos, pero en la fase de pre - evaluación muestra importancia a la identificación de puntos de acceso, que consisten en establecer una posición de inicio o partida para las pruebas de evaluación, considerando para ello el diseño de arquitectura de red y la ayuda técnica del área de TIC.

33 DHCP, Dynamic Host Configuration Protocol, (Protocolo de Configuración de Dinámica de Host)
34 Tabla elaborada por el autor, Fuente: ISSAF versión 0.2.1, página 67

2.2.1.1 Identificación del Diseño de Arquitectura de Red

La metodología ISSAF contiene plantillas que establecen elementos clave, con puntos de acceso a evaluar dentro de cada una de las capas y bloques del diseño de arquitectura de red.

El Centro de Datos de Quito ubicado en el edificio del COEN[35], es el punto principal para la interconexión con las provincias y matriz a través de una red de datos que provee CNT[36]; actualmente solo se tiene definido un diseño de arquitectura de red para las instalaciones del Centro de Datos de Quito, donde se centraliza la infraestructura tecnológica de la SNGR, en todas las otras oficinas no está definida la red por capas; en la figura 2-6, se observa el diagrama de arquitectura de red.

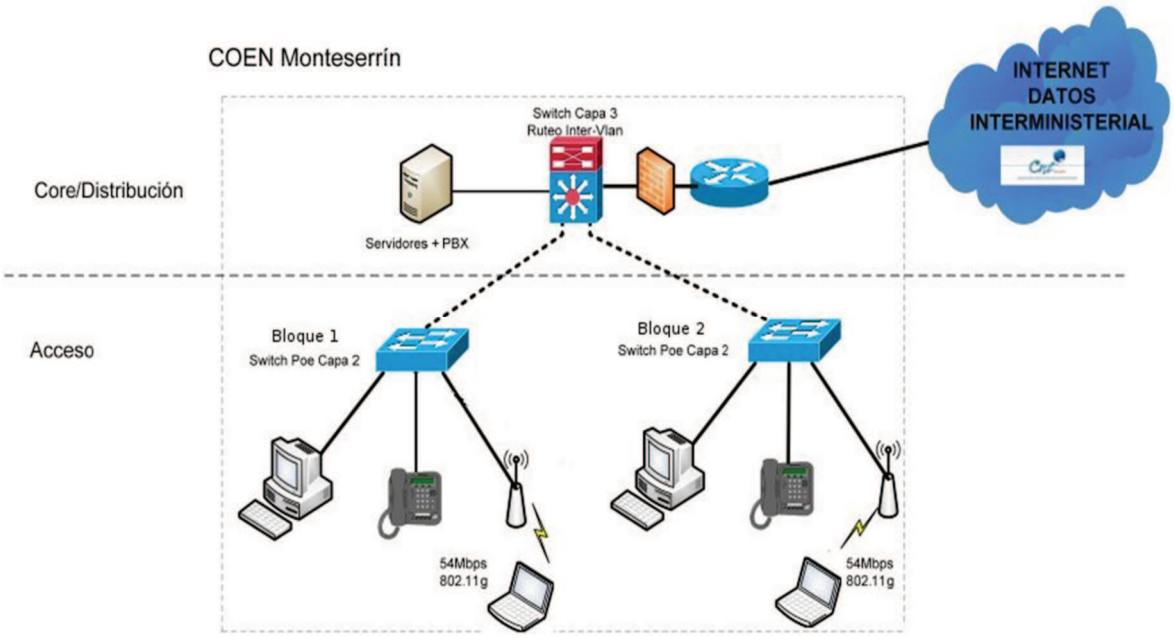


Figura 2-6: Diseño de Arquitectura de Red de la SNGR[37]

35 COEN, Comite de Operaciones de Emergencia Nacional
36 CNT, Corporación Nacional de Telecomunicaciones
37 Fuente, Área de Infraestructura y Telecomunicaciones SNGR

La infraestructura tecnológica de la SNGR cuenta con tecnologías como fibra óptica, ADSL[38] y Wimax[39] que permiten la conexión de los distintos equipos, componente y elementos que forman parte de la arquitectura de red; en la figura 2-7, se observa el diagrama físico de interconexión del Centro de Datos con las provincias y matriz.

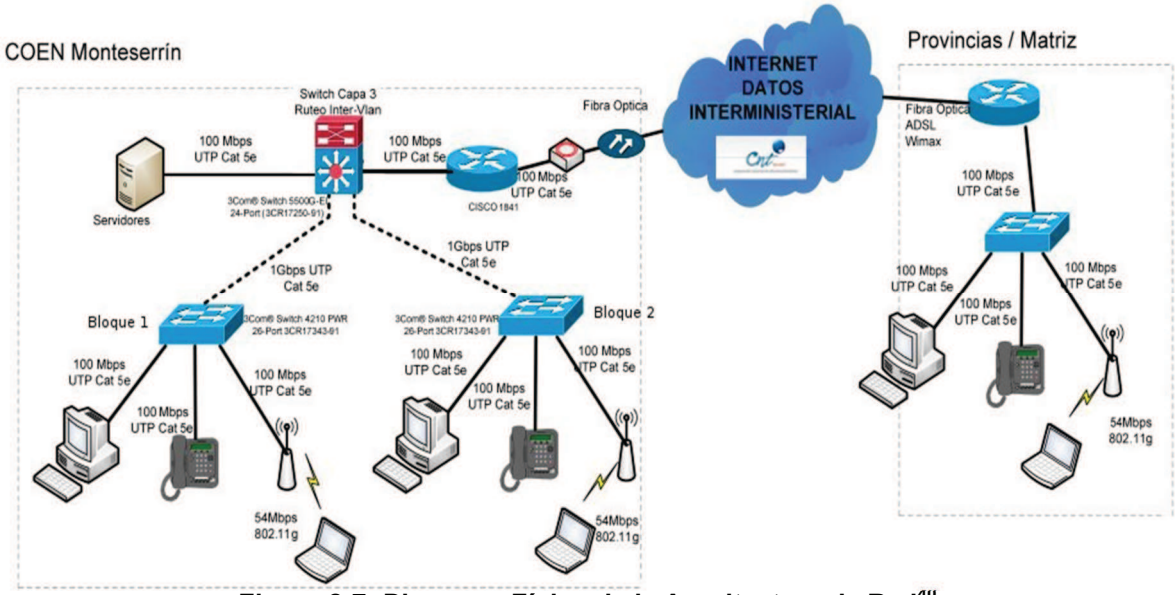


Figura 2-7: Diagrama Físico de la Arquitectura de Red[40]

Capa de acceso

La arquitectura de red de la SNGR tiene separado los diferentes tráficos VLAN[41] con enrutamiento estático; en la tabla 2-4, se muestran los dos switchs PoE[42] capa-2 con sus respectivos puntos de acceso.

Elementos Clave a Evaluar	***Puntos de Acceso***
Switch Capa-2 [Switch Bloque 1]	172.16.200.1/24
Switch Capa-2 [Switch Bloque 2]	172.16.201.1/24

Tabla 2-4: Capa de Acceso[43]

38 ADSL, Asymmetric Digital Subscriber Line, (Línea de Abonado Digital Asimétrico)
39 Wimax, Worldwide Interoperability for Microwave Access, (Interoperabilidad Mundial para Acceso por Microondas)
40 Fuente, Área de Infraestructura y Telecomunicaciones SNGR
41 VLAN, Virtual Local Area Network, (Red de Área Local Virtual)
42 PoE, Power Over Ethernet, (Alimentación a través de Ethernet)
43 Tabla elaborada por el autor, Fuente: ISSAF versión 0.2.1, página 71

Capa Core/Distribución

La metodología ISSAF determina por separado los elementos clave a evaluar para la capa de distribución y para la capa Core, pero la infraestructura tecnológica de la SNGR cuenta solamente con un equipo core que también tiene las funciones de la capa de distribución; en la tabla 2-5, se muestra el switch capa-3 Inter-VLAN y su punto de acceso.

Elementos Clave a Evaluar	Puntos de Acceso
Switch Capa-3 [Core]	192.168.0.22/24

Tabla 2-5: Capa Core[44]

Bloque de servidores

La metodología ISSAF considera a determinados servidores como elementos clave a evaluar para este bloque; en la tabla 2-6, se observan los puntos de acceso para el bloque de servidores.

Elementos Clave a Evaluar	Puntos de Acceso
Firewall	192.168.0.5/24
HIDS[45]	No tiene
NIDS[46]	No tiene
Administración de Voz IP[47]	172.16.108.1/24
Servidor DNS[48]	192.168.0.5/24
Servidor HTTP[49]	192.168.0.16/24 www.snriesgos.gob.ec
Servidor de Correo	172.16.104.30/24
Servidor NTP[50]	No tiene
Servidor de Certificados	No tiene

Tabla 2-6: Bloque de Servidores[51]

44 Tabla elaborada por el autor, Fuente: ISSAF versión 0.2.1, página 73
45 HIDS, Host based Intrusion Detection Systems, (Sistema de Detección de Intrusos basada en Host)
46 NIDS, Network based Intrusion Detection Systems, (Sistema de Detección de Intrusos basada en Red)
47 IP, Internet Protocol, (Protocolo de Internet)
48 DNS, Domain Name System, (Sistema de Nombres de Dominio)
49 HTTP, Hypertext Transfer Protocol, (Protocolo de Transferencia de Hipertexto)
50 NTP, Network Time Protocol, (Protocolo de Tiempo de Red)
51 Tabla elaborada por el autor, Fuente: ISSAF versión 0.2.1, página 76

Bloque de administración

La metodología ISSAF tiene elementos clave a evaluar para el Bloque de Administración, en las que se incluyen puntos de acceso de servidores considerados en la administración de la infraestructura tecnológica de Institución, pero el diseño de arquitectura de red de la SNGR no cuenta con equipos para dicho bloque.

Bloque WAN

En la tabla 2-7, se observa los elementos clave a evaluar para el bloque WAN[52]

Elementos Clave a Evaluar	*Puntos de Acceso*
Firewalls	190.152.148.109/29
NIDS	No tiene
Routers	190.152.148.105/29 186.46.57.225/27

Tabla 2-7: Bloque WAN[53]

Bloque de Internet

La Centro de Datos de Quito cuenta con dos direcciones IP públicas para el servicio de Internet, pero solamente utiliza una de ellas; en la tabla 2-8, se observan los puntos de acceso a evaluar para el bloque de Internet.

Elementos Clave a Evaluar	*Puntos de Acceso*
Firewalls	190.152.148.109/29
HIDS	No tiene
NIDS	No tiene
Concentrador VPN[54]	No tiene
Servidor HTTP	190.152.148.108/29 www.snriesgos.gob.ec
Servidor DNS	190.152.148.109/29

Tabla 2-8: Bloque de Internet[55]

52 WAN, Wide Area Network, (Red de Área Amplia)
53 Tabla elaborada por el autor, Fuente: ISSAF versión 0.2.1, página 77
54 VPN, Virtual Private Network, (Red Privada Virtual)

2.2.2 IDENTIFICACIÓN Y BÚSQUEDA DE VULNERABILIDADES

Las vulnerabilidades son debilidades en los sistemas informáticos y/o de comunicaciones, que pueden estar presentes dentro de procesos u operaciones, y que podrían ser explotadas por una amenaza, con el propósito de obtener acceso no autorizado a la información o de interrumpir procesos críticos.

Ambiente para las pruebas

La metodología ISSAF contiene técnicas específicas para cada una de las pruebas con herramientas recomendadas, ejemplos y resultados; la distribución GNU/Linux "BackTrack 5 R2"[56], contiene una gran variedad de herramientas especializadas en seguridad informática que pueden ser útiles para realizar las pruebas; por tal razón se procede a instalar BackTrack en un entorno virtualizado, y configurado de tal forma que pueda obtener una dirección IP del Servidor DHCP.

2.2.2.1 Recopilación de Información

La recopilación de información se basa esencialmente en usar el Internet para encontrar toda la información posible sobre el objetivo usando técnicas como (DNS / WHOIS[57]), que consiste en consultas a bases de datos en busca de información de un dominio o dirección IP.

Una vez recolectada la mayor cantidad de información del diseño de arquitectura de red, se determina como elemento inicial a evaluar, los puntos de acceso del servidor HTTP del Bloque de Internet; en la figura 2-8, se muestra la consulta mediante línea de comandos a la base de datos whois.

```
~$ whois snriesgos.gob.ec
```

Este TLD[58] no dispone de servidor whois, pero puede acceder a la base de datos de whois en http://www.nic.ec/whois/eng/whois.asp

55 Tabla elaborada por el autor, Fuente: ISSAF versión 0.2.1, página 78
56 BackTrack 5 R2, Fuente: http://www.backtrack-linux.org/, (marzo 2012)
57 WHOIS, protocolo TCP basado en petición y repuesta que efectúa consultas a bases de datos, Fuente: http://es.wikipedia.org/wiki/WHOIS, (mayo 2012)
58 TLD, Top Level Domain, (Dominio de Nivel Superior)

```
~$ whois 190.152.148.109
% Joint Whois – whois.lacnic.net
inetnum:        190.152.148.104/29
status:         reallocated
owner:          SECRETARIA TECNICA DE GESTION DE RIESGOS
ownerid:        EC-STGR-LACNIC
responsible:    JHOJAN CORONEL
address:        DE LOS NARANJOS 0 Y DE LAS AZUCENAS ESQ. N. 60-74, SECTOR
MONTESERRI
address:        3110 - QUITO - PI
phone:          +593  87731418

inetnum-up:     190.152.128/17
person:         Evelin Gavilanes
e-mail:         noc@ANDINANET.NET
phone:          +593 2 2944800
created:        20030402
changed:        20111018
```

Figura 2-8: Consulta con Whois

La primera consulta no encuentra información relacionada al nombre de dominio en las bases de datos de whois, y la consulta con la dirección IP muestra información de contactos, números de teléfono y geolocalización, que es útil como punto de partida, ya que puede ser considerado como objetivo de ingeniería social.

2.2.2.1.1 Selección de la Herramienta de Recopilación de Información

Para determinar la herramienta de recopilación de información a utilizarse; en la tabla 2-9, se comparan aspectos fundamentales de Maltego[59] y de Netglub[60].

59 Maltego, Fuente: http://www.paterva.com/web5/, (mayo 2012)
60 Netglub, Fuente: http://www.netglub.org, (mayo 2012)

ASPECTOS	Maltego	Netglub
Aplicación forense y de recolección de información	Si	Si
Aplicación de Código Abierto	Si	Si
Muestra información referente a la red, al dominio y a personas	Si	Si
Realiza relaciones inteligentes entre elementos de red, dominio y personas	Si	No
Realiza verificación de las direcciones de correo electrónico	Si	No
Identifica vínculos entrantes para sitios web	Si	No
Extrae metadatos desde archivos y fuentes de dominios	Si	No
Realiza búsqueda de blogs y referencias por frases	Si	No
Realiza búsquedas más profundas	Si	No
Exporta y/o salvar los resultados obtenidos	Si	Si

Tabla 2-9: Comparación de Herramientas de Recopilación de Información[61]

Del análisis comparativo se determina que Maltego, es una herramienta que reúne los aspectos más importantes para la recopilación de información de Internet.

Maltego

Es una herramienta rápida, flexible y centralizada que permite la minería y recolección de información útil del Internet, además de la representación de esta información de una forma útil para que sea sencilla de analizar; junto con sus librerías gráficas permite identificar relaciones clave entre la información e identificar previamente relaciones con la posibilidad de entrelazar y encadenar los resultados.

Maltego permite consultar registros de servidores de nombres NS[62] y de intercambio de correo MX[63]; en la figura 2-9, se muestran los principales registros del dominio snriesgos.gob.ec, con sus respectivas direcciones IP.

61 Tabla elaborada por el autor

62 NS, Name Server, (Servidor de Nombres), Registro que asocia un nombre de dominio con servidores de nombres que almacenan información de dicho dominio.

63 MX, Mail Exchange, (Intercambio de Correo), Registro que asocia un nombre de dominio a una lista de servidores de intercambio de correo para dicho dominio.

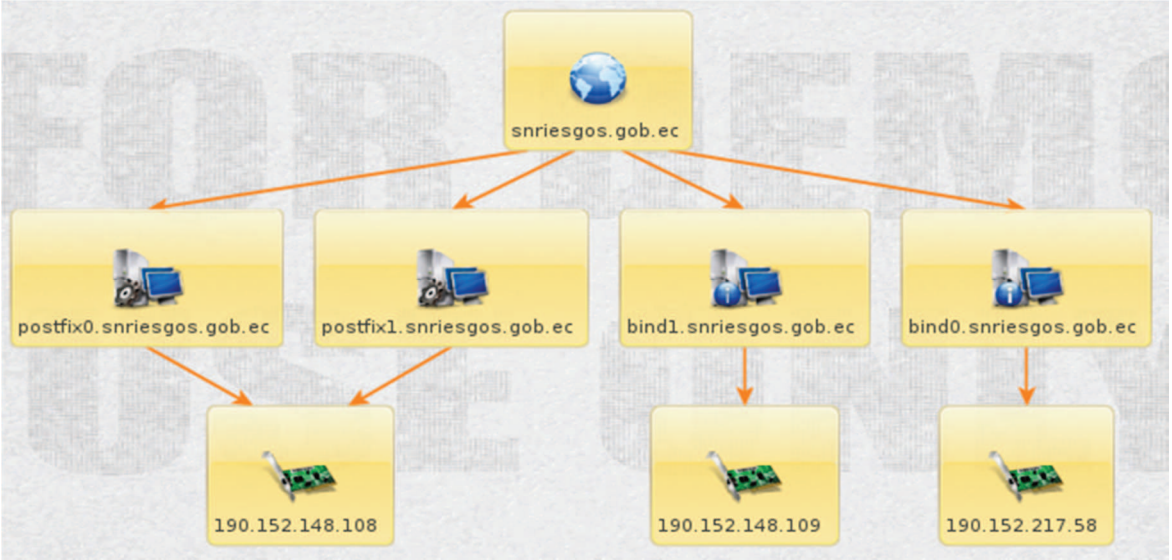


Figura 2-9: Consulta a Registros NS y MX con Maltego

Maltego, también permite realizar consultas que se realizan de un DNS primario a un DNS secundario, más conocido como transferencia de zonas AXFR[64]; en la figura 2-10, se muestran nombres de dominio y direcciones IP relacionadas al dominio snriesgos.gob.ec.

64 AXFR, Automatic Zone Transfer, (Transferencia de Zona Automática)

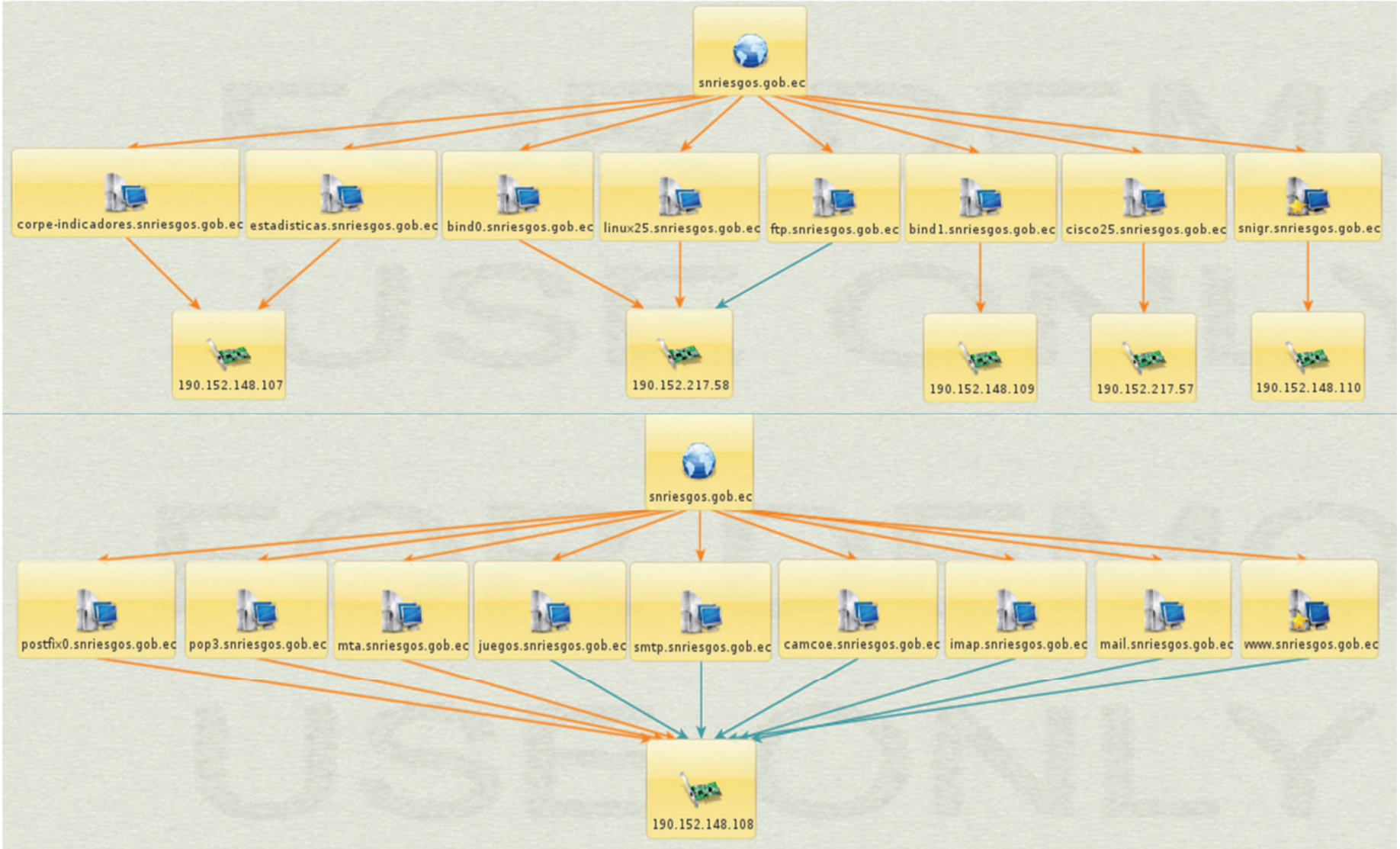


Figura 2-10: Consulta AXFR con Maltego

DiG[65] (comando)

Es una herramienta por línea de comandos que permite interrogar a un servidor DNS en busca de información útil sobre un determinado dominio ya sea desde el Internet o desde la red interna del objetivo; en la figura 2-11, se observan los registros NS y MX del dominio snriesgos.gob.ec, con sus respectivas direcciones IP internas.

```
~$ dig ns mx snriesgos.gob.ec
; <<>> DiG 9.7.0-P1 <<>> ns mx snriesgos.gob.ec
;; QUESTION SECTION:
;snriesgos.gob.ec.                    IN[66]    MX
g
;; ANSWER SECTION:
snriesgos.gob.ec.          3600   IN    MX    20 postfix1.snriesgos.gob.ec.
snriesgos.gob.ec.          3600   IN    MX    10 postfix0.snriesgos.gob.ec.

;; AUTHORITY SECTION:
snriesgos.gob.ec.          3600   IN    NS    bind1.snriesgos.gob.ec.
snriesgos.gob.ec.          3600   IN    NS    bind0.snriesgos.gob.ec.

;; ADDITIONAL SECTION:
postfix0.snriesgos.gob.ec. 3600   IN    A[67]  172.16.104.30
postfix1.snriesgos.gob.ec. 3600   IN    A     172.16.104.30
bind0.snriesgos.gob.ec.    3600   IN    A     192.168.25.2
bind1.snriesgos.gob.ec.    3600   IN    A     192.168.0.5
;; SERVER: 192.168.0.5#53(192.168.0.5)
```

Figura 2-11: Consulta a Registros NS y MX con DIG

DIG, también permite realizar consultas que se realizan de un DNS primario a un DNS secundario; en la figura 2-12, se muestran la consulta AXFR con los nombres de dominio y las IP internas relacionadas al dominio snriesgos.gob.ec

65 DIG, Domain Information Groper, (Buscador o Rastreador de Información de Dominios), http://wiki.aulavirtual.miguelbayon.com/version01/index.php?title=Comando_dig, (mayo 2012)

66 IN, Internet Class, Clase de DNS relacionada a protocolos de Internet

67 A, Address, (Dirección), Registro que se usa para traducir nombres de hosts a direcciones IPv4.

```
~$ dig AXFR snriesgos.gob.ec
; <<>> DiG 9.7.0-P1 <<>> AXFR snriesgos.gob.ec
snriesgos.gob.ec.                    3600   IN      SOA[68]  bind0.snriesgos.gob.ec.
hostmaster.snriesgos.gob.ec. 2012040204 3600 900 1209600 3600

snriesgos.gob.ec.                    3600   IN      NS       bind0.snriesgos.gob.ec.
snriesgos.gob.ec.                    3600   IN      NS       bind1.snriesgos.gob.ec.
snriesgos.gob.ec.                    3600   IN      MX       10 postfix0.snriesgos.gob.ec
snriesgos.gob.ec.                    3600   IN      MX       20 postfix1.snriesgos.gob.ec
bind0.snriesgos.gob.ec.              3600   IN      A        192.168.25.2
bind1.snriesgos.gob.ec.              3600   IN      A        192.168.0.5
camcoe.snriesgos.gob.ec.             3600   IN      A        192.168.0.245
cisco25.snriesgos.gob.ec.            3600   IN      A        192.168.25.1
corpe-dev.snriesgos.gob.ec.          3600   IN      A        192.168.40.21
corpe-indicadores.snriesgos.gob.ec.3600     IN      CNAME[69]estadisticas.snriesgos.gob.ec
directorio.snriesgos.gob.ec.         3600   IN      A        192.168.0.9
estadisticas.snriesgos.gob.ec.       3600   IN      A        192.168.0.7
ftp.snriesgos.gob.ec.                3600   IN      A        192.168.25.2
imap.snriesgos.gob.ec.               3600   IN      A        172.16.104.30
juegos.snriesgos.gob.ec.             3600   IN      A        172.16.104.20
linux25.snriesgos.gob.ec.            3600   IN      A        192.168.25.2
mail.snriesgos.gob.ec.               3600   IN      A        172.16.104.30
mta.snriesgos.gob.ec.                3600   IN      A        172.16.104.30
pop3.snriesgos.gob.ec.               3600   IN      A        172.16.104.30
postfix0.snriesgos.gob.ec.           3600   IN      A        172.16.104.30
postfix1.snriesgos.gob.ec.           3600   IN      A        172.16.104.30
smtp.snriesgos.gob.ec.               3600   IN      A        172.16.104.30
snigr.snriesgos.gob.ec.              3600   IN      A        190.152.148.110
webcal.snriesgos.gob.ec.             3600   IN      A        192.168.0.5
www.snriesgos.gob.ec.                3600   IN      A        192.168.0.16
;; SERVER: 192.168.0.5#53(192.168.0.5)
```

Figura 2-12: Consulta AXFR con DIG

68 SOA, Start Of Authority, (Inicio de Autoridad), Registro que proporciona información del servidor de nombre de dominio con autoridad en la zona.

69 CNAME, Canonical Name, (Nombre Canónico), Registro que permite crear nombres de hosts adicionales, o alias, para los hosts de un nombre de dominio.

En la tabla 2-10, se resumen las direcciones IP públicas obtenidas con Maltego, las direcciones IP internas obtenidas con DIG y los nombres de dominio que se relacionan a ambos resultados.

IP Publica	Nombres de Dominio	IP Interna
190.152.217.57	cisco25.snriesgos.gob.ec	192.168.25.1
190.152.217.58	bind0.snriesgos.gob.ec linux25.snriesgos.gob.ec ftp.snriesgos.gob.ec	192.168.25.2
190.152.148.107	corpe-indicadores.snriesgos.gob.ec estadisticas.snriesgos.gob.ec	192.168.0.7
190.152.148.108	juegos.snriesgos.gob.ec	172.16.104.20
	postfix0.snriesgos.gob.ec postfix1.snriesgos.gob.ec pop3.snriesgos.gob.ec mta.snriesgos.gob.ec imap.snriesgos.gob.ec smtp.snriesgos.gob.ec mail.snriesgos.gob.ec	172.16.104.30
	www.snriesgos.gob.ec	192.168.0.16
	camcoe.snriesgos.gob.ec	192.168.0.245
190.152.148.109	bind1.snriesgos.gob.ec	192.168.0.5
190.152.148.110	snigr.snriesgos.gob.ec	No tiene

Tabla 2-10: Direcciones IP y Nombres de Dominio de la SNGR[70]

Una vez identificadas las direcciones IP internas, se determina que hay dos servidores DNS, un servidor de correos y un servidor HTTP; datos que concuerdan con los recolectados en las fases anteriores de la metodología.

Con la herramienta DIG, también se procede a consultar información de la versión del BIND[71] en uso; en la figura 2-13, se muestra la versión instalada del BIND del dominio snriesgos.gob.ec.

70 Tabla elaborada por el autor.
71 BIND, Berkeley Internet Name Domain, Fuente: https://www.isc.org/software/bind, (mayo 2012)

```
~$ dig snriesgos.gob.ec version.bind ch[72] txt[73]
; <<>> DiG 9.7.3 <<>> snriesgos.gob.ec version.bind ch txt
;; QUESTION SECTION:
;version.bind.                  CH      TXT
;; ANSWER SECTION:
version.bind.           0       CH      TXT     "9.5.1-P3"
;; AUTHORITY SECTION:
version.bind.           0       CH      NS      version.bind.

;; SERVER: 192.168.0.5#53(192.168.0.5)
```

Figura 2-13: Consulta Versión del BIND con DIG

El resultado de la consulta muestra la versión instalada del BIND, e indica que el servidor DNS no está bien configurado, porque permite consultas de la versión del BIND en uso.

En la tabla 2-11, se presenta una lista de vulnerabilidades identificadas en este capítulo.

Vulnerabilidad	***Descripción***
Muestra detalles de la dirección IP publica	Muestra información de contactos: nombres y números de teléfono
Nombres de Dominio relacionadas a IP's publicas	El dominio snriesgos.gob.ec muestra detalles completos de los nombres de dominio relacionados a IP's publicas
Nombres de Dominio relacionadas a IP's internas	El dominio snriesgos.gob.ec muestra detalles completos de los nombres de dominio relacionados a IP's internas
Muestra versión instalada del BIND	Muestra detalles de versión instalada del BIND

Tabla 2-11: Vulnerabilidades de la Recopilación de Información[74]

72 CH, Chaos Class, Fuente: http://en.wikipedia.org/wiki/Chaosnet, (mayo 2012)
73 TXT, TeXT, (Información Textual) Registro que permite al dominio identificarse de modo arbitrario.
74 Tabla elaborada por el autor

2.2.2.2 Mapeo de Red

Después de la primera sección, cuando toda la información posible sobre el objetivo ha sido adquirida, un enfoque más técnico se lleva a cabo para identificar la red y los recursos en cuestión como son host activos, escaneo de puertos y servicios, identificación de servicios críticos, identificación de sistemas operativos y mapeo del perímetro de red.

2.2.2.2.1 Selección de la Herramienta de Mapeo de Red

Para determinar la herramienta de mapeo de red a utilizarse; en la tabla 2-12, se comparan aspectos fundamentales de nmap[75], netcat[76] y hping[77]

ASPECTOS	Nmap	Netcat	Hping
Herramienta de código abierto	Si	Si	Si
Realiza escaneo de puertos	Si	Si	Si
Realiza escaneo avanzado de puertos	Si	No	Si
Determina que servicios se están ejecutando	Si	No	No
Determina que Sistema Operativo y versión utiliza el objetivo	Si	No	Si
Obtiene características del Hardware del objetivo	Si	No	No
Permite realizar traceroute	Si	No	Si
Contiene librerías graficas	Si	No	No

Tabla 2-12: Comparación de Herramientas de Mapeo de Red[78]

Del análisis comparativo se determina que nmap, es una herramienta que reúne los aspectos más importantes para realizar el mapeo de red.

75 NMAP, Network Mapper, (Mapeador de Redes) Fuente: http://nmap.org/man/es/, (mayo 2012)
76 Netcat, Fuente: http://netcat.sourceforge.net/, (mayo 2012)
77 Hping, Fuente: http:// http://www.hping.org/, (mayo 2012)
78 Tabla elaborada por el autor

2.2.2.2.2 Identificación de Puertos y Servicios

El objetivo de este capítulo es escanear todos los 65535 puertos que tiene la red, luego identificar qué servicios están actualmente activos, servicios críticos y servicios conectados pero no deseables, como por ejemplo algún troyano que esté a la escucha.

Ping[79]

Con la herramienta por línea de comandos ping, se puede comprobar por medio del envío de paquetes ICMP[80] de solicitud y de respuesta, el estado de la conexión con los servidores DNS, HTTP y Correo; en la figura 2-14, se observa el estado de la conexión con dichos servidores.

```
File  Edit  View  Terminal  Help
root@bt:~# ping 192.168.25.2
PING 192.168.25.2 (192.168.25.2) 56(84) bytes of data.
64 bytes from 192.168.25.2: icmp_seq=1 ttl=63 time=1.56 ms
File  Edit  View  Terminal  Help
root@bt:~# ping 192.168.0.5
PING 192.168.0.5 (192.168.0.5) 56(84) bytes of data.
64 bytes from 192.168.0.5: icmp_seq=1 ttl=63 time=3.66 ms
File  Edit  View  Terminal  Help
root@bt:~# ping 192.168.0.16
PING 192.168.0.16 (192.168.0.16) 56(84) bytes of data.
64 bytes from 192.168.0.16: icmp_seq=1 ttl=63 time=4.84 ms
File  Edit  View  Terminal  Help
root@bt:~# ping 172.16.104.30
PING 172.16.104.30 (172.16.104.30) 56(84) bytes of data.
64 bytes from 172.16.104.30: icmp_seq=1 ttl=63 time=4.37 ms
```

Figura 2-14: Estado de los Servidores con PING

Luego de la consulta, se observa que los servidores si responden al envío de paquetes ICMP; lo que indica que están activos, pero también el resultado muestra que el Firewall no está configurado correctamente, ya que permite los ping provenientes de la red.

---

79 PING, Packet Internet Groper, (Buscador o Rastreador de Paquetes de Internet)
80 ICMP, Internet Control Message Protocol, (Protocolo de Mensajes de Control de Internet)

NMAP y ZENMAP[81]

Nmap o zenmap el equivalente en modo gráfico es una herramienta de código abierto que se utiliza para la exploración de red y auditoría de seguridad, que está diseñado para analizar rápidamente grandes redes, o bien para equipos individuales; utilizando paquetes IP en sus formas originales permite determinar qué equipos se encuentran disponibles en una red, qué servicios (nombre y versión de la aplicación) ofrecen, qué sistemas operativos (y sus versiones se ejecutan), qué tipo de filtros de paquetes o cortafuegos se están utilizando así como docenas de otras características.

Nmap permite realizar sondeo TCP[82] SYN[83], que es una técnica de escaneo relativamente sigilosa, ya que no llega a completar las conexiones TCP y que consiste en enviar un paquete SYN como si se fuera a abrir una conexión real y después se espera una respuesta; si se recibe un paquete SYN/ACK[84] significa que el puerto está en escucha (abierto), mientras que si se recibe un RST[85] (reset) indica que no hay nada escuchando en el puerto, y si no se recibe ninguna respuesta se asume que está filtrado; luego para evitar que se complete la conexión se envía un paquete RST, con el propósito de evitar que el firewall registre el suceso como un intento de escaneo.

Las opciones -sS[86] y -p[87] de la herramienta nmap, permiten verificar el estado los 65535 puertos TCP; en la figura 2-15, se observan los puertos abiertos y filtrados de los servidores DNS.

---

81 ZENMAP, Fuente: http://nmap.org/zenmap/, (mayo 2012)
82 TCP, Transmission Control Protocol, (Protocolo de Control de Transmisión)
83 SYN, http://es.wikipedia.org/wiki/SYN, (junio 2012)
84 ACK, Acknowledgement, http://es.wikipedia.org/wiki/ACK, (junio 2012)
85 RST, http://es.wikipedia.org/wiki/Flag_RST, (junio 2012)
86 -sS, Scan TCP SYN, (Escaneo TCP SYN)
87 -p, Port Ranges, (Rango de Puertos), Utilizado solo para sondear puertos indicados

Command: nmap -sS -p 1-65535 192.168.25.2

Hosts | Services | Nmap Output | Ports / Hosts | Topology | Host Detail

OS	Host
	192.168.25.2

Port	Protocol	State	Service
1	tcp	open	tcpmux
11	tcp	open	systat
15	tcp	open	netstat
21	tcp	open	ftp
53	tcp	open	domain
79	tcp	open	finger
111	tcp	open	rpcbind
119	tcp	open	nntp
143	tcp	open	imap
540	tcp	open	uucp
635	tcp	open	rlzdbase
1080	tcp	open	socks
1524	tcp	open	ingreslock
2000	tcp	open	cisco-sccp
5742	tcp	open	
6667	tcp	open	irc
8022	tcp	open	oa-system
11000	tcp	open	irisa
12345	tcp	open	netbus
12346	tcp	open	netbus
20034	tcp	open	
27665	tcp	open	Trinoo_Master
31337	tcp	open	Elite
32771	tcp	open	sometimes-rpc5
32772	tcp	open	sometimes-rpc7
32773	tcp	open	sometimes-rpc9
32774	tcp	open	sometimes-rpc11
40421	tcp	open	
49724	tcp	open	
54320	tcp	open	bo2k

Filter Hosts

Command: nmap -sS -p 1-65535 192.168.0.5

Hosts | Services | Nmap Output | Ports / Hosts | Topology | Host Details

OS	Host
	192.168.0.5

Port	Protocol	State	Service
1	tcp	open	tcpmux
11	tcp	open	systat
15	tcp	open	netstat
53	tcp	open	domain
79	tcp	open	finger
80	tcp	open	http
111	tcp	open	rpcbind
119	tcp	open	nntp

143	tcp	open	imap
540	tcp	open	uucp
635	tcp	open	rlzdbase
1080	tcp	open	socks
1524	tcp	open	ingreslock
2000	tcp	open	cisco-sccp
3128	tcp	open	squid-http
5742	tcp	open	
6667	tcp	open	irc
11100	tcp	open	unknown
12345	tcp	filtered	netbus
12346	tcp	filtered	netbus
20034	tcp	open	
22222	tcp	open	unknown
27665	tcp	open	Trinoo_Master
31337	tcp	open	Elite
32771	tcp	open	sometimes-rpc5
32772	tcp	open	sometimes-rpc7
32773	tcp	open	sometimes-rpc9
32774	tcp	open	sometimes-rpc11
40421	tcp	open	
49724	tcp	open	
54320	tcp	open	bo2k

Filter Hosts

Figura 2-15: Puertos abiertos/filtrados de los Servidores DNS con ZENMAP

La información detallada de los puertos TCP, se encuentra en el *Anexo 3*.

En la figura 2-16, se observan los puertos abiertos del servidor de correo.

Command: nmap -sS -p 1-65535 172.16.104.30

Hosts | Services | Nmap Output | Ports / Hosts | Topology | Host

OS	Host
	172.16.104.30

Port	Protocol	State	Service
25	tcp	open	smtp
27	tcp	open	nsw-fe
80	tcp	closed	http
110	tcp	open	pop3
143	tcp	open	imap
443	tcp	open	https
995	tcp	open	pop3s
7071	tcp	open	iwg1
22222	tcp	open	unknown

Figura 2-16: Puertos abiertos del Servidor de Correo con ZENMAP

En la figura 2-17, se observan los puertos abiertos del servidor HTTP.

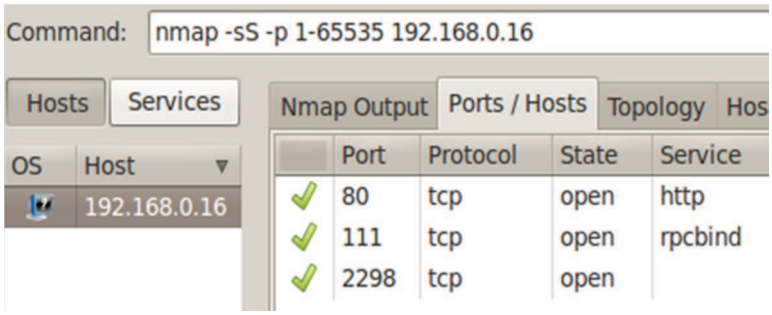


Figura 2-17: Puertos abiertos del Servidor HTTP con ZENMAP

Una vez identificados los puertos abiertos y filtrados, se procede a identificar las versiones de los servicios con la opción -sV[88] de la herramienta nmap; en la figura 2-18, se observan las versiones de los servicios que tienen los servidores DNS.

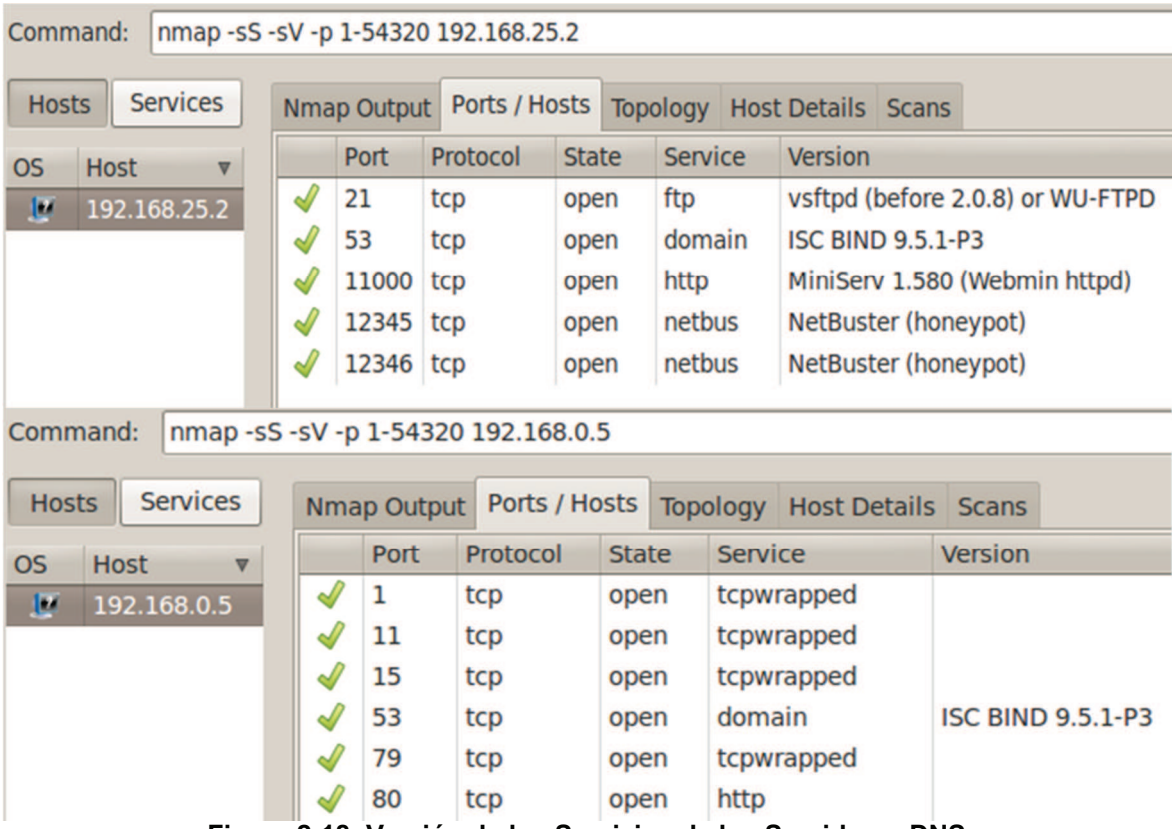


Figura 2-18: Versión de los Servicios de los Servidores DNS

88 -sV, Service Version, Sondea puertos abiertos en busca de información de la versión del servicio.

La consulta al servidor DNS0 solamente muestra la versión de 5 servicios, y el servidor DNS1 muestra la versión de un servicio, esto es debido a que dicha consulta alerta al firewall de intento de ataque o intrusión, ocasionando que la dirección IP asignada dinámicamente para las pruebas sea bloqueada por el Firewall.

La herramienta nmap cuenta con opciones útiles para evadir sistemas de detección de intrusos y en algunos casos restricciones de Firewall; una es evitar realizar ping antes de iniciar el análisis, otra es fragmentar los paquetes enviados en pequeños trozos de 8 bytes o incluso menos, sin embargo, si se especifica dos veces esta opción se duplica el tamaño de los fragmentos en 16 bytes, y otra opción es realizar un escaneo con peticiones enviadas a la máquina objetivo desde direcciones IP distintas a la dirección IP origen.

Las opciones -Pn[89], -f[90], y -D[91] de la herramienta nmap, son utilizadas para realizar un escaneo que sea un poco más difícil para el Firewall identificar que se trata de un escaneo de puertos; en la figura 2-19, se realiza la consulta al servidor DNS1 utilizando la dirección IP objetivo como señuelo.

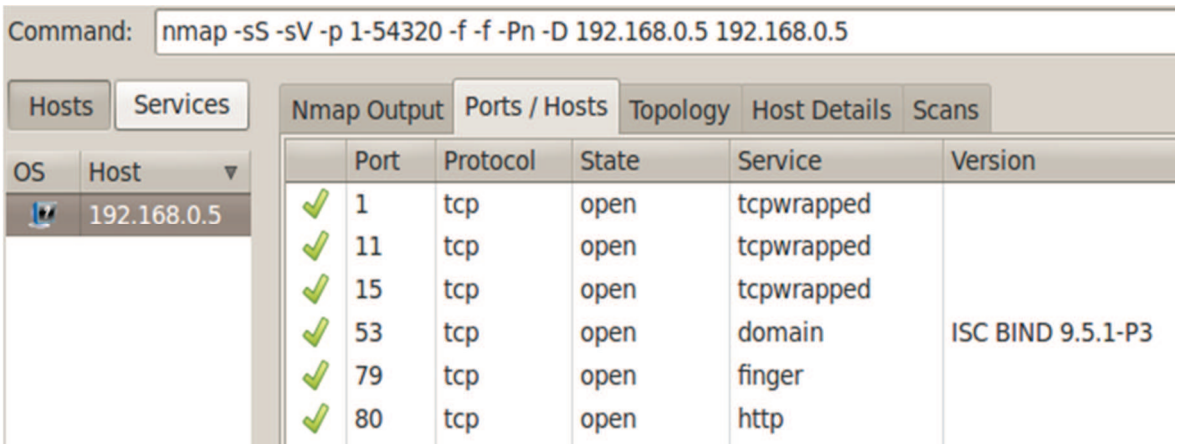


Figura 2-19: Versión de los Servicios del servidor DNS1 evitando el Firewall

89 -Pn, (No Ping), Indica que los host están activos y que no se debe realizar ping.
90 -f, Opción que intenta fragmentar los paquetes que se envían al objetivo en pequeños trozos.
91 -D, Decoy, Opción que ejecuta un escaneo con señuelos usando direcciones IP indicadas con esta opción.

La consulta provoca nuevamente que la dirección IP origen sea bloqueada por el Firewall, lo que indica que se cuenta con políticas de seguridad que permiten detectar y bloquear a intrusos cuando se realiza un escaneo de puertos.

Luego se procede a identificar la versión de los servicios activos de los otros servidores; en la figura 2-20, se observa la versión de los servicios activos del servidor de HTTP.

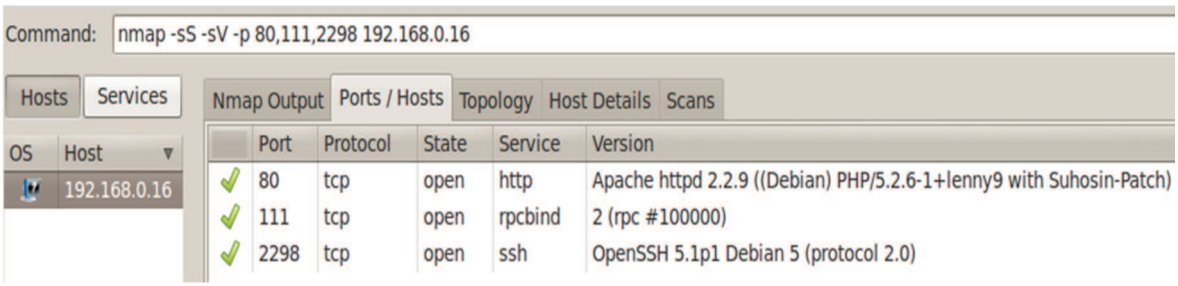


Figura 2-20: Versión de los Servicios del Servidor HTTP

En la figura 2-21, se observa la versión de los servicios del servidor de correo.

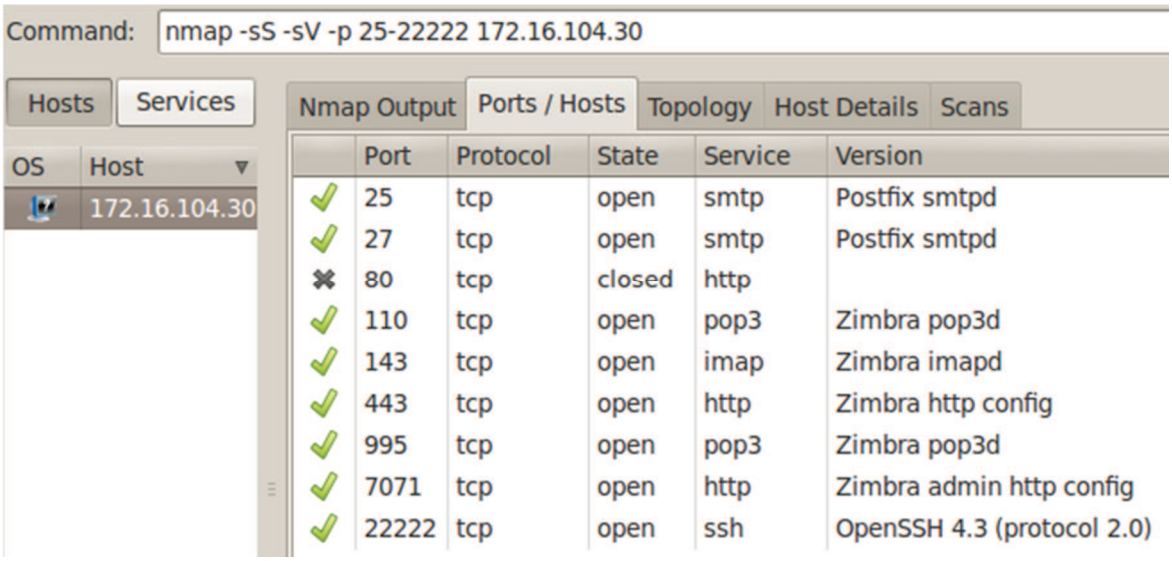


Figura 2-21: Versión de los Servicios del Servidor de Correo

Finalmente, con los resultados obtenidos de las consultas realizadas a los servidores DNS y al servidor de correo, se realiza un análisis de los puertos abiertos y servicios que están escuchando, observando que hay puertos en común abiertos en los servidores mencionados y que solamente ciertos servicios muestran la versión actual instalada; en la tabla 2-13, se observan los puertos abiertos, servicios y versiones de los servidores DNS0 y de correo.

Servidor DNS0	***Servidor de Correo***
Puerto 21; FTP[92]	Puerto 25,27; SMTP[93]
Puerto 53; DNS	Puerto 110,995; POP3[94]
Puerto 11000; HTTP Webmin	Puerto 143; IMAP[95]
Puerto 12345; Netbuster	Puerto 443,7071; HTTP Zimbra
Puerto 12346; Netbuster	Puerto 22222; SSH[96]

Tabla 2-13: Puertos y Servicios de los Servidores DNS0 y Correo[97]

El servidor DNS1 también tiene abiertos los puertos 53, 12345, 12346 y 22222, adicionalmente se observa que el servidor DNS1 tiene el puerto 80 abierto, por lo que es necesario escanearlo ya que puede contener información de su sistema operativo; la figura 2-22, se observa la consulta con nmap de los puertos antes indicados.

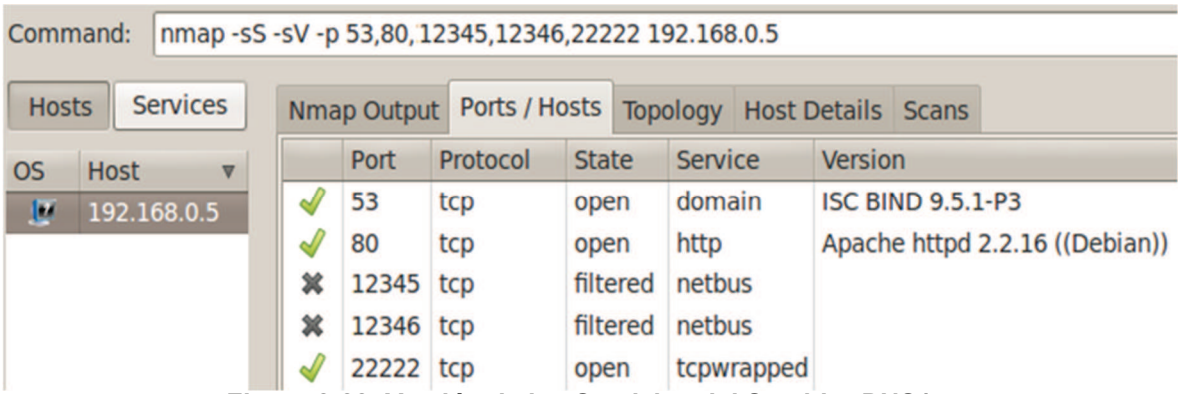


Figura 2-22: Versión de los Servicios del Servidor DNS1

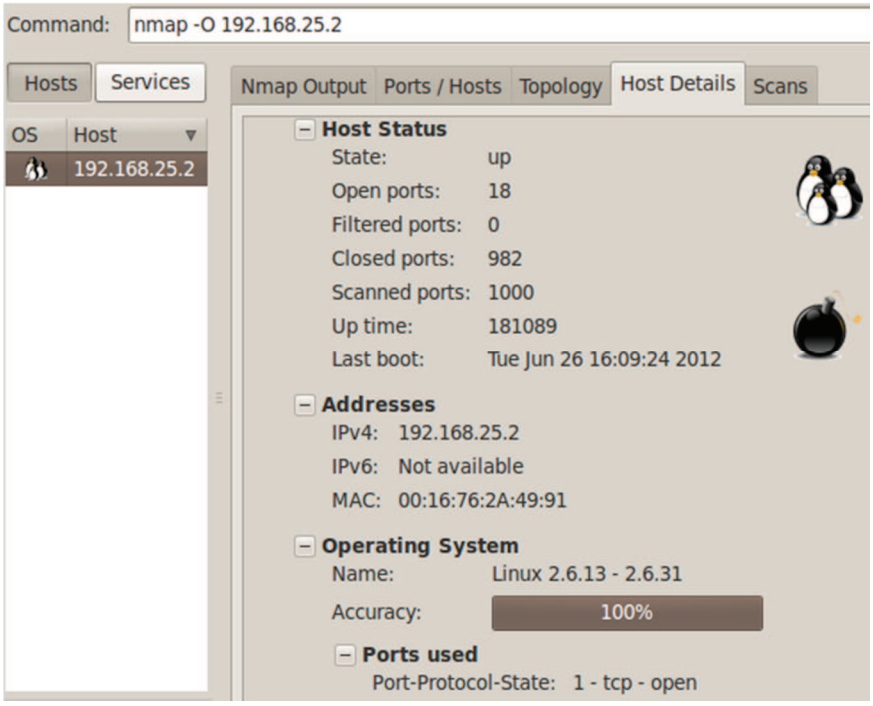
92 FTP, File Transfer Protocol, (Protocolo de Transferencia de Archivos)
93 SMTP, Simple Mail Transfer Protocol, (Protocolo Simple de Transferencia de Correo)
94 POP3, Post Office Protocol 3, (Protocolo de Oficina de Correo 3)
95 IMAP, Internet Message Access Protocol, (Protocolo de Acceso a Mensajes de Internet)
96 SSH, Secure Shell, (Interprete de Ordenes Seguro)
97 Tabla elaborado por el autor

2.2.2.2.3 Identificación del Sistema Operativo

El objetivo de este capítulo es identificar el Sistema Operativo de los servidores ya identificados, y para esto es necesario realizar un análisis del paquete de respuesta que es enviado por el servidor a identificar.

La herramienta NMAP permite detectar el Sistema Operativo y su versión en base a la comprobación de huellas TCP/IP; enviando una serie de paquetes TCP y UDP[98] al sistema objetivo, luego se compara prácticamente todos los bits de las respuestas con su base de datos nmap-os-fingerprints, y cuando existe una coincidencia se presentan en pantalla los detalles del sistema operativo identificado.

En la figura 2-23, se observa el Sistema Operativo de los servidores DNS identificados con la opción -O[99] de la herramienta nmap.



98 UDP, User Datagram Protocol, (Protocolo de Datagrama de Usuario)
99 -O, Opción que activa la detección del Sistema Operativo

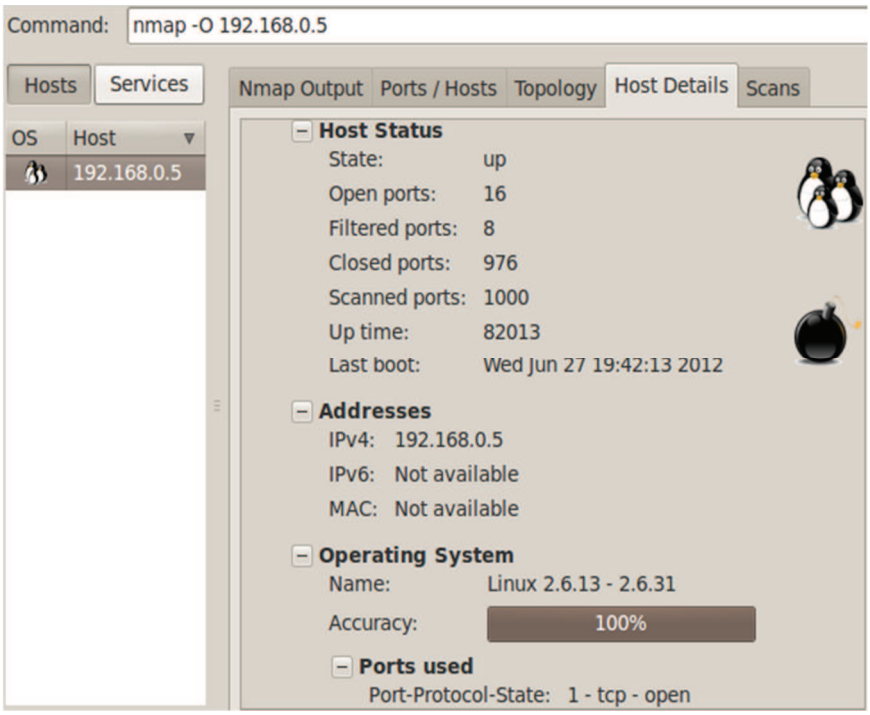


Figura 2-23: Sistema Operativo de los Servidores DNS con ZENMAP

La consulta con nmap muestra que ambos servidores DNS tienen un Kernel Linux 2.6.13 – 2.6.31, pero no indica cual es la Distribución GNU/Linux instalada.

Ahora para identificar la Distribución GNU/Linux es necesario realizar una consulta al servicio HTTP y revisar la variable "Server", que es la que nos puede dar más información sobre el Sistema Operativo; en el capítulo anterior solamente el servidor DNS1 tiene el servicio HTTP activo en el puerto 80, y se observa que se trata de un sistema GNU/Linux con base Debian; por lo tanto se puede estar seguro que es una Distribución GNU/Linux Debian y Kernel 2.6.13 – 2.6.31.

También en el capítulo anterior se identifica la versión del servicio en el puerto 80 del servidor HTTP, y se observa que se trata de un sistema GNU/Linux Debian; en la figura 2-24, se observa la versión del Kernel Linux del servidor HTTP.

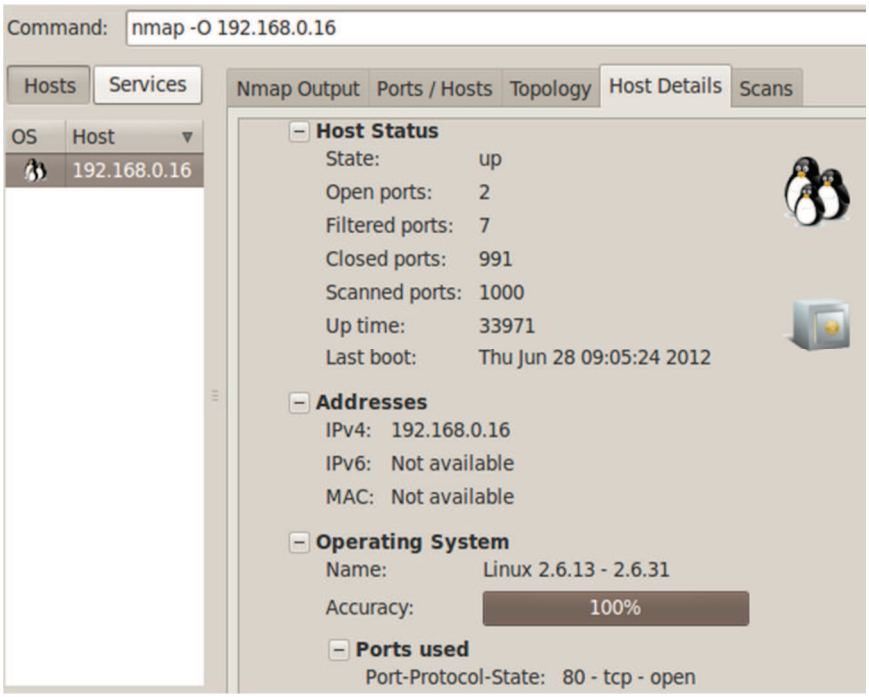


Figura 2-24: Sistema Operativo del Servidor HTTP con ZENMAP

En la figura 2-25, se observa la versión del Kernel Linux del servidor de Correo.

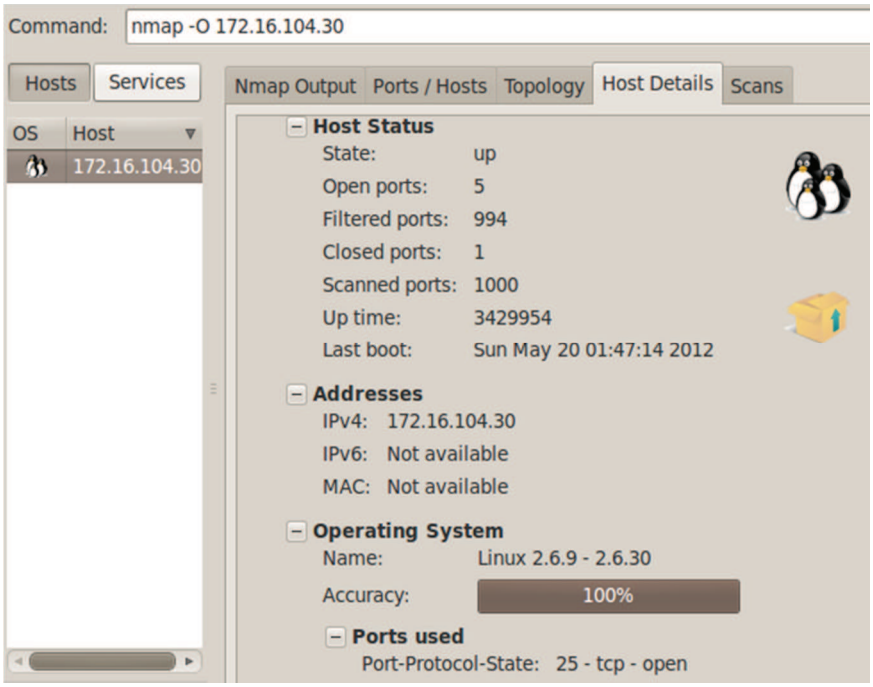


Figura 2-25: Sistema Operativo del Servidor de Correo con ZENMAP

En la tabla 2-14, se resume la información de los servidores y servicios que se identifica con nmap.

Dirección IP	Sistema Operativo	Servicios			
192.168.25.2	GNU/Linux	tcpmux	systat	*Vsftpd (before 2.0.8) o WU-FTPD*	
		netstat	finger	*ISC BIND 9.5.1-P3*	
		rpcbind	nntp	imap	uucp
		rizdbase	socks	ingreslock	cisco-sccp
		irc	oa-system	*MiniServ 1.580 (Webmin httpd)*	
		Netbuster (honeypot)		Trino_Master	
		Elite	Sometimes-rpc		bo2k
192.168.0.5	GNU/Linux Debian	tcpmux	systat	netstat	finger
		ISC BIND 9.5.1-P3		*Apache httpd 2.2.16*	
		rpcbind	nntp	imap	uucp
		rizdbase	socks	ingreslock	cisco-sccp
		squid-http	irc	*MiniServ 1.580 (Webmin httpd)*	
		Netbus	Trino_Master		Elite
		Sometimes-rpc		bo2k	
192.168.0.16	GNU/Linux Debian	*Apache httpd 2.2.9, PHP/5.2.6-1*			rpcbind
		OpenSSH 5.1p1 (protocolo 2.0)			
172.16.104.30	GNU/Linux	Postfix smtpd	Zimbra pop3d	Zimbra imapd	Zimbra http confi
		Zimbra admin http config		*OpenSSH 4.3 (protocolo 2.0)*	

Tabla 2-14: Servicios y Sistemas Operativos identificados con NMAP[100]

100 Tabla elaborada por el autor

2.2.2.2.4 Identificación del Perímetro de Red

El objetivo es identificar todo lo posible sobre el router y el firewall que separa la red de la Institución con el Internet; para ello se utiliza Firewalking, que es un método que permite recoger información de una red protegida por un firewall.

El Firewalking permite en muchos casos ver casi todos los routers entre el dispositivo de filtrado y el destino final; con técnicas como tracerouting que consiste en enviar a un host destino paquetes de tipo TCP, UDP o ICMP, y que se incrementan poco a poco en cada salto con diversos valores TTL[101]; para el valor TTL que es un campo del datagrama IP utilizado para limitar el número de nodos por los que se desea que viaje el datagrama antes de ser descartado, el proceso es decrementar en 1 el valor TTL cada vez que el paquete pase por un nodo, de esta forma cuando el valor TTL sea cero ya no se reenviara más el paquete evitando se produzcan bucles de red; y cuando un nodo elimina el paquete genera un mensaje de error ICMP, que es enviado al host de origen indicando en qué nodo expiró el paquete.

Traceroute[102]

Es una herramienta que permite realizar la técnica antes mencionada y que es utilizada para realizar un mapa de todos los host que están en la ruta hasta un destino indicado, la interfaz gráfica de nmap contiene una pestaña que permite ver gráficamente los resultados obtenidos con traceroute; en la figura 2-26, se muestra las direcciones IP que están en la ruta al servidor de correo y al servidor web.

[101]TTL, Time To Live, (Tiempo de vida)
[102]Traceroute, fuente: http://es.wikipedia.org/wiki/Traceroute, (julio 2012)

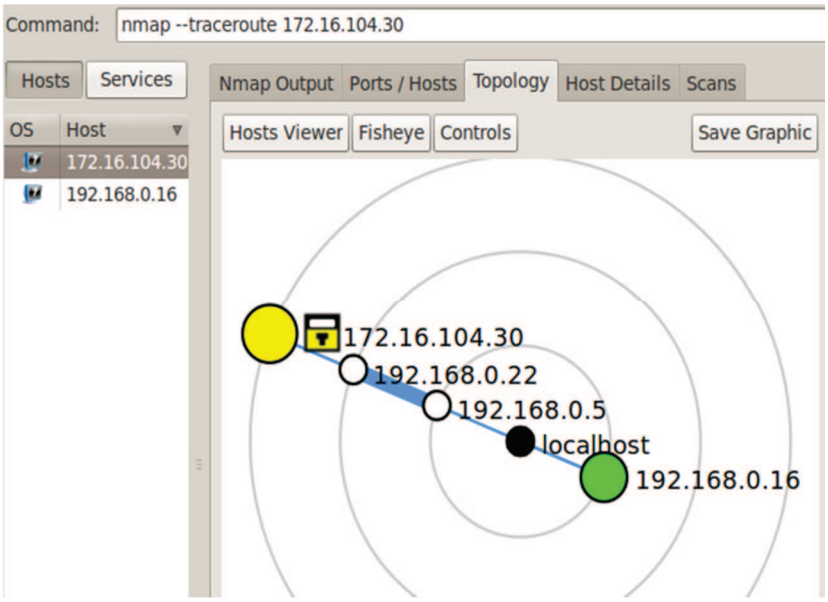


Figura 2-26: Perímetro de Red con ZENMAP

Las direcciones IP obtenidas con la herramienta muestran datos que concuerdan con los recolectados en la fase inicial de la metodología; y se observa que la dirección IP 192.168.0.5 además de ser un servidor DNS es un Firewall, dato que puede ser tomado en cuenta para el análisis por cuanto el servidor DNS debe estar tras el firewall y no ser parte del mismo.

En la tabla 2-15, se presenta una lista de vulnerabilidades del mapeo de red.

Vulnerabilidad	***Descripción***
Respuestas ICMP de Servidores	Los servidores responden al envío de paquetes ICMP
Puertos abiertos en los servidores DNS, Correo y HTTP	Servidores DNS, Correo y HTTP, presentan varios puertos abiertos no identificados
Servidores muestran versión de servicios activos y del Sistema Operativo	Servidores muestran detalles de la versión de los servicios activos y del Kernel Linux
Detalles del perímetro de RED	Muestra las direcciones de routers, el Firewall y los servidores de Correo y HTTP
El Firewall también es el servidor DNS	La dirección IP del servidor DNS también es la dirección IP del Firewall

Tabla 2-15: Vulnerabilidades del Mapeo de Red[103]

103 Tabla elaborada por el autor

2.2.2.3 Seguridad en las Contraseñas

La metodología contempla que las pruebas de seguridad para las contraseñas sean pruebas de obtención de acceso a los sistemas y posterior escalada de privilegios de forma intrusiva; pero en la tabla 2-2, se determina que la naturaleza de las pruebas no sean intrusivas, por lo que solamente se procede a verificar la estructura de las contraseñas y su seguridad.

Los puntos de acceso revisados en los capítulos anteriores contienen contraseñas con cierto nivel de seguridad que puede ser verificadas de acuerdo a cuán difícil es descifrarlas, ya sea por fallos en el sistema de cifrado, o en debilidades introducidas por factor humano; en la tabla 2-16, se muestra información de la estructura de las contraseñas utilizadas en los servidores identificados.

Parámetros de Seguridad	***Características***
Contraseñas en los Servidores	Contraseñas distintas para cada servidor
Uso de palabras conocidas o comunes	No
Utilización del login como contraseña	No
Longitud de las contraseñas	Contienen más de 15 caracteres
Uso de mayúsculas y minúsculas	Si
Utilización de letras y números	Si
Utilización de símbolos y aceptos	Si
Cambio regular de las contraseñas	Solo cuando sale un funcionario de la Institución
Contraseñas escritas en notas	No

Tabla 2-16: Parámetros de Seguridad de las Contraseñas[104]

Las características que presentan las contraseñas de los servidores de la SNGR muestran cierto nivel de seguridad, y pueden ser analizadas posteriormente.

104 Tabla elaborada por el autor, Fuente: Área de Infraestructura y Telecomunicaciones SNGR, (julio 2012)

2.2.2.4 Seguridad de los switch

La metodología establece un conjunto de pruebas de seguridad para los equipos que están en la capa de acceso del diseño de arquitectura de red, y para ello considera los puntos de acceso de los switch capa-2; en la figura 2-27, se observa el estado de la conexión con las direcciones IP de los switch capa-2.

```
File  Edit  View  Terminal  Help
root@bt:~# ping 172.16.200.1
PING 172.16.200.1 (172.16.200.1) 56(84) bytes of data.
^C
--- 172.16.200.1 ping statistics ---
12 packets transmitted, 0 received, 100% packet loss, time 11017ms

root@bt:~# ping 172.16.201.1
PING 172.16.201.1 (172.16.201.1) 56(84) bytes of data.
^C
--- 172.16.201.1 ping statistics ---
19 packets transmitted, 0 received, 100% packet loss, time 18145ms
```

Figura 2-27: Estado de los Switch con Ping

Se observa que las direcciones IP de los switch capa-2 no responden al envío de paquetes ICMP, lo que indica que existe algún tipo de seguridad o bloqueo a dichas peticiones por parte de los switch, y por tal motivo no es posible ver el estado de los equipos, llegando a la conclusión de que los equipos están configurados con cierto nivel de seguridad especialmente de anti-escaneo.

2.2.2.5 Seguridad del Router

La seguridad del router consiste en identificar puertos abiertos/filtrados, servicios activos, sistema operativo, protocolos de enrutamiento del router, y en fases anteriores se identifica la dirección IP del router; en la figura 2-28, se observan los puertos abiertos/filtrados del router con la herramienta nmap.

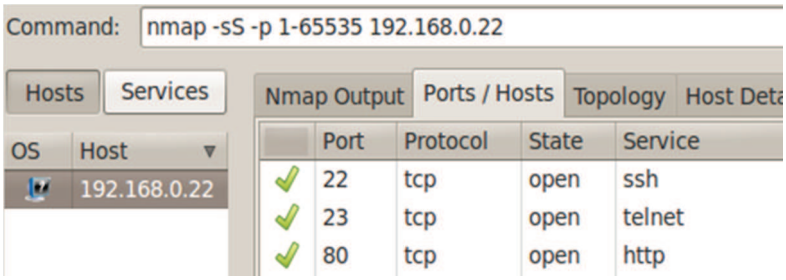


Figura 2-28: Puertos TCP abiertos del router con ZENMAP

Con nmap se identifica solamente 3 puertos abiertos; en la figura 2-29, se observan las versiones de los servicios activos y el sistema operativo del router.

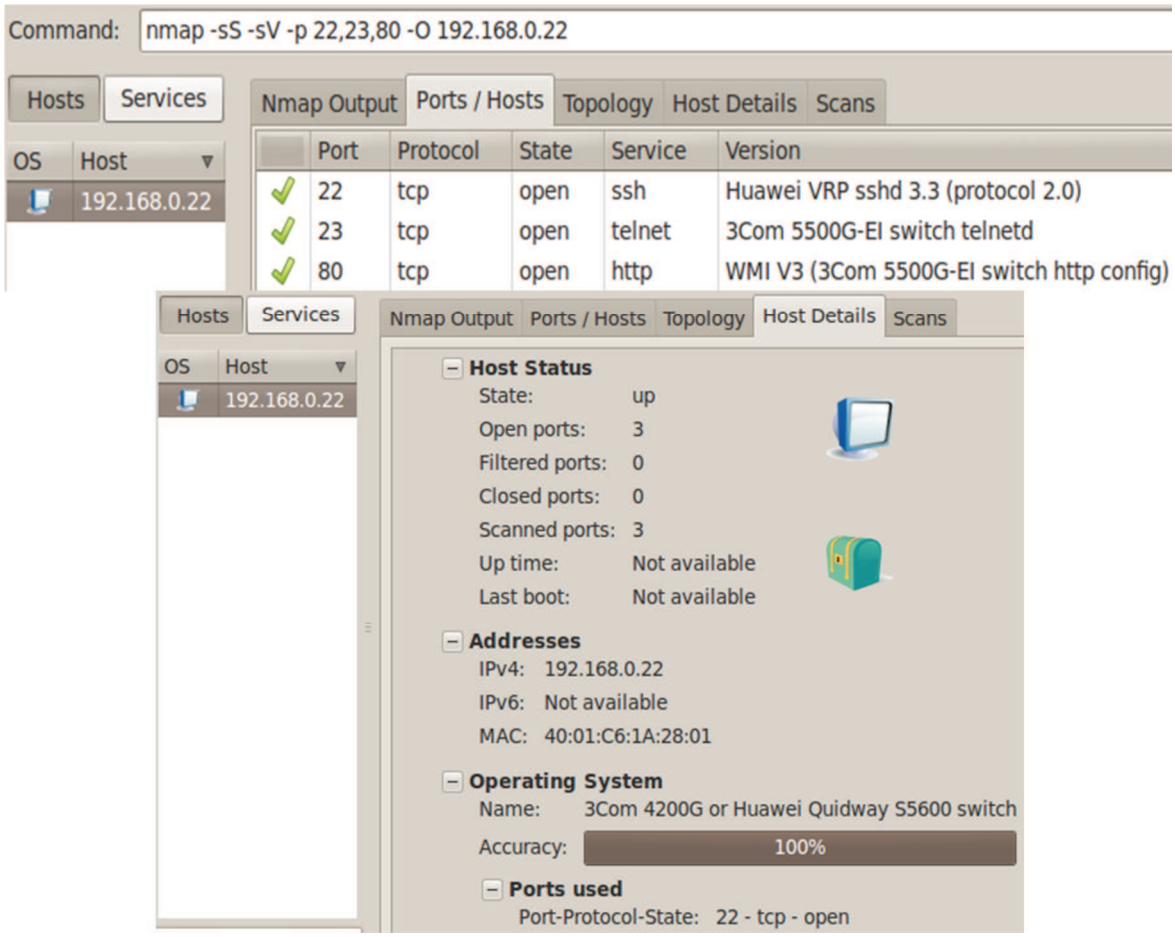


Figura 2-29: Versión de los servicios y Sistema Operativo del router

También con la ayuda de la herramienta nmap se procede a identificar los protocolos de enrutamiento que soporta el router, utilizando una técnica muy similar al escaneo de puertos TCP, con la diferencia de que los números de puerto son números de protocolo IP utilizados por el objetivo.

Para ello se envía cabeceras de paquetes IP repetidamente con un campo de 8 bits el cual indica el protocolo IP, luego se espera la recepción de mensajes de ICMP “protocolo no alcanzable” en lugar de mensajes ICMP “puerto no alcanzable”, y en caso de recibir respuesta se marca el protocolo identificado como abierto; pero en fases anteriores se indicó que el enrutamiento es estático y la técnica menciona es solo para protocolos de enrutamiento dinámico.

En la tabla 2-17, se presenta la lista de vulnerabilidades identificadas en este capítulo.

Vulnerabilidad	***Descripción***
Router muestra puertos abiertos y servicios activos.	El router muestra puertos abiertos y servicios activos
Router muestra versión del Sistema Operativo	El router muestra detalles de la versión del Sistema Operativo
Router muestra protocolos de enrutamiento	Router tiene protocolos de enrutamiento estático

Tabla 2-17: Vulnerabilidades del Router[105]

2.2.2.6 Seguridad del Firewall

El objetivo de este capítulo es localizar el firewall, identificar puertos abiertos, puertos filtrados, servicios activos y reglas activas; en fases anteriores se identifica que el Firewall tiene la misma dirección IP del servidor DNS1, se localiza la dirección IP en el perímetro de red, se identifica los puertos abiertos/filtrados y los servicios activos en la figura 2-15.

105 Tabla elaborada por el autor

La metodología establece que si se identifican asuntos críticos en la seguridad durante el proceso de evaluación, se proceda a informar verbalmente a la Institución; por tal motivo se procede a consultar al Área de Infraestructura si todos los puertos identificados de la figura 2-15 deberían estar abiertos, a lo que el área indica que solamente deben estar activos los servicios relacionados con el servidor DNS en los puertos 53, 111 y los servicios relacionados al Squid[106], Webmin[107] y OpenSSH[108] en los puertos 3128, 11100 y 22222 respectivamente.

Luego con la opción -sA[109] de la herramienta nmap se verifica si el Firewall contiene reglas activas que permitan filtrar el contenido de los puertos activos; en la figura 2-30, se muestran puertos filtrados por reglas del Firewall.

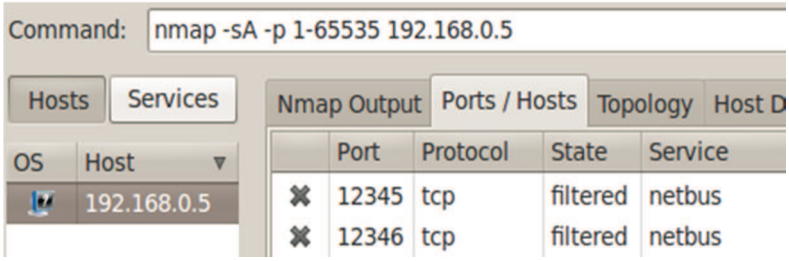


Figura 2-30: Reglas de filtrado del Firewall

El resultado muestra solamente dos puertos con reglas de filtrado, lo que indica que los puertos abiertos que no son usados por servicios de TIC, pueden estar en uso por programas maliciosos, troyanos o como backdoors.

En este caso se puede realizar pruebas de acceso a puertos con servicios activos no establecidos por el Área de Infraestructura, pero dichas pruebas son intrusivas y son pruebas que intentan explotar vulnerabilidades para cada puerto abierto, entre las cuales incluyen pruebas de Backdoors.

En el *Anexo 4* se encuentra información detallada de puertos que son usados por troyanos.

---

106 SQUID, Fuente: http://www.squid-cache.org/, (agosto 2012)
107 WEBMIN, Fuente: http://www.webmin.com/, (agosto 2012)
108 OpenSSH, Open Secure Shell, Fuente: http://www.openssh.org/, (agosto 2012)
109 -sA, Escaneo TCP ACK que permite mapear reglas de Firewalls

En la tabla 2-18, se presenta una lista de vulnerabilidades identificadas en este capítulo.

Vulnerabilidad	Descripción
Firewall muestra puertos abiertos y servicios activos	El firewall muestra detalles de los puertos abiertos y servicios activos
Firewall presenta puertos con servicios utilizados por la Dirección de TIC	Firewall muestra puertos abiertos utilizados para servicios de DNS, Webmin, Squid, OpenSSH
Firewall presenta puertos abiertos no establecidos por la Dirección de TIC	Firewall muestra puertos identificados que no son parte de servicios de TIC
Firewall tiene pocas reglas de filtrado	Firewall presenta pocas reglas de filtrado
Firewall presenta puertos con troyanos	Firewall presenta puertos que pueden ser usados por troyanos

Tabla 2-18: Vulnerabilidades del Firewall[110]

2.2.2.7 Seguridad del Sistema de Detección de Intrusos

La metodología establece que un sistema de detección de intrusos (IDS) proporcione una capa adicional de protección a un firewall; con el propósito principal de examinar el tráfico local o de red, en busca de signos de intentos de ataques, intrusiones o violaciones de seguridad en la red, y que luego puedan ser reportadas al administrador.

Existen dos tipos de IDS, los basados en Host (HIDS) y los basados en red (NIDS); los primeros se instalan localmente en máquinas como servidores y estaciones de trabajo, y tienen la función de analizar paquetes de dichos Host en busca de posibles intentos de ataque o intrusiones; los segundos son agentes que se colocan en la tarjeta de interfaz de red de modo que sea capaz de analizar todo el tráfico que cruza por la interfaz dentro de un segmento de red específico, con el fin de determinar la ocurrencia de una intrusión o intento de ataque.

110 Tabla elaborada por el autor

En la fase inicial de la metodología se establece los puntos de acceso para los elementos clave a evaluar, entre los cuales incluyen Host IDS y Network IDS; pero la Infraestructura Tecnológica de la SNGR no tiene instalado en sus equipos ninguno de los dos tipos de Sistemas de Detección de Intrusos, por lo que no existe puntos de acceso y se puede considerar como una vulnerabilidad que puede ser analizada posteriormente.

2.2.2.8 Seguridad del Sistema Anti-virus

La metodología incluye la evaluación de la seguridad que proporciona el Sistema Anti-virus, la gestión de políticas de control y las pautas para la administración del Anti-virus; este puede dividirse en dos tipos, los que se instalan en la infraestructura de red y los que están instalados en equipos de usuarios finales.

La metodología indica que en la infraestructura de red los sistemas Anti-virus sean instalados junto con el Firewall y con los servidores de correo, con el fin de eliminar virus a nivel de red; en la tabla 2-19, se muestran los parámetros de seguridad y las características del Sistemas Anti-virus que está instalado en los equipos de la SNGR.

Parámetros de Seguridad	***Características***
Anti-virus instalado con el Firewall	No
Anti-virus instalado en el Servidor de Correo	Si
Anti-virus instalado en equipos de usuarios finales	Si
Detecta y protege de virus, gusanos, troyanos y macros	Si
Servidor Anti-virus permite administración y gestión del Sistema	Si
Configuración por defecto del Sistema Anti-virus	Módulos del Sistema Anti-Virus protegen todo el equipo, pero es necesario activar el escaneo para las unidades externas

Actualización automática de la versión del Sistema Anti-virus	Si
Usuarios tienen acceso a desactivar o deshabilitar el Sistema Anti-virus	No
Eventos de virus son identificados por el Servidor Anti-virus	Si
Actualización automática de las definiciones de virus	Si
Definiciones de virus cada 30 minutos	Si
Actualizaciones en los equipos cliente	Cada 2 días
Escaneo de virus es programado automáticamente	Cada 15 días

Tabla 2-19: Parámetros de Seguridad del Sistema Anti-virus[111]

2.2.2.9 Seguridad en la Red de Área de Almacenamiento

Las Redes de Área de Almacenamiento SAN[112], son diseñadas básicamente para la alta disponibilidad y la seguridad del almacenamiento de datos; contemplando varios parámetros, en la tabla 2-20 se muestran los parámetros de seguridad y las características de la Red de Área de Almacenamiento.

Parámetros de Seguridad	***Características***
Administración del Almacenamiento	Si
Red de Almacenamiento	Si
Contraseñas para la Administración	Contraseñas según la tabla 2-13
Acceso autorizado a los medios de cinta	Solo por el Administrador
Protección de los datos en reposo	Si
Protección y Control de Acceso a los datos en vuelo	Si
Servidor de Gestión con valores por defecto	No
Actualización del Firmware	Solo cuando hay problemas en el Storage

111 Tabla elaborada por el autor, Fuente: Audit Antivirus Management Strategy, Fuente: ISSAF versión 0.2.1, páginas 524, 525, 526 y 527

112 SAN, Storage Area Network, (Red de Área de Almacenamiento)

Integridad de los datos	Los respaldos de información solo se realiza 1 vez al año
Confidencialidad de los datos	Si
Disponibilidad de los datos	Siempre y en especial en situaciones de emergencia declarada

Tabla 2-20: Parámetros de Seguridad de la Red de Área de Almacenamiento[113]

2.2.2.10 Seguridad en la Red Inalámbrica

El objetivo de este capítulo es identificar las redes inalámbricas, testear los canales, el ESSID[114], los puntos de acceso desde el exterior de la instalación, y recopilar direcciones IP y direcciones MAC[115] de los puntos de acceso y de los clientes.

Las pruebas que la metodología establece para las redes inalámbricas (WLAN[116]) son intrusivas y principalmente externas, esto con el propósito de comprobar los niveles de seguridad implementados en la configuración de los dispositivos de acceso inalámbrico; pero en la tabla 2-3, se determina que las pruebas no sean intrusivas y que sean internas, por lo que se procede únicamente a verificar la configuración general de los dispositivos inalámbricos.

En la tabla 2-21, se muestran los parámetros de seguridad y las características de la Red Inalámbrica.

Parámetros de Seguridad	***Características***
Tipo de Red WLAN	Estándar "IEEE 802.11g"[117]
Modo de Operación de Red WLAN	Puntos de Acceso de Infraestructura
Configuración del dispositivo WLAN por defecto	No

113 Tabla elaborada por el autor, Fuente: ISSAF versión 0.2.1, páginas 533, 534 y 535
114 ESSID, Extended Service Set Identifier (Identificador del Conjunto de Servicios Extendidos)
115 MAC, Media Access Control, (Control de Acceso Medio)
116 WLAN Wireless Local Area Network, (Red de Área Local Inalámbrica)
117 IEEE 802.11g, Fuente: http://es.wikipedia.org/wiki/IEEE_802.11, (agosto 2012)

SSID configurado por defecto	No
Posee autenticación RADIUS[118]	No
Tipo de autenticación	WPA2[119]
Tipo de encriptación	TKIP[120] ó AES[121]
Administración de las claves de acceso	Solo personal de TIC
Longitud de clave	Superior a 10 dígitos
Control de acceso a la Administración	Si
Contiene controles basados en direcciones MAC	Si
SSID Broadcast activo	Si
Actualización de Firmware	Solo cuando hay problemas en los equipos
Los dispositivos permiten establecer políticas y controles	Si

Tabla 2-21: Parámetros de Seguridad de la Red Inalámbrica[122]

2.2.2.11 Seguridad del Servidor Web

ISSAF establece evaluaciones de seguridad para el Microsoft Internet Information Server, ya que este contiene una gran cantidad de vulnerabilidades, pero para el caso de Apache no establece evaluaciones, ya que lo considera seguro.

En capítulos anteriores se identifica que el servidor Web utilizado por la SNGR es Apache, por lo que no se procede a evaluar la seguridad de dicho servidor, pero si se procede a verificar características generales para el servidor; en la tabla 2-22, se muestran se muestran los parámetros de seguridad y las características del Servidor Web.

118 RADIUS, Remote Authentication Dial-In User Server
119 WPA2, Wi-Fi Protected Access 2, (Acceso Protegido Wi-Fi 2)
120 TKIP, Temporal Key Integrity Protocol, (Protocolo de Integridad de Clave Temporal)
121 AES, Advanced Encryption Standard, (Estándar de Encriptación Avanzada)
122 Tabla elaborada por el autor, Fuente: ISSAF versión 0.2.1, páginas 541, 542, 546 y 547

Parámetros de Seguridad	Características
Acceso al servidor WEB	Solo Administrador
Permite el acceso remoto	Si
El acceso a la administración es segura	Si
Acceso al servidor solo desde determinadas direcciones IP	Acceso desde cualquier dirección IP
Servidor WEB tiene servicios no esenciales desactivados	Si
Sistema Operativo del servidor tiene las últimas actualizaciones	Si
Habilitada la exploración de directorios	Si
Acceso por FTP	No
El servidor se ejecuta como usuario root	No
El servidor tiene balanceo de carga	No

Tabla 2-22: Parámetros de Seguridad del Servidor WEB[123]

2.2.2.12 Seguridad de las Aplicaciones Web

En las fases anteriores de la metodología se identifica puertos, servicios, versiones y el sistema operativo del servidor HTTP; en este capítulo el objetivo es identificar las tecnologías utilizadas en el portal web de la SNGR.

2.2.12.1 Selección de la Herramienta para el Análisis de Aplicaciones Web

Para determinar la herramienta para las tecnologías en aplicaciones web a utilizarse; en la tabla 2-23, se comparan aspectos fundamentales de WhatWeb[124] y de cms-explorer[125]

123 Tabla elaborada por el autor, Fuente: ISSAF versión 0.2.1, páginas 715, 716 y 717
124 WhatWeb, Fuente: http://www.morningstarsecurity.com/research/whatweb, (junio 2012)
125 CMS-Explorer, Fuente: https://code.google.com/p/cms-explorer/, (junio 2012)

ASPECTOS	WhatWeb	Cms-explorer
Identifica Sistemas de Gestión de Contenidos	Si	Si
Identifica versiones del Sistema de Gestión de Contenidos	Si	No
Identifica correos electrónicos	Si	No
Identifica errores SQL	Si	No
Identifica blogs y servidores web	Si	No

Tabla 2-23: Comparación de Herramientas de Análisis de Aplicaciones Web[126]

Del análisis comparativo se determina que WhatWeb, es una herramienta que reúne los aspectos más importantes para identificar las tecnologías del portal Institucional.

WhatWeb

Es una herramienta por línea de comandos que permite reconocer las tecnologías utilizadas en un sitio web, incluyendo CMS[127], plataformas de blogs, bibliotecas JavaScript, servidores web, dispositivos embebidos, números de versión, direcciones de correo y muchas más características.

En la figura 2-31, se muestra información detallada del portal web de la SNGR, utilizando whatweb opción -v[128].

```
File  Edit  View  Terminal  Help
root@bt:/pentest/enumeration/web/whatweb# ./whatweb -v http://www.snriesgos.gob.ec
http://www.snriesgos.gob.ec/ [200]
http://www.snriesgos.gob.ec [200] Google-Analytics[UA-15853288-1], Title[Secretar%C3
%ADa Nacional de Gesti%C3%B3n de Riesgos], Joomla[1.5], JQuery, Email[informacion@sn
riesgos.gob.ec], Apache[2.2.9], MetaGenerator[Joomla! 1.5 - Open Source Content Mana
gement], IP[192.168.0.16], Country[RESERVED][ZZ], HTTPServer[Debian Linux][Apache/2.
2.9 (Debian) PHP/5.2.6-1+lenny9 with Suhosin-Patch], Frame, X-Powered-By[PHP/5.2.6-1
+lenny9], PHP[5.2.6-1+lenny9][Suhosin-Patch], Cookies[82f49cef539bb03b5848add7f95ceb
92]
URL    : http://www.snriesgos.gob.ec
Status : 200
```

126 Tabla elaborada por el autor
127 CMS, Content Management System, (Sistema de Gestión de Contenidos)
128 -v, Opción que muestra la información de manera detallada y por secciones.

```
Apache ----------------------------------------------------------------
     Description: The Apache HTTP Server Project is an effort to develop and
                  maintain an open-source HTTP server for modern operating
                  systems including UNIX and Windows NT. The goal of this
                  project is to provide a secure, efficient and extensible
                  server that provides HTTP services in sync with the current
                  HTTP standards. - homepage: http://httpd.apache.org/
     Version    : 2.2.9

Country ---------------------------------------------------------------
     Description: Shows the country the IPv4 address belongs to. This uses
                  the GeoIP IP2Country database from
                  http://software77.net/geo-ip/. Instructions on updating the
                  database are in the plugin comments.
     String     : RESERVED
     Module     : ZZ
Email -----------------------------------------------------------------
     Description: Extract email addresses. Find valid email address and
                  syntactically invalid email addresses from mailto: link
                  tags. We match syntactically invalid links containing
                  mailto: to catch anti-spam email addresses, eg. bob at
                  gmail.com. This uses the simplified email regular
                  expression from
                  http://www.regular-expressions.info/email.html for valid
                  email add
     String     : informacion@snriesgos.gob.ec

HTTPServer ------------------------------------------------------------
     Description: HTTP server header string. This plugin also attempts to
                  identify the operating system from the server header.
     Os         : Debian Linux
     String     : Apache/2.2.9 (Debian) PHP/5.2.6-1+lenny9 with Suhosin-Patch (fr
om server string)

IP --------------------------------------------------------------------
     Description: IP address of the target, if available.
     String     : 192.168.0.16
Joomla ----------------------------------------------------------------
     Description: Opensource CMS written in PHP. Aggressive version detection
                  compares just 5 files, valid for versions 1.5.0-1.5.22 and
                  1.6.0-1.6.1. Homepage: http://joomla.org.
     Version    : 1.5

MetaGenerator ---------------------------------------------------------
     Description: This plugin identifies meta generator tags and extracts its
                  value.
     String     : Joomla! 1.5 - Open Source Content Management

PHP -------------------------------------------------------------------
     Description: PHP is a widely-used general-purpose scripting language
                  that is especially suited for Web development and can be
                  embedded into HTML. This plugin identifies PHP errors,
                  modules and versions and extracts the local file path and
                  username if present. - Homepage: http://www.php.net/
     Version    : 5.2.6-1+lenny9
     Module     : Suhosin-Patch
     Version    : 5.2.6-1+lenny9

Title -----------------------------------------------------------------
     Description: The HTML page title
     String     : Secretaría Nacional de Gestión de Riesgos (from page title)
```

Figura 2-31: Identificación de las Tecnologías del Portal Web de la SNGR

La consulta con la herramienta whatweb muestra información que concuerda con datos obtenidos en fases anteriores de la metodología; adicionalmente, se identifica una dirección de correo electrónico, y como Sistema de Gestión de Contenidos al Joomla![129] versión 1.5.

JoomScan[130]

Es una herramienta por línea de comandos que escanea y localiza vulnerabilidades conocidas de joomla! y de sus extensiones; en la figura 2-32, se observan 2 vulnerabilidades encontradas con la herramienta joomscan con la opción -u[131].

```
~$ ./joomscan.pl -u www.snriesgos.gob.ec
Target: http://www.snriesgos.gob.ec
## Checking if the target has deployed an Anti-Scanner measure
[!] Scanning Passed ..... OK
## Detecting Joomla! based Firewall ...
[!] .htaccess shipped with Joomla! is being deployed for SEO purpose
[!] It contains some defensive mod_rewrite rules
## Fingerprinting in progress ...
~Generic version family ..... [1.5.x]
~1.5.x en-GB.ini revealed [1.5.12 - 1.5.14]
~1.5.x admin en-GB.com_config.ini revealed [1.5.12 - 1.5.14]
~1.5.x adminlists.html revealed [1.5.7 - 1.5.14]
* Deduced version range is : [1.5.12 – 1.5.14]
Vulnerabilities Discovered. There are 2 vulnerable points in 40 found entries!
# 13
Info -> Core: Admin Backend Cross Site Request Forgery Vulnerability
Versions effected: 1.0.13 <=
Check: /administrator/
Exploit: It requires an administrator to be logged in and to be tricked into a specially crafted webpage.
Vulnerable? Yes
```

129 Joomla, Fuente: http://www.joomla.org/, (junio 2012)
130 JoomScan, Joomla Security Scanner, Fuente: http://sourceforge.net/projects/joomscan/, (julio 2012)
131 -u, Opción que indica la dirección URL a escanear.

```
# 30
Info -> CoreComponent: com_mailto timeout Vulnerability
Versions effected: 1.5.13 <=
Check: /components/com_mailto/
Exploit: [Requires a valid user account] In com_mailto, it was possible to bypass timeout
protection against sending automated emails.
Vulnerable? Yes
```

Figura 2-32: Verificación de Vulnerabilidades con JoomScan

La resultados muestran la posible versión del joomla!, así como un informe de vulnerabilidades que será analizado posteriormente; luego, se procede a detectar si el portal web tiene instalado algún tipo de protección para sus servicios, como puede ser un WAF[132] que detecte comportamientos anómalos en el trafico entrante y saliente.

Waffit[133]

Es una herramienta por linea de comandos que detecta cerca de 20 aplicaciones WAF; su funcionamiento se basa en los build-in rules utilizados por los Firewalls para detectar ataques, de este modo Waffit utiliza estos ataques para delatar la precedencia del propio WAF; en la figura 2-33, se observa que no se ha detectado ningún WAF instalado en el portal institucional.

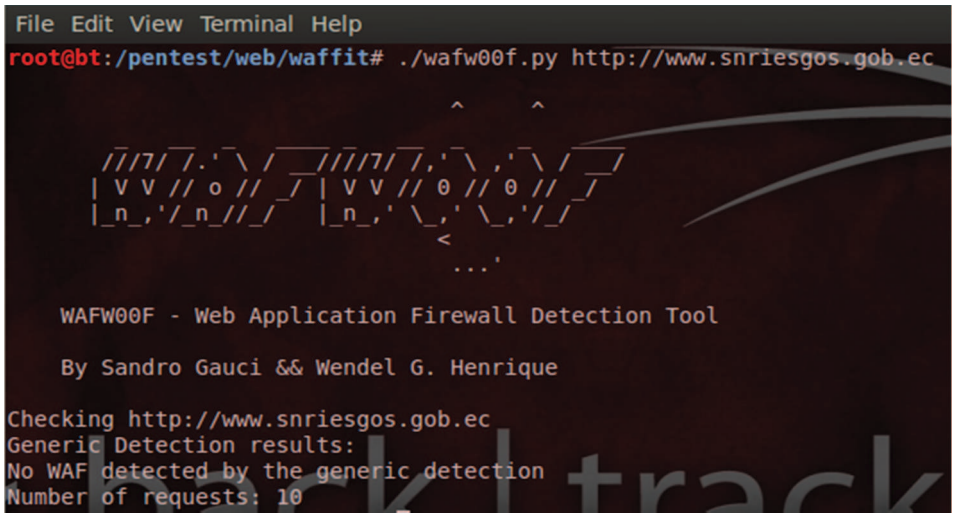


Figura 2-33: Identificación del WAF con WAFFIT

132 WAF, Web Application Firewall, (Cortafuegos de Aplicación Web)
133 WAFFIT, o WAFW00D, Herramienta de Detección WAF

En la tabla 2-24, se presenta una lista de vulnerabilidades identificadas en este capítulo.

Vulnerabilidad	Descripción
Portal web muestra versión del Apache	Portal web muestra detalles de la versión instalada del Apache
Portal web muestra correos electrónicos	Portal web muestra un correo electrónico de la Institución
Portal web muestra CMS instalado y su versión	Portal web muestra detalles del CMS instalado y de su versión
Portal web muestra versión del PHP	Portal web muestra detalles de la versión del PHP utilizado
Joomla! no tiene anti-escaner	Joomla! no tiene configurado un Anti-escaner
No hay protección ante el envío de correos automáticos	Vulnerabilidad de joomla!
Inicio de sección insegura para el administrador	
Portal web no tiene WAF	Portal web sin protección WAF

Tabla 2-24: Vulnerabilidades de la Aplicación Web[134]

2.2.2.13 Seguridad de Usuarios de Internet

La metodología establece evaluaciones para el IRC[135], Internet Explorer, Microsoft Outlook y la administración remota de equipos; en la tabla 2-25, se muestran parámetros de seguridad y características de usuarios de Internet.

Parámetros de Seguridad	Características
Revelación de direcciones IP por parte del usuario	Solamente en las Direcciones Provinciales
Aplicaciones IRC instaladas	Skype como medio interno, pero en Direcciones Provinciales no existe control de otros IRC
Transferencia de código malicioso	No controlado

134 Tabla elaborada por el autor
135 IRC, Internet Relay Chat

Compartición de archivos P2P	Restringido, pero no es controlado
Ingeniería Social	Varios usuarios son víctimas de correo dudoso y publicidad falsa
Uso de Internet Explorer	Pocos usuarios, la mayoría son de las Direcciones Provinciales
Uso de otros Exploradores	Si, especialmente Mozilla Firefox
Ultimas versiones y parches de los Exploradores	Solo en Matriz en las Direcciones Provinciales no están actualizados
Uso de Microsoft Outlook	Pocos usuarios
Uso de otros programas para correos electrónicos	No, la mayoría usa el correo por vía web.
Análisis HTML[136] habilitado en Outlook	Si
Uso de programas de administración remota	Si, mayormente Team Viewer
Uso de contraseñas seguras para la administración remota	Contraseñas proporcionadas aleatoriamente por la aplicación
Habilitada la conexión al escritorio remoto de Windows	En ningún equipo, solo para el servidor Anti-virus

Tabla 2-25: Parámetros de Seguridad de los Usuarios de Internet[137]

2.2.2.14 Seguridad Física

El objetivo en este capítulo es verificar que la seguridad física y ambiental sea la adecuada, garantizando el acceso a los sistemas de hardware y otros elementos vitales como el servicio de energía eléctrica, el aire acondicionado, teléfono y líneas de datos.

La metodología contempla 4 puntos de revisión: el sistema de control de acceso, protección contra fuego, control ambiental e interceptación de datos; en la tabla 2-26, se muestran parámetros de seguridad física para los puntos de revisión.

136 HTML, HyperText Markup Language, (Lenguaje de Marcado de Hipertexto)
137 Tabla elaborada por el autor, Fuente: ISSAF versión 0.2.1, páginas 560, 561, 562 y 563

Parámetros de Seguridad	Características
Centro de Datos protegido por barreras	Si
Guardias permiten ingreso a zonas sensibles	No hay guardias
Existe PACS[138] a zonas sensibles	Si
Existe tarjetas de proximidad o magnéticas para PACS	No
Existe identificación de Huellas digitales	Si
Personal con acceso a zonas sensibles	Solo personal de TIC
Registro de PACS es supervisado	No hay supervisión
Hay evaluación de actividades anómalas	Sin control
Control de ingresos y salidas a zonas sensibles por CCTV[139]	No
Existe sensores de movimiento	Si
Existe sistema de detección de incendios	Si
Funcionarios capacitados en caso de incendio	Si
Existe equipos de extensión de fuego	Si
Existe Sistema de Aire acondicionado y Control de Temperatura	Si
Existe UPS y acondicionamiento de energía eléctrica	Si
Equipos críticos conectados a UPS	Si
Existe generador de energía eléctrica	Si
Existen Interferencia Electromagnética	No
Sistemas críticos muestran información sensible en pantallas	No

Tabla 2-26: Parámetros de la Seguridad Física[140]

2.3 ANÁLISIS DE RIESGOS

Esta fase tiene como objetivo identificar vulnerabilidades de los parámetros de las entidades de evaluación, verificar las vulnerabilidades listadas en las fases anteriores, buscar falsos positivos, y luego definir una lista de riesgos para su evaluación.

138 PACS, Physical Access Control System, (Sistema de Control de Acceso Físico)
139 CCTV, Closed Circuit Television Monitoring
140 Tabla elaborada por el autor, Fuente: ISSAF versión 0.2.1, páginas 885, 886, 887, 888 y 889

2.3.1 VERIFICACIÓN DE VULNERABILIDADES

En la fase anterior no se identifica vulnerabilidades en todas las entidades de evaluación indicadas en el Anexo 2; por tal razón en la tabla 2-27, se muestran las entidades de evaluación y el motivo por el cual no se realiza la identificación de vulnerabilidades.

Entidad de Evaluación	***Parámetro***
Seguridad de los Switch	Posee cierto nivel de seguridad
Seguridad en la Red Privada Virtual (VPN)	SNGR no cuenta con servicio VPN
Seguridad AS/400	SNGR no cuenta con dicho Equipo
Seguridad Lotus Notes	SNGR no utiliza dicha aplicación
Seguridad de Sistemas UNIX y GNU/Linux	En otras entidades de evaluación se identifico vulnerabilidades de Servidores GNU/Linux
Seguridad de Sistemas Windows	Servidores de la SNGR usan Sistemas GNU/Linux
Seguridad Novell Netware	SNGR no tiene Servidores con Novell Netware
Seguridad de las Bases de Datos	Restringido por el Área de Alcance
Ingeniería Social	Usuarios no disponen de tiempo para contestar cuestionarios de Ingeniería Social

Tabla 2-27: Entidades de Evaluación sin Identificación de Vulnerabilidades[141]

Identificadas las entidades excluidas del análisis de riesgos, se procede a identificar vulnerabilidades de los parámetros de seguridad de Contraseñas, del Sistema Anti-virus, de la Red de Área de Almacenamiento, de la Red Inalámbrica, del Servidor Web, de los Usuarios de Internet y de la seguridad Física.

En la tabla 2-28, se muestran los parámetros identificados como vulnerabilidades.

[141] Tabla elaborada por el autor

Entidad de Evaluación	Vulnerabilidad
Seguridad de Contraseñas	Ninguna
Seguridad del Sistema Antivirus	Anti-virus no esta instalado en el Firewall
Seguridad SAN	La Información no se respalda continuamente
Seguridad en la Red Inalámbrica	SSID Broadcast activo
Seguridad del Servidor Web	Acceso al servidor desde cualquier dirección IP
	Servidor Web tiene habilitada la exploración de directorios
	Servidor Web no tiene balanceo de carga
Seguridad de los usuarios de Internet	Revelación de direcciones IP por parte del usuario
	Instalación de IRC's no permitidos
	Transferencia de código malicioso
	Instalación de aplicaciones P2P no permitidas
	Usuarios víctimas de correo no deseado
Seguridad Física	No hay guardias de Seguridad
	PACS no tiene tarjetas de proximidad o magnéticas
	No hay control ni supervisión del PACS
	No hay CCTV

Tabla 2-28: Parámetros identificados como vulnerabilidades[142]

La verificación de las vulnerabilidades que no son consideradas como falsos positivos se establece que son vulnerabilidades propiamente identificadas como riesgos, ya que las pruebas realizadas en fases anteriores de acuerdo a la metodología son de verificación y pueden ser evaluadas en la siguiente fase.

"Los falsos positivos se refieren a cuestiones que son detectadas incorrectamente"[143], y con el propósito de reducir la probabilidad de falsas detecciones en la tabla 2-29, se muestran las vulnerabilidades consideradas como falsos positivos.

142 Tabla elaborada por el autor
143 Fuente:Handling False Detection Rates, Fuente: ISSAF versión 0.2.1, página 1176

Entidad de Evaluación	Vulnerabilidad
Seguridad en la Red Inalámbrica	SSID Broadcast activo
Seguridad Física	PACS no tiene tarjetas de proximidad o magnéticas

Tabla 2-29: Falsos positivos[144]

Es necesario que este activo el SSID Broadcast, para que los usuarios puedan conectarse a la red dependiendo del sitio o de la señal proporcionada por el dispositivo, y no es necesario contar con tarjetas magnéticas para PACS, porque ya se cuenta con acceso por Huella digital; por tal motivo se puede descartar las vulnerabilidades consideradas como falsos positivos.

2.4 EVALUACIÓN DE LOS RIESGOS

El objetivo de este capítulo es el de establecer valores de riesgo, probabilidad de ocurrencia y su posible impacto técnico y de negocio; en la tabla 2-30, se muestra el número de vulnerabilidades para cada entidad de evaluación.

Entidad de Evaluación	Vulnerabilidades
Recopilación de Información	4
Mapeo de Red	5
Seguridad de Contraseñas	0
Seguridad del Router	3
Seguridad del Firewall	5
Seguridad del IDS	2
Seguridad del Sistema Anti-Virus	1
Seguridad VLAN	0
Seguridad SAN	1
Seguridad del Servidor Web	3
Seguridad de las Aplicaciones Web	8
Seguridad de los Usuarios de Internet	5
Seguridad Física	3

Tabla 2-30: Vulnerabilidades a evaluar[145]

144 Tabla elaborada por el autor

2.4.1 VALORACIÓN DEL RIESGO

La metodología contempla valoraciones de riesgo de impacto técnico y de impacto de negocio; la primera se determina en conjunto con la parte técnica de TIC, y la segunda se determina de acuerdo a la posibilidad de ocurrencia de una amenaza en los procesos de negocio de la organización.

La valoración de riesgo de vulnerabilidades de impacto técnico generalmente se realiza automáticamente con herramientas de análisis de vulnerabilidades, descartando los falsos positivos y con la ayuda técnica de TIC; en la tabla 2-31, se muestra los valores de acuerdo al nivel de vulnerabilidad.

Severidad	Valor asignado
Vulnerabilidad de Riesgo Muy Alto	1
Vulnerabilidad de Riesgo Alto	0.8
Vulnerabilidad de Riesgo Medio	0.6
Vulnerabilidad de Riesgo Bajo	0.4
Vulnerabilidad de Riesgo Muy Bajo	0.2

Tabla 2-31: Valoración de Riesgo en el Impacto Técnico[146]

"Las amenazas son eventos que pueden conducir a un daño potencial y causar efectos no deseados y cada amenaza debe ser claramente definida como un evento que podría suceder, independientemente de la probabilidad o posibilidad de que se produzca."[147]

La valoración de riesgo de vulnerabilidades de impacto de negocio se realiza en función de las amenazas y el efecto que tengan en los procesos críticos de negocio; en la tabla 2-32, se muestran los valores de probabilidad que se pueden asignar a las amenazas.

145 Tabla elaborada por el autor, Fuente: Anexo 5, Vulnerabilidades de la SNGR
146 Tabla elaborada por el autor, Fuente: ISSAF versión 0.2.1, páginas 99
147 Fuente: Risk Assessment, Fuente: ISSAF versión 0.2.1, página 98

Clasificación	Probabilidad de Ocurrencia
Casi Seguro	Muy alta, puede ocurrir varias veces por año en la misma ubicación, operación o actividad.
Probable	Alta, puede ocurrir varias veces por año en la Institución.
Posible	Posible, puede ocurrir por lo menos una vez al año o se produce previamente en algún instante de tiempo.
Improbable	No es imposible, probablemente pueda ocurrir durante los próximos años.
Raro	Muy bajo, muy poco probable durante los próximos años.

Tabla 2-32: Valores de Probabilidad de Amenazas[148]

En la tabla 2-33, se describe el criterio de valoración de riesgo de vulnerabilidades en función del impacto de negocio.

Severidad	Criterio de Valoración
Vulnerabilidad de Riesgo Alto	Las vulnerabilidades se clasifican como de alto riesgo, si hay una amenaza inmediata de impacto alto y adverso en los procesos críticos de negocio de la organización. Es decir las vulnerabilidades que permiten compromiso para los sistemas de apoyo a los procesos críticos de negocio, o las vulnerabilidades que permiten la propagación masiva malware que afecte a estos sistemas o que los servicios de estos sistemas se vean comprometidos.
Vulnerabilidad de Riesgo Medio	Las Vulnerabilidades se clasifican como de riesgo medio, si hay una amenaza de alto impacto y que tenga efectos adversos a los sistemas no críticos en términos de negocio. Además, si no existe una amenaza inmediata de gran impacto y exista una vulnerabilidad que afecte críticamente a los sistemas de negocio como por ejemplo dejar fuera de operación a los servicios del sistema sin afectar al negocio, la vulnerabilidad se clasifica como medio.
Vulnerabilidad de Riesgo Bajo	La vulnerabilidad debe ser clasificada como un riesgo bajo cuando las vulnerabilidades técnicas y el impacto de negocio son bajas, como por ejemplo revelación de información.

Tabla 2-33: Valoración de Riesgo en el Impacto de Negocio[149]

[148] Tabla elaborada por el autor, Fuente: ISSAF versión 0.2.1, páginas 98

2.4.2 ANÁLISIS DE IMPACTO

El objetivo es obtener una lista definitiva de vulnerabilidades según la gravedad de riesgo en base al impacto en los procesos de negocio y teniendo en cuenta que esta clasificación puede ser diferente a la clasificación de riesgo técnico.

2.4.2.1 Análisis de Impacto Técnico

El análisis de impacto técnico se lo realiza en conjunto con funcionarios del Área de Infraestructura y Telecomunicaciones de la Dirección de TIC de la Institución y utilizando los valores de riesgo de la tabla 2-31.

En la tabla 2-34, se presentan los valores de riesgo para cada una de las vulnerabilidades de las entidades de evaluación.

Entidad de Evaluación	Vulnerabilidades	Valor de Riesgo
Recopilación de Información	Muestra detalles de la dirección IP publica	0.2
	Nombres de Dominio relacionadas a IP's publicas	0.4
	Nombres de Dominio relacionadas a IP's internas	0.6
	Muestra versión instalada del BIND	0.8
Mapeo de Red	Respuestas ICMP de Servidores	0.8
	Puertos abiertos en los servidores DNS, Correo y HTTP	1
	Servidores muestran versión de servicios activos y del Sistema Operativo	1
	Detalles perímetro de RED	0.6
	El Firewall también es el servidor DNS	1
Seguridad del Router	Router muestra puertos abiertos y servicios activos	0.8
	Router muestra versión del Sistema Operativo	0.4
	Router tiene protocolos de enrutamiento estático	0.8
Seguridad del Firewall	Firewall muestra puertos abiertos y servicios activos	1
	Firewall presenta puertos con servicios utilizados por la Dirección de TIC	0.6

[149] Tabla elaborada por el autor, Fuente: ISSAF versión 0.2.1, páginas 250, 251 y 252

Seguridad del Firewall	Firewall presenta puertos abiertos no establecidos por la Dirección de TIC	1
	Firewall tiene pocas reglas de filtrado	0.6
	Firewall presenta puertos que pueden ser usados por troyanos	1
Seguridad del IDS	HIDS Instalado	1
	NIDS Instalado	1
Seguridad del Sistema Anti-Virus	Anti-virus no está instalado en el Firewall	1
Seguridad SAN	La Información no se respalda continuamente	0.8
Seguridad del Servidor Web	Acceso al servidor desde cualquier dirección IP	0.6
	Servidor Web tiene habilitada la exploración de directorios	0.8
	Servidor Web no tiene balanceo de carga	0.8
Seguridad de las Aplicaciones Web	Portal web muestra versión del Apache	0.2
	Portal web muestra correos electrónicos	0.4
	Portal web muestra CMS instalado y su versión	0.6
	Portal web muestra versión del PHP	0.2
	Joomla! no tiene anti-escaner	0.6
	No hay protección ante el envío de correos automáticos	0.8
	Inicio de sección insegura para el administrador	1
	Portal web no tiene WAF	1
Seguridad de los Usuarios de Internet	Revelación de direcciones IP por parte del usuario	0.4
	Instalación de IRC's no permitidos	0.6
	Transferencia de código malicioso	1
	Instalación de aplicaciones P2P no permitidas	0.6
	Usuarios víctimas de correo no deseado	0.6
Seguridad Física	No hay guardias de Seguridad	0.8
	No hay control ni supervisión del PACS	0.2
	No hay CCTV	0.8

Tabla 2-34: Análisis de Impacto Técnico[150]

150 Tabla elaborada por el autor, Fuente: Anexo 5, Vulnerabilidades de la SNGR

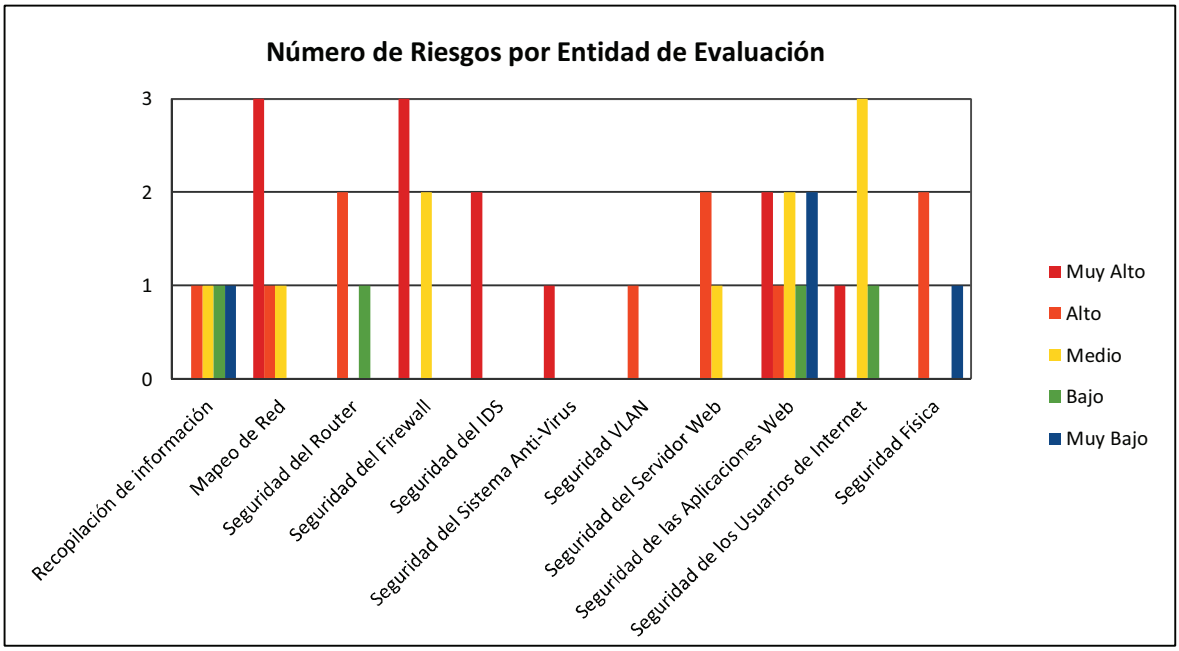
Luego se presenta un sumario de vulnerabilidades del impacto técnico; en la tabla 2-35, se muestran las entidades de evaluación y el número de vulnerabilidades para cada nivel de riesgo.

Entidad de Evaluación	Muy Alto	Alto	Medio	Bajo	Muy Bajo
Recopilación de Información	-	1	1	1	1
Mapeo de Red	3	1	1	-	-
Seguridad del Router	-	2	-	1	-
Seguridad del Firewall	3		2	-	-
Seguridad del IDS	2	-	-	-	-
Seguridad del Sistema Anti-Virus	1	-	-	-	-
Seguridad SAN	-	1	-	-	-
Seguridad del Servidor Web	-	2	1	-	-
Seguridad de las Aplicaciones Web	2	1	2	1	2
Seguridad de los Usuarios de Internet	1	-	3	1	-
Seguridad Física	-	2	-	-	1

Tabla 2-35: Sumario de Riesgos de Impacto Técnico[151]

El sumario muestra que hay 12 vulnerabilidades de riesgo muy alto, 10 vulnerabilidades de riesgo alto, 10 vulnerabilidades de riesgo medio, 4 vulnerabilidades de riesgo bajo y 4 vulnerabilidades de riesgo muy bajo; en la figura 2-34, se muestran gráficamente el número de riesgos y el porcentaje de riesgos del Sumario de Riesgos de Impacto Técnico.

151 Tabla elaborada por el autor



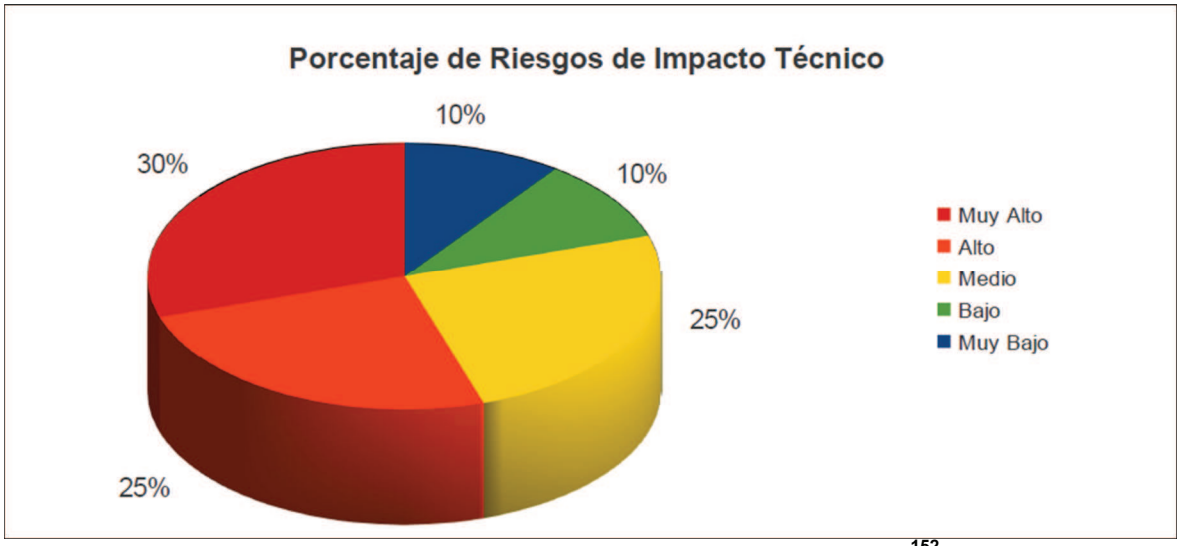


Figura 2-34: Sumario de Riesgos de Impacto Técnico[152]

2.4.2.2 Análisis de Impacto de Negocio

Los procesos críticos de la SNGR son: servicios de Internet, SNIGR, Correo electrónico y Portal web; en la tabla 2-36, se muestran las posibles amenazas, su descripción y la probabilidad de que ocurran dichas amenazas.

152 Gráficos elaborados por el Autor

Amenaza	Descripción	Procesos Críticos	Ocurrencia
Programas maliciosos	Programas destinados a perjudicar o a hacer uso ilícito de los recursos de servicios o sistemas.	Todos los servicios SNGR	Probable
Intrusos	Personas que consiguen acceder a los datos o programas de los cuales no tienen acceso permitido.	Todos los servicios SNGR	Probable
Siniestro	Mala manipulación o malintención que derivan en pérdida o robo de información.	Correo electrónico	Improbable
Usuarios	Problemas de seguridad ligados al uso de servicios o sistemas.	Todos los servicios SNGR	Casi Seguro
Ingeniería Social	Obtener información confidencial a través de la manipulación de usuarios legítimos.	Correo electrónico	Posible

Tabla 2-36: Amenazas, Procesos Críticos y Posibilidad de Ocurrencia[153]

El análisis de impacto de negocio se lo realiza utilizando la valoración de riesgos de la tabla 2-33, y la información de la tabla 2-36; en la tabla 2-37, se presentan los niveles de riesgo para cada una de las vulnerabilidades.

Entidad de Evaluación	Vulnerabilidades	Nivel de Riesgo
Recopilación de Información	Muestra detalles de la dirección IP publica	Bajo
	Nombres de Dominio relacionadas a IP's publicas	Bajo
	Nombres de Dominio relacionadas a IP's internas	Medio
	Muestra versión instalada del BIND	Medio
Mapeo de Red	Respuestas ICMP de Servidores	Bajo
	Puertos abiertos en los servidores DNS, Correo y HTTP	Alto
	Servidores muestran versión de servicios activos y del Sistema Operativo	Alto
	Detalles perímetro de RED	Medio
	El Firewall también es el servidor DNS	Alto
Seguridad del Router	Router muestra puertos abiertos y servicios activos	Medio
	Router muestra versión del Sistema Operativo	Bajo

153 Tabla elaborada por el autor

	Router tiene protocolos de enrutamiento estático	Medio
Seguridad del Firewall	Firewall muestra puertos abiertos y servicios activos	Alto
	Firewall presenta puertos con servicios utilizados por la Dirección de TIC	Medio
	Firewall presenta puertos abiertos no establecidos por la Dirección de TIC	Alto
	Firewall tiene pocas reglas de filtrado	Medio
	Firewall presenta puertos que pueden ser usados por troyanos	Alto
Seguridad del IDS	HIDS Instalado	Alto
	NIDS Instalado	Alto
Seguridad del Sistema Anti-Virus	Anti-virus no está instalado en el Firewall	Alto
Seguridad SAN	La Información no se respalda continuamente	Alto
Seguridad del Servidor Web	Acceso al servidor desde cualquier dirección IP	Medio
	Servidor Web tiene habilitada la exploración de directorios	Medio
	Servidor Web no tiene balanceo de carga	Alto
Seguridad de las Aplicaciones Web	Portal web muestra versión del Apache	Bajo
	Portal web muestra correos electrónicos	Bajo
	Portal web muestra CMS instalado y su versión	Medio
	Portal web muestra versión del PHP	Bajo
	Joomla! no tiene anti-escaner	Medio
	No hay protección ante el envío de correos automáticos	Alto
	Inicio de sección insegura para el administrador	Alto
	Portal web no tiene WAF	Alto
Seguridad de los Usuarios de Internet	Revelación de direcciones IP por parte del usuario	Bajo
	Instalación de IRC's no permitidos	Medio
	Transferencia de código malicioso	Alto
	Instalación de aplicaciones P2P no permitidas	Bajo
	Usuarios víctimas de correo no deseado	Alto
Seguridad Física	No hay guardias de Seguridad	Alto
	No hay control ni supervisión del PACS	Bajo
	No hay CCTV	Alto

Tabla 2-37: Análisis de Impacto de Negocio[154]

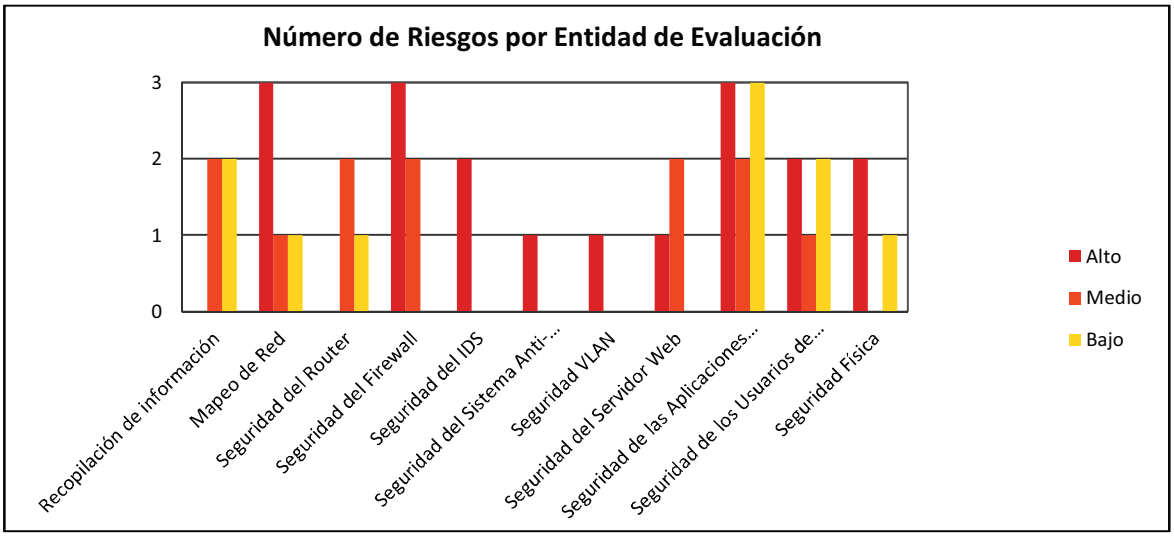
154 Tabla elaborada por el autor, Fuente: Anexo 5, Vulnerabilidades de la SNGR

Luego se presenta un sumario de vulnerabilidades del impacto de negocio; en la tabla 2-38, se muestran las entidades de evaluación y el número de vulnerabilidades para cada nivel de riesgo.

Entidad de Evaluación	Alto	Medio	Bajo
Recopilación de Información	-	2	2
Mapeo de Red	3	1	1
Seguridad del Router	-	2	1
Seguridad del Firewall	3	2	-
Seguridad del IDS	2	-	-
Seguridad del Sistema Anti-Virus	1	-	-
Seguridad SAN	1	-	-
Seguridad del Servidor Web	1	2	-
Seguridad de las Aplicaciones Web	3	2	3
Seguridad de los Usuarios de Internet	2	1	2
Seguridad Física	2	-	1

Tabla 2-38: Sumario de Riesgos de Impacto de Negocio[155]

El sumario muestra que hay 18 vulnerabilidades de riesgo alto, 12 vulnerabilidades de riesgo medio y 10 vulnerabilidades de riesgo bajo; en la figura 2-35, se muestran gráficamente el número de riesgos y el porcentaje de riesgos para cada nivel del Sumario de Riesgos de Impacto de Negocio.



155 Tabla elaborada por el autor

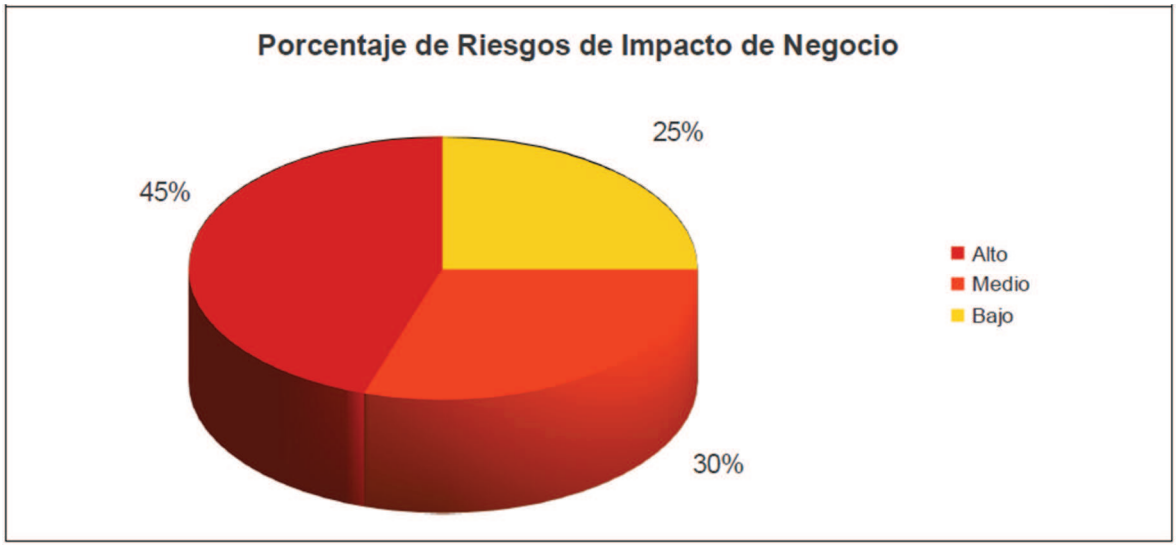


Figura 2-35: Sumario de Riesgos de Impacto de Negocio[156]

CAPÍTULO 3

3 TRATAMIENTO DE LOS RIESGOS

3.1 PLAN DE MITIGACIÓN DE RIESGOS EN BASE A LOS ANÁLISIS DE IMPACTO

El plan de mitigación de riesgos es una tarea que tiene como objetivo principal elaborar un conjunto de programas de mitigación de riesgos basado en el análisis de impacto técnico y de impacto de negocio, con actividades que permitan reducir el impacto al mínimo nivel.

3.1.1 CONTRAMEDIDAS PARA LAS ENTIDADES DE EVALUACIÓN

ISSAF contemplan un conjunto de contramedidas específicas para cada una de las pruebas realizadas en las fases de la metodología, así como contramedidas globales para cada entidad de evaluación.

156 Gráficos elaborados por el autor

Recopilación de información

a) No dar nombres ni números telefónicos de la persona técnica para la base de datos de Whois.
b) Utilizar nombres genéricos como “hostmaster” y/o “postmaster”.
c) No asociar correos electrónicos con base de datos de Whois.
d) Restringir transferencias de zona a los servidores de confianza.
e) Restringir transferencias de zona desde el Internet.
f) Permitir la transferencia de zona sólo para dominios autorizados.
g) Permitir el puerto 53 TPC en el firewall sólo para dominios autorizados.
h) Usar DNS de horizonte dividido (zonas internas y externas separadas)
i) Asegurar que los registros HINFO[157] no se visualicen en los archivos de zona DNS.”[158]

Mapeo de red

a) “Bloquear peticiones ICMP en el firewall y en el router.
b) Desactivar todos los servicios innecesarios en los servidores DNS.
c) Permitir solo los servicios necesarios, y limitar los servicios innecesarios en la frontera del Firewall.
d) Bloquear paquetes TPC SYN innecesarios.
e) Bloquear paquetes UDP innecesarios.
f) Configurar el firewall permitiendo solo lo absolutamente necesario.
g) Restringir las direcciones de origen en el firewall si un determinado puerto o servicio no debe ser accesible a cualquiera.
h) Cambiar nombres y números de versión de los servicios instalados.
i) Modificar información en las cabeceras de paquetes para la identificación de sistemas críticos.
j) Filtrar salida ICMP TTL excedido y los paquetes de destino inaccesible.
k) Permitir el tráfico a través del firewall sólo a hosts específicos.
l) Filtrar puertos de administración.

157 HINFO, Host INFOrmation, (Información de Host)
158 Fuente: ISSAF versión 0.2.1, páginas 206 y 207

m) Si es posible, filtrar respuestas ICMP de sistemas críticos para el Internet."[159]

Seguridad del router

"Los dispositivos de enrutamiento son componentes críticos y requieren de una correcta configuración, las contramedidas señaladas son:

a) Configuración del registro y seguimiento de logs regularmente.
b) Filtrado de paquetes por ACL[160]
c) Limitar el acceso por Telnet[161]
d) Limitar el acceso local.
e) Deshabilitar todos los servicios no esenciales.
f) Configurar Anti-Spoofing[162].
g) Configurar filtrado de paquetes para evitar ataques DoS[163].
h) Desactivar la difusión dirigida por IP para evitar ataques DDoS[164].
i) Limitar el envío de paquetes ICMP.
j) Implementar interceptación TCP para evitar inundaciones SYN.
k) Crear listas de acceso reflexivo para prevenir conexiones Hijacking[165].
l) Implementar router basado en IDS."[166]

Seguridad del firewall

a) "Permitir el tráfico basándose en políticas de acceso a los servicios definidas por el tráfico que está permitido dentro de la red, el tráfico que se le permite salir de red y negando el resto de tráfico.
b) Utilizar aplicaciones proxies.

---

159 Fuente: ISSAF versión 0.2.1, páginas 212, 214, 220, 222 y 247
160 ACL, Access Control Lists, (Listas de Control de Acceso)
161 Telnet, TELecommunication NETwork, (Redes de Telecomunicación)
162 Spoofing, Fuente: http://es.wikipedia.org/wiki/Spoofing, (septiembre 2012)
163 DoS, Denial of Service, (Denegación de Servicio)
164 DDoS, Distributed Denial of Service, (Denegación de Servicio Distribuido)
165 Hijacking, http://es.wikipedia.org/wiki/Hijacking, (septiembre 2012)
166 Fuente: ISSAF versión 0.2.1, páginas 433, 434 y 435

c) Tener una regla “Drop All” como ultima regla en la base de reglas.
d) Evitar que el firewall envié paquetes procedentes de la puerta de enlace.
e) Evitar el uso de “Any” en la base de reglas
f) Deshabilitar o cambiar la configuración predeterminada del Firewall tanto como sea posible.”[167]

Seguridad de las redes de área de almacenamiento (SAN)

a) “Asegurar los datos almacenados en matrices de almacenamiento, bibliotecas de cintas y dispositivos SAN mediante el control de acceso, autenticación, cifrado y compresión.
b) Examinar los puntos de acceso del software de almacenamiento para asegurarse de que es seguro y limita el acceso a los datos cruciales.
c) Examinar los medios para asegurar la estructura de almacenamiento contra acceso no autorizado y no autenticado.
d) Asegurar que los equipos SAN soportan integración con IPsec[168], VLAN's, así como firewalls y sistemas de detección de intrusos.”[169]

Seguridad del servidor web

a) “Limitar el acceso a los administradores del servidor web y permitir el acceso a través de mecanismos seguros de autenticación.
b) En los escenarios de administración remota, las direcciones IP que permiten administrar el servidor web deben estar claramente definidas y los procesos administrativos restringidos a esas direcciones IP.
c) El acceso administrativo debe hacer uso de medios seguros, como ssh o VPN.
d) Servidor Web debe tener servicios no esenciales desactivados.
e) Configuración de SYN cookies a nivel de sistema operativo para protegerlo contra ataques de inundación SYN.

167 Fuente: ISSAF versión 0.2.1, páginas 467 y 468
168 IPsec, Internet Protocol Security, (Seguridad en el Protocolo de Internet)
169 Fuente: ISSAF versión 0.2.1, páginas 537

f) El servidor Web debe estar actualizado con los últimos parches de seguridad para el sistema operativo y para el CMS.
g) Desactivar la exploración de directorios especialmente en las carpetas que contienen scripts o ejecutables.
h) El servidor Web debe tener un número mínimo de cuentas de acceso al sistema.
i) Eliminar las asignaciones no utilizadas de secuencias de comandos.
j) Ejecutar el servidor web como usuario no root.
k) Implementar servidor Web con balanceo de carga."[170]

Seguridad de las aplicaciones web

"Para la seguridad de las aplicaciones web, las contramedidas se puede dividir en dos partes: contramedidas para el lado del cliente y contramedidas para el lado del servidor.
Contramedidas para el lado del cliente:

a) No seleccionar "recordar o guardar" en las opciones del navegador.
b) Utilizar SSL[171] para las opciones de login estándar y de seguridad.
c) Usar parches en el navegador para protegerse de ataques "Cross-site Scripting"[172].

Contramedidas para el lado del servidor:

a) Usar parches en el servidor Web con regularidad.
b) Verificar continuamente los registros del servidor Web en busca de anomalías.
c) Las aplicaciones web deben validar los datos en el servidor y en el lado del cliente.
d) Dar solo los privilegios necesarios a los usuarios.
e) Utilizar parámetros escritos de forma inflexible, si es posible en

170 Fuente: ISSAF versión 0.2.1, páginas 715, 716 y 717
171 SSL, Secure Sockets Layer, (capa de Conexión Segura)
172 Cross-Site Scripting, (Secuencias de comandos en sitios cruzados) Fuente: http://es.wikipedia.org/wiki/Cross-site_scripting, (septiembre 2012)

combinación con procedimientos almacenados, para las consultas en la base de datos."[173]

Seguridad de usuarios de Internet

a) "No utilizar IRC en los sistemas de producción.
b) En caso de usar IRC desactivar la capacidad de DCC[174].
c) Utilizar los parches sugeridos para los navegadores.
d) Desactivar análisis HTML en Outlook."[175]

Seguridad del IDS, seguridad del sistema Anti-Virus y seguridad Física

La metodología no contempla contramedidas específicas ni globales para las tres entidades de evaluación, pero si considera que la infraestructura tecnológica de la Institución cuente con dispositivos, sistemas y bloqueos que minimicen los riesgos detectados en dichas entidades de evaluación.

3.1.2 PLAN DE MITIGACIÓN DE RIESGOS

El plan de mitigación de riesgos consiste en establecer soluciones o medidas que permitan minimizar el Impacto Técnico e Impacto de Negocio de los riesgos detectados de acuerdo al nivel de criticidad y las consecuencias que puedan ocasionar, así como tiempos y responsables para dichas soluciones.

En el análisis de riesgos de Impacto Técnico e Impacto de Negocio se establecieron niveles de riesgo para cada una de las vulnerabilidades detectadas, dichos niveles también pueden ser usados para establecer la criticidad de riesgo, además con la ayuda del sumario de Impacto Técnico e Impacto de Negocio se pueden establecer cuáles son las entidades de evaluación que tienen el mayor número de riesgos de alto impacto y mayor criticidad.

---

173 Fuente: ISSAF versión 0.2.1, páginas 779 y 806
174 DCC, Direct Client-to-Client, Fuente: http://es.wikipedia.org/wiki/Direct_Client-to-Client, (septiembre 2012)
175 Fuente: ISSAF versión 0.2.1, páginas 560, 561 y 562

En la tabla 3-1, se muestran el plan de mitigación para el Impacto Técnico y para el Impacto de Negocio.

IDENTIFICACIÓN		CUANTIFICACIÓN				MITIGACIÓN
#	Descripción del Evento de Riesgo	Criticidad (%)			Consecuencias	Solución (Contramedidas)
		Bajo	Medio	Alto		
		0 - .35	.35 -. 65	.65 - 1.0		
1	Muestra versión instalada del BIND			x	Posible ataque al servidor DNS	Contramedidas Recopilación de Información (g)
2	Puertos abiertos en los servidores DNS, Correo y HTTP			x	Posible intrusión y/o ataque a los servidores	Contramedidas Mapeo de Red (d - g)
3	Servidores muestran versión de servicios activos y del Sistema Operativo			x	Posible intrusión y/o ataque a los servidores	Contramedidas Mapeo de Red (b), (c) y (h)
4	El Firewall también es el servidor DNS			x	Posible intrusión y/o ataque	Separar Firewall del Servidor DNS
5	Firewall muestra puertos abiertos y servicios activos			x	Posible intrusión y/o ataque	Contramedidas Seguridad del Firewall (a) y (f)
6	Firewall presenta puertos abiertos no establecidos por la Dirección de TIC			x	Posible intrusión y/o ataque	Contramedidas Seguridad del Firewall (a) y (f)
7	Firewall presenta puertos que pueden ser usados por troyanos			x	Posible intrusión y/o ataque	Contramedidas Seguridad del Firewall (a)
8	HIDS Instalado			x	Intrusión y/o ataque no detectado	Instalar HIDS
9	NIDS Instalado			x	Intrusión y/o ataque no detectado	Instalar NIDS

10	Anti-virus no está instalado en el Firewall			x	Programas maliciosos no detectados	Instalar Anti-Virus en el Firewall
11	La Información no se respalda continuamente			x	Perdida de Información	Contramedidas Seguridad SAN (a)
12	Servidor Web tiene habilitada la exploración de directorios			x	Robo de información	Contramedidas Seguridad del Servidor Web (g)
13	No hay protección ante el envío de correos automáticos			x	Posible ataque	Contramedidas Seguridad de las Aplicaciones Web, lado del servidor (b) y (c)
14	Inicio de sección insegura para el administrador			x	Posible ataque	Contramedidas Seguridad de las Aplicaciones Web, lado del servidor (c) y (d)
15	Portal web no tiene WAF			x	Intrusión y/o ataque no detectado	Instalar WAF
16	Respuestas ICMP de Servidores		x		Identificación de Hosts	Contramedidas Mapeo de Red (a) y (m)
17	Detalles perímetro de RED		x		Identificación de Hosts	Contramedidas Mapeo de Red (i - l)
18	Router muestra puertos abiertos y servicios activos		x		Posible intrusión y/o ataque	Contramedidas Seguridad del Router (a-d)
19	Router tiene protocolos de enrutamiento estático		x		Posible ataque	Contramedidas Seguridad del Router (f - l)
20	Firewall presenta puertos con servicios utilizados por la Dirección de TIC		x		Posible intrusión y/o ataque	Contramedidas Seguridad del Firewall (a-f)
21	Firewall tiene pocas reglas de filtrado		x		Posible intrusión y/o ataque	Contramedidas Seguridad del Firewall (a-f)
22	Servidor Web no tiene balanceo de carga		x		Problemas con los sistemas y servicios	Contramedidas Seguridad del Servidor Web (k)

23	Portal web muestra CMS instalado y su versión		x		Posible ataque	Configurar servidor para ocultar información
24	Joomla! No tiene anti-escaner		x		Intrusión no detectada	Instalar un Anti-escaner
25	Transferencia de código malicioso		x		Instalación de Programas Maliciosos	Realizar transferencia de archivos de manera segura o restringirla
26	No hay guardias de Seguridad		x		Robo de información y/o equipos	Contratar Seguridad privada
27	No hay CCTV		x		Robo de información y/o equipos	Instalar un sistema completo de CCTV
28	Muestra detalles de la dirección IP publica	x			Ingeniería Social	Contramedidas Recopilación de Información (a - c)
29	Nombres de Dominio relacionadas a IP's publicas	x			Identificación de Sistemas y equipos	Contramedidas Recopilación de Información (d - i)
30	Nombres de Dominio relacionadas a IP's internas	x			Identificación de Sistemas y equipos	Contramedidas Recopilación de Información (f)
31	Router muestra versión del Sistema Operativo	x			Identificación de Host	Contramedidas Mapeo de Red (k) y (m)
32	Acceso al servidor desde cualquier dirección IP	x			Acceso de personal no autorizado	Contramedidas Seguridad del Servidor Web (a - c)
33	Portal web muestra versión del Apache	x			Posible ataque	Configurar servidor para ocultar información
34	Portal web muestra correos electrónicos	x			Ingeniería Social	Configurar servidor para ocultar información
35	Portal web muestra versión del PHP	x			Posible ataque	Configurar servidor para ocultar información
36	Revelación de direcciones IP por parte	x			Acceso de personal no	Restringir la revelación de direcciones IP

	del usuario				autorizado	
37	Instalación de IRC's no permitidos	x			Instalación de Programas Maliciosos	Contramedidas Seguridad de Usuarios de Internet (a)
38	Instalación de aplicaciones P2P no permitidas	x			Instalación de Programas Maliciosos y/o robo de información	Restringir compartición de archivos P2P
39	Usuarios víctimas de correo no deseado	x			Acceso a información no autorizada	Educar a los usuarios sobre Ingeniería Social
40	No hay control ni supervisión del PACS	x			Robo de información y/o equipos no detectado	Supervisar y registrar las actividades anómalas

Tabla 3-1: Plan de mitigación de Riegos para el Impacto Técnico y para el Impacto de Negocio[176]

176 Tabla elaborada por el autor, Fuente: ISSAF versión 0.2.1, página 50, Anexo 5, Vulnerabilidades de la SNGR

En el capítulo anterior se establecieron contramedidas que permiten solucionar o minimizar el impacto de los riesgos detectados para cada entidad de evaluación y que pueden ser aplicados como solución de cada uno de los riesgos del plan de mitigación de riesgos.

El plan de mitigación muestra cada uno de los riesgos ordenados de acuerdo a su criticidad, indicando la consecuencia en caso de que ocurra y principalmente indicando la solución; y para la aplicación de dicho plan es necesario la coordinación por parte de la Administradora de Infraestructura y de TIC para realizar las correcciones respectivas estableciendo tiempos y plazos para cada uno de los riesgos de acuerdo a su criticidad.

3.2 PRESENTACIÓN DE CONCLUSIONES Y RECOMENDACIONES PARA MITIGAR LOS RIESGOS

El objetivo principal es dar a conocer a las personas encargadas de la administración de la Infraestructura Tecnológica de la SNGR, que áreas de la institución se encuentran con mayor valor de riesgo y que son criticas ante posibles amenazas, las cuales pueden ser minimizadas con las oportunas y debidas medidas de seguridad.

Para alcanzar el objetivo de este proyecto se realiza el Análisis de Riesgos y Vulnerabilidades de los Sistemas, Servicios y Equipos de la Infraestructura Tecnológica de la SNGR ubicada en el COE Quito, mediante el uso de la metodología de Ethical Hacking "ISSAF" y con herramientas recomendadas por la misma metodología.

Las conclusiones y recomendaciones expuestas a continuación están basadas en el Análisis de Riesgos y Vulnerabilidades que se realizada en el presente proyecto, y que tienen el propósito de mitigar los riesgos detectados.

Conclusiones para mitigar los riesgos

- El análisis de riesgos y vulnerabilidades muestra varios puertos abiertos y servicios activos innecesarios no utilizados por los Servidores DNS0, DNS1, y por el Firewall, además se identifica que uno de los servidores DNS es parte del Firewall; llegando a concluir que dichos servidores presentan un nivel de criticidad muy alto ya que no cuentan con políticas de seguridad.

- Se identifica que la Infraestructura Tecnológica no cuenta con Sistemas de Detección de Intrusos de Host y Red, ni cuenta con un Sistema Anti-Virus para el Firewall, lo que permite a intrusos y atacantes no ser detectados, y que la infraestructura de red pueda ser infectada por programas maliciosos.

- Los riesgos encontrados en otras áreas muestran problemas de seguridad relacionados a la revelación y acceso de información de Host y de equipos de infraestructura, llegando a concluir que son riesgos con un nivel de criticidad medio y que no cuentan con medidas de control para la publicación de información.

- Del análisis de riesgos y vulnerabilidades se determina que el servidor web y el portal institucional presentan problemas de seguridad tanto para el acceso del administrador, para la versión instalada del joomla! y para la estructura de directorios, además muestra información que puede ser usada para ingeniería social, llegando a la conclusión de que son riesgos con un nivel de criticidad alto y no cuentan con medidas de seguridad.

- También se identifica que los usuarios de Internet tienen riesgos relacionados al uso e instalación de programas no autorizados, problemas con programas maliciosos o virus, y el área física no cuenta con guardias, ni con sistemas de circuito cerrado de cámaras cctv; concluyendo que son riesgos de nivel medio o bajo, y que pueden ser resueltos o corto plazo.

- En base al análisis de impacto técnico e impacto de negocio se elabora el plan de mitigación de riesgos para el presente proyecto, en el que se toma en cuenta la criticidad y principalmente la posible solución para cada riesgo detectado.

Recomendaciones para mitigar los riesgos

- Se recomienda limitar la publicación de información de servidores y sistemas al público de Internet y liberar únicamente información básica de la Institución.

- Se recomienda configurar correctamente el firewall para permitir solamente el tráfico basado en políticas de control de acceso a servicios definidos por TIC, tanto para el tráfico que entra como para el que sale de la red de la SNGR, y además bloquear puertos, servicios y paquetes innecesarios.

- La administración de los servidores se debe realizar de manera remota, sin necesidad de ingresar al Centro de Datos a menos que sea necesario, además es necesario configurar el inicio de sesión de sistemas y servicios críticos con advertencias a los usuarios contra el acceso no autorizado o no autenticado.

- Se recomienda implementar salvaguardas preventivas o controles dependiendo de los niveles de criticidad: “muy alto, alto, medio, bajo y muy bajo” hasta que se implemente el plan de mitigación, esto con el objetivo de minimizar en lo posible la ocurrencia de riesgos de alto impacto.

CAPÍTULO 4

4 CONCLUSIONES Y RECOMENDACIONES

4.1 CONCLUSIONES

Las principales conclusiones obtenidas de este proyecto han sido:

- En la introducción de este trabajo se menciona la necesidad de utilizar metodologías de ethical hacking que permitan descubrir y analizar las vulnerabilidades de los entornos informáticos, y posteriormente proponer medidas que permitan minimizar su riesgo; por lo que el presente proyecto sirve como una aplicación de la metodología de ethical hacking ISSAF en el análisis de riesgos y vulnerabilidades, y que puede ser usada tanto para instituciones públicas como privadas.

- ISSAF es una metodología práctica y factible en el análisis de riesgos y vulnerabilidades que permite convertir entornos informáticos inseguros en entornos protegidos, logrando una clara evaluación de los mismos; en la que se describen técnicas y métodos con distintas herramientas recomendadas por la propia metodología, para cada uno de los casos mencionados en el presente proyecto de titulación, además establece medidas específicas y globales que permitan mitigar los riesgos detectados.

- Se identifica las principales vulnerabilidades de la Infraestructura Tecnológica de la Institución, lo que permite determinar las áreas que requieren mayor atención, el nivel de seguridad en general y los aspectos de seguridad más débiles en relación a los requerimientos de seguridad generales y específicos, y se concluye que no se cuenta con procedimientos de seguridad establecidos o en funcionamiento, por lo cual hay una alta probabilidad de que ocurran riesgos que provoquen un impacto considerable a la institución o que puedan ocasionar consecuencias mencionadas en el plan de mitigación.

- Es imprescindible conocer los riesgos y vulnerabilidades a los que están sometidos las distintas áreas de trabajo, para saber cuán seguros o inseguros están los activos de la institución, y de acuerdo a eso establecer medidas que permitan disminuir el impacto que estas ocasionen a nivel técnico y de negocio.

4.2 RECOMENDACIONES

Las principales recomendaciones de este proyecto son las siguientes:

- Se recomienda la metodología ISSAF, porque contempla métodos estructurados, factibles, ordenados y efectivos, con guías y herramientas recomendadas para la identificación de vulnerabilidades, y con los respectivos análisis de riesgos tanto de criticidad e impacto, que luego permiten determinar las posibles formas de mitigarlos.

- Se debe registrar y documentar información aunque sea parcial de inventarios, de procesos, activos de información, recursos de información, actividades y tareas del personal que maneja los sistemas informáticos, puesto que ello aumenta significativamente la eficiencia y la calidad del análisis al contar con un trabajo previo al presente proyecto.

- Es necesario integrar la información de negocio que tenga relación con la información tecnológica, para así poder determinar lo que es importante y lo que no lo es para el cumplimiento de los objetivos institucionales, y con ello establecer los elementos que son necesarios proteger para asegurar un soporte adecuado al cumplimiento de los objetivos de negocio.

- Un aspecto muy importante para realizar análisis de riesgos y vulnerabilidades es la aplicación minuciosa y completa de la metodología ISSAF, de modo que las técnicas, métodos y criterios empleados sean adecuados y homogéneos, además es importante mantener reuniones de coordinación en las que se traten todos los casos particulares identificados, y que se documenten los criterios seguidos de modo que sean conocidos por el personal de TIC.

- Los resultados del análisis de riesgos debe conocerlos la Dirección de TIC, así como del plan de mitigación de riesgos, con el fin de que sepan que acciones realizar en caso de presentarse incidentes de seguridad y con el propósito de establecer actividades para mitigar o reducir los riesgos detectados con medidas de seguridad necesarias para proteger la información de la Institución.

BIBLIOGRAFÍA

- HERZOG, Peter Vincent. MANUAL DE METODOLOGÍA ABIERTA DE TESTEO DE SEGURIDAD (OSSTMM) 2.1., Institute for Security and Open Methodologies (ISECOM), 23 de Agosto de 2003.

- HERZOG, Peter Vincent. OPEN-SOURSE SECURITY TESTING METHODOLOGY MANUAL (OSSTMM) 2.2., Institute for Security and Open Methodologies (ISECOM), 13 de Diciembre de 2006.

- INFORMATION SYSTEMS SECURITY ASSESSMENT FRAMEWORK (ISSAF) DRAFT 0.2.1, Open Information Systems Security Group (OISSG), 30 de Abril de 2006, http://www.oissg.org/

- HOLGUIN, José Miguel. PENTEST: RECOLECCIÓN DE INFORMACIÓN (INFORMATION GATHERING), Instituto Nacional de Tecnologías de la Comunicación (INTECO), España, http://www.inteco.es/

- BISOGNO, María Victoria. METODOLOGÍA PARA EL ASEGURAMIENTO DE ENTORNOS INFORMATIZADOS, Universidad de Buenos Aires, Argentina, 12 de octubre de 2004 .

- MATALOBOS VEIGA, Juan Manuel. ANÁLISIS DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN, Universidad Politécnica de Madrid, España, Mayo 2009.

- VILLACRES MACHADO, Danny Napoleón. PROPUESTA METODOLÓGICA PARA ASEGURAR REDES INALÁMBRICAS Y SU APLICACIÓN EN LA ESPOCH, Escuela Superior Politécnica de Chimborazo, Riobamba, 2011.

- Ambiente de pruebas de seguridad, http://www.backtrack-linux.org/, junio 2012.

- Guía de referencia de Nmap, http://nmap.org/man/es/, agosto 2012.

- Servicios y números de puerto TCP, http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xml, julio 2012.

- Listado de puertos usados por Troyanos, http://www.seguridadenlared.org/es/index5esp.html, agosto 2012.

- Proyecto colaborativo con recursos y laboratorios de entrenamiento e investigación sobre Seguridad Informática, http://www.sec-track.com/, julio 2012

ANEXOS

ANEXO 1: Módulos del Mapa de Seguridad de OSSTMM versión 2.2

1. Seguridad de la Información
    1. Revisión de la Inteligencia Competitiva
    2. Revisión de Privacidad
    3. Recolección de Documentos
2. Seguridad de los Procesos
    1. Testeo de Solicitud
    2. Testeo de Sugerencia Dirigida
    3. Testeo de las Personas Confiables
3. Seguridad en las tecnologías de Internet
    1. Logística y Controles
    2. Sondeo de Red
    3. Identificación de los Servicios de Sistemas
    4. Búsqueda de Información Competitiva
    5. Revisión de Privacidad
    6. Obtención de Documentos
    7. Búsqueda y Verificación de Vulnerabilidades
    8. Testeo de Aplicaciones de Internet
    9. Enrutamiento
    10. Testeo de Sistemas Confiados
    11. Testeo de Control de Acceso
    12. Testeo de Sistema de Detección de Intrusos
    13. Testeo de Medidas de Contingencia
    14. Descifrado de Contraseña
    15. Testeo de Denegación de Servicios
    16. Evaluación de Políticas de Seguridad

4. Seguridad en las Comunicaciones
    1. Testeo de Private Branch Exchange (PBX)
    2. Testeo del Correo de Voz
    3. Revisión del FAX
    4. Testeo del Modem
5. Seguridad Inalámbrica
    1. Verificación de Radiación Electromagnética
    2. Verificación de Redes Inalámbricas [802.11]
    3. Verificación de Redes Bluetooth
    4. Verificación de Dispositivos de Entrada Inalámbricos
    5. Verificación de Dispositivos de Mano Inalámbricos
    6. Verificación de Comunicaciones sin Cable
    7. Verificación de Dispositivos de Vigilancia Inalámbricos
    8. Verificación de Dispositivos de Transacción Inalámbricos
    9. Verificación de Identificación por Radiofrecuencia
    10. Verificación de Sistemas Infrarrojos
    11. Revisión de Privacidad
6. Seguridad Física
    1. Revisión de Perímetro
    2. Revisión de Monitoreo
    3. Evaluación de Controles de Acceso
    4. Revisión de Respuesta de Alarmas
    5. Revisión de Ubicación
    6. Revisión de Entorno

ANEXO 2: Entidades de Evaluación de ISSAF versión 0.2.1

- Recopilación de Información
- Mapeo de Red
- Seguridad en las Contraseñas
- Seguridad de los Switch
- Seguridad del Router
- Seguridad del Firewall
- Seguridad del Sistema de Deteción de Intrusos
- Seguridad en la Red Privada Virtual (VPN)
- Seguridad del Sistema Anti-Virus
- Seguridad en la Red de Área de Almacenamiento (SAN)
- Seguridad en la Red Inalámbrica (WLAN)
- Seguridad de los Usuarios de Internet
- Seguridad AS/400
- Seguridad Lotus Notes
- Seguridad del Servidor Web
- Seguridad de Aplicaciones Web
- Seguridad en Sistemas UNIX y GNU/Linux
- Seguridad en Sistemas Windows
- Seguridad Novell Netware
- Seguridad de las Bases de Datos
- Seguridad Física
- Ingeniería Social

ANEXO 3: Registro de números de Puerto TPC y UDP

# Puerto	TCP	UDP	Descripción	Estatus
1	x	x	TCP Puerto de Servicio Multiplexer (TCPMUX)	Oficial
11	x	x	Usuarios activos (systat service)	Oficial
15	x	x	Previously netstat service	No Oficial
21	x		FTP control	Oficial
53	x	x	Domain Name System (DNS)	Oficial
79	x		Finger Protocol	Oficial
80	x		Hypertext Transfer Protocol (HTTP)	Oficial
111	x	x	ONC RPC (Sun RPC)	Oficial
119	x		Network News Transfer Protocol (NNTP)	Oficial
143	x		Internet Message Access Protocol (IMAP)	Oficial
540	x		UUCP (Unix-to-Unix Copy Protocol)	Oficial
635	x	x	RLZ DBase	Oficial
1080	x		SOCKS proxy	Oficial
1524	x	x	ingreslock, ingres	Oficial
2000	x	x	Cisco SCCP (Skinny)	Oficial
3128	x		Web caches and the default for the Squid (software)	No Oficial
3128	x		Tatsoft default client connection	No Oficial
5742	x	x	IDA Discover Port 2	Oficial
6665–6669	x		Internet Relay Chat (IRC)	Oficial
12345			NetBus – herramienta de administración remota (por Trojanos). También usado por NetBuster. Little Fighter 2	No Oficial
22222	x		Davis Instruments, WeatherLink IP	No Oficial
27500-27900		x	id Software's QuakeWorld	No Oficial
31337	x		Back Orifice - herramienta de administración remota (usado por Trojanos)	No Oficial

ANEXO 4: Puertos usados por Troyanos

# Puerto	Troyanos
1	(UDP) Sockets des Troie
15	B2
21	Back Construction, Blade Runner, Cattivik FTP Server, CC Invader, Dark FTP, Doly Trojan, Fore, FreddyK, Invisible FTP, Juggernaut 42, Larva, MotIv FTP, Net Administrator, Ramen, RTB 666, Senna Spy FTP server, The Flu, Traitor 21, WebEx, WinCrash
53	ADM worm, Lion
79	CDK, Firehotcker
80	711 trojan (Seven Eleven), AckCmd, Back End, Back Orifice 2000 Plug-Ins, Cafeini, CGI Backdoor, Executor, God Message, God Message 4 Creator, Hooker, IISworm, MTX, NCX, Noob, Ramen, Reverse WWW Tunnel Backdoor, RingZero, RTB 666, Seeker, WAN Remote, Web Server CT, WebDownloader
119	Happy99
1080	SubSeven 2.2, WinHole
1524	Trinoo
2000	Der Späher / Der Spaeher, Insane Network, Last 2000, Remote Explorer 2000, Senna Spy Trojan Generator
3128	Reverse WWW Tunnel Backdoor, RingZero
5742	WinCrash
6667	Dark FTP, EGO, Maniac rootkit, Moses, ScheduleAgent, SubSeven, Subseven 2.1.4 DefCon 8, The Thing (modified), Trinity, WinSatan
11000	Senna Spy Trojan Generator
12345	Adore sshd, Ashley, cron / crontab, Fat Bitch trojan, GabanBus, icmp_client.c, icmp_pipe.c, Mypic, NetBus, NetBus Toy, NetBus worm, Pie Bill Gates, ValvNet, Whack Job, X-bill
12346	Fat Bitch trojan, GabanBus, NetBus, X-bill
20034	NetBus 2.0 Pro, NetBus 2.0 Pro Hidden, NetRex, Whack Jobz
22222	Donald Dick, Prosiak, Ruler, RUX The TIc.K
27665	Trinoo
31337	Back Orifice, Deep BO
40421	Agent 40421, Masters Paradise
54320	Back Orifice 2000

ANEXO 5: Vulnerabilidades de la SNGR

Entidad de Evaluación	***Vulnerabilidades***
Recopilación de Información	Muestra detalles de la dirección IP publica
	Nombres de Dominio relacionadas a IP's publicas
	Nombres de Dominio relacionadas a IP's internas
	Muestra versión instalada del BIND
Mapeo de Red	Respuestas ICMP de Servidores
	Puertos abiertos en los servidores DNS, Correo y HTTP
	Servidores muestran versión de servicios activos y del Sistema Operativo
	Detalles perímetro de RED
	El Firewall también es el servidor DNS
Seguridad del Router	Router muestra puertos abiertos y servicios activos
	Router muestra versión del Sistema Operativo
	Router tiene protocolos de enrutamiento estático
Seguridad del Firewall	Firewall muestra puertos abiertos y servicios activos
	Firewall presenta puertos con servicios utilizados por la Dirección de TIC
	Firewall presenta puertos abiertos no establecidos por la Dirección de TIC
	Firewall tiene pocas reglas de filtrado
	Firewall presenta puertos que pueden ser usados por troyanos
Seguridad del IDS	HIDS Instalado
	NIDS Instalado
Seguridad del Sistema Anti-Virus	Anti-virus no esta instalado en el Firewall
Seguridad SAN	La Información no se respalda continuamente
Seguridad del Servidor Web	Acceso al servidor desde cualquier dirección IP
	Servidor Web tiene habilitada la exploración de directorios
	Servidor Web no tiene balanceo de carga
Seguridad de las Aplicaciones Web	Portal web muestra versión del Apache
	Portal web muestra correos electrónicos
	Portal web muestra CMS instalado y su versión

	Portal web muestra versión del PHP
	Joomla! no tiene anti-escaner
Seguridad de las Aplicaciones Web	No hay protección ante el envío de correos automáticos
	Inicio de sección insegura para el administrador
	Portal web no tiene WAF
Seguridad de los Usuarios de Internet	Revelación de direcciones IP por parte del usuario
	Instalación de IRC's no permitidos
	Transferencia de código malicioso
	Instalación de aplicaciones P2P no permitidas
	Usuarios víctimas de correo no deseado
Seguridad Física	No hay guardias de Seguridad
	No hay control ni supervisión del PACS
	No hay CCTV