METODOLOGÍA PARA EL DIAGNÓSTICO CONTINUO DE LA SEGURIDAD INFORMÁTICA DE LA RED DE DATOS DE LA UNIVERSIDAD MILITAR NUEVA GRANADA

JUAN SEBASTIAN ECHEVERRY PARADA
CÓDIGO: 1400173

UNIVERSIDAD MILITAR NUEVA GRANADA
FACULTAD DE INGENIERÍA
PROGRAMA DE INGENIERÍA EN TELECOMUNICACIONES
BOGOTÁ, D.C. MAYO 2009.

METODOLOGÍA PARA EL DIAGNÓSTICO CONTINUO DE LA SEGURIDAD INFORMÁTICA DE LA RED DE DATOS DE LA UNIVERSIDAD MILITAR NUEVA GRANADA

JUAN SEBASTIAN ECHEVERRY PARADA
CÓDIGO: 1400173

Trabajo de Auxiliar de Investigación presentado como requisito para optar por el título de Ingeniero en Telecomunicaciones

Director

Ing. EDWARD PAUL GUILLEN PINTO, M. Sc.

UNIVERSIDAD MILITAR NUEVA GRANADA
FACULTAD DE INGENIERÍA
PROGRAMA DE INGENIERÍA EN TELECOMUNICACIONES
BOGOTÁ, D.C. MAYO 2009.

Nota de aceptación

_____

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Bogotá, D.C., _____

Dedico todo mi esfuerzo realizado en el desarrollo de mi vida académica a mis padres Carlos y Rosa.

Juan Sebastian

AGRADECIMIENTOS

Este trabajo de investigación hace parte importante de mi vida, por esto le agradezco a Dios y, en especial, a mis padres por todo el apoyo y el aliento dado en los momentos que mi ánimo decaía, también por la oportunidad que me dieron de estudiar a pesar de los sacrificios hechos por mi desarrollo académico. También estoy agradecido con mis hermanos por acompañarme incondicionalmente durante todos estos años y por confiar en mí.

Le agradezco a mi Director de tesis, el Ingeniero Edward Paul Guillén, por su asesoramiento y orientación para la elaboración de este trabajo.

Gracias a los funcionarios de la División de Informática de la universidad por toda su colaboración y apoyo, en especial a los Ingenieros Weimar Santos y Mario Castro por su paciencia y orientación.

A la Universidad Militar Nueva Granada y al ITEC porque por medio de sus educadores me brindaron un sin número de conocimientos para mi desarrollo académico.

A mis compañeros y amigos porque durante todos estos años de estudios fueron de gran ayuda en el aprendizaje de nuevos conocimientos.

TABLA DE CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

LISTA DE ANEXOS

1. INTRODUCCIÓN

Debido a la necesidad de mantener la información privada fuera del alcance de personas ajenas a la organización, los responsables de la administración de la red utilizan herramientas y prácticas que aseguren al máximo la información. Dentro de las prácticas recomendadas está la ejecución de evaluaciones de seguridad de la red informática, permitiendo identificar las vulnerabilidades dentro de la red, para luego clasificarlas según su grado de criticidad, y buscar la solución que mejor se adapte a los requerimientos de la organización. Una forma óptima de realizar esas tareas de evaluación es seguir una metodología, que defina unos pasos ordenados para tal fin, evitando que durante el proceso de evaluación se obvien aspectos importantes de la seguridad. La metodología para el diagnóstico de la seguridad de una red informática es un conjunto de pasos ordenados que se ponen en práctica para identificar los problemas de seguridad dentro de la red informática; pasos que permitirán ejecutar una evaluación de seguridad ordenada y lo más completa posible.

El trabajo se desarrolló al interior del Grupo de Investigación en Seguridad y Sistemas de Comunicaciones (GISSIC) del programa de Ingeniería en Telecomunicaciones de la Universidad Militar Nueva Granada, el cual está compuesto por los semilleros Enigma y Claude Shanon, para seguridad en comunicaciones y procesamiento de señales respectivamente, con el fin de desarrollar, implementar y proponer sistemas y metodologías para el desarrollo de los sistemas de seguridad y de comunicaciones con aplicabilidad local y globalizada. En conjunto con la División Informática de la Universidad Militar Nueva Granada, quienes están a cargo de los recursos informáticos dispuestos para los procesos académicos y administrativos y en

gran parte, los directos responsables del sistema de información de la institución.

El trabajo consiste en definir una metodología para diagnosticar el estado de la seguridad informática de la red de datos de la Universidad, de acuerdo con los resultados de ejecutar una evaluación del riesgo a la red de datos, lo que permite identificar cuales son las áreas con mayor grado de criticidad y donde se debe hacer énfasis en el diagnóstico. El diagnóstico de la seguridad se lleva a cabo con la ejecución de unas tareas, que son realizadas con la utilización de aplicaciones de seguridad, en su gran mayoría software libre, y que a la vez quedan propuestas dentro de la metodología como una opción para ejecutar el diagnóstico. La metodología propuesta genera unos resultados que son los reportes del diagnóstico, que muestran cuales son los problemas de seguridad encontrados, y un documento con propuestas para la solución de dichos problemas, teniendo en cuenta los requerimientos de la División Informática.

Este trabajo surgió por la necesidad de la División Informática de identificar los problemas de seguridad de su red de datos, para de esta forma comenzar a definir las políticas de seguridad de la División, que con los resultados de la implementación de la Metodología tienen el primer paso para comenzar a establecer las políticas de seguridad que aplicarán para la red de datos de la Universidad. Para el grupo de investigación GISSIC el presente trabajo es importante en cuanto ofrece un aporte en las áreas de *Ethical Hacking* (Hacking ético) y políticas de seguridad, ésto debido a que el presente trabajo, en términos generales, consiste en utilizar técnicas de penetración para evaluar la seguridad de la red de datos, y con sus resultados ayudar en la definición de políticas de seguridad para la red de datos de la Universidad.

El libro se encuentra dividido en cinco capítulos, donde el primer capítulo presenta la parte introductoria del trabajo elaborado, aquí se ofrece una breve descripción del título del trabajo, las necesidades que llevaron a

desarrollar el trabajo junto con los objetivos a cumplir para completarlo. El segundo capítulo es el marco teórico, donde se definen los conceptos más relevantes utilizados para la realización de este trabajo. El tercer capítulo contempla la ingeniería del proyecto, donde se hace un análisis de las variables de ingeniería. El desarrollo del trabajo se detalla en el cuarto capítulo. Y por último se encuentra el quinto capítulo que expone las conclusiones obtenidas durante el desarrollo del trabajo y las recomendaciones.

1.1. TÍTULO

El trabajo consiste en implementar una metodología que permita diagnosticar el estado en el que se encuentra la red cableada y no cableada de la Universidad en cuanto a la seguridad informática. Para la implementación de la metodología se tomarán como base las ya existentes; sobre ellas se partirá para elaborar la metodología a implementar. Por lo anterior el trabajo se ha titulado “Metodología para el diagnóstico continuo de la seguridad informática de la red de datos de la Universidad Militar Nueva Granada”.

1.2. PLANTEAMIENTO DEL PROBLEMA

La División Informática de la Universidad Militar Nueva Granada es la encargada de la administración de la red de datos de la institución, y dentro de esa administración está la seguridad informática de la red. Debido a la ausencia de una política de seguridad organizada se llegó a la necesidad de comenzar un proceso para establecerlas dentro de la División. Como primer paso se planteó, por ellos, la necesidad de desarrollar un trabajo que permitiera diagnosticar el estado de la seguridad de la red de datos, y con su resultado tener conocimiento de los aspectos en que se debe trabajar para definir una política de seguridad organizada y precisa con los requerimientos

de la red. El grupo de investigación GISSIC teniendo en cuenta la necesidad de la División Informática, planteó la necesidad de trabajar en una metodología, que mediante un conjunto de tareas de evaluación, permitiera diagnosticar el estado de la seguridad de la red de datos de la Universidad.

Para implementar una metodología en la Universidad se deben estudiar los estándares y metodologías referentes a evaluaciones de seguridad, para tenerlas en cuenta como base para la definición de la metodología. Con el propósito de elaborar esta metodología, que esté acorde a la red de la Universidad se debe estudiar su estructura, y así identificar los servicios y procesos que se ejecutan en la red, además de los sistemas presentes. Una vez estudiadas las variables anteriores se deben identificar los riesgos a que está expuesta la red.

1.3. OBJETIVOS

Para el desarrollo del trabajo se plantea un objetivo general que representa el resultado final, y unos objetivos específicos que representan los pasos a seguir para llegar al resultado final, que es la implementación de una metodología para el diagnóstico de la seguridad en la Universidad.

1.3.1. Objetivo general

Realizar un estudio de ingeniería para la implementación de una metodología para el diagnóstico de la seguridad informática de la red de datos de la Universidad Militar Nueva Granada, que pueda ser usado continuamente.

1.3.2. Objetivos específicos

- Realizar una evaluación de riesgos para la seguridad informática de la red de la Universidad.
- Diseñar la metodología de acuerdo con una evaluación de riesgos.

- Comprobar la efectividad de la metodología propuesta mediante el diagnóstico de la seguridad de la red de datos de la Universidad.
- Presentar un reporte que indiquen las debilidades que presenten un mayor grado de criticidad.
- Elaborar una propuesta con la mejor solución a las debilidades encontradas durante el diagnóstico.

1.4. ANTECEDENTES

A comienzos del año 2007 se publicó el trabajo de investigación titulado "Diseño de metodología para el diagnóstico de seguridad a las redes de datos de ETECSA", desarrollado por el Ingeniero Alexander López Gavilán para la empresa cubana ETECSA (Empresa de Telecomunicaciones de Cuba), quien presta servicios públicos de telecomunicaciones en todo el territorio de la república de Cuba. Este trabajo propone una metodología partiendo de un estudio de las ya existentes y de las herramientas de seguridad utilizadas por estas para realizar un diagnóstico de seguridad. El propósito de la metodología es ayudar a especialistas no experimentados y a expertos a obtener resultados eficientes y confiables a la hora de realizar diagnósticos de seguridad a las redes, los servicios y las aplicaciones. [1]

En la Universidad Militar Nueva Granada la Ingeniera Jenny Catherine Ortiz, estudiante de Ingeniería en Telecomunicaciones en la institución, en el primer semestre del año 2006 presentó la monografía titulada "Metodología para la detección y erradicación de ataques Web - *data tampering & SQL injection* - en los procesos de la página de la Universidad Militar Nueva Granada", como trabajo para la obtención del grado de Ingeniera. Esta metodología fue elaborada con el fin de detectar y erradicar los ataques informáticos conocidos como data tampering y SQL injection en los diferentes

procesos manejados en la página Web, tales como correo electrónico, carga académica y consulta de notas, de la Universidad Militar Nueva Granada. [2]

En enero de 2005 el *Information Security Forum* (ISF) – Foro de Seguridad de la Información publicó el "The Standard of Good Practice for Information Security", que en español significa "El Estándar de Buenas Prácticas para la Seguridad de la Información" para ayudar a cualquier organización a mantener los riesgos del negocio asociados con sus sistemas de información dentro de unos límites aceptables mediante una serie de controles que permiten verificar el estado de la seguridad en los sistemas de información. El ISF es una asociación internacional de más de 260 organizaciones líderes que financian y cooperan en el desarrollo de un programa de investigación práctico en seguridad de la información. [3]

El día 29 de septiembre de 2004 Gregory Braunton publicó su trabajo titulado "B.A.S.E. A Security Assessment Methodology" para el instituto SANS (SysAdmin, Audit, Network, Security). BASE es un protocolo de evaluación de seguridad de la información elaborado por SANS (SysAdmin, Audit, Network, Security), orientado a organizaciones no muy grandes. SANS es un instituto, fundado en 1989, que se dedica a la investigación y educación en el campo de la Seguridad de la Información. Se encarga también de entrenar y certificar, además de desarrollar investigaciones que están disponibles, en su mayoría, sin ningún costo. Esta metodología propone y prácticamente aplica el protocolo de evaluación BASE, cuyas siglas hacen referencia a las palabras en inglés Baseline, Audit and Assess, Secure, Evaluate and Educate. BASE enmarca un protocolo básico de evaluación de vulnerabilidades para el Aseguramiento de la Información, que también incluye el uso de herramientas sin costos. Todo esto con el fin de proporcionar una metodología para evaluar la seguridad de la información que sea económica y ejecutable por todos, desde un usuario doméstico hasta un ingeniero de seguridad en una empresa. La metodología se divide

en cuatro fases: Baseline, Audit and Assess, Secure, Evaluate and Educate. El proceso de evaluación que se plantea con estas fases comienza desde la documentación de los procesos, servicios, configuraciones y sistemas que serán objeto de la evaluación, pasando por una evaluación de vulnerabilidades, con ayuda de herramientas libres. Luego se ejecuta un plan de corrección de las áreas potencialmente vulnerables, y el paso final, se evalúa la ejecución de la seguridad y asegura que las necesidades funcionales del negocio no se hayan afectado con su ejecución. [4]

Durante el día jueves, 13 de diciembre de 2006 se publicó la última versión del “Manual de la Metodología Abierta de Testeo de Seguridad” OSSTMM 2.2 - Open Source Security Testing Methodology Manual, cuya versión original fue entregada el lunes, 18 de diciembre de 2000. El OSSTMM es un trabajo realizado por el Instituto para la Seguridad y Metodologías Abiertas (ISECOM), que comenzó en enero de 2001 en Estados Unidos y España. ISECOM se dedica a la investigación, certificación, entrenamiento e integridad de los negocios, en el campo de la seguridad práctica. El OSSTMM es una metodología para realizar pruebas de seguridad, las cuales se dividen en cinco secciones que hacen referencia a: controles para información y datos, niveles para seguridad atada al personal, niveles de control para ingeniería social y fraude, computadores y redes de telecomunicaciones, dispositivos inalámbricos, dispositivos móviles, controles de acceso para seguridad física, seguridad de procesos, y localizaciones físicas tales como edificios, perímetros y zonas desmilitarizadas. El OSSTMM presenta un enfoque principal sobre que debe hacer un auditor de seguridad. [5]

2. MARCO TEÓRICO

Para el mejor entendimiento del trabajo de investigación se presenta en este capítulo los conceptos más relevantes. Éstos se encuentran separados en dos grupos los conceptos generales que se enmarcan dentro del área de la investigación, y los conceptos específicos.

2.1. MARCO TEÓRICO CONCEPTUAL

A continuación se explican conceptos generales que hacen referencia al trabajo de investigación y que buscan aclaran los conceptos más relevantes.

2.1.1. Red de datos

Una red de datos es un conjunto de elementos que permiten conectar dos o más computadoras con el fin de intercambiar datos entre ellas. En la figura 1 se muestra una configuración típica de una red de datos. Esos elementos se pueden dividir en tres categorías: software, hardware y protocolo.

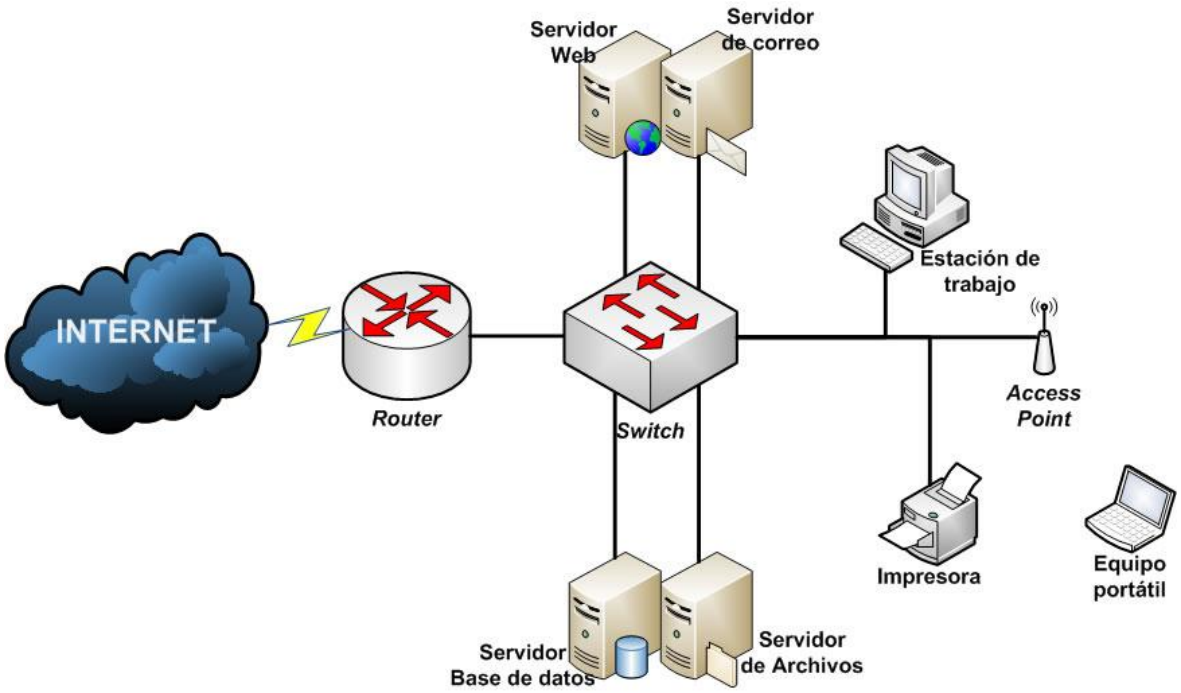

Figura 1 Configuración básica de red

- Software: son todos los programas informáticos que permiten a los usuarios de la red comunicarse para compartir información, como imágenes, documentos u otros archivos, y para utilizar los recursos de la red, que pueden ser impresoras o discos duros. También permite la fácil administración de la red y de los sistemas en ella.

- Hardware: son todos aquellos elementos físicos que pertenecen a la red y los cuales permiten hacer uso de los recursos de ésta (Ej. estaciones de trabajo), así como también permiten comunicar a todos los equipos (Ej. conmutadores). Algunos equipos de gran importancia presentes en una red son los servidores, en una red se tiene básicamente lo que son los servidores Web, de correo, de base de datos y de archivos de acuerdo a los requerimientos de la organización.

- Protocolo: es el conjunto de normas o reglas establecidas para llevar a cabo el intercambio de datos entre equipos que conforman una

red. Dentro de los protocolos utilizados en una red están: TCP, IP, SNMP, FTP, Telnet y HTTP.

2.1.2. Seguridad informática

Para dar una definición clara de Seguridad Informática se deben definir primero sus dos palabras por separado:

- Seguridad: garantía de que un sistema esta libre de cualquier peligro o amenaza, que afecte su disponibilidad, integridad y confiabilidad.
- Informática: conjunto de conocimientos sistematizados y técnicas que hacen posible el tratamiento automático y racional de la información, mediante el uso de herramientas computacionales.

Dados los conceptos de las palabras Seguridad e Informática, se puede decir que Seguridad Informática es la garantía de que los procesos llevados a cabo para el tratamiento de la información se mantengan aislados, en lo posible, de las amenazas que puedan afectar la integridad, disponibilidad y confiabilidad de la información.

Para mantener un sistema informático seguro, se debe tener en cuenta los principios básicos de la seguridad informática, los cuales son:

- Integridad: es la garantía de que la información no puede ser alterada antes, durante ni después del proceso de transmisión.
- Confidencialidad: es garantizar que la información no puede ser conocida por personas no autorizadas para ello.
- Disponibilidad: asegurar que se puede tener acceso a la información cuando se requiera.

2.1.3. Evaluación de la seguridad informática

La evaluación de seguridad es el proceso en el que se examina el estado de la seguridad de una red informática, mediante la realización de pruebas a los sistemas y procesos de una red, en busca de vulnerabilidades y debilidades

que comprometan la integridad de ésta. En términos generales el proceso de evaluación de la seguridad sigue las siguientes fases:

- Recopilación de la información: En esta fase el evaluador recoge información para tener conocimiento del sistema. Dentro de esta fase se maneja los conceptos de caja negra, gris y blanca, que tienen relación con el conocimiento previo del entorno en el que se realizará la evaluación.
    - Caja blanca: al evaluador se le suministra conocimiento total del entorno a ser evaluado.
    - Caja gris: al evaluador se le suministra algún conocimiento del entorno a ser evaluado.
    - Caja negra: al evaluador no se le suministra conocimiento del entorno a ser evaluado.
- Análisis de vulnerabilidades: Detección, comprobación y evaluación de las vulnerabilidades presentes en el sistema.
- Finalización: La evaluación finaliza con el análisis de los resultados y la elaboración del reporte de la evaluación, que contiene los problemas de seguridad encontrados y las recomendaciones para solucionarlos.

2.1.4. Amenazas informáticas

Una amenaza es un evento o suceso desfavorable que requiere de una oportunidad para que cause una violación en la seguridad de un sistema de información. Dentro de un análisis de riesgos donde se intenta encontrar las amenazas que pueden repercutir en la confidencialidad, disponibilidad e integridad del activo en las actividades de una organización busca responder a las preguntas ¿qué se intenta evitar? o ¿qué se teme que le suceda al activo?, haciendo más fácil la identificación de las amenazas. También es

buena práctica apoyarse en los estándares de seguridad informática para la investigación de las amenazas, ya que ellos dan una visión clara de que puede ser una amenaza a los sistemas de información. La **ISO/IEC 27002** es un claro ejemplo de norma que se puede tener en cuenta para la identificación de amenazas, ya que los controles definidos en ella están basados en las amenazas que pueden afectar un sistema de información.

2.1.5. Vulnerabilidades

Una vulnerabilidad es el grado de debilidad presente en un sistema informático o activo que define que tan susceptible puede ser frente a una o varias amenazas. Estas debilidades pueden deberse a procedimientos de seguridad mal definidos, errores de programación en las aplicaciones, sistemas operativos con actualizaciones de seguridad pendientes, edificaciones inestables y/o con brechas de seguridad, entre otros. Las vulnerabilidades varían o surgen con el tiempo en la medida que los errores de programación se detectan, o se hacen modificaciones a las aplicaciones, o las instalaciones físicas se cambian, o en el peor de los casos se es víctima de un ataque informático debido a una brecha de seguridad no descubierta o no publicada a tiempo por los profesionales en seguridad. Para identificar las vulnerabilidades se cuenta con diversas herramientas, entre las que están los analizadores de vulnerabilidades como Nessus, base de datos de vulnerabilidades publicadas en Internet como secunia.com, y las normas y guías de seguridad en conjunto con el análisis de las instalaciones físicas de los equipos.

2.1.6. ISO/IEC 27001 – Information security management systems (Sistema de administración de la seguridad de la información)

ISO/IEC 27001 es un estándar para la seguridad informática publicado por la Organización Internacional para la Normalización (ISO) y por la Comisión Electrotécnica Internacional (IEC) durante el año 2005. Esta norma busca establecer los requerimientos necesarios para establecer, implementar,

operar, revisar, monitorear, mantener y mejorar el sistema de administración de la seguridad dentro del contexto de los riesgos de la organización. La norma especifica los requerimientos para la implementación de controles de seguridad y está diseñada para asegurar la selección de éstos de una forma adecuada. Para la aplicación de esta norma se requiere tener en cuenta la ISO/IEC 17799:2005 ahora llamada ISO/IEC 27002. [6]

2.1.7. Trusted Computer System Evaluation Criteria (TSEC) (Criterios confiados para la evaluación del sistema informático)

El TSEC es un estándar del Departamento de Defensa de los Estados Unidos y que es más conocido como el *Orange Book* – Libro naranja. El TSEC define cuatro divisiones jerárquicas de seguridad para protección de la información: D, C, B y A, donde la división A representa el nivel más alto de confiabilidad que puede implementarse en un sistema de información. Cada división está constituida por una o más clases, y las cuales definen un grupo de criterios que debe cubrir un sistema. La definición de los criterios parte de seis requerimientos fundamentales para la seguridad informática, donde cuatro tratan acerca de que es necesario proveerse para controlar el acceso a la información; y los dos restantes tratan acerca de cómo puede obtenerse una garantía creíble lograda en un sistema informático confiable.

- Políticas de seguridad: Debe existir una política de seguridad explicita y bien definida respetada por el sistema.
- Marcas: De acuerdo a unas reglas de una política de seguridad obligatoria, debe ser posible marcar cada objeto con una etiqueta que de forma confiable identifique el nivel de la sensibilidad del objeto y/o los modos de acceso acordados a los individuos que pueden potencialmente acceder los objetos.
- Identificación: Cada acceso a la información debe ser registrado basado en quien accede a la información y que clase de información ellos están autorizados a tratar. Dichos registros deben ser

mantenidos de forma segura por los sistemas informáticos y ser asociado con cada elemento activo que ejecuta una acción relevante en el sistema.

- Responsabilidad: La información de auditorias debe ser selectivamente guardadas y protegidas de modos que las acciones que afecten la seguridad puedan trazar al responsable.
- Aseguramiento: Los sistemas informáticos deben contener mecanismos de hardware y software que puedan suministrar suficiente seguridad al sistema, para cumplir con los cuatro requerimientos iniciales.
- Protección continua: Los mecanismos confiados que hacen cumplir los requerimientos de seguridad deben ser protegidos contra cambios no autorizados.

Estos criterios fueron desarrollados buscando cumplir tres objetivos: (a) proveer al usuario un criterio con el cual determinar el grado de confianza que se puede tener en los sistemas informáticos para el proceso de aseguramiento de información clasificada o sensible; (b) proporcionar una estándar a los fabricantes en cuanto a que características de seguridad tener en cuenta al fabricar sus nuevos productos comerciales y satisfacer los requerimientos de seguridad para las aplicaciones sensibles; y (c) proporcionar una base para especificar requerimientos de seguridad en especificaciones de la adquisición. A continuación se ofrece una breve descripción de las cuatros divisiones:

- División D – Protección Mínima: Contiene una sola clase, que se reserva para los sistemas evaluados, pero que no logran satisfacer las exigencias para una clase de evaluación más alta.
- División C – Protección Discrecional: Define dos clases para el aseguramiento de la protección discrecional, a través de la inclusión

de las capacidades de auditoría, responsabilidad de los temas y acciones que ellas inician. La primera clase se refiere a la separación de los usuarios y los datos incorporando algunos controles capaces de hacer cumplir las limitaciones de acceso. La segunda clase hace cumplir los controles de acceso discrecional, responsabilizando a los usuarios de sus acciones a través de procedimientos de conexión, auditorias de los eventos de seguridad relevantes y aislamiento de recursos.

- División B – Protección Obligatoria: Los sistemas en esta división deben tener las etiquetas de sensibilidad en las estructuras de datos importantes del sistema con el fin de hacer cumplir un conjunto de reglas obligatorias del control de acceso.
- División A – Protección Verificada: utiliza métodos formales para la verificación de la seguridad para asegurar que los controles discrecionales y obligatorios pueden proteger efectivamente la información clasificada y sensible. [7]

2.1.8. Control Objectives for Information and Related Technology (COBIT) (Objetivos de control para la información y la tecnología relacionada)

COBIT es un trabajo elaborado por ISACA (Information Systems Audit and Control Association), que es una organización global que establece las pautas para los profesionales de gobernación, control, seguridad y auditoría de información. COBIT brinda buenas prácticas a través de un marco de trabajo de dominios y procesos, y presenta las actividades en una estructura manejable y lógica. Las buenas prácticas están enfocadas fuertemente en el control y menos en la ejecución. Estas prácticas ayudan a optimizar las inversiones facilitadas por la TI, asegurarán la entrega del servicio y brindan una medida contra la cual juzgar cuando las cosas no vayan bien. [8]

2.1.9. The Standard of Good Practice for Information Security (El Estándar de Buenas Prácticas para la Seguridad de la Información)

El Estándar representa una gran ayuda para las organizaciones que quieren conocer como se encuentra la seguridad en su sistema de información o para aquellas que quieren saber que es lo que deben hacer en cuanto a la seguridad de su sistema de información. El Estándar está dividido en cinco grandes aspectos, y en cada uno de ellos se tratan unas áreas específicas que a la vez agrupa dentro de una secciones las buenas prácticas. Las buenas prácticas son unos controles de seguridad para ser aplicados en el sistema de información y de esta forma asegurar la información y los sistemas. A continuación se ofrece una breve descripción de cada uno de los cinco aspectos en que se divide el Estándar:

- Administración de la seguridad: su finalidad es mantener bajo control los riesgos del negocio asociados al sistema de información. Plantea un tratamiento de la seguridad desde el órgano administrativo de la empresa, estableciendo unos controles que permitan una adecuada asignación de los recursos, arreglos efectivos para promover una buena práctica de la seguridad de la información y establecer un ambiente seguro.

- Aplicaciones críticas del negocio: las aplicaciones del negocio se tratan como las más críticas debido a que son las destinadas para manejar la información confidencial de la empresa, por eso requieren de controles más estrictos que las demás aplicaciones. Éste aspecto provee unas buenas bases para identificar los riesgos del negocio y determinar el nivel de protección requerido para mantener los riesgos dentro de límites aceptables.

- Instalaciones de computadores: establece controles para mantener una buena administración de las instalaciones en los computadores de la empresa, independiente de donde la información se procesa.

- Redes: Debido a que las redes son un canal de acceso a los sistemas de información, son claros objetivos para ser abusados y por lo tanto se trata como un aspecto, por ser un elemento crítico en la seguridad. En este aspecto se trabaja en las áreas de administración de la red, definiendo controles acerca de los roles en la administración, el diseño, documentación y otros. Otra área tiene relación con la administración del tráfico, donde un punto importante son los controles para los *firewalls* y los controles de acceso tanto externo como para red inalámbrica.
- Desarrollo de sistemas: se enfoca en los controles a tener en cuenta durante el desarrollo de los sistemas de información, como las prácticas a realizar para implementar un sistema seguro y bien estructurado, partiendo de los requerimientos del negocio. Además presenta controles para probar todo los elementos del sistema antes de poner en funcionamiento los sistemas. [3]

2.1.10. Open Source Security Testing Methodology Manual (OSSTMM) (Manual de la Metodología Abierta de Testeo de Seguridad)

El OSSTMM es un trabajo realizado por el Instituto para la Seguridad y Metodologías Abiertas (ISECOM). ISECOM se dedica a la investigación, certificación, entrenamiento e integridad de los negocios, en el campo de la seguridad práctica. El OSSTMM es una metodología diseñada para realizar pruebas de seguridad, que se encuentra dividida por secciones, módulos y tareas. En cada sección se trata un área que conforma el sistema de información de una organización. El OSSTMM propone en cada sección la ejecución de unas tareas con el fin de encontrar la existencia de problemas que afecten en gran medida la seguridad de una organización.

2.1.11. B.A.S.E. – A Security Assesment Methodology (B.A.S.E. – Metodología para la evaluación de la seguridad)

La metodología para la evaluación de la seguridad B.A.S.E. de SANS fue preparada por su grupo GSEC para el año 2004. Esta metodología fue propuesta para organizaciones no muy grandes, que no requieran de un esfuerzo muy grande para la evaluación de todos sus sistemas de información. Está orientado tanto para organizaciones medianas como para redes domésticas. La metodología se divide en cuatro fases fundamentales, basadas en el protocolo de evolución llamado B.A.S.E., cuyas iniciales indican las distintas fases: ***B****aseline*, ***A****udit and Assess*, ***S****ecure the environment*, y ***E****valuate and Educate*. Cada una de las fases se describe a continuación:

- Baseline: Control de cambios. Paso en el que se documentan todos los procesos, servicios, configuraciones de hardware, aplicaciones instaladas, funciones de las aplicaciones y del personal, y demás componentes que hacen parte del funcionamiento de la red. Proceso esencial para la solución de problemas y recuperación de desastres.

- Audit and Assess: en este paso se llevan a cabo dos procesos, auditoría y evaluación. Para la auditoría se puede utilizar tareas manuales y herramientas automatizadas. Este proceso se planea y ejecuta de acuerdo a lo establecido en el Baseline. Lo siguiente a la auditoría es la evaluación de los resultados de ésta en términos de configuraciones técnicas y necesidades del negocio. Lo anterior sirve para identificar que medidas son necesarias. Cuando la seguridad interviene en las necesidades funcionales del negocio se requiere de un análisis de riesgos.

- Secure the environment: paso en el que se ejecuta el plan de corrección de las áreas potencialmente vulnerables. Incluye cambios

técnicos, así como la implementación o cambios en las políticas y procedimientos.

- Evaluate and Educate: es el paso final, en el que se evalúa la ejecución de la seguridad y asegura que las necesidades funcionales del negocio no se hayan afectado con su ejecución. Las lecciones aprendidas resultantes de todos los pasos son útiles para educar a la organización para incrementar la conciencia y competencia de la seguridad de la organización.

Dentro de la metodología se describe los pasos que se deben seguir durante el proceso de evaluación, junto con las herramientas que se pueden utilizar para recoger la información necesaria para el diagnóstico de la seguridad. Las herramientas propuestas son, en su gran mayoría, de distribución libre y algunas son versiones de pruebas. Por medio de la metodología se evalúa lo que es la seguridad física de las instalaciones y equipos que conforman el sistema de información, las estaciones de trabajo y los servidores. En cada uno de estos aplica las cuatro fases descritas anteriormente.

2.1.12. NIST 800-42. Guideline on Network Security Testing (Pautas en la prueba de la seguridad de la red)

El National Institute of Standards and Technology es una organización federal de Los Estados Unidos que desarrolla y promueve medidas, estándares y tecnología. Mediante su documento NIST 800-42 pretende dar una guía para las pruebas de seguridad en las redes informáticas, identificando los requerimientos de prueba de la red y de que forma establecer las prioridades en las actividades con recursos limitados. El principal objetivo del documento es suministrar información básica acerca de las técnicas y herramientas de software útiles para realizar pruebas de seguridad a cualquier sistema de redes, aunque más dirigido hacia los tipos de sistemas con: *firewalls*, *routers*, *switches*, sistemas de detención de

intrusos, servidores Web, servidores de correo y otros servidores de aplicaciones, y servidores tales como DNS o de archivo (FTP). [9]

2.2. MARCO TEÓRICO REFERENCIAL

En este numeral se definen los conceptos específicos que se tienen en cuenta durante el desarrollo del trabajo de investigación. Dentro de estos conceptos se ofrece una breve descripción de las herramientas de seguridad utilizadas durante el diagnóstico de la seguridad informática de la red de datos.

2.2.1. ISO/IEC 27002 - Code of practice for information security management (Código de práctica para la gestión de la seguridad de la información)

ISO/IEC 27002 es un estándar para la seguridad informática publicado por la Organización Internacional para la Normalización (ISO) y por la Comisión Electrotécnica Internacional (IEC) durante el año 2000 y revisada por última vez en el año 2005. La norma establece directrices y principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información en una organización. Esta norma está compuesta por once secciones, de las que cada una contiene unas categorías principales de seguridad. Estas secciones sobre controles de seguridad se encuentran divididas como se relacionan a continuación:

- Política de seguridad: tiene como objetivo apoyar y orientar a la dirección con respecto a la seguridad de la información, de acuerdo con los requisitos del negocio, los reglamentos y las leyes.
- Organización de la seguridad de la información: su fin es brindar controles para gestionar la seguridad de la información dentro de la organización y mantener la seguridad de la información y de los servicios de la organización a los que tienen acceso terceras personas.

- Gestión de activos: su objetivo es lograr y mantener la protección adecuada de los activos de la organización, así como asegurar que la información recibe el nivel de protección adecuado.
- Seguridad de los recursos humanos: tiene como fin asegurar que los empleados, usuarios y cualquier persona que tenga alguna relación laboral con la organización estén conscientes de las amenazas y preocupaciones respecto a la seguridad de la información, sus responsabilidades y sus deberes, y que estén equipados para apoyar la política de seguridad de la organización, al igual que reducir el riesgo de error humano. También asegurase de que éstos abandonan la organización de forma ordenada.
- Seguridad física y del entorno: busca evitar el acceso físico sin autorización, el daño o la interferencia a las instalaciones y a la información de la organización, además de prevenir pérdida, daño, robo o puesta en peligro de los activos, y la interrupción de las actividades de la organización.
- Gestión de comunicaciones y operaciones: su objetivo es asegurar la operación correcta y segura de todos los sistemas, procesos y aplicaciones presentes dentro de la organización.
- Control de acceso: busca asegurar el acceso de usuarios autorizados y evitar el acceso no autorizado a los sistemas de información.
- Adquisición, desarrollo y mantenimiento de sistemas de información: pretende establecer unos requisitos de seguridad para los procesos de adquisición, desarrollo y mantenimiento de los sistemas de información en la organización. Define unos requisitos como la utilización de controles criptográficos, seguridad en los archivos y

aplicaciones. También busca reducir los riesgos que puedan resultar de la explotación de las vulnerabilidades técnicas publicadas.

- Gestión de los incidentes de seguridad de la información: busca asegurar la aplicación de un enfoque consistente y eficaz para la gestión de la seguridad de la información, y asegura que los eventos y las debilidades de seguridad se entrelazan de forma que permitan tomar las acciones correctivas oportunamente.
- Gestión de la continuidad del negocio: establece controles que permitan contrarrestar las interrupciones en las actividades del negocio y proteger sus procesos críticos contra fallas del sistema de información, y asegurar su restauración oportuna.
- Cumplimiento: evitar el incumplimiento de cualquier requisito legal, y asegurar que los sistemas están acorde con las normas y políticas de seguridad de la organización. [10]

2.2.2. Ataques informáticos

Se puede definir ataque informático como toda acción que busca comprometer la integridad, confidencialidad y disponibilidad de un sistema informático, con el objetivo de ganar privilegios en el sistema permitiéndole tener control sobre él, ya sea para el robo de información o el colapso del sistema. En la actualidad existe una gran variedad de ataques, que facilitan al atacante comprometer a cualquier sistema. A continuación se define los tipos de ataques más comunes.

- Virus: Son programas informáticos que ejecutan código malicioso y pueden infectar otros programas para afectar de forma negativa a los ordenadores.
- Troyanos: también llamados caballos de Troya son un programa malicioso que se esconde dentro de otro programa no maligno, y que al ejecutarse este último el código malicioso también se ejecuta,

siendo transparente para el usuario. El troyano hace que el atacante tenga acceso remoto a la información y recursos de la víctima, permitiéndole robar o dañar información del equipo.

- Gusanos o *worms*: es un código maligno que al ejecutarse realiza copias de si mismo con el fin de consumir memoria hasta desbordar la memoria RAM y desestabilizar al sistema.
- Bombas lógicas: son programas que permanecen ocultos en memoria y se activan cuando se realiza una acción determinada, que es programada por el creador del código o en determinado tiempo.
- *Exploits*: Programa informático que busca explotar las vulnerabilidades de otros programas. Esas vulnerabilidades son errores de programación. El uso principal es explotar una vulnerabilidad con el fin es inhabilitar el sistema a atacar para obtener acceso privilegiado a un equipo.
- *Data tampering*: Es la modificación desautorizada de los datos que se envían por la red.
- SQL *injection*: Ataque en el que se busca aprovechar una vulnerabilidad causada por errores de programación en las base de datos. Este ataque consiste en insertar un código SQL malicioso, por medio de los parámetros dados por el usuario, dentro de una sentencia SQL para alterar su funcionamiento normal, ejecutando el código malicioso en la base de datos.
- *Network mapping* (Mapeo de red): El propósito de este tipo de ataque es identificar la red, conocer que sistemas y equipos hacen parte de la red por medio de las respuestas comunes de los sistemas.

- SPAM: Es el envío masivo de mensajes no solicitados, en su gran mayoría son de tipo publicitario. El medio más común para enviar estos mensajes es el correo electrónico, y otros medios que son afectados por el SPAM son los foros, grupos de noticias, e incluso los teléfonos móviles por medio de mensajes de texto.

- Denegación de servicio – DoS (*Denial of Service*): Ataque a un sistema que busca limitar el acceso de los usuarios a un servicio, volviéndolo inaccesible. El ataque se realiza por medio de envíos masivos de solicitudes al servicio hasta sobrepasar la capacidad máxima que puede soportar éste, y de esta forma tumbar el servicio o el sistema en el que se ejecuta. En la **Figura 2** se muestra la forma en que se realiza un ataque de DoS a un servidor.

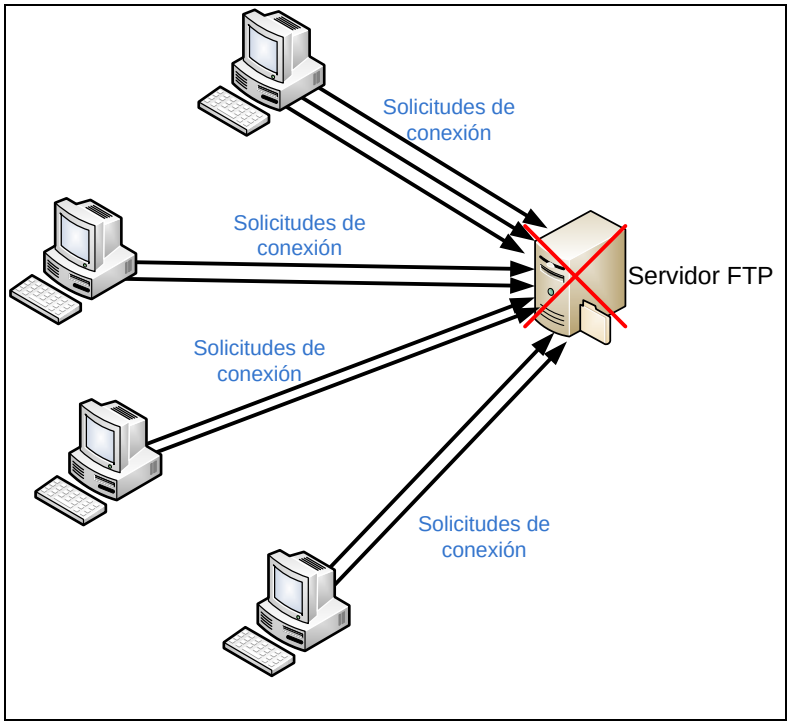

Figura 2 Esquema de ataque DoS a un servidor FTP

- *Man-in-the-middle*: Técnica de ataque en la que un atacante tiene la capacidad de intervenir en la comunicación entres dos entidades, logrando capturar paquetes en forma pasiva, es decir sin que las

víctimas tengan conocimiento de él. En la **Figura 3** se muestra un ataque *Man-in-the-middle* en el que el atacante interfiere la comunicación y modifica los datos hacia una de las victimas.

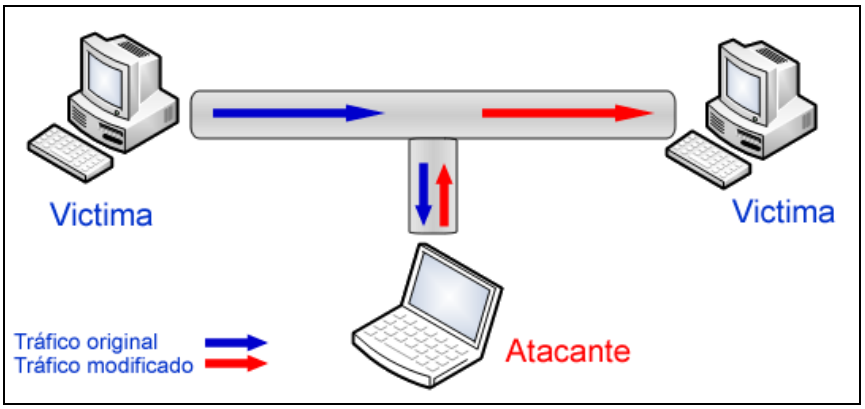

Figura 3 Ejemplo de un ataque Man-in-the-Middle

- ARP *Spoofing*: Es una técnica de ataque orientada a las redes segmentadas por *switches*, en la que se busca redirigir el tráfico con destino determinada dirección MAC hacia el equipo atacante. Esta técnica busca falsificar la tabla ARP de una victima para que éste envíe los paquetes al atacante y no al verdadero destino. En la **Figura 4** se muestra un ejemplo de ataque utilizando la técnica ARP *Spoofing*. En el ejemplo el atacante falsifica la tabla ARP y se hace pasar como el servidor para que el Host A le envíe los paquetes hacia él.

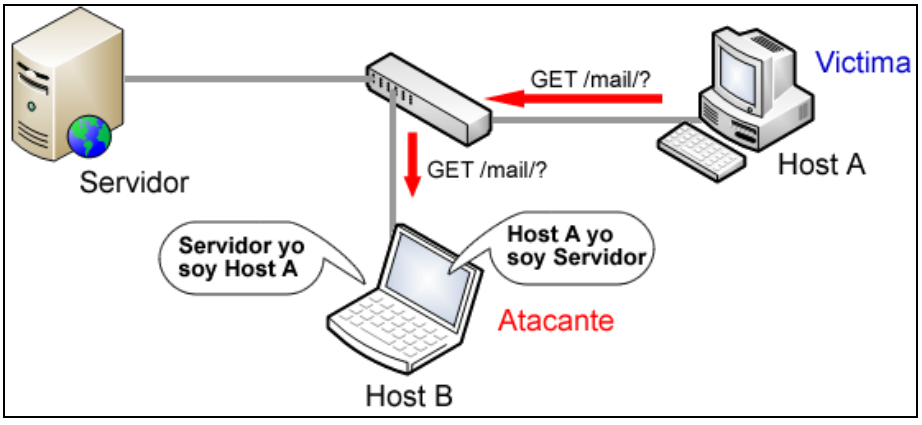

Figura 4 Ejemplo de un ataque ARP Spoofing

2.2.3. Herramientas para la evaluación de la seguridad

Para la realización del proceso de evaluación de la seguridad los evaluadores tienen una buena variedad de herramientas. Estas herramientas tienen las características de ser de software libre o comercial, y en la gran mayoría son las mismas que utilizan los atacantes para efectuar sus ataques. A continuación se describe cada una de las herramientas que ofrecen una buena opción para trabajar dentro de la metodología para el diagnóstico de la seguridad.

- BackTrack: es una de las más populares herramientas para las auditorias de seguridad. BackTrack es una distribución de Linux en live-CD orientada a los profesionales de seguridad informática, y en la cual se incluye más de 300 herramientas para realizar evaluaciones de la seguridad informática, desde *sniffers*, *exploits*, auditoria *wireless*, análisis forense y otras.

- Wireshark: es un analizador de protocolos de red, que permite capturar cualquier paquete que circule por la red. Con este programa se puede verificar si por medio de la red se capturan datos sin cifrar, es decir que existe la posibilidad de que determinada aplicación envíe información confidencial que puede ser fácilmente interceptada por cualquier persona dentro de la red.

- Ettercap: es una herramienta para realizar ataques de "*man in the middle*" sobre las redes LAN, en especial en las basadas en switches. Entre sus características se encuentra las de *sniffer*, ARP *Spoofing* y otras para el análisis de redes y equipos.

- NetStumbler: es una herramienta en Windows que permite detectar redes inalámbricas usando 802.11a, 802.11b y 802.11g, y permite identificar la presencia de redes inalámbricas inseguras, conocer la

cobertura de las redes, detectar interferencias de otras redes, y otros usos más.

- Nessus: es una herramienta que se utiliza para escanear uno o varios equipos de la red con el fin de encontrar sus vulnerabilidades. Con esta herramienta se puede identificar si el equipo tiene algún problema de seguridad que puede ser aprovechado por alguien para comprometer el equipo. Puede indicar si al equipo le falta algún parche o está desactualizado.
- Metasploit Framework: es una completa herramienta para escribir, probar y usar código exploit, que son utilizados para aprovechar las vulnerabilidades de los equipos de red. Esta herramienta es una sólida plataforma para las pruebas de penetración e investigación de vulnerabilidades.
- Nmap: herramienta de código abierto para la exploración de red y auditoría de la seguridad. Nmap permite encontrar los equipos disponibles en la red, detectar que servicios ofrecen, conocer los sistemas operativos que ejecutan, y otras funciones más que ayudan a los administradores de red a encontrar fallas en la red y a los auditores a realizar las evaluaciones de seguridad.
- Yersinia: Herramienta de red diseñada para aprovechar debilidades en diferentes protocolos de la capa de enlace, como STP, DTP, CDP, IEEE 802.1Q, IEEE 802.1X, VTP y otros. Permite realizar ataques de negación de servicio a dichos protocolos, ganar privilegios dentro de las redes segmentadas en VLAN's y así capturar todo el tráfico de otras VLAN's.

2.2.4. Política de seguridad

Es una declaración de principios que presenta la posición de la administración para el área de seguridad, con el fin de que tengan aplicación

a largo plazo y guíen el desarrollo de reglas y criterios más específicos. La política debe estar soportada por estándares, mejores prácticas, guías y procedimientos. Una política de seguridad debe ser aprobada por las directivas de una organización y deben ser obligatorias. [11]

2.2.5. Evaluación de riesgos en seguridad informática

Es un proceso en el que se lleva a cabo el análisis de las vulnerabilidades y amenazas que existen o pueden afectar a determinado sistema de información. El paso inicial es recopilar información sobre el sistema, es decir cada uno de los elementos que conforman dicho sistema, para de esta forma calificar cada componente de acuerdo a su nivel de importancia. El siguiente paso es identificar las vulnerabilidades y amenazas que puedan afectar a cada componente del sistema, para así definir su nivel de exposición. Para identificar las vulnerabilidades se puede recurrir al uso de herramientas informáticas, como analizadores de vulnerabilidades, además del uso de estándares y guías de buenas prácticas. En este punto ya se puede clasificar el impacto correspondiente a que una amenaza se haga efectiva. El paso siguiente es establecer la probabilidad de que ocurra una amenaza debido a la presencia de vulnerabilidades, con lo que se obtiene el nivel de riesgo para cada elemento evaluado.

3. INGENIERÍA DEL PROYECTO

Como uno de los pasos antes de comenzar el desarrollo del trabajo de investigación se requirió llevar a cabo el análisis de dos factores relevantes. El primero de ellos es investigar acerca del estado del arte del proyecto, y el segundo de ellos es tratar el problema planteado desde el punto de vista de ingeniería mediante un análisis de las variables de ingeniería.

3.1. ESTADO DEL ARTE

La División de Informática, quien es la encargada de la seguridad informática en la UMNG, no tiene definida una metodología que le permita realizar diagnósticos de la seguridad en la red de datos administrada por ella. Además dentro del grupo de investigación GISSIC no se cuenta, tampoco, con una metodología que permita el diagnóstico de la seguridad.

3.2. ANÁLISIS DE VARIABLES

La necesidad de definir una metodología para realizar el diagnóstico de la seguridad en la red de datos de la Universidad, desde el punto de vista de ingeniería conlleva a analizar unas variables de ingeniería, que son la base para el desarrollo de la presente investigación. Las variables que son tema de análisis para cumplir con esta necesidad son las amenazas, vulnerabilidades y los riesgos asociados a los sistemas en la red.

3.2.1. Exposición del activo

Dentro de un contexto de análisis de riesgos la exposición es el alcance de daños posibles que pueda causar la combinación de una amenaza y una vulnerabilidad de un activo independiente de su clasificación dentro de una

organización. El nivel de exposición puede ser clasificado de acuerdo a tres criterios que se relacionan en la tabla 1.

Tabla 1 Criterio para clasificar el nivel de exposición del activo. [21]

CRITERIOS PARA CLASIFICAR EL NIVEL DE EXPOSICIÓN DEL ACTIVO	
Pérdida grave o completa del activo	**ALTA**
Pérdida limitada o moderada	**MEDIA**
Pérdida menor o no hay pérdida	**BAJA**

3.2.2. Nivel de impacto

El impacto es la repercusión negativa sobre el rendimiento del negocio causado por el aprovechamiento de una vulnerabilidad. El impacto se clasifica mediante la tabla 2, el cual se determina de acuerdo a la clasificación del activo y su nivel de exposición a determinada amenaza/vulnerabilidad.

Tabla 2 Clasificación del impacto. [21]

Clase de Activo	**ALTO**	**3**	**Impacto Medio**	**Impacto Alto**	**Impacto Alto**
	MEDIO	**2**	**Impacto Bajo**	**Impacto Medio**	**Impacto Alto**
	BAJO	**1**	**Impacto Bajo**	**Impacto Bajo**	**Impacto Medio**
			1	**2**	**3**
			BAJO	**MEDIO**	**ALTO**
			Nivel de exposición		

Como resultado de relacionar la clasificación del activo y su exposición se obtiene uno de los tres niveles de impacto, que son alto, medio y bajo.

3.2.3. Probabilidad de la amenaza

Estimación de la ocurrencia de una amenaza debido a la facilidad existente de aprovechar una vulnerabilidad del activo. La probabilidad puede ser clasificada como **alta**, cuando la vulnerabilidad correspondiente a una amenaza presenta factores que hacen fácil su explotación y por lo tanto no requiere de muchos conocimientos en seguridad para tal efecto; **media**, cuando ya no es fácil aprovechar la vulnerabilidad pero no se necesita de

privilegios de administrador y conocimientos tan avanzados; y **baja**, cuando ya es necesario de conocimientos avanzados y privilegios de administrador para aprovechar la vulnerabilidad. Los criterios para clasificar la probabilidad se muestran en la tabla 3.

Tabla 3 Criterios para estimar la probabilidad de las amenazas. [21]

CRITERIOS PARA DE ESTIMAR LA PROBABILIDAD DE LAS AMENAZAS
ALTA – 3
Ejecutable remotamente Requiere de privilegios anónimos Método para explotar la vulnerabilidad publicado Posibilidad de programar el ataque para buscar automáticamente vulnerabilidades Requiere de pocos conocimientos para realizar un ataque Las condiciones externas favorecen a que la amenaza se haga efectiva
MEDIA – 2
Requiere de expertos o especialistas para realizar un ataque No ejecutable remotamente Requiere de privilegios de usuario Método para explotar la vulnerabilidad no publicado Sin posibilidad de programar el ataque para buscar automáticamente vulnerabilidades Las condiciones externas dificultan que la amenaza se haga efectiva
BAJA – 1
Requiere de conocimientos avanzados para realizar un ataque No ejecutable remotamente Requiere de privilegios de administrador Método para explotar la vulnerabilidad no publicado Sin posibilidad de programar el ataque para buscar automáticamente vulnerabilidades Las condiciones externas no favorecen a que la amenaza se haga efectiva

3.2.4. Nivel de riesgo

Las redes de datos están expuestas a una gran cantidad de amenazas, desde amenazas naturales (Ej.: terremoto e inundaciones) hasta amenazas técnicas, en las que se requiere de herramientas técnicas para afectar las tecnologías utilizadas en la red. Sin embargo, para que lo anterior se llegue a presentar en una red, ésta debe tener alguna vulnerabilidad, como construcciones sin protecciones sísmicas o errores de configuración en los equipos. La presencia de estas dos características hace que se tenga un riesgo asociado a la red. El riesgo se define como el daño potencial causado

por una amenaza que pueda explotar las vulnerabilidades de un activo [20]. Esta relación puede ser representada por la siguiente ecuación:

$$RIESGO = AMENAZA \times VULNERABILIDAD$$

La anterior ecuación refleja que la existencia de un riesgo está determinada por la presencia de una amenaza y, al menos, una vulnerabilidad, mas no representa un nivel de riesgo, el cual es determinado al estimar un nivel de exposición del activo, un nivel de impacto de acuerdo a la clasificación del activo y una probabilidad de ocurrencia de dicha amenaza debido a facilidad de aprovechar la vulnerabilidad del activo.

Con el fin de identificar los riesgos a que están expuestos los activos presentes en la red de datos y de esta forma identificar los aspectos más críticos de la red y en los que se debe tener mucha precaución durante una evaluación de seguridad, se lleva a cabo una evaluación de riesgos. Esta evaluación de riesgo se basará de acuerdo a algunos lineamientos definidos en el documento elaborado por Microsoft en su "**Guía de administración de riesgos de seguridad**", en su capítulo cuarto: **Evaluación del riesgo** [21]. El proceso seguido para realizar la evaluación del riesgo en la red de datos de la UMNG se muestra en la figura 5.

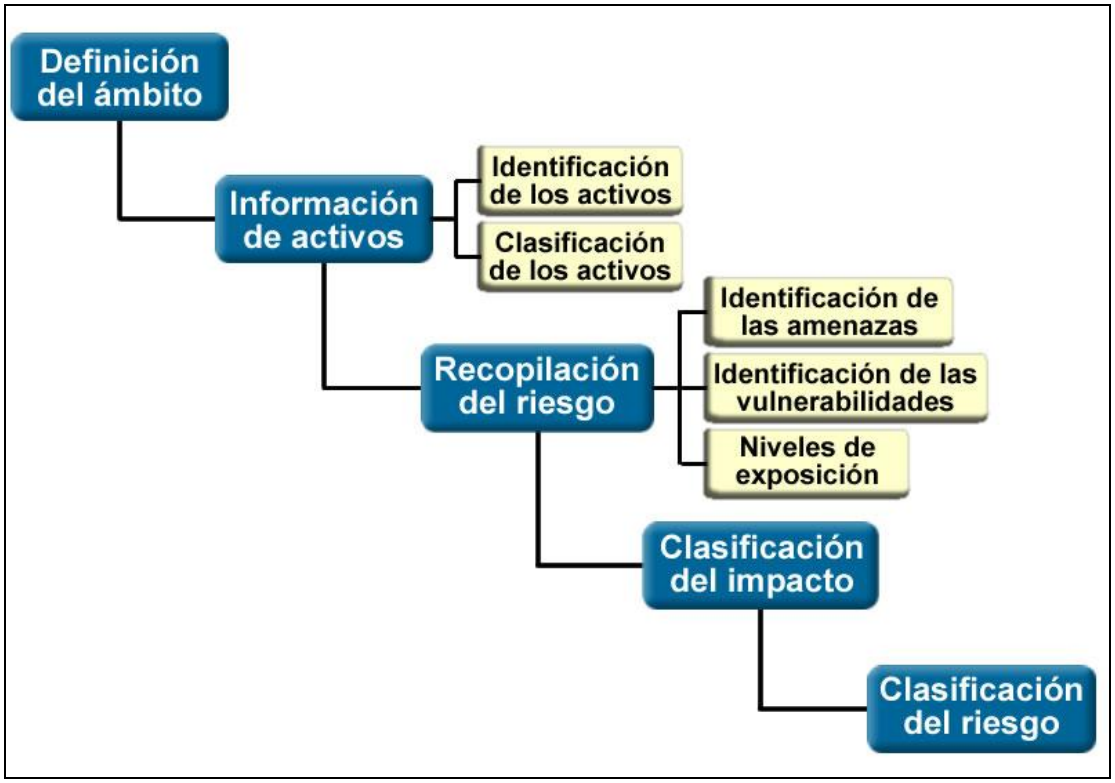

Figura 5 Proceso de evaluación del riesgo

- Definición del ámbito: es el primer paso para el proceso de evaluación, y en él se define el campo de acción o el área que es objeto de evaluación.
- Información de activos: busca obtener información sobre los activos que se encuentran dentro del área de trabajo. En este paso se obtiene información sobre los activos y se clasifican según el papel que desempeñen y su importancia en el sistema.
- Recopilación del riesgo: esta recopilación consiste en identificar las amenazas a que se encuentra expuesta cada activo y si existe alguna vulnerabilidad que haga efectiva esa amenaza, además se establece el nivel de exposición del activo, que es el alcance de daños posibles

- Clasificación del impacto: el impacto es la repercusión negativa sobre el rendimiento del negocio causado por el aprovechamiento de una vulnerabilidad.
- Clasificación del riesgo: es el último paso del proceso y en el cual se obtiene el nivel de riesgo asociado al activo, al estimar la probabilidad de que una amenaza se haga efectiva. Para clasificar el riesgo se debe relacionar el impacto y la probabilidad estimada de acuerdo a la tabla 4.

Tabla 4 Clasificación del riesgo. [21]

CLASIFICACIÓN DEL RIESGO					
Impacto	ALTO	3	Riesgo Moderado	Riesgo Alto	Riesgo Alto
	MEDIO	2	Riesgo Bajo	Riesgo Moderado	Riesgo Alto
	BAJO	1	Riesgo Bajo	Riesgo Bajo	Riesgo Moderado
			1	2	3
			BAJO	MEDIO	ALTO
			Nivel de Probabilidad		

Como resultado se obtiene el nivel de riesgo para cada una de las amenazas asociadas al activo, por lo que se hace necesario aplicar la siguiente formula matemática para determinar el nivel de riesgo promedio en el que se encuentra el activo.

$$\overline{Nivel\ de\ Riesgo} = \frac{\sum Clasificac\,ión\ de\ Riesgo}{Cantidad\ \ de\ amenazas}$$

4. DESARROLLO DEL PROYECTO

En el presente capítulo se encuentra todo el proceso elaborado durante el desarrollo del presente trabajo de investigación.

4.1. ESQUEMA DE SEGURIDAD EN LA UMNG

Inicialmente la División de Informática de la UMNG tenía definido un esquema de seguridad informática que no se encontraba muy bien estructurado para la realización de una metodología, debido a que concentraba todos sus sistemas críticos en una única sección de las cuatro que se definían. Por esa razón se debió estructurar en una mejor forma la seguridad del sistema de información de la UMNG, y para esto se contó con la ayuda de los funcionarios de la División de Informática y con la aprobación de ellos del esquema renovado. En los siguientes numerales se describen los dos esquemas: el primero es con el que contaba la División antes de la realización del presente trabajo de investigación, y el segundo es el esquema renovado y aprobado por la División.

4.1.1. Esquema de seguridad informática inicial en la UMNG

Antes de la realización de este trabajo de investigación la seguridad en la red de la Universidad se centraba en proteger sus sistemas críticos teniendo como finalidad la seguridad física y lógica de éstos, como objetivo principal. Adicional a ésto, definía como frentes principales controles para la protección de la información, concientización de usuarios y acceso controlado desde fuera de la red, lo cual no reflejaba un fuerte esquema de seguridad. En la **figura 6** se muestra el esquema de la seguridad informática que manejaba la División de Informática. El esquema se dividía en cuatro secciones y cada una cubría un grupo de elementos, que se relacionaban con el objetivo de cada sección.

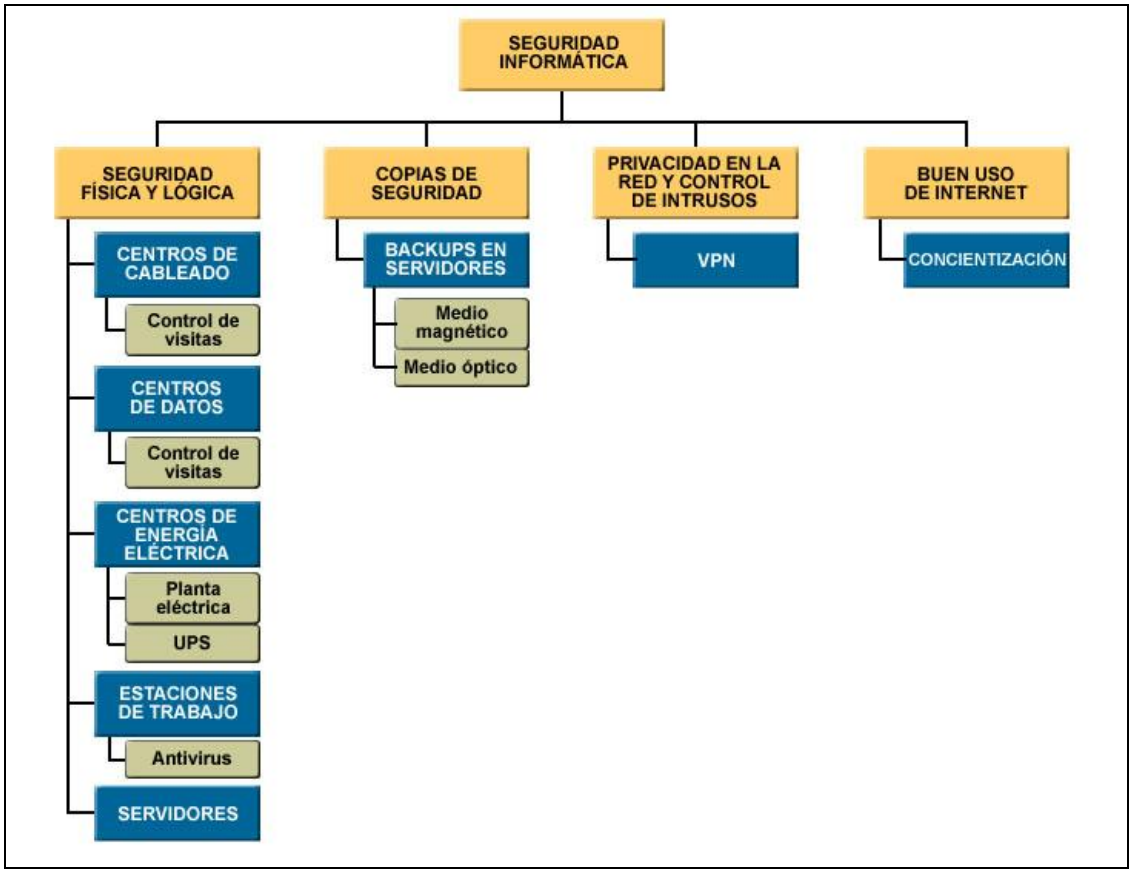

Figura 6 Esquema de seguridad en la red de la UMNG

- Seguridad física y lógica: la seguridad física hace referencia a los Centros de Datos y Cableado donde el acceso es restringido a personal de Informática y se lleva un control de visitas. La seguridad en las estaciones de trabajo se maneja con segmentación por VLAN, utilización de antivirus con actualización permanente y autenticación local. Por último, los servidores están configurados para prestar sólo los servicios para que están destinados, además los servidores de carácter público están protegidos por *firewalls* internos.

- Copias de seguridad: los servidores que contienen información importante para la institución que es manejada por las diferentes

aplicaciones y servicios se les realizan copias de seguridad, que son guardadas en medio magnético y óptico.

- Privacidad en la red y control de intrusos: en la Universidad los equipos del personal de trabajo se conectan, mediante sus equipos de cómputo, a la Intranet de la institución, allí se maneja información confidencial. Los segmentos de red donde los estudiantes tienen acceso a Internet están restringidos a la Intranet. En los casos que se necesite tener acceso a esa información desde fuera de la Intranet, se utiliza el servicio de VPN (Red Privado Virtual).
- Buen uso de Internet: la División de Informática está en el deber de concienciar a la comunidad de la Universidad, el uso adecuado de Internet orientado a cumplir la misión de la institución.

4.1.2. Esquema propuesto de seguridad en la UMNG

Para la implementación de una metodología para el diagnóstico de la seguridad informática se debió estructurar de una manera más organizada la seguridad en el sistema de información de la Universidad. El nuevo esquema se separa en cinco secciones, que agrupa los diferentes elementos del sistema de información de acuerdo al papel que desempeñan dentro de él. En la figura 7 se encuentra la organización del nuevo esquema de seguridad. Este nuevo esquema se elaboró con la ayuda de los funcionarios de la División de Informática encargados de la administración del sistema de información.

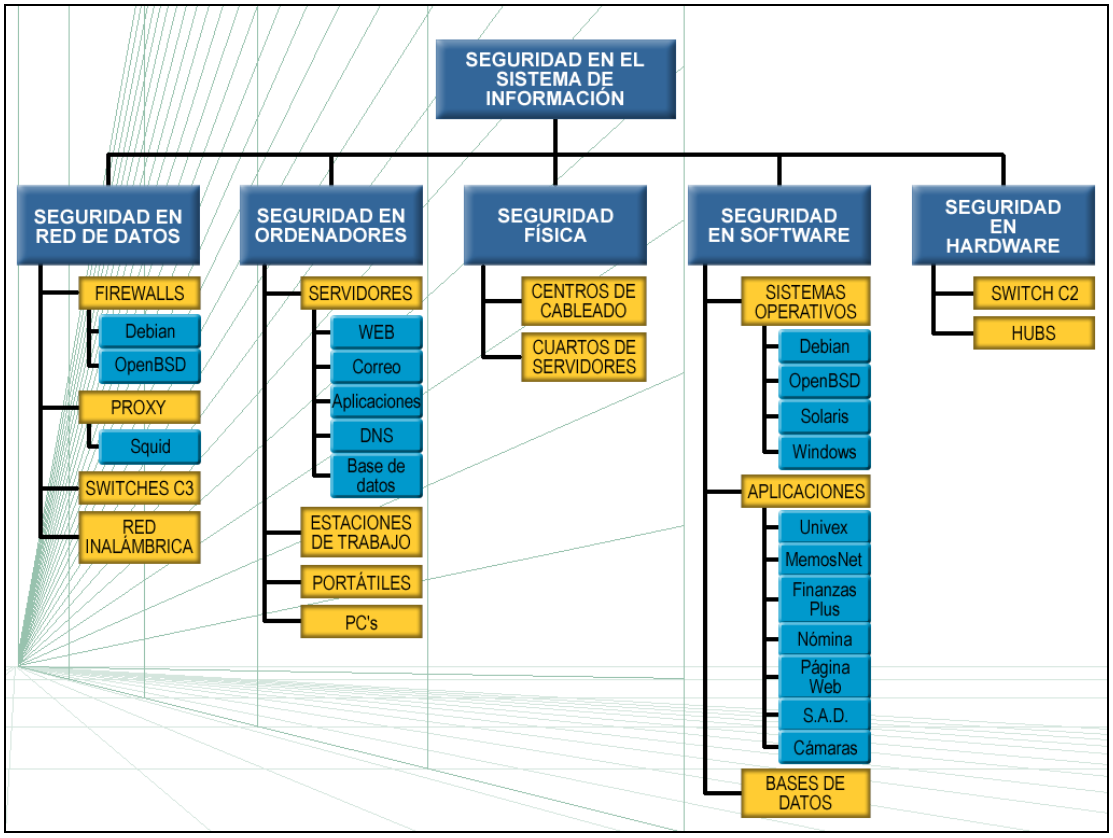

Figura 7 Seguridad en el sistema de información de la UMNG

- Seguridad en red de datos: En esta sección la seguridad se centra en aquellos equipos de red que permiten protegerla de comunicaciones o accesos no autorizados a determinados servicios e información confidencial. Los elementos que ofrecen este tipo de seguridad en la red son los *firewalls*, *proxies*, y *switches* de capa tres. La red inalámbrica debido a que esta configurada para acceso libre es un elemento de cuidado dentro de la red, y por ésto se tiene en cuenta dentro de esta sección, porque implica un gran riesgo en la seguridad de la red.

- Seguridad en ordenadores: En esta sección se tiene lo que concierne a la seguridad en estaciones de trabajo, equipos portátiles, y la seguridad de los servidores instalados en la red. El enfoque principal está en los equipos que trabajan como servidores,

y en donde se maneja información crítica para los procesos de la Universidad.

- Seguridad física: Esta sección comprende la seguridad en los centros de cableado, en las oficinas y en los cuartos donde se encuentran los servidores. En esta área los aspectos críticos son los controles de seguridad en el acceso a equipos, también factores que puedan afectar la integridad y disponibilidad de ellos.
- Seguridad en software: Esta es una de las secciones más críticas, y se encuentra separada en tres diferentes áreas, una de ellas son las aplicaciones desarrolladas en la Universidad, otra son los sistemas operativos instalados en servidores y demás equipos de trabajo, y por último están las bases de datos donde se administra toda la información confidencial de la Universidad.
- Seguridad en hardware: Esta área cubre todos los equipos activos utilizados para interconectar los distintos segmentos de red y que no son un factor muy crítico en la prestación de seguridad en la red. Hacen parte de este grupo todos los *switches* de capa dos y *hubs*.

4.2. EVALUACIÓN DE RIESGOS A LA RED DE DATOS

A continuación se describe el proceso llevado a cabo para realizar la evaluación de riesgos a la red y los resultados obtenidos, con los que serán la base para definir la metodología. Como se dijo en el numeral 3.2.4 el proceso sigue lineamientos dados en el documento, generado por Microsoft, "**Guía de administración de riesgos de seguridad**" [21].

4.2.1. Ámbito de la evaluación de riesgos

La evaluación de riesgos a realizar comprende los activos de *hardware* dentro de la categoría de servidores, *firewall*, *Proxy*, *switches* de capa 3 y red

inalámbrica, que hacen parte de la red de datos de la Universidad Militar “Nueva Granada” en su sede de la calle 100.

4.2.2. Recopilación de la información

La red de datos de la Universidad Militar Nueva Granada, en su sede central, se encuentra dividida en dos segmentos principales que parten de un *firewall* ubicado en el perímetro de la red y que filtra el tráfico desde y hacia la Internet. Los dos segmentos principales se describen a continuación:

- El primer segmento es de direccionamiento público. Éste es donde se encuentra la DMZ, es decir la zona desmilitarizada, que está compuesta por los **servidores** de acceso desde la Internet, así como desde la red interna. Desde el *switch* de la DMZ se desprende un Proxy que se encarga de dar acceso a Internet a los segmentos de red de la sala de Internet, la **red inalámbrica** y los laboratorios, y aislarlos de la intranet.

- El segundo segmento es la intranet. En ella se encuentran aproximadamente 1000 computadores, separados en varias VLAN’s por medio del uso de ***switches* de capa 3**. Cada VLAN agrupa los equipos pertenecientes a cada división institucional. También se encuentra el sistema telefónico de la Universidad.

La seguridad de la red se encuentra soportada en tres equipos:

- Firewall: encargado de la protección perimetral, filtra el tráfico proveniente desde Internet hacia los diferentes segmentos de la red.

- Proxy de la Intranet: funciona como NAT, es decir que se encarga de la traducción de las direcciones privadas de la intranet a direcciones públicas con el fin de tener acceso a Internet. También mediante unas listas de acceso se encarga de filtrar tráfico a la intranet.

- Proxy de la red pública: restringe el tráfico hacia la intranet desde los segmentos de la sala de Internet, la red inalámbrica y los

laboratorios; segmentos a que tienen acceso cualquier persona que ingrese a las instalaciones de la Universidad.

En la figura 8 muestra como se encuentra estructurada la red de la sede central de la UMNG.

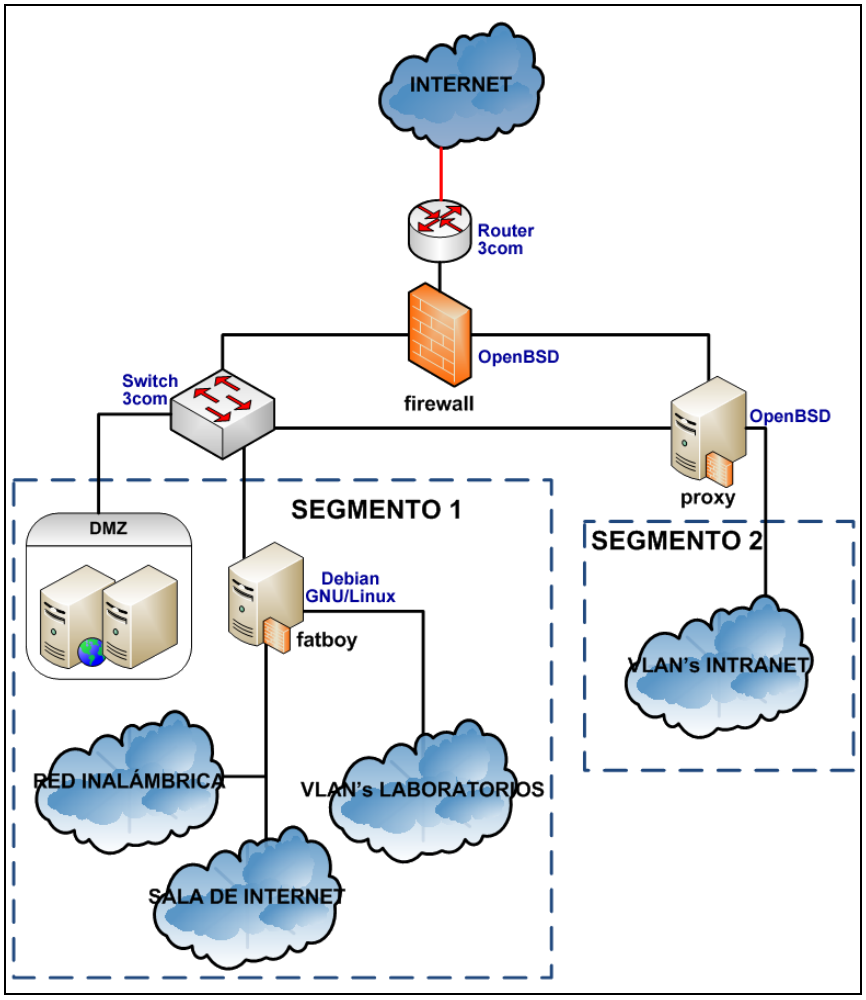

Figura 8 Estructura de la red de la sede central de la UMNG

Toda la información fue suministrada por cada uno de los funcionarios de la División de Informática encargados de los respectivos elementos.

4.2.3. Clasificación de los activos

Después de recopilar la información sobre los activos de la red que se encuentran dentro del ámbito de la presente evaluación y con la ayuda de los funcionarios de la División de Informática se clasifican los activos en alta,

media y baja importancia, de acuerdo al papel que desempeñan y la repercusión en la confidencialidad, integridad y disponibilidad de éstos en el rendimiento de la institución. En la tabla 5 se encuentra la clasificación dada para cada activo.

Tabla 5 Clasificación de los activos en la red de la universidad

	NOMBRE	DESCRIPCIÓN	CLASIFICACIÓN
1	**Firewall**	Equipo encargado de la seguridad perimetral de la red.	ALTA – 3
2	**Proxy red privada**	Equipo que ejecuta las funciones de Proxy para el segmento privado de la red de la UMNG o la Intranet	ALTA – 3
3	**Proxy segmento público**	Ofrece los servicios necesarios para permitirle conexión a Internet a los segmentos de red públicos compuestos por la sala de Internet, laboratorios de la Universidad y la red inalámbrica.	MEDIA – 2
4	**Servidor Antispam**	Servidor que cumple el papel de reducir las cantidades de correo spam entrante al servidor de correo.	ALTA – 3
5	**Servidor de Correo electrónico**	Servidor por el cual se presta el servicio de correo electrónico para los estudiantes y funcionarios de la universidad.	ALTA – 3
6	**Servidor de pruebas**	Maquina virtual en el servidor Multi-servidores utilizada para realizar pruebas de aplicaciones, sistemas operativos, etc.	BAJA – 1
7	**Servidor de Registro**	Maquina virtual en el servidor Multi-servidores destinada para los procesos de Registro y Control académico	ALTA – 3
8	**Servidor GISSIC**	Equipo que aloja la página Web del grupo de investigación GISSIC y que opera como apoyo para las investigaciones en desarrollo.	BAJA – 1
9	**Servidor Librejo - Gestión bibliotecaria**	Servidor destinado para alojar la aplicación en desarrollo Librejo para la gestión bibliotecaria	BAJA – 1
10	**Servidor Oracle**	Servidor que aloja las bases de datos para los distintos procesos y servicios usados en la red.	ALTA – 3
11	**Servidor SAD Virtual**	Maquina virtual en el servidor Multi-servidores que destinada para el servicio de digitalización de documentos mediante el SAD Virtual	MEDIA – 2
12	**Servidor multi-servidores**	Servidor con maquinas virtuales donde se alojan los servicios de página Web, registro, pagos en línea, SAD virtual y servidor de pruebas.	MEDIA – 2
13	**Servidor Web**	Maquina virtual en el servidor Multi-servidores donde se alojan la página Web de la Institución	BAJA – 1

14	**Servidor NFS**	Servidor utilizado como almacenamiento de los datos generados con los servicios de correo electrónico y cámaras de vigilancia.	MEDIA – 2
15	**Switches capa 3**	Equipos de la red que se encargan de segmentarla en distintas VLAN's.	MEDIA – 2
16	**Red inalámbrica**	Red de acceso público dentro del campus.	BAJA – 1

4.2.4. Identificación de las amenazas y vulnerabilidades

Las amenazas asociadas a cada uno de los elementos en el área de seguridad en red de datos se encuentran diferenciadas en dos grupos: las no técnicas y las técnicas. Las amenazas no técnicas se identificaron mediante la observación y con base a lo contemplado por el estándar ISO/IEC 27002. Estas amenazas se identifican analizando las condiciones de las instalaciones en donde se encuentran los equipos, evaluando la seguridad física implementada para mitigar los riesgos de daño o robo de los equipos debido a un incendio o vandalismo. Las amenazas técnicas se identificaron por medio de la información técnica suministrada, como las configuraciones de los equipos. En el capítulo nueve, sobre seguridad física y del entorno, de el estándar ISO/IEC 27002 y con la realización de visitas a las ubicaciones de equipos de la red se determinaron las amenazas a que están expuestos los equipos de la red, las cuales se listan en la tabla 6.

Tabla 6 Amenazas presentes en los activos de la red de la UMNG

AMENAZAS
Acceso no autorizado
Ataque por un pirata informático
Calentamiento del equipo
Divulgación de información sobre el activo
Incendio
Interrupción del servicio
Persona malintencionada
Recopilación información sobre los equipos protegidos por el firewall
Robo de credenciales
Robo de identidad o suplantación
Robo de información privada
Robo del equipo

Para identificar las vulnerabilidades se requirió de las herramientas de seguridad Nmap, Nessus, Ettercap, Arpspoof, NetStumbler, Wireshark y el CD BackTrack que recoge algunas de las herramientas anteriores. A continuación se describirá la utilización de cada herramienta y la función desempeñada para la búsqueda de las vulnerabilidades.

- Nmap: su función es detectar la condición de los puertos y los servicios activos en cada equipo a analizar, y evaluar el funcionamiento del *firewall* para filtrar tráfico hacia la red. El comando utilizado para identificar el estado de los puertos es:

  nmap –sS <Dirección IP del equipo>

  Mediante este comando se envían peticiones de conexión (SYN) para el protocolo TCP a los puertos del equipo remoto. El tipo de respuesta obtenido es la siguiente.

  Starting Nmap 4.20 (http://insecure.org) at 2007-05-15 15:30 Hora est. del Pacífico de SA
  Interesting ports on 172.16.15.1:
  Not shown: 1683 closed ports

PORT	*STATE*	*SERVICE*
21/tcp	*open*	*ftp*
80/tcp	*open*	*http*
135/tcp	*filtered*	*msrpc*
137/tcp	*filtered*	*netbios-ns*
138/tcp	*filtered*	*netbios-dgm*
139/tcp	*filtered*	*netbios-ssn*
445/tcp	*filtered*	*microsoft-ds*
1214/tcp	*filtered*	*fasttrack*
3128/tcp	*open*	*squid-http*
4444/tcp	*filtered*	*krb524*
4660/tcp	*filtered*	*mosmig*
4662/tcp	*filtered*	*edonkey*
6346/tcp	*filtered*	*gnutella*
6881/tcp	*filtered*	*bittorent-tracker*

  Nmap finished: 1 IP address (1 host up) scanned in 29.125 seconds

  En la respuesta anterior se puede observar un listado de puertos TCP con su respectivo estado y nombre del servicio. El equipo

escaneado tiene los puertos 80 y 3128 porque éste el servicio de proxy. El puerto 21 se encuentra también abierto y puede llegar a ser una vulnerabilidad, si en ese equipo no se presta el servicio de FTP.

- Nessus: este escáner de vulnerabilidades tiene como fin comprobar si el equipo presenta alguna vulnerabilidad conocida. En la figura 9 se puede observar el escaneo realizado a cinco direcciones IP, en ella se muestra el progreso, junto con la cantidad de puertos abiertos, problemas de seguridad encontrados y notas generadas por el programa.

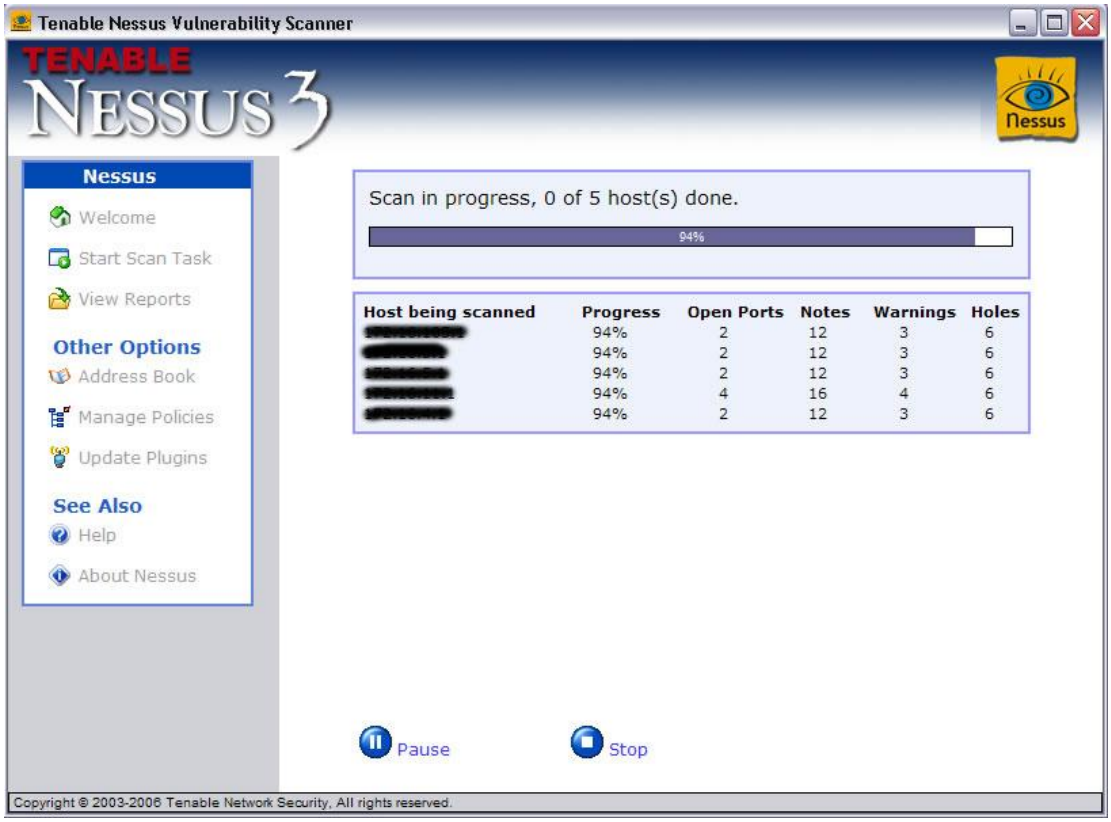

Figura 9 Progreso del escaneo de vulnerabilidades a cinco direcciones IP

El resultado del escaneo con Nessus es un reporte, en formato HTML, con el listado de los puertos abiertos y los problemas de seguridad encontrados en esos puertos.

Como resultado del análisis de vulnerabilidades se obtuvo las vulnerabilidades relacionadas en la tabla 7 para los activos que hacen parte del análisis. Algunas de las vulnerabilidades encontradas son comunes para varios activos debido a que la gran mayoría cuentan con las mismas características de instalación física, por lo que se encuentran en un mismo cuarto.

Tabla 7 Listado de vulnerabilidades asociadas a los activos analizados.

VULNERABILIDADES
Problema de configuración. Permite realizar conexiones a puertos sensibles dándole la capacidad a un atacante evitar las reglas del firewall y conectarse a puertos no permitidos.
Cross Site Scripting (XSS). El sistema de validación de HTML permite ejecutar scripts maliciosos
Cross Site Tracing (XST). Causada por algún error de filtrado y del uso del comando TRACE de HTTP
Falta de monitores de las condiciones ambientales.
Instalación predeterminada de TOMCAT
Ausencia de extintores en el cuarto.
Las paredes del cuarto y la presencia de elementos como cajas puede ser factor para la propagación rápida del fuego.
En el mismo cuarto se almacena elementos ofimáticos, tales como resmas de papel y cajas.
Off-by-one buffer overflow. Versión del Apache desactualizada,
Versión de Apache con múltiples vulnerabilidades. » Buffer overflow. » Ejecución de código arbitrario. » DoS. » Cross Site Scripting (XSS)
No se tiene un control de las visitas al cuarto donde se encuentra el equipo.
El router administrado por el proveedor de Internet está ubicado en el mismo cuarto del equipo.
El firewall permite enumerar lo equipos detrás del firewall.
Uso de autenticación en texto plano
Los switches están expuestos a ataques ARP Spoofing.
DNS cache poisoning. La resolución remota de DNS no utiliza puertos aleatorios cuando hace consultas al servidor DNS

DNS Cache Snooping. El servicio de DNS permite que un tercero pueda obtener información sobre los nombre de dominio que han sido resueltos por el servidor.
No se tiene habilitado un protocolo de cifrado que permita cifrar los datos y permitir el acceso a sólo usuarios de la UMNG.
Paredes del cuarto muy débiles. Falta de mecanismos de control para el acceso no autorizado como alarmas y cámaras.
Paredes del cuarto no reforzadas.

4.2.5. Clasificación del nivel de exposición

Una vez definidas las amenazas y vulnerabilidades asociadas a cada activo objeto de la evaluación se debe clasificar la exposición del activo, o en otras palabras los daños que puede causar la amenaza que es aprovechada por una vulnerabilidad, independiente de la clasificación del activo. Para clasificar el nivel de exposición se toma como referencia los criterios definidos en la tabla 1. Como resultado del análisis para determinar el nivel de exposición se llegó a la tabla 8, en la que se muestra la amenaza junto con la vulnerabilidad asociada y el correspondiente nivel de exposición.

Tabla 8 Niveles de exposición para cada relación Amenaza/Vulnerabilidad

AMENAZA	VULNERABILIDAD	NIVEL DE EXPOSICIÓN
Ataque por un pirata informático	Problema de configuración. Permite realizar conexiones a puertos sensibles dándole la capacidad a un atacante evitar las reglas del firewall y conectarse a puertos no permitidos.	MEDIA
Ataque por un pirata informático	Cross Site Scripting (XSS). El sistema de validación de HTML permite ejecutar scripts maliciosos	MEDIA
Ataque por un pirata informático	Cross Site Tracing (XST). Causada por algún error de filtrado y del uso del comando TRACE de HTTP	BAJA
Calentamiento del equipo	Falta de monitores de las condiciones ambientales.	MEDIA
Divulgación de información sobre el activo	Instalación predeterminada de TOMCAT	BAJA
Incendio.	Ausencia de extintores en el cuarto.	ALTA

Incendio.	Las paredes del cuarto y la presencia de elementos como cajas puede ser factor para la propagación rápida del fuego.	ALTA
Incendio.	En el mismo cuarto se almacena elementos ofimáticas, tales como resmas de papel y cajas.	ALTA
Interrupción del servicio	Off-by-one buffer overflow. Versión del Apache desactualizada,	MEDIA
Interrupción del servicio	Versión de Apache con múltiples vulnerabilidades. » Buffer overflow. » Ejecución de código arbitrario. » DoS. » Cross Site Scripting (XSS)	MEDIA
Persona malintencionada	No se tiene un control de las visitas al cuarto donde se encuentra el equipo.	BAJA
Persona malintencionada / Acceso no autorizado	El router administrado por el proveedor de Internet está ubicado en el mismo cuarto del equipo.	MEDIA
Recopilar información sobre los equipos protegidos por el firewall	El firewall permite enumerar lo equipos detrás del firewall.	BAJA
Robo de credenciales	Uso de autenticación en texto plano	MEDIA
Robo de identidad o suplantación.	Los switches están expuestos a ataques ARP Spoofing.	MEDIA
Robo de información	DNS cache poisoning. La resolución remota de DNS no utiliza puertos aleatorios cuando hace consultas al servidor DNS	BAJA
Robo de información	DNS Cache Snooping. El servicio de DNS permite que un tercero pueda obtener información sobre los nombre de dominio que han sido resueltos por el servidor.	BAJA
Robo de información	No se tiene habilitado un protocolo de cifrado que permita cifrar los datos y permitir el acceso a sólo usuarios de la UMNG.	BAJA
Robo del equipo/Acceso no autorizado	Paredes del cuarto muy débiles. Falta de mecanismos de control para el acceso no autorizado como alarmas y cámaras.	ALTA
Vandalismo.	Paredes del cuarto no reforzadas.	ALTA

4.2.6. Clasificación del impacto

Para determinar la repercusión negativa causada por la explotación de una vulnerabilidad asociada a una amenaza, basado en la clasificación del activo y el nivel de exposición, se utiliza la matriz de clasificación del impacto, según la tabla 2. En la tabla 9 se muestra la matriz de impacto resultante del

proceso de clasificación del impacto para cada una de las parejas amenaza/vulnerabilidad asociadas a cada activo. En la matriz se muestra la identificación de cada una de las parejas amenaza/vulnerabilidad y su ubicación en la matriz según el resultado obtenido.

Tabla 9 Matriz de impacto resultante de la clasificación del impacto.

CLASE DEL ACTIVO	BAJO	MEDIO	ALTO
ALTO	1.4 6.4 1.8 6.8 2.4 9.4 4.4 9.11 4.11 9.12 4.12 10.4	1.3 4.8 9.7 1.7 4.9 9.8 2.3 4.10 9.9 2.7 6.3 9.10 4.3 6.7 10.3 4.7 9.3 10.7	1.1 2.5 6.1 9.5 1.2 2.6 6.2 9.6 1.5 4.1 6.5 10.1 1.6 4.2 6.6 10.2 2.1 4.5 9.1 10.5 2.2 4.6 9.2 10.6
MEDIO	3.4 14.4 3.8 3.9 3.10 11.4 12.4	3.3 12.7 3.7 14.3 3.11 14.7 11.3 15.2 11.7 12.3	3.1 11.5 14.1 3.2 11.6 14.2 3.5 12.1 14.5 3.6 12.2 14.6 11.1 12.5 15.1 11.2 12.6
BAJO	5.4 7.4 8.4 8.9 13.4 16.1	5.3 8.3 5.7 8.7 5.8 8.8 7.3 13.3 7.7 13.7 7.8	5.1 7.5 13.1 5.2 7.6 13.2 5.5 8.1 13.5 5.6 8.2 13.6 7.1 8.5 7.2 8.6

ALTO
MEDIO
BAJO

NIVEL DE EXPOSICIÓN

4.2.7. Estimación del nivel de probabilidad

Para la estimación de la probabilidad de que se haga efectiva una amenaza debido a las facilidades existentes para explotar una vulnerabilidad del activo, se utilizó como criterios básicos los establecidos en la tabla 3 para el análisis, obteniendo la tabla 10. En la tabla se relacionan las parejas amenaza/vulnerabilidad que se detectaron en los diferentes activos *hardware* de la red.

Tabla 10 Niveles de probabilidad para cada pareja Amenaza/Vulnerabilidad

AMENAZA	VULNERABILIDAD	NIVEL DE PROBABILIDAD
Ataque por un pirata informático	Cross Site Tracing (XST). Causada por algún error de filtrado y del uso del comando TRACE de HTTP	MEDIA
Ataque por un pirata informático	Problema de configuración. Permite realizar conexiones a puertos sensibles dándole la capacidad a un atacante evitar las reglas del firewall y conectarse a puertos no permitidos.	MEDIA
Ataque por un pirata informático	Cross Site Scripting (XSS). El sistema de validación de HTML permite ejecutar scripts maliciosos	ALTA
Calentamiento del equipo	Falta de monitores de las condiciones ambientales.	MEDIA
Divulgación de información sobre el activo	Instalación predeterminada de TOMCAT	BAJA
Incendio.	Ausencia de extintores en el cuarto.	MEDIA
Incendio.	Las paredes del cuarto y la presencia de elementos como cajas puede ser factor para la propagación rápida del fuego.	MEDIA
Incendio.	En el mismo cuarto se almacena elementos ofimáticas, tales como resmas de papel y cajas.	MEDIA
Interrupción del servicio	Off-by-one buffer overflow. Versión del Apache desactualizada,	MEDIA
Interrupción del servicio	Versión de Apache con múltiples vulnerabilidades. » Buffer overflow. » Ejecución de código arbitrario. » DoS. » Cross Site Scripting (XSS)	MEDIA
Persona malintencionada	No se tiene un control de las visitas al cuarto donde se encuentra el equipo.	MEDIA
Persona malintencionada / Acceso no autorizado	El router administrado por el proveedor de Internet está ubicado en el mismo cuarto del equipo.	BAJA
Recopilar información sobre los equipos protegidos por el firewall	El firewall permite enumerar lo equipos detrás del firewall.	ALTA
Robo de credenciales	Uso de autenticación en texto plano	ALTA
Robo de identidad o suplantación.	Los switches están expuestos a ataques ARP Spoofing.	MEDIA
Robo de información	DNS Cache Snooping. El servicio de DNS permite que un tercero pueda obtener información sobre los nombre de dominio que han sido resueltos por el servidor.	MEDIA

Robo de información	No se tiene habilitado un protocolo de cifrado que permita cifrar los datos y permitir el acceso a sólo usuarios de la UMNG.	ALTA
Robo del equipo/Acceso no autorizado	Paredes del cuarto muy débiles. Falta de mecanismos de control para el acceso no autorizado como alarmas y cámaras.	BAJA
Vandalismo.	Paredes del cuarto no reforzadas.	ALTA

4.2.8. Resultado de la evaluación de riesgos

Como paso final se identificó el nivel de riesgo para cada amenaza/vulnerabilidad, de acuerdo al nivel de impacto encontrado y a la estimación del nivel de probabilidad, que fue el resultado de un análisis de probabilidad de ocurrencia de una amenaza. El método para hallar el nivel de riego es relacionando el impacto y la probabilidad como se indica en la tabla 4. El resultado final de la evaluación de riesgos es la matriz de riesgos que muestra la tabla 11, donde se encuentran cada una de las relaciones amenaza/riesgo de cada activo analizado en el correspondiente nivel.

Tabla 11 Matriz de riesgos resultante de la evaluación de riesgos

NIVEL DEL IMPACTO	BAJO	MEDIO	ALTO
ALTO	1.2 4.3 10.3 1.3 6.2 11.2 2.2 6.3 12.2 2.3 9.2 14.2 3.2 9.3 4.2 10.2	1.5 3.5 4.9 9.7 11.5 15.1 1.6 3.6 6.5 9.8 11.6 1.7 4.5 6.6 9.9 12.5 2.5 4.6 6.7 10.5 12.6 2.6 4.7 9.5 10.6 14.5 2.7 4.8 9.6 10.7 14.6	1.1 9.1 2.1 9.10 3.1 10.1 4.1 11.1 4.10 12.1 6.1 14.1
MEDIO	3.3 12.3 5.2 13.2 6.8 14.3 7.2 8.2 11.3	1.4 4.12 8.5 11.7 2.4 5.5 8.6 12.7 3.7 5.6 9.4 13.5 3.1 6.4 9.11 13.6 4.4 7.5 9.12 14.7 4.11 7.6 10.4 15.2	1.8 5.1 7.1 8.1 13.1
BAJO	5.3 7.3 8.3 13.3	3.4 7.4 12.4 3.8 7.7 13.4 3.9 8.4 13.7 3.10 8.7 14.4 5.4 8.9 5.7 11.4	5.8 7.8 8.8 16.1

ALTO
MEDIO
BAJO

NIVEL DE PROBABILIDAD

Cada uno de estos pasos se realiza para cada activo, y se registra en la tabla de resultados de la evaluación, obteniendo al finalizar los resultados mostrados en la figura 10, donde se muestra el nivel de riesgo para cada activo resultante de las amenazas y vulnerabilidades identificadas.

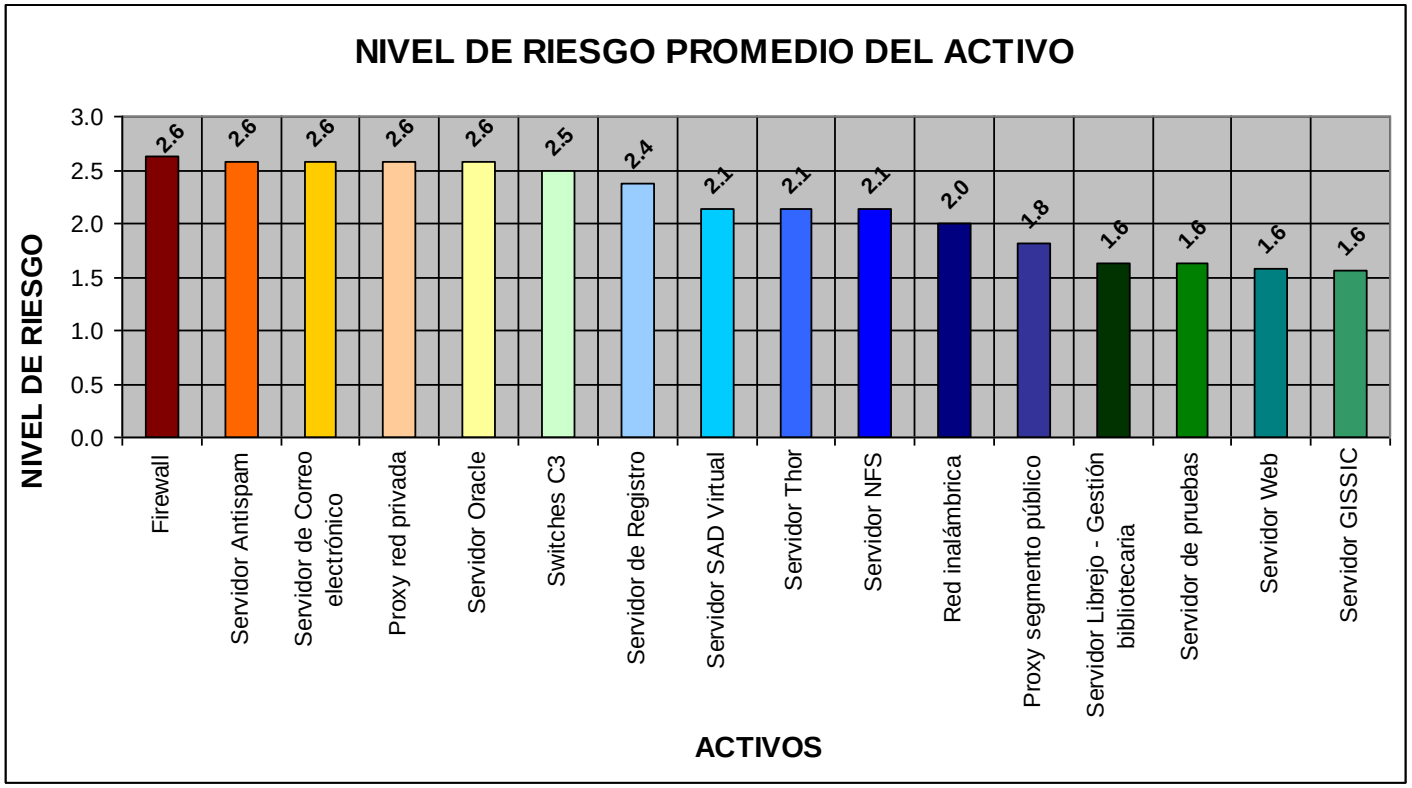

Figura 10 Nivel de riesgo obtenido en la evaluación de riesgos para los activos de la red

Donde se considera que el nivel de riesgo es **alto** si éste está entre 2.1 y 3.0, **medio** si está entre 1.1 y 2.0, y **bajo** si es menor a 1. Con esto se concluye que todos los activos evaluados están dentro de un nivel de riesgo alto y medio, ya sea por la ausencia de eficientes controles de seguridad, falta de sistemas que aporten mayor seguridad a la red, como sistemas de detección de intrusos, y otros más mecanismos para reforzar la seguridad.

Partiendo de lo anterior es que a continuación se define una metodología que permita evaluar la seguridad para dichos activos de hardware, encontrando deficiencias en la red y de alguna forma mejorar la seguridad.

4.3. METODOLOGÍA PARA EL DIAGNÓSTICO CONTINUO DE LA SEGURIDAD INFORMÁTICA DE LA RED DE DATOS DE LA UNIVERSIDAD MILITAR NUEVA GRANADA

Para la definición de la metodología se tomaron como base, principalmente, el documento **OSSTMM**, el estándar de buenas prácticas de la **ISF** y la norma **ISO/IEC 27002**, de los cuales se tuvieron en cuenta recomendaciones planteadas allí que ofrecen un gran aporte a la definición de una metodología acorde a los requerimientos de la red de datos de la UMNG. A continuación se muestra la organización de la metodología para el diagnóstico de la seguridad informática y la metodología como tal.

4.3.1. Ámbito de la metodología

La presente metodología para diagnóstico de la seguridad informática se encuentra limitada al diagnóstico en los activos dentro de la categoría de servidores, *firewall*, *Proxy*, *switches* de capa 3 y red inalámbrica, que hace parte de la red de datos de la Universidad Militar “Nueva Granada” en su sede de la calle 100.

4.3.2. Recopilar información sobre los sistemas a diagnosticar

Antes de realizar el diagnóstico de la seguridad a la red de datos y una vez definido el contexto en el cual se llevará a cabo es necesario recoger toda la información posible con los funcionarios a cargo sobre cada sistema objeto del diagnóstico. Es importante que se obtenga toda la información bajo un compromiso de confidencialidad firmado por el auditor y dirigido a la División de Informática.

4.3.3. Herramientas propuestas

A continuación se propone la utilización de unas herramientas computacionales para realizar el diagnóstico de la seguridad de la red. El uso de cualquier otra herramienta es libre mientras está no comprometa el buen funcionamiento de la red.

- WIRESHARK: Analizador de protocolos de red, que permite capturar cualquier paquete que circule por la red. Con este programa se puede verificar si por medio de la red se capturan datos sin cifrar, es decir que existe la posibilidad de que determinada aplicación envíe información confidencial que puede ser fácilmente interceptada por cualquier persona dentro de la red. [12]
- ETTERCAP: Herramienta para realizar ataques de "*man in the middle*" sobre las redes LAN, en especial en las basadas en switches. Entre sus características se encuentra las de *sniffer*, ARP *Spoofing* y otras para el análisis de redes y equipos. [13]
- NETSTUMBLER: Herramienta en Windows que permite detectar redes inalámbricas usando 802.11a, 802.11b y 802.11g, y permite identificar la presencia de redes inalámbricas inseguras, conocer la cobertura de las redes, detectar interferencias de otras redes, y otros usos más. [14]
- NESSUS: Herramienta que se utiliza para escanear uno o varios equipos de la red con el fin de encontrar sus vulnerabilidades. Con esta herramienta se puede identificar si el equipo tiene algún problema de seguridad que puede ser aprovechado por alguien para comprometer el equipo. Puede indicar si al equipo le falta algún parche o está desactualizado. [15]
- METASPLOIT FRAMEWORK: Una completa herramienta para escribir, probar y usar código exploit, que son utilizados para aprovechar las vulnerabilidades de los equipos de red. Esta herramienta es una sólida plataforma para las pruebas de penetración e investigación de vulnerabilidades. [16]
- NMAP: Herramienta de código abierto para la exploración de red y auditoria de la seguridad. Útil para realizar escaneo de puertos,

enumeración de equipos activos en una red e identificación de los sistemas operativos utilizados en cada equipo. Mediante Nmap se identifica el estado de los puertos TCP y UDP, así como los servicios que se ejecutan en el equipo junto con sus versiones. Nmap identifica los estados de los puertos de diferentes maneras de acuerdo al tipo de escaneo. [17]

- YERSINIA: Herramienta de red diseñada para aprovechar debilidades en diferentes protocolos de la capa de enlace, como STP, DTP, CDP, IEEE 802.1Q, IEEE 802.1X, VTP y otros. Permite realizar ataques de negación de servicio a dichos protocolos, ganar privilegios dentro de las redes segmentadas en VLAN's y así capturar todo el tráfico de otras VLAN's. [18]
- BackTrack: es una de las más populares herramientas para las auditorias de seguridad. BackTrack es una distribución de Linux en live-CD orientada a los profesionales de seguridad informática, y en la cual se incluye más de 300 herramientas para realizar evaluaciones de la seguridad informática, desde *sniffers*, *exploits*, auditoria *wireless*, análisis forense y otras.

4.3.4. Mapa de seguridad

"El mapa de seguridad es una imagen de la presencia de seguridad". [5] Éste se compone de varias secciones de seguridad que pueden variar de acuerdo al sistema de información, las cuales tienen elementos en común que se relacionan de forma directa e indirecta. Para la red de la Universidad se define en la Figura 11 el mapa de seguridad de acuerdo al análisis de seguridad hecho en el capítulo 4.1.2.

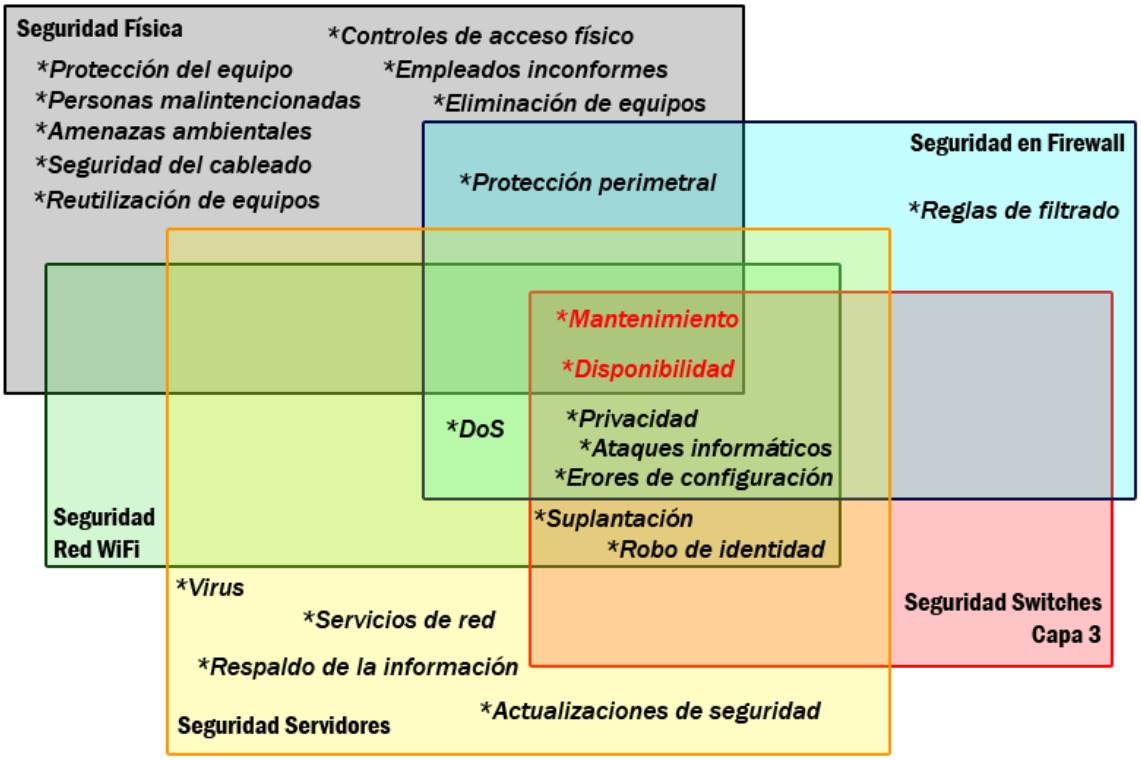

Figura 11 Mapa de seguridad para la red de la Universidad

4.3.5. Estructura de la metodología

La metodología se encuentra dividida en módulos y tareas, donde los módulos son cuatro en total y hacen referencia a los sistemas que ofrecen seguridad a la red de datos, y las tareas son las labores que se realizan para analizar el estado de la seguridad en cada módulo, de éstas se desprenden unos pasos, en los que se propone la utilización de una herramienta y la forma de utilizarla.

4.3.6. Módulo I – Seguridad física

En este módulo se busca verificar las medidas de seguridad del perímetro para los activos de la red.

- Tarea 1: Verificar los controles de acceso físico.
    - Las paredes del área deben estar sólidas y sin ninguna brecha que facilite cualquier violación.

    - Las puertas y ventanas del cuarto deben tener cerradura.
    - Presencia de un sistema de control de intrusos.
    - Registro de la entrada de visitantes.
    - El equipo se encuentra ubicado de manera que evite que cualquiera sin autorización pueda manipular las conexiones.
    - El equipo se encuentra protegido en un gabinete con cerradura o un cuarto con cerradura en la puerta y ventanas.
- Tarea 2: Verificar las protecciones contra amenazas físicas.
    - Se evita tener elementos que propaguen o provoquen un incendio dentro del cuarto.
    - Se cuenta con equipo contra incendio apropiado y acorde con los requerimientos que exige el cuarto.
    - Se debería contar con sistemas para el monitoreo de las condiciones ambientales.
- Tarea 3: Verificar el cableado en los equipos.
    - Los cables se encuentran debidamente rotulados.
    - Los cables se encuentran ordenados.
    - Los cables están protegidos evitando cualquier interceptación o daño físico.
- Tarea 4: Verificar que el cuarto cumpla con los estándares apropiados para el buen funcionamiento de los sistemas de información.

4.3.7. Módulo II – Seguridad en firewall

En este módulo se busca analizar el nivel de seguridad ofrecido por el equipo *firewall* que se encarga del filtrado de tráfico hacia y desde la red a Internet.

- Tarea 1– Verificar el funcionamiento del *firewall*: Verificar que el *firewall* está filtrando determinados tipos de paquetes que pueden ser utilizados para evadir la protección del *firewall* y efectuar un ataque a la red.
    - Verificar la posibilidad de escanear, desde un equipo en Internet, a través del *firewall* para enumeración de equipos.

      Herramienta: Nmap

      Comando: *nmap –sP* <***Dirección de red/Sufijo de la Mascara***>
    - Ejecutar un sondeo SYN desde un equipo en Internet hacia un equipo detrás del *firewall*, para descubrir puertos abiertos.

      Herramienta: Nmap

      Comando: *nmap –sS* <***Dirección IP***> *-P0*
    - Ejecutar un sondeo ACK desde un equipo en Internet hacia un equipo detrás del *firewall*.

      Herramienta: Nmap

      Comando: *nmap –sA* <***Dirección IP***> *-P0*
    - Ejecutar un sondeo WIN desde un equipo en Internet hacia un equipo detrás del *firewall*.

      Herramienta: Nmap

      Comando: *nmap –sW* <***Dirección IP***> *-P0*
    - Ejecutar un sondeo NULL desde un equipo en Internet hacia un equipo detrás del *firewall*.

      Herramienta: Nmap

      Comando: *nmap –sN* <***Dirección IP***> *-P0*

- Ejecutar un sondeo FIN desde un equipo en Internet hacia un equipo detrás del *firewall*.

  Herramienta: Nmap

  Comando: *nmap –sF <**Dirección IP**> -P0*

- Ejecutar un sondeo XMAS desde un equipo en Internet hacia un equipo detrás del *firewall*.

  Herramienta: Nmap

  Comando: *nmap –sX <**Dirección IP**> -P0*

- Desde un equipo en Internet testear la respuesta del firewall a paquetes con la bandera RST activada.

  Herramienta: Nmap

  Comando: *nmap --scanflags RST <**Dirección IP**> -P0*

- Realizar sondeos de tipo UDP para enumerar puertos UDP abiertos, cerrados o filtrados.

  Herramienta: Nmap

  Comando: *nmap –sU <**Dirección IP**> -p <rango_puertos> -P0*

- Realizar un escaneo de puertos, desde un equipo en Internet, con una dirección IP de origen falsa para determinar si el *firewall* esté haciendo detección de direcciones IP orígenes falsas.

  Herramienta: Nmap

  *Comando: nmap <**Dirección IP**> -e <**Interfaz física local**> -S <**Dirección IP Falsa**> -P0*

- Realizar un escaneo de puertos, desde un equipo en Internet, con una dirección MAC de origen falsa para determinar si el

firewall esté haciendo detección de direcciones MAC orígenes falsas hacia un equipo detrás del *firewall*.

Herramienta: Nmap

Comando: nmap <***Dirección IP***> *-e* <***Interfaz física local***> *--spoof-mac* <***Dirección MAC Falsa***> *-P0*

- Desde un equipo en Internet verificar la habilidad del firewall para manejar fragmentos de paquetes diminutos y evitar ataques por fragmentación.

  Herramienta: Nmap

  Comando 1: *nmap –f* <***Dirección IP***> *-P0*

  Comando 2: *nmap –-mtu* <***valor_fragmento***> <***Dirección IP***> *-P0*

- Verificar si el cortafuego está filtrando el tráfico de la red local hacia afuera.

- Tarea 2 – Análisis de las reglas del *firewall*: Analizar las reglas definidas en el *firewall* con el objetivo de que éstas estén acorde con la política de seguridad de la red y esté filtrando tráfico que afecte la seguridad.
  - Verificar que el *firewall* esté evitando la divulgación de información sobre la red.
  - Verificar que el *firewall* maneje controles para proteger las comunicaciones que son propensas a ser abusadas (Ej. DNS, FTP, Telnet, SMTP).
  - Verificar que el *firewall* bloqueé paquetes utilizados para realizar ataques de denegación del servicio, tales como ICMP echo, UDP y TCP echo.

- Negar todo el tráfico entrante y saliente en el que se encuentre que la dirección de origen es falsa.
- Verificar que el *firewall* esté configurado para bloquear o restringir las comunicaciones basadas en específicas direcciones y/o puertos.
- El filtrado de tráfico debería estar basado en reglas predefinidas que hayan sido elaboradas por funcionarios de confianza en base a las políticas de seguridad y requerimientos de usuarios, además cumplan las siguientes características:
  - Estar definidas bajo el principio de 'menos acceso'.
  - Estar sujetas a revisiones periódicas.
  - Estar documentadas y mantenerse actualizadas.

4.3.8. Módulo III – Seguridad en servidores

En este módulo se busca analizar la seguridad en los servidores. Determinar en qué estado se encuentra el entorno físico donde se encuentran los equipos que manejan servicios e información sensibles a la organización. Se pretende identificar la existencia de vulnerabilidades que afecten el buen funcionamiento de los servidores.

- Tarea 1 – Análisis de puertos: El análisis de puertos consiste en ejecutar diferentes tipos de sondeos a los servidores para conocer el estado de los puertos e información acerca de los servicios que están escuchando por dichos puertos. Mediante este análisis se puede detectar la presencia de *backdoors* y de puertos abiertos innecesariamente. En la **tabla 12** se encuentran los sondeos que se deben llevar a cabo desde Internet y segmento público de la red. Los comandos son para ejecutar con la herramienta propuesta Nmap.

Tabla 12 Pasos para el análisis de puertos

TIPO DE SONDEO	COMANDO
TCP SYN	*nmap -sS <**Dirección IP**> -P0*
VERSION	*nmap -sV <**Dirección IP**> -P0*
TCP ACK	*nmap -sA <**Dirección IP**> -P0*
VENTANA TCP	*nmap -sW <**Dirección IP**> -P0*
TCP NULL	*nmap -sN <**Dirección IP**> -P0*
TCP FIN	*nmap -sF <**Dirección IP**> -P0*
TCP XMAS	*nmap -sX <**Dirección IP**> -P0*
TCP RESET	*nmap --scanflags RST <**Dirección IP**> -P0*
UDP	*nmap -sU <**Dirección IP**> -p <**rango_ puertos**> -P0*

- Tarea 2 – Análisis de vulnerabilidades: Comprobar la existencia de vulnerabilidades en los servidores, con mayor grado de criticidad, que afecten el funcionamiento de los equipos.
    - Identificar las vulnerabilidades en el equipo mediante un escáner de vulnerabilidades.

      Herramienta: Nessus
    - Analizar el reporte generado por el escáner de vulnerabilidades. Enumerando los puertos abiertos y clasificando cada una de las vulnerabilidades asociadas a los puertos abiertos.
    - Mediante una herramienta que ejecute *Exploits* buscar en su base de datos de *exploits*, uno que haga referencia a las vulnerabilidades encontradas y comprobar la presencia de la vulnerabilidad, en lo posible.

      Herramienta: Metasploit Framework 3

4.3.9. Módulo IV – Seguridad en *switches* de capa 3

Este módulo buscar identificar los problemas de seguridad asociados a los switches de capa 3 utilizados en la red para la segmentación de ésta en VLAN's.

- Tarea – Análisis de vulnerabilidades: Comprobar la existencia de vulnerabilidades en los *switches*, con mayor grado de criticidad, que afecten el funcionamiento de los equipos.
    - Verificar si los switches son susceptibles a un ataque ARP spoofing.

      Herramienta: Ettercap
    - Mediante un analizador de protocolos identificar los protocolos de capa de enlace utilizados en la red.

      Herramienta: Wireshark
    - Con la ayuda de una herramienta de ataque diseñada para aprovechar las vulnerabilidades de los protocolos de capa de enlace (Ej.: VTP, STP, DTP y CDP) llevar a cabo ataques a los switches en la red.

      Herramienta: Yersinia

4.3.10. Módulo V – Seguridad en red inalámbrica 802.11

El análisis de la seguridad en las redes inalámbricas 802.11 de la Universidad es de vital importancia debido a que es una red que está expuesta físicamente a cualquier persona dentro del campo de cobertura. Las tareas a continuación pretenden encontrar los problemas de seguridad en la red inalámbrica.

- Tarea 1 – Inventario de los puntos de acceso: Enlistar los puntos de acceso instalados en el Campus con el objetivo de identificar cuales no están autorizados.
    - Solicitar al funcionario(s) encargado(s) de la administración de la red inalámbrica un listado de los puntos de acceso instalados en la red y autorizados por ellos.
    - Identificar los puntos de acceso inalámbricos dentro de toda el área de la Universidad, mediante un equipo portátil con

tarjeta de red inalámbrica y una herramienta de software que identifique los puntos de acceso a la red.

Herramienta: NetStumbler

- Tarea 2 – Análisis general de la WLAN: Con un equipo portátil con conexión a la red inalámbrica de la Universidad realizar los siguientes pasos:
    - Realizar un mapeo de la red para identificar los puntos de acceso (AP) inalámbrico, encontrando sus direcciones IP.

      Herramienta: Nmap

      Comando: nmap –sP <Segmento de red: 10.0.0.0/16>
    - Verificar que los puntos de acceso tienen habilitado un sistema de cifrado para el tráfico de la red (Ej.: WEP y WPA).

      Herramienta: Wireshark
    - Con un explorador de Internet acceder a las direcciones de los AP e intentar acceder a la configuración con el usuario y contraseña *admin*.

4.3.11. Plantillas para el reporte de resultados

Las siguientes plantillas son para llevar el seguimiento del diagnóstico de seguridad y necesarias para el análisis de resultados de este proceso.

- Plantilla para la verificación del funcionamiento del firewall: En la tabla 13 se debe ingresar los resultados obtenidos al realizar la tarea 1 del módulo II.

Tabla 13 Plantilla de resultados para la verificación del *Firewall*

ENUMERACIÓN DE EQUIPOS		
No.	**Equipos encontrados**	**Equipo detrás del *firewall***
1		☐ SÍ ☐ NO
2		☐ SÍ ☐ NO
3		☐ SÍ ☐ NO
Sondeo SYN		

Equipo		No.	Puerto abierto	Servicio
		1		
		2		
		3		
Sondeo ACK				
Equipo		**No.**	**Puerto abierto**	**Servicio**
		1		
		2		
		3		
Sondeo WIN				
Equipo		**No.**	**Puerto abierto**	**Servicio**
		1		
		2		
		3		
Sondeo NULL				
Equipo		**No.**	**Puerto abierto**	**Servicio**
		1		
		2		
		3		
Sondeo FIN				
Equipo		**No.**	**Puerto abierto**	**Servicio**
		1		
		2		
		3		
Sondeo XMAS				
Equipo		**No.**	**Puerto abierto**	**Servicio**
		1		
		2		
		3		
Sondeo RESET				
Equipo		**No.**	**Puerto abierto**	**Servicio**
		1		
		2		
		3		
Sondeo UDP				
Equipo		**No.**	**Puerto abierto**	**Servicio**
Puertos:		1		
		2		
		3		
Respuesta a la falsificación de dirección IP origen				
Puerto	**Estado**		**Respuesta es correcta**	
			☐ SÍ ☐ NO	
Respuesta a la falsificación de dirección MAC origen				
Puerto	**Estado**		**Respuesta es correcta**	
			☐ SÍ ☐ NO	
Respuesta a fragmentos de paquetes pequeños				
Puerto	**Estado**		**Respuesta es correcta**	
			☐ SÍ ☐ NO	

- Plantilla para el análisis de puertos en servidores: En la tabla 14 se debe ingresar los resultados obtenidos al realizar el escaneo de puertos para cada equipo, hecho en la tarea 1 del Módulo III.

Tabla 14 Plantilla para el análisis de puertos

Equipo	***Dirección IP***	***Nombre del equipo***	
Sondeo SYN			
No.	**Puerto abierto**	**Servicio**	**Observaciones**
1			
2			
3			
Sondeo VERSION			
No.	**Puerto/Servicio**	**Versión**	
1			
2			
3			
Sondeo ACK			
No.	**Puerto abierto**	**Servicio**	**Observaciones**
1			
2			
3			
Sondeo WIN			
No.	**Puerto abierto**	**Servicio**	**Observaciones**
1			
2			
3			
Sondeo NULL			
No.	**Puerto abierto**	**Servicio**	**Observaciones**
1			
2			
3			
Sondeo FIN			
No.	**Puerto abierto**	**Servicio**	**Observaciones**
1			
2			
3			
Sondeo XMAS			
No.	**Puerto abierto**	**Servicio**	**Observaciones**
1			
2			
3			
Sondeo RESET			
No.	**Puerto abierto**	**Servicio**	**Observaciones**
1			
2			
3			
Sondeo UDP			
No.	**Puerto abierto**	**Servicio**	**Observaciones**

1			
2			
3			

- Plantilla para el análisis de vulnerabilidades en servidores: En la tabla 15 se debe hacer una breve descripción de los resultados obtenidos en el análisis de vulnerabilidades hecho a cada equipo, de acuerdo a la tarea 2 del Módulo III.

Tabla 15 Plantilla para el análisis de vulnerabilidades

Equipo	***Dirección IP***	***Nombre del equipo***	
Puerto / Servicio	**Vulnerabilidad**	**Descripción**	**Factor de riesgo**

4.3.12. Análisis de resultados del diagnóstico de seguridad

Para el análisis de resultados del diagnóstico realizado de acuerdo a los módulos y tareas definidos anteriormente, a continuación se dan las indicaciones para realizar el análisis de la seguridad de los equipos y sistemas involucrados en el diagnóstico, enmarcando los resultados obtenidos dentro de cinco principios de seguridad. Con ésto se determinara cual es el grado de criticidad de cada uno, mediante una calificación de 1 a 4, donde 1 es la mejor calificación y 4 la peor. Para este análisis se utilizará la tabla 16 que permitirá identificar el grado de criticidad en se encuentra un sistema o equipo, en cuanto a seguridad.

Tabla 16 Plantilla para la **e**valuación de la seguridad del sistema o equipo de acuerdo a los principios de seguridad

PRINCIPIO DE SEGURIDAD	**PESO**	**CALIFICACIÓN (1 hasta 4)**	**PESO PONDERADO (Peso * Calificación)**
Control de acceso	0,13		
Autenticación	0,12		
Integridad	0,25		
Confidencialidad	0,25		
Disponibilidad	0,25		

TOTAL	**1**		

En la primera columna se encuentran los principios de seguridad que se tendrán en cuenta para evaluar como se encuentra el sistema en lo referente a la seguridad; La segunda columna es para el peso, que es un valor entre 0 y 1 cuya suma total de todos los principios es 1; la calificación se ubica en la tercera columna y es un valor de 1, 2, 3, y 4, para Muy bueno, bueno, regular y malo respectivamente; y la última columna se calcula el peso ponderado, que es el producto entre el peso y la calificación, y cuyo valor total indica en qué grado de criticidad se encuentra la seguridad del sistema.

La seguridad informática se fundamenta principalmente en tres principios, que son **Confidencialidad**, **Integridad** y **Disponibilidad**, por esta razón el peso asignado para cada uno de ellos es de 25%, mientras que los dos restantes, control de acceso y autenticación, que no son menos importantes ya que están relacionados con los tres anteriores, y que por su finalidad de garantizar acceso autorizado auténtico a los recursos de un sistema informático los complementa reforzando la seguridad informática. Entre estos dos últimos se reparte el 25% restante para completar el total de 1, de esta manera, un 13% para el control de acceso y 12% para la autenticación. A continuación se relacionan la forma de calificar cada principio.

- Control de acceso: Para calificar este aspecto se parte de que cada equipo debe tener controles que eviten su acceso no autorizado de forma física y por medio de la red desde un equipo remoto. Los niveles de evaluación son los siguientes:
    - Nivel 1 – Muy bueno: Se cuenta con una muy buena protección perimetral física del equipo y existen mecanismos para evitar el acceso no privilegiado al equipo desde la red (Ej.: Listas de acceso)
    - Nivel 2 – Bueno: Se cuenta con una buena protección perimetral física del equipo y existen mecanismos para evitar

el acceso no privilegiado al equipo desde la red (Ej.: Listas de acceso)

- Nivel 3 – Regular: Se cuenta con una deficiente protección perimetral física del equipo y no hay eficientes mecanismos para evitar el acceso no privilegiado al equipo desde la red (Ej.: Listas de acceso)
- Nivel 4 – Malo: Se cuenta con una muy deficiente protección perimetral física del equipo ni existen mecanismos para evitar el acceso no privilegiado al equipo desde la red (Ej.: Listas de acceso)

- Autenticación: Para calificar este aspecto se parte de las formas utilizadas para la autenticación de usuarios.
  - Nivel 1 – Muy bueno: Se utilizan mecanismo para manejar autenticación fuerte para acceder a los servicios y administración remota de los equipos (Ej.: Uso de un Token y contraseña de usuario). No se accede remotamente mediante el usuario root.
  - Nivel 2 – Bueno: Se hace uso de autenticación fuerte para acceder a los servicios y administración remota de los equipos (Ej.: Uso de un Token y contraseña de usuario), pero no se lleva a cabo bajo un protocolo cifrado. No se accede remotamente mediante el usuario root.
  - Nivel 3 – Regular: Se hace uso de autenticación sencilla (Ej. Sólo uso de contraseña de usuario) de acuerdo a unas guías de contraseñas seguras para acceder a los servicios y administración remota de los equipos mediante un protocolo cifrado. Se permite el acceso remoto mediante el usuario root para la administración de los equipos.

    - Nivel 4 – Malo: No se tiene habilitada la autenticación o se hace uso de autenticación sencilla sin la aplicación de guías de contraseñas seguras ni mediante un protocolo cifrado para acceder a los servicios y administración remota de los equipos. Se utilizan usuarios y contraseñas por defecto para acceder remotamente a la administración de los equipos.

- Integridad: Para calificar este aspecto se tiene en cuenta la utilización de algoritmos que permitan establecer la integridad de la información trasmitida y la prevención de ataques Man-in-the-middle.
    - Nivel 1 – Muy bueno: Se utilizan firmas digitales y mecanismo para evitar ataques Man-in-the-middle.
    - Nivel 2 – Bueno: Se utiliza un algoritmo de resumen de mensaje o mensaje digest (Ej.: MD5) y mecanismo para evitar ataques Man-in-the-middle.
    - Nivel 3 – Regular: No se utiliza un algoritmo de resumen de mensaje o mensaje digest, pero si mecanismo para evitar ataques Man-in-the-middle.
    - Nivel 4 – Malo: No se utiliza un algoritmo de resumen de mensaje o mensaje digest ni mecanismo para evitar ataques Man-in-the-middle.
- Confidencialidad: Se tiene en cuenta la utilización de algoritmos de cifrado durante la comunicación para ofrecer una comunicación privada o el uso de protocolos seguros para la administración remota de los equipos.
    - Nivel 1 – Muy bueno: Se utiliza un algoritmo de cifrado robusto de clave pública para la comunicación.

    - Nivel 2 – Bueno: Se utiliza un algoritmo de cifrado de clave pública o un protocolo seguro (Ej.: SSH) para la comunicación remota con una configuración avanzada.
    - Nivel 3 – Regular: Uso de un algoritmo de cifrado simétrico o un protocolo seguro (Ej.: SSH) para la comunicación remota con la configuración predeterminada.
    - Nivel 4 – Malo: No se utiliza ningún algoritmo de cifrado ni protocolo seguro.
- Disponibilidad: Para calificar este aspecto se analiza la susceptibilidad a que se presente una caída del equipo o sistema y se vea afectado el servicio correspondiente.
    - Nivel 1 – Muy bueno: No es susceptible a ataques de DoS y se tiene equipos que respalden sus funciones. La prestación del servicio es continua.
    - Nivel 2 – Bueno: Susceptible a ataques de DoS, pero se tienen equipos que respalden sus funciones. La prestación del servicio es continua.
    - Nivel 3 – Regular: No susceptible a ataques de DoS, pero no se tiene equipos que respalden sus funciones. Además presenta interrupciones de los servicios.
    - Nivel 4 – Malo: Susceptible a ataques de DoS y no se tiene equipos que respalden sus funciones. La continuidad del servicio es deficiente.

Como resultado final se busca conocer la calificación obtenida para toda la red en general, y esto se hace tomando las calificaciones a los principios de cada uno de los activos y promediarlos de acuerdo a una clasificación dada, entre alta (3), media (2) y baja (1), que determina el papel de cada activo en la red. Para ésto se aplica la siguiente fórmula matemática.

$$\overline{Calificaci\acute{o}n} = \frac{\sum(Clasificaci\acute{o}nActivo \times Calificaci\acute{o}nPrincipio)}{\sum Clasificaci\acute{o}nActivo}$$

Teniendo cada una de las calificaciones se ingresan a la tabla 17 y se calcula el total.

Tabla 17 Plantilla para la evaluación de la seguridad de la red de datos de acuerdo a los principios de seguridad

	Red de datos UMNG		
PRINCIPIO DE SEGURIDAD	**PESO**	**CALIFICACIÓN (1 hasta 4)**	**PESO PONDERADO (Peso * Calificación)**
Control de acceso	0,13	$\overline{Calificaci\acute{o}n}$	
Autenticación	0,12	$\overline{Calificaci\acute{o}n}$	
Integridad	0,25	$\overline{Calificaci\acute{o}n}$	
Confidencialidad	0,25	$\overline{Calificaci\acute{o}n}$	
Disponibilidad	0,25	$\overline{Calificaci\acute{o}n}$	
TOTAL	**1**	----	

4.4. ANÁLISIS DE RESULTADOS DEL DIAGNÓSTICO DE SEGURIDAD

A continuación se presentan los resultados obtenidos por la ejecución del diagnóstico de seguridad realizado a la red de datos de la UMNG. Las pruebas fueron realizadas de acuerdo a la metodología para el diagnóstico continuo de la seguridad informática de la red de datos de la Universidad Militar Nueva Granada (MDCSIRD).

4.4.1. Diagnóstico al *firewall*

En la Tabla 18 se encuentran los resultados de la verificación del funcionamiento del *firewall*, que consistieron en la ejecución de diferentes tipos de escaneos hechos desde un equipo fuera de la red, es decir en un entorno con menos privilegios sobre la red de la institución. Cada una de las pruebas fue realizada por medio de escaneos al equipo “Multi-servidores”, que se encuentra detrás del *firewall*, el cual se encontró previamente tenía el

puerto 80/HTTP abierto, debido a que este equipo presta el servicio de página Web.

Tabla 18 Resultados del diagnóstico al *firewall*

ENUMERACIÓN DE EQUIPOS				
No.	**Equipos encontrados**	**Equipo detrás del *firewall***		
1	64.76.51.1	☐ SÍ	☑ NO	
2	64.76.51.41	☐ SÍ	☑ NO	
Sondeo SYN				
Equipo	**Multi-servidores**	**No.**	**Puerto abierto**	**Servicio**
		1	80	http
Comentarios:	El puerto abierto se debe a que el equipo presta el servicio de página Web.			
Sondeo ACK				
Equipo	**Multi-servidores**	**No.**	**Puerto abierto**	**Servicio**
		1	NINGUNO	
Comentarios:	Se encontraron todos los puertos filtrados, lo que indica que el firewall tiene la capacidad de bloquear técnicas de enumeración con paquetes TCP ACK.			
Sondeo WIN				
Equipo	**Multi-servidores**	**No.**	**Puerto abierto**	**Servicio**
		1	NINGUNO	
Comentarios:	Se encontraron todos los puertos filtrados, lo que indica que el firewall tiene la capacidad de bloquear técnicas de enumeración con paquetes TCP WIN.			
Sondeo NULL				
Equipo	**Multi-servidores**	**No.**	**Puerto abierto**	**Servicio**
		1	NINGUNO	
Comentarios:	Se encontraron todos los puertos *open|filtered*, lo que indica que el firewall tiene la capacidad de bloquear técnicas de enumeración con paquetes TCP NULL.			
Sondeo FIN				
Equipo	**Multi-servidores**	**No.**	**Puerto abierto**	**Servicio**
		1	NINGUNO	
Comentarios:	Se encontraron todos los puertos *open|filtered*, lo que indica que el firewall tiene la capacidad de bloquear técnicas de enumeración con paquetes TCP FIN.			
Sondeo XMAS				
Equipo	**Multi-servidores**	**No.**	**Puerto abierto**	**Servicio**
		1	NINGUNO	
Comentarios:	Se encontraron todos los puertos *open|filtered*, lo que indica que el firewall tiene la capacidad de bloquear técnicas de enumeración con paquetes TCP con todas las banderas activas.			
Sondeo RESET				
Equipo	**Multi-servidores**	**No.**	**Puerto abierto**	**Servicio**
		1	NINGUNO	
Comentarios:	Se encontraron todos los puertos filtrados, lo que indica que el firewall tiene la capacidad de bloquear técnicas de enumeración con paquetes TCP ACK.			

Sondeo UDP				
Equipo	**Multi-servidores**	**No.**	**Puerto abierto**	**Servicio**
		1	NINGUNO	
Comentarios:	Se encontraron todos los puertos UDP filtrados, lo que indica que el firewall está configurado para filtrar paquetes UDP.			

Respuesta a la falsificación de dirección IP origen			
Equipo	**Puerto**	**Estado**	**Respuesta es correcta**
Multi-servidores	80	filtered	☐ SÍ ☑ NO
Comentarios:	La respuesta es incorrecta porque no corresponde al estado real del puerto, lo que se debe a que el firewall está configurado para evitar direcciones IP de origen falsas.		

Respuesta a la falsificación de dirección MAC origen			
Equipo	**Puerto**	**Estado**	**Respuesta es correcta**
Multi-servidores	80	filtered	☐ SÍ ☑ NO
Comentarios:	La respuesta es incorrecta porque no corresponde al estado real del puerto, lo que se debe a que el firewall está configurado para evitar direcciones MAC de origen falsas.		

Respuesta a fragmentos de paquetes pequeños			
Equipo	**Puerto**	**Estado**	**Respuesta es correcta**
Multi-servidores	80	Open|filtered	☐ SÍ ☑ NO
Comentarios:	La respuesta es incorrecta porque no corresponde al estado real del puerto, lo que se debe a que el firewall no es susceptible a ataques por fragmentación.		

Con los anteriores resultados se puede llegar a las siguientes conclusiones:

- El *firewall* no permite la enumeración de equipos detrás de él, lo que evita que un atacante pueda preparar un ataque hacia un equipo dentro de la red de la institución.
- El *firewall* no permite la enumeración de equipos detrás de él, lo que evita que un atacante pueda preparar un ataque hacia un equipo dentro de la red de la institución.
- El *firewall* está filtrando los escaneos TCP ACK, WIN, NULL, FIN, XMAS, RESET y los UDP, que ayudan a un atacante a obtener mayor información sobre los equipos detrás de él.
- El *firewall* está evitando los paquetes cuyas dirección IP y/o MAC de origen son falsas, lo que permite durante un ataque tener un registro del equipo que lanza el ataque.

- Como punto negativo el *firewall* permite la realización de escaneos TCP SYN para encontrar puertos abiertos y las versiones de los servicios que se ejecutan en dicho puertos.

De acuerdo a la verificación del entorno físico se encontró que el cuarto donde está el equipo no cumple con los estándares para alojar sistemas de información ni con controles de seguridad adecuados, dentro de los cuales se relacionan algunos a continuación.

- El equipo se encuentra ubicado físicamente en un cuarto con un perímetro de seguridad frágil, que podría ser susceptible a una fácil intrusión, debido a que cuenta con paredes frágiles, puertas inseguras y sin controles de acceso muy efectivos.
- El cuarto contiene materiales que podrían facilitar la propagación del fuego, como cajas almacenadas y paredes de un material inadecuado.
- El cuarto no cuenta con extintores de fuego cerca.
- No se tiene implementado monitores ambientales para controlar la temperatura del equipo.

4.4.2. Diagnóstico a los servidores en la red

Los siguientes resultados se obtuvieron al realizar las tareas del Módulo II de la metodología MDCSIRD las cuales consistieron de un análisis del entorno físico donde se examinaron los controles en cuanto a la protección física del equipo, un análisis de puertos y por último un análisis de vulnerabilidades.

- Resultados del análisis del entorno físico: Los servidores en la red se encuentran ubicados dentro del mismo cuarto por lo que la verificación del entorno físico aplica para todos los servidores. En dicha verificación se encontró que el cuarto de servidores no cumple con los estándares para alojar sistemas de información ni con

controles de seguridad adecuados, dentro de los cuales se relacionan algunos a continuación.

- El equipo se encuentra ubicado físicamente en un cuarto con un perímetro de seguridad frágil, que podría ser susceptible a una fácil intrusión, debido a que cuenta con paredes frágiles, puertas inseguras y sin controles de acceso muy efectivos.
- No se lleva de forma estricta un control de visitas al cuarto.
- El cuarto contiene materiales que podrían facilitar la propagación del fuego, como cajas almacenadas y paredes de un material inadecuado.
- El cuarto no cuenta con extintores de fuego cerca.
- No se tiene implementado monitores ambientales en el cuarto.
- Los cables de red no se encuentran debidamente rotulados ni ordenados.

- Resultados del análisis de puertos a los servidores en la red: A continuación se muestran los resultados que arrojaron los escaneos de tipo TCP SYN y VERSION hechos según las indicaciones en la metodología MDCSIRD para el análisis de puertos en los servidores de la red. En las siguientes tablas se indican los puertos que se encontraron abiertos en cada equipo, además se relaciona la versión de la aplicación que está escuchando por cada puerto. Los siguientes resultados fueron de pruebas hechas desde un equipo en Internet.

Tabla 19 Resultado del análisis de puertos para el servidor Antispam

Equipo		**Servidor Antispam**	
Sondeo SYN			
No.	**Puerto abierto**	**Servicio**	**Observaciones**
1	25/tcp	smtp	Para el servicio de correo electrónico.
2	80/tcp	http	Para el acceso al correo desde un *Web browser*.

3	81/tcp	http	Abierto innecesariamente.
4	110/tcp	pop3	Para el servicio de correo electrónico.
Sondeo VERSION			
No.	**Puerto/Servicio**	**Versión**	
1	25/smtp	OpenBSD spamd	
2	80/http	Apache httpd 1.3.33 ((Debian GNU/Linux) PHP/4.3.10-22)	
3	81/http	Apache httpd 1.3.33 ((Debian GNU/Linux))	
4	110/pop3	qmail pop3d	
Comentarios			
Los puertos abiertos corresponden a los servicios autorizados para ser usados desde Internet. En el puerto 81/TCP está corriendo una página Web que no se está usando y que está mostrando la página resultante de una instalación del Apache, que además muestra información del equipo.			

Tabla 20 Resultado del análisis de puertos para el servidor Web

Equipo		**Servidor Web**	
Sondeo SYN			
No.	**Puerto abierto**	**Servicio**	**Observaciones**
1	80/tcp	http	Para la página Web pública de la institución
Sondeo VERSION			
No.	**Puerto/Servicio**	**Versión**	
1	80/http	Apache Tomcat/Coyote JSP engine 1.1	
Comentarios			
El puerto abierto corresponde al servicio autorizado de página Web pública.			

Tabla 21 Resultado del análisis de puertos para el Proxy del segmento público

Equipo		**Proxy segmento público**	
Sondeo SYN			
No.	**Puerto abierto**	**Servicio**	**Observaciones**
1	80/tcp	http	Para prestar el servicio de *Proxy*.
2	81/tcp	http	Abierto innecesariamente.
Sondeo VERSION			
No.	**Puerto/Servicio**	**Versión**	
1	80/http	Apache httpd 1.3.33 ((Debian GNU/Linux))	
2	81/http	Apache httpd 2.0.55 ((Ubuntu) PHP/4.4.2-1build1)	
Comentarios			
El puerto abierto corresponde al servicio autorizado de página Web pública. En el puerto 81/TCP está corriendo una página Web que no se está usando y que está mostrando la página resultante de una instalación del Apache, que además muestra información del equipo.			

Tabla 22 Resultado del análisis de puertos para el servidor Librejo

Equipo		**Servidor Librejo - Gestión bibliotecaria**	
Sondeo SYN			
No.	**Puerto abierto**	**Servicio**	**Observaciones**
1	80/tcp	http	Para la página Web de la aplicación

			bibliotecaria.
2	3389/tcp	microsoft-rdp	Para acceso remoto al escritorio del equipo.
Sondeo VERSION			
No.	**Puerto/Servicio**	**Versión**	
1	80/http	Microsoft IIS webserver 6.0	
2	3389/microsoft-rdp	Microsoft Terminal Service	
Comentarios			
El puerto abierto corresponde al servicio autorizado de página Web pública. En el puerto 3389/TCP está corriendo el servicio de escritorio remoto de Windows, con el fin de brindar soporte desde Internet. Se recomienda evaluar la necesidad de usar este servicio en lugar del uso de una VPN.			

Tabla 23 Resultado del análisis de puertos para el servidor de registro

Equipo		**Servidor de Registro**	
Sondeo SYN			
No.	**Puerto abierto**	**Servicio**	**Observaciones**
1	80/tcp	http	Abierto innecesariamente.
Sondeo VERSION			
No.	**Puerto/Servicio**	**Versión**	
1	80/http	Apache Tomcat/Coyote JSP engine 1.1	
Comentarios			
En el puerto abierto está corriendo una página Web que no se está usando y que está mostrando la página resultante de una instalación del Apache, que además muestra información sobre la instalación en el equipo.			

Tabla 24 Resultado del análisis de puertos para el servidor de pruebas

Equipo		**Servidor de pruebas**	
Sondeo SYN			
No.	**Puerto abierto**	**Servicio**	**Observaciones**
1	8080/tcp	http	Abierto innecesariamente.
Sondeo VERSION			
No.	**Puerto/Servicio**	**Versión**	
1	8080/http	Apache Tomcat/Coyote JSP engine 1.1	
Comentarios			
En el puerto abierto está corriendo una página Web que no se está usando y que está mostrando la página resultante de una instalación del Apache, que además muestra información sobre la instalación en el equipo.			

Tabla 25 Resultado del análisis de puertos para el servidor GISSIC

Equipo		**Servidor GISSIC**	
Sondeo SYN			
No.	**Puerto abierto**	**Servicio**	**Observaciones**
1	80/tcp	http	Para la página Web pública del grupo de investigación GISSIC.
Sondeo VERSION			
No.	**Puerto/Servicio**	**Versión**	

1	80/http	Apache httpd 2.2.0 ((Fedora))
Comentarios		
El puerto abierto corresponde al servicio autorizado de página Web pública.		

Tabla 26 Resultado del análisis de puertos para el servidor de correo electrónico

Equipo		**Servidor de Correo electrónico**	
Sondeo SYN			
No.	**Puerto abierto**	**Servicio**	**Observaciones**
1	25/tcp	smtp	Para prestar el servicio de correo.
2	80/tcp	http	Para prestar el servicio de correo por medio de *Web browser*.
3	110/tcp	pop3	Para prestar el servicio de correo.
Sondeo VERSION			
No.	**Puerto/Servicio**	**Versión**	
1	25/smtp	qmail smtpd	
2	80/http	Apache httpd 1.3.33 ((Debian GNU/Linux) PHP/4.3.10-22)	
3	110/pop3	qmail pop3d	
Comentarios			
Los puertos abiertos corresponden a los servicios autorizados de correo para ser usados desde Internet.			

Los siguientes resultados fueron de pruebas hechas desde un equipo en la red inalámbrica de la institución.

Tabla 27 Resultado del análisis de puertos para el proxy del segmento público hecho desde la red inalámbrica

Equipo		**Proxy segmento público**	
Sondeo SYN			
No.	**Puerto abierto**	**Servicio**	**Observaciones**
1	80/tcp	http	Para prestar el servicio de *Proxy*.
2	3128/tcp	squid-http	Para prestar el servicio de *Proxy*.
Sondeo VERSION			
No.	**Puerto/Servicio**	**Versión**	
1	80/http	Apache httpd 1.3.33 ((Debian GNU/Linux))	
2	3128/squid-http	Apache httpd 1.3.33 ((Debian GNU/Linux))	
Equipo	**64.76.51.10**	**Proxy segmento público**	
Sondeo SYN			
No.	**Puerto abierto**	**Servicio**	**Observaciones**
1	80/tcp	http	Para prestar el servicio de *Proxy*.
2	81/tcp	http	Abierto innecesariamente.
Sondeo VERSION			
No.	**Puerto/Servicio**	**Versión**	

1	80/http	Apache httpd 1.3.33 ((Debian GNU/Linux))
2	81/http	Apache httpd 2.0.55 ((Ubuntu) PHP/4.4.2-1build1)
Comentarios		
Los puertos abiertos corresponden al servicio de proxy para los equipos en el segmento público de la red en la institución. En el puerto 81/TCP está corriendo una página Web que no se está usando y que está mostrando la página resultante de una instalación del Apache, que además muestra información del equipo.		

Tabla 28 Resultado del análisis de puertos para el servidor Antispam hecho desde la red inalámbrica

Equipo		**Servidor Antispam**	
Sondeo SYN			
No.	**Puerto abierto**	**Servicio**	**Observaciones**
1	25/tcp	smtp	Para el servicio de correo electrónico.
2	53/tcp	domain	Para el servicio de DNS.
3	80/tcp	http	Para el acceso al correo desde un *Web browser*.
4	81/tcp	http	Abierto innecesariamente.
5	110/tcp	pop3	Para el servicio de correo electrónico.
6	587/tcp	smtp	Para el servicio de correo electrónico.
Sondeo VERSION			
No.	**Puerto/Servicio**	**Versión**	
1	25/smtp	OpenBSD spamd	
2	53/domain	ISC Bind 9.X	
3	80/http	Apache httpd 1.3.33 ((Debian GNU/Linux) PHP/4.3.10-22)	
4	81/http	Apache httpd 1.3.33 ((Debian GNU/Linux))	
5	110/pop3	qmail pop3d	
6	587/smtp	Sendmail 8.13.4	
Comentarios			
Los puertos abiertos corresponden a los servicios autorizados de correo y DNS para ser usados por los equipos en el segmento público de la red en la institución. En el puerto 81/TCP está corriendo una página Web que no se está usando y que está mostrando la página resultante de una instalación del Apache, que además muestra información del equipo.			

Tabla 29 Resultado del análisis de puertos para el servidor Web hecho desde la red inalámbrica

Equipo		**Servidor Web**	
Sondeo SYN			
No.	**Puerto abierto**	**Servicio**	**Observaciones**
1	21/tcp	ftp	Abierto innecesariamente.
2	22/tcp	ssh	Abierto innecesariamente.
3	80/tcp	http	Para la página Web pública de la institución.
4	111/tcp	rpcbind	Abierto innecesariamente.
5	898/tcp	sun-manageconsole	Abierto innecesariamente.
6	4045/tcp	nlockmgr	Abierto innecesariamente.

7	7100/tcp	tcpwrapped	Abierto innecesariamente.
8	8080/tcp	http	Abierto innecesariamente.
Sondeo VERSION			
No.	**Puerto/Servicio**	**Versión**	
1	21/ftp	No identificado.	
2	22/ssh	SunSSH 1.1 (protocol 2.0)	
3	80/http	Apache Tomcat/Coyote JSP engine 1.1	
4	111/rpcbind	2-4 (rpc #100000)	
5	898/sun-manageconsole	No identificado.	
6	4045/nlockmgr	1-4 (rpc #100021)	
7	7100/tcpwrapped	No identificado.	
8	8080/http	Apache httpd 2.0.53 ((Unix) DAV/2)	
Comentarios			
El puerto 80/TCP corresponde al servicio de página Web pública. Los demás puertos corresponden a servicios que en lo posible no deberían estar disponibles a los usuarios en el segmento público.			

Tabla 30 Resultado del análisis de puertos para el servidor general Multi-servidores hecho desde la red inalámbrica

Equipo		**Servidor General Multi-servidores**	
Sondeo SYN			
No.	**Puerto abierto**	**Servicio**	**Observaciones**
1	22/tcp	ssh	Abierto innecesariamente.
2	80/tcp	http	Para el servicio de página Web.
3	111/tcp	rpcbind	Abierto innecesariamente.
4	4045/tcp	nlockmgr	Abierto innecesariamente.
5	7100/tcp	tcpwrapped	Abierto innecesariamente.
6	32771/tcp	status	Abierto innecesariamente.
7	32772/tcp	fmproduct	Abierto innecesariamente.
8	32773/tcp	mdcommd	Abierto innecesariamente.
9	32774/tcp	metad	Abierto innecesariamente.
10	32775/tcp	rpc.metamedd	Abierto innecesariamente.
11	32776/tcp	metamhd	Abierto innecesariamente.
12	32777/tcp	rpc	Abierto innecesariamente.
Sondeo VERSION			
No.	**Puerto/Servicio**	**Versión**	
1	22/ssh	SunSSH 1.1 (protocol 2.0)	
2	80/http	Squid webproxy 2.5.STABLE9	
3	111/rpcbind	No identificado.	
4	4045/nlockmgr	No identificado.	
5	7100/tcpwrapped	No identificado.	
6	32771/status	1 (rpc #100024)	
7	32772/fmproduct	1 (rpc #1073741824)	
8	32773/mdcommd	1 (rpc #100422)	
9	32774/metad	1-2 (rpc #100229)	
10	32775/rpc.metamedd	1 (rpc #100242)	

11	32776/metamhd	1 (rpc #100230)
12	32777/rpc	No identificado.
Comentarios		
El puerto 80/TCP corresponde al servicio de página Web pública. Los demás puertos corresponden a servicios que en lo posible no deberían estar disponibles a los usuarios en el segmento público.		

Tabla 31 Resultado del análisis de puertos para el proxy de la red interna hecho desde la red inalámbrica

Equipo		**Proxy red interna**	
Sondeo SYN			
No.	**Puerto abierto**	**Servicio**	**Observaciones**
1	80/tcp	http	Para prestar el servicio de *Proxy*.
2	3128/tcp	squid-http	Para prestar el servicio de *Proxy*.
Sondeo VERSION			
No.	**Puerto/Servicio**	**Versión**	
1	80/http	Apache httpd 1.3.33 ((Debian GNU/Linux))	
2	3128/squid-http	Apache httpd 1.3.33 ((Debian GNU/Linux))	
Comentarios			
Los puertos abiertos corresponden al servicio de proxy para los equipos en la red privada de la red en la institución.			

Tabla 32 Resultado del análisis de puertos para el servidor Oracle hecho desde la red inalámbrica

Equipo		**Servidor Oracle**	
Sondeo SYN			
No.	**Puerto abierto**	**Servicio**	**Observaciones**
1	22/tcp	Ssh	Abierto innecesariamente.
2	80/tcp	http	Abierto innecesariamente.
3	111/tcp	rpcbind	Abierto innecesariamente.
4	898/tcp	http	Abierto innecesariamente.
5	1521/tcp	oracle-tns	Abierto innecesariamente.
6	8080/tcp	http	Abierto innecesariamente.
7	32773/tcp	sometimes-rpc9	Abierto innecesariamente.
Sondeo VERSION			
No.	**Puerto/Servicio**	**Versión**	
1	22/ssh	SunSSH 1.1 (protocol 2.0)	
2	80/http	Squid webproxy 2.5.STABLE9	
3	111/rpcbind		
4	898/http	Solaris management console server (Java 1.4.2_04; Tomcat 2.1; SunOS 5.9 sparc)	
5	1521/oracle-tns	Oracle TNS Listener	
6	8080/http	No identificado.	
7	32773/sometimes-rpc9	No identificado.	

Comentarios
Los puertos abiertos en este equipo corresponden a servicios que en lo posible no deberían estar disponibles para los usuarios en el segmento público.

Tabla 33 Resultado del análisis de puertos para el servidor Librejo hecho desde la red inalámbrica

Equipo		Servidor Librejo - Gestión bibliotecaria	
Sondeo SYN			
No.	**Puerto abierto**	**Servicio**	**Observaciones**
1	80/tcp	http	Para la página Web de la aplicación bibliotecaria.
2	3389/tcp	microsoft-rdp	Para acceso remoto al escritorio del equipo.
Sondeo VERSION			
No.	**Puerto/Servicio**	**Versión**	
1	80/http	Microsoft IIS webserver 6.0	
2	3389/microsoft-rdp	Microsoft Terminal Service	
Comentarios			
El puerto abierto corresponde al servicio autorizado de página Web pública. En el puerto 3389/TCP está corriendo el servicio de escritorio remoto de Windows, con el fin de brindar soporte desde Internet. Se recomienda evaluar la necesidad de usar este servicio en lugar del uso de una VPN.			

Tabla 34 Resultado del análisis de puertos para el servidor de registro hecho desde la red inalámbrica

Equipo		Servidor de Registro	
Sondeo SYN			
No.	**Puerto abierto**	**Servicio**	**Observaciones**
1	22/tcp	ssh	Abierto innecesariamente.
2	80/tcp	http	Abierto innecesariamente.
3	111/tcp	rpcbind	Abierto innecesariamente.
4	898/tcp	http	Abierto innecesariamente.
5	7100/tcp	tcpwrapped	Abierto innecesariamente.
6	8009/tcp	ajp13	Abierto innecesariamente.
Sondeo VERSION			
No.	**Puerto/Servicio**	**Versión**	
1	22/ssh	SunSSH 1.1 (protocol 2.0)	
2	80/http	Squid webproxy 2.5.STABLE9	
3	111/rpcbind	2-4 (rpc #100000)	
4	898/http	Sun Solaris Management Console (Runs Tomcat webserver)	
5	7100/tcpwrapped	No identificado.	
6	8009/ajp13	No identificado.	
Comentarios			
Los puertos abiertos en este equipo corresponden a servicios que en lo posible no deberían estar disponibles para los usuarios en el segmento público.			

Tabla 35 Resultado del análisis de puertos para el servidor Pagos en línea hecho desde la red inalámbrica

Equipo		**Servidor Pagos en Línea**	
Sondeo SYN			
No.	**Puerto abierto**	**Servicio**	**Observaciones**
1	21/tcp	ftp	Abierto innecesariamente.
2	22/tcp	ssh	Abierto innecesariamente.
3	80/tcp	http	Para prestar el servicio de pago en línea por Web browser
4	111/tcp	rpcbind	Abierto innecesariamente.
5	898/tcp	http	Abierto innecesariamente.
6	4045/tcp	nlockmgr	Abierto innecesariamente.
7	7100/tcp	tcpwrapped	Abierto innecesariamente.
Sondeo VERSION			
No.	**Puerto/Servicio**	**Versión**	
1	21/ftp	Solaris ftpd	
2	22/ssh	SunSSH 1.1 (protocol 2.0)	
3	80/http	Squid webproxy 2.5.STABLE9	
4	111/rpcbind	2-4 (rpc #100000)	
5	898/http	Sun Solaris Management Console (Runs Tomcat webserver)	
6	4045/nlockmgr	1-4 (rpc #100021)	
7	7100/tcpwrapped	No identificado.	
Comentarios			
El puerto abierto corresponde al servicio autorizado de página Web pública. Los demás puertos abiertos en este equipo corresponden a servicios que en lo posible no deberían estar disponibles a los usuarios en el segmento público.			

Tabla 36 Resultado del análisis de puertos para el servidor NFS hecho desde la red inalámbrica

Equipo		**Servidor NFS**	
Sondeo SYN			
No.	**Puerto abierto**	**Servicio**	**Observaciones**
1	21/tcp	ftp	Abierto innecesariamente.
2	23/tcp	telnet	Abierto innecesariamente.
3	25/tcp	smtp	Abierto innecesariamente.
4	79/tcp	finger	Abierto innecesariamente.
5	80/tcp	http	Abierto innecesariamente.
6	111/tcp	rpc	Abierto innecesariamente.
7	513/tcp	rlogin	Abierto innecesariamente.
8	514/tcp	tcpwrapped	Abierto innecesariamente.
9	587/tcp	smtp	Abierto innecesariamente.
10	2049/tcp	nfs	Abierto innecesariamente.
11	4045/tcp	nlockmgr	Abierto innecesariamente.

12	7100/tcp	tcpwrapped	Abierto innecesariamente.
13	32771/tcp	metad	Abierto innecesariamente.
14	32772/tcp	mdcommd	Abierto innecesariamente.
15	32773/tcp	rpc.metamedd	Abierto innecesariamente.
16	32774/tcp	metamhd	Abierto innecesariamente.
17	32775/tcp	rusersd	Abierto innecesariamente.
18	32776/tcp	mountd	Abierto innecesariamente.
19	32777/tcp	status	Abierto innecesariamente.
Sondeo VERSION			
No.	**Puerto/Servicio**	**Versión**	
1	21/ftp	Solaris ftpd	
2	23/telnet	BSD-derived telnetd	
3	25/smtp	Sendmail 8.13.6+Sun/8.13.6	
4	79/finger	Sun Solaris fingerd	
5	80/http	Squid webproxy 2.5.STABLE9	
6	111/rpc	No identificado.	
7	513/rlogin	No identificado.	
8	514/tcpwrapped	No identificado.	
9	587/smtp	Sendmail 8.13.6+Sun/8.13.6	
10	2049/nfs	2-4 (rpc #100003)	
11	4045/nlockmgr	1-4 (rpc #100021)	
12	7100/tcpwrapped	No identificado.	
13	32771/metad	1-2 (rpc #100229)	
14	32772/mdcommd	1 (rpc #100422)	
15	32773/rpc.metamedd	1 (rpc #100242)	
16	32774/metamhd	1 (rpc #100230)	
17	32775/rusersd	2-3 (rpc #100002)	
18	32776/mountd	1-3 (rpc #100005)	
19	32777/status	1 (rpc #100024)	
Comentarios			
Los puertos abiertos en este equipo corresponden a servicios que en lo posible no deberían estar disponibles a los usuarios en el segmento público.			

Tabla 37 Resultado del análisis de puertos para el servidor del SAD Virtual hecho desde la red inalámbrica

Equipo		**Servidor del SAD Virtual**	
Sondeo SYN			
No.	**Puerto abierto**	**Servicio**	**Observaciones**
1	22/tcp	ssh	Abierto innecesariamente.
2	80/tcp	http	Abierto innecesariamente.
3	111/tcp	rpcbind	Abierto innecesariamente.
4	7100/tcp	tcpwrapped	Abierto innecesariamente.
Sondeo VERSION			
No.	**Puerto/Servicio**	**Versión**	
1	22/ssh	SunSSH 1.1 (protocol 2.0)	
2	80/http	Apache httpd 1.3.33 ((Unix) PHP/4.3.11 mod_perl/1.29)	

3	111/rpcbind	No identificado.
4	7100/tcpwrapped	No identificado.
Comentarios		
Los puertos abiertos corresponden a servicios que en lo posible no deberían estar disponibles a los usuarios en el segmento público para este equipo.		

Tabla 38 Resultado del análisis de puertos para el servidor de pruebas hecho desde la red inalámbrica

Equipo		**Servidor de pruebas**	
Sondeo SYN			
No.	**Puerto abierto**	**Servicio**	**Observaciones**
1	21/tcp	ftp	Abierto innecesariamente.
2	80/tcp	http	Abierto innecesariamente.
3	111/tcp	rpc	Abierto innecesariamente.
4	898/tcp	http	Abierto innecesariamente.
5	4045/tcp	nlockmgr	Abierto innecesariamente.
6	7100/tcp	tcpwrapped	Abierto innecesariamente.
7	8009/tcp	ajp13	Abierto innecesariamente.
8	8080/tcp	http	Abierto innecesariamente.
Sondeo VERSION			
No.	**Puerto/Servicio**	**Versión**	
1	21/ftp	Solaris ftpd	
2	80/http	Squid webproxy 2.5.STABLE9	
3	111/rpc		
4	898/http	Sun Solaris Management Console (Runs Tomcat webserver)	
5	4045/nlockmgr	1-4 (rpc #100021)	
6	7100/tcpwrapped	No identificado.	
7	8009/ajp13	No identificado.	
8	8080/http	Apache Tomcat/Coyote JSP engine 1.1	
Comentarios			
Los puertos abiertos en este equipo corresponden a servicios que en lo posible no deberían estar disponibles a los usuarios en el segmento público.			

Tabla 39 Resultado del análisis de puertos para el servidor de correo hecho desde la red inalámbrica

Equipo		**Servidor de Correo electrónico**	
Sondeo SYN			
No.	**Puerto abierto**	**Servicio**	**Observaciones**
1	25/tcp	smtp	Para el servicio de correo electrónico.
2	53/tcp	domain	Para el servicio de DNS.
3	80/tcp	http	Para el acceso al correo desde un *Web browser*.
4	81/tcp	http	Abierto innecesariamente.
5	110/tcp	pop3	Para el servicio de correo electrónico.
6	443/tcp	http	Para el acceso al correo desde un *Web browser*.
7	3306/tcp	mysql	Abierto innecesariamente.

Sondeo VERSION		
No.	**Puerto/Servicio**	**Versión**
1	25/smtp	OpenBSD spamd
2	53/domain	ISC Bind 9.2.4
3	80/http	Apache httpd 1.3.33 ((Debian GNU/Linux) PHP/4.3.10-22)
4	81/http	Apache httpd 1.3.33 ((Debian GNU/Linux))
5	110/pop3	qmail pop3d
6	443/http	Apache httpd 1.3.33 ((Debian GNU/Linux) PHP/4.3.10-16 mod_ssl/2.8.22 OpenSSL/0.9.7e)
7	3306/mysql	MySQL 4.0.24_Debian-10sarge1-log
Comentarios		
Los puertos abiertos corresponden a los servicios autorizados de correo y DNS para ser usados por los equipos en el segmento público de la red en la institución. En el puerto 81/TCP está corriendo una página Web que no se está usando y que está mostrando la página resultante de una instalación del Apache, que además muestra información del equipo. El puerto 3306/TCP se recomienda en lo posible no tenerlo disponible para los usuarios en el segmento público de la red.		

- Resultados del análisis de vulnerabilidades a los servidores en la red: A continuación se dan los resultados del análisis de vulnerabilidades hecho con la herramienta Nessus. Cada tabla muestra las vulnerabilidades encontradas para cada uno de los servidores con un comentario y su respectivo factor de riesgo, que para los resultados mostrados puede ser ALTO o MEDIO.

Tabla 40 Análisis de vulnerabilidades para el servidor Antispam

Equipo		**Servidor Antispam**	
Puerto / Servicio	**Vulnerabilidad**	**Comentarios**	**Factor de riesgo**
80/HTTP	Off-by-one buffer overflow	La versión de Apache es menor a la 1.3.37, la cual tiene una vulnerabilidad en el módulo del Apache "Mod_rewrite", que puede ser usado para remapear solicitudes basadas en juegos de expresiones regulares de las solicitadas URI.	ALTO

80/HTTP	Versión con múltiples vulnerabilidades. » Buffer overflow. » Ejecución de código arbitrario. » DoS. » *Cross Site Scripting* (XSS)	Versión PHP anterior a la 4.4.1 con múltiples problemas de seguridad que pueden llegar a bloquear el servicio o comprometer el equipo.	ALTO
80/HTTP	Uso de autenticación en texto plano	El servidor Web contiene formularios HTML con campos de entrada de contraseñas que son transmitidas en texto plano hacia el servidor.	MEDIO
80/HTTP	*Cross Site Tracing* (XST)	Vulnerabilidad causada por algún error de filtrado y del uso del comando TRACE de HTTP, con el que se puede capturar credenciales en la cache de cualquier sitio Web.	MEDIO
53(UDP)/DNS	DNS Cache Snooping	El servicio de DNS permite que un tercero pueda obtener información sobre los nombre de dominio que han sido resueltos por el servidor, permitiéndole crear un perfil de navegación de los usuarios de la red.	MEDIO

Tabla 41 Análisis de vulnerabilidades para el Proxy del segmento público

Equipo		**Proxy segmento público**	
Puerto / Servicio	**Vulnerabilidad**	**Comentarios**	**Factor de riesgo**
53(TCP)/DNS	DNS cache poisoning	La resolución remota de DNS no utiliza puertos aleatorios cuando hace consultas al servidor DNS, lo cual permite el envenenamiento de la información en el servidor DNS, comprometiendo los clientes del servidor.	ALTO
81/HTTP	*Cross Site Tracing* (XST)	Vulnerabilidad causada por algún error de filtrado y del uso del comando TRACE de HTTP, con el que se puede capturar credenciales en la cache de cualquier sitio Web.	MEDIO
53(UDP)/DNS	DNS Cache Snooping	El servicio de DNS permite que un tercero pueda obtener información sobre los nombre de dominio que han sido resueltos por el servidor, permitiéndole crear un perfil de navegación de los usuarios de la red.	MEDIO

Tabla 42 Análisis de vulnerabilidades para el servidor Librejo

Equipo		**Servidor Librejo - Gestión bibliotecaria**

Puerto / Servicio	Vulnerabilidad	Comentarios	Factor de riesgo
80/http	Uso de autenticación en texto plano	El servidor Web contiene formularios HTML con campos de entrada de contraseñas que son transmitidas en texto plano hacia el servidor.	MEDIO

Tabla 43 Análisis de vulnerabilidades para el servidor de registro

Equipo		Servidor de Registro	
Puerto / Servicio	**Vulnerabilidad**	**Comentarios**	**Factor de riesgo**
80/HTTP	Instalación predeterminada de TOMCAT.	La instalación por defecto incluye dos servlets (SnoopServlet y TroubleShooter) que revelan información sobre el equipo donde se encuentra instalado Tomcat, útil para un atacante.	MEDIO

Tabla 44 Análisis de vulnerabilidades para el servidor de pruebas

Equipo		Servidor de pruebas	
Puerto / Servicio	**Vulnerabilidad**	**Comentarios**	**Factor de riesgo**
8080/HTTP	*Cross Site Scripting* (XSS)	Vulnerabilidades del sistema de validación de HTML que permite ejecutar scripts maliciosos.	MEDIO

Tabla 45 Análisis de vulnerabilidades para el servidor GISSIC

Equipo		Servidor GISSIC	
Puerto / Servicio	**Vulnerabilidad**	**Comentarios**	**Factor de riesgo**
80/HTTP	*Cross Site Tracing* (XST)	Vulnerabilidad causada por algún error de filtrado y del uso del comando TRACE de HTTP, con el que se puede capturar credenciales en la cache de cualquier sitio Web.	MEDIO
80/HTTP	Uso de autenticación en texto plano	El servidor Web contiene formularios HTML con campos de entrada de contraseñas que son transmitidas en texto plano hacia el servidor.	MEDIO

Tabla 46 Análisis de vulnerabilidades para el servidor de correo

Equipo		Servidor de Correo electrónico	
Puerto / Servicio	**Vulnerabilidad**	**Comentarios**	**Factor de riesgo**

80/Apache < 1.3.37	Off-by-one buffer overflow	Vulnerabilidad presente en el módulo del Apache "Mod_rewrite", que puede ser usado para remapear solicitudes basadas en juegos de expresiones regulares de las solicitadas URI.	ALTO
80/PHP < 4.4.1	Versión con múltiples vulnerabilidades. » Buffer overflow. » Ejecución de código arbitrario. » DoS. » *Cross Site Scripting* (XSS)	Versión con múltiples problemas de seguridad que pueden llegar a bloquear el servicio o comprometer el equipo.	ALTO
53(TCP)/DNS	DNS cache poisoning	La resolución remota de DNS no utiliza puertos aleatorios cuando hace consultas al servidor DNS, lo cual permite el envenenamiento de la información en el servidor DNS, comprometiendo los clientes del servidor.	ALTO
80/http	Uso de autenticación en texto plano	El servidor Web contiene formularios HTML con campos de entrada de contraseñas que son transmitidas en texto plano hacia el servidor.	MEDIO
80/HTTP	*Cross Site Tracing* (XST)	Vulnerabilidad causada por algún error de filtrado y del uso del comando TRACE de HTTP, con el que se puede capturar credenciales en la cache de cualquier sitio Web.	MEDIO

Tabla 47 Análisis de vulnerabilidades para el proxy del segmento público en sus direcciones privadas

Equipo		**Proxy segmento público**	
Puerto / Servicio	**Vulnerabilidad**	**Comentarios**	**Factor de riesgo**
80/HTTP	Problema de configuración	El proxy permite ejecutar solicitudes CONNECT a puertos sensibles. Este problema le da la capacidad a un atacante evitar las reglas del firewall y conectarse a puertos no permitidos.	ALTO
3128/Proxy	Problema de configuración	El proxy permite ejecutar solicitudes CONNECT a puertos sensibles. Este problema le da la capacidad a un atacante evitar las reglas del firewall y conectarse a puertos no permitidos.	ALTO

4.4.3. Análisis general de resultados

Como parte final del análisis de resultados del diagnóstico realizado, a continuación se da a conocer la calificación final para cada equipo de acuerdo al análisis de los cinco principios de seguridad definidos en la metodología MDCSIRD, plasmada en una matriz de evaluación. En la tabla 48 se muestra el resultado final por equipo o sistema del diagnóstico, donde se hace un análisis numérico de los cinco principios de seguridad que se tuvieron en cuenta. Para cada equipo o sistema se obtiene una calificación final que indica el nivel de riesgo, en una escala de 1 a 4, donde 1 es Muy bueno y 4 es Malo, a que está expuesto por las distintas vulnerabilidades o problemas de seguridad encontrados.

Tabla 48 Resultado del diagnóstico de la seguridad según principios de seguridad

	PRINCIPIO DE SEGURIDAD	Control de acceso	Autenticación	Integridad	Confidencialidad	Disponibilidad	**TOTAL**
	PESO	**0,13**	**0,12**	**0,25**	**0,25**	**0,25**	**1**
Firewall	Calificación	2	3	4	3	1	----
	Peso ponderado	0,26	0,36	1,00	0,75	0,25	**2,62**
Servidor Antispam	Calificación	3	3	4	3	2	----
	Peso ponderado	0,39	0,36	1,00	0,75	0,50	**3,00**
Servidor de Correos	Calificación	3	3	4	3	2	----
	Peso ponderado	0,39	0,36	1,00	0,75	0,50	**3,00**
Proxy red privada	Calificación	3	3	4	3	2	----
	Peso ponderado	0,39	0,36	1,00	0,75	0,50	**3,00**
Servidor Oracle	Calificación	3	3	4	3	2	----
	Peso ponderado	0,39	0,36	1,00	0,75	0,50	**3,00**
Switches C3	Calificación	3	3	4	2	1	----
	Peso ponderado	0,39	0,36	1,00	0,50	0,25	**2,50**
Servidor de Registro	Calificación	3	3	4	3	2	----
	Peso ponderado	0,39	0,36	1,00	0,75	0,50	**3,00**
Servidor SAD Virtual	Calificación	3	3	4	3	2	----
	Peso ponderado	0,39	0,36	1,00	0,75	0,50	**3,00**
Multi-servidores	Calificación	3	3	4	3	2	----
	Peso ponderado	0,39	0,36	1,00	0,75	0,50	**3,00**
Servidor NFS	Calificación	3	3	4	3	2	----
	Peso ponderado	0,39	0,36	1,00	0,75	0,50	**3,00**
Red inalámbrica	Calificación	3	3	4	4	4	----
	Peso ponderado	0,39	0,36	1,00	1,00	1,00	**3,75**

- Firewall: Según la tabla 48 la calificación final es de 2.62 indicando que la seguridad está regular, lo que quiere decir que se deben implementar muchos más mecanismos para mejorar la seguridad como tal del equipo, como la que ofrece éste a la red. De acuerdo al diagnóstico realizado, esta calificación se debe a que los controles no están implementados de acuerdo a la política de seguridad.
- Servidor Antispam: servidor que cumple el papel de reducir las cantidades de correo spam entrante al servidor de correo. Presenta falencias principalmente en la autenticación para la administración del equipo.
- Servidor de correo electrónico: servidor por el cual se presta el servicio de correo electrónico para los estudiantes y funcionarios de la universidad. El nivel de riesgo obtenido se debe principalmente a que el servicio no tiene un protocolo de cifrado para el acceso, que impida enviar en texto plano sobre la red el nombre de usuario y contraseña, y ser interceptado fácilmente.
- Proxy red privada: Equipo que ejecuta las funciones de Proxy para el segmento privado de la red de la UMNG o la Intranet. En este equipo es indispensable tener buenos controles para evitar que un usuario no autorizado gane acceso privilegiado, además de ofrecer buena disponibilidad evitando interrupción del servicio de Internet. El nivel de riesgo obtenido se debe a que aún se usan mecanismo de autenticación no muy confiables para el acceso administrativo al equipo y que hacen fácil que un usuario no autorizado acceda al equipo, pero se puede apreciar que se maneja controles de acceso para evitar, en parte, una mayor facilidad para el acceso no autorizado.
- Servidor de base de datos Oracle: Servidor que aloja las bases de datos para los distintos procesos y servicios usados en la red.

Debido a que este equipo maneja gran flujo de información confidencial es importante tener buenos controles para los cinco aspectos de seguridad, pero mucho más importante es la disponibilidad que pueda ofrecer el servidor ya que almacena información que continuamente es manipulada por los funcionarios de la institución. Para la administración remota del equipo y de sus aplicaciones aún se usan mecanismos de autenticación no muy recomendados junto algoritmos de cifrado simples, con los que se podría correr el riesgo de que, al ser interceptado, un usuario malintencionado gane privilegios en el equipo y la aplicación Oracle.

- *Switches* capa 3: Equipos de la red que se encargan de segmentarla en distintas VLAN's. Estos equipos no representan un factor de alto riesgo para la red, debido a que los controles de acceso son, principalmente, hechos por los servidores *proxy* y cortafuego, sin embargo, pueden ser usados para capturar información confidencial de los usuarios de la red. Por este motivo los aspectos más críticos tenidos en cuenta son el control de acceso y la integridad. Los equipos cuentan con una aceptable seguridad para controlar el acceso físico, también con medidas que eviten el acceso remoto no autorizado al equipo mediante el uso de VLAN's. En cuanto a la integridad se evitan ataques, como el *man-in-the-middle* o de interceptación, mediante la buena configuración de los protocolos de enrutamiento de capa de enlace, aunque no es suficiente.
- Servidor multiservicios: Servidor con maquinas virtuales donde se alojan los servicios de página Web, registro, pagos en línea, SAD virtual y servidor de pruebas. Para este equipo y los servicios alojados en él es crítico tener buenos controles que ofrezcan una autenticación confiable y segura, por lo que se le ha otorgado el mayor peso para la evaluación. De acuerdo a la evaluación se

encontró que no se restringe el uso de usuarios no recomendados para el acceso remoto administrativo ni se tienen en cuenta guías de contraseñas seguras para el uso de los servicios.

- Servidor NFS: Servidor utilizado como almacenamiento de los datos generados con los servicios de correo electrónico y cámaras de vigilancia. Debido a que este equipo almacena información privada de los usuarios del correo electrónico y videos tomados por las cámaras de vigilancia, se hace indispensable estrictos controles parar la autenticación y el control de acceso al equipo. La calificación dada a la autenticación se debe a que se hace de prácticas no recomendadas, ya que podrían facilitarle a un usuario malintencionado obtener los datos de un usuario privilegiado en el equipo.
- Red inalámbrica: Red de acceso público dentro del campus. Está red es la que menos controles de seguridad tiene, por lo que obtuvo el nivel de riesgo más alto. Los principales problemas encontrados son en cuanto a la disponibilidad del servicio, integridad y confidencialidad. Los problemas de disponibilidad se debe a que la cobertura de la red no es muy buena debido a las características físicas de las instalaciones del campus. En cuanto a integridad se puede decir que al usuario no se le garantiza que el punto de acceso al que se conecta sea auténtico ya que no se hace control sobre los puntos autorizados. Para la conexión con el punto de acceso no se usan mecanismos de cifrado que evite que cualquier usuario de la red pueda capturar información de otros.

Como resultado final, en la tabla 49 se muestra la calificación obtenida por la red de datos de la Universidad de acuerdo a cada una de las calificaciones de los equipos y sistemas analizados anteriormente.

Tabla 49 Resultado del diagnóstico de la seguridad según principios de seguridad a la red de datos de la UMNG.

	Red de datos UMNG		
PRINCIPIO DE SEGURIDAD	**PESO**	**CAL**	**PP**
Control de acceso	0,13	2,9	0,38
Autenticación	0,12	3,0	0,36
Integridad	0,25	4,0	1,00
Confidencialidad	0,25	3,0	0,75
Disponibilidad	0,25	1,9	0,47
TOTAL	**1**	----	**2,96**

4.5. SOLUCIONES PROPUESTAS A DEBILIDADES ENCONTRADAS

Luego de llevar a cabo el diagnóstico de la seguridad en la red de datos, surgen como resultado algunas deficiencias de seguridad que se reflejan más como un problema administrativo de la red y se debe a la ausencia de varios controles de seguridad que hagan parte de una política de seguridad, por lo que a continuación se elabora la propuesta de una política que permita tener un mejor control sobre los recursos y sistemas que conforman la red de la UMNG.

4.5.1. Política de seguridad

La División de Informática es la encargada de administrar el sistema de información que hace uso la Universidad Militar Nueva Granada, además de ofrecer servicios de red a todos los usuarios de la organización. Lo anterior conlleva a la necesidad de emitir la presente Política de Seguridad.

- PROPÓSITO DE LA POLÍTICA: Ayudar a minimizar el riesgo de pérdida o daño de la información por actividades criminales, las cuales también pueden afectar los servicios de la red, estableciendo las directrices para lograr una apropiada protección de la información, incluyendo las reglas de comportamiento esperado de los usuarios y administradores del sistema en el uso y administración de los servicios informáticos y los recursos que hacen

parte de la red. Por medio de esta política también se pretende autorizar al personal de la División de Informática a monitorear la red informática con el fin de prevenir cualquier uso indebido de los recursos de ésta, e investigar cualquier incidente de seguridad.

- ALCANCE DE LA POLÍTICA: La presente Política establece las directrices para la seguridad de la información en la red de datos administrada por la División de Informática para la UMNG, la cual afecta a todos los empleados, estudiantes y demás usuarios finales que hacen uso de los recursos informáticos de la UMNG, quienes a partir de este momento se llamarán como USUARIO.
- RESPONSABILIDADES: La División de Informática es la responsable de dar a conocer la Política de Seguridad entre quienes hagan uso de los sistemas de información de la organización. De acuerdo al perfil del usuario, en ocasiones no es necesario dar a conocer la Política completa. Es responsabilidad de cada usuario cumplir con cada una de las directrices que se definen dentro de esta Política de Seguridad.
- DEFINICIONES: Las siguientes definiciones son hechas con el fin de aclarar algunos conceptos para el entendimiento de la presente política.
    - **Información confidencial de la institución**: toda información relacionada con la institución que en caso de pérdida o robada puede resultar en serios daños o problemas para la institución.
    - **Sistema informático**: Conjunto de hardware y software que relacionados entre sí forman un ordenador
    - **Sistema de información**: es un conjunto de elementos, compuestos por información, personas y recursos, que

interactúan entre si para procesar la información y distribuirla en la manera más adecuada dentro de una organización.;

- USO DEL CORREO ELECTRÓNICO E INTERNET

  El correo electrónico no debe ser utilizado para transmitir información confidencial de la institución. En caso de que exista la necesidad de usar este medio para tal fin, se recomienda utilizar mecanismos para proteger la información de personas no autorizadas.

  El correo electrónico debe ser de uso personal, del que cada usuario se hace responsable de asignar una contraseña segura y de hacer el uso correcto de éste.

  El correo electrónico ni la Internet deben ser usados para publicar propaganda política, ni mensajes racistas, ni contenido sexual y ningún otro contenido que pueda afectar negativamente a los usuarios de dichos servicios.

  El servicio de la Internet debe ser utilizado exclusivamente como un medio de consulta para fines académicos o para el cumplimiento de los objetivos institucionales.

  La División de Informática deberá incentivar el buen uso de Internet, evitando que se haga uso indebido y malintencionado de Internet y de los servicios que sobre éste se brindan.

- ADMINISTRACIÓN DE CUENTAS DE USUARIO

  Se debe tener definido claramente los perfiles de usuario de acuerdo a las funciones que desempeña y de su tipo de vinculación dentro de la institución. De acuerdo a esos perfiles los usuarios tendrán los permisos correspondientes para realizar determinadas modificaciones (Ej.: instalación de software en computadores personales) en los distintos sistemas informáticos.

La División de Informática es la responsable de definir los perfiles de usuario y la única de crear las cuentas de usuario teniendo en cuenta los perfiles ya definidos.

- AUTENTICACIÓN

  El acceso a los servicios o sistemas que manejen información confidencial de la institución, obligatoriamente, debe incluir un mecanismo de autenticación.

  Todos los servicios informáticos deberían incluir autenticación de usuario, como contraseñas, certificados u otros mecanismos.

  Se deberían establecer reglas para definir contraseñas seguras, como sólo permitir contraseñas que incluyan caracteres alfanuméricos y especiales dentro de la contraseña o cantidades mínimas de caracteres en la contraseña.

  Los usuarios y contraseñas para acceder a los distintos servicios, computadoras y demás sistemas informáticos son personales y no deben compartirse con otros usuarios.

  Las contraseñas deben ser memorizadas, y no se debe recurrir a la práctica de escribirlas en papeles ni en otro medio al cual puedan acceder otros usuarios.

  El responsable del equipo no debe otorgar acceso al equipo a otras personas sin autorización de la División de Informática.

- CONTROL DE ACCESO

  El acceso a las áreas que contengan sistemas con información confidencial (Ej.: servidores) o permitan acceso privilegiado a la red (Ej.: switch) deberá ser registrado con la fecha, hora de entrada y salida, y motivo de la visita.

  La visita de personas que no pertenezcan a la División de Informática a los cuartos de servidores y equipos deberá ser bajo

supervisión del personal de la División de Informática o una persona delegada para tal fin por parte de la División.

Se deberá generar mecanismos que restrinjan el acceso a personas no autorizadas a las áreas que contengan sistemas con información confidencial o permitan acceso privilegiado a la red de acuerdo al nivel de criticidad del área.

Se deben tener mecanismos que no permitan el acceso a los servidores por usuarios no autorizados.

Se deben establecer diferentes zonas lógicas en la red, en las que se separen los recursos de acceso público con los de acceso privado, filtrando tráfico de la red entre las dichas zonas.

- AUTORIZACIÓN DE ACCESO A LA INFOMACIÓN Y SISTEMAS

  Se debe tener definido los diferentes niveles de autorización para los usuarios de acuerdo a sus roles dentro de la institución.

  La autorización para acceder a la información de la institución y sistemas debe sólo ser concedida de acuerdo al nivel requerido por el rol del usuario.

  La autorización para acceder a la información y sistemas debe ser verificada como mínimo en periodos de un año.

- SEGURIDAD FÍSICA

  Los equipos que procesen información sensible o crítica deben ser ubicados en lugares seguros, que tengan un perímetro de seguridad física definido y donde existan controles de acceso. [ISO]

  Los equipos de red deberán ser ubicados en lugares que cumplan con los requerimientos básicos de seguridad exigidos por la División de Informática.

  Se deberá implementar mecanismos para protección contra incendio, tales como detectores de humo, extintores de fuego o los que se consideren necesarios. [ISO]

Se debe evitar almacenar material combustible o que pueda ayudar a la propagación de un incendio en los cuartos con equipos que manejen información sensible o sean de gran importancia para el funcionamiento de la red. [ISO]

Es recomendable el monitoreo de las condiciones ambientales, tales como temperatura, con el de controlar las condiciones que puedan afectar el funcionamiento de los equipos. [ISO]

- SOFTWARE

  En los equipos se deberán mantener actualizado aquel software del que se emita una mejora en seguridad o cualquiera que contribuya con el buen funcionamiento de éste.

  En los equipos que manejen información sensible se deberá instalar la actualización del software garantizando que ésta no afecte con el funcionamiento del equipo.

  El software instalado en los equipos debe cumplir con el licenciamiento apropiado y acorde a la propiedad intelectual a que dé lugar.

  En los sistemas críticos se debería planear la actualización del software, el cual es recomendable realizar bajo un procedimiento de instalación emitido por la División de Informática.

  Todo software que desde el punto de vista de la División de Informática afecte la integridad de los recursos de la red no se debe permitir.

  Corresponde a la División de Informática la autorización de la adquisición del software.

  La División de Informática es la responsable de llevar a cabo revisiones a los sistemas informáticos propiedad de la UMNG con el fin de asegurar que sólo software licenciado se encuentre instalado en ellos.

El software utilizado en la UMNG deberá ser usado exclusivamente para asuntos relacionados con las actividades de la institución.

- INSTALACIÓN Y MANTENIMIENTO DE LOS EQUIPOS

La División de Informática deberá llevar un inventario de todos los equipos propiedad de la UMNG.

Los equipos que deban o estén conectados a la red de la UMNG deberán estar sujetos a los requerimientos de instalación emitidos por la División de Informática y tener la configuración de seguridad básica exigida por ella.

Es deber del responsable del equipo en conjunto con la División de Informática dar cumplimiento a los requerimientos de instalación e informar sobre cualquier cambio que afecte la instalación del equipo.

El responsable del equipo debe velar por la integridad física del equipo.

Es responsabilidad de la División de Informática del mantenimiento preventivo y correctivo de lo equipos propiedad de la UMNG.

La División de Informática puede otorgar mantenimiento preventivo y correctivo cuando lo estimen necesario, con previó aviso al responsable del equipo.

Se debe procurar mantener actualizados los equipos con el fin de mantener el buen funcionamiento de éste o mejorarlo.

Cuando se requiera reutilizar cualquier dispositivo se debe borrar la información que contenga mediante el uso de técnicas que permitan que la dicha información no pueda ser recuperada.

En caso de que se necesite dar de baja un dispositivo, este debe ser destruido físicamente de tal forma que no pueda recuperarse la información.

Los equipos que vayan a ser reutilizados o eliminados deberán ser revisados, con el propósito de no eliminar software licenciado, ni información confidencial de los cuales no se tenga copia.

Se deberá contar con autorización previa de la División de Informática para la reutilización o eliminación de un equipo.

Para cada equipo eliminado se deberá tener un documento que contenga el motivo por el cual se da de baja, el responsable en dar de baja el equipo, la fecha y cualquier otra información que se considere importante.

- ACCESO REMOTO DESDE UN ENTORNO DE INTERNET

  Se deben implementar protocolos capaces de cifrar la comunicación que se establezca desde el exterior de la red en la cual se transmita información sensible.

  La División de Informática es la encargada de asignar los correspondientes accesos remotos a los servicios de la red con autorización del responsable del servicio, en los casos que la criticidad del servicio lo amerite, por ejemplo acceso mediante VPN o sesión Telnet.

- DESARROLLO DE SERVICIOS DE RED

  La implementación de los servicios de red deberá tener el aval de la División de Informática.

  Al responsable del servicio de red corresponde la implementación de la protección adecuada.

  La programación e implementación de los servicios de red deberán estar de acuerdo a los requerimientos emitidos por la División de Informática.

- BACKUP DE LA INFORMACIÓN

  La información que para la institución se considere crítica se le deberá realizar copias de seguridad.

- MANEJO DE LA INFORMACIÓN

  El usuario no deberá divulgar o revelar información confidencial de la institución a personas no autorizadas. En caso de ser necesario

compartir información confidencial con cualquier persona, entidad o firma fuera de la UMNG se debe solicitar autorización a la División de Informática, quienes a su vez darán el manejo adecuado para dicha solicitud.

Dentro de la institución, la información confidencial se revelará a aquellas personas cuyas funciones ameriten tener tal conocimiento.

Aquellas personas que manejan información confidencial no deberán revelarla a ninguna otra persona de la Institución.

Ningún usuario tiene, automáticamente, derecho a acceso a toda la información de la institución.

La persona que recibe información confidencial no deberá reproducirla, a menos que se le autorice por parte del dueño de la información. En caso que se autorice realizar copias de la información suministrada, éstas deben ser controladas.

- EVALUACIONES DE SEGURIDAD

  Las evaluaciones de seguridad deberían realizarse con regularidad con el fin de identificar las posibles vulnerabilidades del sistema.

  Toda información necesaria para la evaluación que se le suministre al evaluador o evaluadores deberá ser entregada bajo un compromiso de confidencialidad, que garantice no sea divulgada.

  El proceso de evaluación debería ayudar a encontrar las vulnerabilidades del sistema y a su vez los controles de seguridad adecuados para minimizarlas.

  El proceso de evaluación debería asegurar que los resultados sean documentados.

  Realizar evaluaciones de seguridad con regularidad podría ayudar a mejorar la Política de Seguridad.

4.5.2. Implementación de un servidor de dominio

Con el fin de facilitar la administración de las cuentas de usuario y equipos en la red, además de asegurar, en gran parte del cumplimiento de la política de seguridad, se recomienda la implementación de un servidor de dominio que permita agrupar los equipos y usuarios dentro de un dominio.

Con el uso de un dominio cada persona que acceda a los recursos de la red se identifica con un único usuario, lo que facilita la auditoría de usuarios, ya que se puede rastrear los sucesos de cada uno de éstos, permitiéndole al administrador saber que usuario es el que comente una violación a la seguridad. También permite una mejor administración de las directivas de seguridad para todos los usuarios, porque no se requiere definir directivas en cada equipo conectado a la red.

Con esta medida se asegura de que los equipos en la red no son manipulados, por parte de los usuarios, de manera que afecte la seguridad de la red.

4.5.3. Filtrado por MAC para conexiones físicas en la Intranet

Como medida para evitar la conexión a la red de equipos no aprobados por la División de Informática, que afecten la seguridad de ésta, se propone implementar el filtrado por MAC. Ésto ayuda a los administradores a saber que equipos están conectados a la red, y estar seguros de que cumplan con los requerimientos exigidos por ellos para operar de forma segura. Al implementar esta medida se reduce en gran parte que usuarios conecten equipos infectados y así propagar un virus a todos los demás equipos, o por otra parte, a que conecten un punto de acceso no permitido que brinde acceso a usuarios no permitidos para un segmento de red restringido.

4.5.4. Implementación de detección o prevención de intrusos (IDS o IPS)

El sistema de detección de intrusos (IDS) está diseñado para detectar cualquier acceso no autorizado, ataque informático o cualquier violación a un

equipo o a una red. La función del IDS es detectar las violaciones e informar al administrador de red, quien debe establecer el mecanismo para evitar dichas amenazas, mientras que un sistema de prevención de intrusos (IPS) es un dispositivo capaz de realizar las funciones de un IDS más las de prevenir las violaciones informáticas detectadas en la red.

Como medida para reducir los ataques informáticos en la red se recomienda el la implementación de estos sistemas en la red en puntos estratégicos, que le permita a los administradores de la red a detectar con mayor facilidad de donde proviene la gran mayoría de ataques y poder prevenir el éxito de éstos.

4.5.5. Resumen de recomendaciones para solucionar los problemas críticos en la red

La tabla 50 relaciona los problemas de seguridad informática con mayor relevancia detectados en la red y las recomendaciones hechas como solución de dichos problemas.

Tabla 50 Cuadro resumen de recomendaciones hechas como solución de problemas de seguridad

Equipo	Descripción del problema	Recomendación
Firewall Servidores Proxies	Los equipos se encuentran ubicados físicamente en un cuarto con un perímetro de seguridad frágil, que podría ser susceptible a una fácil intrusión, debido a que cuenta con paredes frágiles, puertas inseguras y sin controles de acceso muy efectivos	Implementación de los capítulos "**Seguridad Física**" y "**Control de Acceso**" de la Política de seguridad propuesta
Firewall Servidores Proxies	El cuarto contiene materiales que podrían facilitar la propagación del fuego, como cajas almacenadas y paredes de un material inadecuado.	Implementación del capítulo "**Seguridad Física**" de la Política de seguridad propuesta
Firewall Servidores Proxies	El cuarto no cuenta con extintores de fuego cerca.	Implementación del capítulo "**Seguridad Física**" de la Política de seguridad propuesta
Firewall Servidores Proxies	No se tiene implementado monitores ambientales para controlar la temperatura en los equipos.	Implementación del capítulo "**Seguridad Física**" de la Política de seguridad propuesta
Firewall	Las reglas para el filtrado de paquetes del firewall no están definidas de acuerdo a una política de seguridad.	Implementación de la Política de seguridad propuesta

Firewall	Es posible recopilar información sobre la red desde la Internet.	Implementación de un IDS o IPS
Servidor Antispam Servidor de Correo electrónico	Versión del Apache desactualizada, con vulnerabilidades de seguridad publicadas.	Actualizar a la versión estable. Implementación del capítulo "**Software**" de la Política de seguridad propuesta
Firewall Servidores Proxies	Equipos de terceros dentro del mismo cuarto de servidores de la institución.	Implementación del capítulo "**Control de Acceso**" de la Política de seguridad propuesta
Proxy segmento público	Problema de configuración. Permite realizar conexiones a puertos sensibles dándole la capacidad a un atacante evitar las reglas del firewall y conectarse a puertos no permitidos.	Corregir problemas de configuración en la aplicación proxy.
Servidor Antispam Servidor de Correo electrónico Servidor GISSIC Servidor Librejo - Gestión bibliotecaria	Uso de autenticación en texto plano.	Implementar mecanismos para el cifrado de las credenciales de usuario.
Servidor de Registro	Instalación predeterminada de TOMCAT	Deshabilitar la página predeterminada de la instalación de Tomcat
Switches	En el mismo cuarto se almacena elementos ofimáticos, tales como resmas de papel y cajas.	Implementación del capítulo "**Seguridad Física**" de la Política de seguridad propuesta
Switches	Los switches están expuestos a ataques ARP Spoofing.	Filtrado por MAC en los *Switches*
Red inalámbrica	No se tiene habilitado un protocolo de cifrado que permita cifrar los datos y permitir el acceso a sólo usuarios de la UMNG.	Implementar un servidor de autenticación para el acceso a la red inalámbrica
Firewall Servidores Proxies	La instalación de los equipos es deficiente y no está acorde a ninguna normatividad sobre instalación de equipos para sistemas de información.	Implementar las recomendaciones y normas para la instalación de servidores y equipos de red

5. CONCLUSIONES Y RECOMENDACIONES

En este capítulo se presentarán las conclusiones y recomendaciones finales de este trabajo.

5.1. CONCLUSIONES

Las conclusiones obtenidas con la realización del presente trabajo son las siguientes:

- Al recopilar información sobre la administración de la seguridad en la red de la universidad se dedujo que ésta se hacía dentro de un esquema de seguridad que agrupaba los aspectos más críticos dentro de un objetivo global que tenía como finalidad el acceso controlado desde el punto de vista físico y lógico, dejando, con debilidades y sin ninguna relación entre ellos, otros aspectos no menos importantes aislados en otros frentes de seguridad.
- Antes de realizar una evaluación de riesgos en una red informática es vital llevar a cabo un análisis del entorno de la institución, ya que le permite al evaluador identificar que elementos deben ser objeto de su evaluación como parte crítica de los procesos y servicios que se ofrecen de acuerdo a la misión de la institución.
- El uso de metodologías para la evaluación de la seguridad informática en conjunto con los estándares y guías de buenas prácticas ayudan detectar problemas de seguridad que no son de fácil percepción en las labores cotidianas de la administración de red, además son útiles para el mejoramiento de las tecnologías informáticas, desde el punto de vista de seguridad, ofreciendo confiabilidad a los clientes en el uso de los recursos de la red.

- Se encontró que la metodología OSSTMM estaba más acorde para ser la base de la metodología a definir, debido a que tiene una estructura sencilla de entender con tareas específicas a ejecutar, facilitando la ejecución para personas que no tienen conocimientos muy avanzados en seguridad, el cual es el caso de los funcionarios de la división de informática, quienes hasta hace poco han estado empapándose del tema de seguridad.
- Los resultados arrojados por el proceso de evaluación permiten concluir que, efectivamente, la administración de la red no estaba siendo soportada sobre unos principios fundamentales de seguridad informática, debido a que la seguridad no tenía un papel fundamental dentro de los procesos y servicios ofrecidos.
- Al realizar el diagnóstico de seguridad en la red de la Universidad se evidenció que las falencias encontradas en la seguridad se debieron a la ausencia de una política de seguridad, que rigiera la adecuada administración de los recursos de la red y el buen comportamiento de los usuarios y administradores.

5.2. RECOMENDACIONES

Se aconseja la aplicación de la guía de buenas prácticas ISF para la implementación de procedimientos y guías de seguridad que ayuden a complementar la política de seguridad entregada en la presente investigación.

Con el fin de mejorar la seguridad en la red de la universidad se recomienda definir un comité de seguridad que periódicamente se reúna para revisar la política de seguridad y la metodología definidas en el presente trabajo, y así generar comentarios y recomendaciones que contribuyan a la mejora de estos documentos.

BIBLIOGRAFÍA

[1] López Gavilán, Alexander. Diseño de metodología para el diagnóstico de seguridad a las redes de datos de ETECSA. Pinar del Río, Cuba, 2007. [citado en 19 de febrero de 2007]. Disponible en Internet: <http://www.informaticahabana.co.cu/evento_virtual/?q=node/123&ev=VIII%20Seminario%20Iberoamericano%20de%20Seguridad%20en%20las%20TICs>

Documento electrónico que contempla el trabajo desarrollado para diseñar una metodología para el diagnóstico de la seguridad a las redes de datos de la empresa cubana ETECSA.

[2] Ortiz, Jenny Catherine. – Metodología para la detección y erradicación de ataques Web - *data tampering* & *SQL injection* - en los procesos de la página de la Universidad Militar Nueva Granada. Bogotá, D.C., 2006, Monografía (Ingeniera en Telecomunicaciones). Universidad Militar Nueva Granada. Facultad de Ingeniería.

En esta monografía se propone una metodología para detectar y erradicar los ataques informáticos conocidos como *data tampering* & *SQL injection* a los servicios Web de la Universidad.

[3] INFORMATION SECURITY FORUM. The Standard of Good Practice for Information Security. London: ISF, 2007. 372 p. “Texto en inglés”. Disponible en Internet: <https://www.isfsecuritystandard.com/SOGP07/pdfs/SOGP_2007.pdf>

La dirección anterior conduce a un archivo en formato PDF que contiene el Estándar de buenas prácticas para la seguridad de la información en su versión 4.1 de enero de 2005.

[4] SysAdmin, Audit, Network, Security Institute. B.A.S.E – A Security Assessment Methodology [en línea]. Braunton, Gregory. Versión 1.4b. SANS Institute, 29 de septiembre de 2004 [citado en 10 de febrero de 2009]. "Texto en inglés". Disponible en Internet: <http://www.sans.org/reading_room/whitepapers/auditing/b_a_s_e_%E2%80%93_a_security_assessment_methodology_1587>

[5] Herzog, Pete. OSSTMM 2.2. Open-Source Security Testing Methodology Manual – Manual de la Metodología Abierta de Testeo de Seguridad [en línea]. Versión 2.2. Institute for Security and Open Methodologies, jueves, 13 de diciembre de 2006 [citado en 8 de abril de 2007]. "Texto en inglés". Disponible en Internet: <http://isecom.securenetltd.com/osstmm.en.2.2.pdf>

[6] INTERNATIONAL ORGANITATION FOR STADARDIZATION. Information technology – Security techniques – Information security management systems – Requirements. Octubre de 2005 [citado en 20 de septiembre de 2007]. "Texto en inglés". Disponible en Internet: <http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42103>

En esa página Web se encuentra una breve descripción del documento de la norma ISO/IEC 27001.

[7] DEPARTMENT OF DEFENSE (Los Estados Unidos). Department Of Defense Trusted Computer System Evaluation Criteria. DoD, 1985. p. 116. Disponible en Internet: <http://csrc.nist.gov/publications/history/dod85.pdf>

Documento que contiene el estándar del Departamento de Defensa de Los Estados Unidos más conocido como el *Orange Book* o Libro Naranja, y el cual define los criterios para la evaluación de la seguridad informática.

[8] INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION. Control Objectives for Information and Related Technology (COBIT). ISACA. p. 207. Disponible en Internet: <http://www.isaca.org/Content/NavigationMenu/Members_and_Leaders/COBIT6/Obtain_COBIT/CobiT4_Espanol.pdf>

[9] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. Guideline on Network Security Testing. NIST, octubre de 2003 [citado en 28 de abril de 2007], 92 p (SP 800-42). “Texto en inglés”. Disponible en Internet: <http://csrc.nist.gov/publications/nistpubs/800-42/NIST-SP800-42.pdf>

[10] INTERNATIONAL ORGANITATION FOR STADARDIZATION. Information technology – Security techniques – Code of practice for information security management. Geneva: ISO/IEC, 2005, 107 p (ISO/IEC 17799:2005 (E)).

[11] DIRECCIÓN NACIONAL DE INFORMÁTICA Y COMUNICACIONES. Guía para la elaboración de políticas de seguridad [en línea]. Bogotá Universidad Nacional de Colombia, 2003 [citado en 20 de junio de 2008].

Disponible en Internet: <http://www.dnic.unal.edu.co/docs/guia_para_elaborar_politicas_v1_0.pdf>

[12] Sharpe, Richard y Warnicke, Ed. Wireshark User's Guide [en línea]. "Texto en inglés". Disponible en Internet: <http://www.wireshark.org/docs/wsug_html_chunked/>

[13] Manual Reference Pages – ETTERCAP [en línea]. "Texto en inglés". Disponible en Internet: <http://www.irongeek.com/i.php?page=backtrack-3-man/ettercap>

[14] Milner, Marius. NetStumbler v0.4.0 Release Notes [en línea]. "Texto en inglés". Disponible en Internet: <http://www.stumbler.net/readme/readme_0_4_0.html>

[15] Tenable Network Security, Inc. NessusClient 3.2 User Guide [en línea]. Revisión 8. 25 de Julio de 2008. "Texto en inglés". Disponible en Internet: <http://www.nessus.org/documentation/NessusClient_3.2_User_Guide.pdf>

[16] METASPLOIT.com. Metasploit Framework User Guide [en línea]. Versión 3.1. "Texto en inglés". Disponible en Internet: <http://www.metasploit.com/documents/users_guide.pdf>

[17] Gordon "Fyodor". Nmap Network Scanning [en línea]. Lyon. Insecure.org. 16 de julio de 2008. "Texto en inglés". Disponible en Internet: <http://nmap.org/book/toc.html>

[18] Barroso, David y Berrueta, Andrés. YERSINIA Framework for layer 2 attacks [en línea]. Estados Unidos. Blackhat. 2005. "Texto en inglés".

Disponible en Internet: <http://blackhat.com/presentations/bh-europe-05/BH_EU_05-Berrueta_Andres/BH_EU_05_Berrueta_Andres.pdf>

[19] REMOTE-EXPLOIT.ORG. BackTrack [en línea] “Texto en inglés”. Disponible en Internet: <http://www.remote-exploit.org/backtrack.html>

[20] European Network and information Security Agency (ENISA). Glossary of Risk Management [en línea] “Texto en inglés”. Disponible en Internet: <http://www.enisa.europa.eu/rmra/glossary.html>

[21] Dillar, Kurt y Pfost, Jared. Guía de administración de riesgos de seguridad. Capítulo 4: Evaluación del riesgo [en línea]. Microsoft Corporation, 15 de octubre de 2004 [citado en 10 de febrero de 2009]. “Texto en español”. Disponible en Internet: <http://www.microsoft.com/spain/technet/recursos/articulos/srsgch04.mspx>

ANEXO A. HERRAMIENTAS DE SOFTWARE USADAS PARA EL DIAGNÓSTICO DE LA SEGURIDAD INFORMÁTICA

Como anexo al presente trabajo se hace entrega del software utilizado para el diagnóstico de la seguridad, el cual fue mencionado en el capítulo 2.2.3. A continuación se lista el software mencionado junto con el enlace para poder descargarlo. Este software se encuentra en el CD donde radica el presente documento.

- BacTrack 2: http://www.remote-exploit.org/backtrack_download.html.
- Wireshark 1.0.3: http://www.wireshark.org/download.html
- Nessus 3: http://www.nessus.org/download/
- Metasploit Framework 3.2: http://www.metasploit.com/framework/download/
- Ettercap 0.73: Versión para Linux http://ettercap.sourceforge.net/download.php. También incluida en BackTrack 2.
- NetStumbler: 0.4.0: http://www.netstumbler.com/downloads/
- Nmap 4.20: http://nmap.org/download.html
- Yersinia: Está incluida en el BackTrack 2

ANEXO B. TABLA DE RESULTADOS DE LA EVALUACIÓN DE RIESGOS

Activo	Clasificación Del Activo	Id	Amenaza	Vulnerabilidad	Nivel De Exposición	Clasificación Del Impacto	Nivel De Probabilidad	Clasificación Del Riesgo
1. Firewall	ALTA	1.1	Vandalismo.	Paredes del cuarto no reforzadas.	ALTA	ALTA	ALTA	ALTA
	ALTA	1.2	Robo del equipo/Acceso no autorizado	Paredes del cuarto muy débiles. Falta de mecanismos de control para el acceso no autorizado como alarmas y cámaras.	ALTA	ALTA	BAJA	MEDIA
	ALTA	1.3	Persona malintencionada / Acceso no autorizado	El router administrado por el proveedor de Internet está ubicado en el mismo cuarto del equipo.	MEDIA	ALTA	BAJA	MEDIA
	ALTA	1.4	Persona malintencionada	No se tiene un control de las visitas al cuarto donde se encuentra el equipo.	BAJA	MEDIA	MEDIA	MEDIA
	ALTA	1.5	Incendio.	Ausencia de extintores en el cuarto.	ALTA	ALTA	MEDIA	ALTA
	ALTA	1.6	Incendio.	Las paredes del cuarto y la presencia de elementos como cajas puede ser factor para la propagación rápida del fuego.	ALTA	ALTA	MEDIA	ALTA
	ALTA	1.7	Calentamiento del equipo	Falta de monitores de las condiciones ambientales.	MEDIA	ALTA	MEDIA	ALTA
	ALTA	1.8	Recopilar información sobre los equipos protegidos por el firewall	El firewall permite enumerar lo equipos detrás del firewall.	BAJA	MEDIA	ALTA	ALTA
2. Proxy red privada	ALTA	2.1	Vandalismo.	Paredes del cuarto no reforzadas.	ALTA	ALTA	ALTA	ALTA
	ALTA	2.2	Robo del equipo/Acceso no autorizado	Paredes del cuarto muy débiles. Falta de mecanismos control para el acceso no autorizado como alarmas y cámaras.	ALTA	ALTA	BAJA	MEDIA
	ALTA	2.3	Persona malintencionada / Acceso no autorizado	El router administrado por el proveedor de Internet está ubicado en el mismo cuarto del equipo.	MEDIA	ALTA	BAJA	MEDIA

	ALTA	2.4	Persona malintencionada	No se tiene un control de las visitas al cuarto donde se encuentra el equipo.	BAJA	MEDIA	MEDIA	MEDIA
	ALTA	2.5	Incendio.	Ausencia de extintores en el cuarto.	ALTA	ALTA	MEDIA	ALTA
	ALTA	2.6	Incendio.	Las paredes del cuarto y la presencia de elementos como cajas puede ser factor para la propagación rápida del fuego.	ALTA	ALTA	MEDIA	ALTA
	ALTA	2.7	Calentamiento del equipo	Falta de monitores de las condiciones ambientales.	MEDIA	ALTA	MEDIA	ALTA
3. Proxy segmento público	MEDIA	3.1	Vandalismo.	Paredes del cuarto no reforzadas.	ALTA	ALTA	ALTA	ALTA
	MEDIA	3.2	Robo del equipo/Acceso no autorizado	Paredes del cuarto muy débiles. Falta de mecanismos control para el acceso no autorizado como alarmas y cámaras.	ALTA	ALTA	BAJA	MEDIA
	MEDIA	3.3	Persona malintencionada / Acceso no autorizado	El router administrado por el proveedor de Internet está ubicado en el mismo cuarto del equipo.	MEDIA	MEDIA	BAJA	BAJA
	MEDIA	3.4	Persona malintencionada	No se tiene un control de las visitas al cuarto donde se encuentra el equipo.	BAJA	BAJA	MEDIA	BAJA
	MEDIA	3.5	Incendio.	Ausencia de extintores en el cuarto.	ALTA	ALTA	MEDIA	ALTA
	MEDIA	3.6	Incendio.	Las paredes del cuarto y la presencia de elementos como cajas puede ser factor para la propagación rápida del fuego.	ALTA	ALTA	MEDIA	ALTA
	MEDIA	3.7	Calentamiento del equipo	Falta de monitores de las condiciones ambientales.	MEDIA	MEDIA	MEDIA	MEDIA
	MEDIA	3.8	Robo de información	DNS cache poisoning. La resolución remota de DNS no utiliza puertos aleatorios cuando hace consultas al servidor DNS	BAJA	BAJA	MEDIA	BAJA
	MEDIA	3.9	Ataque por un pirata informático	Cross Site Tracing (XST). Causada por algún error de filtrado y del uso del comando TRACE de HTTP	BAJA	BAJA	MEDIA	BAJA

	MEDIA	3.10	Robo de información	DNS Cache Snooping. El servicio de DNS permite que un tercero pueda obtener información sobre los nombre de dominio que han sido resueltos por el servidor.	BAJA	BAJA	MEDIA	BAJA
	MEDIA	3.11	Ataque por un pirata informático	Problema de configuración. Permite realizar conexiones a puertos sensibles dándole la capacidad a un atacante evitar las reglas del firewall y conectarse a puertos no permitidos.	MEDIA	MEDIA	MEDIA	MEDIA
4. Servidor Antispam	ALTA	4.1	Vandalismo.	Paredes del cuarto no reforzadas.	ALTA	ALTA	ALTA	ALTA
	ALTA	4.2	Robo del equipo/Acceso no autorizado	Paredes del cuarto muy débiles. Falta de mecanismos control para el acceso no autorizado como alarmas y cámaras.	ALTA	ALTA	BAJA	MEDIA
	ALTA	4.3	Persona malintencionada / Acceso no autorizado	El router administrado por el proveedor de Internet está ubicado en el mismo cuarto del equipo.	MEDIA	ALTA	BAJA	MEDIA
	ALTA	4.4	Persona malintencionada	No se tiene un control de las visitas al cuarto donde se encuentra el equipo.	BAJA	MEDIA	MEDIA	MEDIA
	ALTA	4.5	Incendio.	Ausencia de extintores en el cuarto.	ALTA	ALTA	MEDIA	ALTA
	ALTA	4.6	Incendio.	Las paredes del cuarto y la presencia de elementos como cajas puede ser factor para la propagación rápida del fuego.	ALTA	ALTA	MEDIA	ALTA
	ALTA	4.7	Calentamiento del equipo	Falta de monitores de las condiciones ambientales.	MEDIA	ALTA	MEDIA	ALTA
	ALTA	4.8	Interrupción del servicio	Off-by-one buffer overflow. Versión del Apache desactualizada,	MEDIA	ALTA	MEDIA	ALTA
	ALTA	4.9	Interrupción del servicio	Versión de Apache con múltiples vulnerabilidades. » Buffer overflow. » Ejecución de código arbitrario. » DoS. » Cross Site Scripting (XSS)	MEDIA	ALTA	MEDIA	ALTA
	ALTA	4.10	Robo de credenciales	Uso de autenticación en texto	MEDIA	ALTA	ALTA	ALTA

				plano				
	ALTA	4.11	Ataque por un pirata informático	Cross Site Tracing (XST). Causada por algún error de filtrado y del uso del comando TRACE de HTTP	BAJA	MEDIA	MEDIA	MEDIA
	ALTA	4.12	Robo de información	DNS Cache Snooping. El servicio de DNS permite que un tercero pueda obtener información sobre los nombre de dominio que han sido resueltos por el servidor.	BAJA	MEDIA	MEDIA	MEDIA
5. Servidor Librejo - Gestión bibliotecaria	BAJA	5.1	Vandalismo.	Paredes del cuarto no reforzadas.	ALTA	MEDIA	ALTA	ALTA
	BAJA	5.2	Robo del equipo/Acceso no autorizado	Paredes del cuarto muy débiles. Falta de mecanismos control para el acceso no autorizado como alarmas y cámaras.	ALTA	MEDIA	BAJA	BAJA
	BAJA	5.3	Persona malintencionada / Acceso no autorizado	El router administrado por el proveedor de Internet está ubicado en el mismo cuarto del equipo.	MEDIA	BAJA	BAJA	BAJA
	BAJA	5.4	Persona malintencionada	No se tiene un control de las visitas al cuarto donde se encuentra el equipo.	BAJA	BAJA	MEDIA	BAJA
	BAJA	5.5	Incendio.	Ausencia de extintores en el cuarto.	ALTA	MEDIA	MEDIA	MEDIA
	BAJA	5.6	Incendio.	Las paredes del cuarto y la presencia de elementos como cajas puede ser factor para la propagación rápida del fuego.	ALTA	MEDIA	MEDIA	MEDIA
	BAJA	5.7	Calentamiento del equipo	Falta de monitores de las condiciones ambientales.	MEDIA	BAJA	MEDIA	BAJA
	BAJA	5.8	Robo de credenciales	Uso de autenticación en texto plano	MEDIA	BAJA	ALTA	MEDIA
6. Servidor de Registro	ALTA	6.1	Vandalismo.	Paredes del cuarto no reforzadas.	ALTA	ALTA	ALTA	ALTA
	ALTA	6.2	Robo del equipo/Acceso no autorizado	Paredes del cuarto muy débiles. Falta de mecanismos control para el acceso no autorizado como alarmas y cámaras.	ALTA	ALTA	BAJA	MEDIA
	ALTA	6.3	Persona malintencionada / Acceso no autorizado	El router administrado por el proveedor de Internet está ubicado en el mismo cuarto del equipo.	MEDIA	ALTA	BAJA	MEDIA

	ALTA	6.4	Persona malintencionada	No se tiene un control de las visitas al cuarto donde se encuentra el equipo.	BAJA	MEDIA	MEDIA	MEDIA
	ALTA	6.5	Incendio.	Ausencia de extintores en el cuarto.	ALTA	ALTA	MEDIA	ALTA
	ALTA	6.6	Incendio.	Las paredes del cuarto y la presencia de elementos como cajas puede ser factor para la propagación rápida del fuego.	ALTA	ALTA	MEDIA	ALTA
	ALTA	6.7	Calentamiento del equipo	Falta de monitores de las condiciones ambientales.	MEDIA	ALTA	MEDIA	ALTA
	ALTA	6.8	Divulgación de información sobre el activo	Instalación predeterminada de TOMCAT	BAJA	MEDIA	BAJA	BAJA
7. Servidor de pruebas	BAJA	7.1	Vandalismo.	Paredes del cuarto no reforzadas.	ALTA	MEDIA	ALTA	ALTA
	BAJA	7.2	Robo del equipo/Acceso no autorizado	Paredes del cuarto muy débiles. Falta de mecanismos control para el acceso no autorizado como alarmas y cámaras.	ALTA	MEDIA	BAJA	BAJA
	BAJA	7.3	Persona malintencionada / Acceso no autorizado	El router administrado por el proveedor de Internet está ubicado en el mismo cuarto del equipo.	MEDIA	BAJA	BAJA	BAJA
	BAJA	7.4	Persona malintencionada	No se tiene un control de las visitas al cuarto donde se encuentra el equipo.	BAJA	BAJA	MEDIA	BAJA
	BAJA	7.5	Incendio.	Ausencia de extintores en el cuarto.	ALTA	MEDIA	MEDIA	MEDIA
	BAJA	7.6	Incendio.	Las paredes del cuarto y la presencia de elementos como cajas puede ser factor para la propagación rápida del fuego.	ALTA	MEDIA	MEDIA	MEDIA
	BAJA	7.7	Calentamiento del equipo	Falta de monitores de las condiciones ambientales.	MEDIA	BAJA	MEDIA	BAJA
	BAJA	7.8	Ataque por un pirata informático	Cross Site Scripting (XSS). El sistema de validación de HTML permite ejecutar scripts maliciosos	MEDIA	BAJA	ALTA	MEDIA
8. Servidor	BAJA	8.1	Vandalismo.	Paredes del cuarto no reforzadas.	ALTA	MEDIA	ALTA	ALTA

GISSIC	BAJA	8.2	Robo del equipo/Acceso no autorizado	Paredes del cuarto muy débiles. Falta de mecanismos control para el acceso no autorizado como alarmas y cámaras.	ALTA	MEDIA	BAJA	BAJA
	BAJA	8.3	Persona malintencionada / Acceso no autorizado	El router administrado por el proveedor de Internet está ubicado en el mismo cuarto del equipo.	MEDIA	BAJA	BAJA	BAJA
	BAJA	8.4	Persona malintencionada	No se tiene un control de las visitas al cuarto donde se encuentra el equipo.	BAJA	BAJA	MEDIA	BAJA
	BAJA	8.5	Incendio.	Ausencia de extintores en el cuarto.	ALTA	MEDIA	MEDIA	MEDIA
	BAJA	8.6	Incendio.	Las paredes del cuarto y la presencia de elementos como cajas puede ser factor para la propagación rápida del fuego.	ALTA	MEDIA	MEDIA	MEDIA
	BAJA	8.7	Calentamiento del equipo	Falta de monitores de las condiciones ambientales.	MEDIA	BAJA	MEDIA	BAJA
	BAJA	8.8	Robo de credenciales	Uso de autenticación en texto plano	MEDIA	BAJA	ALTA	MEDIA
	BAJA	8.9	Ataque por un pirata informático	Cross Site Tracing (XST). Causada por algún error de filtrado y del uso del comando TRACE de HTTP	BAJA	BAJA	MEDIA	BAJA
9. Servidor de Correo electrónico	ALTA	9.1	Vandalismo.	Paredes del cuarto no reforzadas.	ALTA	ALTA	ALTA	ALTA
	ALTA	9.2	Robo del equipo/Acceso no autorizado	Paredes del cuarto muy débiles. Falta de mecanismos control para el acceso no autorizado como alarmas y cámaras.	ALTA	ALTA	BAJA	MEDIA
	ALTA	9.3	Persona malintencionada / Acceso no autorizado	El router administrado por el proveedor de Internet está ubicado en el mismo cuarto del equipo.	MEDIA	ALTA	BAJA	MEDIA
	ALTA	9.4	Persona malintencionada	No se tiene un control de las visitas al cuarto donde se encuentra el equipo.	BAJA	MEDIA	MEDIA	MEDIA
	ALTA	9.5	Incendio.	Ausencia de extintores en el cuarto.	ALTA	ALTA	MEDIA	ALTA

	ALTA	9.6	Incendio.	Las paredes del cuarto y la presencia de elementos como cajas puede ser factor para la propagación rápida del fuego.	ALTA	ALTA	MEDIA	ALTA
	ALTA	9.7	Calentamiento del equipo	Falta de monitores de las condiciones ambientales.	MEDIA	ALTA	MEDIA	ALTA
	ALTA	9.8	Interrupción del servicio	Off-by-one buffer overflow. Versión del Apache desactualizada,	MEDIA	ALTA	MEDIA	ALTA
	ALTA	9.9	Interrupción del servicio	Versión de Apache con múltiples vulnerabilidades. » Buffer overflow. » Ejecución de código arbitrario. » DoS. » Cross Site Scripting (XSS)	MEDIA	ALTA	MEDIA	ALTA
	ALTA	9.10	Robo de credenciales	Uso de autenticación en texto plano	MEDIA	ALTA	ALTA	ALTA
	ALTA	9.11	Ataque por un pirata informático	Cross Site Tracing (XST). Causada por algún error de filtrado y del uso del comando TRACE de HTTP	BAJA	MEDIA	MEDIA	MEDIA
	ALTA	9.12	Robo de información	DNS Cache Snooping. El servicio de DNS permite que un tercero pueda obtener información sobre los nombre de dominio que han sido resueltos por el servidor.	BAJA	MEDIA	MEDIA	MEDIA
10. Servidor Oracle	ALTA	10.1	Vandalismo.	Paredes del cuarto no reforzadas.	ALTA	ALTA	ALTA	ALTA
	ALTA	10.2	Robo del equipo/Acceso no autorizado	Paredes del cuarto muy débiles. Falta de mecanismos control para el acceso no autorizado como alarmas y cámaras.	ALTA	ALTA	BAJA	MEDIA
	ALTA	10.3	Persona malintencionada / Acceso no autorizado	El router administrado por el proveedor de Internet está ubicado en el mismo cuarto del equipo.	MEDIA	ALTA	BAJA	MEDIA
	ALTA	10.4	Persona malintencionada	No se tiene un control de las visitas al cuarto donde se encuentra el equipo.	BAJA	MEDIA	MEDIA	MEDIA
	ALTA	10.5	Incendio.	Ausencia de extintores en el cuarto.	ALTA	ALTA	MEDIA	ALTA

	ALTA	10.6	Incendio.	Las paredes del cuarto y la presencia de elementos como cajas puede ser factor para la propagación rápida del fuego.	ALTA	ALTA	MEDIA	ALTA
	ALTA	10.7	Calentamiento del equipo	Falta de monitores de las condiciones ambientales.	MEDIA	ALTA	MEDIA	ALTA
11. Servidor SAD Virtual	MEDIA	11.1	Vandalismo.	Paredes del cuarto no reforzadas.	ALTA	ALTA	ALTA	ALTA
	MEDIA	11.2	Robo del equipo/Acceso no autorizado	Paredes del cuarto muy débiles. Falta de mecanismos control para el acceso no autorizado como alarmas y cámaras.	ALTA	ALTA	BAJA	MEDIA
	MEDIA	11.3	Persona malintencionada / Acceso no autorizado	El router administrado por el proveedor de Internet está ubicado en el mismo cuarto del equipo.	MEDIA	MEDIA	BAJA	BAJA
	MEDIA	11.4	Persona malintencionada	No se tiene un control de las visitas al cuarto donde se encuentra el equipo.	BAJA	BAJA	MEDIA	BAJA
	MEDIA	11.5	Incendio.	Ausencia de extintores en el cuarto.	ALTA	ALTA	MEDIA	ALTA
	MEDIA	11.6	Incendio.	Las paredes del cuarto y la presencia de elementos como cajas puede ser factor para la propagación rápida del fuego.	ALTA	ALTA	MEDIA	ALTA
	MEDIA	11.7	Calentamiento del equipo	Falta de monitores de las condiciones ambientales.	MEDIA	MEDIA	MEDIA	MEDIA
12. Servidor Thor	MEDIA	12.1	Vandalismo.	Paredes del cuarto no reforzadas.	ALTA	ALTA	ALTA	ALTA
	MEDIA	12.2	Robo del equipo/Acceso no autorizado	Paredes del cuarto muy débiles. Falta de mecanismos control para el acceso no autorizado como alarmas y cámaras.	ALTA	ALTA	BAJA	MEDIA
	MEDIA	12.3	Persona malintencionada / Acceso no autorizado	El router administrado por el proveedor de Internet está ubicado en el mismo cuarto del equipo.	MEDIA	MEDIA	BAJA	BAJA
	MEDIA	12.4	Persona malintencionada	No se tiene un control de las visitas al cuarto donde se encuentra el equipo.	BAJA	BAJA	MEDIA	BAJA
	MEDIA	12.5	Incendio.	Ausencia de extintores en el cuarto.	ALTA	ALTA	MEDIA	ALTA

	MEDIA	12.6	Incendio.	Las paredes del cuarto y la presencia de elementos como cajas puede ser factor para la propagación rápida del fuego.	ALTA	ALTA	MEDIA	ALTA
	MEDIA	12.7	Calentamiento del equipo	Falta de monitores de las condiciones ambientales.	MEDIA	MEDIA	MEDIA	MEDIA
13. Servidor Web	BAJA	13.1	Vandalismo.	Paredes del cuarto no reforzadas.	ALTA	MEDIA	ALTA	ALTA
	BAJA	13.2	Robo del equipo/Acceso no autorizado	Paredes del cuarto muy débiles. Falta de mecanismos control para el acceso no autorizado como alarmas y cámaras.	ALTA	MEDIA	BAJA	BAJA
	BAJA	13.3	Persona malintencionada / Acceso no autorizado	El router administrado por el proveedor de Internet está ubicado en el mismo cuarto del equipo.	MEDIA	BAJA	BAJA	BAJA
	BAJA	13.4	Persona malintencionada	No se tiene un control de las visitas al cuarto donde se encuentra el equipo.	BAJA	BAJA	MEDIA	BAJA
	BAJA	13.5	Incendio.	Ausencia de extintores en el cuarto.	ALTA	MEDIA	MEDIA	MEDIA
	BAJA	13.6	Incendio.	Las paredes del cuarto y la presencia de elementos como cajas puede ser factor para la propagación rápida del fuego.	ALTA	MEDIA	MEDIA	MEDIA
	BAJA	13.7	Calentamiento del equipo	Falta de monitores de las condiciones ambientales.	MEDIA	BAJA	MEDIA	BAJA
14. Servidor NFS	MEDIA	14.1	Vandalismo.	Paredes del cuarto no reforzadas.	ALTA	ALTA	ALTA	ALTA
	MEDIA	14.2	Robo del equipo/Acceso no autorizado	Paredes del cuarto muy débiles. Falta de mecanismos control para el acceso no autorizado como alarmas y cámaras.	ALTA	ALTA	BAJA	MEDIA
	MEDIA	14.3	Persona malintencionada / Acceso no autorizado	El router administrado por el proveedor de Internet está ubicado en el mismo cuarto del equipo.	MEDIA	MEDIA	BAJA	BAJA
	MEDIA	14.4	Persona malintencionada	No se tiene un control de las visitas al cuarto donde se encuentra el equipo.	BAJA	BAJA	MEDIA	BAJA
	MEDIA	14.5	Incendio.	Ausencia de extintores en el cuarto.	ALTA	ALTA	MEDIA	ALTA

	MEDIA	14.6	Incendio.	Las paredes del cuarto y la presencia de elementos como cajas puede ser factor para la propagación rápida del fuego.	ALTA	ALTA	MEDIA	ALTA
	MEDIA	14.7	Calentamiento del equipo	Falta de monitores de las condiciones ambientales.	MEDIA	MEDIA	MEDIA	MEDIA
15. Switches C3	MEDIA	15.1	Incendio.	En el mismo cuarto se almacena elementos ofimáticos, tales como resmas de papel y cajas.	ALTA	ALTA	MEDIA	ALTA
	MEDIA	15.2	Robo de identidad o suplantación.	Los switches están expuestos a ataques ARP Spoofing.	MEDIA	MEDIA	MEDIA	MEDIA
16. Red inalámbrica	BAJA	16.1	Robo de información	No se tiene habilitado un protocolo de cifrado que permita cifrar los datos y permitir el acceso a sólo usuarios de la UMNG.	BAJA	BAJA	ALTA	MEDIA