ACIS XI Jornada de Seguridad Informática

Seguridad de la Información:
Una nueva década para avanzar

Sistema de Medición de Riesgos en Enrutadores bajo el estándar 802.11g basándose en los lineamientos planteados por la OSSTMM

Ing. Eduardo A. García M.
Ing. Robinson J. Navarro I.
Director: Ing. Siler Amador Donado

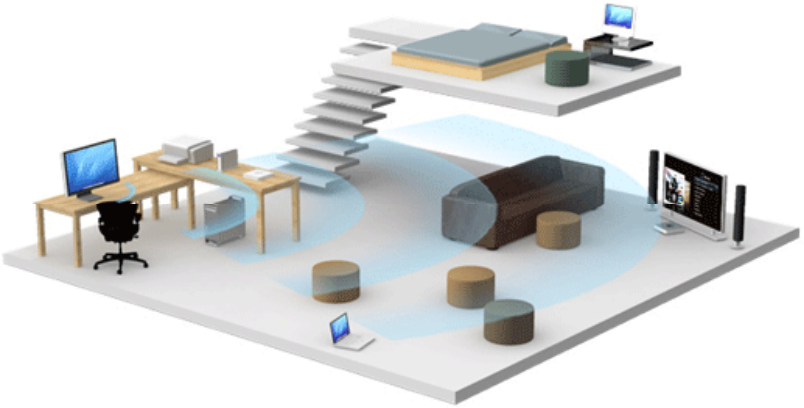
POSTERIS LUMEN MORITVRVS EDAT
1827
UNIVERSIDAD DEL CAUCA

- Planteamiento del problema
- Objetivos
- Gestión de riesgo
- Cuantificación del riesgo
- Lineamientos de seguridad
- Implementación de SiMeR
- Video
- Aportes
- Conclusiones y trabajos futuros

Planteamiento del Problema

- Internet es el servicio de mayor crecimiento con casi 28.7% de la población mundial y un crecimiento de 444.8% desde el año 2000 hasta junio de 2010 [1] .

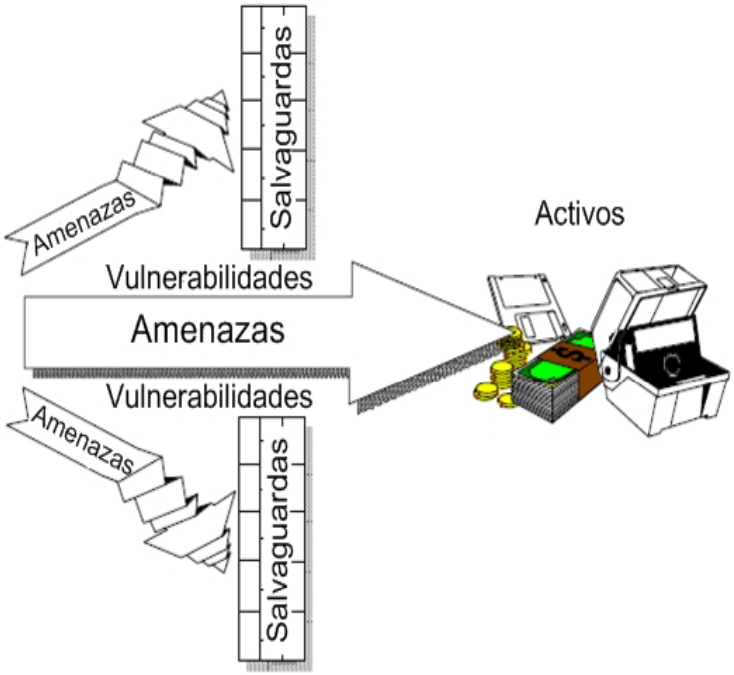
SOHO (Small Office/ Home Office)



[1] Miniwatts Marketing Group, "Internet Usage Statistics: The Internet Big Picture World Internet Users And Population Stats," Internet World Stats: Usage And Population Stadistics.

Amenazas en redes inalámbricas:

Amenazas	Probabilidad / Característica afectada
Eavesdropping	Alta / Confidencialidad
Spoofing	Media / Integridad
WarDriving	Alto / Confidencialidad
Warchalking	Baja / Confidencialidad
Negación de servicio	Media / Disponibilidad

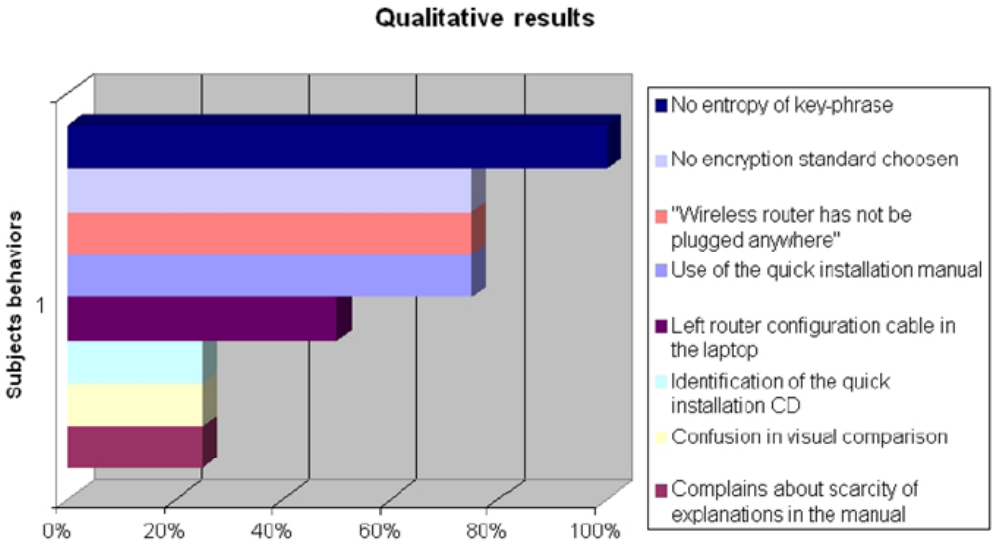


Activos

WRT54GH

Perdida:

- Confidencialidad
- Integridad
- Disponibilidad



- El enrutador viene configurado con parámetros por defecto.

- Falta de conocimiento por parte de los usuarios.

Item	Total	(%)
Redes ad-hoc	22	4.2
Redes BSS (AP)	496	96
AP'S que envian SSID	476	96
AP'S sin encriptación	203	40.9
AP'S S config. X defecto	102	20.6
Canal más usado	6	41.9
Total de detecciones	522	
AP'S 802.11B	276	56
AP'S 802.11G	217	44

Pregunta de Investigación

- ¿Cómo identificar las vulnerabilidades presentes en un enrutador utilizado para el acceso a la red inalámbrica de acuerdo a sus parámetros de configuración?

Objetivo Principal

- Definir un sistema que realice medición de riesgos basada en los lineamientos planteados por la OSSTMM (Open Source Security Testing Methodology Manual) para enrutadores que cumplan con el estándar IEEE 802.11g.

Objetivos Específicos

1. Clasificar las amenazas y vulnerabilidades que presenta un enrutador de una manera cualitativa y cuantitativa de acuerdo a las tablas de evaluación de riesgo especificadas por GAO (Government Accountability Office).
2. Generar lineamientos de seguridad a partir del manual de la metodología abierta de testeo de seguridad OSSTMM tomando como caso de estudio el estándar IEEE 802.11g.
3. Diseñar e implementar una herramienta de medición de riesgos de seguridad informática que brinde al usuario conocer la confiabilidad del dispositivo utilizado.

Objetivo Específico 1

Clasificar las amenazas y vulnerabilidades que presenta un enrutador de una manera cualitativa y cuantitativa de acuerdo a las tablas de evaluación de riesgo especificadas por GAO.

Lista de actividades

1. Estudio de la guía para gestión de riesgo GAO.
2. Selección de base de datos de Vulnerabilidades.
3. Creación de la Base de Datos SiMeR
4. Elección de Variables del enrutador.

Gestión del Riesgo

1.1 Guía para la gestión de Riesgo GAO

GAO
Accountability ★ Integrity ★ Reliability

Se utiliza para evaluar la solidez de la metodología del análisis de riesgos.

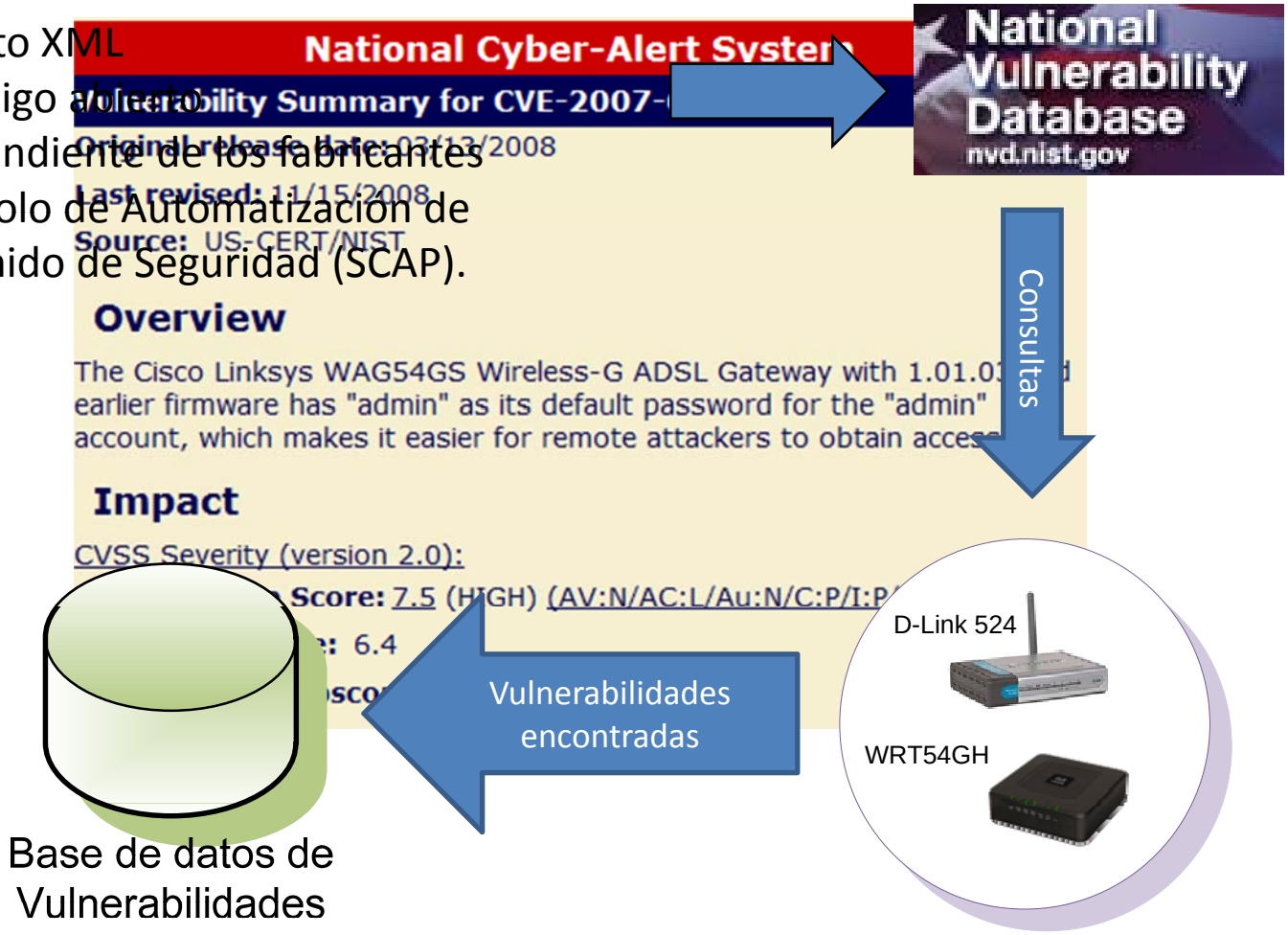
Provee procedimientos de evaluación de riesgo prácticos que han sido adoptados satisfactoriamente por organizaciones.

1.2 Selección de las Bases de Datos de Vulnerabilidades

Soporte a diferentes fabricantes
Puntaje de Severidad
Numeración
Soporte de grupos de investigación para la gestión de sus BD.

1.3 Creación Bases de Datos de SiMeR

- Formato XML
- De código abierto
- Independiente de los fabricantes
- Protocolo de Automatización de Contenido de Seguridad (SCAP).

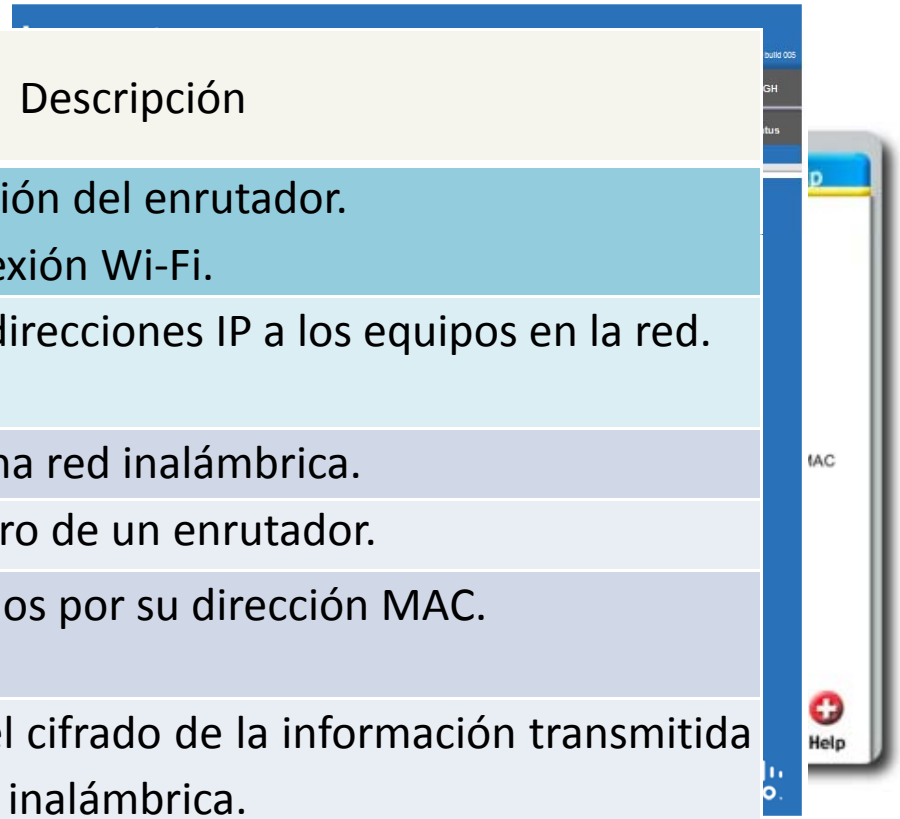


1.4 Elección de Variables del enrutador

Características de las variables escogidas.

1. Impacto en la seguridad inalámbrica.
2. Disponibilidad en la página Web de configuración del enrutador.
3. Posibilidad de cambios.

Nombre de la variable	Descripción
Contraseña	Administrar la configuración del enrutador. Obtener acceso a la Conexión Wi-Fi.
Servidor DHCP	Asignar dinámicamente direcciones IP a los equipos en la red.
SSID	Nombre que identifica una red inalámbrica.
Firmware	Software embebido dentro de un enrutador.
Filtrado MAC	Restringe acceso a usuarios por su dirección MAC.
Cifrado	Protocolos usados para el cifrado de la información transmitida a través de una conexión inalámbrica.



1.5 Elección de Variables del enrutador

Identificador CVE	Variable asociada
CVE-2009-3341	SSID
CVE-2009-1561	Contraseña
CVE-2008-1247	Contraseña
CVE-2008-1263	DHCP
CVE-2008-1264	Contraseña
CVE-2008-1265	SSID
CVE-2008-1268	Contraseña
CVE-2008-0228	Filtrado MAC
CVE-2007-1585	Firmware
CVE-2006-5202	Cifrado
CVE-2005-2915	SSID

Cont	
Filtrado MAC	Deshabilitado
Cifrado	deshabilitado
	WEP /WAP/WPA2

Cuantificación del Riesgo

Métricas de Explotabilidad

Impacto en la disponibilidad

Impacto en la integridad

Vector de Acceso: Refleja cómo de cerca un atacante debe autenticarse para poder explotar una vulnerabilidad.

Vector de Acceso (AC)	Valor
Local(L)	0.395
Red Adyacente (A)	0.646
Remoto (R)	1.0

Complejidad de Acceso: Mide la complejidad del ataque requerido para explotar la vulnerabilidad.

Complejidad de Acceso (AC)	Valor
Alta (A)	0.35
Media (M)	0.61
Baja (B)	0.71

Simple (S)	0.56
Ninguna (N)	
Alta	0.660
Media	0.275
Baja	0.0

Formulas CVSS para encontrar la severidad de las variables identificadas.

$$BaseScore = \left((0.6 * Impact) + (0.4 * Exploitability) - 1.5\right) * f(\quad)Impact$$

$$Impact = 10.41 * (1 - (1 - ImpConf) * (1 - ImpInt) * (1 - ImpDisp))$$

$$Explotabilidad = 20 * VectorAcceso * CompAccess * Autentificacion$$

$$f(Impact) = 0 \; si \; Impact = 0$$

$$f(Impact) = 1.176 \; si \; Impact \neq 0$$

Cuantificación del Riesgo

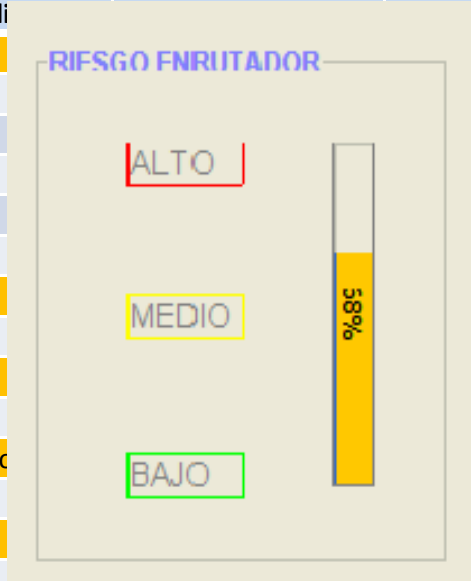
$$Riesgo = Probabilidad\ de\ ocurrencia * Severidad$$ [3]

Encuesta para obtener la probabilidad de ocurrencia [2].

Calculo del riesgo en el enrutador con sus parámetros por defecto.

Riesgo total que presenta el enrutador con parámetros por defecto.

Variable	Estado de vulnerabili	Probabilidad de	Puntaje de veridad	Riesgo
Contraseña de Administración	Débil		9,4	6,60
	Mediana		6,98	1,75
	Fuerte		1,74	0,09
Contraseña Wi-Fi	Débil		9,67	5,56
	Mediana		7,48	2,62
	Fuerte		1,74	0,13
Servidor DHCP	Habilitado		7,79	7,59
	Deshabilitado		1,74	0,04
Difusión SSID	Habilitado		8,47	7,20
	Deshabilitado		1,74	0,26
FirmWare	Desactualizado		8,01	7,41
	Actualizado		1,74	0,04
Filtrado MAC	Deshabilitado		4,75	4,63
	Habilitado	0,025	1,45	0,04
Cifrado	Deshabilitado	0,725	9,67	7,01
	WEP	0,175	7,48	1,31
	WPA	0,05	3,56	0,18
	WPA2	0,05	1,74	0,09



[2] GAO: "Information Security Risk Assessment: practices of leading organizations"
[3] https://spreadsheets.google.com/viewform?formkey=dDkxcUdgOEqbRpqWVvN0w4aVpqbUE6MQ

Objetivos Específico 2

2. Generar lineamientos de seguridad a partir del manual de la metodología abierta de testeo de seguridad OSSTMM tomando como caso de estudio el estándar IEEE 802.11g.

Lista de actividades

1. Estudio de OSSTMM.
2. Generación de lineamientos SiMeR.
3. Creación de controles.

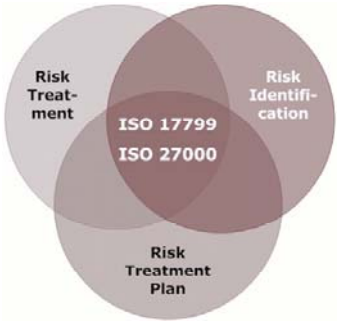
Lineamientos de Seguridad

2.1 Estudio de OSSTMM

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

Construida sobre las mejores practicas de fuentes como:

NIST
MITRE
ITIL



AUDITORIAS

SANS IT AUDIT with David Hoelzer
GIAC Global Information Assurance Certification

FABRICANTES

White Papers y recomendaciones de los fabricantes.

LINKSYS by Cisco Knowledge Base
D-Link
AirLink 101
3com
ENCORE ELECTRONICS
BELKIN
NETGEAR
TRENDnet

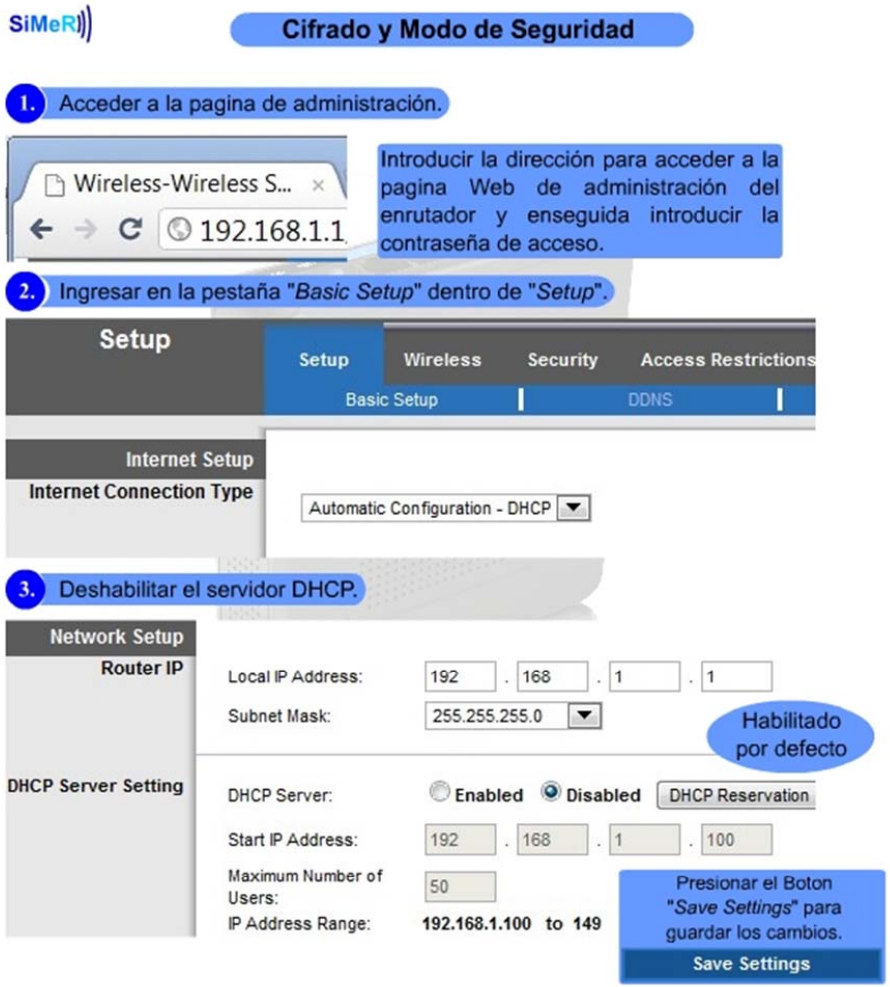
Lineamientos de Seguridad

OSSTMM
www.osstmm.org
Open Source Security Testing Methodology Manual

2.2 Generación de lineamientos SiMeR

Lineamiento	Acción
Proteger el Acceso a la red inalámbrica	Fortalecer la contraseña.
Proteger el acceso a la página de configuración del enrutador.	Cambiar regularmente el nombre de usuario y contraseña.
Actualizar Firmware	Realizar la verificación de la versión del Firmware.
Difusión del SSID	Desactivar su difusión.
Elegir un modo de Autenticación	Habilitar el modo de seguridad
Configuración del servidor DHCP	Deshabilitar el parámetro DHCP y crear una lista propia de usuarios autorizados.
Filtrado MAC	Habilitar y registrar la dirección MAC de los equipos autorizados

2.3 Creación de controles



Objetivo específico 3

3. Diseñar e implementar una herramienta de análisis de medición de riesgos de seguridad informática que brinde al usuario conocer la confiabilidad del dispositivo utilizado.

Lista de actividades

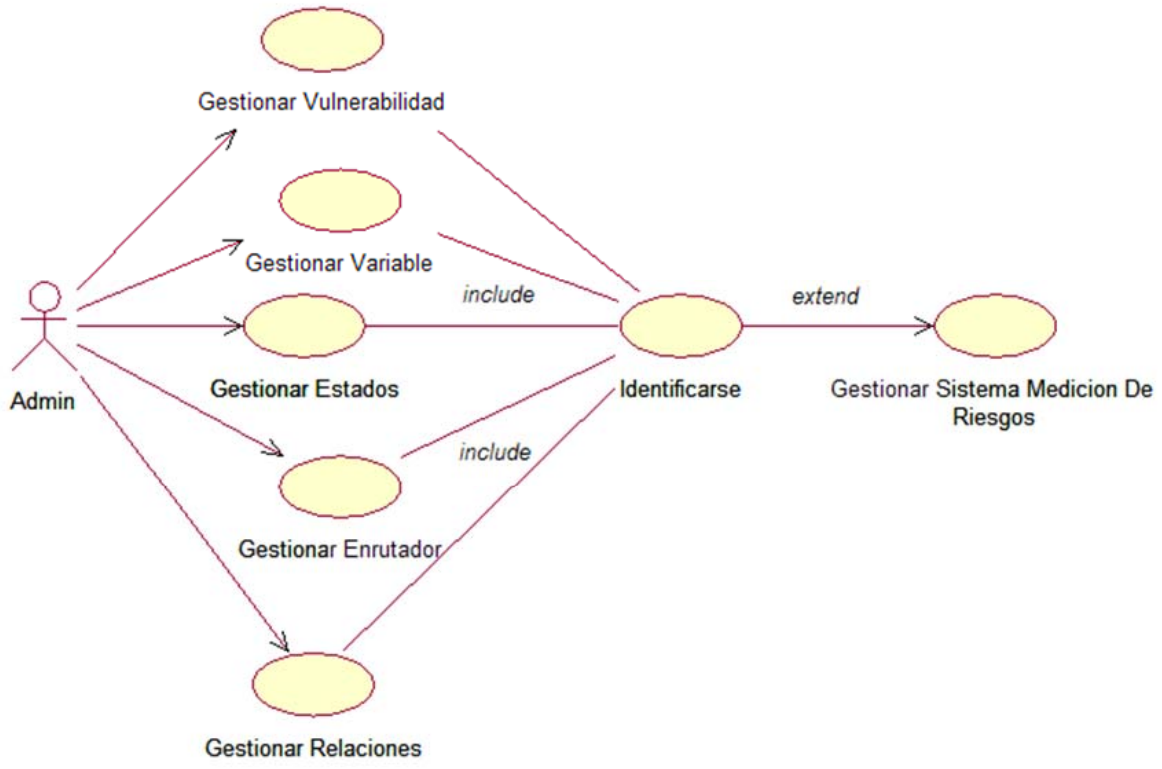
1. Definición de requerimientos del sistema.
2. Diseño de SiMeR.
3. Implementación del sistema.
4. Pruebas al sistema.

3.1 Definición de requerimientos del sistema

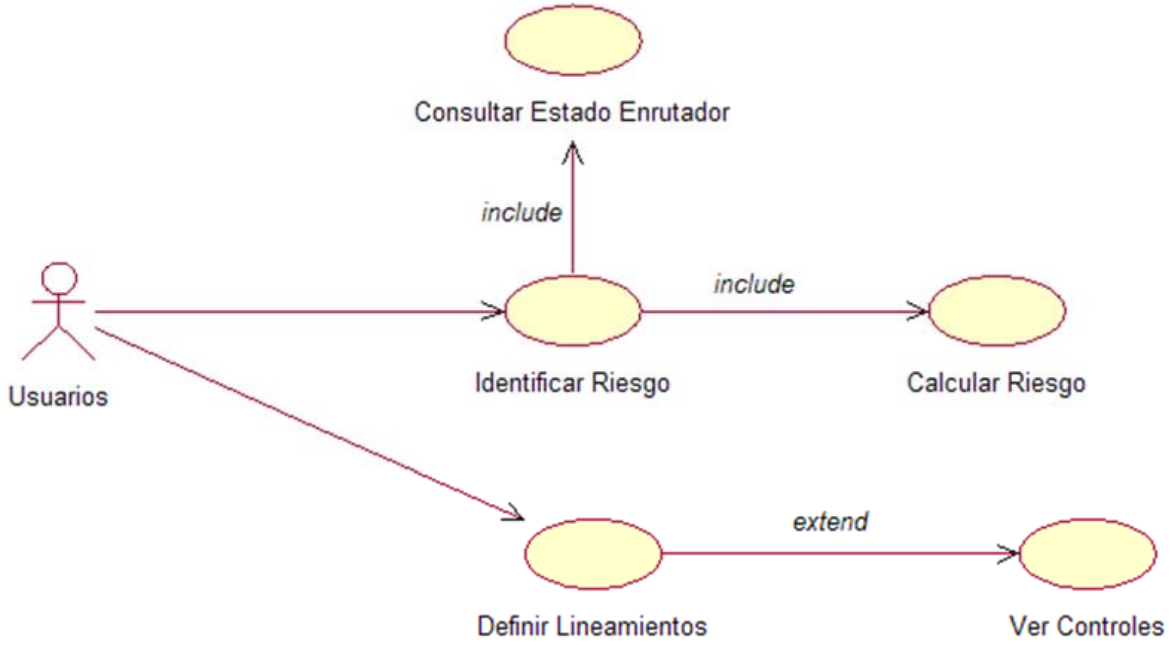
- Gestionar las vulnerabilidades, enrutadores y variables.
- Presentar el estado actual de la configuración del enrutador.
- Calcular el nivel de riesgo que presenta el enrutador.
- Presentar de manera gráfica y detallada los controles para mitigar el riesgo.

Implementación de SiMeR

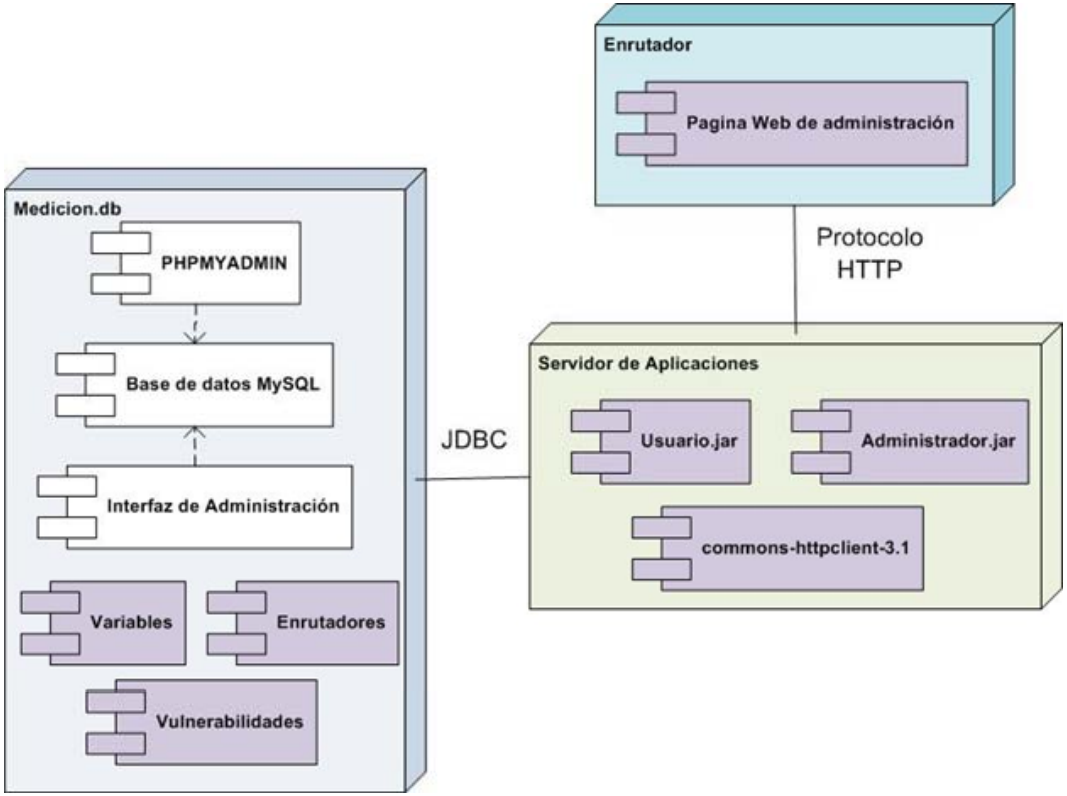
3.2 Diseño Casos de uso



3.2 Diseño Casos de uso



3.2 Diseño Diagrama de Despliegue



3.3 Implementación del sistema

- Entorno de desarrollo.
- Lenguaje de programación.
- Librerías.
- Base de Datos.

JAKARTA COMMONS
HTTPCLIENT

The Apache Software Foundation
http://www.apache.org/

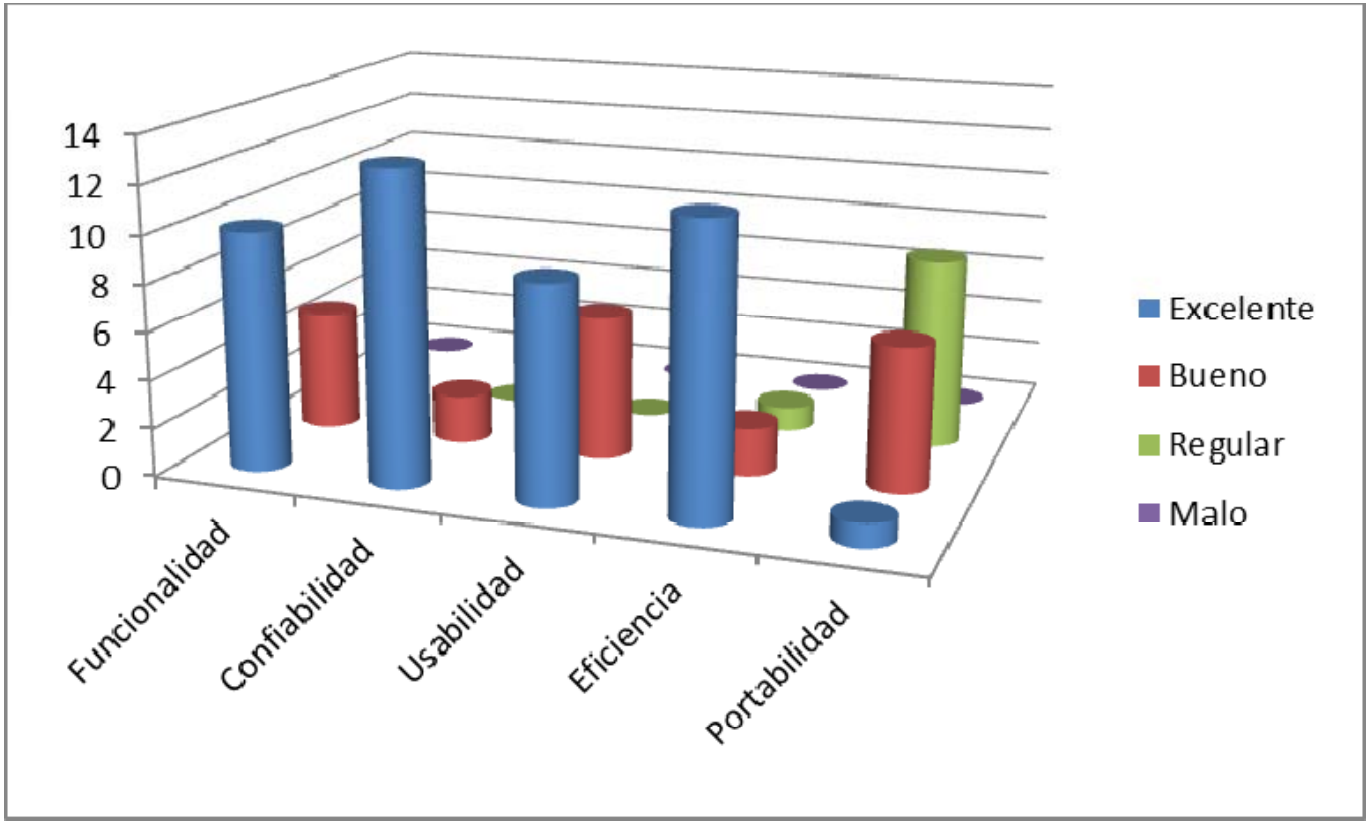
3.4 Pruebas del Prototipo

A nivel **Funcional** se verificó:

- Las interfaces de despliegue
- La conexión con la Base de Datos
- La adición de información por parte del administrador.
- El acceso por parte del usuario al sistema.
- El estado actual del enrutador a través de SiMeR.
- La cuantificación del riesgo.
- Disminución del riesgo al ejecutar cada uno de los controles.

3.5 Pruebas del Prototipo

Con un **Usuario SOHO**: se aplico una encuesta, la cual midió:



Video

Aportes

- Lineamientos para la disminución del riesgo basándose en OSSTMM.
- Sistema de medición de riesgos aplicado a los enrutadores 802.11g SOHO.
- Nivel de riesgo del dispositivo inalámbrico a partir de los elementos considerados por la matriz de evaluación propuesta por GAO.
- Base de Datos que recopila las vulnerabilidades de los enrutadores analizados.
- Incursión en sistemas de seguridad aplicados a usuario SOHO.

Conclusiones

- Disminución del riesgo presente en los enrutadores 802.11g con las variables seleccionadas y la aplicación de los lineamientos de seguridad propuestos.
- Protección de la información mediante la adecuada configuración de los parámetros del enrutador.
- Desconocimiento por parte de los usuarios SoHo del conjunto de parámetros configurables de los enrutadores que les permitirán proteger sus activos.
- SiMeR fue concebido inicialmente como un sistema de medición del riesgo, adicionalmente brinda un conjunto de controles gráficos que le permiten aumentar su nivel de seguridad.

Trabajos futuros

- Adicionar a la base de datos del sistema mas enrutadores que cumplan con el estándar 802.11g.
- Automatizar algunos de los controles que se sugieren al usuario.

POSTERIS LVMEN MORITVRVS EDAT
1827
UNIVERSIDAD DEL CAUCA
Universidad
del Cauca