ANÁLISIS DE RIESGOS POR VULNERABILIDADES EN LAS INFRAESTRUCTURAS TECNOLÓGICAS DE LAS REDES EMPRESARIALES

Angel Chinchero Villacís, Quito-Ecuador

***Resumen*— Este documento establece un modelo de guía para el análisis cualitativo y cuantitativo de los niveles de riesgo por vulnerabilidades o inseguridades de las infraestructuras tecnológicas en las redes empresariales, en función de la medición del nivel de seguridad informática. [1]**

I. INTRODUCCIÓN

Los riesgos tecnológicos son todos los elementos que afectan a la estructura, el funcionamiento, la disponibilidad, la privacidad, la integridad de la información, la calidad de los procesos y la imagen de las empresas.

Para el Análisis Cualitativo y Cuantitativo de los Riesgos de las Infraestructuras Tecnológicas Actuales ocasionados por las vulnerabilidades informáticas, se requiere realizar las siguientes tareas:

- Análisis de la situación actual de la infraestructura tecnológica.
- Análisis del nivel de seguridad informática de la infraestructura tecnológica actual

El marco referencial utilizado para la evaluación de los riesgos por inseguridades o vulnerabilidades informáticas se indica en la Fig. 1.

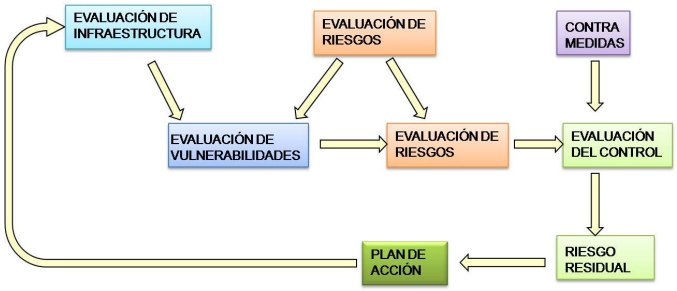

Fig. 1. Marco referencial para el Análisis de Riesgos

Las vulnerabilidades se refieren a la exposición que tiene la infraestructura a los diferentes riesgos.

La evaluación de los riesgos corresponde a la ponderación de los diferentes riesgos que pueden existir en cada uno de los elementos integrantes de la infraestructura tecnológica.

Los procesos para la gestión de los riesgos en tecnología se indican en la Fig. 2, en el cual se realizan las siguientes tareas: [7]

- Medición de los parámetros importantes de los elementos que más influyen en el funcionamiento del negocio.
- Evaluación de los riesgos involucrados en cada uno de los elementos funcionales del negocio.
- Mejoramiento continúo de los elementos influyentes, para reducir o eliminar los riesgos que afecten al funcionamiento del negocio.

Fig. 2. Proceso de gestión de riesgos.

El análisis de los riesgos de la infraestructura actual, se lo realiza mediante:

- La identificación de los riesgos en cada uno de los elementos de la red de datos actual.
- La valoración de la probabilidad de ocurrencia del riesgo.
- La valoración de la importancia del riesgo en la infraestructura.

II. ANÁLISIS DEL NIVEL DE SEGURIDAD INFORMÁTICA DE LA INFRAESTRUCTURA TECNOLÓGICA

Para el análisis del nivel de seguridad de la infraestructura, se realiza:

- El cálculo del nivel de riesgo por vulnerabilidades detectadas.
- El cálculo del nivel de protección entregado por los equipos y sistemas de seguridad.
- El cálculo del nivel de riesgo real por inseguridades en función del nivel de riesgo por vulnerabilidades detectadas y el nivel de protección entregado por los equipos y sistemas de seguridad.

A. Nivel de riesgo por vulnerabilidades detectadas

Los niveles de riesgo por vulnerabilidades informáticas detectadas se miden en base a los niveles de vulnerabilidad detectados en cada unos los equipos y a la importancia de estos equipos dentro de la red de datos, utilizando (1) y (2) y la Tabla I. [4], [5], [8]

$$\text{Nivel de riesgo acumulado por vulnerabilidades} = \sum_{i=1}^{n}\left(\text{Nivel de vulnerabilidad}_{(i)}\right) * \text{Importancia}_{(i)} \quad (1)$$

$$\text{Nivel de riesgo por vulnerabilidad detectadas} = \frac{\sum_{i=1}^{n} \text{Nivel de vulnerabilidad}_{(i)} * \text{Importancia}_{(i)}}{\sum_{i=1}^{n} \text{Importancia}_{(i)}} \quad (2)$$

TABLA I
CÁLCULO DEL NIVEL DE RIESGO ACUMULADO POR INSEGURIDAD

NIVEL DE VULNERABILIDAD DETECTADA	
CRITERIO	NIVEL
Mínimo -	1
Mínimo +	2
Bajo -	3
Bajo +	4
Medio -	5
Medio	6
Alto -	7
Alto +	8
Crítico -	9
Crítico +	10

x

IMPORTANCIA DEL EQUIPO	
CRITERIO	NIVEL
Bajo	1
Normal	2
Alto	3
Crítico	4

=

NIVEL DE RIESGO ACUMULADO POR VULNERABILIDAD	
CRITERIO	NIVEL
Mínimo -	4
Mínimo +	8
Bajo -	12
Bajo +	16
Medio -	20
Medio +	24
Alto -	28
Alto +	32
Crítico -	36
Crítico +	40

El nivel de vulnerabilidad de la red, se lo puede medir mediante el cálculo de los niveles de vulnerabilidad detectados en los siguientes equipos:

- Servidores
- Usuarios
- Equipos de comunicaciones
- Sistemas de seguridad informática

1) Nivel de vulnerabilidad promedio de Servidores

El nivel de vulnerabilidad promedio de los servidores de comunicaciones, servidores de correo electrónico, servidor web, servidores de producción y desarrollo, se obtiene en forma individual mediante el analizador de vulnerabilidades GFI-LanGuard 9.5, GFI Report Center, como muestra en las Fig. 3, Fig. 4, Fig. 5, Fig. 6, Fig. 7 y Fig. 8, y cuyos resultados se resumen en la Tabla II.

TABLA II
NIVEL DE RIESGO DE LOS SERVIDORES

SERVIDORES	NIVEL DE RIESGO	
	Criterio	Valor Medido
Servidor de Producción 1	Alto +	8/10
Servidor de Producción 2	Alto +	8/10
Servidor de Producción 3	Alto +	8/10
Servidor de Producción 4	Alto +	8/10
Servidor Web	Alto +	8/10
Servidor de Desarrollo 1	Alto +	8/10
Servidor de Desarrollo 2	Alto +	8/10
Servidor de Comunicaciones	Alto +	8/10
Servidor de Correo electrónico	Alto +	8/10

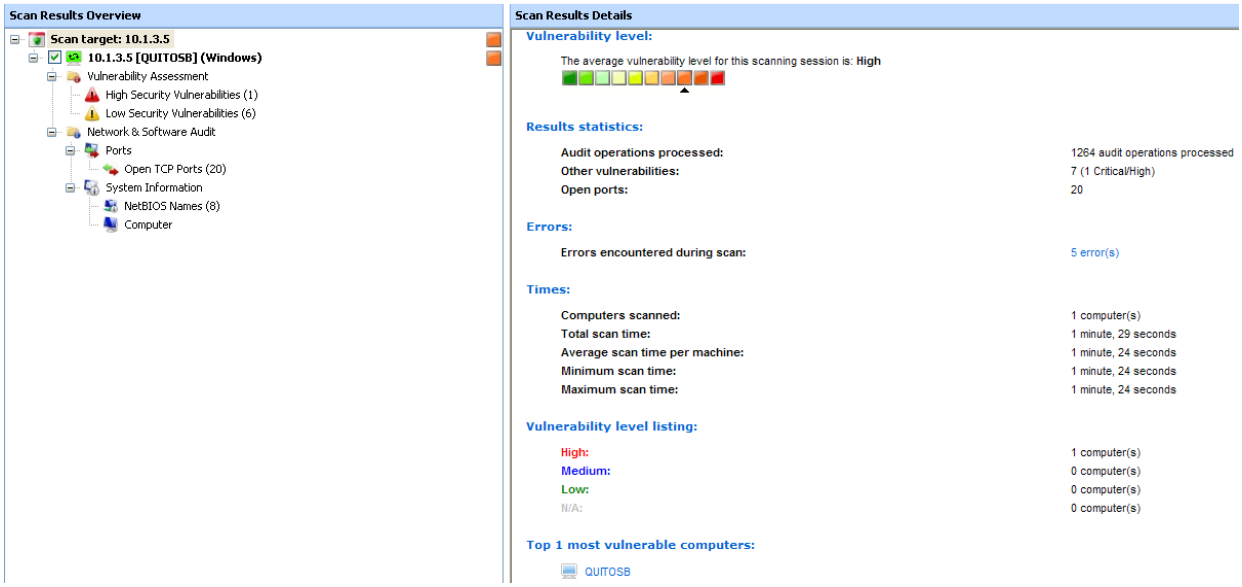

Fig. 3. Ejemplo de reporte de vulnerabilidades en el Servidor de Comunicaciones

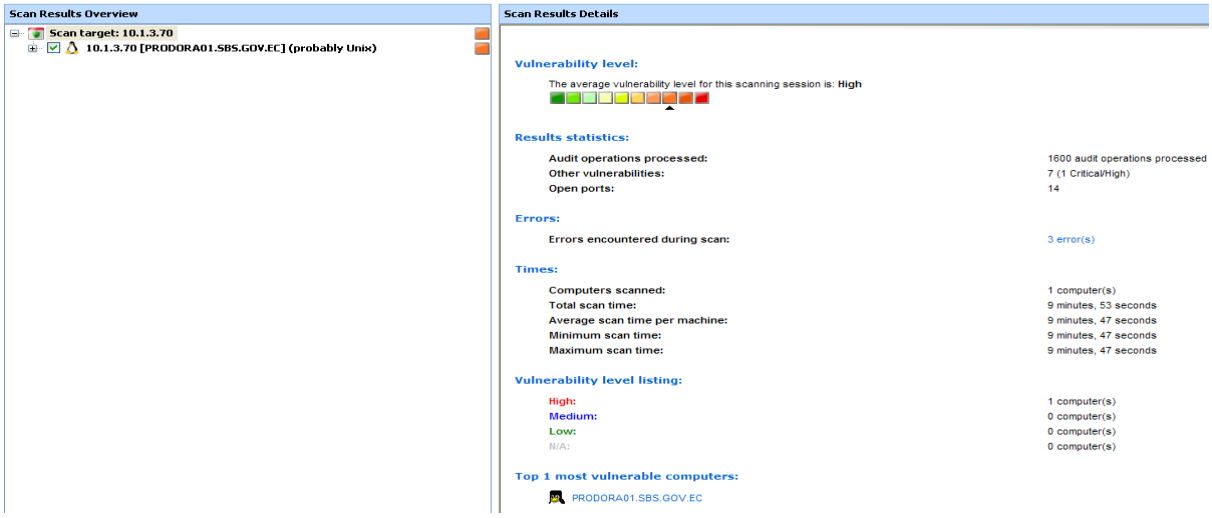

Fig. 4. Reporte de vulnerabilidades en Servidor de Producción 1

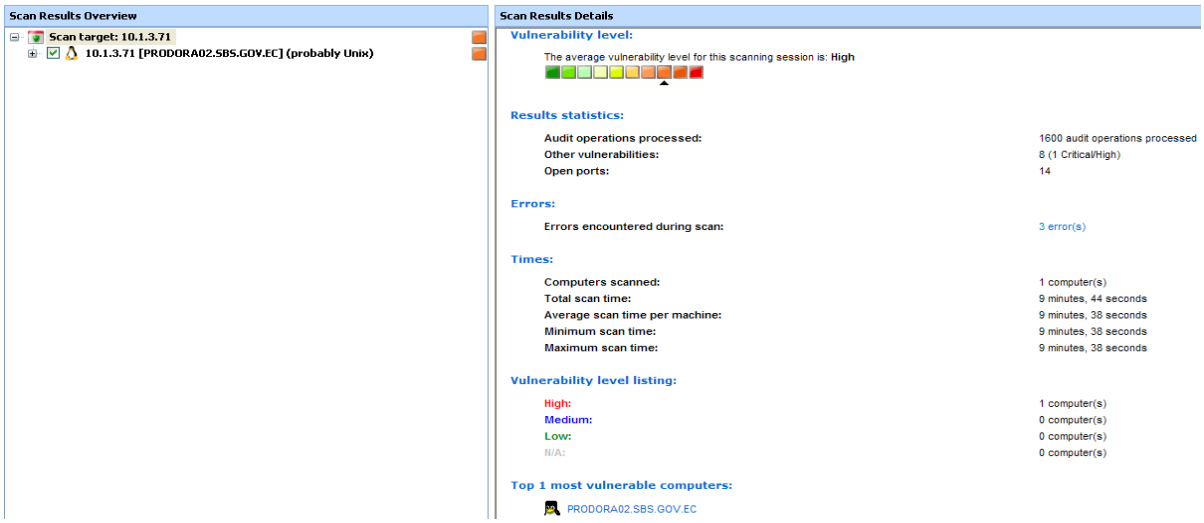

Fig. 5. Reporte de vulnerabilidades en Servidor de Producción 2

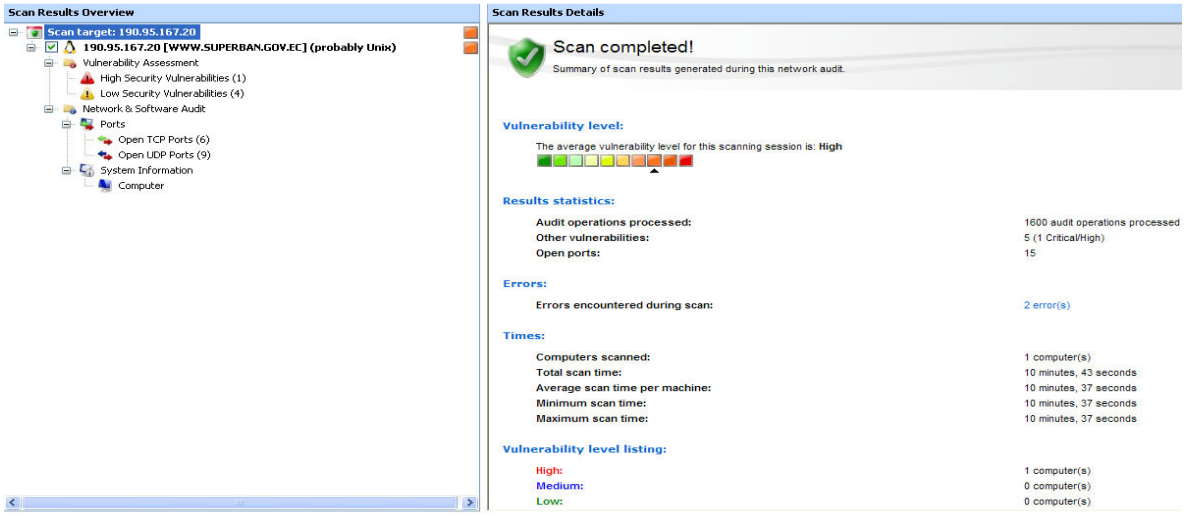

Fig. 6. Reporte de vulnerabilidades en Servidor de Web

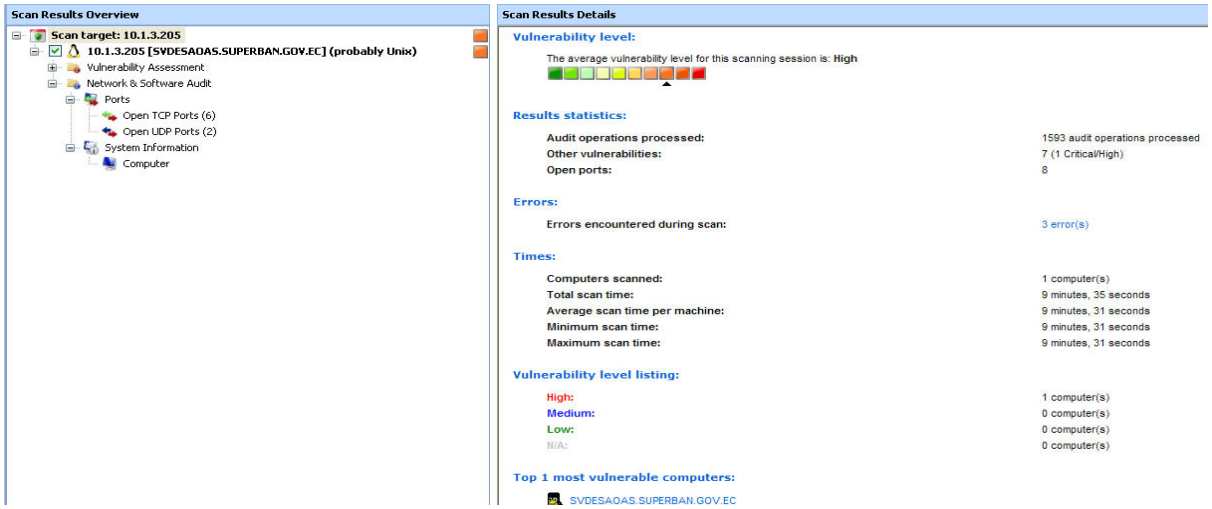

Fig. 7. Reporte de vulnerabilidades en Servidor de Desarrollo 1

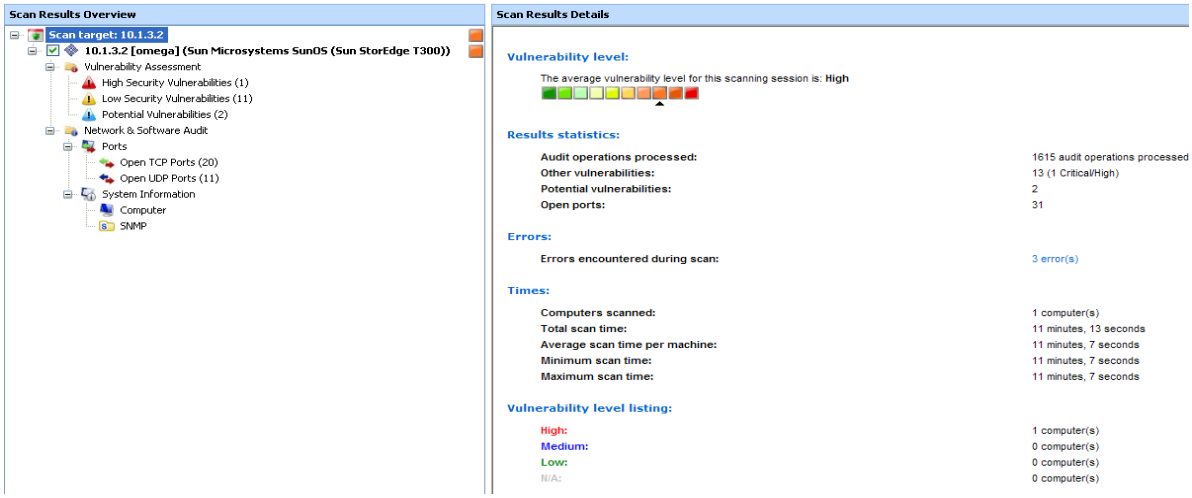

Fig. 8. Reporte de vulnerabilidades en Servidor de Correo Electrónico

2) Nivel de vulnerabilidad promedio de Usuarios

El nivel de vulnerabilidad promedio de los usuarios se obtiene, analizando las vulnerabilidades en cada uno de los segmentos de red internos, mediante el analizador de vulnerabilidades GFI-LanGuard 9.5, GFI Report Center, como muestran los reportes de las Fig. 9, Fig. 10, Fig. 11, Fig. 12 y Fig. 13 cuyos resultados se resumen en la Tabla III.

TABLA III
RESUMEN DE NIVEL DE RIESGO DE LOS USUARIOS INTERNOS.

USUARIOS INTERNOS	NIVEL DE RIESGO	
	Criterio	Valor Medido
Subred 10.1.0.0/24	Alto +	8/10
Subred 10.1.1.0/24	Alto +	8/10
Subred 10.1.2.0/24	Alto +	8/10
Subred 10.1.4.0/24	Alto +	8/10
Subred 10.1.5.0/24	Alto +	8/10

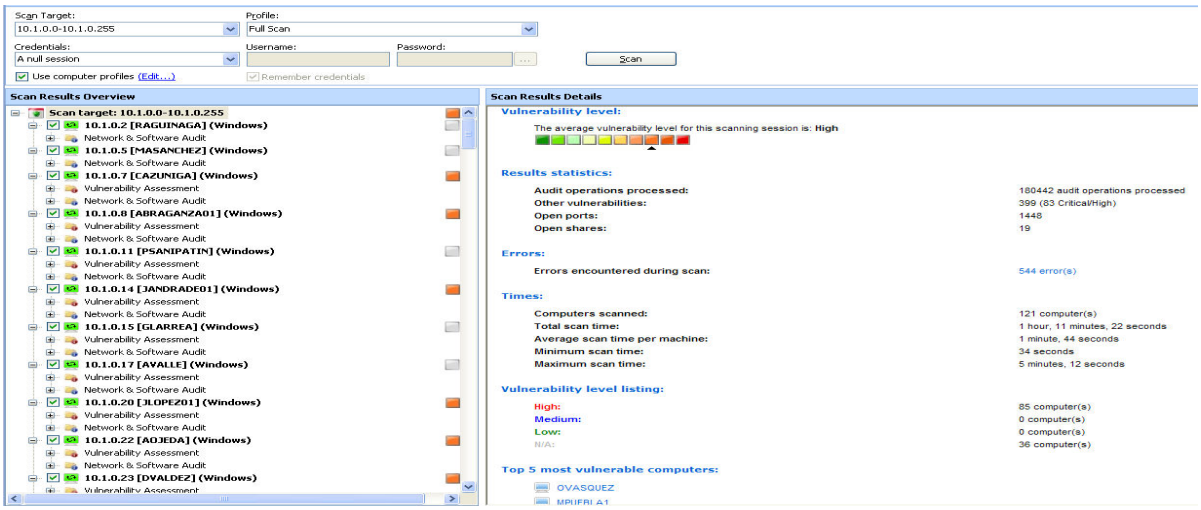

Fig. 9. Reporte de vulnerabilidades del segmento de red 10.1.0.0/24

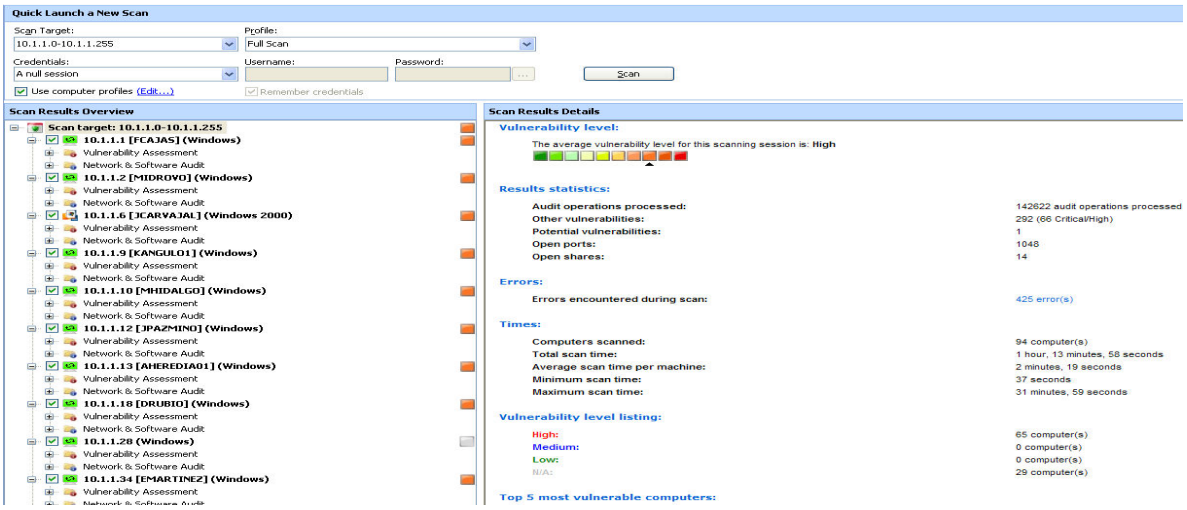

Fig. 10. Reporte de vulnerabilidades del segmento 10.1.1.0/24

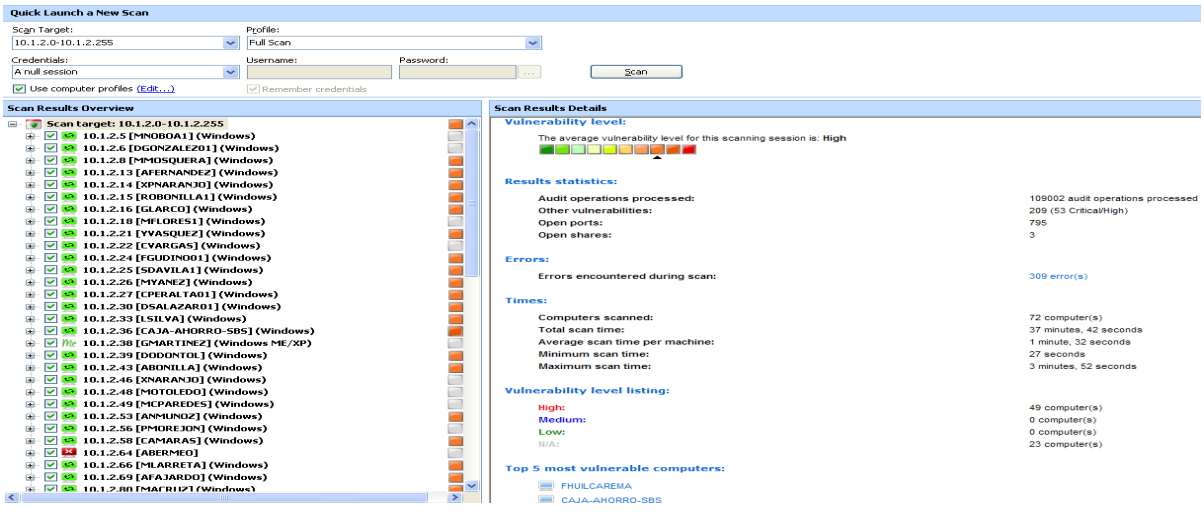

Fig. 11. Reporte de vulnerabilidades del segmento 10.1.2.0/24

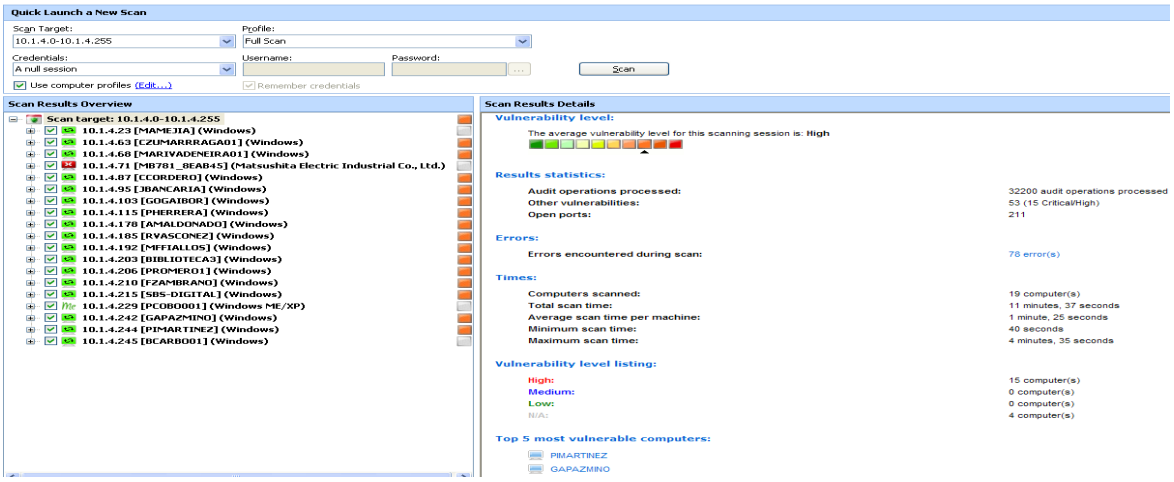

Fig. 12. Reporte de vulnerabilidades del segmento 10.1.4.0/24

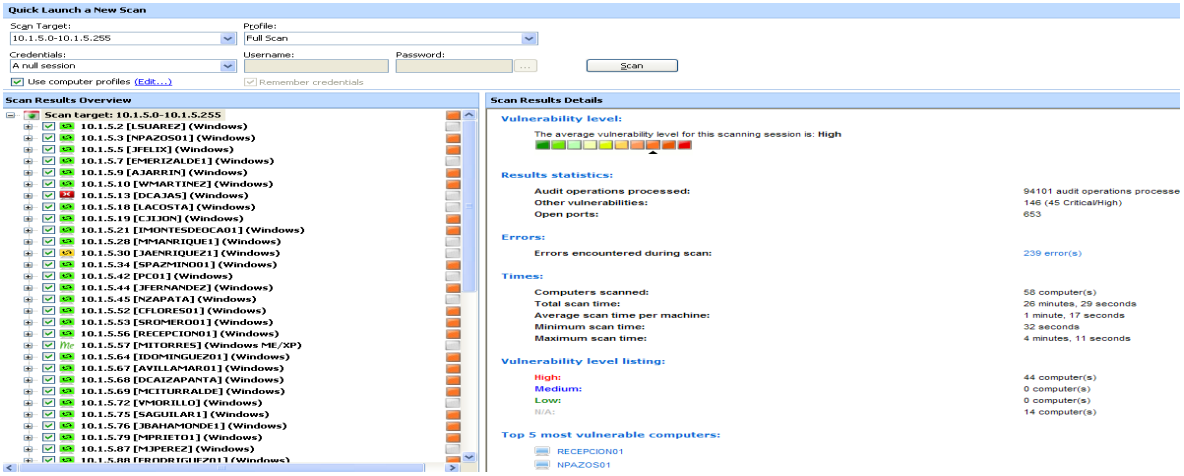

Fig. 13 Reporte de vulnerabilidades del segmento 10.1.5.0/24

3) Nivel de vulnerabilidad de los equipos de comunicaciones

El cálculo del nivel de vulnerabilidad de los equipos de comunicaciones en los que se incluyen a los equipo de red activos y sistemas de seguridad informática, se realiza utilizando los reportes de Nessus 4 y considerando los niveles de riesgo de las vulnerabilidades descrito en la Tabla IV.

Para cada uno de los equipos de comunicaciones analizados, se obtiene los reportes con la cantidad de vulnerabilidades de cada nivel como indican los ejemplos de las Fig. 14, Fig. 15 y Fig. 16.

TABLA IV
NIVEL DE RIESGO DE LAS VULNERABILIDADES

NIVEL DE RIESGO DE LAS VULNERABILIDADES		
Criterio	**Valor**	**Porcentaje**
. Mínimo -	1	10 %
. Mínimo +	2	20 %
. Bajo -	3	30 %
. Bajo +	4	40 %
. Medio -	5	50 %
. Medio +	6	60 %
. Alto -	7	70 %
. Alto +	8	80 %
. Crítico -	9	90 %
. Crítico +	10	100 %

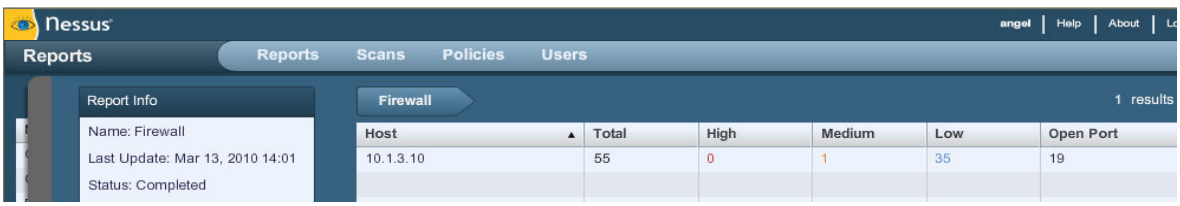

Fig. 14. Ejemplo de reporte de vulnerabilidades detectadas en el Firewall

Fig. 15. Ejemplo de reporte de vulnerabilidades detectadas en el Sistema de Protección de Intrusos

Fig. 16. Ejemplo de reporte de vulnerabilidades detectadas en el Sistema de Filtrado de Correo

El nivel de vulnerabilidad de cada equipo de comunicaciones se obtiene mediante (3) y (4):

$$\text{Nivel de Vulnerabilidad} = \frac{\sum_{i=1}^{10}\left(\text{Número de vulnerabilidades(i)}\right)*\left(\text{Nivel de riesgo de la vulnerabilidad(i)}\right)}{\sum_{i=1}^{10}\text{Número de vulnerabilidades(i)}} \quad (3)$$

$$\text{Nivel de Vulnerabilidad} = \frac{\text{Riesgo Acumulado Total}}{\text{Cantidad total de vulnerabilidades}} \quad (4)$$

Estos cálculos se indican en la Tabla V.

TABLA V
NIVEL DE VULNERABILIDAD DE EQUIPOS DE COMUNICACIONES UTILIZANDO NESSUS 4

EQUIPOS	NÚMERO DE VULNERABILIDADES	NIVEL DE RIESGO DE LA VULNERABILIDAD		RIESGO ACUMULADO	NIVEL DE VULNERABILIDAD Riesgo Acumulado Total / Total de Vulnerabilidades	
		Criterio	Valor		Criterio	Valor
FIREWALL						
		Mínimo -	1	0		
		Mínimo +	2	0		
	35	Bajo -	3	105		
		Bajo +	4	0		
		Medio -	5	0		
	1	Medio +	6	6		
		Alto -	7	0		
		Alto +	8	0		
		Crítico -	9	0		
		Crítico +	10	0		
	36			111,00	BAJO +	3,08
IPS						
		Mínimo -	1	0		
		Mínimo +	2	0		
	23	Bajo -	3	69		
		Bajo +	4	0		
		Medio -	5	0		
	4	Medio +	6	24		
		Alto -	7	0		
		Alto +	8	0		
		Crítico -	9	0		
		Crítico +	10	0		
	27			93,00	BAJO +	3,44
MAIL FILTER						
		Mínimo -	1	0		
		Mínimo +	2	0		
	31	Bajo -	3	93		
		Bajo +	4	0		
		Medio -	5	0		
	1	Medio +	6	6		
		Alto -	7	0		
		Alto +	8	0		
		Crítico -	9	0		
		Crítico +	10	0		
	32			99,00	BAJO +	3,09
SWITCH DE NUCLEO						
		Mínimo -	1	0		
		Mínimo +	2	0		
	12	Bajo -	3	36		
		Bajo +	4	0		
		Medio -	5	0		
	1	Medio +	6	6		
		Alto -	7	0		
		Alto +	8	0		
		Crítico -	9	0		
		Crítico +	10	0		
	13			42,00	BAJO +	3,23
SWITCHES DE ACCESO						
		Mínimo -	1	0		
		Mínimo +	2	0		
	9	Bajo -	3	27		
		Bajo +	4	0		
		Medio -	5	0		
		Medio +	6	0		
		Alto -	7	0		
		Alto +	8	0		
		Crítico -	9	0		
		Crítico +	10	0		
	9			27,00	BAJO -	3,00

Con la información obtenida se genera una matriz de riesgos, la cual se utiliza para calcular el nivel de riesgo por vulnerabilidades detectadas en la red de datos.

El resumen de los cálculos de los niveles de vulnerabilidad se indica en la Tabla VI.

TABLA VI
RESUMEN DE NIVELES DE VULNERABILIDAD DETECTADOS EN LA RED DE DATOS

IDENTIFICACIÓN DEL RIESGO	HERRAMIENTA UTILIZADA	NIVEL DE VULNERABILIDAD PARCIAL		IMPORTANCIA DEL EQUIPO		NIVEL DE RIESGO ACUMULADO POR VULNERABILIDAD	
		CRITERIO	VALOR	CRITERIO	VALOR	CRITERIO	VALOR
EQUIPOS ACTIVOS DE RED LAN							
• 1 Switch de Núcleo de fibra óptica	Nessus 4	. Bajo -	3	Crítico	4	Bajo -	12
• 3 Switches de Núcleo RJ45	Nessus 4	. Bajo -	3	Crítico	4	Bajo -	12
• 37 Switches de Acceso	Nessus 4	. Bajo -	3	Alto	3	Bajo -	9
		BAJO -	3			BAJO -	11
SISTEMA DE SEGURIDAD INFORMÁTICA							
• Firewall	Nessus 4	. Bajo -	3	Crítico	4	Bajo -	12
• IPS	Nessus 4	. Bajo -	3	Alto	3	Bajo -	9
• Mail Filter	Nessus 4	. Bajo -	3	Alto	3	Bajo -	9
		BAJO -	3			BAJO -	10
SERVIDORES DE COMUNICACIONES							
• Servidor de Dominio	GFILanguard 9	. Alto +	8	Crítico	4	Alto +	32
• Servidor de Filtrado Web	GFILanguard 9	. Alto +	8	Alto	3	Mínimo +	24
• Servidor de monitoreo de servicios	GFILanguard 9	. Alto +	8	Alto	3	Mínimo +	24
		ALTO +	8,00			ALTO -	26,67
SERVIDOR DE CORREO ELECTRÓNICO							
• Servidor de Correo	GFILanguard 9	. Alto +	8	Crítico	4	Alto +	32
		ALTO +	8			ALTO +	32
SERVIDOR WEB							
• Servidor Web	GFILanguard 9	. Crítico -	9	Crítico	4	Crítico -	36
		CRÍTICO -	9			CRÍTICO -	36
SERVIDOR S FTP							
• Servidor FTP Seguro	GFILanguard 9	. Alto +	8	Crítico	4	Alto +	32
		ALTO +	8			ALTO +	32
SERVIDORES DE PRODUCCIÓN							
• Servidor Producción 1	GFILanguard 9	. Alto +	8	Crítico	4	Alto +	32
• Servidor Producción 2	GFILanguard 9	. Alto +	8	Crítico	4	Alto +	32
• Servidor Producción 3	GFILanguard 9	. Crítico -	9	Crítico	4	Crítico -	36
• Servidor Producción 4	GFILanguard 9	. Alto +	8	Alto	3	Mínimo +	24
		CRÍTICO -	8,25			ALTO +	31
SERVIDORES DE DESARROLLO							
• Servidor Desarrollo 1	GFILanguard 9	. Alto +	8	Alto	3	Mínimo +	24
• Servidor Desarrollo 2	GFILanguard 9	. Alto +	8	Alto	3	Mínimo +	24
		ALTO +	8			MÍNIMO +	24
USUARIOS INTERNOS							
• Subred 10.1.0.0/24	GFILanguard 9	. Alto +	8	Normal	2	Bajo +	16
• Subred 10.1.1.0/24	GFILanguard 9	. Alto +	8	Normal	2	Bajo +	16
• Subred 10.1.2.0/24	GFILanguard 9	. Alto +	8	Normal	2	Bajo +	16
• Subred 10.1.4.0/24	GFILanguard 9	. Alto +	8	Normal	2	Bajo +	16
• Subred 10.1.5.0/24	GFILanguard 9	. Alto +	8	Normal	2	Bajo +	16
		ALTO +	8			BAJO +	16,00
				TOTAL	**74**		**495,00**

TOTAL DE RIESGO ACUMULADO POR VULNERABILIDADES DETECTADAS	495,00	
TOTAL DE IMPORTANCIA DE EQUIPOS	74	
NIVEL DE RIESGO POR VULNERABILIDADES DETECTADAS SOBRE 10	**6,69**	**ALTO -**
NIVEL DE RIESGO POR VULNERABILIDAD DETECTADAS 100 %	**66,9%**	**ALTO -**

De acuerdo a la Tabla VI, el nivel de riesgo por las vulnerabilidades detectadas en la infraestructura actual es (**6,69 / 10**), correspondiente al **66,9 %** de vulnerabilidad.

B. Nivel de protección proporcionado por los Sistemas de Seguridad Informática

El nivel de protección entregado por los equipos de seguridad informática, se calcula en base a los niveles de protección que proporcionan cada uno de ellos y a su respectiva importancia o influencia en la red de datos, utilizando (5) y (6) y la Tabla VII. [4], [8]

$$\text{Nivel de Protección Acumulada} = \sum_{i=1}^{n} \text{Nivel de Protección}_{(i)} * \text{Importancia}_{(i)} \quad (5)$$

$$\text{Nivel de Protección} = \frac{\sum_{i=1}^{n} \text{Nivel de Protección}_{(i)} * \text{Importancia}_{(i)}}{\sum_{i=1}^{n} \text{Importancia}_{(i)}} \quad (6)$$

TABLA VII
CÁLCULO DEL NIVEL DE PROTECCIÓN ACUMULADA POR EQUIPOS DE SEGURIDAD INFORMÁTICA

NIVEL DE PROTECCIÓN PROPORCIONADA	
CRITERIO	NIVEL
Mínimo -	1
Mínimo +	2
Bajo -	3
Bajo +	4
Medio -	5
Medio +	6
Alto -	7
Alto +	8
Excelente -	9
Excelente +	10

x

IMPORTANCIA DEL EQUIPO	
CRITERIO	NIVEL
Bajo	1
Normal	2
Alto	3
Crítico	4

=

NIVEL DE PROTECCIÓN ACUMULADA	
CRITERIO	NIVEL
Mínimo -	4
Mínimo +	8
Bajo -	12
Bajo +	16
Medio -	20
Medio +	24
Alto -	28
Alto +	32
Excelente -	36
Excelente +	40

Los equipos y sistemas de seguridad informática que se analizan para el cálculo del nivel de protección son:

1) Sistema de Prevención de Intrusos
2) Sistema de Seguridad Perimetral Firewall
3) Sistema de Filtrado de Correo Electrónico
4) Sistema de Filtrado Web
5) Sistema Antivirus empresarial

Los niveles de protección individual de los sistemas anteriores se calculan en los numerales 1), 2), 3), 4) y 5) de la sección B respectivamente y cuyos resultados se indican en la Tabla de resumen VIII, y que son utilizados para calcular el Nivel de Protección de la infraestructura en función de (5), (6) y la Tabla VII.

TABLA VIII
RESUMEN DE LOS NIVELES DE PROTECCIÓN ENTREGADOS POR LOS EQUIPOS Y SISTEMAS DE SEGURIDAD

EQUIPO	NIVEL DE PROTECCIÓN PROPORCIONADO		IMPORTANCIA EN LA RED DE DATOS		NIVEL DE PROTECCIÓN ACUMULADO
	100%	10%	Criterio	Valor	
FIREWALL CHECK POINT	58,11%	5,80	Crítico	4	23,2
IPS PROVENTIA G1200	43,30%	4,33	Alto	3	12,99
FILTRADO DE CORREO SYMANTEC BRIGHTMAIL	50,68%	5,07	Normal	2	10,136
FILTRADO WEB WEBSENSE	20,03%	2,00	Normal	2	4,006
ANTIVIRUS SYMANTEC	47,66%	4,76	Bajo	1	4,76
		TOTAL		**12**	**55,092**

TOTAL DE PROTECCIÓN ACUMULADA	55,09	
TOTAL DE IMPORTANCIA EN LA RED DE DATOS	12	
NIVEL DE PROTECCIÓN O SEGURIDAD ENTREGADA POR LOS EQUIPOS SOBRE 10	**4,59**	**MEDIO -**
NIVEL DE PROTECCIÓN O SEGURIDAD ENTREGADA POR LOS EQUIPOS 100 %	**45,91%**	**MEDIO -**

De acuerdo a los resultados de la Tabla VIII, el nivel de protección entregado por los equipos y sistemas de seguridad instalados en la red de datos es de (**4,59 / 10)** correspondiente al **45,91 %** de protección.

1) Nivel de protección entregado por el Sistema de Prevención de Intrusos

El nivel de protección entregado por el IPS se calcula analizando el tipo, la cantidad, el nivel de severidad de los ataques y eventos producidos en la red de datos y las acciones automáticas ejecutadas por el IPS sobre estos, en un período mínimo de 30 días, dependiendo de la capacidad de almacenamiento de su sistema de gestión.

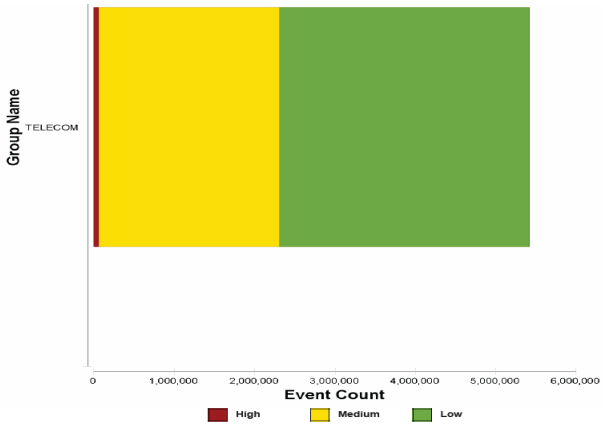

Fig. 17. Reporte mensual de intrusiones del IPS

Del reporte generado se obtuvieron las siguientes intrusiones que fueron controladas por el IPS, en un mes:

- 3.106.183 intrusiones de nivel bajo
- 2.249.568 intrusiones de nivel medio
- 67.518 intrusiones de nivel alto.

El nivel de seguridad entregado por el IPS se obtiene mediante (7) y (8):

$$\text{Nivel de Seguridad} = \frac{\sum_{i=1}^{10}\left(\text{Número de vulnerabilidades controladas(i)}\right)*\left(\text{Nivel de riesgo de la vulnerabilidad(i)}\right)}{\sum_{i=1}^{10}\text{Número de vulnerabilidades controladas(i)}} \quad (7)$$

$$\text{Nivel de Seguridad} = \frac{\text{Riesgo controlado acumulado total}}{\text{Cantidad total de vulnerabilidades controladas}} \quad (8)$$

TABLA IX
CÁLCULO DEL NIVEL DE PROTECCIÓN ENTREGADO POR EL IPS

EQUIPOS DE PROTECCIÓN	NÚMERO DE VULNERABILIDADES CONTROLADAS	NIVEL DE RIESGO DE LA VULNERABILIDAD		RIESGO CONTROLADO ACUMULADO	NIVEL DE PROTECCIÓN Total de Riesgo Controlado Acumulado / Total de Vulnerabilidades	
		Criterio	Valor		Criterio	Valor
IPS						
		. Mínimo -	1	0		
		. Mínimo +	2	0		
	3.106.183	. Bajo -	3	9318549		
		. Bajo +	4	0		
		. Medio -	5	0		
	2.249.568	. Medio +	6	13497408		
		. Alto -	7	0		
		. Alto +	8	0		
		. Crítico -	9	0		
	67.518	. Crítico +	10	675180		
	5.423.269			23.491.137,00	MEDIO -	4,33

De acuerdo a los resultados de la Tabla IX, el nivel de seguridad brindado por el IPS es del **(4,33 / 10)** que corresponde al **43,3 %**, cuyo valor es utilizado para calcular el nivel de protección proporcionado por los equipos de seguridad, en la Tabla VIII de resumen.

2) Nivel de protección entregado por el Sistema de Seguridad Perimetral Firewall

El nivel de protección o seguridad entregado por el Firewall Check Point, se calcula en función del número de paquetes permitidos, número de paquetes bloqueados o tumbados y el número de paquetes rechazados, en un período de 15 días, que depende de la capacidad de almacenamiento del sistema de gestión del Firewall, de acuerdo a (9) y (10), cuyos resultados se indican en la Tabla X:

$$\text{Nivel de Protección} = \frac{\left(\text{Total de paquetes tumbados}\right)+\left(\text{Total de paquetes rechazados}\right)}{\text{Total del paquetes procesados}} * 100\% \quad (9)$$

$$\text{Total de paquetes procesados} = \left(\text{Total de paquetes aceptados}\right) + \left(\text{Total de paquetes tumbados o bloqueados}\right) + \left(\text{Total de paquetes rechazados}\right) \quad (10)$$

TABLA X
CÁLCULO DEL NIVEL DE PROTECCIÓN ENTREGADO POR EL FIREWALL CHECK POINT

TIPO DE PAQUETES PROCESADOS EN 15 DIAS	CANTIDAD DE PAQUETES PROCESADOS
PAQUETES ACEPTADOS	271.320,00
PAQUETES RECHAZADOS	2.462,00
PAQUETES TUMBADOS	373.890,00
TOTAL DE PAQUETES PROCESADOS	**647.672,00**
NIVEL DE PROTECCIÓN DEL FIREWALL	**58,11%**

De acuerdo a los resultados de la Tabla X, el nivel de protección entregado por el firewall es del **58,11%** que corresponde a **(5,8 / 10)**, cuyo valor es utilizado para calcular el nivel de protección proporcionado por los equipos de seguridad, en la Tabla VIII de resumen.

3) Nivel de protección entregado por el Sistema de Filtrado de Correo Electrónico

El nivel de protección entregado por el Sistema de Filtrado de Correo Electrónico se mide en base al tipo, la cantidad y los niveles de severidad de los ataques a través de correo electrónico, utilizando su herramienta de gestión.

En este caso, el nivel de protección entregado por servidor de filtrado de correo electrónico Symantec BrightMail, se calcula en función de los mensajes permitidos y bloqueados obtenidos de los reportes del tráfico de correo entrante y saliente en un período de un mes, como se indica en la Fig. 18 y en la Tabla XI, para lo cual se utiliza (11), (12) y (13):

$$\text{Nivel de Seguridad} = \frac{\text{Total de mensajes bloqueados}}{\text{Total del mensajes procesados}} * 100\% \quad (11)$$

$$\text{Total de mensajes procesados} = \left(\text{Total de mensajes permitidos}\right) + \left(\text{Total de mensajes bloqueados}\right) \quad (12)$$

$$\text{Total de mensajes bloqueados} = \left(\text{mensajes de amenazas simples}\right) + \left(\text{mensajes de amenaza múltiples}\right) \quad (13)$$

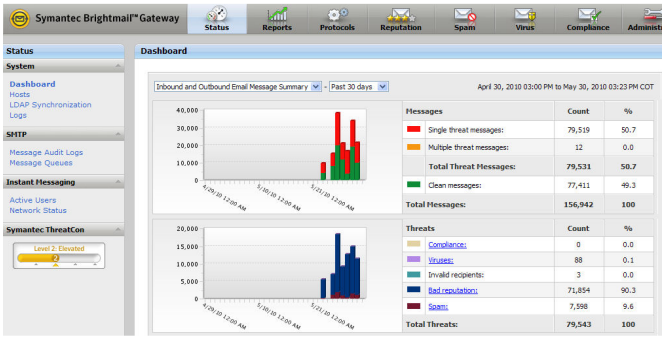

Fig. 18. Reporte mensual de filtrado de correo electrónico Symantec BrightMail

TABLA XI
CÁLCULO DEL NIVEL DE PROTECCIÓN DE SYMANTEC BRIGHTMAIL

TIPO DE MENSAJES	NÚMERO DE MENSAJES
MENSAJES DE AMENAZA BLOQUEADOS	
Mensajes de amenaza Individual	79.519,00
Mensajes de amenaza Múltiple	12,00
TOTAL DE MENSAJES BLOQUEADOS MENSUAL	**79.531,00**
MENSAJES PERMITIDOS	
Mensajes aceptados limpios	77.411,00
TOTAL DE CONEXIONES BLOQUEADAS MENSUAL	**77.411,00**
TOTAL DE MENSAJES CONTROLADOS MENSUAL	**156.942,00**
NIVEL DE PROTECCIÓN MENSUAL	**50,68%**

De acuerdo a los resultados de la Fig. 18 y a la Tabla XI, el nivel de protección entregado por el servidor de filtrado de correo electrónico Symantec BrightMail es del **50,68 %** correspondiente a **(5 / 10)**, cuyo valor es utilizado para calcular el nivel de protección proporcionado por los equipos de seguridad, en la Tabla VIII de resumen.

4) Nivel de protección entregado por el Sistema de Filtrado Web

El nivel de seguridad entregado por el Sistema de Filtrado Web se calcula en función del número de conexiones o hits hacia internet permitidas y bloqueadas, de acuerdo a (14) y (15):

$$\text{Nivel de bloqueo mensual} = \frac{\text{Total de conexiones bloqueadas mensual}}{\text{Total del conexiones mensual}} * 100\% \quad (14)$$

$$\text{Total de conexiones mensuales} = \left(\text{Total de conexiones permitidas mensuales}\right) + \left(\text{Total de conexiones bloqueadas mensuales}\right) \quad (15)$$

En este caso, el número de hits o conexiones mensuales hacia internet se obtienen de los reportes del Sistema de Filtrado Web Websense Enterprise, los cuales se describen en la Fig. 19 y en la Tabla XII.

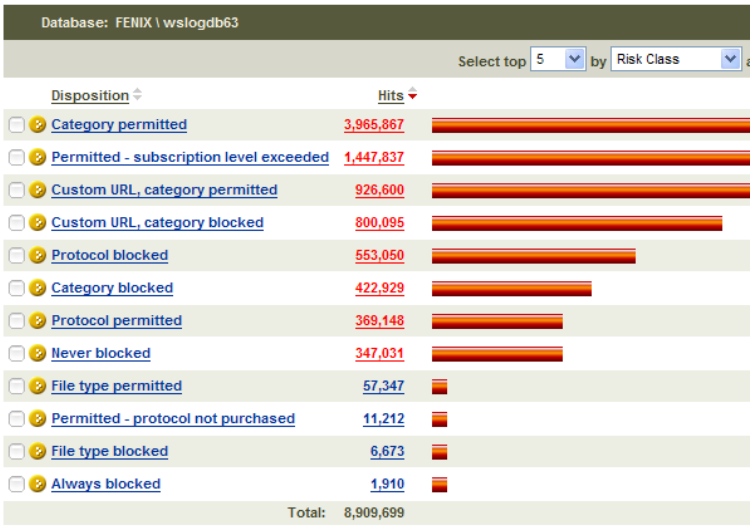

Fig. 19. Reporte de conexiones o hits mensuales hacia Internet

TABLA XII
CÁLCULO DEL NIVEL DE PROTECCIÓN ENTREGADO POR EL SISTEMA DE FILTRADO WEB-WEBSENSE

TIPO DE TRÁFICO CONTROLADO	NÚMERO DE HITS O INTENTOS DE CONEXIÓN MENSUAL
CONEXIONES PERMITIDAS MENSUAL	
Categorías permitidas	3.965.867,00
Permitido bajo suscripción	1.447.837,00
Categoría permitida, URLs personalizados	926.600,00
Protocolos permitidos	369.148,00
Nunca Bloqueado	347.031,00
Tipo de archivos permitidos	57.347,00
Protocolos permitidos no comprados	11.212,00
TOTAL DE CONEXIONES PERMITIDAS MENSUAL	**7.125.042,00**
CONEXIONES BLOQUEADAS MENSUAL	
Categorías blouqeadas	422.929,00
Categoría bloqueada, URLs personalizados	800.095,00
Protocolos bloqueados	553.050,00
Tipo de archivos bloqueados	6.673,00
Siempre bloqueados	1.910,00
TOTAL DE CONEXIONES BLOQUEADAS MENSUAL	**1.784.657,00**
TOTAL DE CONEXIONES CONTROLADAS MENSUAL	**8.909.699,00**
NIVEL DE BLOQUEO O PROTECCIÓN MENSUAL	**20,03%**

De acuerdo con los resultados de la Tabla XII, el nivel de bloqueo o de protección entregado por el Sistema de Filtrado Web-Websense es del **20 %** de seguridad, que corresponde a **(2 / 10)**, cuyo valor es utilizado para calcular el nivel de protección proporcionado por los equipos de seguridad, en la Tabla VIII de resumen.

5) Nivel de protección entregado por el Sistema Antivirus Empresarial

El nivel de protección entregado por el Sistema Antivirus Corporativo Symantec Endpoint Protection 11, se calcula en

función de las acciones de detección de infecciones ejecutadas en cada una de las estaciones de trabajo, en un período de un mes, como se indica en la Fig. 20 y en la Tabla XIII, para lo cual se utiliza (16) y (17):

$$\text{Nivel de protección} = \frac{\text{Infecciones detectadas controladas}}{\text{Total de Infecciones}} * 100\% \quad (16)$$

$$\text{Total de Infecciones} = (\text{Infecciones detectadas eliminadas}) + (\text{Infecciones detectadas no eliminadas}) \quad (17)$$

Symantec Endpoint Protection

Detection Action Summary

03 May 2010 00:00 AM to 03 June 2010 11:59 PM

Action	Viruses	Security Risks
Cleaned	142	0
Suspicious	0	0
Blocked	465	1
Quarantined	9623	3
Deleted	8442	75
Manually repaired / Repair in progress	343	19
Logged Commercial or Forced detections	0	0
Newly Infected	185	2
Still Infected	505	8

Fig. 20. Reporte mensual de amenazas

TABLA XIII
CÁLCULO DEL NIVEL DE PROTECCIÓN DEL SISTEMA ANTIVIRUS

TIPO DE INFECCIONES	NÚMERO INFECCIONES MENSUALES
INFECCIONES DETECTADAS ELIMINADAS MENSUAL	
Infecciones limpiadas	142
Infecciones sospechosas	0
Infecciones bloqueadas	465
Infecciones borradas o eliminadas	8442
Infecciones reparadas manualmente	343
TOTAL DE AMENAZAS CONTROLADAS MENSUAL	**9392**
INFECCIONES DETECTADAS NO ELIMINADAS MENSUAL	
Infecciones reincidentes	185
Infecciones enviadas a cuarentena	9623
Infecciones permanentes no reparadas	505
TOTAL DE AMENAZAS NO CONTROLADAS MENSUAL	**10313**
TOTAL DE AMENAZAS MENSUAL	**19705**
NIVEL DE PROTECCIÓN MENSUAL	**47,66%**

De acuerdo con los resultados de la Tabla XIII, el nivel de protección entregado por Symantec Endpoint Protection 11 es del **47,66 %** de seguridad, que corresponde a **(4,7 / 10)**, cuyo valor es utilizado para calcular el nivel de protección proporcionado por los equipos de seguridad, en la Tabla VIII de resumen.

C. Nivel de Riesgo Real de la Seguridad Informática

El nivel de riesgo real de la seguridad informática de la red de datos se calcula en función del nivel de riesgo por vulnerabilidades detectadas, el nivel de protección entregado por los equipos y sistemas de seguridad y el riesgo residual, mediante (18) "propuesta" y la Tabla XIV.

$$\text{Nivel de riesgo real de la seguridad informática} = \left(\text{Nivel de riesgo por las vulnerabilidades detectadas}\right) - \left[\text{Nivel de protección entregado por los equipos y sistemas de seguridad}\right] * \left[\text{Nivel de riesgo por las vulnerabilidades detectadas}\right] + \left(\text{Riesgo residual}\right) \quad (18)$$

Riesgo residual, es aquel que no se ha considerado y que no ha sido controlado por los equipos de seguridad, el cual se asume como de 5 %.

TABLA XIV
RIESGO REAL DE LA SEGURIDAD INFORMÁTICA

TIPO DE NIVELES	VALOR
NIVEL DE PROTECCIÓN 100 %	45,91%
NIVEL DE RIESGO POR VULNERABILIDADES DETECTADAS	66,89%
RIESGO RESIDUAL	5%
NIVEL DE RIESGO REAL DE LA SEGURIDAD INFORMÁTICA	**41%**

De acuerdo a los resultados obtenidos en la Tabla XIV, el Nivel de Riesgo Real de la Seguridad Informática en la infraestructura corresponde al **41 %** de vulnerabilidad.

III. NIVEL DE RIESGO REAL DE LA INFRAESTRUCTURA TECNOLÓGICA

El Nivel de Riesgo Real de la infraestructura tecnológica, se obtiene de los resultados obtenidos en los análisis de los riesgos de la infraestructura actual, los niveles de disponibilidad y los niveles de vulnerabilidad actual, para lo cual se realiza una comparación con los siguientes niveles de referencia:

- Nivel de referencia crítico, para un caso no deseado.
- Nivel de referencia óptimo, para un caso ideal, que en este caso se asume un riesgo del 10 %

Considerando el caso de los equipos de comunicaciones de red LAN el resumen de resultados son los indicados en la Tabla XV y en la Fig. 21.

TABLA XV
RESUMEN COMPARATIVO DE LOS NIVELES DE RIESGO POR VULNERABILIDAD DE LA RED ACTUAL

	NIVEL DE RIESGO DE LA SEGURIDAD INFORMÁTICA
NIVEL DE REFERENCIA CRÍTICO	100,00%
NIVEL REAL	41,00%
NIVEL DE REFERENCIA ÓPTIMO	10,00%

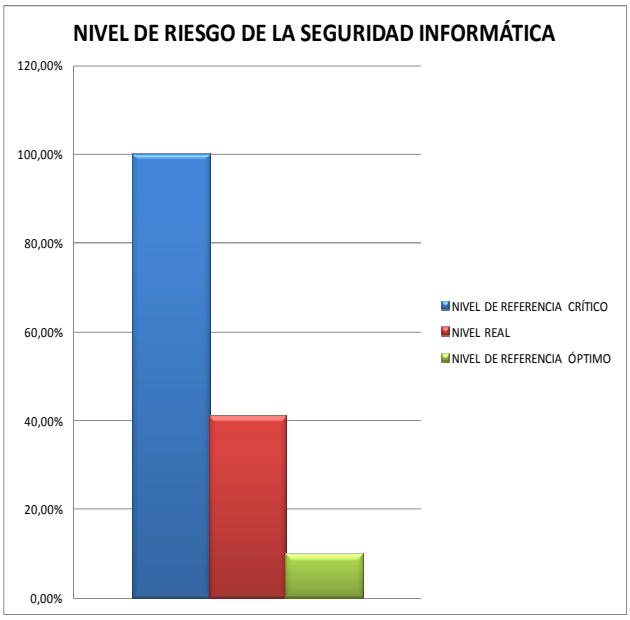

Fig. 21. Resumen comparativo de los niveles de riesgo por, vulnerabilidad de la red.

IV. CONCLUSIONES

De los resultados anteriores se determina en forma matemática que se debe realizar mejoras sustanciales en las seguridades informáticas en la red de datos, a través de la implementación de esquemas de seguridad avanzados que permitan:

- Controlar el acceso de los usuarios y dispositivos a la red de datos, controlándolos directamente en el puerto del Switch en los cuales se conectan.
- Controlar el tipo de tráfico que utilizan los usuarios y dispositivos, mediante el análisis de protocolos y aplicaciones en las capas 2, 3, 4 y 7, directamente en el puerto donde se conecta el usuario.
- Crear ambientes de remediación y cuarentena para aislar a los usuarios y dispositivos que no cumplan con las políticas de seguridad establecidas en la institución.
- Crear ambientes de usuarios y dispositivos invitados.
- Crear ambientes de actualización de parches para los servidores.
- Crear zonas de protección para los servidores.

V. REFERENCIAS

Tesis:

[1] Chinchero, A., "*Análisis y diseño de una red segura convergente de alto rendimiento para la oficina matriz Quito de la Superintendencia de Bancos y Seguros,"* Proyecto de grado para la obtención del título de Maestría en Redes de Información y Conectividad, ESPE. 2010.

Libros:

[2] Ministerio de Administraciones Públicas. Magerit V2. *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Guía de Técnicas*. Madrid: 2006, páginas 5-21.

[3] Ministerio de Administraciones Públicas. Magerit V2. *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Método*. Madrid: 2006, páginas 2-30

[4] C. Alberts, *Managing Information Security Risks*. Boston: Addison Wesley, 2002.

[5] E. Cole, *Network Security Bible. Second Edition. Information System Security Principles*. Indianápolis: Wiley Publishing, 2009, capítulo 4, páginas 35-71.

[6] K Schmidt, *High availability and disaster recovery*. Frankfurt: Springer, 2006, página 24

Artículos:

[7] E. Leyton, *Fundamentos de análisis de riesgos*. 2009 [Fecha de consulta: Noviembre 2009]. Disponible en: http://www.eduardoleyton.com//apuntes/01_Fundamentos_Riesgo.pdf

[8] Evaluación de riesgos. Niveles de riesgo. 2009[Fecha de consulta: Diciembre 2009]. Disponible en: http://www.segu-info.com.ar/politicas/nivelesriesgo.htm

VI. BIOGRAFIA

Angel Chinchero Villacís, egresó en el año 1991 y recibió el título de Ingeniería en Electrónica y Telecomunicaciones en la Escuela Politécnica Nacional del Ecuador, en el año 1997.

Actualmente es aspirante al título de Máster en Redes de Información y Conectividad en la Escuela Politécnica del Ejército.

Las áreas de interés están en el diseño, implementación y administración de las redes seguras empresariales.

Actualmente se desempeña como administrador de la red y las seguridades perimetrales de la Superintendencia de Bancos y Seguros del Ecuador.
achinchero@superban.gov.ec; achinchero@sbs.gob.ec
angelchinchero_2007@hotmail.com

Verónica Orellana Navarrete, recibió el título de Ingeniería en Electrónica y Telecomunicaciones en la Escuela Politécnica Nacional del Ecuador, en el año 2002.

Obtuvo su título de Magister en E-Bussiness y Gestión de TICs, en el Politécnico de Turín, en el año 2006.

Colaboró en el proyecto de grado del Ing. Angel Chinchero como directora de tesis.

Actualmente se desempeña como profesor principal en la Universidad de las Américas.
anavo@yahoo.com