UNIVERSIDAD PERUANA DE LAS AMÉRICAS

ESCUELA PROFESIONAL DE INGENIERÍA DCOMPUTACIÓN Y SISTEMAS

Implementación de un Firewall TMG Forefront para la Seguridad Perimetral de la Red de Datos de la Clínica Aliada

PARA OBTAR EL TITULO DE INGENIERO EN COMPUTACIÓN Y SISTEMAS

AUTORES:

Bach. CASTILLO PALOMINO, RENZO GIANCARLO

Bach. DOMINGUEZ CHAVEZ, MIGUEL ANGEL

Bach. SULCA GALARZA, CARLOS IVÁN

ASESOR:

Mg. Jose Ogosi Auqui

LINEA DE INVESTIGACIÓN: SISTEMAS DE GESTIÓN DE INFORMACIÓN Y CONOCIMIENTOS

LIMA, PERÚ

FEBRERO, 2017

DEDICATORIA:

Este presente trabajo agradecemos a nuestros padres y familiares porque nos brindaron su apoyo tanto moral y económicamente para seguir estudiando y lograr el objetivo trazado para un futuro mejor y ser el orgullo para ellos y de toda la familia.

A la **Universidad Peruana de las Américas**, alma mater de la tecnología porque nos está formando para un futuro como Ingenieros de Computación y Sistemas.

De igual manera a mis queridos formadores en especial al docente de **Redes IV** de nuestra carrera puesto que ellos nos guiaron para hacer el presente trabajo.

AGRADECIMIENTOS:

Agradecemos a Dios ser maravilloso que nos dio fuerza y fe para creer lo que nos parecía imposible terminar. A nuestras familias por ayudarnos en cada momento de nuestras vidas.

RESUMEN

La seguridad informática no solo depende de recursos tecnológicos, también depende de procesos y recursos humanos capacitados y especializados. Pues siempre hay cambios, ya que día a día se descubren nuevas amenazas, nuevos tipos de ataques a los sistemas institucionales, convirtiendo la seguridad en una tarea sumamente compleja y demandante.

La presente investigación trata sobre el desarrollo de la seguridad perimetral en la intranet de la Clínica ALIADA, viendo las amenazas de seguridad desde perspectivas distintas, de esta manera se conocerá los riesgos que puedan afectar a la clínica.

A continuación, se diseña una implementación de seguridad perimetral utilizando el firewall TMG FOREFRONT, en las que se indican los procedimientos de actuación frente a determinadas incidencias de seguridad, como pueden ser fallos en elementos de red, detección de vulnerabilidades, detección de ataques, cambios en políticas de seguridad, etc.

Finalmente se detallarán las conclusiones que se obtienen de la realización del presente proyecto.

Palabras Clave: SEGURIDAD PERIMETRAL, FIREWALL, VULNERABILIDADES, ATAQUES, VIRUS

ABSTRACT

Computer security not only depends on technological resources, it also depends on trained and specialized human resources and processes. Well, there are always changes, since every day new threats are discovered, new types of attacks on institutional systems, making security an extremely complex and demanding task.

The present investigation deals with the development of perimeter security in the intranet of the ALIADA Clinic, seeing the security threats from different perspectives, in this way we will know the risks that may affect the clinic.

Next, a perimeter security implementation is designed using the TMG FOREFRONT firewall, which indicates the procedures for action against certain security incidents, such as failures in network elements, vulnerability detection, attack detection, changes in security policies, etc.

Finally, the conclusions obtained from the realization of the present project will be detailed.

Keywords: PERIMETER SECURITY, FIREWALL, VULNERABILITIES, ATTACKS, VIRUSES

DESARROLLO DE TESIS

Tabla de Contenidos

INDICE DE TABLAS

INDICE DE FIGURAS

INTRODUCCIÓN

Todas las áreas cumplen un rol muy importante en la empresa realizando sus diversos procesos que ayudan a la empresa a seguir creciendo. Actualmente los responsables de las respectivas áreas de la Clínica Aliada han detectado problemas que son reportados a diario por su personal a cargo, los cuales se evidencia al realizar sus laborares en el día a día, como lentitud en el uso del correo electrónico, pagos online sin finalizar, lentitud en la atención a los clientes, no existe seguridad alguna en la navegación por internet, no existe un control de acceso web.

A falta de una medida de seguridad perimetral, esta puede impactar de manera negativa las prestaciones que brinda la Clínica, ocasionando pérdidas muy grandes como también una mala imagen con los clientes en temas de calidad de servicio. El objetivo de una solución perimetral es limitar e inspeccionar qué datos entran a la empresa o salen de ella. El atributo primordial de este prototipo de seguridad es que concede al administrador pensar en los puntos de entrada, sin omitir la securización de todos los servidores internos de nuestra red, para custodiarlos ante una futura intromisión de hackers.

Podemos incurrir en la equivocación y creer que se puede acceder a un sistema de seguridad total, desatendiendo el sostenimiento y dejar de lado una política de seguridad instaurada. En esta política, uno de los temas más relevantes es adquirir todos los equipos actualizados, desarrollar una preparación de debilidades o una precisa planificación de backup.

El siguiente proyecto propone un esquema de seguridad perimetral específico, aunque no se avala la totalidad de la custodia, pero sí certifica un significativo nivel de seguridad en la organización. Dentro de un esquema en el que se establece, una positiva dirección de los componentes y posibles contratiempos, y una buena política de seguridad, la organización no tendrá vulnerabilidades en casos de amenazas del exterior.

“IMPLEMENTACIÓN DE UN FIREWALL TMG FOREFRONT PARA LA SEGURIDAD PERIMETRAL DE LA RED DE DATOS DE LA CLÍNICA ALIADA”

Capítulo I:
ANÁLISIS EMPRESARIAL

1.1. Acerca de la empresa

ALIADA es un centro médico especializado en Oncología Integral que maneja los más altos patrones internacionales en sus planes de previsión, evaluación y tratamiento del cáncer. La orientación y la singularidad que nos distinguen y resaltan se podrían resumir en tres puntos primordiales:

Una visión plena del paciente. Prestigiosos expertos en todas las especialidades relacionadas al cáncer laboran en una orientación multidisciplinario para sostener un preciso análisis y el tratamiento más conveniente para cada paciente. Esta personalización podemos verla igualmente plasmada en la aptitud de nuestra esmero por el paciente y sus familiares.

Tratamientos y tecnología de avanzada. Nuestros profesionales dedican prácticas médicas superiores valiéndose de los más modernos desarrollos en ciencia y tecnología. Manejamos modelos idénticos a los principales centros oncológicos del mundo, tanto en los cuadros de tratamiento como en el infraestructura tecnológica.

Acreditaciones y afiliaciones internacionales. Tenemos un acuerdo de asistencia y asesoría integral con Johns Hopkins Medicine International, hospital que ha sido reconocido durante 21 años consecutivos como el mejor de Estados Unidos. Igualmente, nuestra infraestructura y buenas prácticas han sido certificadas por la AAAHC (Accreditation Association of Ambulatory Health Care, USA)

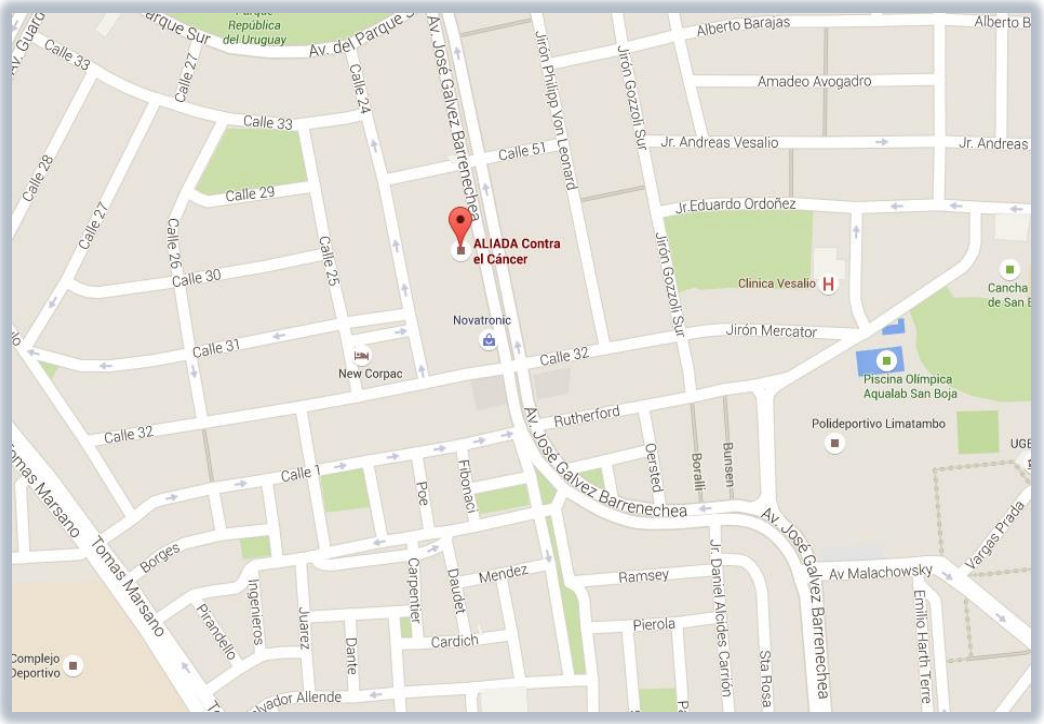


Figura 1: Ubicación de la Empresa
Elaborado: Por autores

Misión

Brindamos a las familias la tranquilidad de contar con el mejor aliado posible en su lucha contra el cáncer a través de un equipo humano experto en programas de prevención, detección y tratamiento.

Visión

Ser la red de tratamiento integral contra el cáncer referente en Latinoamérica, brindando acceso a los más altos estándares de calidad y seguridad médica.

1.2 Organigrama de la Empresa

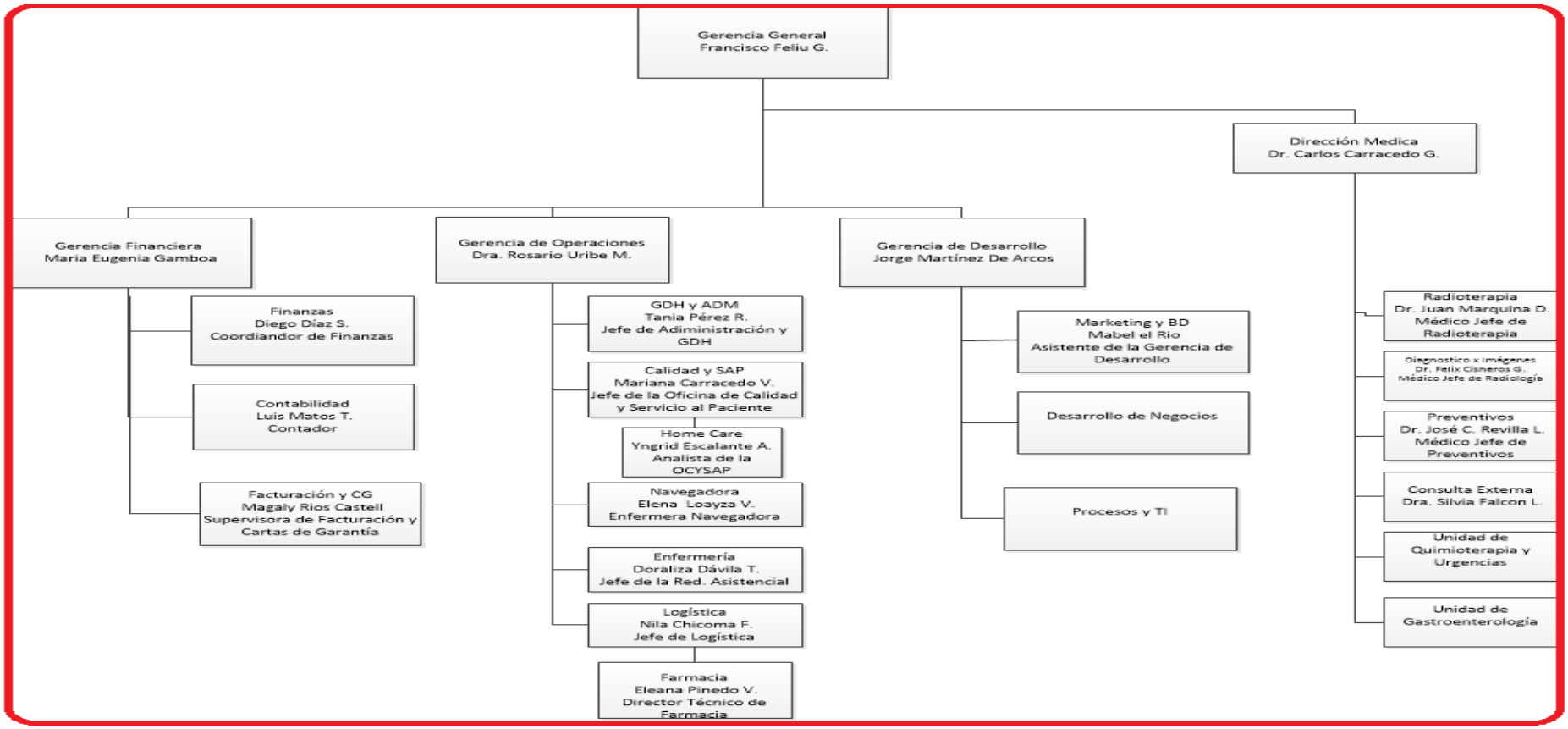


Figura 2: Organigrama
Elaborado: Por autores

1.3. Análisis Foda

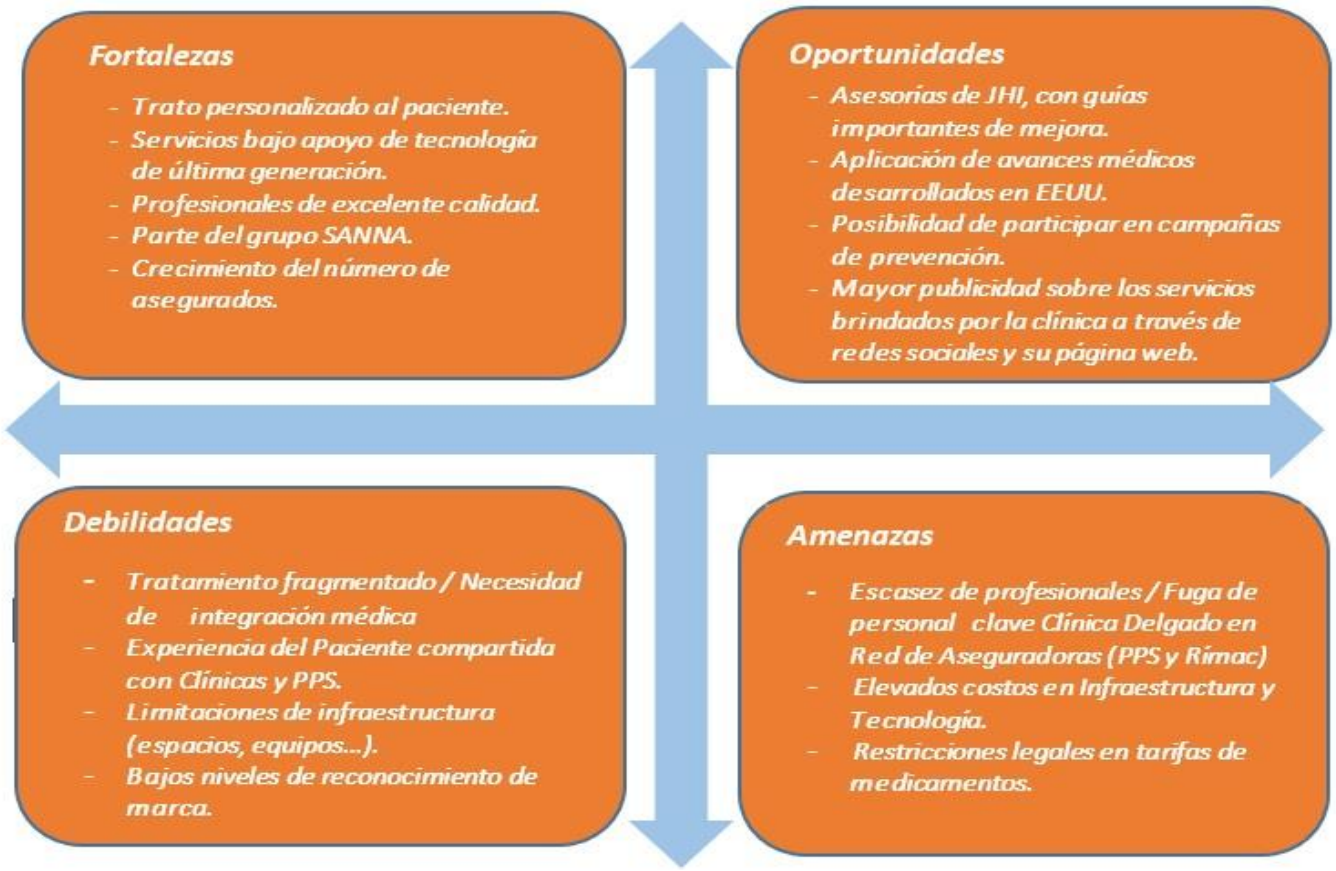


Figura3: Análisis Foda
Elaborado: Por autores

1.3.1. Matriz Foda

FACTORES INTERNOS / FACTORES EXTERNOS	FORTALEZAS(F)	DEBILIDADES(D)
	✓ Servicios bajo apoyo de tecnología de última generación. ✓ Profesionales de excelente calidad. ✓ Parte del grupo SANNA. ✓ Crecimiento del número de asegurados. ✓ Trato personalizado al paciente.	✓ Tratamiento fragmentado / Necesidad de integración médica ✓ Falta de especialidades para atencion a pacientes con enfermedades extrañas. ✓ Bajos niveles de reconocimiento de marca. ✓ Limitaciones de infraestructura.
OPORTUNIDADES(O) ✓ Aplicación de avances médicos desarrollados en EEUU. ✓ Posibilidad de participar en campañas de prevención. ✓ Mayor publicidad sobre los servicios brindados por la clínica a través de redes sociales y su página web. ✓ Asesorías de JHI, con guías importantes de mejora.	**ESTRATEGIAS (FO)** ➢ Brindando servicios con tecnologia de ultima generacion, que sasisface a nuestros pacientes, nos motiva a adquirir aplicaciones medicos desarrollados en EEUU. ➢ Con profesionales de excelente calidad,nos da la confianza de participar en campañas de prevencion. ➢ Al ser parte del grupo SANNA, nuestra publicidad garantiza una confianza en nuestros pacientes.	**ESTRATEGIAS(DO)** ➢ Con la adquicision de nuevas aplicaciones nos ayudara resolver los tratamientos fragmentados y mejorara la integracion medica. ➢ La posibilidad de participar en campañas, nos permite tomar experiencia en pacientes con extrañas enfermedades. ➢ Mediante la publicidad sobre nuestros servicios medicos, seremos mas reconocimos y solicitados por los pacientes.
AMENAZAS(A) ✓ Demora en el creciemiento de la clinica en el mercado. ✓ Escasez de profesionales / Fuga de personal clave Clínica Delgado en Red de Aseguradoras (PPS y Rímac) ✓ Elevados costos en Infraestructura y Tecnología. ✓ Restricciones legales en tarifas de medicamentos.	**ESTRATEGIAS(FA)** ➢ Contando con tecnologia de ultima generacion nos ayudara a crecer rapidamente y ser mas competitivo en el mercado. ➢ Al ser parte de grupo SANNA,nuestros profesionales estaran orgullosos de pertenecer aun solido grupo corporativo por medio de la clinica Aliada. ➢ Gracias al crecimiento de asegurados, nos permitira mayores ingresos economicos y solventar gastos en infraestructura y tecnologicas.	**ESTRATEGIAS(DA)** 

Tabla 1: Matriz Foda
Elaborado: Por los autores

1.4. Cadena de Valor

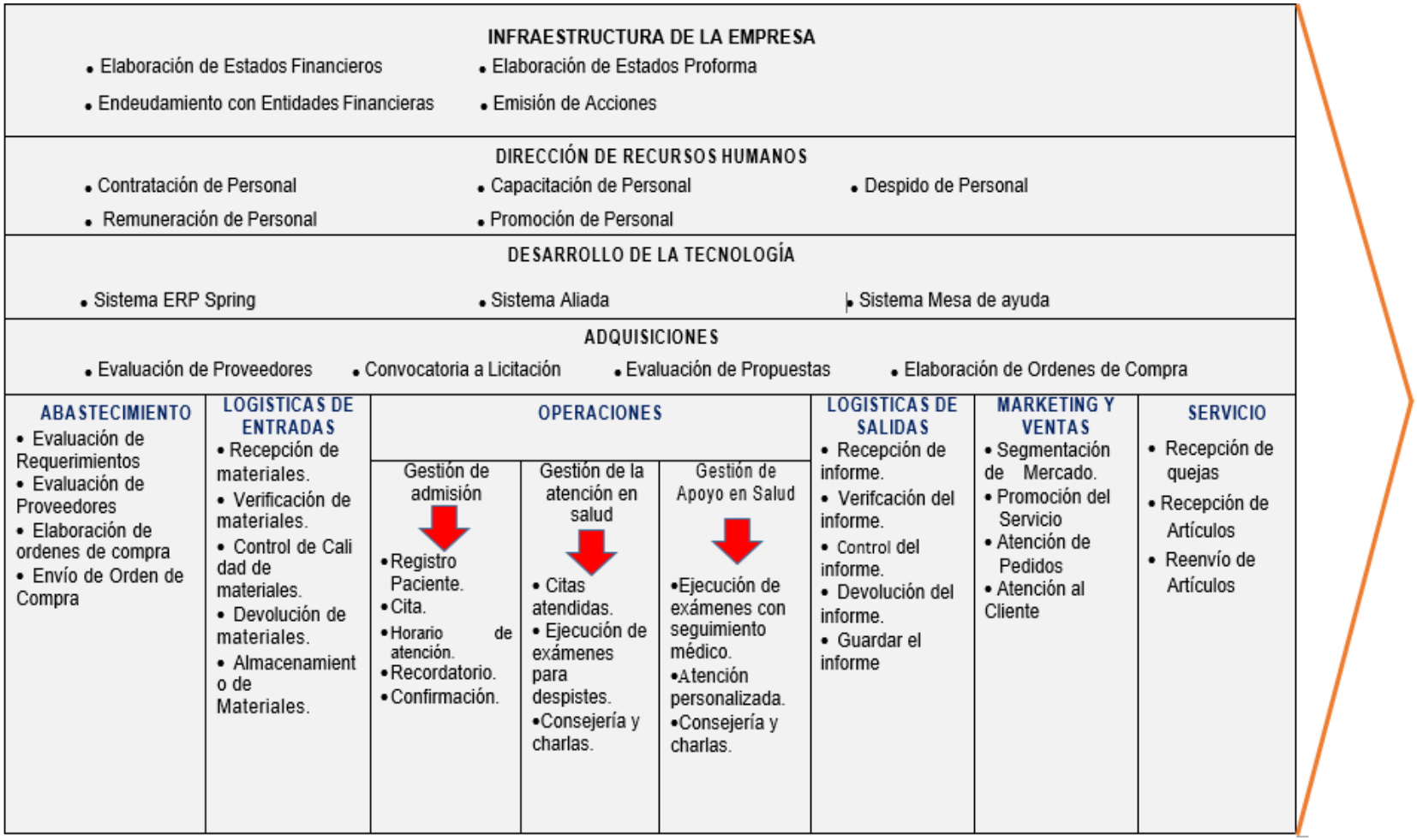


Figura 4: Cadena de Valor
Elaborado: Por autores

1.5. Análisis Canvas

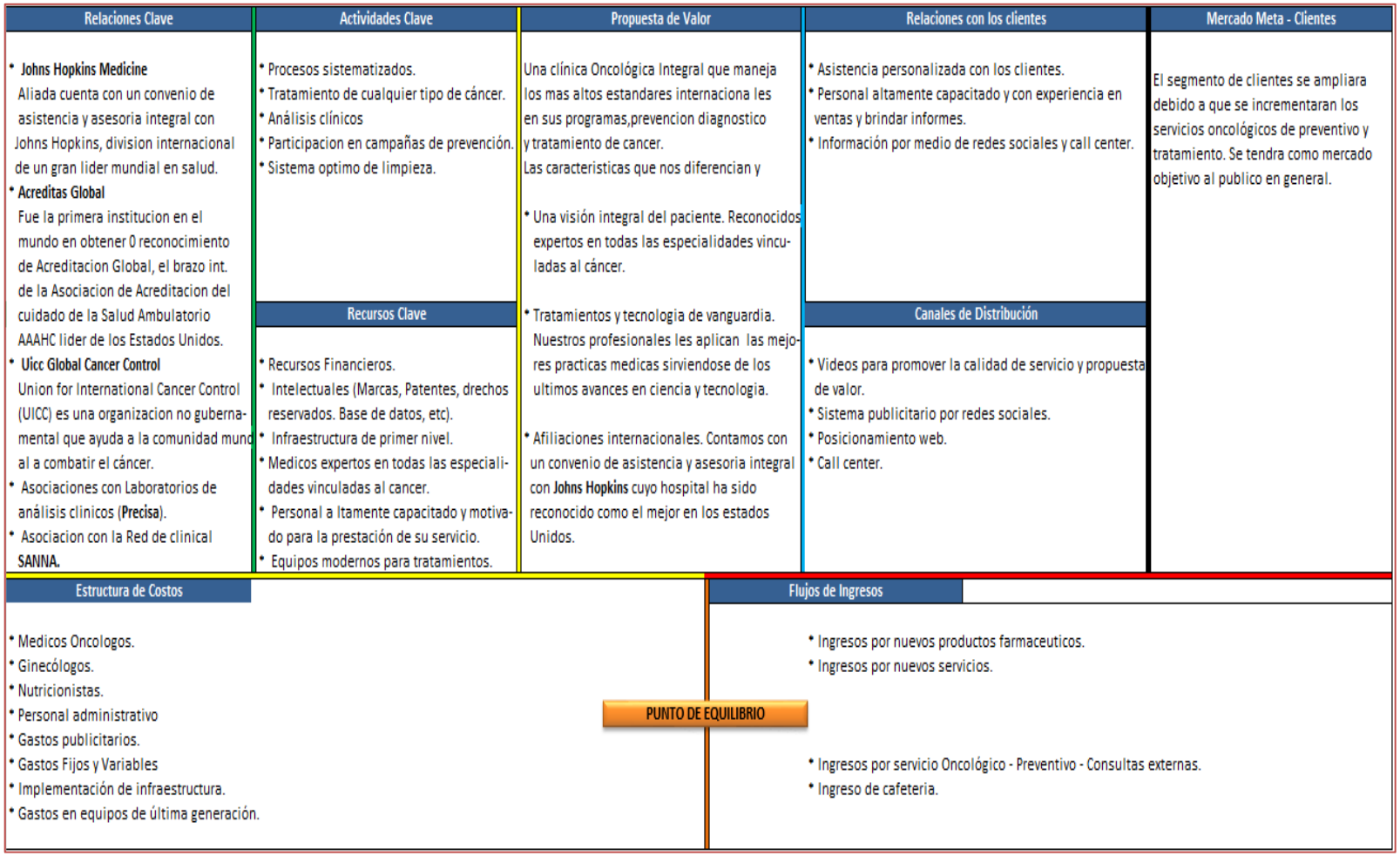


Figura 5: Análisis Canvas
Elaborado: Por autores

1.6 Mapa de Procesos

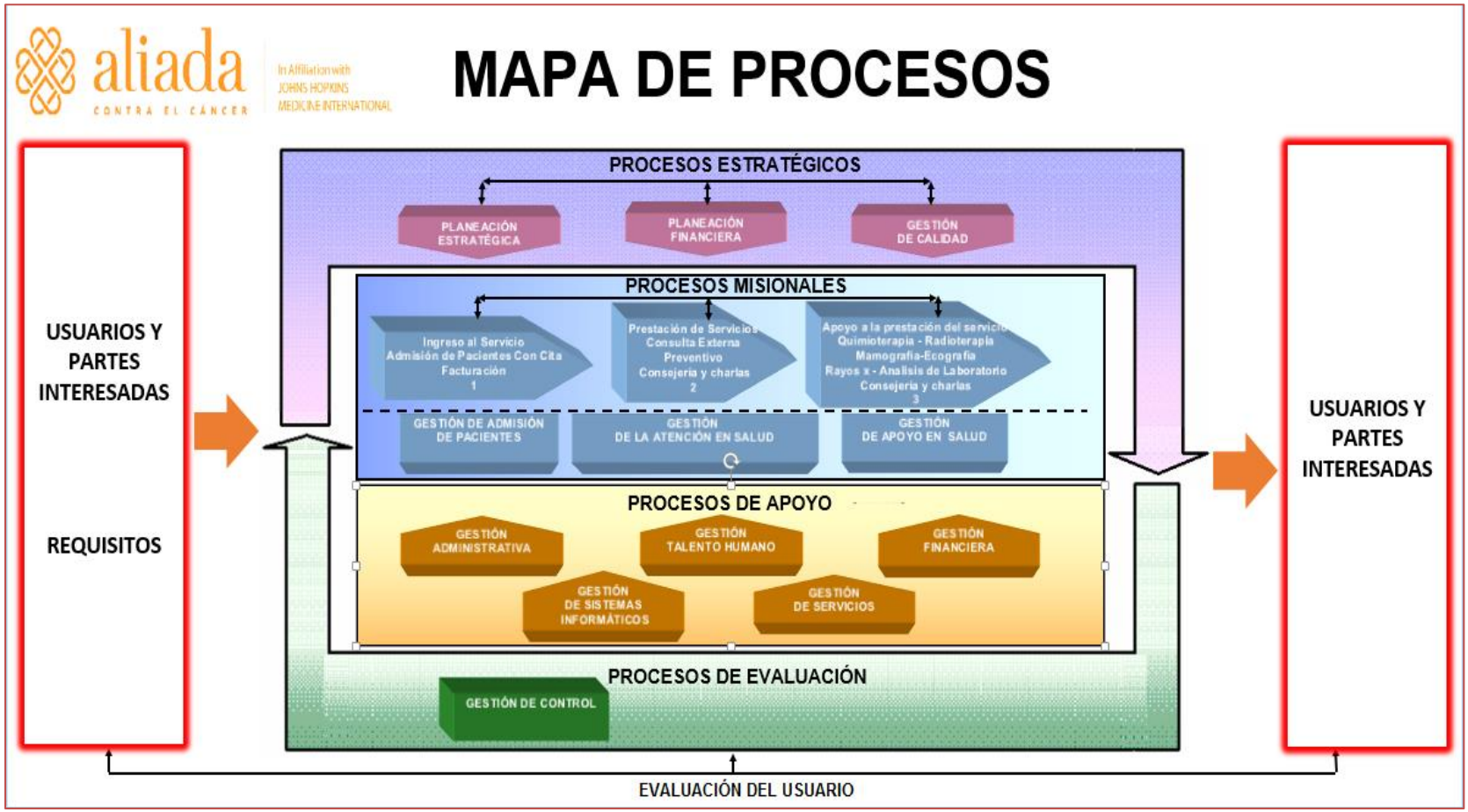


Figura 6: Mapa de Procesos
Elaborado: Por los autores

1.7 Diagrama de Subprocesos y Diagrama Workflow BPM detallado

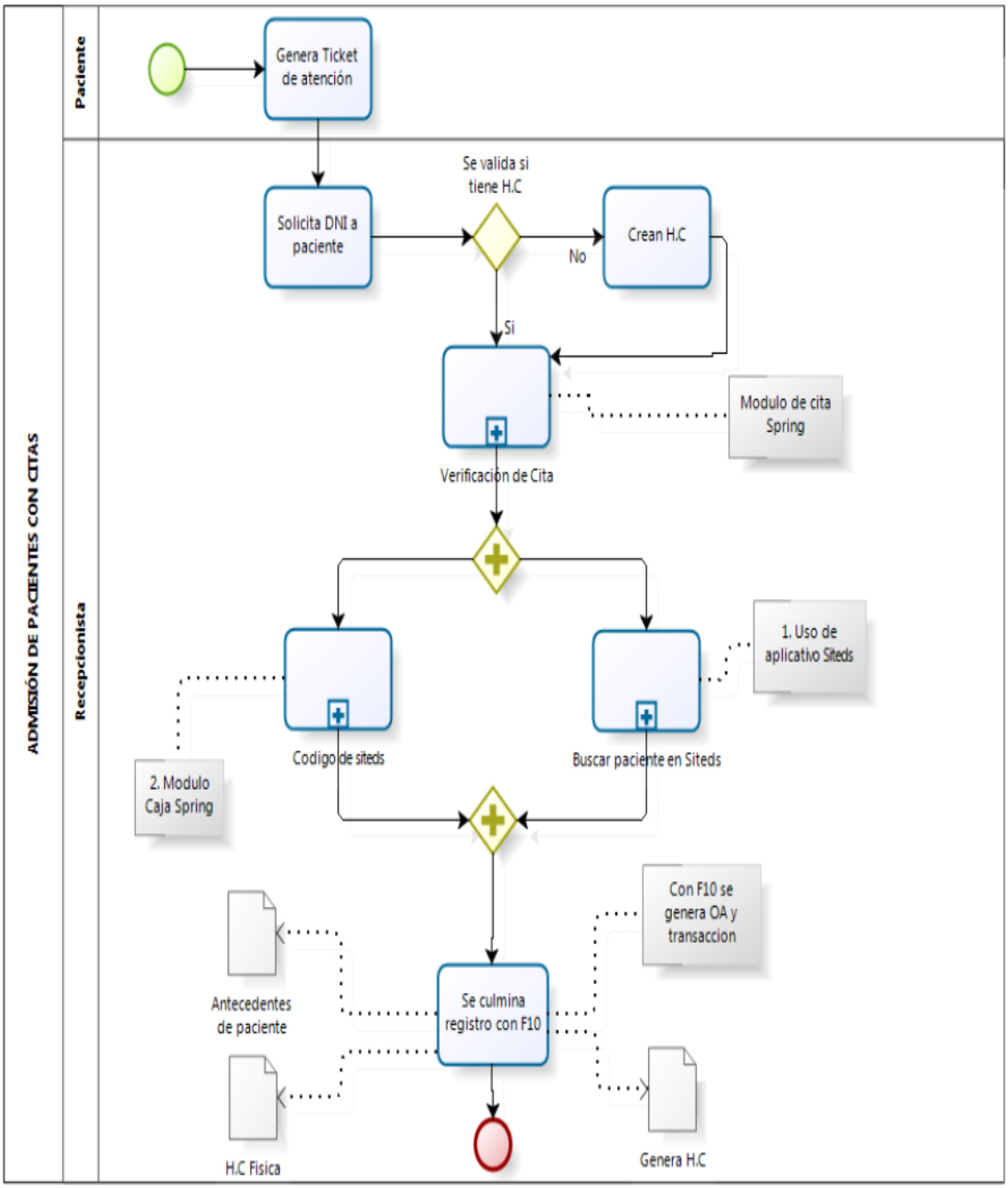


Figura 7: Mapa de Procesos – Gestión de Admisión de Pacientes
Elaborado: Por los autores

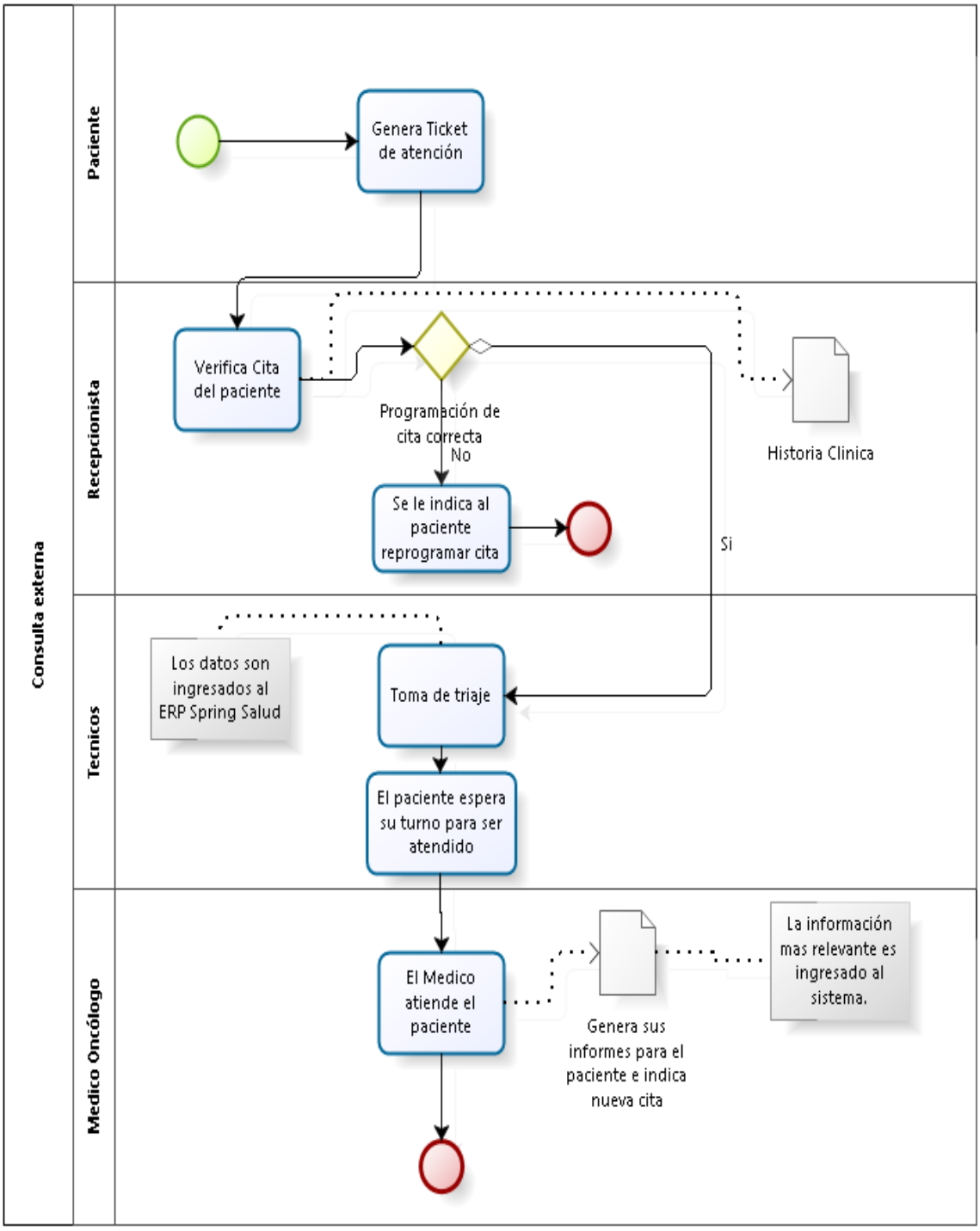


Figura 8: Mapa de Procesos – Gestión de la Atención en Salud
Elaborado: Por los autores

1.8 Definición del problema

Actualmente con el desarrollo impulsivo de la tecnología a nivel global han surgido diversas soluciones que permiten a las personas comunicarse y desarrollarse en muchos ámbitos en cada una de las etapas de su vida, día a día estas nuevas tecnologías se actualizan y poco a poco desplazan y se imponen sobre las viejas, este cambio a su vez da lugar a circunstancias que llevan al mal uso de las tecnologías convergentes comprometiendo a la integridad de la información en el medio personal y corporativo.

ALIADA es un centro médico especializado en Oncología Integral constituido hace más de 21 que maneja los más altos patrones internacionales en sus planes de previsión, evaluación y tratamiento del cáncer. La problemática nace del uso que se le da a la tecnología, siendo más específico a los computadores, software e internet. Los usuarios, en este caso los empleados de la clínica Aliada, actualmente tienen la libertad de aprovechar una serie de comodidades tecnológicas en favor a las funciones que realizan como gestionar su trabajo en la red interna como también como también de la red pública de internet. Esto puede suponer un problema muy relevante si no se cumplen ciertas medidas de seguridad para evitar las violaciones de datos que se puedan irrumpir en la red.

Actualmente la clínica Aliada no cuenta con una solución que permita proteger, gestionar y centralizar la seguridad perimetral y los accesos a nivel LAN y WAN por lo que pone en alto riesgo la privacidad de la información y los datos que puedan manejarse, así pues este proyecto se enfoca concretamente a brindar una solución a las necesidades expuestas bajo un escenario empresarial.

En las condiciones y el contexto planteado es obvia la importancia de encontrar una solución al problema de la seguridad, así pues con el estudio de diferentes Firewalls pretendemos implementar una solución que llegue a acomodarse a los

requerimientos expuestos y nos brinde a su vez numerosas ventajas y propiedades de integración con las tecnologías que actualmente maneja todo el departamento de Sistemas de la clínica Aliada.

La solución que se brindará atacará las diversas necesidades de protección de la información en de la red perimetral como también tener una medida de control de autenticación de accesos que se pueda tener desde la red externa hacia la red interna, también tener un control sobre la navegación e ingreso a ciertos websites que apeligren la productividad del personal o la estabilidad de la red interna evitándose alguna manifestación de ataque desde la red externa por medio de hacker o un virus, spyware, malware etc. Otro problema a tratarse será la confidencialidad de la información puesto que actualmente el personal puede acceder libremente a sus correos personales creados en dominios públicos como Hotmail, Gmail, Yahoo, etc. Abriéndose una gran oportunidad para el tráfico ilícito de información interna. Para culminar se manifiesta en este documento la necesidad obligatoria de contar con la implementación y trabajo en la red de un dispositivo de seguridad que permita al área de sistemas mantener la seguridad y el control total sobre toda la infraestructura del parque tecnológico de la clínica Aliada.

1.9. Diagrama de Causa y Efecto

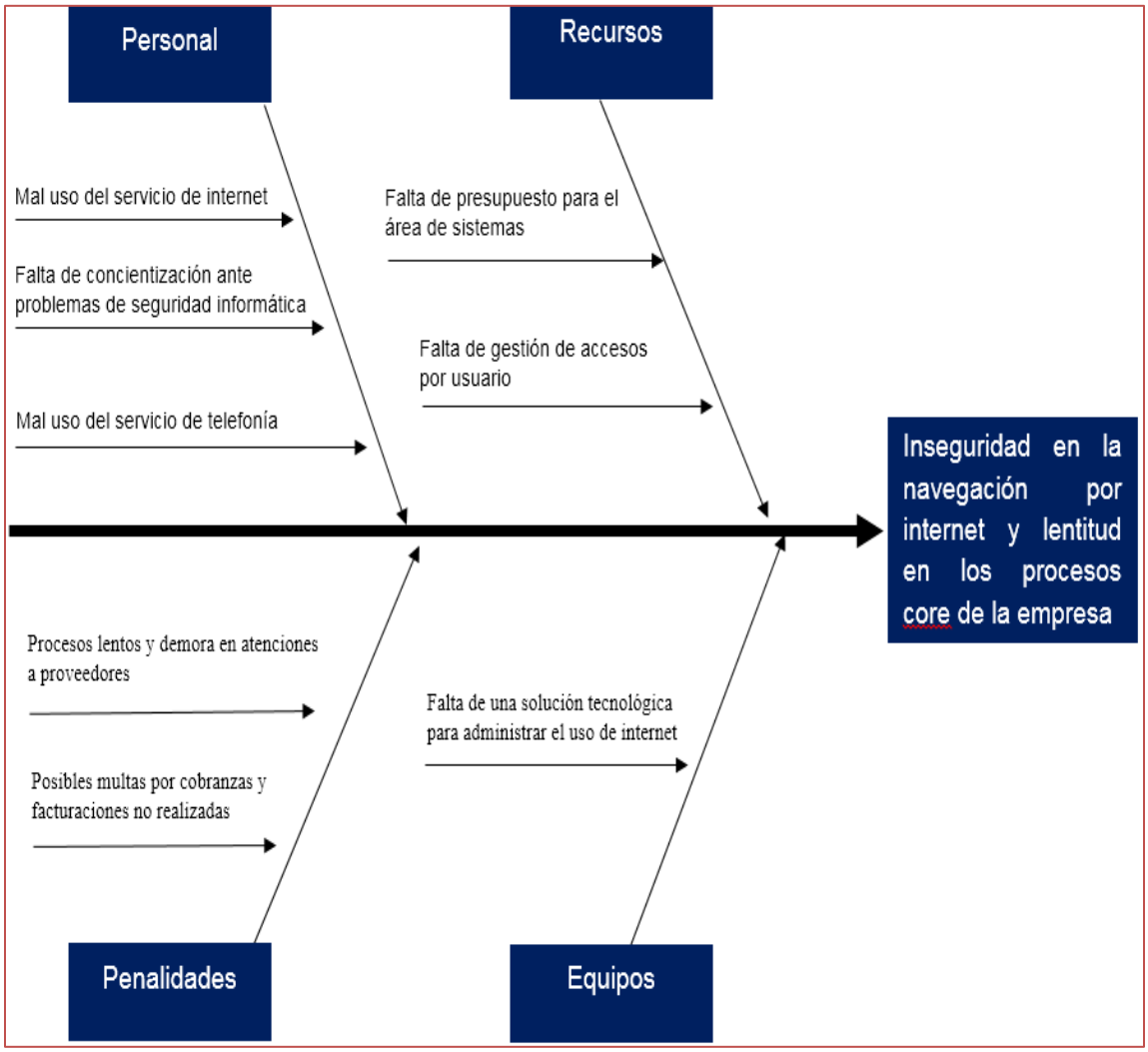


Figura 9: Mapa de Procesos – Gestión de la Atención en Salud
Elaborado: Por los autores

1.10. Alternativas de Solución

Se analizaron diferentes Firewalls que cubran las necesidades de seguridad anteriormente expuestas, en este proceso hemos encontrado muchas soluciones que nos brindan diversos beneficios de seguridad en diferentes entornos, se han evaluado soluciones basadas en plataformas de SO como:

- FreeBSD
- LINUX
- Windows

Así también en soluciones basadas en Hardware como:

- Cisco
- Juniper
- Barracuda
- Fortigate
- Mikrotik RouterBoard
- Check Point Appliance
- Sonic Wall
- Lanner Launches
- Blue Coat
- AnexGATE

La solución que se implementara es basada en TMG Forefront 2010 por trabajar en sincronización con el servidor de directorio activo de la Clínica Aliada beneficiándonos en:

- Administración centralizada
- Aplicación de políticas de negocio por usuario
- Sistema de Inspección de red
- Sistema de antivirus
- Administración de conexiones vpn
- Ahorro de Costos

1.11. Evaluación Financiera

EVALUACIÓN FINANCIERA DEL PROYECTO	CÓDIGO	
APROBADO POR: GERENTE GENERAL	FECHA DE INICIO DE VIGENCIA	
IMPLEMENTACION DE FIREWALL TMG FOREFRONT	21/11/2016	

RECURSOS HUMANOS

Cargo		Cantidad	Tiempo (Meses)	Dedicacion	Total Mensual Costo (SOLES)	Proyecto Implementacion Firewall	Total
	Jefe de Proyectos	1	1	100%	3500	3500	3500
	Analista de Diseño	1	1	100%	2500	2500	2500
	Analista Implementador	1	1	100%	2500	2500	2500
					Total		8500

RECURSOS HARDWARE Y SOFTWARE

Recursos		Cantidad	Costo Unit. S/	Subtotal
Firewall TMG ForeFront				
	Servidor HP Proliant	1	6246	6246
	Licencia Firewall Forefront	1	2276	2276
	Windows Server 2008 R2 Estándar	1	300	300
			Total (S/)	8822

Recursos y Salarios		Mes 1	Mes 2	Mes 3
	Recursos HW y SW	8822	0	0
	Jefe de Proyectos	3500	3500	3500
	Analista de Diseño	2500	2500	2500
	Analista Implementador	2500	2500	2500
Flujo de Pago (S/)		17322	8500	8500

Total Salario x 3 meses	8500 x 3 meses	25500
Primer Mes Recursos HW y SW + Salario 1 mes	8822 + 8500	17322

Total Inversión	
Recursos y Salarios	34322.00

EVALUACIÓN FINANCIERA DEL PROYECTO	CÓDIGO	
APROBADO POR: GERENTE GENERAL	FECHA DE INICIO DE VIGENCIA	
IMPLEMENTACION DE FIREWALL TMG FOREFRONT	21/11/2016	

Flujo de Ingreso	Mes 1	Mes 2	Mes 3
Implem. Firewall TMG Forefront			
Presupuesto Total	57090	9000	9000
	57090	9000	9000
Total x 3 meses S/	75090		

Ingresos	75090
Margen de Contribución de la Empresa	30000
	45090

* Esta Incluido el Margen de Contribucion de la Empresa que es S/ 30000 y el total es S/ 75090

EVALUACIÓN FINANCIERA DEL PROYECTO	CÓDIGO	
APROBADO POR: GERENTE GENERAL	FECHA DE INICIO DE VIGENCIA	
IMPLEMENTACION DE FIREWALL TMG FOREFRONT	01/06/2015	

11.1.5 FLUJO DE CAJA

Meses del Proyecto	0	1	2	3
Inversión del Proyecto	-34322.00			
Egresos Mensuales		-17322.00	-8500.00	-8500.00
Ingresos Mensuales		57090.00	9000.00	9000.00
Recuperación Ingresos no Percibidos		0.00	0.00	0.00
Flujo Neto desp. Impuesto	**-34322.00**	**39768.00**	**500.00**	**500.00**
Valor Presente de Flujos	-34322.00	33701.69	359.09	304.32
Recuperación de la Inversión		-620.31	-261.21	43.10

Periodo de recuperación de la Inversión	meses
Periodo de recuperación de la Inversión	mes

11.2. RENTABILIDAD DEL PROYECTO Y JUSTIFICACION TECNICA ECONOMICA

a) Costo de oportunidad del Proyecto	0.18	
Valor Presente del proyecto	34365.10	
Valor Presente Neto del Proyecto	43.10	VAN >=0, Se acepta la propuesta

b) Tasa Interna de Rendimiento (TIR del Proyecto)

Tasa Interna de Retorno	0.18 > 1.39 % , se acepta el proyecto

c) Indicador costo/beneficio

B/C=	797.29

“IMPLEMENTACIÓN DE UN FIREWALL TMG FOREFRONT PARA LA SEGURIDAD PERIMETRAL DE LA RED DE DATOS DE LA CLÍNICA ALIADA”

Capítulo II:
PLAN DEL PROYECTO

2.1. Antecedentes de la Investigación

Para garantizar los buenos resultados y el éxito del proyecto a implementar fue necesario consultar con diferentes y diversas fuentes o trabajos de investigación relacionados a la propuesta de solución que estamos planteando como proyecto a la clínica ALIADA.

Jorge Luis Valenzuela Gonzales (2012) Universidad Católica del Perú, Lima / Perú. Presentó su trabajo de tesis titulado: Diseño de una arquitectura de seguridad perimetral de una red de computadoras para una empresa pequeña.

En el trabajo realizado se presenta una solución de seguridad perimétrica que cubra los requerimientos de una red de computadoras de una empresa pequeña. Se muestra además una simulación del diseño propuesto en un ambiente de pruebas controlado.

En el primer capítulo se presenta el estado actual y riesgos de la información, y la importancia de la misma. Se presenta además la seguridad perimetral de la red de datos como parte de una problemática mayor. La seguridad de la información.

En el segundo capítulo se muestra en detalle y de manera técnica, los riesgos, amenazas contra la integridad de una red de computadoras de una empresa pequeña y las contramedidas que pueden ser adoptadas.

En el tercer capítulo se explica el escenario de trabajo, sus requerimientos y sus necesidades sin especificar aun producto alguno, sea software o hardware. En el cuarto capítulo se presentan los criterios que fueron tomados en consideración para la selección de la solución más idónea para el escenario planteado en el tercer capítulo.

En el quinto capítulo, se desarrollan la política de seguridad que debe ser aplicada en la solución seleccionada en el cuarto capítulo, se plasma en los

componentes que la conforman y se evalúa su desempeño en un ambiente de pruebas.

Finalmente se presenta las conclusiones que se desprenden del análisis del escenario planteado, así como las recomendaciones para mantener un nivel de seguridad adecuado.

Nuttsy Aurora Lazo García (2012). Universidad Católica del Perú, Lima/Perú.

Presentó su trabajo de tesis titulado: Diseño e implementación de una red LAN (Local Área Network) y WLAN (Wireless Local Área Network) con sistema de control de acceso AAA (Authentication, Authorization and Accounting).

En el primer capítulo se definió todas las tecnologías que se emplearon en la implementación de la solución y cuál fue la evolución tecnológica para llegar a ellas.

El estudio se hizo de manera separada para la LAN y para la WLAN porque al tratarse de redes con interfaces diferentes, cada una tiene definida de forma independiente métodos y estándares de seguridad para el acceso a la red.

En el segundo capítulo se planteó un estudio del problema y se le ubicó en un escenario real con el fin de especificar las exigencias de la empresa, la cual requiere una solución de una red LAN y WLAN que garantice la seguridad de la información y el uso adecuado de los recursos de la red.

En el tercer capítulo se diseñó la solución, realizando un análisis de los requerimientos propuestos en el segundo capítulo. Una vez terminado el análisis se decidió cuáles de los métodos y estándares estudiados en el capítulo uno se usarían en la implementación.

En el cuarto capítulo se muestran los resultados y el análisis de la implementación de la solución diseñada en el laboratorio de redes de la especialidad. En el quinto capítulo se realizó el análisis económico para medir la rentabilidad del proyecto haciendo uso de la tasa interna de retorno (TIR) y el valor actual neto (VAN) como métodos financieros de inversión.

Pablo Galdámez (2016). Empresa de Seguridad Cysbec, Buenos Aires / Argentina.

Presentó un artículo titulado: Los desafíos de la ciberseguridad y la ciberdefensa.

La principal función de la seguridad informática es cuidar los bienes informáticos preciados de la organización, que pueden ser la información, el hardware o el software. Rigiéndose a cierto tipo de medidas, la seguridad informática apoya la organización en el cumplimiento de sus metas, cuidando sus bienes económicos, sus sistemas, su reputación, su situación legal, y otros bienes tanto tangibles como intangibles. Lamentablemente, muchas veces vemos a la ciberseguridad como un obstáculo en la consecución de los propios objetivos de la organización, puesto que diseña métodos y técnicas rigurosas a los usuarios, a los sistemas y a los gestores. Pero tiene que señalarse a la seguridad informática como un soporte para lograr los objetivos de la organización.

Hay diversas formas de aplicar disposiciones de seguridad para intentar minimizar el riesgo de pérdidas por cuestión de situaciones en los sistemas informáticos, aunque la mayoría de veces solo son consideradas técnicas conocidas, como antivirus, cortafuegos, copias de seguridad, pero las medidas que son más certeras son las planificadas a mediano y largo plazo viéndolo estratégica y tácticamente

Las disposiciones de seguridad más habituales se agrupan en dos aspectos. Medidas de gestión y medidas técnicas. Las primeras son propuestas por los gestores de organizaciones y las segundas medidas son pertinentes a herramientas y sistemas técnicos que intentarán evitar, contrarrestar o recobrar los perjuicios que son ocasionados a los sistemas por parte de amenazas de seguridad.

Empresa de Seguridad Eset Latinoamérica (2014).
Presento un artículo titulado: El desafío de privacidad en internet.

El objetivo del artículo es concienciar a toda la población sobre la situación en el presente de los riesgos informáticos y, con respecto, tratar de evolucionar de la mejor forma viable y así visualizarse en los años venideros. Podemos ver, que en el 2011 hubo un afianzamiento en las botnets y el malware que pretende fines económicos. En 2012 la inclinación primordial fue amenazar directamente a los soportes móviles. Al siguiente año hubo un aumento considerable de los malintencionados para móviles, estas amenazas están en constante crecimiento pero el problema primordial está enlazados con la privacidad en Internet.
En este sentido, casos como el acontecido con Edward Snowden y la Agencia Nacional de Seguridad de los Estados Unidos (NSA) acrecentaron la preocupación de la privacidad en Internet. Sin embargo, eso no disminuyó a los individuos que se vieron agraviadas por algún tipo de código malicioso o amenaza informática. Está claro que esta preocupación es algo así como la iniciativa de los usuarios para con la informática y su seguridad, empero, es primordial que las personas piensen en la Seguridad de la Información, si no es así, no se disminuirán los riesgos informáticos y todo lo relacionado a ellos. La situación es similar a alguien que le preocupa mucho la protección en su casa pero no pone un sistema de alarma, deja pasar a desconocidos, deja puertas y ventanas abiertas, entonces así, hay muchas posibilidades de que ocurra algún episodio de riesgo.

También hubo mucha inclinación en el 2013 y terminará asentándose en los años siguientes el crecimiento numéricamente hablando y complejamente igual con respecto a códigos maliciosos creados en exclusividad para Android. Los delincuentes cibernéticos han iniciado adaptando tácticas clásicas de ataque pero que en teléfonos móviles no se habían aplicado. En este punto, sabiendo

ahora las debilidades principales sus consiguientes beneficios por parte de códigos maliciosos es prácticamente una transformación del cibercrimen que ahora perjudica a la tecnología móvil. Para terminar, la diversificación de dispositivos no tradicionales como autos inteligentes, consolas de juegos, Smart TV y otros, plantea la probabilidad de que en un futuro, se puedan observar amenazas diseñadas para esta forma de tecnología.

Considerando los puntos anteriores, ¿será posible la privacidad en Internet?

2.2. Marco Teórico

La seguridad y defensa de la información en una empresa es el contenido principal de estas páginas, viendo cómo podemos defender a los clientes como a los empleados, con respecto al contenido al que acceden si este es fraudulento o indebido, se propone dotar de un Servidor/Firewall de Microsoft y así poder terminar con ese problema informático.

2.3. Bases Teóricas

2.3.1. Firewall

Un firewall o cortafuegos en español es un sistema o una red que se encarga principalmente de obstruir el acceso no autorizado, descifrando la comunicación entrante y saliente del internet e intranet. Estos cortafuegos aparte de ser equipados en hardware y software pueden ser combinados por ambos.

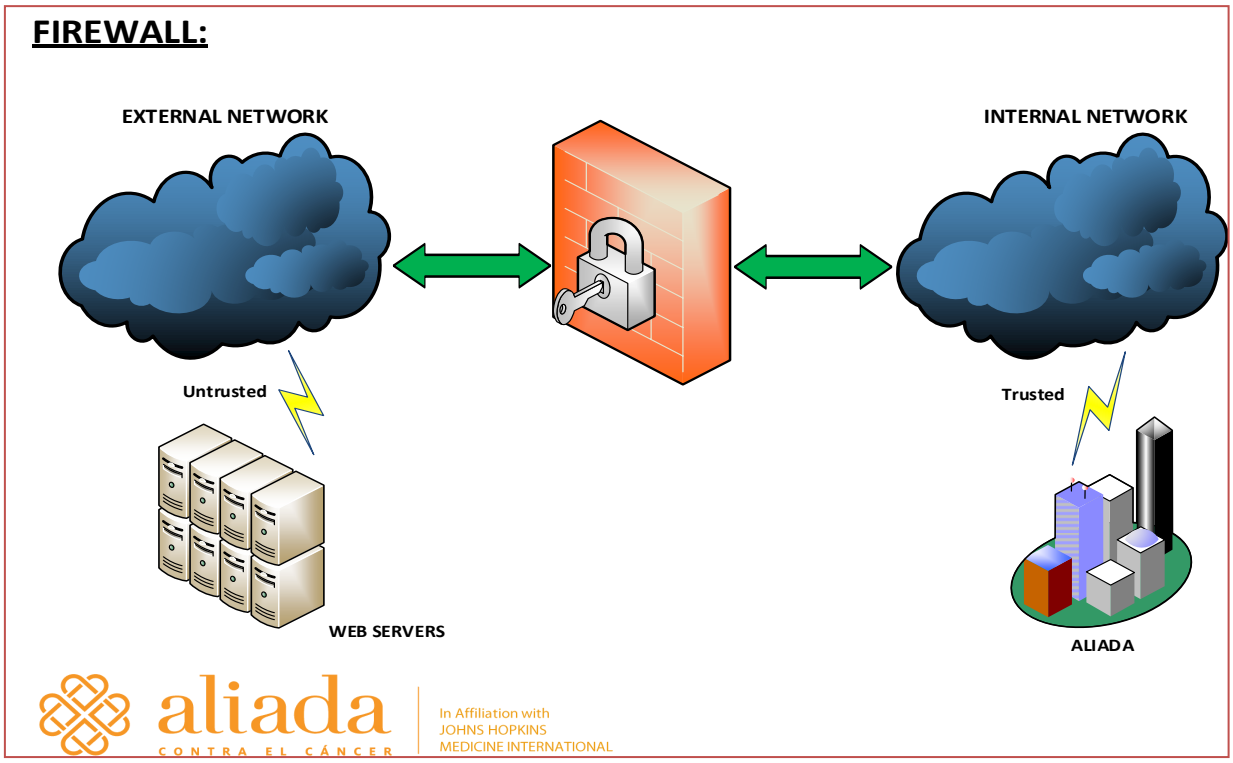


Figura 10: Firewall
Elaborado: Por los autores

2.3.2. Importancia del firewall en una red

Siempre cuando se ha pensado en seguridad informática y se ha tocado el punto tan relevante como lo es implementar un Firewall en la red corporativa surge la pregunta de ¿qué tan importante es?, así entonces facilitamos estos argumentos sólidos para decidir por la adquisición:

- Internet es el lugar primordial de relación con entes maliciosos para el sistema. No solo virus, sino asimismo de apps capaces de dañar al sistema.

- La finalidad de un cortafuego es denegar la entrada al sistema a personas extrañas a él o a la red.

- La idea de un Firewall es alejar a los extraños de los trabajos que son de nuestra propiedad

- Es garantía de que la conexión a Internet es segura.

- El 100% de información que llega de Internet y va para el mismo podrá ser revisada por el cortafuegos.

2.3.3. Contra que nos protege un firewall en una red

Complementando lo argumentado anteriormente podemos mencionar las siguientes características de las cuales nos protege un firewall:

- Impide ingresos no consentidos y extraños al sistema, habitualmente originario de direcciones IP inestables y débiles.

- Incomunica el tráfico originado de fuera hacia adentro.

- Establecen un punto de inclinación de seguridad y pruebas de control, que puede ser estructurado como para componentes exteriores al sistema, tanto para personas que trabajen desde dentro del sistema.

- Un firewall vigila la intranet de una empresa y la cuida de cualquier riesgo de las redes públicas o compartidas por esta misma.

- Ayuda principalmente, a precaver actos de pillajes en ordenadores y programas de nuestra red.

2.3.4. Tipos de Firewall

Podemos encontrar principalmente dos tipos de Firewall a implementarse en una red, Firewall por Software y Firewall por Hardware.

2.3.4.1. Firewall por Software:

Los cortafuegos permiten poner en funcionamiento a través de hardware, lo que sería más preferible aunque es algo costoso en comparación a un firewall por software.

Los Firewalls personales o de software son programas que depuran la circulación de datos que entra y sale de una computadora. Una vez asentados, el cliente necesita establecer el nivel de protección: aprueba o niega la entrada de ciertos software a Internet (por un lapso o definitivamente) y concede o no la entrada desde el exterior.

En el caso de las redes domésticas, las computadoras están normalmente conectadas a Internet, por eso se requiere de un cortafuego por software. Algunas empresas brindan un servicio de protección por hardware, pero este tipo de sistema casi siempre se limita a empresas y se trata de conexiones mucho más costosas que las creadas para el hogar.

Los Firewalls de software no son tan complicados como otros aciertos profesionales mucho más caros y creados para empresas, pero eso sí, colman las expectativas y bastan para la protección de una pc conectada a Internet o una red doméstica.

Para poder elegir un buen Firewall de software se debe pensar, evidentemente el nivel de protección que nos ofrece el programa. Pero como es un software

dirigido a un público el cual la mayoría es novato, el correcto funcionamiento de este programa debe ser casi automático totalmente.

Que ofrece un Firewall de software:

- Tiene el gran beneficio de ser otorgado de manera gratuita para uso personal.
- Brinda una distribución de opciones muy simple y también un control absoluto en relación a los filtros.
- Incluye actualizaciones automáticas y soporte técnico en español y también en varios idiomas.
- Funciona sobre cualquier versión de Windows.
- Hay una confirmación de que no se envían datos personales.
- Realiza una supervisión de los programas que aparecen accionados y bloquea cualquier intento y forma de daño al sistema.
- Tiene dos sentidos al momento del filtro de la pc: inspeccionando el tráfico del sistema y el de las aplicaciones.
-
- Hay Firewall que traen tres rangos de configuración automática (baja, media y alta protección). Aunque también puedes personalizarlo.

- Pueden realizar avisos a través de mail si acaso ocurre alguna acción sospechosa de peligro.
- Siempre que hay un daño o intento de el en una conexión externa se emite un informe y se cuestiona el acceso.

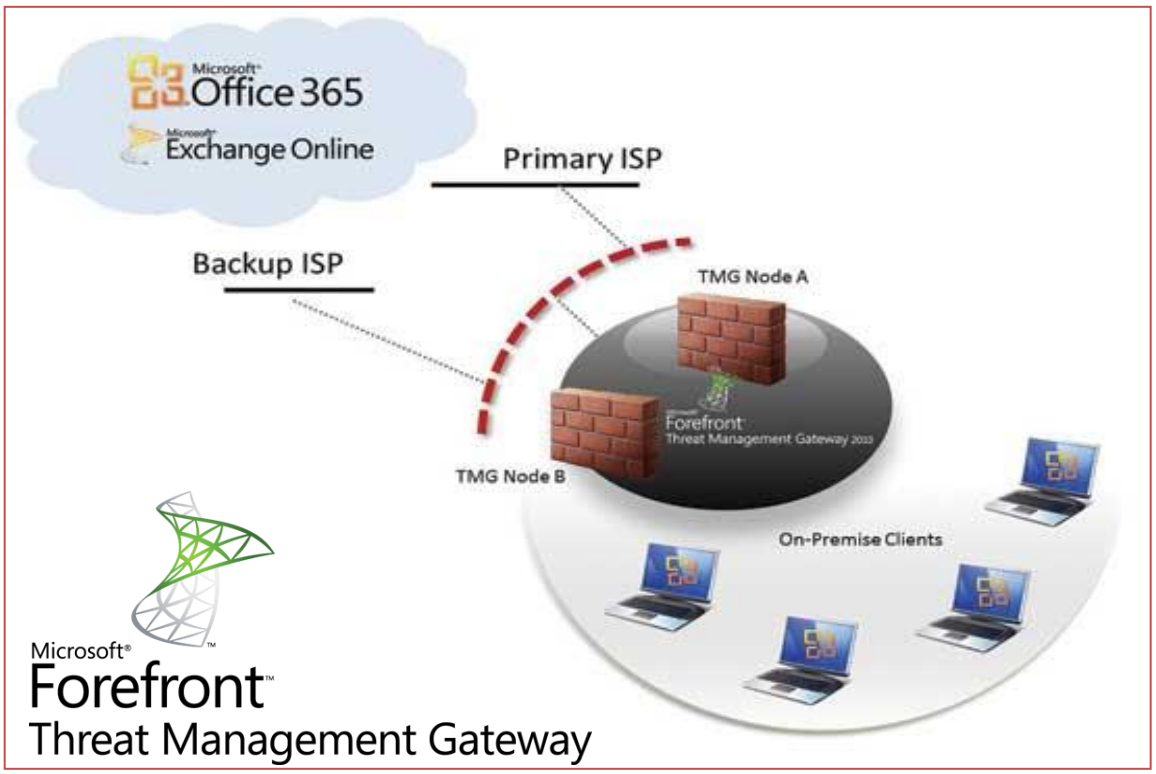


Figura 11: Tmg Forefront
Elaborado: Por los autores

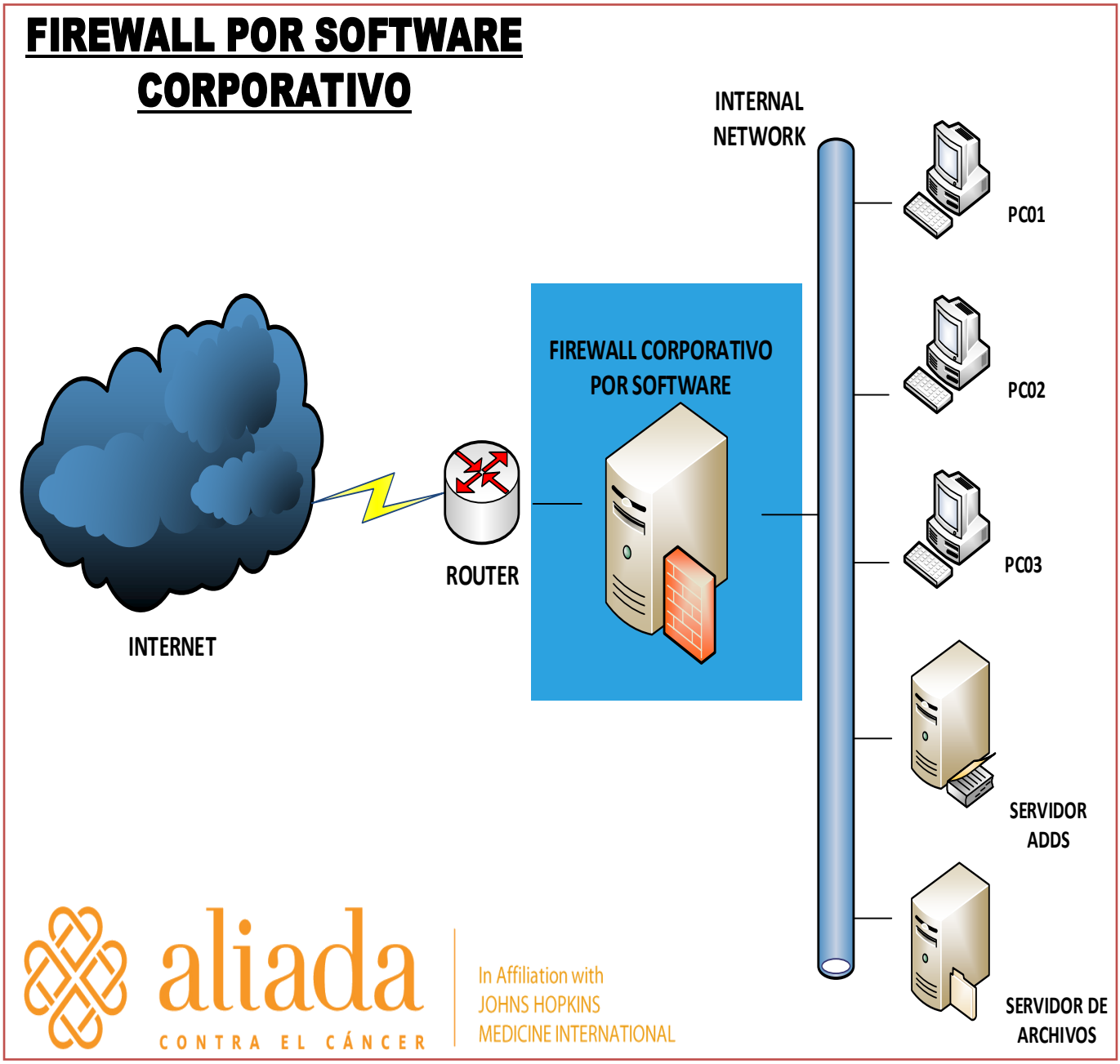


Figura 12: Firewall por Software
Elaborado: Por los autores

2.3.4.2. Firewall por Hardware:

Un cortafuegos es un hardware específico con un sistema operativo que filtra el tráfico y resuelve si la información ingresa, se cambia, o se suprime.
Es necesario tener como mínimo dos tarjetas de red para que así un firewall se desempeñe con total normalidad.

El bosquejo tradicional de un firewall para custodiar una red local que se encuentra enlazada a internet por intermedio de un router. El cortafuegos tiene que ir entre el router, con un solo cable y la red local, conectado al dispositivo hub. Si se tienen otras necesidades para con cada red, también es posible colocarse más de un Firewalls para instalar diversos cercos de seguridad con respecto al sistema que se desea resguardar.

Es muy común que se requiera exponer un servidor a internet, podría ser un servidor web, un servidor de correo, u otro. Es ahí precisamente que se permite todo tipo de conexión con ellos. Aconsejamos en estos casos situar el servidor en un sitio muy aparte de la red, llamamos ese lugar DMZ o también conocida como zona desmilitarizada.

Ese lugar está preparado para admitir los servidores que sean necesarios. Es así que ingresar a internet por parte del servidor es permisible, y si fuera el caso de un ataque o acceso no permitido, la red local sigue en constante protección por el Firewall.

Los cortafuegos están aptos para ser utilizado en una red cualquiera. Es normal usarlos como seguridad de internet en las organizaciones, no obstante son también utilizados por una doble función: examinar las entradas externas para

adentro, asimismo los internos hacia afuera; lo mencionado al final se realiza con el firewall.

Este es el esquema típico de un cortafuegos que cuida una red local enlazada a internet por intermedio de un router. El cortafuegos se tiene que colocar entre el router (con un solo cable) y la red local (conectado al switch o al hub de la LAN).

El bosquejo tradicional de un firewall para custodiar una red local que se encuentra enlazada a internet por intermedio de un router. El cortafuegos tiene que ir entre el router, con un solo cable y la red local, conectado al dispositivo hub.

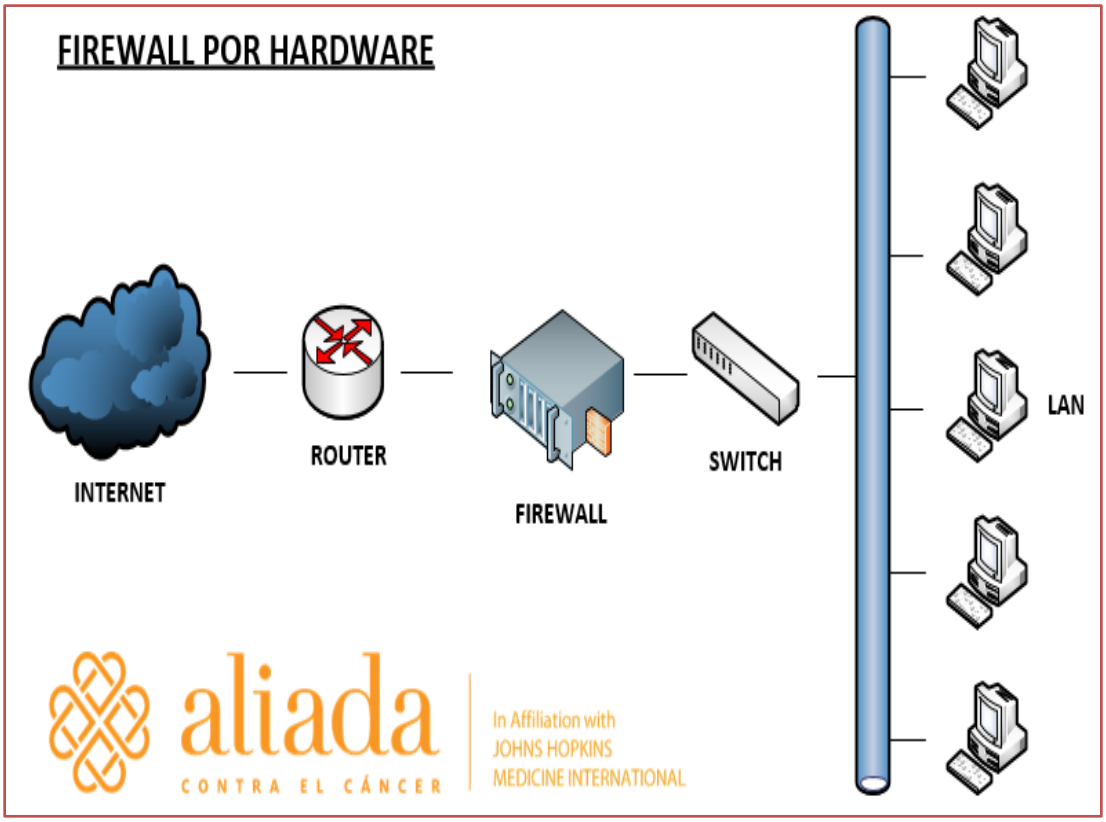


Figura 13: Firewall por Hardware
Elaborado: Por los autores

2.3.5. Operación del Firewall

Dentro de las muchas características y beneficios que nos puede brindar un firewall según sea el producto elegido aremos mención a cuatro puntos de los cuales a la vez hacen referencia a nuestras variables del proyecto, los puntos importantes son:

2.3.5.1. Filtrado de paquetes:

Es la técnica que aparece en la primera generación de Firewalls, y se encarga de verificar todo la comunicación de red, cada paquete al ingresar o salir de la red es revisado y su rechazo o aceptación está regido a las normas impuestas por el usuario.

Lo único que podemos acotar al cliente es que el filtrado a pesar de ser seguro y transparente es muy complicado cuando se va a configurar. El Firewall revisa minuciosamente los datagramas y así poder definir si este pertenece solo a un paquete filtrado por el cortafuegos y también si ha sido aprobado por intermedio de sus reglas.

Todas las normas del filtrado se fundan en reexaminar todos los datos que tiene cada paquete en su encabezado, y así posibilita su traslado en un proceso de IP. Este contenido radica en la dirección IP fuente, el IP destino, el protocolo encapsulado (TCP, UDP, ICMP,), el puerto fuente TCP/UDP, el puerto destino TCP/UDP, el tipo de mensaje ICMP, la interface de entrada del paquete, y la interface de salida del paquete.

Al encontrarse el mensaje o correspondencia y las normas ceden permiso para que el paquete ingrese, este va a ser trasladado de acuerdo a la información a la tabla de ruteo, si al contrario la información no cumple con las reglas, estas le negarán el paso y será rechazada.

Si no son parte de las reglas, ciertos parámetros decidirán si ceden permiso o niegan el paso del paquete.

Algunas peculiaridades de filtrado que un administrador de redes podría gestionar en un Firewall filtra-paquetes para afinar su actividad serian:

- Permitir la entrada de sesiones Telnet solamente a una lista especifica de servidores internos.
- Permitir la entrada de sesiones FTP únicamente a los servidores internos determinados.
- Permitir todas las salidas para sesiones Telnet.
- Permitir todas las salidas para sesiones FTP.
- Rehusar todo el tráfico UDP.

Casi todos los firewall se despliegan solamente con ruteadores filtra paquetes. Aunque algunos planean los filtros configurando a la vez el ruteador, sea o no pequeño, el precio para la implementación el filtro de paquetes no es costoso; ya que ahora también contienen los ruteadores revisiones de software. .

A partir de ahí las entradas a la internet se da habitualmente por una interfaz WAN, optimizando la función del ruteador supervisando el tráfico y determinando menos cantidad de filtros. Por último, el ruteador de filtro es habitualmente transparente a sus últimos clientes y a las aplicaciones para lo cual no necesita entrenamiento especializado o programa particular que requiera ser instalado en cada servidor.

Determinar el filtro de paquetes resulte ser una labor difícil puesto que el administrador de redes requiere un meticuloso análisis de diferentes servicios de la internet, como los formatos de encabezados de paquetes y también valores específicos esperados a ubicar en cada campo. Si los requerimientos de filtro son muy complicado, se requerirá soporte complementario para que el grupo de normas de filtro inicie su complicación y extienda el sistema dificultando su administración y entendimiento.

Por último, es más difícil de comprobar las correcciones de las normas de filtro luego de su configuración en el Firewall. Quizá se podría dejar una localidad vierta sin comprobar su fragilidad. Todo paquete que ingresa desde un Firewall podría ser probablemente utilizado como el comienzo de un ciberataque.

Normalmente, los paquetes con respecto al Firewall, minimizan con respecto al número de filtros usados y su incremento. Los cortafuegos son mejorados para buscar la dirección destino IP de todos los paquetes, formulando simple la consulta a la tabla de ruteo, y el movimiento de paquetes para la interface adecuada de la transmisión.

Puede que el filtro tenga autorización, el ruteador no será el único que tomará las decisiones de desplazar cada paquete, aunque puede suceder fijando la totalidad de las reglas. En este caso se podría agotar ciclos de CPU e impactar la correcta actividad de su estructura.

El filtrado de paquetes IP no consigue ser apto para abastecer todo el control del tráfico. Un Firewall Filtra-Paquetes permite o impide un servicio específico, empero no logra entender el contexto/dato del servicio.

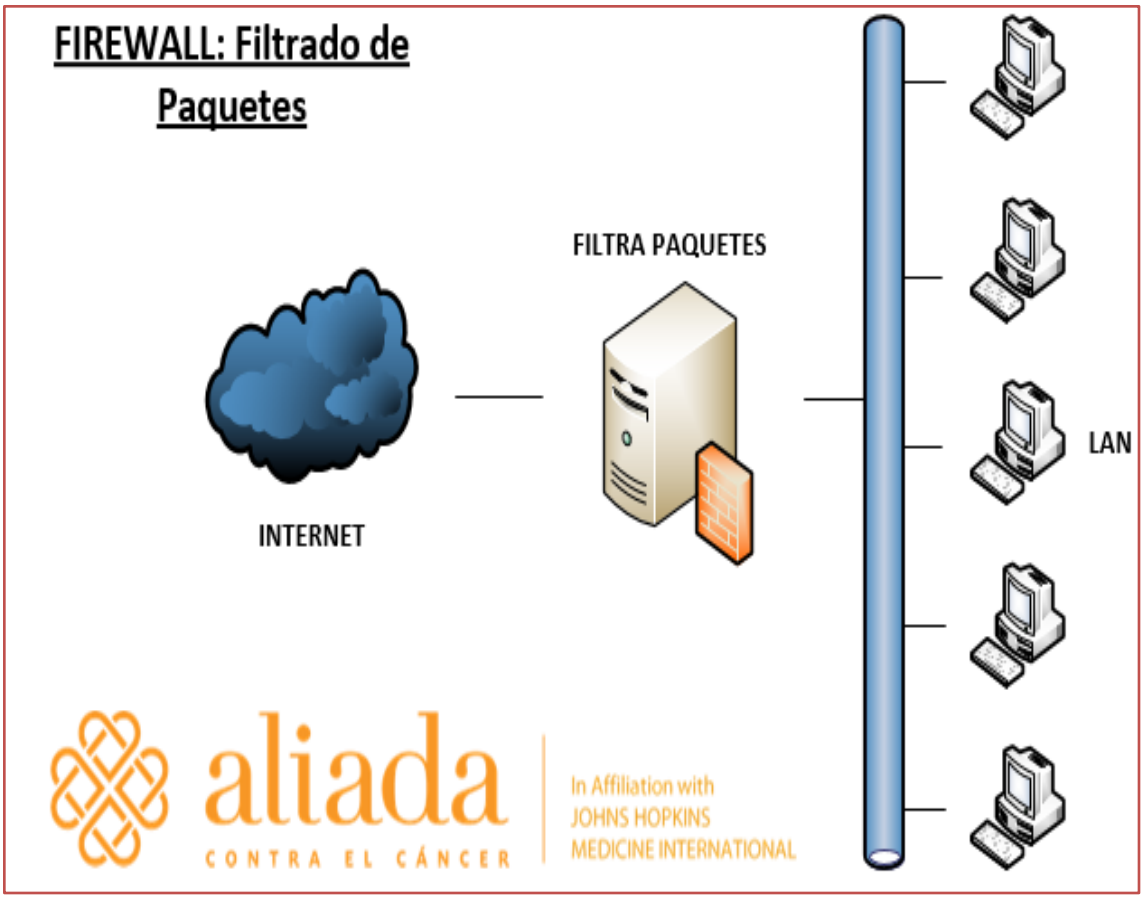


Figura 14: Firewall Filtrado de Paquetes
Elaborado: Por los autores

2.3.5.2. Firewall a nivel de Aplicación:

Es parte de la tercera generación de Firewalls. Revisa el contenido completo de los paquetes de la red y conserva el nivel de la conexión y el orden de toda información. Dentro de esta tecnología podemos certificar claves para ingresar y ciertos patrones de peticiones de servicios.

Casi todos estos Firewalls solicitan programas especiales y servicios Proxy. Hay que acordarnos que el servicio Proxy es un software que toma la mecánica segura a algunas aplicaciones, tales como FTP o HTTP.

Un servicio Proxy aumenta también en algunos casos el control para ingresar, desarrollar chequeos pormenorizados a los datos y realizar inspecciones con respecto al contenido transmitido.

Normalmente son hosts que van siempre bajo servidores Proxy, y niegan el tráfico directo entre redes y que desarrollan logines realizados e inspeccionan el tráfico que va por medio de ellas.

Los cortafuegos a nivel de aplicación pueden ser utilizados también como interpretadores de direcciones de red, a partir del tráfico cuando entra por un extremo hasta su salida por el otro. Cuando iniciaron los Firewalls a nivel de aplicación no eran tan transparentes a los usuarios finales, pero ya ahora en la modernidad a nivel de aplicación son muy transparentes.

Estos Cortafuegos de nivel de aplicación, nos dan considerables pormenores en sus informes de inspección y llevan a cabo arquetipos de preservación de la seguridad.

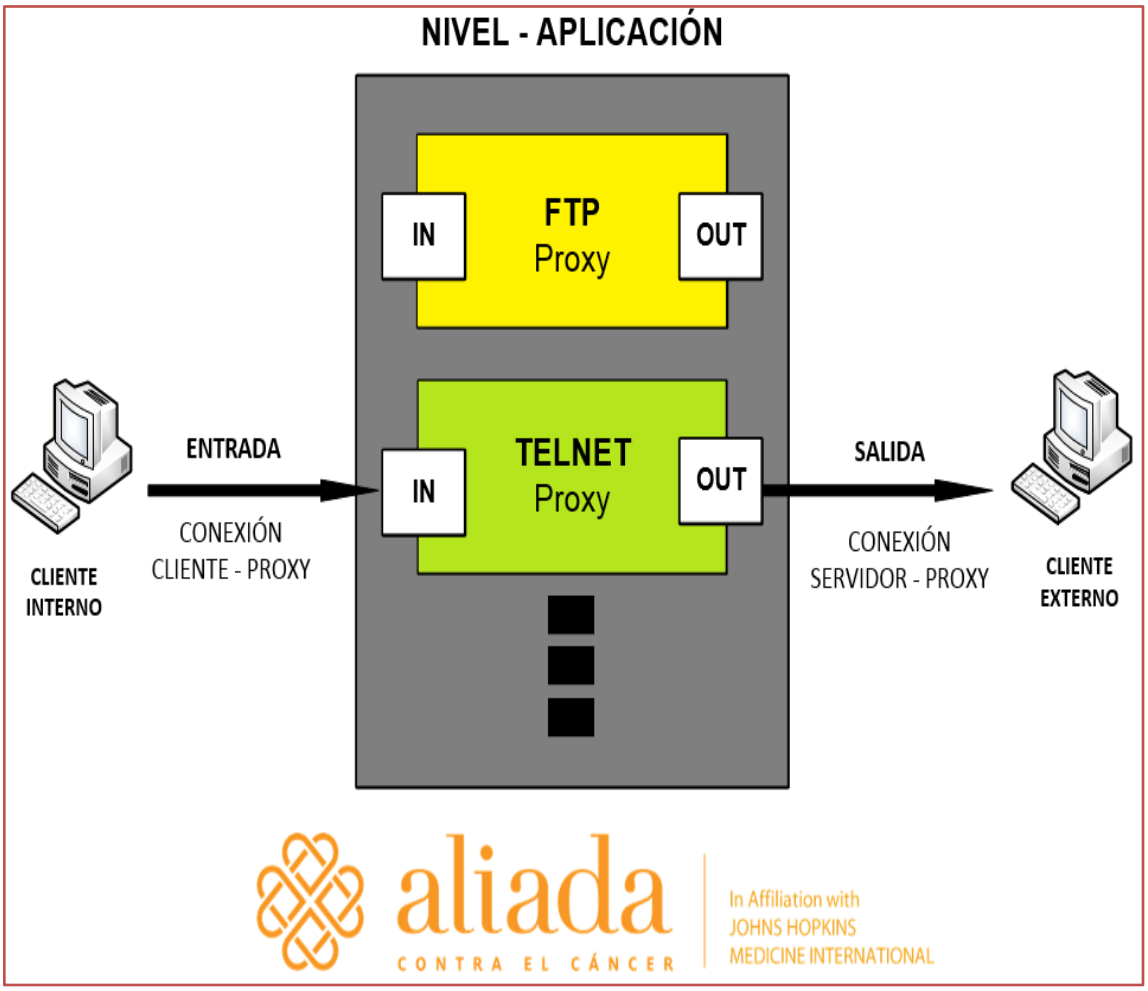


Figura 15: Firewall Nivel Aplicación
Elaborado: Por los autores

En este ejemplo, se representa un Firewall a nivel de aplicación llamada "dual homed gateway". Un Firewall de este tipo es un host de alta seguridad que corre bajo software Proxy. Consta de 2 interfaces de red (uno a cada red) los cuales bloquean todo el tráfico que pasa a través del host.

Un Firewall filtra-paquetes admite el tráfico directo de los paquetes dentro y fuera del sistema, en cambio, el Firewall a nivel-aplicación accede a que la información esté entre los sistemas aunque no deja que haya intercambio directo de paquetes.

Hay un peligro que debemos tener en cuenta, pues el dejar que los paquetes se intercambien adentro y afuera del sistema es porque el servidor residente en los sistemas de protección de la red podría ser protegida de todo riesgo simbolizada por los servicios que se admiten.

Un Cortafuegos a nivel-aplicación normalmente está explicado como un "servidor de defensa" puesto que es un mecanismo esquematizado acorazado y protegido en caso ocurra cualquier imprevisto. Hay una diversidad de utilidades que están dentro de un Cortafuegos nivel-aplicación. Pues ellos administrando la red ofrecen la totalidad de observación en los servicios desde aplicaciones proxy limitadas por un compuesto de comandos y la especificación del servidor interno adonde accedemos a los servicios.

A pesar que el administrador de la red maneje todo el control sobre cuáles son los servicios permitidos a partir de la falta de un servicio proxy para uno en específico se podría mencionar que el servicio está totalmente cerrado.

Los Cortafuegos a nivel-aplicación poseen una capacidad para mantener autenticaciones obligando al usuario a suministrar información minuciosa de registro. Por último, las normas de filtro de un cortafuegos con este patrón es bastante más sencillo en su configuración y prueba que el Firewall filtra-paquetes.

Posiblemente la gran limitación de un cortafuegos a nivel de app es que se necesita cambiar el comportamiento del cliente o solicita de la puesta en marcha de software especializado en cada sistema que accede a los servicios Proxy.

2.3.5.3. Firewall a nivel de Red:

Los Firewalls a nivel de red, adquieren las resoluciones fundándose en la fuente, dirección de destino y puertos, esto en paquetes individuales IP. Solo un router es un cortafuegos a nivel de red, específicamente, a partir del momento que no resuelve situaciones sofisticadamente en ilación con la información o paquete en este momento o desde donde llega ahora.

Los modernos Cortafuegos a nivel de red ahora están perfeccionándose considerablemente, y tienen datos internos en relación a la situación de los enlaces que van por intermedio de ellos, la información de determinados datagramas y más cosas. Un matiz significativo que diferencia a los cortafuegos a nivel de red es que estos enrutan la circulación de modo directo a partir de ellas, de manera que un cliente cualquiera debe poseer un bloque válido de dirección IP asignado. Los cortafuegos a nivel de red procuran ser más rápidos y transparentes a los usuarios.

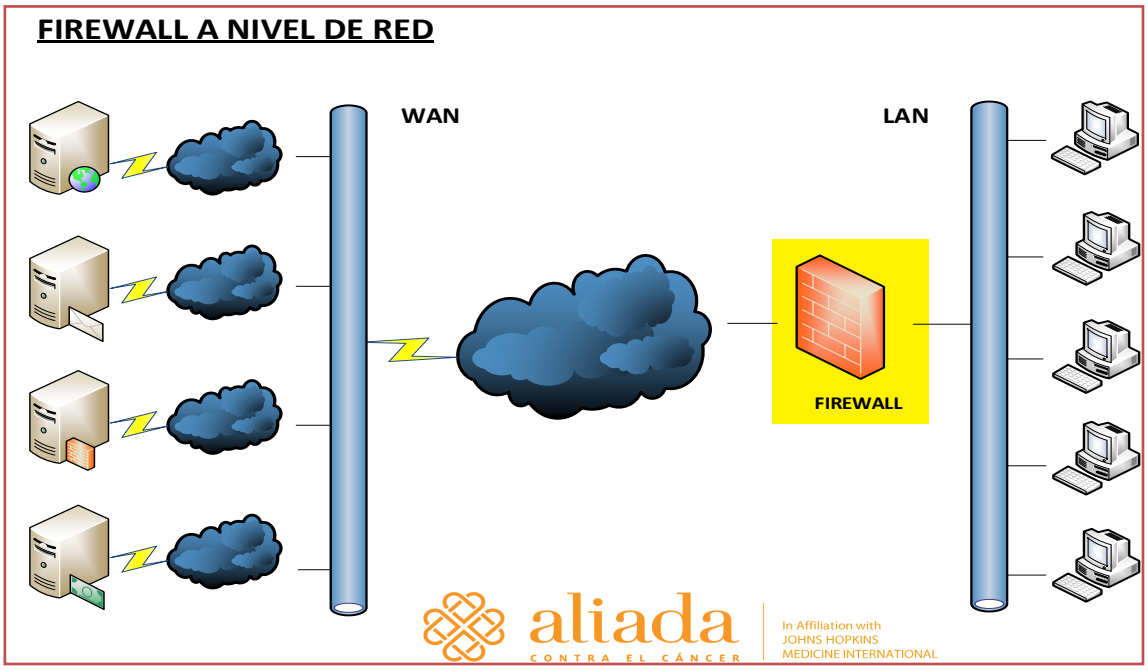


Figura 16: Firewall a Nivel de Red
Elaborado: Por los autores

2.3.5.4. Firewall a nivel de Circuito:

Este mecanismo corresponde a la segunda generación de cortafuegos y certifica que los paquetes correspondan así sea a una petición de conexión o también a una conexión entre dos pc´s. Asigna dispositivos de protección en el momento que una conexión TCP o UDP es instaurada. Ya cuando la conexión se constituye, los paquetes pueden trasladarse por intermedio de las computadoras y no ser inspeccionados cada vez.

El firewall sostiene una tabla de conexiones legítimas, que son permisibles para que los paquetes de la red se trasladen por intermedio de ella si coincide con algún registro de la mencionada tabla. Cuando la conexión concluye, la tabla se suprime y la trasferencia de comunicación de estas computadoras termina.

Un Firewall a nivel-circuito es simplemente una opción perfeccionable en un Firewall a nivel-aplicación. A nivel-circuito solo emite las conexiones TCP incumpliendo todo tipo de mecanismo adicional en filtrado de paquetes.

El Firewall a nivel-circuito es utilizado comúnmente a favor de las conexiones de salida donde el administrador de sistemas domina a los usuarios internos. La superioridad que prepondera es que el servidor de defensa podría estar constituido como un Firewall "híbrido" soportando nivel-aplicación o servicios Proxy para conexiones de venida y a la vez funciones de nivel-circuito para conexiones de ida.

Entonces así es que el sistema de cortafuegos se vuelve sencillo de usar para los clientes internos ya que ellos son los anhelan un acceso directo al Internet durante se abastece el desempeño del firewall necesario para cuidar la empresa de los riesgos exteriores.

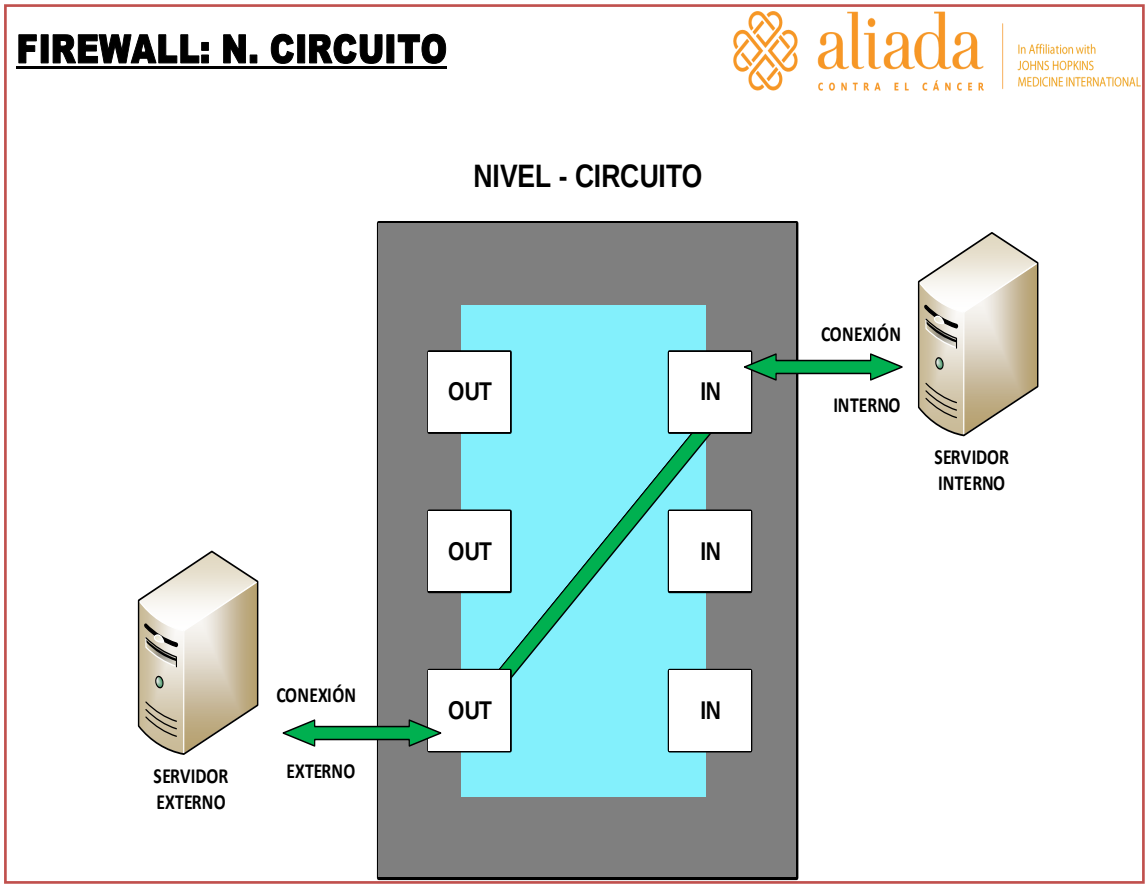


Figura 17: Firewall nivel circuito
Elaborado: Por los autores

2.3.5.5. Arquitectura del Firewall

Existen tres tipos de Firewalls:

- Firewalls de la capa de red
  - Screened Host
  - Screened Subnet
- Firewalls de la capa de aplicación
  - Dual-Homed Host
- Firewalls híbridos

Y tienen marcadas disimilitudes, pero esto no marca superioridad entre ellos, porque cada uno está preparado para un contexto diferente.

Lo que los diferencia unos de otros es el mecanismo que utiliza para dejar pasar el tráfico de una zona a otra. El modelo de International Standards Organization (ISO) Open Systems Interconnect (OSI) precisa siete capas, y en todas se proporcionan los servicios que capas superiores requieren de ellos.

Es valioso saber que mientras es bajo el nivel al que pertenece el mecanismo de "Forwarding", menos compleja será la supervisión del paquete, con lo cual estos Firewalls serán más rápidos pero más vulnerables ante el peligro. En la actualidad encontramos los cortafuegos híbridos que filtran por intermedio de la red y algunas investigaciones a nivel de aplicación cuyo análisis del paquete dependerá del vendedor, del producto, del protocolo y la versión.

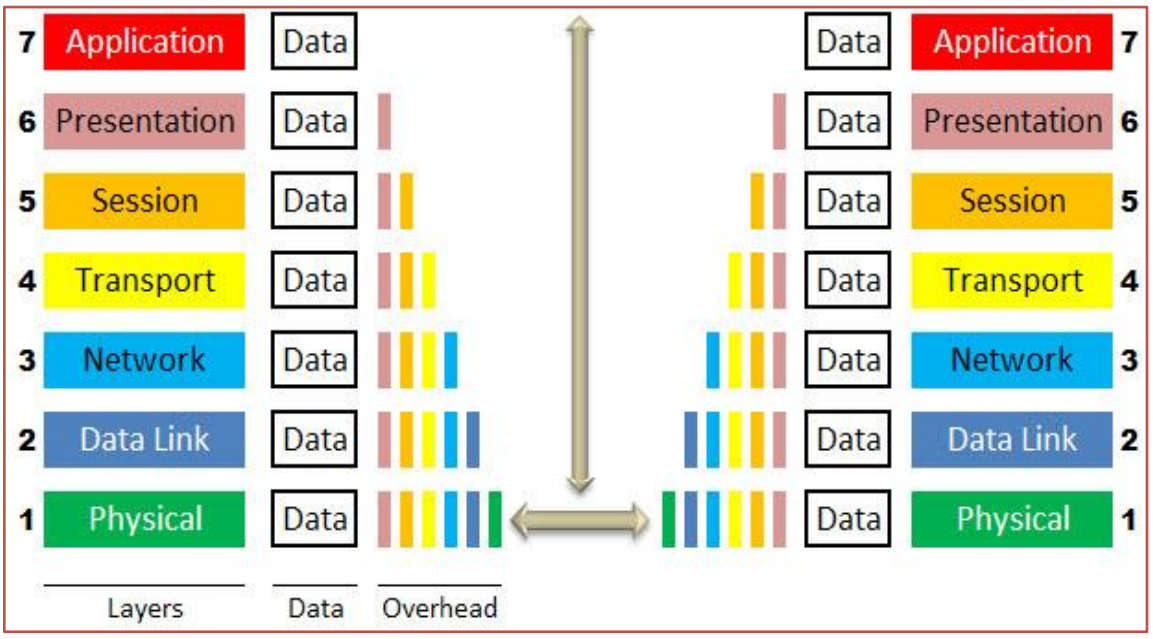


Figura 18: Modelo Osi
Elaborado: Por los autores

2.3.5.6. Firewall de la capa de Red: SCREENED HOST

En este esquema utilizamos un router enlazando las redes internas y externas (Internet), aunque también se estructura el router con filtrado de paquetes y así se imposibilite el acceso directo a redes internas y externas, salvo que se haga con el bastion host quien funciona como un proxy.

El host bastion lo encontramos en la red interna. El filtraje de paquetes es realizado en el Screened Host (router) quien se parametra para que solamente el bastion host pueda admitir conexiones externas. Todo sistema externo que procure ingresar sistema interno o a los servicios internos tendrá que realizarlo por intermedio del bastion host. Es por eso que el host mencionado tiene que ser altamente seguro.

También el Screened Host utilizando el filtro de paquetes señalará qué conexiones son admitidas a partir de la red interna al mundo externo, continuando con sus políticas de seguridad. Otros de los servicios externos podría realizarse desde el Screened Host o por qué no del bastion host mediante el proxy.

Este esquema nos deja trasmitir paquetes desde fuera a dentro de la red, por eso nos hace presentarse como si fuera menos seguro que una arquitectura dual-homed host, que está designada especialmente para no dejar ingresar ningún tipo de paquete externo a la red interna.

En la arquitectura Screened Host se protege de una manera muy simple el router, que brinda servicios muy condicionados, a comparación con el dual-homed host. Para absolutamente todas sus finalidades, el Screened Host facilita más protección y mayor usabilidad a comparación que la Dual-Homed host. Pero en una balanza con el siguiente sistema, hay inconvenientes. El más grande es que

si un atacante maneja el bastion host, entonces toda la red interna está en peligro inminente. El router también simboliza un singular espacio de fallo. Es por este motivo que el siguiente esquema es el más conocido.

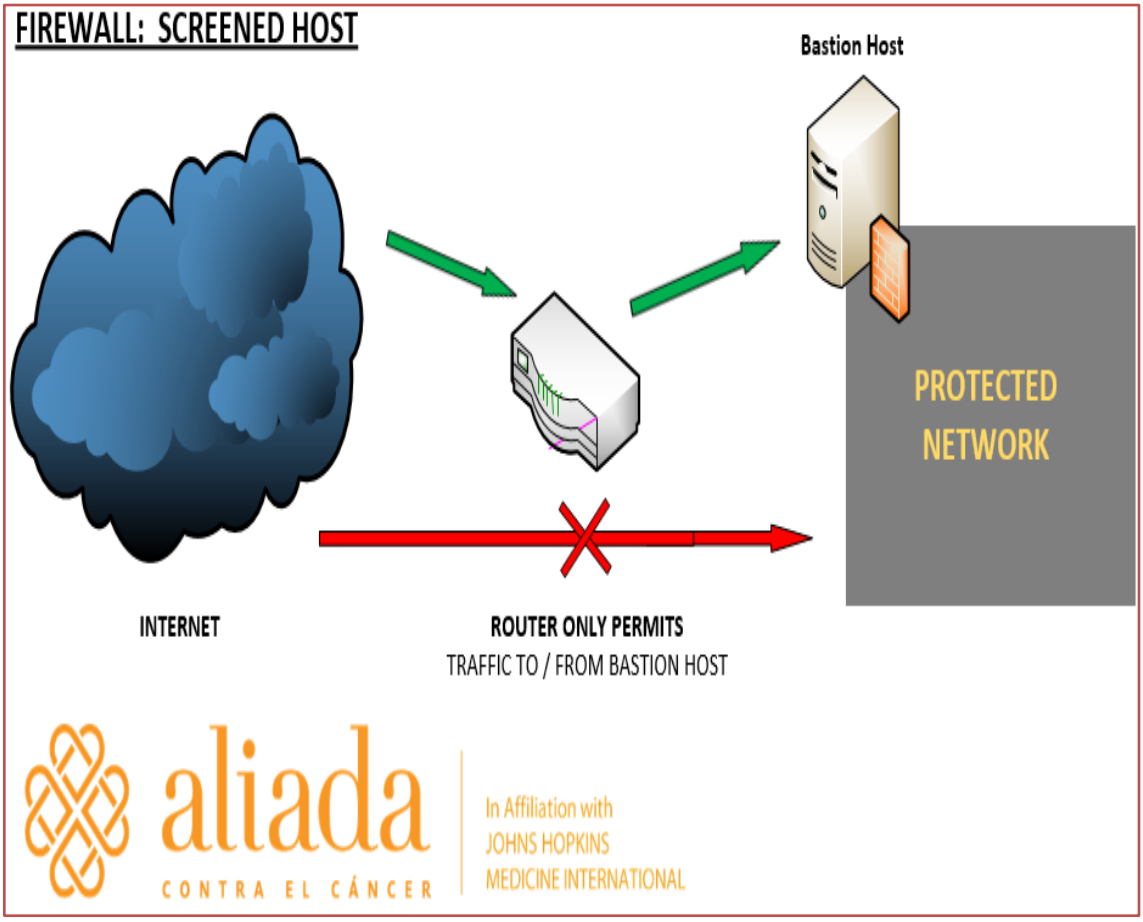


Figura 19: Firewall Screened Host
Elaborado: Por los autores

2.3.5.7. Firewall de la capa de Red: SCREENED SUBNET

El esquema Screened Subnet otorga un punto de protección más que la anterior arquitectura, agregando una red de exterior conocida igualmente como perimeter network en inglés, que recluye la red interna de Internet. La forma de diseñar esto es tener un router conectado a Internet, tras el router una red con un host bastion haciendo las funciones proxy y conectado a la perimeter network, y en esa misma red se conecta otro router que da acceso a la red interna.

Pero, ¿por qué lo hacemos? Porque los ordenadores bastion son las máquinas con mayor debilidad de la red. Así nos esforcemos por su seguridad, son los principales mecanismos especialmente que son embestidos, puesto que es posible vulnerarlos. Ajá, los esquemas screened host, pueden ser atacados por intermedio del host bastion, ahí a que el bastion sea el objetivo principal, puesto a que es indefenso entre las otras máquinas. Si pudieran burlar la protección del bastion host en un esquema Screened Host, es como si se hubiera sacado el premio mayor de la lotería, pues se encuentra junto de la misma red interna con todos los ordenadores indefensos. En el lugar de la arquitectura Screende Subnet si logra ingresar en el host bastion es imposible hacer daño a los ordenadores, ya que este se encuentra aislado, posiblemente intente dañar con la instalación de un snifer, pero no ingresar a la red interna.

La manera sencilla de formar un esquema Screende Subnet es enlazando dos routers al “perimeter net”. Una entre la perimeter net y la red interna, y otro entre la perimeter net y la conexión externa, que es comúnmente el internet. Entonces el ciberataque solo podría ser exitoso si logra burlar a los dos routers, así haya logrado romper el host bastion, tiene que ingresar al router interno.

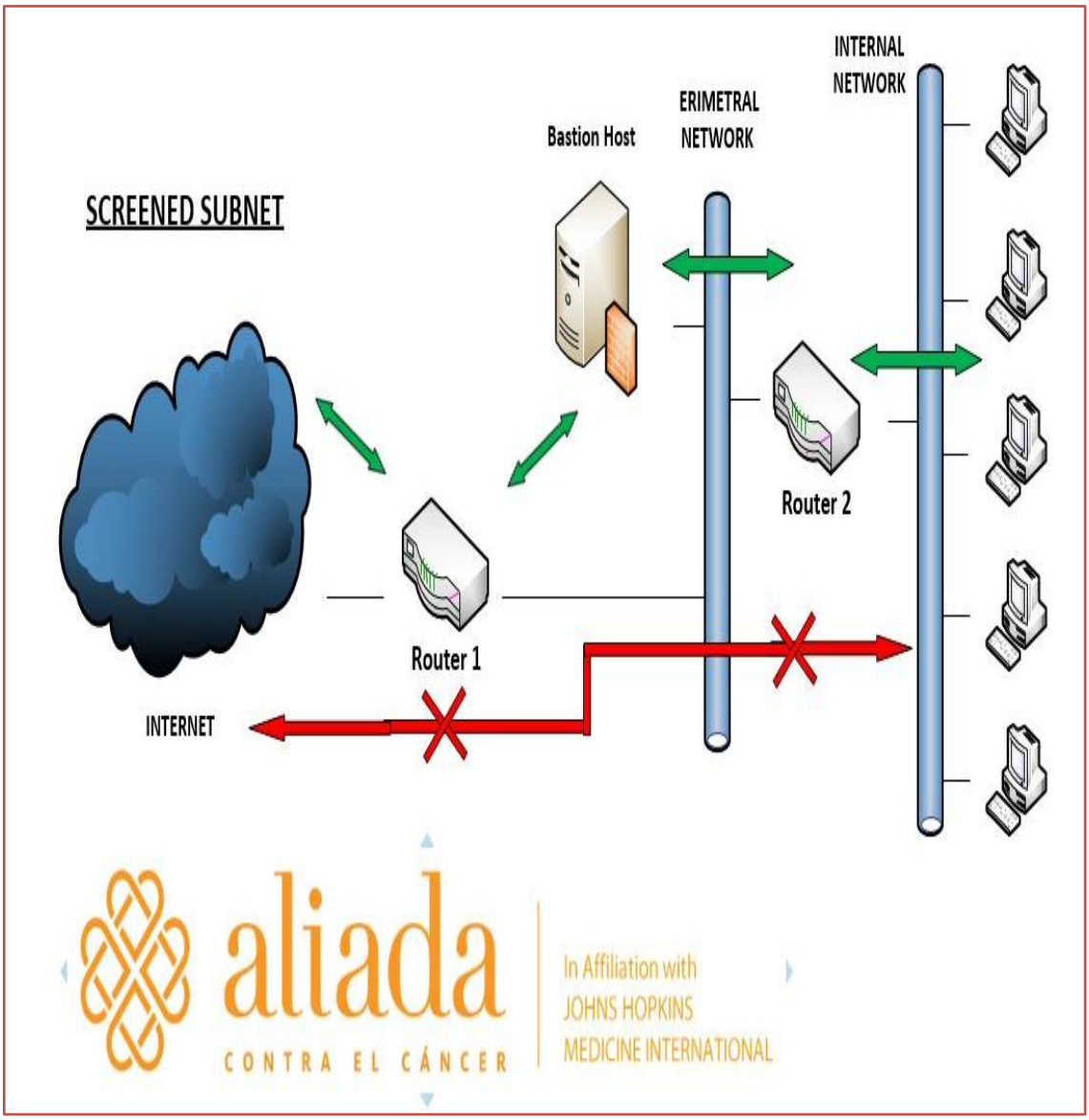


Figura 20: Firewall Subnet
Elaborado: Por los autores

En ocasiones, se realiza un conjunto de redes perimetrales entre la red externa y la red interna. Teniendo en cuenta de la seguridad y confiabilidad de los servicios ubicados en los perímetros. Los servicios más frágiles se colocan en las redes externas y la red interna se ubica al inicio.

2.3.5.8. Firewall de la capa de Aplicación: DUAL-HOMED HOST

El esquema de un cortafuegos Dual-Homed Host es demasiado sencillo: el ordenador Dual-Homed Host se encuentra antes de la red a custodiar, enlazado directamente, entre la red interna e Internet.

Este esquema es elaborado en torno al ordenador dual-homed host, es un ordenador que tiene mínimo dos interfaces de red. Incluso está apto para enrutar paquetes IP de una a otra red, si se implementa una arquitectura Dual-Homed Host se limita esta actividad de enrutaje. Esto ocasiona que los paquetes de una red no estén enlazados directamente a la otra red. Los métodos dentro del cortafuegos se podrían trasmitir con el Dual-Homed Host, y los sistemas fuera del cortafuegos (de Internet) puede comunicarse con el Dual-Homed Host, empero estos sistemas no podrán tener una comunicación entre ellos. El tráfico IP está completamente restringido. Toda circulación en dirección hacia afuera tiene que ser producida por el firewall.

Este esquema podría suministrar altos estándares de control. Puesto que todos los paquetes provienen del firewall. Es seguro también que todo paquete que se encuentra en la red interna que tenga la dirección origen con una IP externa causará de alguna forma un inconveniente de seguridad.

Solo hay una forma para que la red interna se enlace con el exterior y es por intermedio de los servicios proxy que se encuentran en el cortafuegos, y así poder valer de conexión. Aunque tiene una desventaja, ya que no la totalidad de los servicios son posibles de traspasar por Proxy y lo que señala que los usuarios

deberían asociarse a cuentas de usuario en el firewall y enlazarse al exterior a partir de este mismo.

Y esto se torna fastidioso para los usuarios y un probable agujero originario de usuarios internos.

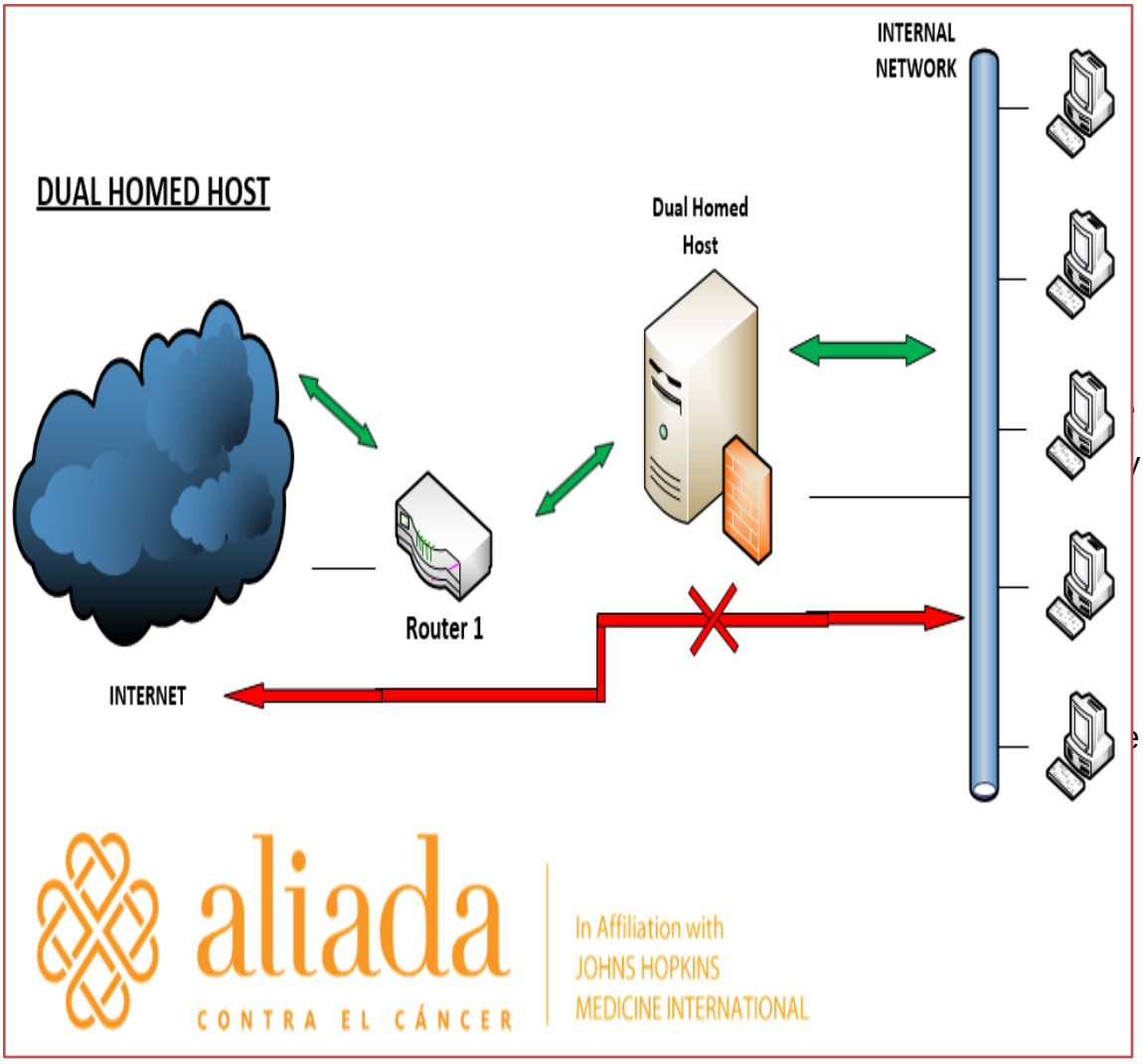


Figura 21: Firewall Dual Homed Host
Elaborado: Por los autores

2.3.6. Filtrado de Paquetes en el Firewall

Tal como se dice en la introducción hacia los firewalls, el filtrado de paquetes es solo uno de los dos tipos de firewalls que existe, el otro sistema es el firewall proxy. Cada uno sube hasta un nivel concreto de la capa OSI. Mientras el primero solo trata hasta el nivel 3 de la capa OSI, donde se ubican los paquetes y basa sus resoluciones en la comunicación que hay en la cabecera del paquete IP. La otra, los sistemas proxy, asciende hasta en nivel de aplicación, pues debe fundamentar sus resoluciones en la información que hay en los datos del nivel más alto. La labor solo se ahonda en el primer procedimiento, y es por eso que se profundiza más en este sistema: el filtrado de paquetes.

El filtrado de paquetes es un dispositivo de seguridad que labora inspeccionando los datos que viajan de ida y vuelta por la red. Se necesita tener claro las razones que se han expresado en la sección TCP/IP para comprender a la perfección esta sección.

Al traspasar información por medio de la red, la información está dividida en pequeños fragmentos, cada una de ellas se destina por separado. Partiendo la información en trozos permite a los sistemas compartir la red, mandando piezas por turnos. En las redes IP, que son las que trato en el trabajo, estas piezas de datos se llaman paquetes. Todos los datos que se traspasan por medio de las redes IP se hacen en forma de paquetes.

El equipamiento elemental que conectan entre sí redes IP se llaman routers. Un router puede ser una pieza dedicada de hardware si otro propósito, o puede ser también un programa que corre en un sistema de propósito general como un PC. Los paquetes atravesando una red viajan de un router a otro hasta llegar a su destino. Internet es de por sí una red de redes.

Los routers determinan la dirección para cada paquete que reciben, tienen que disponer a dónde enviarlo fundamentándose en el destino de desenlace del paquete. Resumiendo, un paquete no lleva ninguna otra información que la IP de destino para asistir al router a tomar su resolusión. El paquete dice al router donde quiere ir, pero no por donde lo debe enviar. Los routers se notifican entre ellos utilizando los 'protocolos de Routing' o 'protocolos de enrutaje' conforme el lenguaje, como por ejemplo Routing

Information Protocol (RIP) es uno de los más sencillos, o bien Open Shortest Path First (OSPF) para elaborar las tablas de enrutaje o tablas de routing, con las que definen cómo dirigir los paquetes a sus destinos. Cuando se enruta un paquete, el router coteja la dirección de destino con las entradas que establece en la tabla de routing y envía el paquete a través de la interfaz que se señala en la misma tabla. En algunas ocasiones no se encuentra ruta determinada para un destino en específico, es así el router utiliza la ruta por defecto o también 'default gateway' que es como se le conoce, y se envía a routers que tienen un mejor enlace, o quizá a los routers que se sospecha puedan conocer el destino.

Al decidir cómo remitir un paquete a su destino, un router observa solamente la dirección destino del paquete y se hace la premisa ¿a dónde debo enviar este paquete? Empero también se debe considerar la pregunta ¿debo enviar este paquete? Pues, bien por la política de seguridad programa en el router se recomienda prescindir el paquete o bien porque a lo mejor el destino no es asequible y es mejor deshacerse del paquete para que ya no de vueltas. En el primer punto se usa lo que se llama filtrado de paquetes, en el segundo se habla del campo TTL (Time To Live). Reflexionaremos sobre el filtrado de paquetes, que es el objetivo de este trabajo final de carrera.

2.3.7. Características del Filtrado de Paquetes

Lo primordial del filtrado de paquetes es la capacidad de brindar, en un solo lugar, seguridad para toda una red. Tomando el servicio Telnet como modelo. Si se restringe el Telnet cerrando en servicio de telnet en todos los computadores, todavía se debería tener precaución por si alguien en la empresa instala en una nueva máquina un servidor de Telnet. También, si el telnet se desactiva desde el router, filtrando la totalidad de paquetes que ayuden a tal propósito, se custodia a la red desde un inicio, sin considerar si hay alguien utilizando un servidor Telnet o no. Otro cosa provechosa es que los routers suelen ser poco, mucho menos que servidores, por eso se entiende que podemos adaptar un mejor control centrando la seguridad en ellos.

Algunas custodias son capaces de proveerse con routers de filtrado de paquetes, y solamente cuando están situadas en ciertas localizaciones de la red. Veremos, es muy buena elección detener todos los paquetes que tengan como dirección de origen una IP que pertenece a un ordenador interno, aunque lo más seguro que se pretenda un ataque spoofing. Se ve ahí que, un atacante intente suplantar a otra máquina 'amiga' o conocida escondiendo su identidad. Para resolver esta situación se necesita bloquear todos los paquetes entrantes con una IP origen que pertenezca a la red interna. Este tipo de soluciones solo pueden hacerse con un router o firewall que tenga la opción de filtrado de paquetes y que esté situado en el perímetro de la red. Y solamente un router en esa localización (por perímetro se entiende que conecta las dos redes a través de él) es capaz de reconocer un paquete así, observando las direcciones origen de todos los paquetes que entren desde fuera de la red.

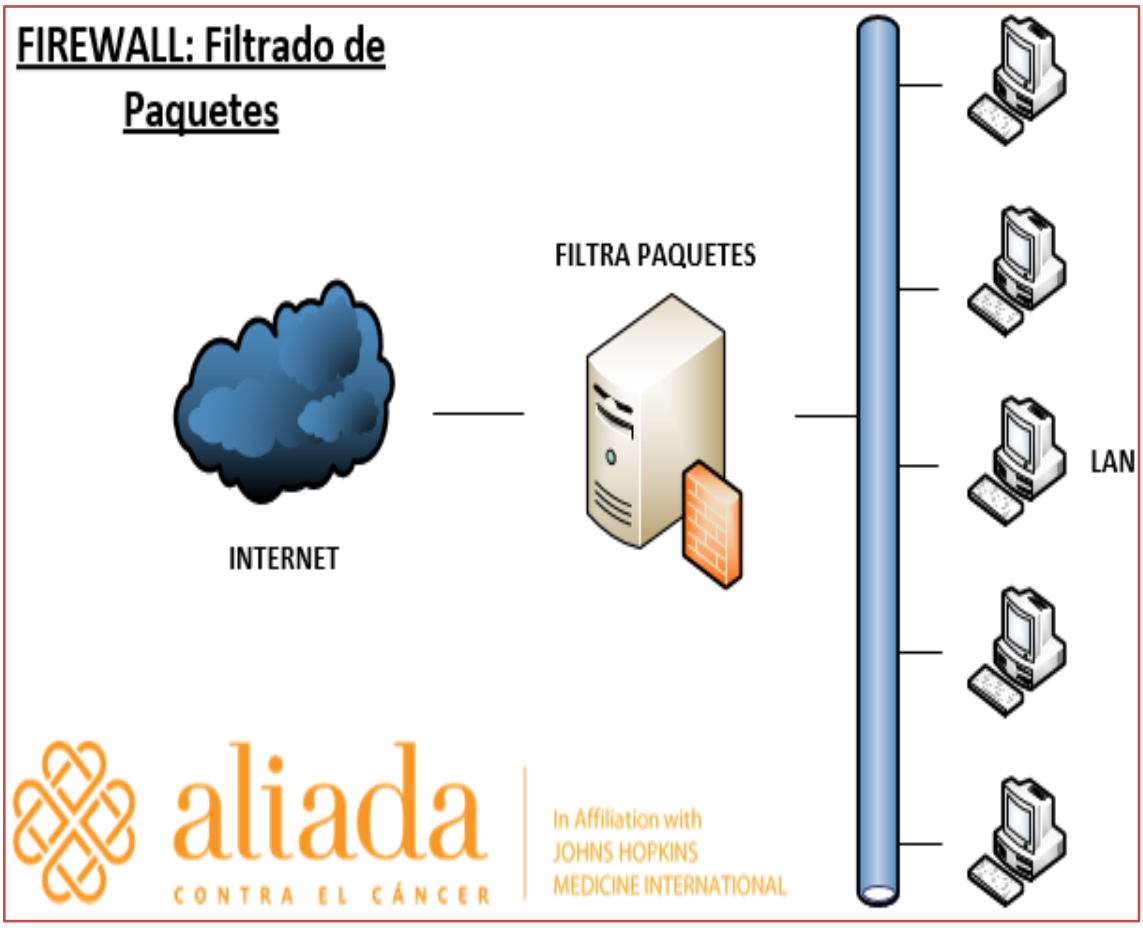


Figura 22: Firewall Filtrado de Paquetes
Elaborado: Por los autores

2.3.8. Firewall Proxy Server

Los servicios proxy son software especializados que están en un firewall: ya sea un host dual-homed con una interfaz en la red interna y otra en la red externa, o bien un host bastion que tiene acceso a Internet a través de otra máquina interna. Estos software redirigen los requests de los servicios que solicitan los usuarios (como sesiones FTP o sesiones SSH), las envía dependiendo las políticas de seguridad. Los proxies sustituyen las conexiones externas y actúan de Gateway a esos servicios. Por esa razón se les conoce también como gateways del nivel de aplicación.

Los sistemas proxy, permanecen más o menos de manera transparente entre el usuario dentro de la red y el servicio fuera de la red. En vez de hablar directamente uno con el otro cada uno de ellos habla con el proxy. Estos tratan las conexiones entre usuarios y los servicios de una manera transparente. La trasparencia es la mejor ventaja de las administraciones intermedias. Para el cliente, un intermediario muestra el engaño que está administrando específicamente con el servidor genuino. Para el servidor genuino, el intermediario muestra la fantasía de que se está manejando directamente con un cliente en la PC intermediaria, en lugar de ser el cliente genuino en otra PC.

Los servicios proxy son efectivos solo cuando se usan en conjunción con algún mecanismo que restringe las comunicaciones directas entre los ordenadores externos e internos. Si los hosts internos pueden comunicarse directamente con los hosts externos, no hay razón para tener un proxy. Un proxy es una solución de software, se debe usar junto con un firewall.

Los servidores intermediarios no solo desvían el movimiento del cliente a administraciones de Internet externas. Los servidores intermediarios controlan lo que hacen, a la luz del hecho de que sintonizan con todo lo que hacen los clientes y, según los enfoques de seguridad, dejan pasar la sustancia. Por ejemplo, un intermediario web puede obstaculizar todas las páginas del sitio que contienen VBScript con el argumento de que ejecutan programas que pueden ser extremadamente peligrosos. Y todo directamente al cliente.

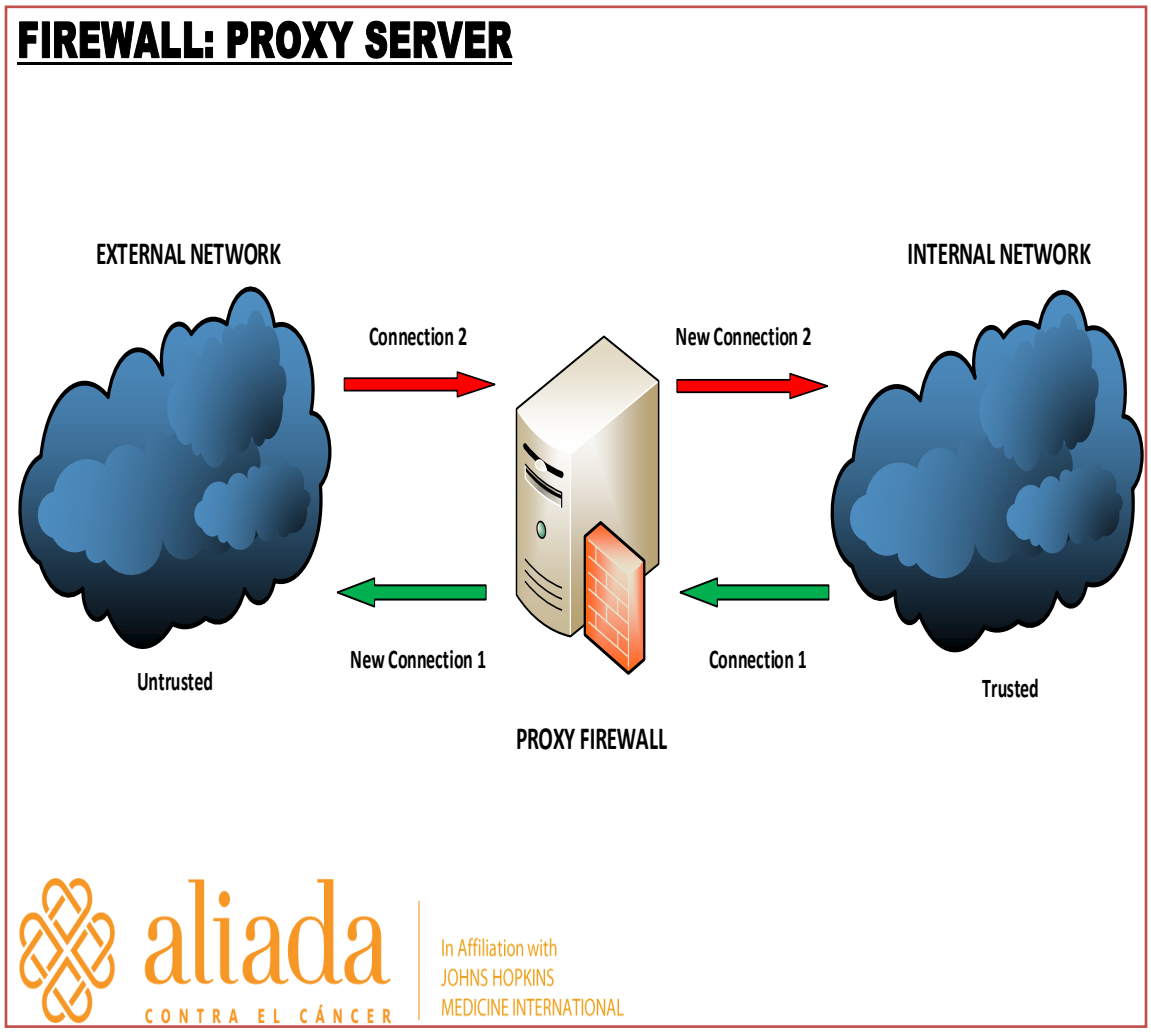


Figura 23: Firewall Proxy Server
Elaborado: Por los autores

2.3.9. Seguridad en Redes

La seguridad en redes consiste en las previsiones hechas en la infraestructura subyacente a una red de computadoras, las políticas adoptadas por el administrador de una red para proteger la red y los recursos accesibles de esta de accesos no autorizados y la efectividad de estas técnicas combinadas.

2.3.10. Seguridad en Redes Comparada con Seguridad en Cómputo

Asegurar la infraestructura de una red es asegurar los posibles puntos de ataque en un terreno instalando las defensas apropiadas. La seguridad en cómputo es proveer las formas de proteger una simple computadora contra intrusiones externas. Las medidas preventivas tratan de asegurar el acceso a las computadoras individuales –la red en si misma- de ese modo proteger las computadoras y otros recursos compartidos como impresoras, sistemas de almacenamiento en red, etc. Los ataques pueden detenerse en su punto de entrada antes que estos se extiendan. Contrario a esto, la seguridad en una computadora, las medidas tomadas se enfocan en la seguridad de hosts individuales. Un host cuya seguridad se ha comprometido, probablemente puede infectar a otros equipos conectados a una red potencialmente insegura. La seguridad en una computadora es vulnerable ante los usuarios con altos privilegios en esos equipos.

2.3.11. Atributos de una red Segura

La seguridad en una red comienza desde la autentificación de cualquier usuario, más conocido como el nombre de usuario y password. Una vez establecida la autentificación, un firewall cumple las políticas de acceso como que servicios pueden acceder los usuarios de la red. Aunque estos métodos son efectivos para prevenir accesos no autorizados, estos fallan al analizar contenidos potencialmente dañinos como los gusanos informáticos que se transmiten a través de una red. Un sistema de prevención de intrusiones (IPS) ayuda a detectar y prevenir de malware. Un IPS también monitorea tráfico en la red sospechoso de contenido, volumen y anomalías para proteger a la red de ataques como denegación de servicios. La comunicación entre 2 hosts en una red, debería ser cifrada para mantener la privacidad. Los eventos individuales ocurridos en la red pueden ser registrados con propósitos de auditoria y para un análisis de más alto nivel.

2.3.12. Seguridad Perimetral

La seguridad se convierte continuamente en una parte más destacada en la base de TI de cualquier asociación y es una tendencia general a diseñar estrategias que salvaguarden sus marcos de datos.

Contingente a la criticidad de la tierra y la preocupación por el bienestar de la organización hay diversos tipos de seguridad para garantizar los beneficios de la misma.

La seguridad fronteriza construye su lógica con respecto a la seguridad de toda la organización de PC de una organización "considerando todo", es decir, estableciendo un caparazón que asegura cada componente sensible contra diferentes peligros, por ejemplo, infecciones, gusanos, troyanos, rechazo de asaltos de la administración, robo o aniquilación de información, pirateo de sitios corporativos, etcétera

Esta tipología de peligros concebibles ha instigado una división del seguro de borde en dos inclinaciones: a nivel de sistema, en el cual podemos descubrir los peligros que hablan de los asaltos de los programadores, las interrupciones o el robo de datos en las asociaciones remotas; y en el nivel de sustancias, que incorpora los peligros que son infecciones, gusanos, troyanos, spyware, phishing y diferentes tipos de malware, spam o spam y contenido web que no se ajusta a las organizaciones. Esta división razonable, junto con la forma en que los peligros han avanzado últimamente, ha llevado al mercado de seguridad fronteriza a centrarse en la producción de artilugios dedicados a cualquiera de las dos razones.

El cortafuegos / VPN es el par de seguridad fronteriza con crónicas y los marcos IDS (sistemas de detección de intrusiones) e IPS (sistemas de prevención de intrusiones) se han consolidado para controlar la entrada a los marcos de una organización del exterior.

En principio, el firewall o cortafuegos se necesitan para controlar y monitorizar las comunicaciones. Además, se encarga de examinar las acciones de las

aplicaciones que se conectan a la red y los puertos de las máquinas (comunicaciones P2P, por ejemplo).

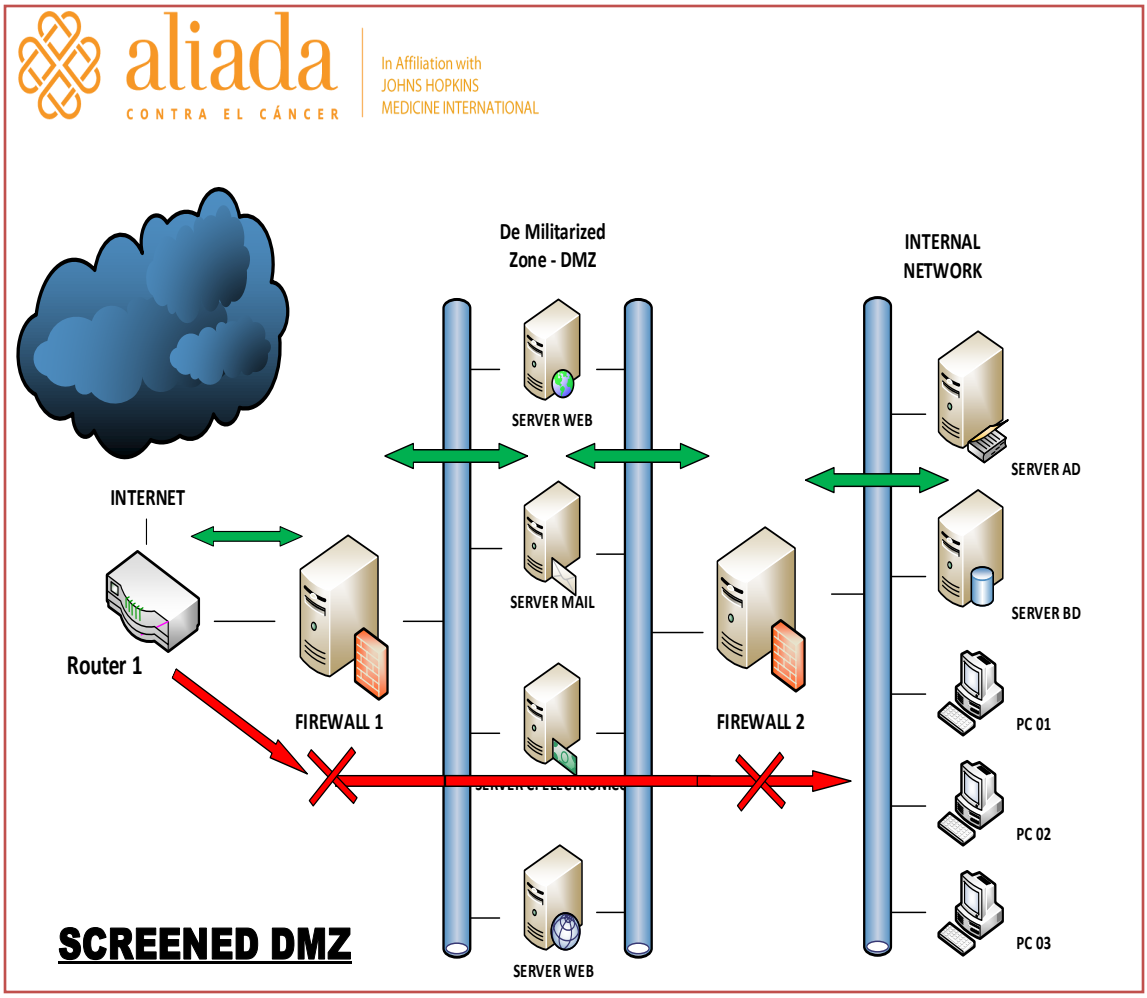


Figura 24: Firewall Screened Dmz
Elaborado: Por los autores

2.3.13. SISTEMA DE DETECCIÓN DE INTRUSOS - IDS

Un Sistema de Detección de Intrusos (IDS) es un programa utilizado para distinguir el acceso no aprobado a una PC o sistema. Estos ataques pueden ser atacados por programadores que utilizan aparatos programados.

El IDS en su mayoría tiene sensores virtuales (por ejemplo, un rastreador de sistema) con los cuales el centro IDS puede obtener información externa (como regla sobre el movimiento de arreglos). El IDS reconoce, a causa de estos sensores, rarezas que pueden mostrar la cercanía de asaltos o precauciones falsas.

Funcionamiento de la IDS

La tarea de estos dispositivos depende del examen punto por punto de la actividad del sistema, que después de entrar en el analizador se contrasta y las marcas de asaltos conocidos o conducta sospechosa, por ejemplo, filtrado de puertos, paquetes contorsionados, etc. El IDS no solo examina qué tipo de movimiento es, sino que además examina la sustancia y su conducta.

Por lo general, este dispositivo se incorpora con un firewall. El buscador de interrupciones no puede detener los ataques sin nadie más, aparte de los que colaboran en un dispositivo de paso con utilidad de cortafuegos, convirtiéndolo en un dispositivo intenso ya que une el conocimiento de IDS y la intensidad de bloqueo del cortafuegos, donde los paquetes deberían pasar esencialmente. y puede ser obstaculizado antes de ingresar al sistema.

El IDS en su mayor parte tiene una base de datos de "marcas" de asaltos conocidos. Estas marcas permiten al IDS reconocer la utilización ordinaria de la PC y el uso engañoso, y / o entre el movimiento típico del sistema y la actividad que puede producirse debido a un ataque o empeño de la misma.

2.3.14. Redes Privadas Virtuales - VPN

La Red Privada Virtual (RPV), Virtual Private Network (VPN), es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada, como por ejemplo Internet.

Las VPNs se utilizan para crear redes seguras a través de redes públicas (y por tanto inseguras) como Internet. Este mecanismo permite conectar puntos remotos con un coste bajo y con un protocolo que garantiza la confidencialidad de la información.

Para hacerlo posible de manera segura es necesario proporcionar los medios para garantizar la autenticación, integridad y confidencialidad de toda la comunicación:

- Autenticación y autorización: Usuario/equipo y qué nivel de acceso debe tener.
- Integridad: La garantía de que los datos enviados no han sido alterados. Para ello se utiliza funciones de Hash. Los algoritmos de hash más comunes son los Message Digest (MD2 y MD5) y el Secure Hash Algorithm (SHA).
- Confidencialidad: Dado que los datos viajan a través de un medio potencialmente hostil como Internet, los mismos son susceptibles de intercepción, por lo que es fundamental el cifrado de los mismos. De este modo, la información no debe poder ser interpretada por nadie más que los destinatarios de la misma. Se hace uso de algoritmos de cifrado como Data Encryption Standard (DES), Triple DES (3DES) y Advanced Encryption Standard (AES).

2.3.15. Tipos de VPN: VPN de Acceso

Es tal vez el modelo más utilizado en la actualidad y se compone de clientes o proveedores que se asocian con la organización desde destinos remotos (lugares de trabajo de negocios, hogares, alojamientos, aviones arreglados, etc.) utilizando Internet como interfaz de entrada. Una vez verificado, tienen un nivel de entrada fundamentalmente el mismo que tienen en el sistema cercano de la organización. Numerosas organizaciones han suplantado su base de acceso telefónico (módems y líneas telefónicas) con esta innovación.

Tipos de VPN: VPN Punto a Punto

Este plan se utiliza para asociar lugares de trabajo remotos con el campamento base de la asociación. El servidor VPN, que tiene una conexión sin cambios a Internet, reconoce las asociaciones de Internet de los destinos y configura la madriguera VPN. Los servidores de las sucursales se asocian con Internet utilizando las administraciones de su proveedor de Internet vecinal, normalmente a través de asociaciones de banda ancha. Esto hace que sea concebible prescindir de las uniones consuetudinarias exorbitantes de punto a punto, particularmente en las correspondencias mundiales. El punto pasado es más típico, también llamado innovación de excavación o tecnología de túnel.

Tunelling

Internet se trabajó desde el primer punto de partida como un medio poco confiable. Una gran parte de las convenciones utilizadas hoy en día para intercambiar información comenzando con una máquina y luego con la siguiente a través del sistema no tienen algún tipo de cifrado o seguridad que impida que nuestros intercambios sean capturados y vigilados. HTTP, FTP, POP3 y muchas otras convenciones generalmente utilizadas, utilizan correspondencias que se mueven en claro sobre el sistema. Este es un problema importante, en todas las circunstancias en las que necesitamos intercambiar datos delicados entre máquinas, por ejemplo, una cuenta de cliente (nombre de usuario y clave secreta), y no tenemos un control absoluto sobre el sistema, para evitar que alguien podemos capturar nuestra correspondencia a través de la estrategia del

hombre en el centro (hombre en el centro), similar a la instancia del sistema de sistemas.

El problema con las convenciones que envían su información clara, es decir, sin codificar, es que cualquier persona que tenga acceso físico al sistema en el que se encuentran las máquinas puede ver dicha información. En esta línea, alguien que asocia su máquina a un sistema y utiliza un rastreador obtendrá y tendrá la capacidad de investigar cada uno de los paquetes que atraviesan este sistema. En el caso de que alguno de esos paquetes tenga un lugar con una convención que envíe sus correspondencias claras, y contenga datos delicados, esos datos estarán en peligro. En la posibilidad de que, en realidad, las correspondencias estén codificadas con un marco que permita que solo las dos máquinas que forman parte de la correspondencia sean comprendidas, cualquier individuo que atrape los paquetes de una tercera máquina no tendrá la capacidad de hacer algo con ellos, ya que no pueden decodificar la información.

Un enfoque para mantener una distancia estratégica de este problema, mientras que todavía se utilizan cada una de esas convenciones que requieren cifrado, es utilizar un procedimiento llamado madriguera. Fundamentalmente, este método comprende la apertura de asociaciones entre dos máquinas a través de una convención protegida, por ejemplo, SSH (Secure SHell), a través de la cual realizaremos intercambios riesgosos, que en consecuencia serán resguardados. De esta similitud viene el nombre del método, siendo la asociación segura (para esta situación ssh) el pasaje a través del cual se envía la información con el objetivo de que nadie más se separe de los interrogadores que están situados en cada final del pasaje, puede ver dicha información. Este tipo de estrategia requiere una cuenta de acceso seguro en la máquina con la que debe impartir.

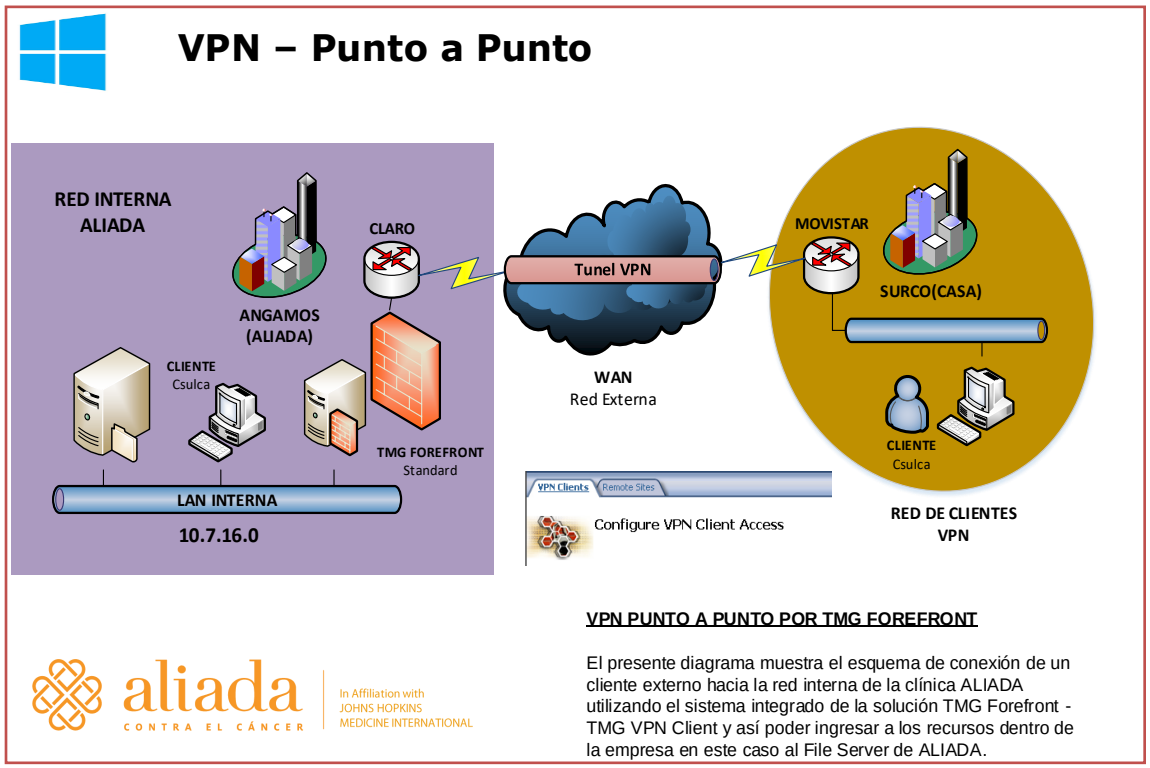


Figura 25: Vpn Punto a Punto
Elaborado: Por los autores

2.3.16. Network Address Translation - NAT

En las redes de computadoras NAT (Network Address Translation) es una técnica que permite trasladar el tráfico de una red a través de un router que reescribe la dirección IP destino y/o fuente y usualmente también el número de puerto TCP/UDP de los paquetes que traslada. Los checksums deben volver a realizarse para tomar en cuenta el cambio. Muchos sistemas que usan NAT lo hacen para habilitar múltiples hosts en una red para acceder a Internet a través de una dirección IP pública sencilla. Muchos administradores de red encuentran el uso de NAT muy conveniente. Sin embargo NAT puede provocar complicaciones en las comunicaciones y puede impactar el desempeño de la red. NAT se hizo popular como una forma de negociar con la escasez de direcciones IP. NAT se ha convertido en una característica estándar en routers para conexiones en casas

y pequeñas oficinas conectadas a Internet, donde el precio de direcciones IP extra podría ser más caro que los beneficios. NAT también es un valor añadido de seguridad ya que oculta la estructura interna de la red: Todo el tráfico proveniente de la red, aparece a terceras partes como originado de la maquina gateway.

En una configuración típica, una red local utiliza una subred con direcciones IP privadas y un router en la red tiene una dirección privada en la misma red. El router también es conectado a Internet con una dirección IP pública. Conforme pasa el tráfico de la red local a Internet, la dirección IP fuente en cada paquete es traducida al instante de la dirección IP privada a la dirección IP pública. El router registra datos básicos sobre cada conexión activa. Cuando regresa una respuesta al router, este usa el registro de datos que almacena durante la fase de envió para determinar a qué parte de la red interna reenviar la respuesta; los números de puerto de los clientes TCP/UDP son utilizados para demultiplexar los paquetes en el caso de una NAT sobrecargada, o la dirección IP y el número de puerto cuando múltiples direcciones están disponibles en el paquete devuelto. Para todo sistema en Internet, el router parece ser el origen y destino de todo el tráfico.

Se ha argumentado que la adopción de IPv6 hará el uso de NAT inútil, como método para manejar la escasez en el espacio de direcciones IP. Sin embargo este argumento ignora la naturaleza de firewall proveída por NAT o asume que los dispositivos utilizados en las redes siempre serán configurados de fábrica para bloquear solicitudes entrantes a los equipos.

Ventajas

Adicionalmente a la conveniencia y bajo costo de NAT, la carencia de una completa conectividad bidireccional puede ser considerada en algunas situaciones como una característica en lugar de una limitación. En gran parte NAT depende de una maquina en la red local para iniciar cualquier conexión con

equipos al otro lado del router, esto previene actividades maliciosas iniciadas desde maquinas externas intentando acceder equipos internos. Esto puede incrementar la confiabilidad de los sistemas locales deteniendo gusanos e incrementando la seguridad desalentando escaneos.

Muchos firewalls que habilitan el uso de NAT, la usan como parte principal de la protección que ofrecen. El mayor beneficio que ofrece NAT es que es una solución práctica para el inminente agotamiento del espacio de direcciones IP. Redes que antes requerían de un rango IP de clase B o un bloque de clase C pueden ahora conectarse a Internet con solo una dirección IP sencilla. La forma más común de organizar es tener equipos que requieren una real conectividad bidireccional e ilimitada con direcciones IP reales y por otro lado tener los equipos que no proveen servicios colocados detrás de la NAT con solo una dirección IP utilizada para habilitar el acceso a Internet.

Desventajas

Los clientes que se encuentran detrás de los routers que habilitan NAT no tienen una conexión real punto a punto y no pueden utilizar algunos protocolos de Internet. Servicios que requieren la inicialización de una conexión TCP desde una red externa, o protocolos como los que usan UDP pueden ser afectados. A menos que el router provea herramientas para soportar dichos protocolos, los paquetes entrantes no podrán alcanzar su destino. Algunos protocolos pueden acomodar una instancia de NAT entre los dispositivos que requieren la conectividad (por ejemplo, FTP en modo pasivo) algunas veces con la asistencia de un gateway de capa de aplicación, pero esto falla cuando ambos sistemas son separados de Internet mediante NAT. El uso de NAT también complica el uso de protocolos que utilizan tunelling como IPsec ya que NAT modifica los valores en las cabeceras lo que interfiere con el chequeo de integridad hecho por IPsec y otros protocolos de ese tipo.

La conectividad punto a punto ha sido el principio fundamental de Internet. Los documentos de la actual estructura de Internet, observan que NAT es una violación al principio de conectividad punto a punto, pero NAT tiene un papel valido con un diseño cuidadoso. Existen diversas opiniones acerca del uso de NAT con IPv6 y muchos diseñadores de IPv6 creen que IPv6 se creó con la intención de eliminar la necesidad de NAT. Algunos proveedores del servicio de Internet (ISP) solo proveen a sus consumidores con direcciones IP locales. De este modo, esos consumidores deben acceder a servicios externos a través de la red del proveedor mediante NAT. Como resultado, se argumenta que esas compañías no ofrecen un servicio apropiado de Internet.

NAT y TCP/UDP

NAT operado con IP solamente, puede o no puede correctamente permitir el paso de protocolos que están totalmente relacionados con la información IP, como ICMP dependiendo de si la información útil es interpretada por el equipo en la red interna o el equipo externo. Tan pronto como la pila de protocolo es rebasada, incluso con un protocolo básico como TCP ò UDP, el protocolo se romperá a menos que NAT tome las medidas detrás de la capa de red.

IP tiene una suma de comprobación en cada cabecera de los paquetes, que provee una detección de errores solo para la cabecera. Los datagramas IP pueden ser fragmentados y es necesario para NAT reensamblar dichos paquetes para permitir el correcto recalculo de la suma de comprobación (checksum) y corregir el registro de paquetes pertenecientes a una conexión.

Los protocolos de la capa de transporte, TCP y UDP, tienen una suma de comprobación que cubre todos los datos que ellos soportan, así como de las cabeceras TCP/UDP, más una pseudo cabecera, que tiene un cheksum que contiene las direcciones IP origen y destino del paquete que transporta la cabecera TCP/UDP. Para que NAT permita el paso exitoso de TCP ò UDP es necesario reconstruir la suma de comprobación de la cabecera TCP/UDP

basándose en las direcciones traducidas, no en las originales, y colocar dicha suma en la cabecera del primer paquete del fragmentado conjunto de paquetes. NAT debe recalcular la suma de comprobación IP en cada paquete que pase hacia el equipo destino, y también reconocer y recalcular la cabecera TCP/UDP utilizando las direcciones retraducidas y la pseudo cabecera. Esto no resuelve completamente el problema, NAT recibe paquetes los reensambla al segmento entero y lo recalcule, puesto que no puede hacer el recalculo sin el checksum de cada uno de los paquetes.

Aplicaciones afectadas por NAT

Algunos protocolos de las capas superiores (como FTP y SIP) envían información de la capa de red dentro de la información útil que utilizan. FTP en modo activo, por ejemplo, utiliza conexiones por separado para controlar el tráfico y para el tráfico de datos. Cuando solicita una transferencia de archivos, el equipo que solicita identifica la correspondiente conexión de datos por su dirección. Si el equipo que hace la solicitud se encuentra tras una NAT, la traducción de la dirección IP y los números de puerto, hacen la información recibida por el servidor inútil.

Un Gateway de capa de aplicación puede resolver el problema. Este Gateway, se ejecuta como modulo del firewall actualizando cualquier información hecha inválida por la traducción de direcciones. Este Gateway necesita entender el protocolo de alto nivel que necesita reparar, y cada protocolo con este problema requiere un Gateway o proxy diferente.

Otra solución posible para este problema es usar técnicas de NAT transversal utilizando protocolos como STUN o ICE. NAT transversal es posible en aplicaciones tanto TCP como UDP, pero el basado en UDP es más simple, más comprensible y más compatible con NAT. En cada caso, el protocolo de alto nivel debe ser diseñado con la NAT transversal en mente y esto no permite un trabajo confiable con NAT simétricas o con otras implementaciones.

Los protocolos cliente servidor más tradicionales, a excepción de FTP, no envían información de contacto de capa 3 y por lo tanto no requieren un uso especial por NAT. De hecho evitar complicaciones para NAT es prácticamente un requerimiento para el diseño de protocolos de capas superiores.

Diferentes tipos de NAT

Algunas aplicaciones que negocian con NAT algunas veces necesitan clasificar a NAT por su tipo. El protocolo STUN propone clasificar NAT como NAT cono completo, NAT cono restringido, NAT cono restringido por puerto y NAT simétrico.

- **NAT cono completo (Full cone NAT)**

  También es conocido como NAT uno a uno. Todos los puertos de las direcciones externas son mapeados a las direcciones internas específicas y al mismo puerto. Un equipo externo puede enviar un paquete arbitrario a la red interna enviando el paquete a la dirección externa mapeada.

- **NAT cono restringido (Restricted cone NAT)**

  Todas las solicitudes desde la misma dirección IP y puerto, son mapeadas a la misma IP externa y puerto. Un equipo externo puede enviar un paquete a un equipo interno solo si el equipo interno ha enviado un paquete previamente.

- **NAT cono restringido (Restricted cone NAT)**

  Algunas veces llamado NAT simétrico. Como el NAT de cono restringido, pero las restricciones incluyen el número de puertos. Un equipo externo envía un paquete a un equipo en particular dentro de

la red protegida por NAT, a un puerto en especial solo si el equipo interno ha enviado previamente un paquete desde ese puerto hacia el equipo externo.

- **NAT Simétrico (Symmetric NAT)**

  Cada solicitud desde la misma dirección IP interna y puerto hacia una dirección IP específica y puerto es mapeada a una única dirección IP destino y puerto. Si el mismo equipo interno envía un paquete hacia diferentes destinos pero con la misma dirección IP origen, un mapeo diferente es utilizado. Solo un equipo externo que ha recibido previamente un paquete desde la red interna puede reenviar paquetes.

2.3.17. LISTAS DE CONTROL DE ACCESO – ACL

Un destacado entre los elementos más fundamentales de un firewall es canalizar parcelas. La parte de filtrado de paquetes mira las direcciones IP (y además los puertos de E / S) del origen y el objetivo de cada parcela, mediante el análisis de su encabezado. A través de una progresión de estándares, llamada lista de control de entrada, el canal decide si reconocer o descartar paquetes IP singulares.

Los registros de acceso (ACL) se utilizan para la separación de paquetes según lo indicado por parámetros específicos, por ejemplo, direcciones de organización de origen u objetivo, puertos de origen o de objetivo, escritura de convención (ip, icmp, tcp, udp, etc.)). Una de las aplicaciones donde se utilizan más los registros es organizar la seguridad. Con las ACL puede cuadrar actividad indeseable en una interfaz ya sea de salida o de entrada. Sea como fuere, las ACL se utilizan como parte de problemas de seguridad, y también se utilizan para canalizar paquetes de reglas en aplicaciones tan diferentes como NAT (Traducción de direcciones de red), en BGP para canalizar cursos mientras se hacen enfoques de dirección, etc.

Hay ACL para varias pilas de convenciones: TCP / IP, IPX / SPX, Apple, etc. La distinción con las otras pilas de convenciones está en el alcance de las ACL que se pueden crear.

Características de las ACL

Para empezar, una ACL está conectada a una interfaz de entrada o de salida. Puede crear una ACL para la interfaz de rendimiento y otra alternativa para esa interfaz de información. En segundo lugar, las ACL son agrupaciones de direcciones que se comparan con el paquete. La solicitud de las instrucciones es crítica, a la luz del hecho de que cuando una línea del arreglo coincide con el cheque, se realiza un movimiento y deja el ACL, es decir, no se comprueba para confirmar que hay una línea diferente de la agrupación que también se produce de verdad.

- ✓ Una ACL es una lista de una o más instrucciones.
- ✓ Se asigna una lista a una o más interfaces.
- ✓ Cada instrucción permite o rechaza tráfico, usando uno o más de los siguientes criterios: el origen del tráfico; el destino del tráfico; el protocolo usado.
- ✓ Es por eso que hay que listar los comandos desde los casos más específicos, hasta los más generales. Las excepciones tienen que estar antes de la regla general.
- ✓ Si no se encuentra una coincidencia en ninguno de los renglones, rechaza automáticamente el tráfico. Debe considerarse que hay una regla que deniega todo implícitamente, al final de cada ACL.
- ✓ Cualquier línea agregada a una ACL se agrega al final. Para cualquier otro tipo de modificación, se tiene que borrar toda la lista y escribirse de nuevo.

- ✓ También se pueden usar ACL nombradas en vez de usar un rango de números.
- ✓ El darles un nombre facilita entender la configuración (y por lo tanto, también facilita hacer correcciones).
- ✓ Si consideramos sólo el tráfico de tipo TCP/IP, para cada interface puede haber sólo una ACL para tráfico entrante, y una ACL para tráfico saliente.
- ✓ Se deben conocer los rangos de números de las ACL, incluso para protocolos que normalmente no nos interesan.

Propósito de las ACL's

Las ACL permiten un control del tráfico de red, a nivel de los routers. Pueden ser parte de una solución de seguridad (junto con otros componentes, como antivirus, anti-espías, firewall, proxy, etc.).

Razones para crear ACL's

- ✓ Limitar el tráfico de red y mejorar el rendimiento de la red: Por ejemplo, restricción de video
- ✓ Brindar control de flujo de tráfico.
- ✓ Proporcionar nivel básico de seguridad para el acceso a la red.

Administración Básica del Tráfico IP

La prueba reconocible podría ser utilizada para canalizar el movimiento y lograr una mejor administración de la actividad mundial del sistema. Los registros de acceso son un aparato viable para controlar el sistema. Los registros de acceso agregan la adaptabilidad para canalizar la secuencia de paquetes que ingresan y salen de interfaces distintivas.

El filtrado de paquetes le permite controlar el desarrollo de estos dentro del sistema. Una lista de acceso IP es un resumen sucesivo de las condiciones de permiso o prohibición que se aplican a las direcciones IP o las convenciones IP

de capa superior. Los registros de entrada reconocen la actividad que debe ser tamizada. Los registros de acceso también se pueden conectar a los puertos de las líneas terminales virtuales para permitir y denegar la actividad entrante o saliente.

Los registros de direcciones IP pueden utilizarse para generar un mejor control o tiempo para aislar la actividad en varias necesidades y líneas personalizadas. En el momento en que un paquete toca la base en una interfaz, si no hay curso en la dirección del objetivo, el paquete se desecha, generalmente el paquete puede enviarse al colchón de rendimiento.
En caso de que el paquete de rendimiento esté ligado a un puerto, que no se haya reunido para obtener un rendimiento, la lista se enviará directamente al puerto planificado. En caso de que el paquete de rendimiento esté vinculado a un puerto, se haya reunido en una lista de acceso activo, antes de que el paquete pueda enviarse al puerto planificado, se confirmará mediante una progresión de instrucciones desde la lista de acceso relacionada con esa interfaz.

Prueba de las Condiciones de ACL's

Las pautas en una lista de entrada funcionan en una solicitud coherente sucesiva. Evaluar paquetes de principio a fin, dirección a la guía. En caso de que el encabezado de un paquete coincida con una guía en la lista de entrada, se omitirá lo que quede de las instrucciones en el resumen, y el paquete será permitido o denegado según lo indicado en la guía hábil. En caso de que el encabezado de un paquete no coordine una dirección en la lista de entrada, la prueba continúa con la siguiente guía en el resumen.

El procedimiento de correlación continúa hasta el punto en que alcanza el final del resumen, cuando el paquete será denegado verificable. Una vez que ocurre una coincidencia, se conecta la alternativa de consentimiento o desautorización y finaliza la prueba de ese paquete. Esto implica una condición que niega que un paquete en una línea guía no pueda ajustarse en otra dirección subsiguiente.

Las ramificaciones de este método de conducta es que la solicitud en la cual aparecen las pautas en la lista de entrada es fundamental. Hay una última directriz que se aplica a todos los paquetes que no pasaron por ninguna de las pruebas anteriores.

Esta última condición se aplica a cada uno de esos paquetes y los resultados en un estado de desacuerdo del paquete. En lugar de salir por una interfaz, todos los paquetes que no cumplen con las instrucciones en la lista de entrada se eliminan. Esta última dirección se conoce como la negativa cierta de todo, hacia el final de cada lista de entrada, debido a esta condición, es fundamental que en cada lista de entrada haya no menos de una directriz indulgente, generalmente la reducción de entrada dificultaría todo movimiento.

Aplicación de Listas de Acceso

Una vez definidos los criterios de filtrado de la lista de acceso, se deben aplicar a una o más interfaces para que se puedan filtrar los paquetes. La lista de acceso se puede aplicar en dirección entrante o saliente en la interfaz.

2.4. Acta de constitución

ACTA DE CONSTITUCIÓN DEL PROYECTO					
PROYECTO	IMPLEMENTACIÓN DE UN FIREWALL TMG FOREFRONT PARA LA SEGURIDAD PERIMETRAL DE LA RED DE DATOS DE LA CLÍNICA ALIADA				
PATROCINADOR	ROBERT CAÑARI - JEFE DE TI				
PREPARADO POR	CARLOS IVAN SULCA GALARZA	FECHA	29	10	16
REVISADO POR	ROBERT CAÑARI	FECHA	01	11	16
APROBADO POR	FRANCISCO FELIU	FECHA	01	11	16
BREVE DESCRIPCIÓN DEL PRODUCTO O SERVICIO DEL PROYECTO					

En este proyecto se implementara un Firewall TMG Forefront para la seguridad perimetral de la red de datos de la clínica Aliada, contaremos con equipos tecnológicos como servidores, con esto vamos a optimizar, gestionar, administrar y controlar la red interna y externa.

OBJETIVOS DEL PROYECTO

Objetivo General:
Implementar un Firewall TMG Forefront para la seguridad perimetral de la red de datos de la Clínica Aliada.
Objetivos Específicos:

- ❖ Implementar el firewall TMG Forefront para las políticas de seguridad en la red de datos de la Clínica Aliada.
- ❖ Implementar el firewall TMG Forefront para ataques de malware y spam en la red de datos de la Clínica Aliada.
- ❖ Implementar el firewall TMG Forefront y optimizar el ancho de banda para la red de datos de la Clínica Aliada.
- ❖ Implementar el firewall TMG Forefront y mejorar la calidad de los servicios de tecnologías de la información en la red de datos de la Clínica Aliada.

FACTORES CRÍTICOS DE ÉXITO DEL PROYECTO

- ✓ Financiamiento adecuado
- ✓ Madurez profesional del personal a cargo
- ✓ Contar con buena iluminación en el centro de cómputo.
- ✓ Contar con suficiente espacio de trabajo para los equipos proporcionados y medios.
- ✓ Contar con un sistema de pozo a tierra para salvaguardar los equipos.

REQUERIMIENTOS DE ALTO NIVEL

- Servidor HP Proliant ML11 GEN5
- Espacio en Gabinete para el Servidor HP
- Licencia TMG Forefront

EXTENSIÓN Y ALCANCE DEL PROYECTO

FASES DEL PROYECTO	PRINCIPALES ENTREGABLES
I. Gestión del Proyecto **-** Gestión de Integración del Proyecto - Gestión del Alcance del Proyecto - Gestión de Tiempo del Proyecto - Gestión de Costo del proyecto - Gestión de Comunicaciones del Proyecto. - Gestión de RR.HH del Proyecto - Gestión de Riesgos - Gestión de Calidad del Proyecto	**I. Gestión del Proyecto** - Acta de constitución - Registros de interesados - Cronograma de Gantt - Matriz de costos **II. Planificación** **-** Kick off del proyecto - Diagrama actual de la red. - Identificación de servidores de la clínica en producción.

- Gestión de Adquisiciones del Proyecto **II. Planificación** - Identificación. - Análisis **III. Diseño** - Seguridad. - Funcionalidad. - Facilidad. - Direccionamiento Ip. **IV. Implementación** - Instalación de servidor. - Instalación del Firewall TMG. **V. Operación** - Pruebas de protección. - Pruebas de administración. **VI. Optimización** - Administración y monitoreo de la red**.**	- Identificación de los equipos de comunicación. - Análisis de ancho de banda actual. **III. Diseño** - Documento de políticas de seguridad para el firewall. - Documento de direccionamiento ip de la red. - Diagrama propuesto de la red. **IV. Implementación** - Servidor preparado para producción. - Aplicación de políticas de seguridad. **V. Operación** - Checklist de pruebas. **VI. Optimización** - Reportes de los servicios.

INTERESADOS CLAVE

- Gerente General
- G. Operaciones
- G. Sistemas
- G. Finanzas
- G. Desarrollo y Marketing

RIESGOS DEL PROYECTO

I. Riesgos Naturales:
-Terremotos.
-Cambios climáticos.

II. Riesgos No Naturales:
-Retraso en la entrega de un avance del proyecto en determinada fecha.
-Perdida de personal clave.
-Cambios en las prioridades.
-Falta de proveedores confiables.
-Trabajos no programados.
-Corte del fluido eléctrico.

HITOS PRINCIPALES DEL PROYECTO

- ✓ Kick off del proyecto.
- ✓ Diagrama actual de la red.
- ✓ Identificación de los servicios de red de la Clínica Aliada.
- ✓ Identificación de los equipos de comunicación.
- ✓ Análisis del ancho de banda actual.
- ✓ Documento de políticas de seguridad del firewall.
- ✓ Documento de direccionamiento IP de la red.
- ✓ Diagrama propuesto de la red.
- ✓ Aplicación de políticas de seguridad.
- ✓ CheckList de pruebas.
- ✓ Reportes de los servicios.

PRESUPUESTO DEL PROYECTO
La Gerencia General financiará el proyecto al 100 %

Fecha de inicio prevista:	Fecha de fin prevista:	Duración en días:

AUTORIZACIONES:

Nombre: Renzo Castillo Palomino

Nombre: Miguel Domínguez Chávez

Nombre: Carlos Sulca Galarza

Cargo: Jefe del Proyecto

2.5. Registro de Interesados

Interesados Internos

Nombre	Rol	Requisitos	Expectativos	Posible Influencia	Clasificación	Fase de Intereses
Renzo Castillo Palomino	Analista de Diseño	Miembro del Proyecto	Utilizar la metodología Cisco, para implementar las buenas prácticas en el diseño de implementación del Firewall, realizara diversas propuestas de diseño después de levantar la información en la fase de planificación.	Realiza cambios en el diseño de la red. Realizara la documentación y diagramas con la información obtenida en cada entrevista, la cual será sometida a la aprobación del cliente.	A favor	Participa en el diseño de la implementación del firewall. Realiza los requerimientos que se van a necesitar, proporciona un análisis del diseño.
Miguel Domínguez Chávez	Analista Implementador	Miembro del Proyecto	Llevar a cabo la implementación del Firewall TMG Forefront 2010 con la información obtenida en la fase 1 y fase 2 del proyecto.	Revisar las políticas de seguridad proporcionada por el cliente, Realiza el CheckList para su desarrollo en la implementación la cual será verificada por el cliente.	A favor	Participa en la implementación del firewall tmg Forefront, aplica las políticas de seguridad, realiza pruebas de los servicios por internet, genera reportes y realiza el monitoreo del firewall.
Carlos Sulca Galarza	Jefe del Proyecto	Miembro del Proyecto	Supervisar y Monitorear todas las fases del proyecto.	Participa en todas las fases del proyecto.	A favor	Participa en todas las fases del proyecto.

Francisco Feliu	Director del Proyecto	Miembro del Proyecto	Monitorea el avance del proyecto	Participa en todo el proyecto	A favor	Participa en todas las reuniones y toma de decisiones del proyecto
Robert Cañarí	Jefe del Proyecto	Miembro del Proyecto	Supervisa todo el proyecto	Participa en todo el proyecto	A favor	Participa en todas las reuniones y toma decisiones del proyecto

Tabla 2: Interesados internos

Elaborado: Por los autores

Interesados Externos

Nombre	Rol	Requisitos	Expectativas	Posible Influencia	Clasificación	Fase de intereses
María Ruiz Fonseca	Encargado de cafetín	Pertenecer a la empresa	Gestiona los problemas y se encarga de la tienda.	Genera ventas y cobros en cajas	a favor	Participa en las ventas.
Rosa Sánchez Rivera	Cajera	Pertenecer a la empresa	Realiza los cobros de los servicios brindados.	Realiza los cobros de los servicios	a favor	Participa en los cobros de las ventas
Rosa del Pino	Analista de cobranzas	Pertenecer a la empresa	Realiza los cobros de las empresas.	Realiza los cobros de servicios.	a favor	Participa en cobros.
Dario Serna Lavalle	Encargado de Almacén	Pertenecer a la empresa	Abastece y controla las cantidades de productos	Realiza los registro de las nuevos productos e actualiza el stock	a favor	Registra y actualiza los nuevos productos.

Cesar Vilca Suarez	Ayudante de Almacén	Pertenecer a la empresa	Apoyar al encargado de Almacén	Apoya al encargado de almacén	a favor	Ayuda y apoya al encargado de almacén.
Enrique Quispe Villa	Facturador	Pertenecer a la empresa	Apoyar al supervisor de facturación	Apoyar al supervisor de facturación	a favor	Genera, lleva control de facturas.
Francisco Feliu	Gerente General	Pertenecer a la empresa.	Planear y desarrollar metas a corto y largo plazo, comunicación eficaz con autoridades de lima.	Coordinar con las oficinas administrativas para asegurar que los registros y los análisis se están ejecutando correctamente.	a favor	Administrar los elementos de ingresos y costos de la empresa.

Tabla 3: Interesados externos
Elaborado: Por los autores

2.6. Gestión de Alcance

Objetivo General

Implementar un Firewall TMG Forefront para la seguridad perimetral de la red de datos de la Clínica Aliada.

Objetivos Específicos:

- ✓ Implementar el firewall TMG Forefront para las políticas de seguridad en la red de datos de la Clínica Aliada.
- ✓ Implementar el firewall TMG Forefront para ataques de malware y spam en la red de datos de la Clínica Aliada.
- ✓ Implementar el firewall TMG Forefront y optimizar el ancho de banda para la red de datos de la Clínica Aliada.
- ✓ Implementar el firewall TMG Forefront y mejorar la calidad de los servicios de tecnologías de la información en la red de datos de la Clínica Aliada.

2.6.1. Enunciado del Alcance del Proyecto

El alcance del Proyecto es instalar el Firewall TMG Forefront 2010, aplicar las políticas de seguridad brindadas por el usuario, realizar las validaciones de los servicios internos de la Clínica Aliada y por último se brindara una semana de afinamiento y monitoreo de los servicios del Firewall.

2.7. Estructura de Desglose del Trabajo

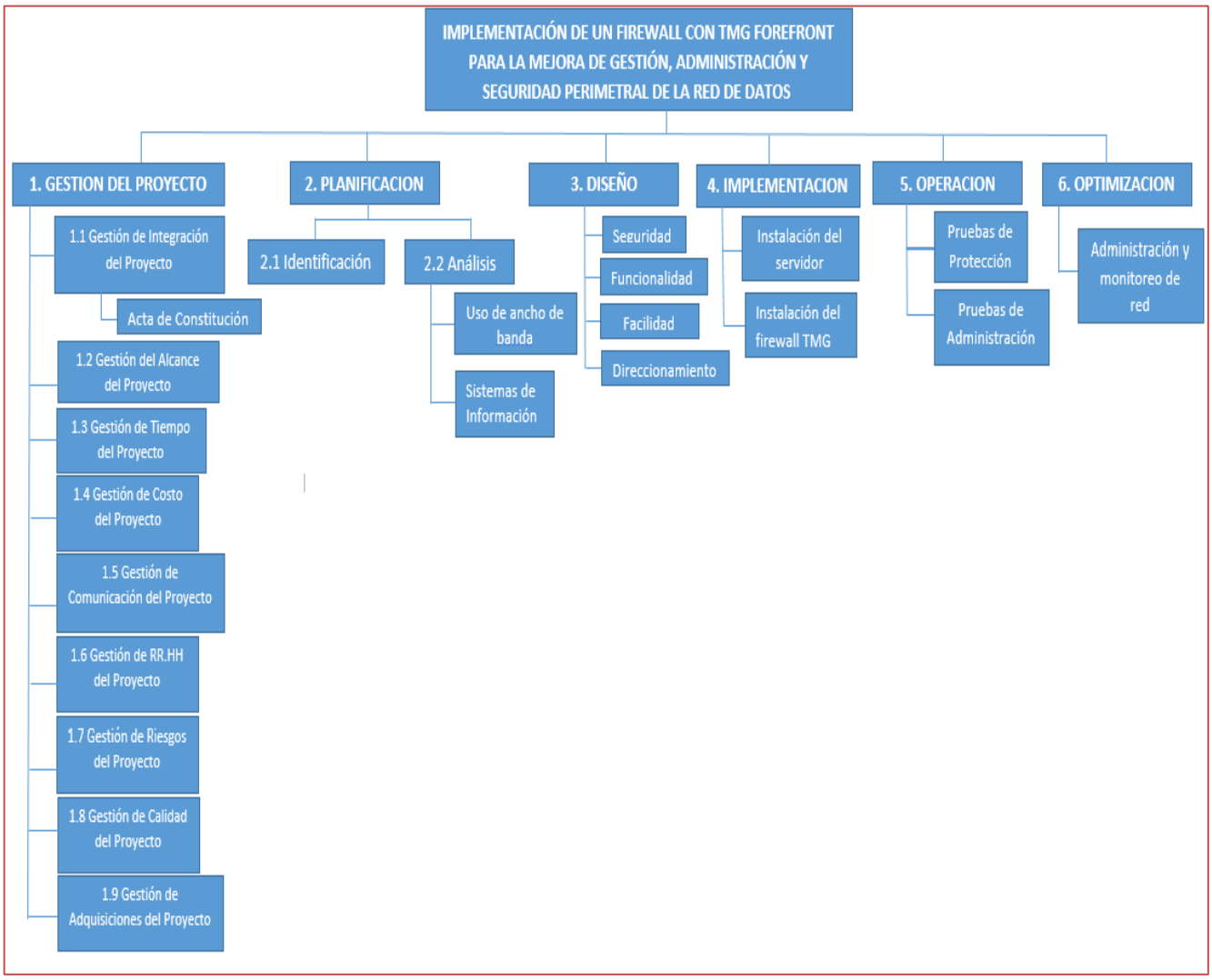


Figura 26: Estructura EDT
Elaborado: Por los autores

2.7.1. Diccionario de la EDT

DICCIONARIO EDT		
1.- Gestión del proyecto	**1.1 Gestión de Integración del Proyecto**	Desarrollar Acta de constitución del Proyecto. Desarrollar el Plan de gestión del Proyecto. Gestionar la ejecución del proyecto. Supervisar y controlar el trabajo del proyecto. Realizar el Control integrado de cambios. Cerrar proyecto o fase.
	1.2 Gestión del Alcance del Proyecto	Instalar el Firewall TMG Forefront 2010, aplicar las políticas de seguridad brindadas por el usuario, realizar las validaciones de los servicios internos de la Clínica Aliada y por último se brindara una semana de afinamiento y monitoreo de los servicios del Firewall.
	1.3 Gestión de Tiempo del Proyecto	**Razones aceptables para cambios en cronograma del Proyecto (por ejemplo, retrasos debido a entrega de materiales o disponibilidad de personal; clima; adelantar el cumplimiento debido a término de fase o proceso, etc.):** - Solicitud de cambio de alcance por parte del Cliente. - Desastres naturales. - Huelgas y revueltas populares. - Accidentes de trabajo. - Incumplimiento del proveedor en la entrega de materiales. - Mal establecimiento de la secuencia de actividades.
	1.5 Gestión de Comunicación del Proyecto	Determina las necesidades e informaciones y comunicación de los interesados: quién necesita qué información, para cuando la necesita, cómo le será suministrada y por quién. El Gerente del Proyecto debe considerar la cantidad de canales necesarios desde un principio con el fin de que la información fluya y llegue a todos los involucrados. Los requisitos de comunicación incluyen: - Organigramas. - Relaciones de responsabilidades de la organización. - Áreas profesionales, departamentos involucrados. - Logística de cuantas personas están involucradas. - Necesidades de información internas.

		- Necesidades de información externas. - Información sobre los interesados
	1.6 Gestión de RR.HH del Proyecto	"Las personas son nuestro activo más importante", lo dicen muchos ejecutivos de empresas. Las personas determinan el éxito o fracaso de las empresas y proyectos. Siempre hay necesidad de buenos trabajadores. Aprovechar de la mejor manera las personas involucradas en los proyectos. Antes de comunicarse con los demás, se debe buscar empatía - una relación de armonía, conformidad, acuerdo o afinidad. Pertenece al grupo del Proceso de Planificación.
	1.7 Gestión de Riesgos del Proyecto	**Alcances** - La identificación, priorización y seguimiento de riesgos más críticos será realizado por el Gerente de Proyectos asignado. - El proceso de Gestión de Riesgo debe ser definido e implantado por toda la clínica **Herramientas** - Opinión de la Alta Gerencia. - Opinión de la Gerencia General. - Tormenta de ideas. - Juicio de expertos entrevista. - CheckList riesgos potenciales. - Análisis de los supuestos identificados.
	1.8 Gestión de Calidad del Proyecto	El Plan de gestión de calidad describe cómo el equipo de dirección del proyecto implementará la política de calidad de la organización ejecutante. Es un componente o un plan subsidiario del plan para la dirección del proyecto. El plan de gestión de calidad proporciona entradas al plan general para la dirección del proyecto y aborda el control de calidad, el aseguramiento de la calidad y métodos de mejora continua de los procesos del proyecto. **Aseguramiento de Calidad.** Es responsable el Supervisor de Calidad ejecutar el Aseguramiento de Calidad durante todo el Proyecto, revisa el Planeamiento de los procesos del proyecto contra lo ejecutado, plantea acciones preventivas o correctivas según sean necesario. Se informa semanalmente en las

		reuniones de Calidad al Gerente del Proyecto y al Equipo del Proyecto.
	1.9 Gestión de Adquisiciones del Proyecto	Para este proyecto los responsables de realizar las labores de compra y contratación son: - El Gerente del Proyecto en la parte de subcontratos, es quien aprueba las subcontrataciones. - El Comprador logístico, quien ejecuta las compras y adquisiciones solicitadas por el Gerente del Proyecto.
2.- Planificación	**2.1 Identificación**	- Identificación de la topología de red. - Identificación de servidores y equipos de comunicaciones.
	2.2 Análisis	- Análisis del uso del ancho de banda de internet. - Análisis de los sistemas de información
3.- Diseño	**Seguridad** La red mantendrá la seguridad a nivel lógico con las políticas que se crearan en el firewall, reglas de acceso, lo cual aumentara la confidencialidad y disminuir la vulnerabilidad de los datos. **Funcionalidad** Con el levantamiento de información realizado, se identificó que la red funciona de manera óptima brindando facilidades para la implementación de Firewall TMG Forefront. **Facilidad** La implementación del firewall podrá brindarnos una administración centralizada ya que el firewall trabaja en sincronización con el directorio activo, permitiendo que las políticas aplicadas a un usuario lo mantendrá en cualquier equipo de la empresa. **Direccionamiento Ip** El direccionamiento ip del Cliente fue proporcionado por el jefe de sistemas, especificando que dicho esquema se mantendrá al 100%, a continuación mostramos el direccionamiento actual	

4.- Implementación	- Instalación del Servidor. - Instalación del Firewall TMG.
5.- Operación	Pruebas de protección. Pruebas de Administración.
6.Optimización	Administración y Monitoreo de red.

Tabla 4: Diccionario EDT
Elaborado: Por los autores

2.7.2. Entregable

Paquete de Trabajo	Id:	Entregable:	Descripción:
Identificación	1	Topología de red actual	Se visualiza la infraestructura de red actual del cliente, para su respectivo análisis pre implementación del firewall.
Seguridad	2	Políticas de Seguridad para el Firewall	El cliente define las políticas de seguridad que se aplicaran en el firewall.
Instalación del servidor	3	Servidor preparado para producción	Instalación y configuración del sistema operativo Windows server 2008 la cual alojara al firewall TMG.

Instalación del firewall TMG	4	Aplicación de políticas de seguridad	Instalación y configuración de Firewall TMG, en la cual se crearan las reglas de seguridad.
Pruebas de Protección	5	Checklist de Pruebas	Pruebas para verificar que todos los servicios de la clínica estén operando de manera correcta.

Tabla 5: Entregable
Elaborado: Por los autores

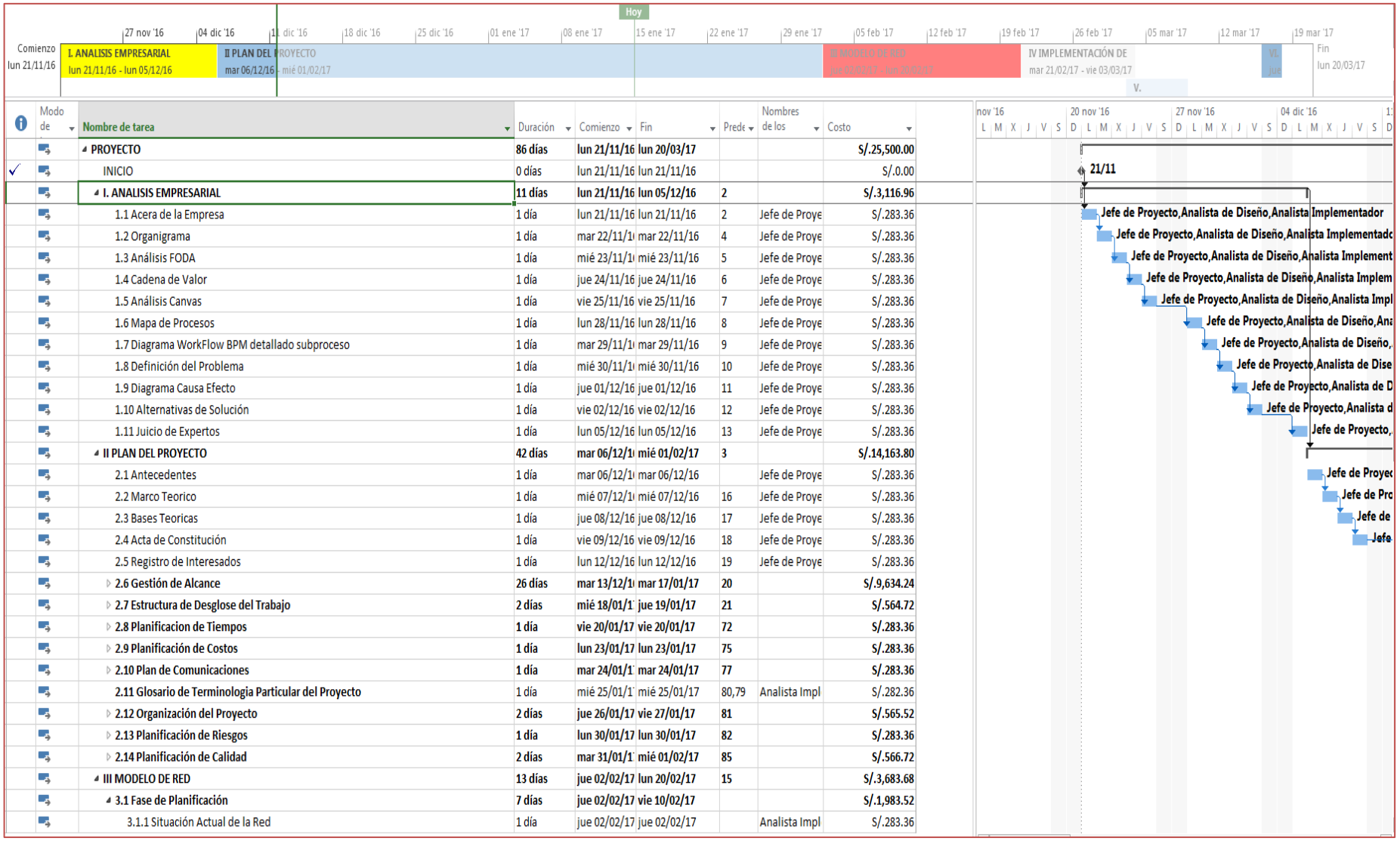
2.8. Planificación de Tiempos

Lista de Actividad

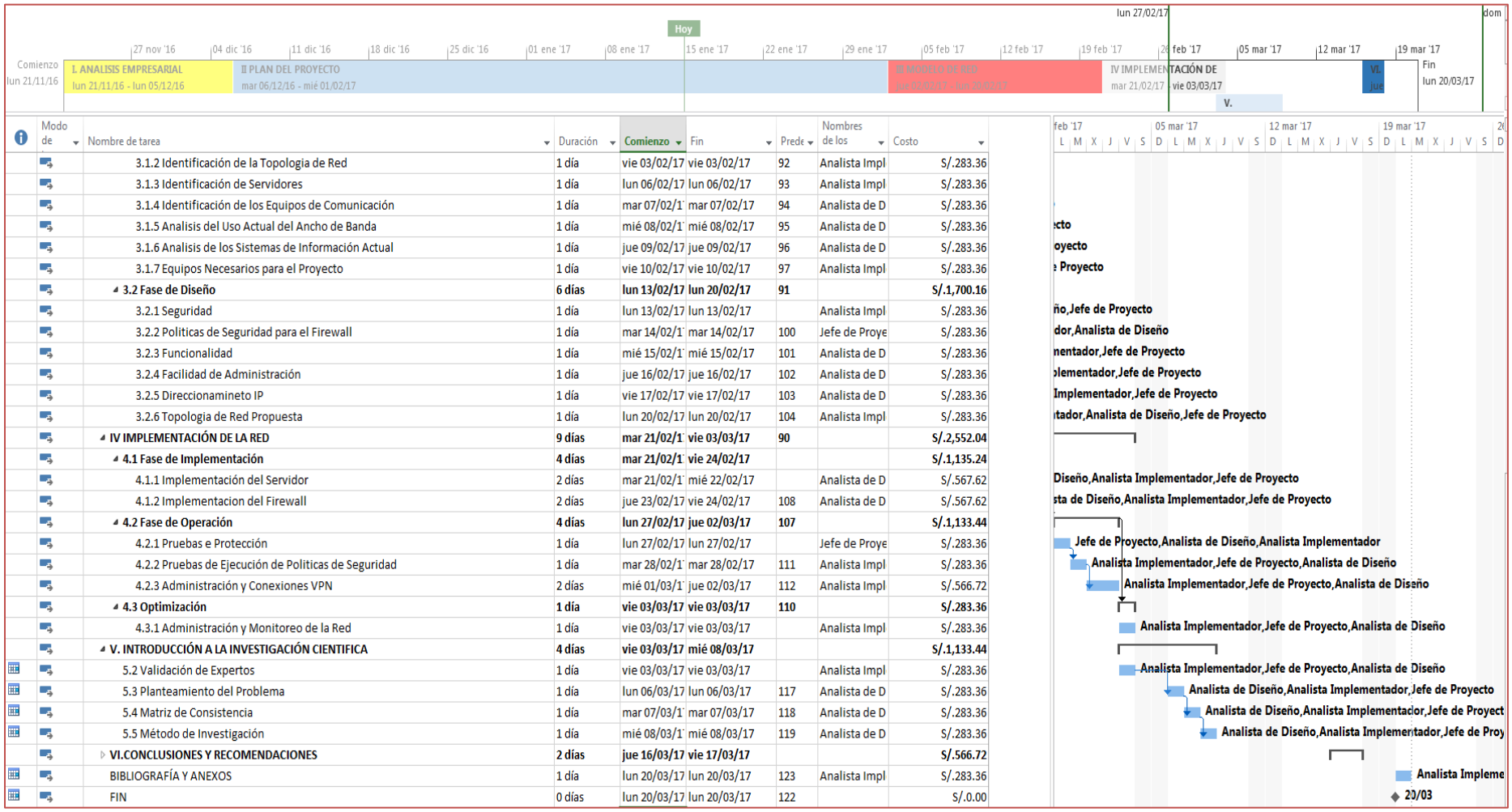
Cuenta de Control:	Inicio:	Fin:	Descripción:
Gestión del Proyecto	06/12/16	31/01/17	Actividad de gestión mientras dure el proyecto.
Planificación	01/02/17	09/02/17	9 días de levantamiento de información.
Diseño	10/02/17	17/02/17	7 días para realizar las propuestas de red.
Implementación	20/02/17	23/02/17	3 días para implementar el servidor y firewall.
Operación	24/02/17	28/02/17	4 días de pruebas de protección, políticas de seguridad, conexiones Vpn.
Optimización	01/03/17	01/03/17	1 día de monitoreo total de los servicios.

Tabla 6: Lista de Actividad
Elaborado: Por los autores

2.8.1. Cronograma (Diagrama de Gantt)



Modo de	Nombre de tarea	Duración	Comienzo	Fin	Prede	Nombres de los	Costo
	PROYECTO	**86 días**	**lun 21/11/16**	**lun 20/03/17**			**S/.25,500.00**
✓	INICIO	0 días	lun 21/11/16	lun 21/11/16			S/.0.00
	I. ANALISIS EMPRESARIAL	**11 días**	**lun 21/11/16**	**lun 05/12/16**	**2**		**S/.3,116.96**
	1.1 Acera de la Empresa	1 día	lun 21/11/16	lun 21/11/16	2	Jefe de Proye	S/.283.36
	1.2 Organigrama	1 día	mar 22/11/1	mar 22/11/16	4	Jefe de Proye	S/.283.36
	1.3 Análisis FODA	1 día	mié 23/11/1	mié 23/11/16	5	Jefe de Proye	S/.283.36
	1.4 Cadena de Valor	1 día	jue 24/11/16	jue 24/11/16	6	Jefe de Proye	S/.283.36
	1.5 Análisis Canvas	1 día	vie 25/11/16	vie 25/11/16	7	Jefe de Proye	S/.283.36
	1.6 Mapa de Procesos	1 día	lun 28/11/16	lun 28/11/16	8	Jefe de Proye	S/.283.36
	1.7 Diagrama WorkFlow BPM detallado subproceso	1 día	mar 29/11/1	mar 29/11/16	9	Jefe de Proye	S/.283.36
	1.8 Definición del Problema	1 día	mié 30/11/1	mié 30/11/16	10	Jefe de Proye	S/.283.36
	1.9 Diagrama Causa Efecto	1 día	jue 01/12/16	jue 01/12/16	11	Jefe de Proye	S/.283.36
	1.10 Alternativas de Solución	1 día	vie 02/12/16	vie 02/12/16	12	Jefe de Proye	S/.283.36
	1.11 Juicio de Expertos	1 día	lun 05/12/16	lun 05/12/16	13	Jefe de Proye	S/.283.36
	II PLAN DEL PROYECTO	**42 días**	**mar 06/12/1**	**mié 01/02/17**	**3**		**S/.14,163.80**
	2.1 Antecedentes	1 día	mar 06/12/1	mar 06/12/16		Jefe de Proye	S/.283.36
	2.2 Marco Teorico	1 día	mié 07/12/1	mié 07/12/16	16	Jefe de Proye	S/.283.36
	2.3 Bases Teoricas	1 día	jue 08/12/16	jue 08/12/16	17	Jefe de Proye	S/.283.36
	2.4 Acta de Constitución	1 día	vie 09/12/16	vie 09/12/16	18	Jefe de Proye	S/.283.36
	2.5 Registro de Interesados	1 día	lun 12/12/16	lun 12/12/16	19	Jefe de Proye	S/.283.36
	2.6 Gestión de Alcance	**26 días**	**mar 13/12/1**	**mar 17/01/17**	**20**		**S/.9,634.24**
	2.7 Estructura de Desglose del Trabajo	**2 días**	**mié 18/01/1**	**jue 19/01/17**	**21**		**S/.564.72**
	2.8 Planificacion de Tiempos	**1 día**	**vie 20/01/17**	**vie 20/01/17**	**72**		**S/.283.36**
	2.9 Planificación de Costos	**1 día**	**lun 23/01/17**	**lun 23/01/17**	**75**		**S/.283.36**
	2.10 Plan de Comunicaciones	**1 día**	**mar 24/01/1**	**mar 24/01/17**	**77**		**S/.283.36**
	2.11 Glosario de Terminologia Particular del Proyecto	1 día	mié 25/01/1	mié 25/01/17	80,79	Analista Impl	S/.282.36
	2.12 Organización del Proyecto	**2 días**	**jue 26/01/17**	**vie 27/01/17**	**81**		**S/.565.52**
	2.13 Planificación de Riesgos	**1 día**	**lun 30/01/17**	**lun 30/01/17**	**82**		**S/.283.36**
	2.14 Planificación de Calidad	**2 días**	**mar 31/01/1**	**mié 01/02/17**	**85**		**S/.566.72**
	III MODELO DE RED	**13 días**	**jue 02/02/17**	**lun 20/02/17**	**15**		**S/.3,683.68**
	3.1 Fase de Planificación	**7 días**	**jue 02/02/17**	**vie 10/02/17**			**S/.1,983.52**
	3.1.1 Situación Actual de la Red	1 día	jue 02/02/17	jue 02/02/17		Analista Impl	S/.283.36



Modo de	Nombre de tarea	Duración	Comienzo	Fin	Prede	Nombres de los	Costo
	3.1.2 Identificación de la Topologia de Red	1 día	vie 03/02/17	vie 03/02/17	92	Analista Impl	S/.283.36
	3.1.3 Identificación de Servidores	1 día	lun 06/02/17	lun 06/02/17	93	Analista Impl	S/.283.36
	3.1.4 Identificación de los Equipos de Comunicación	1 día	mar 07/02/1	mar 07/02/17	94	Analista de D	S/.283.36
	3.1.5 Analisis del Uso Actual del Ancho de Banda	1 día	mié 08/02/1	mié 08/02/17	95	Analista de D	S/.283.36
	3.1.6 Analisis de los Sistemas de Información Actual	1 día	jue 09/02/17	jue 09/02/17	96	Analista de D	S/.283.36
	3.1.7 Equipos Necesarios para el Proyecto	1 día	vie 10/02/17	vie 10/02/17	97	Analista Impl	S/.283.36
	3.2 Fase de Diseño	**6 días**	**lun 13/02/17**	**lun 20/02/17**	**91**		**S/.1,700.16**
	3.2.1 Seguridad	1 día	lun 13/02/17	lun 13/02/17		Analista Impl	S/.283.36
	3.2.2 Politicas de Seguridad para el Firewall	1 día	mar 14/02/1	mar 14/02/17	100	Jefe de Proye	S/.283.36
	3.2.3 Funcionalidad	1 día	mié 15/02/1	mié 15/02/17	101	Analista de D	S/.283.36
	3.2.4 Facilidad de Administración	1 día	jue 16/02/17	jue 16/02/17	102	Analista de D	S/.283.36
	3.2.5 Direccionamineto IP	1 día	vie 17/02/17	vie 17/02/17	103	Analista de D	S/.283.36
	3.2.6 Topologia de Red Propuesta	1 día	lun 20/02/17	lun 20/02/17	104	Analista Impl	S/.283.36
	IV IMPLEMENTACIÓN DE LA RED	**9 días**	**mar 21/02/1**	**vie 03/03/17**	**90**		**S/.2,552.04**
	4.1 Fase de Implementación	**4 días**	**mar 21/02/1**	**vie 24/02/17**			**S/.1,135.24**
	4.1.1 Implementación del Servidor	2 días	mar 21/02/1	mié 22/02/17		Analista de D	S/.567.62
	4.1.2 Implementacion del Firewall	2 días	jue 23/02/17	vie 24/02/17	108	Analista de D	S/.567.62
	4.2 Fase de Operación	**4 días**	**lun 27/02/17**	**jue 02/03/17**	**107**		**S/.1,133.44**
	4.2.1 Pruebas e Protección	1 día	lun 27/02/17	lun 27/02/17		Jefe de Proye	S/.283.36
	4.2.2 Pruebas de Ejecución de Politicas de Seguridad	1 día	mar 28/02/1	mar 28/02/17	111	Analista Impl	S/.283.36
	4.2.3 Administración y Conexiones VPN	2 días	mié 01/03/1	jue 02/03/17	112	Analista Impl	S/.566.72
	4.3 Optimización	**1 día**	**vie 03/03/17**	**vie 03/03/17**	**110**		**S/.283.36**
	4.3.1 Administración y Monitoreo de la Red	1 día	vie 03/03/17	vie 03/03/17		Analista Impl	S/.283.36
	V. INTRODUCCIÓN A LA INVESTIGACIÓN CIENTIFICA	**4 días**	**vie 03/03/17**	**mié 08/03/17**			**S/.1,133.44**
	5.2 Validación de Expertos	1 día	vie 03/03/17	vie 03/03/17		Analista Impl	S/.283.36
	5.3 Planteamiento del Problema	1 día	lun 06/03/17	lun 06/03/17	117	Analista de D	S/.283.36
	5.4 Matriz de Consistencia	1 día	mar 07/03/1	mar 07/03/17	118	Analista de D	S/.283.36
	5.5 Método de Investigación	1 día	mié 08/03/1	mié 08/03/17	119	Analista de D	S/.283.36
	VI.CONCLUSIONES Y RECOMENDACIONES	**2 días**	**jue 16/03/17**	**vie 17/03/17**			**S/.566.72**
	BIBLIOGRAFÍA Y ANEXOS	1 día	lun 20/03/17	lun 20/03/17	123	Analista Impl	S/.283.36
	FIN	0 días	lun 20/03/17	lun 20/03/17	122		S/.0.00

Figura 27: Cronograma
Elaborado: Por los autores

2.9. Planificación de Costos

2.9.1. Matriz de Costos

	2016		Total 2016	2017			Total 2017	Total general
Etiquetas de fila	Noviembre	Diciembre		Enero	Febrero	Marzo		
Proyecto 28-11-2016	2266.88	8500.8	10767.68	6229.72	5669	2833.6	14732.32	25500
Proyecto 28-11-2016	0	0	0	0	0	0	0	0
PROYECTO	2266.88	8500.8	10767.68	6229.72	5669	2833.6	14732.32	25500
PROYECTO	0	0	0	0	0	0	0	0
INICIO	0	0	0	0	0	0	0	0
I. ANALISIS EMPRESARIAL	2266.88	850.08	3116.96	0	0	0	0	3116.96
I. ANALISIS EMPRESARIAL	0	0	0	0	0	0	0	0
1.1 Acera de la Empresa	283.36	0	283.36	0	0	0	0	283.36
1.2 Organigrama	283.36	0	283.36	0	0	0	0	283.36
1.3 Análisis FODA	283.36	0	283.36	0	0	0	0	283.36
1.4 Cadena de Valor	283.36	0	283.36	0	0	0	0	283.36
1.5 Análisis Canvas	283.36	0	283.36	0	0	0	0	283.36
1.6 Mapa de Procesos	283.36	0	283.36	0	0	0	0	283.36
1.7 Diagrama WorkFlow BPM detallado subproceso	283.36	0	283.36	0	0	0	0	283.36
1.8 Definición del Problema	283.36	0	283.36	0	0	0	0	283.36
1.9 Diagrama Causa Efecto	0	283.36	283.36	0	0	0	0	283.36
1.10 Alternativas de Solución	0	283.36	283.36	0	0	0	0	283.36
1.11 Juicio de Expertos	0	283.36	283.36	0	0	0	0	283.36
II PLAN DEL PROYECTO	0	7650.72	7650.72	6229.72	283.36	0	6513.08	14163.8
II PLAN DEL PROYECTO	0	0	0	0	0	0	0	0
2.1 Antecedentes	0	283.36	283.36	0	0	0	0	283.36
2.2 Marco Teórico	0	283.36	283.36	0	0	0	0	283.36
2.3 Bases Teóricas	0	283.36	283.36	0	0	0	0	283.36

2.4 Acta de Constitución	0	283.36	283.36	0	0	0	0	283.36
2.5 Registro de Interesados	0	283.36	283.36	0	0	0	0	283.36
2.6 Gestión de Alcance	0	6233.92	6233.92	3400.32	0	0	3400.32	9634.24
2.7 Estructura de Desglose del Trabajo	0	0	0	564.72	0	0	564.72	564.72
2.8 Planificación de Tiempos	0	0	0	283.36	0	0	283.36	283.36
2.9 Planificación de Costos	0	0	0	283.36	0	0	283.36	283.36
2.10 Plan de Comunicaciones	0	0	0	283.36	0	0	283.36	283.36
2.11 Glosario de Terminología Particular del Proyecto	0	0	0	282.36	0	0	282.36	282.36
2.12 Organización del Proyecto	0	0	0	565.52	0	0	565.52	565.52
2.13 Planificación de Riesgos	0	0	0	283.36	0	0	283.36	283.36
2.14 Planificación de Calidad	0	0	0	283.36	283.36	0	566.72	566.72
III MODELO DE RED	0	0	0	0	3683.68	0	3683.68	3683.68
III MODELO DE RED	0	0	0	0	0	0	0	0
3.1 Fase de Planificación	0	0	0	0	1983.52	0	1983.52	1983.52
3.2 Fase de Diseño	0	0	0	0	1700.16	0	1700.16	1700.16
IV IMPLEMENTACIÓN DE LA RED	0	0	0	0	1701.96	850.08	2552.04	2552.04
IV IMPLEMENTACIÓN DE LA RED	0	0	0	0	0	0	0	0
4.1 Fase de Implementación	0	0	0	0	1135.24	0	1135.24	1135.24
4.2 Fase de Operación	0	0	0	0	566.72	566.72	1133.44	1133.44
4.3 Optimización	0	0	0	0	0	283.36	283.36	283.36
V. INTRODUCCIÓN A LA INVESTIGACIÓN CIENTIFICA	0	0	0	0	0	1133.44	1133.44	1133.44
V. INTRODUCCIÓN A LA INVESTIGACIÓN CIENTIFICA	0	0	0	0	0	0	0	0
5.2 Validación de Expertos	0	0	0	0	0	283.36	283.36	283.36
5.3 Planteamiento del Problema	0	0	0	0	0	283.36	283.36	283.36
5.4 Matriz de Consistencia	0	0	0	0	0	283.36	283.36	283.36
5.5 Método de Investigación	0	0	0	0	0	283.36	283.36	283.36
VI.CONCLUSIONES Y RECOMENDACIONES	0	0	0	0	0	566.72	566.72	566.72
VI.CONCLUSIONES Y RECOMENDACIONES	0	0	0	0	0	0	0	0
6.1 Conclusiones	0	0	0	0	0	283.36	283.36	283.36

6.2 Recomendaciones	0	0	0	0	0	283.36	283.36	283.36
BIBLIOGRAFÍA Y ANEXOS	0	0	0	0	0	283.36	283.36	283.36
FIN	0	0	0	0	0	0	0	0
Total general	2266.88	8500.8	10767.68	6229.72	5669	2833.6	14732.32	25500

Tabla 7: Matriz de Costos
Elaborado: Por los autores

2.10. Plan de Comunicaciones

2.10.1. Plan de Comunicación del Proyecto

Rol	Evento	Entregable	Descripción	Método	Frecuencia	Emisor	Receptor
1	Planificación y Diseño	Diagrama actual de la red/Diagramas propuestos/Políticas de seguridad	Proporciona información detallada de la red actual del cliente/Generas dos propuestas de red para la implementación/Obtiene las políticas de seguridad brindadas por el cliente	Presentación documentada de todos sus avances	Semanal	Renzo Castillo Palomino	Carlos Sulca Galarza

2	Implementación - Operación y Optimización	Implementación del servidor/ Implementación del firewall/Pruebas /Administración de conexiones VPN	Representa el objetivo principal de la solución brindada	Videoconferencias/Correo electrónico/Presentación documentada	Diario	Miguel Domínguez Chávez	Carlos Sulca Galarza
3	Planificación - Diseño - Implementación - Operación- Optimización	Administración y monitoreo de la red	Proporciona una vista detallada de todos los beneficios brindados por la solución implementada	Presentación documentada de los avances del proyecto	Quincenal	Carlos Sulca Galarza	Sponsor Francisco Feliu/Sponsor Robert Canarí

Tabla 8: Plan de Comunicación del Proyecto
Elaborado: Por los autores

2.11. Glosario de Terminología particular del proyecto

VPN

- ✓ Red privada virtual

ACL

- ✓ Lista de accesos con reglas de entrada y salida.

NAT

- ✓ Traducción de direcciones de red.

Router

- ✓ Equipo de comunicación que tiene como función principal enrutar paquetes por la ruta más corta.

Switch

- ✓ Dispositivo de que sirve para conectar varios elementos dentro de una red. Estas pueden ser una PC, una impresora, etc.

Switch Core

- ✓ Estos switch proveen de alta velocidad hacia tu centro de datos o puerto wan, es el cerebro de toda red switchada.

Firewall

- ✓ Hardware o software que permite controlar el acceso hacia una red o computadora por motivos de seguridad informática.

OSI

- ✓ Modelo de interconexión de sistemas abiertos, es un modelo de referencia para los protocolos de la red de arquitectura en capas, creado en el año de 1980.

UDP

- ✓ Protocolo de datagrama de usuario, es un protocolo mínimo de nivel de transporte orientado a mensajes de documento.

TCP

- ✓ Protocolo de control de transmisión, es uno de los principales protocolos de la capa de transporte del modelo TCP/IP.

Infraestructura de red

- ✓ Son todos los elementos básicos e imprescindibles para cualquier institución, las cuales brindan el soporte a todos los servicios de la empresa.

Seguridad Perimetral

- ✓ La seguridad e integridad informática de una empresa es primordial. Los ataques por red y pérdidas de información ocasionan un gran trastornó y no solo la imagen si no también el funcionamiento y progreso de una empresa se ven afectados.

Bastion Host

- ✓ Es una aplicación que se localiza en un servidor con el fin de ofrecer seguridad a la red interna, por lo que ha sido especialmente configurado para la recepción de ataques, generalmente provee un solo servicio.

Servidor Proxy

- ✓ Es un servidor, programa que hace de intermediario en las peticiones de recursos que realiza un cliente A a otro servidor C.

ISP

- ✓ El proveedor de servicios de internet, es una empresa que brinda conexión a internet a su cliente.

2.12. Organigrama del Proyecto

2.12.1. Organigrama

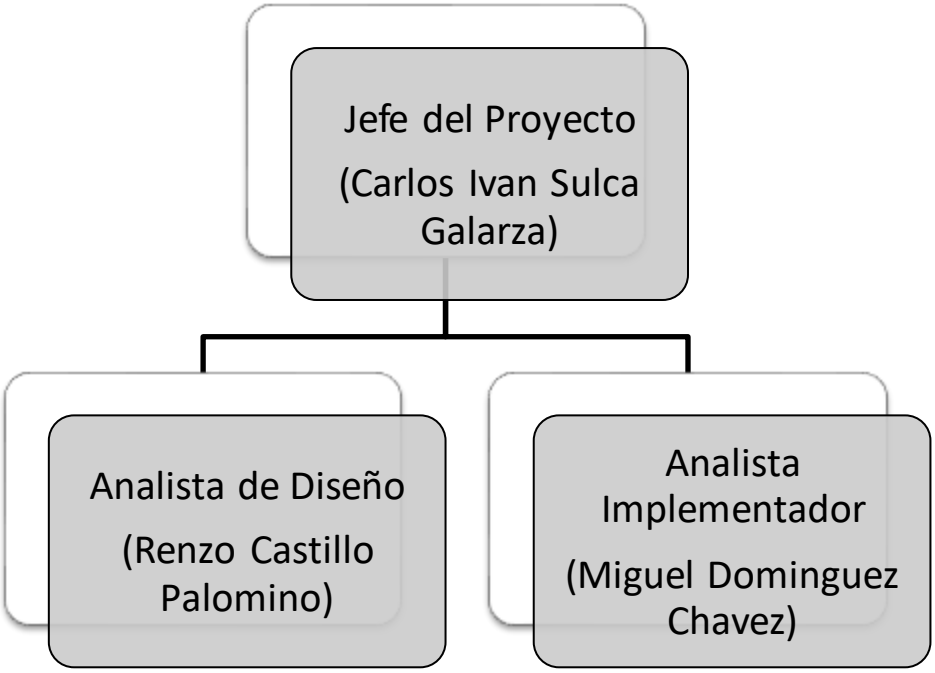


Figura 28: Organigrama del Proyecto
Elaborado: Por los autores

2.12.2. Matriz de Asignación de Responsabilidades

Rol	Responsabilidades	Participación en el proyecto	Nombres y Apellidos
Analista de diseño	Recolectar información de la red actual, identificación de los servidores, equipos de comunicación y sistemas de información, revisión de las políticas de seguridad, elaboración de las propuestas de red.	Participa en la fase de planificación y diseño	Renzo Castillo Palomino
Analista implementador	Implementa el sistema operativo Windows server 2008, implementa el Firewall aplicando las políticas se seguridad brindadas por el usuario, realiza las pruebas del checkList, realizara el monitoreo de los servicios generando reportes.	Participa en la fase de Implementación , operación y optimización	Miguel Domínguez Chávez
Jefe de proyecto	Supervisa y monitorea todos los avances del proyecto	Participa en todas las fases	Carlos Sulca Galarza

Tabla 9: Matriz de Asignación de Responsabilidades
Elaborado: Por los autores

2.13. Planificación de Riesgos

2.13.1. Registro de Riesgos del proyecto

Descripción	Consecuencias	Prob.	Impac.	Severidad	Estrategia de respuesta	Responsable del riesgo	Costo del Riesgo
No alcanzar los objetivos del proyecto debido a una mala definición del alcance	Rechazo de los entregables del proyecto	Bajo	Alto	0.70	Mitigar	Jefe del Proyecto	Por Definir
Retraso en la implementación de la solución debido a falta de experiencia	Demora en el desarrollo de la solución	Medio	Alto	0.50	Mitigar	Jefe del Proyecto	Por Definir
Cambio en algún equipo de comunicación	Retraso en la implementación de la solución por analizar sus especificaciones del nuevo equipo	Medio	Alto	0.70	Mitigar	Jefe del Proyecto(Cliente)	Por Definir
Corte del fluido Eléctrico	Retraso en los trabajos de desarrollo de documentación como entregables.	Medio	Alto	0.70	Mitigar	Jefe del Proyecto(Cliente)	Por Definir
Problemas en la fuente de alimentación del servidor	Retrasos en la implementación del firewall	Bajo	Alto	0.50	Mitigar	Jefe del Proyecto	Por Definir

Tabla 10: Registros de Riesgos del Proyecto
Elaborado: Por los autores

Probabilidad de Ocurrencia/Impacto	Calificación
Alto	0.90
Medio	0.50
Bajo	0.20

2.14. Gestión de Adquisiciones

Entregable / Actividad a realizar	Proveedor	Monto	Tipo de Contrato	Fecha de Inicio y de Fin	Nombre de contacto con el proveedor / email/Teléfono
Servidor listo para producción/Implementación del Servidor	Cliponet	S/.300	Compraventa	20/11/2016	Massiel Gamboa Ruiz/massiel.gamboa@cliponet.com
Servidor listo para producción/Implementación del Servidor	Soluciones de Cableado Estructurado	S/.6,246	Compraventa	20/11/2016	Jonathan Martinez/jonathan.martinez@sce.com.pe
Instalación del firewall tmg forefront/Implementación del firewall	Soluciones de Cableado Estructurado	S/.2,276	Compraventa	23/01/2017	Jonathan Martinez/jonathan.martinez@sce.com.pe
Diagrama Actual de la red/Identificación de la topología de la red	Cliponet	S/. 6.00	Compraventa	21/11/2016	Massiel Gamboa Ruiz/massiel.gamboa@cliponet.com
Documento de políticas de seguridad del firewall/Políticas de seguridad para el firewall	Cliponet	S/. 400	Compraventa	21/11/2016	Massiel Gamboa Ruiz/massiel.gamboa@cliponet.com

Tabla 11: Gestión de Adquisiciones
Elaborado: Por los autores

2.15. Planificación de Calidad

2.15.1. Plan de Calidad del Proyecto

Entregable	Actividad para lograr la calidad	Métrica identificada	Ejecutado por	Aprobado Por
Diagrama actual de la red	Identificación de topología de la red	Tiempo de respuesta en comunicación por la red= menor a 10 segundos	Renzo Castillo Palomino	Carlos Sulca Galarza
identificación de los servicios de red de la Clínica Aliada	Identificación de los sistemas de información actuales	Número de funciones del usuario entre 20 a 30 / total de funciones 5	Renzo Castillo Palomino	Carlos Sulca Galarza
Análisis del ancho de banda actual	Análisis del uso actual del ancho de banda de internet	Tiempo de respuesta en el acceso de páginas web= menor a 10 segundos	Renzo Castillo Palomino	Carlos Sulca Galarza
Documento de políticas de seguridad del Firewall	Políticas de seguridad para el firewall	Número de funciones evidentes al usuario entre 20 a 30 / total de funciones 5	Renzo Castillo Palomino	Carlos Sulca Galarza
Documento de direccionamiento Ip de la red	Direccionamiento IP	Tiempo de respuesta en comunicación por la red=10 segundos	Renzo Castillo Palomino	Carlos Sulca Galarza

Diagrama de red propuesto	Topología de red propuesta	Cambios=número de cambios entre 1 a 2 / total de funciones 1	Renzo Castillo Palomino	Carlos Sulca Galarza
Servidor listo para instalación del firewall	Implementación del servidor	Número de funciones evidentes al usuario entre 10 a 30 / total de funciones 30	Miguel Domínguez Chávez	Carlos Sulca Galarza
Instalación del firewall tmg forefront	Implementación del firewall	Número de funciones evidentes al usuario entre 10 a 20 / total de funciones 20	Miguel Domínguez Chávez	Carlos Sulca Galarza
Check list de pruebas	Pruebas de ejecución de políticas de seguridad	número de casos de prueba en el check list 15/ número de casos de pruebas requeridas 3	Miguel Domínguez Chávez	Carlos Sulca Galarza
Reportes de servicios	Administración y monitoreo de la red	Tiempo de respuesta=5 segundos	Miguel Domínguez Chávez	Carlos Sulca Galarza

Tabla 12: Plan de Calidad del Proyecto
Elaborado: Por los autores

“IMPLEMENTACIÓN DE UN FIREWALL TMG FOREFRONT PARA LA SEGURIDAD PERIMETRAL DE LA RED DE DATOS DE LA CLÍNICA ALIADA”

Capítulo III:
MODELO DE LA RED

3.1. Fase de Planificación

3.1.1. Situación Actual de la red

La actual plataforma del **Cliente** servirá como base para implementar el TMG Forefront 2010 este firewall es desarrollado por Microsoft y proporciona una variedad de soluciones de seguridad perimetral como prevención de accesos no autorizados antivirus, antispam, control web, conexiones vpn.

Actualmente el Cliente no cuenta con una Firewall perimetral, cuenta con 02 proveedores de internet (Claro y Telefónica), estos routers de internet realizan la función de NAT para navegación de los usuarios y publicación de sus servicios.

Por el enlace de Claro salen los usuarios corporativos y por el enlace de TDP Speedy salen por wifi los pacientes y personal externo de la empresa. Todo el enrutamiento interno y externo lo realiza el switch Core identificado con la ip 10.7.0.2

3.1.2. Identificación de la topología de red

La red de computadoras a proteger al momento de iniciar el presente proyecto se encuentra montada según se presentan en el siguiente diagrama.

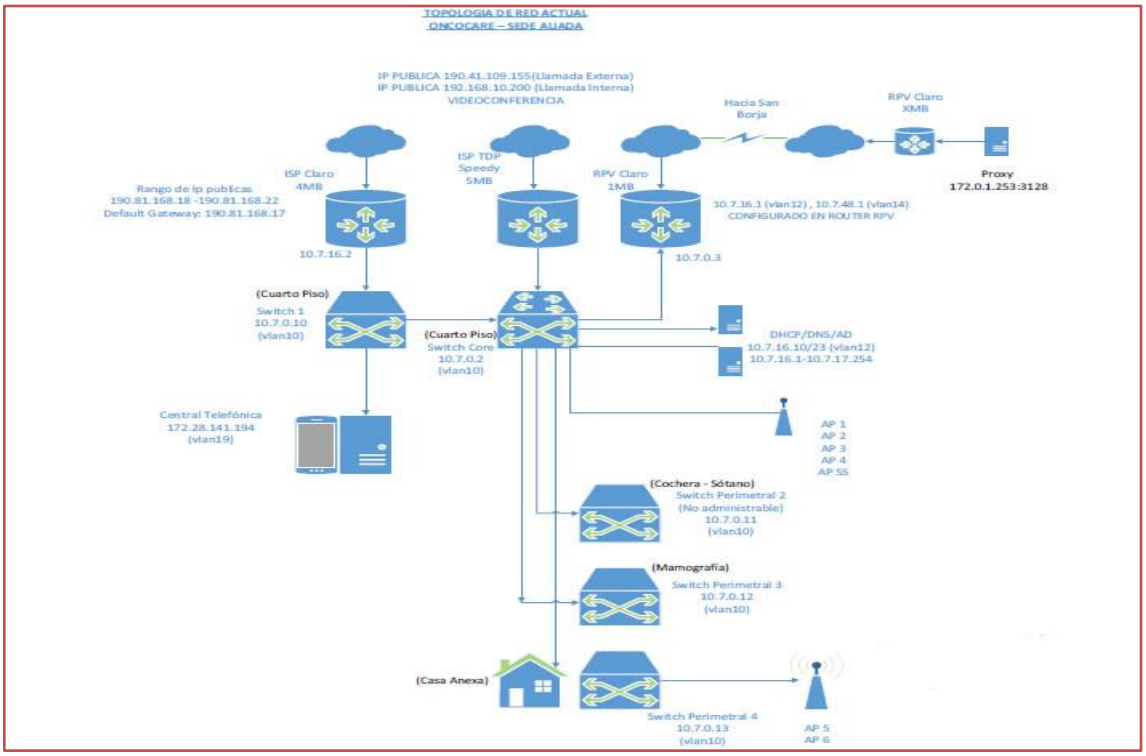


Figura 29: Topología de Red Actual
Elaborado: Por los autores

Leyenda		
Dispositivo	Descripción	Función
	Router de servicio de Internet – RPV (Red Privada)	Brinda el servicio de internet en modo nat, el router RPV brinda el servicio de internet y el servicio de telefonía entre las empresas del grupo.
	Switch Core L3(Capa 3)	Su principal funcionan es el enrutamiento entre la red interna hacia las redes externas del grupo.
	Access Point Cisco	Su función es de trasmitir el servicio de internet mediante señales de radio, para los pacientes de la clínica.
	Servidor Proxy	Este servidor Proxy está ubicada en la Clínica San Borja el cual nos permite salir a internet desde cualquier computadora de la Clínica Aliada.
	Central Telefónica Elastik	La función de este servidor es manejar todo el servicio de telefónica externa (Llamadas externas celulares, larga distancia, llamadas internacionales).
	Servidor Compatible	Este servidor brinda el servicio de dhcp para todas las computadoras de la clínica Aliada.

Tabla 13: Leyenda de diagrama de red actual
Elaborado: Por los autores

3.1.3. Identificación de servidores

Los servidores que a continuación de describirán fueron identificados en una entrevista con el analista de infraestructura de sistemas de la Clínica Aliada.

Servidor	Servicio	Descripción
HP proliant 110 g5	AD-APLICACIONES	Servidor de aplicaciones y de directorio activo
IBM BLADE X220	BASE DE DATOS	Servidor de base de datos
PC COMPATIBLE CORE I5	DHCP	Servidor con servicio DHCP(Asignación de ip)
HP proliant 110 g5	CONSOLA DE ANTIVIRUS	Servidor que cuenta con la consola de administración del antivirus corporativo

Tabla 14: Servidores en producción
Elaborado: Por los autores

3.1.4. Identificación de los equipos de comunicación

Los equipos de comunicación que a continuación de describirán fueron identificados en una entrevista con el jefe de sistemas de la Clínica Aliada.

Local	Equipo	Función	Puertos	Conexión
San Isidro	Switch-Cisco	Interconectar los equipos de la red interna.	24	LAN
San Isidro	Switch-Cisco	Interconectar los equipos de la red interna.	24	LAN
San Isidro	Switch-Cisco	Interconectar los equipos de la red interna.	48	LAN
San Isidro	Switch-Cisco	Interconectar los equipos de la red interna.	48	LAN
San Isidro	Switch-Core-Cisco	Enrutamiento interno y externo.	24	LAN-INTERNET

San Isidro	Switch-DLINK	Interconectar los equipos de la red interna.	24	LAN
San Isidro	Router-ZTE	Brinda el servicio de internet para el uso de wifi, para los pacientes.	5	ISP Telefónica
San Isidro	Router-Cisco	Brinda servicio de internet en modo nat.	5	RPV
San Isidro	Router-Cisco	Brinda el servicio de internet en modo nat, para el uso interno.	5	ISP
San Isidro	AP – Cisco 1602	Transmite el servicio de internet mediante señales de radio, para los pacientes de la clínica.	1	INTERNET
San Isidro	AP – Cisco 1602	Transmite el servicio de internet mediante señales de radio, para los pacientes de la clínica.	1	INTERNET
San Isidro	AP – Cisco 1602	Transmite el servicio de internet mediante señales de radio, para los pacientes de la clínica.	1	INTERNET
San Isidro	AP – Cisco 1602	Transmite el servicio de internet mediante señales de radio, para los pacientes de la clínica.	1	INTERNET
San Isidro	AP – Cisco 1602	Transmite el servicio de internet mediante señales de radio, para los pacientes de la clínica.	1	INTERNET
San Isidro	AP – Cisco 1602	Transmite el servicio de internet mediante señales de radio, para los pacientes de la clínica.	1	INTERNET
San Isidro	AP – Cisco 1602	Transmite el servicio de internet mediante señales de radio, para los pacientes de la clínica.	1	INTERNET

Tabla 15: Equipos de comunicación de la red
Elaborado: Por los autores

3.1.5. Identificación de los sistemas de información actuales

Los sistemas con los que actualmente cuenta la Clínica Aliada son detallados a continuación:

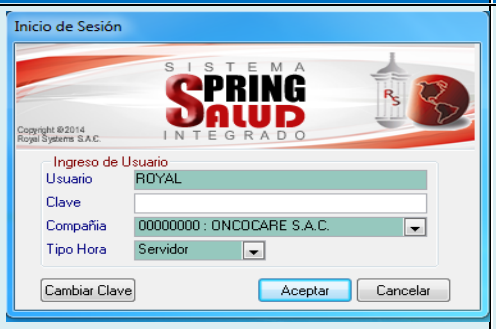
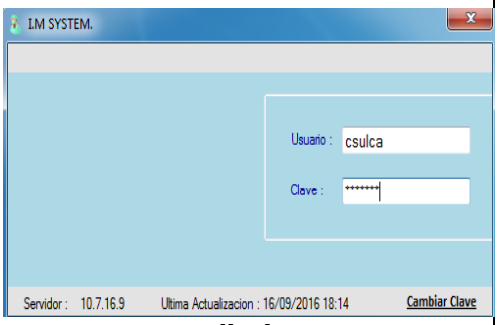
Sistema	Servicio	Requerimientos mínimos de comunicaciones	Observaciones
 **Spring Salud**	Lan	- Lan 10/100 mbps o superior. - Línea dedicada con fibra óptica de 256 kbps o superior.(Red externa entre sedes)	Sistema Core de la clínica, la cual es usado por una empresa de Call Center mediante un terminal server.
 **Aliada**	Lan	- Lan 10/100 mbps o superior.	Sistema de uso interno.

Tabla 16: Identificación de los sistemas de información
Elaborado por: Autores

3.1.6. Análisis del uso actual del ancho de banda de internet

El ancho de banda es la medida de la cantidad de información que puede atravesar la red en un período dado de tiempo. Actualmente la Clínica Aliada cuenta con una línea de Internet de 4 MB disponiendo el servicio de Internet a cualquier interrupción inadvertida lo que atrae consigo perdidas de funcionalidad del servicio.

Para la evaluación del ancho de banda se usó el aplicativo web **Traffic View** el cual nos mostró los siguientes gráficos.

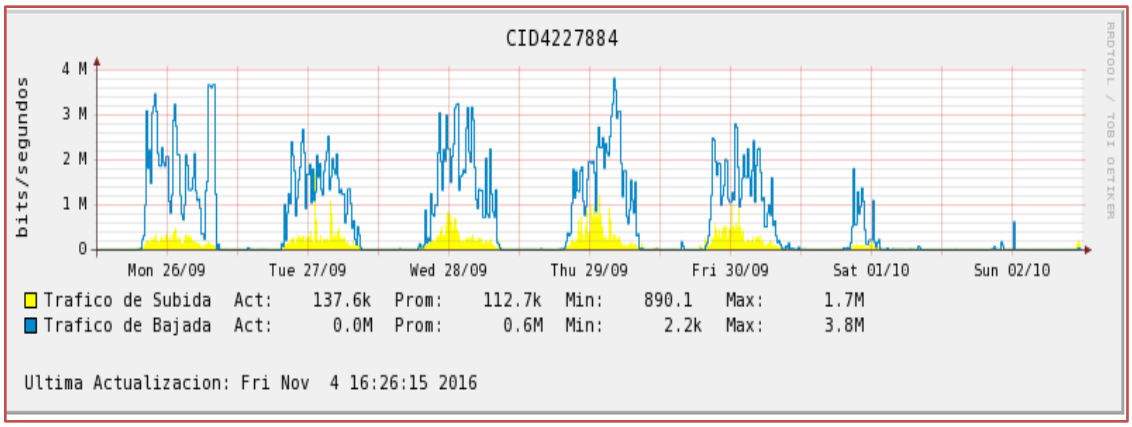


Figura 30: Traffic View 1
Elaborado: Por los autores

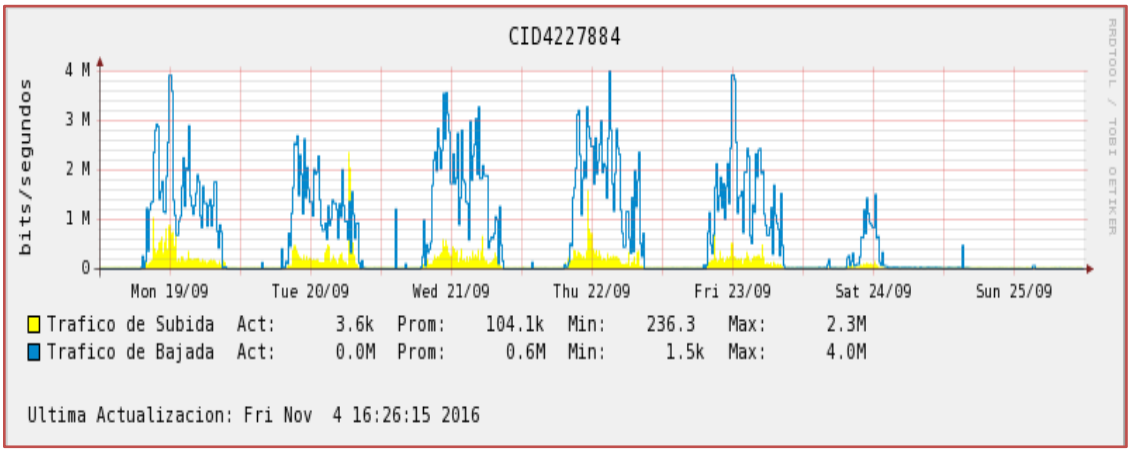


Figura 31: Traffic View 2
Elaborado: Por los autores

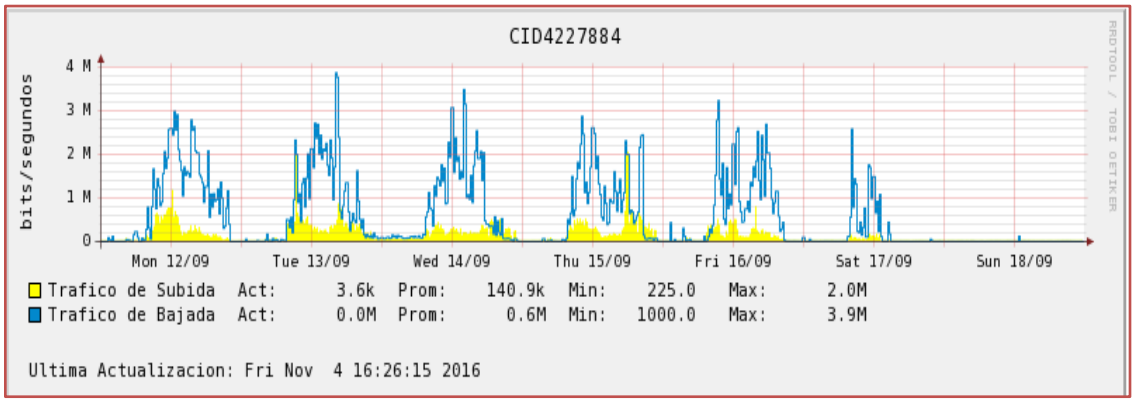


Figura 32: Traffic View 3
Elaborado: Por los autores

Figura	Descripción
Número 27	Se observa un uso de 2 a 4 Mb del ancho de banda de internet.
Número 28	Se observa un uso de 3 a 4 Mb del ancho de banda de internet.
Número 29	Se observa un uso de 1 a 3 MB de ancho de banda de internet.

Tabla 17: Detalles en consumo de ancho de banda
Elaborado: Por los autores

El segundo aplicativo que se usó para poder analizar el uso del ancho de banda es **ManageEngine NetFlow Analyzer**, el cual también nos muestra un gráfico del mes de setiembre.

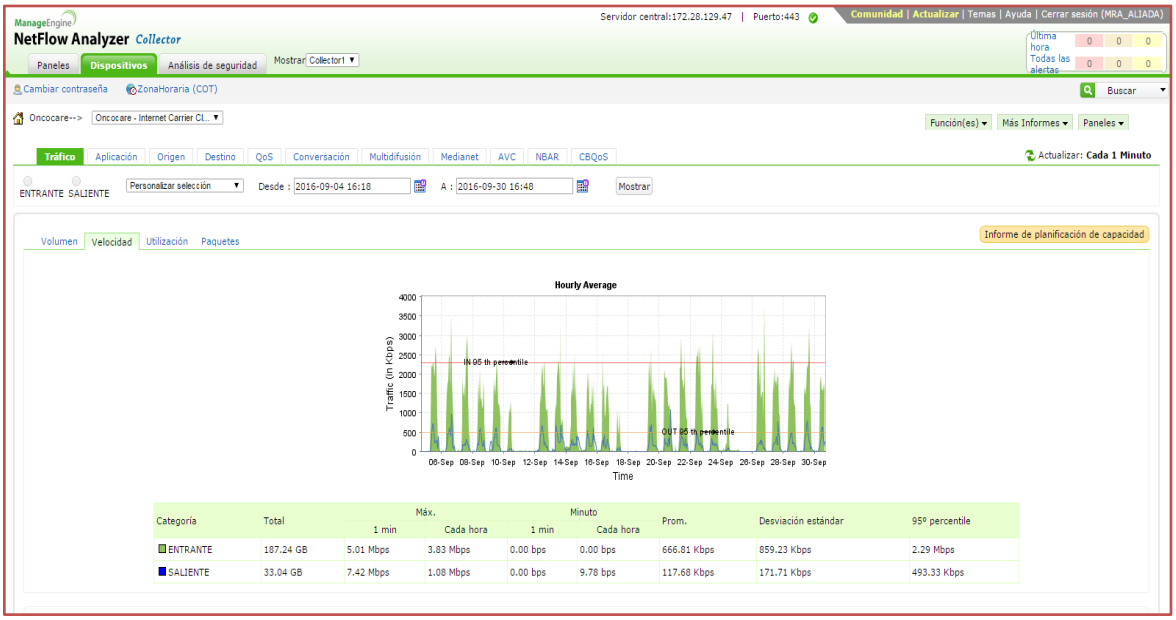


Figura 33: ManageEngine Netflow Analyzer
Elaborado: Por los autores

Podemos concluir que los usuarios por motivos laborales y por falta de control en la navegación por internet consumen **3 MB de un total de 4 MB** de ancho de banda de internet ocasionando problemas de lentitud en toda la red y afectando a los demás usuarios.

Ambos aplicativos detallados anteriormente sirven para analizar el ancho de banda y fueron proporcionados por el Proveedor de Internet Claro Perú, los cuales tiene la función de monitorear el ancho de banda del servicio de internet.

3.1.7. Equipos necesarios para el proyecto

Los equipos y licencias a adquirir por el cliente son los siguientes:

Software - Hardware	Requisitos mínimos
Hp Proliant ml110	Procesador Core i5 , 4 gb de ram, hdd 500 gb
TMG Forefront Standart	-

Tabla 18: Equipos necesarios para la implementación
Elaborado por: Autores

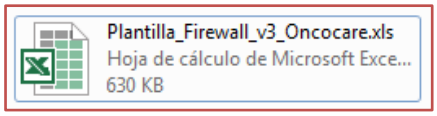
3.2. Fase de Diseño

3.2.1. Seguridad

La red mantendrá la seguridad a nivel lógico con las políticas que se crearan en el firewall, reglas de acceso, lo cual aumentara la confidencialidad y disminuir la vulnerabilidad de los datos.

3.2.2. Políticas de seguridad para el firewall

Las políticas que se implementaran en el firewall, serán definidas por el Cliente el cual ira registrando en el siguiente archivo:



Descripción	EJEMPLO								
Sub Category	Grupo_1	Grupo_2	Grupo_3	Grupo_4	Grupo_5	Grupo_6	Grupo_7	Grupo_8	Grupo_9
Drug Abuse	X	X	X	X	X	X	X	X	X
Hacking	X	X	X	X	X	X	X	X	X
Illegal or Unethical	X	X	X	X	X	X	X	X	X
Discrimination	X	X	X	X	X	X	X	X	X
Explicit Violence	X	X	X	X	X	X	X	X	X
Extremist Groups	X	X	X	X	X	X	X	X	X
Proxy Avoidance	X	X	X	X	X	X	X	X	X
Plagiarism	X	X	X	X	X	X	X	X	X
Child Abuse	X	X	X	X	X	X	X	X	X
Alternative Beliefs	X	X	X	X	X	X	X	X	X
Abortion	X	X	X	X	X	X	X	X	X
Other Adult Materials	X	X	X	X	X	X	X	X	X
Advocacy Organizations	X	X	X	X	X	X	X	X	X
Gambling	X	X	X	X	X	X	X	X	X
Nudity and Risque	X	X	X	X	X	X	X	X	X
Pornography	X	X	X	X	X	X	X	X	X
Dating	X	X	X	X	X	X	X	X	X
Weapons (sales)	X	X	X	X	X	X	X	X	X
Marijuana	X	X	X	X	X	X	X	X	X
Sex Education	X	X	X	X	X	X	X	X	X
Alcohol	X	X	X	X	X	X	X	X	X
Tobacco	X	X	X	X	X	X	X	X	X
Lingerie and Swimsuit	X	X	X	X	X	X	X	X	X
Sports Hunting and War Games	X	X	X	X	X	X	X	X	X
Freeware and Software Downloads	✓	X	X	X	✓	X	X	X	X
File Sharing and Storage	✓	X	X	X	X	X	X	X	X
Streaming Media y Download	✓	X	X	X	X	X	X	X	X
Peer-to-peer File Sharing	✓	X	X	X	X	X	X	X	X

DHCP | DNS | Políticas de Firewall | IP Pool | Virtual IP | Servicios | Grupos de direcciones | Filtro Web | Application Filter

Figura 34: Plantilla de políticas de seguridad
Elaborado: Por los autores

El archivo tendrá los siguientes puntos importantes.

- ✓ Grupo de direcciones ip
- ✓ Filtrado web
- ✓ Filtrado por aplicación
- ✓ Nat para servidores
- ✓ Usuarios VPN

3.2.3 Funcionalidad

Con el levantamiento de información realizado, se identificó que la red funciona de manera óptima brindando facilidades para la implementación de Firewall TMG Forefront. La red proporcionará conectividad al usuario consumiendo diversos servicios internos como aplicaciones corporativas con una velocidad deteriorada debido a la falta de una solución perimetral que actualmente se estará implementando para dar solución a los diversos problemas de seguridad identificados.

3.2.4 Facilidad de administración

La implementación del firewall podrá brindarnos una administración centralizada ya que el firewall trabaja en sincronización con el directorio activo, permitiendo que las políticas aplicadas a un usuario lo mantendrá en cualquier equipo de la empresa.
El Firewall TMG nos brindara una interface muy amigable e intuitiva para poder crear reglas de acceso, verificar los log de acceso a páginas web, ver en tiempo real alertas de ataques de virus informáticos, visualizar las conexiones vpn activas y esto facilita y centraliza la administración al personal de sistemas.

3.2.5 Direccionamiento IP

El direccionamiento ip del Cliente fue proporcionado por el jefe de sistemas, especificando que dicho esquema se mantendrá al 100%, a continuación mostramos el direccionamiento actual.

VLAN ALIADA							
ID_VLAN	NOMBRE VLAN	ID	HOST	GW	MASK	MASK BITS	MAX HOST
10	GESTION						
11	SERVIDORES						
12	ADMINISTRATIVO		10.7.16.1-10.7.17.254	10.7.16.1	255.255.254.0	23	510
13	ADMIN_WIFI						
14	EQUIPOS_MEDICOS		10.7.48.1-10.7.49.254	10.7.48.1	255.255.254.0	23	510
15	IMAGENES_MEDICAS						
16	CAMARAS_VIGILANCIA						
17	WIFREE (VOZ SANNA)		192.168.1.1 - 192.168.1.254	192.168.1.1	255.255.255.0	24	
18	(PUBLICO WIFI SANNA)						
19	VOZ_IP		172.28.141.194-172.28.141.254	172.28.141.193	255.255.255.192	26	62
	IP SIP 172.28.129.82		172.28.167.34-172.28.167.46	172.28.167.33	255.255.255.240	28	14
	ENLACE						

Figura 35: Direccionamiento Ip
Elaborado: Por los autores

3.2.6 Topología de red propuesta

Con el levantamiento de información realizado en la fase de planificación se brindaron 2 propuestas

Propuesta 1

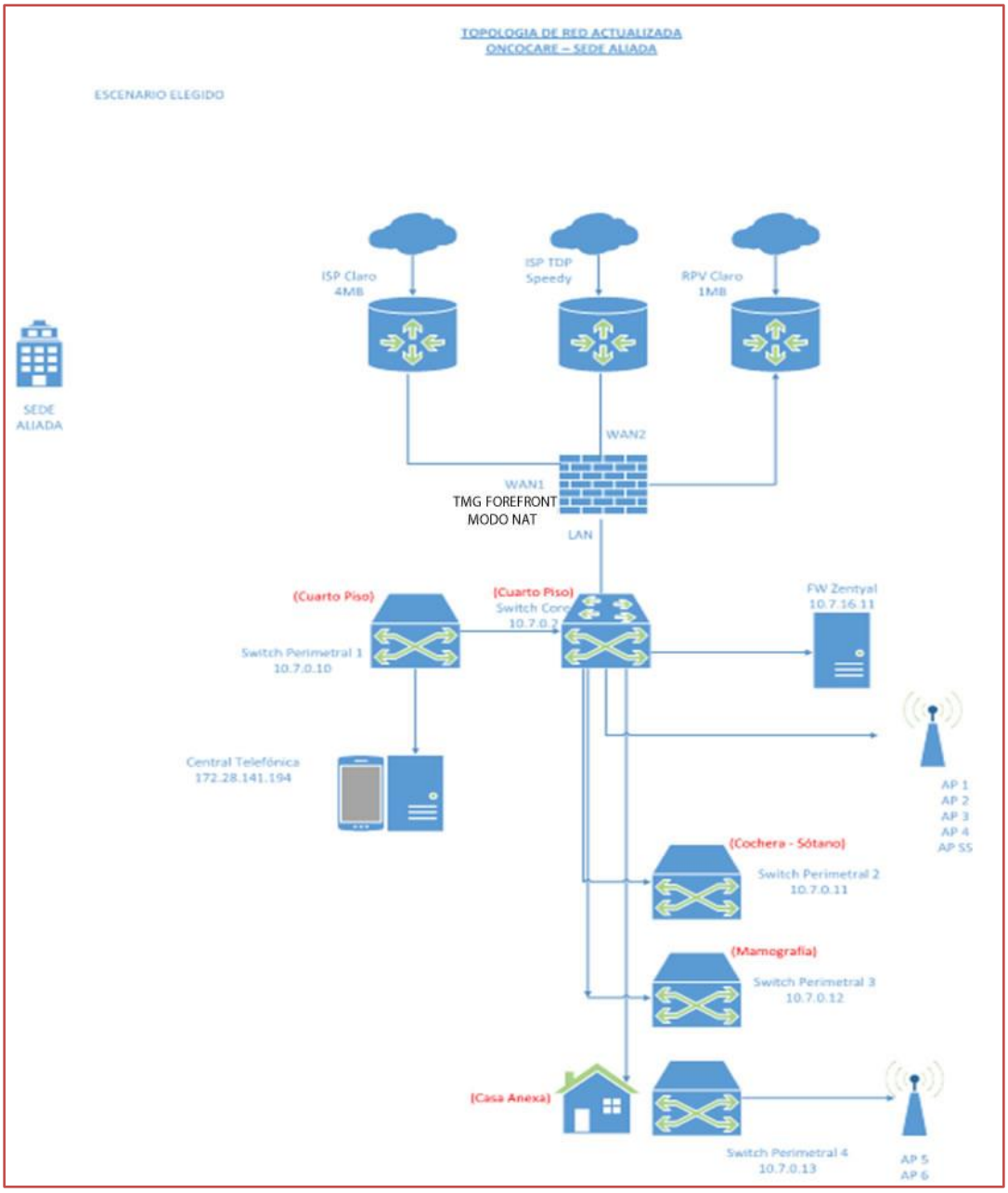


Figura 36: Propuesta Número 1
Elaborado: Por los autores

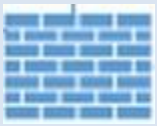
Leyenda		
Dispositivo	Descripción	Función
	Router de servicio de Internet – RPV (Red Privada)	Brinda el servicio de internet en modo nat, el router RPV brinda el servicio de internet y el servicio de telefonía entre las empresas del grupo.
	Switch Core L3(Capa 3)	Su principal funcionan es el enrutamiento entre la red interna hacia las redes externas del grupo.
	Access Point Cisco	Su función es de transmitir el servicio de internet mediante señales de radio, para los pacientes de la clínica.
	Firewall TMG Forefront 2010	La función principal del firewall será brindar seguridad perimetral a toda la red interna.
	Central Telefónica Elastik	La función de este servidor es manejar todo el servicio de telefónica externa (Llamadas externas celulares, larga distancia, llamadas internacionales).
	Servidor Compatible	Este servidor brinda el servicio de dhcp para todas las computadoras de la clínica Aliada.

Tabla 19: Leyenda de diagrama de red - propuesta 1
Elaborado: Por los autores

Propuesta 2

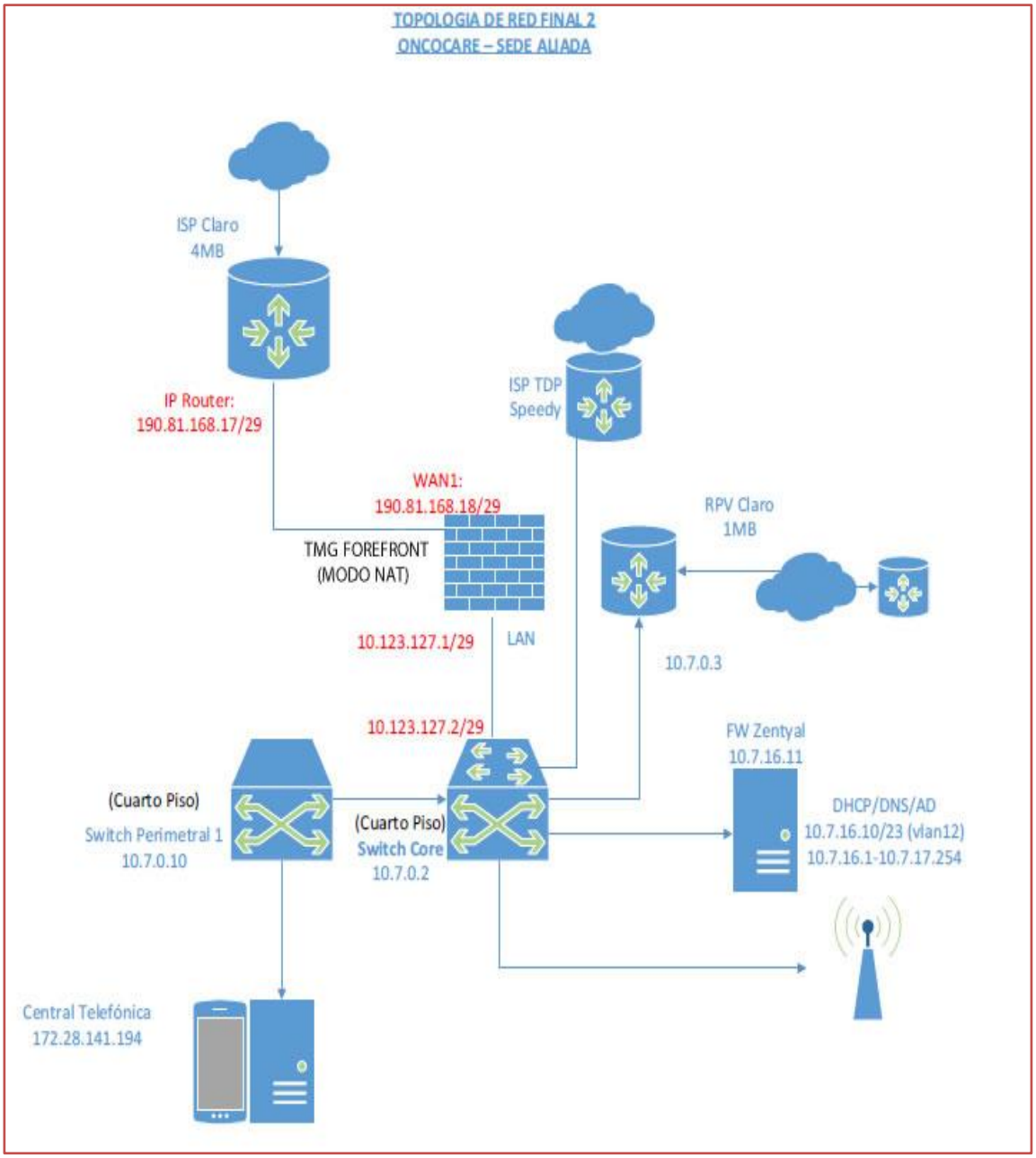


Figura 37: Propuesta Número 2
Elaborado: Por los autores

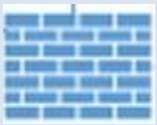
Leyenda		
Dispositivo	Descripción	Función
	Router de servicio de Internet – RPV (Red Privada)	Brinda el servicio de internet en modo nat, el router RPV brinda el servicio de internet y el servicio de telefonía entre las empresas del grupo.
	Switch Core L3(Capa 3)	Su principal funcionan es el enrutamiento entre la red interna hacia las redes externas del grupo.
	Access Point Cisco	Su función es de transmitir el servicio de internet mediante señales de radio, para los pacientes de la clínica.
	Firewall TMG Forefront 2010	La función principal del firewall será brindar seguridad perimetral a toda la red interna.
	Central Telefónica Elastik	La función de este servidor es manejar todo el servicio de telefónica externa (Llamadas externas celulares, larga distancia, llamadas internacionales).
	Servidor Compatible	Este servidor brinda el servicio de dhcp para todas las computadoras de la clínica Aliada.

Tabla 20: Leyenda de diagrama de red – propuesta 2
Elaborado: Por los autores

Esta segunda propuesta fue elegida por el Cliente, y será el bajo este diseño de red que se trabajara la implementación.

IMPLEMENTACIÓN DE UN FIREWALL TMG FOREFRONT PARA LA SEGURIDAD PERIMETRAL DE LA RED DE DATOS DE LA CLÍNICA ALIADA”

Capítulo IV:
IMPLEMENTACIÓN DE LA RED

4.1 Fase de Implementación

4.1.1 Implementación del Servidor

Instalación de Windows Server 2008 R2 en el servidor HP Proliant ML110

- ✓ Insertar DVD de Windows Server 2008 R2

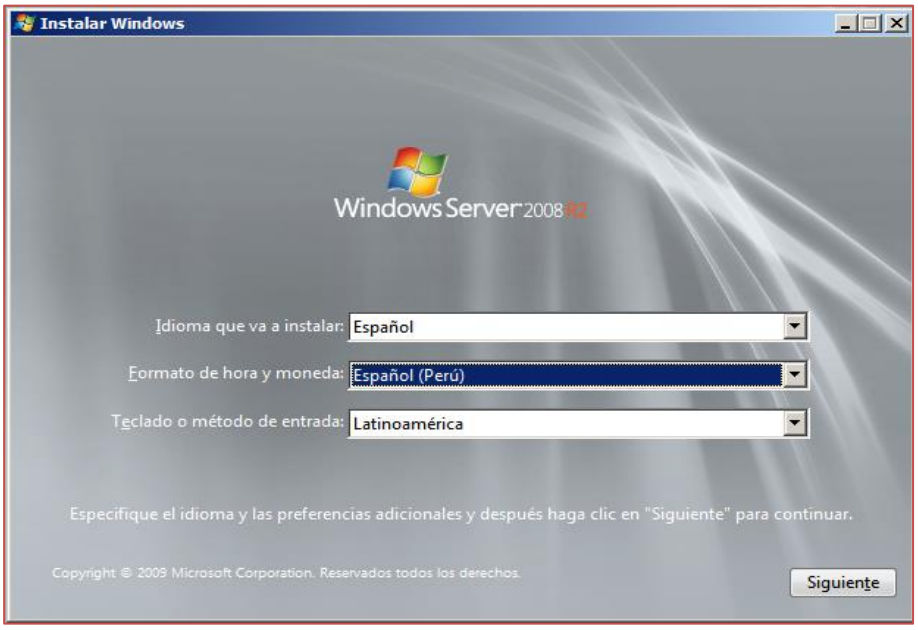


Figura 38: Instalación Paso 1
Elaborado: Por los autores

- ✓ Presionar "Instalar ahora"

Figura 39: Instalación Paso 2
Elaborado: Por los autores

✓ Ahora elegimos el Sistema operativo que deseamos, en este caso será "Windows Server 2008 R2 Standart (Instalación completa) de 64 bits" que es la versión gráfica.

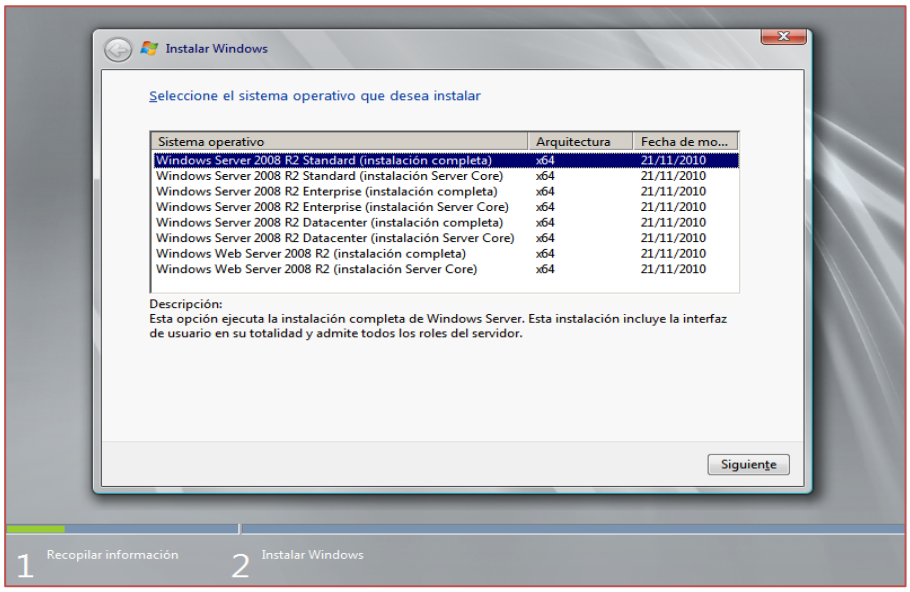


Figura 40: Instalación Paso 3
Elaborado: Por los autores

✓ Ahora aceptamos los términos de Licencia.

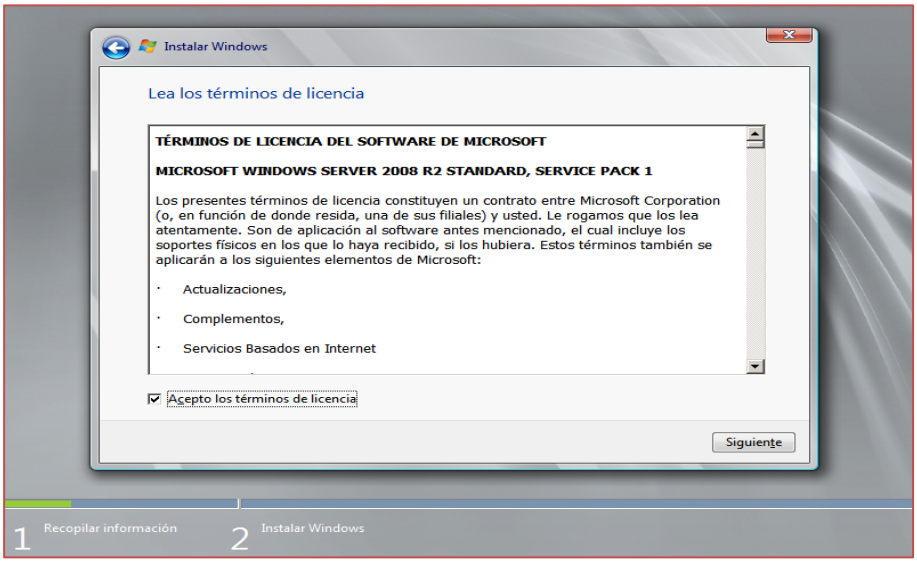


Figura 41: Instalación Paso 4
Elaborado: Por los autores

- ✓ Ahora seleccionamos **“Personalizada (avanzada)”** si deseamos particionar, en nuestro caso instalaremos nuestro sistema operativo en una sola partición (100 GB) y damos clic en **“siguiente”**

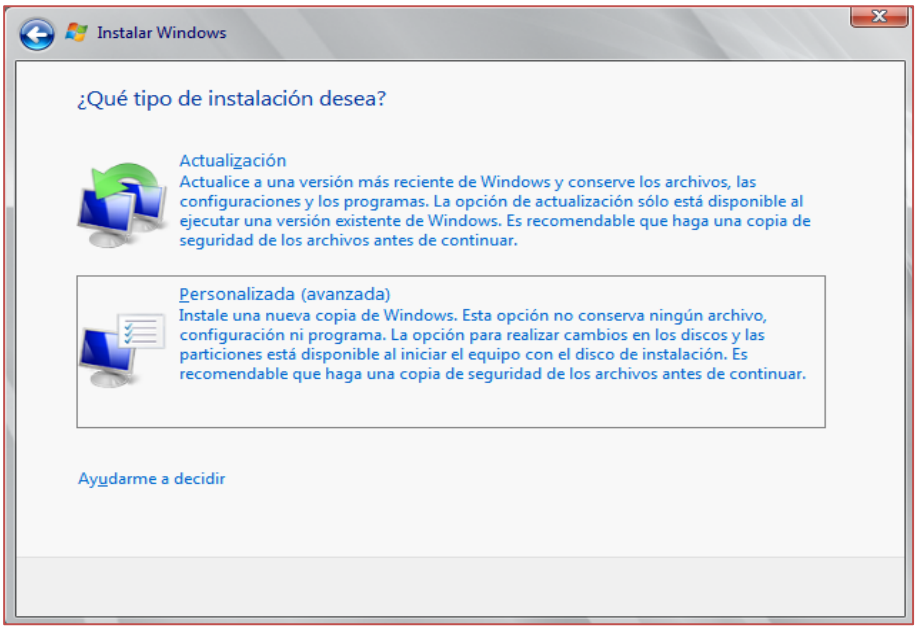


Figura 42: Instalación Paso 5
Elaborado: Por los autores

- ✓ Ahora esperamos a que termine la instalación y se reiniciará.

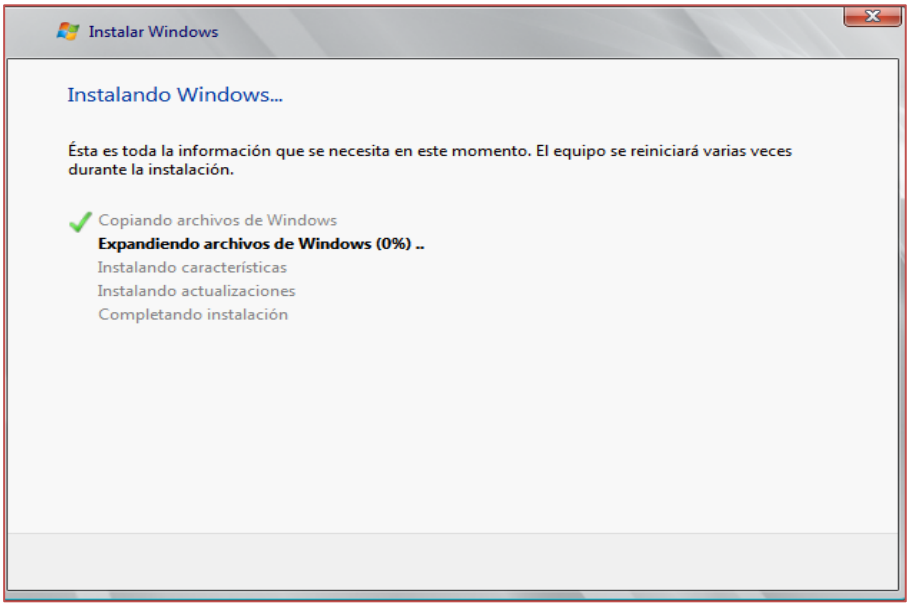


Figura 43: Instalación Paso 6
Elaborado: Por los autores

- ✓ Nos pedirá que cambiemos la contraseña, le damos clic en **"Aceptar"** e ingresamos una contraseña.

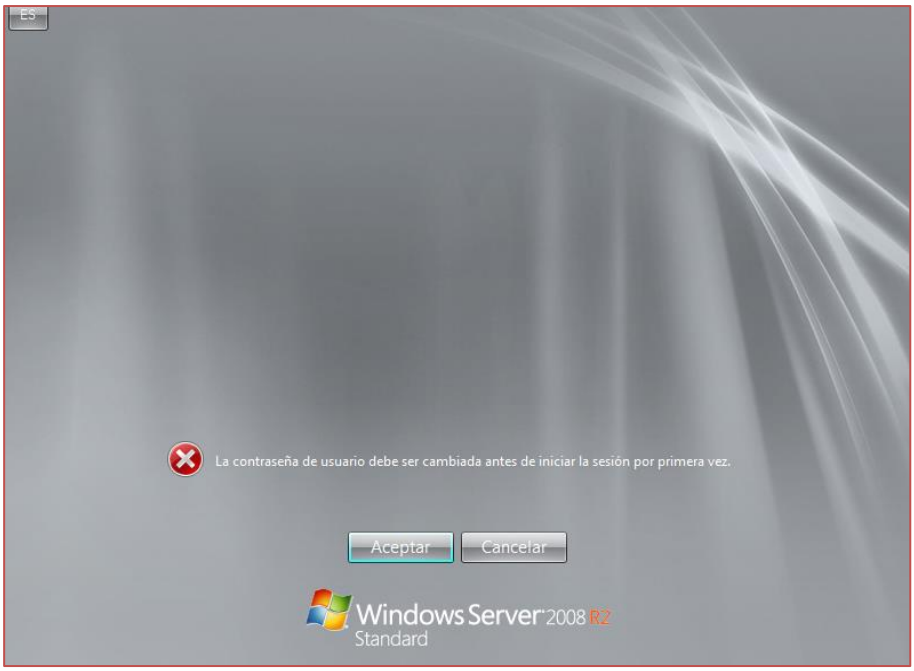


Figura 44: Instalación Paso 7
Elaborado: Por los autores

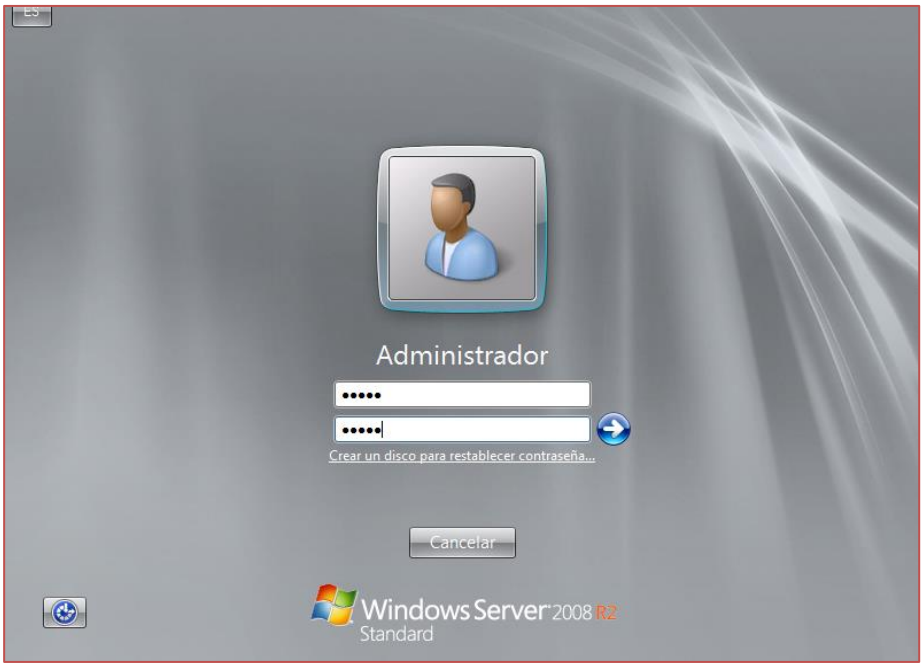


Figura 45: Instalación Paso 8
Elaborado: Por los autores

✓ Para cambiar de nombre a nuestro equipo, damos clic en “Proporcionar nombre del equipo y dominio”, luego en el botón “cambiar”.

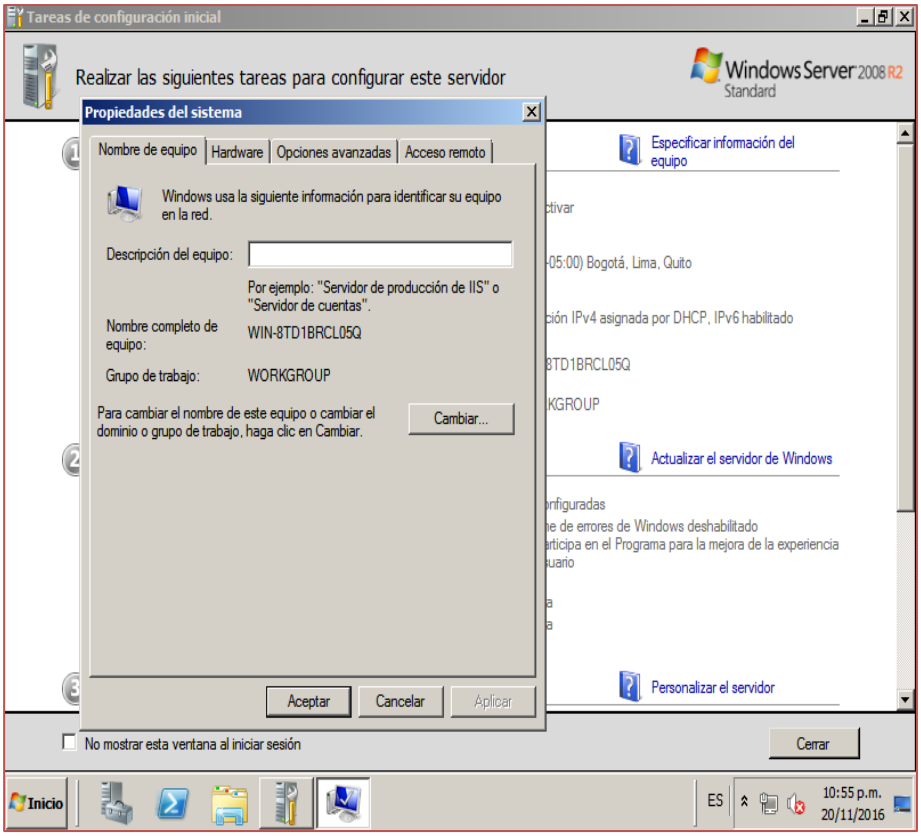


Figura 46: Instalación Paso 9
Elaborado: Por los autores

- Ingresamos “Nombre de Equipo” el cual sera SRVLIMTMG01.
- Y en dominio ASIH.ALIADA.COM

✓ Aceptamos y nos pedira reiniciar el sistema para que los cambios surgan efecto, damos clic en **“Reiniciar ahora”.**

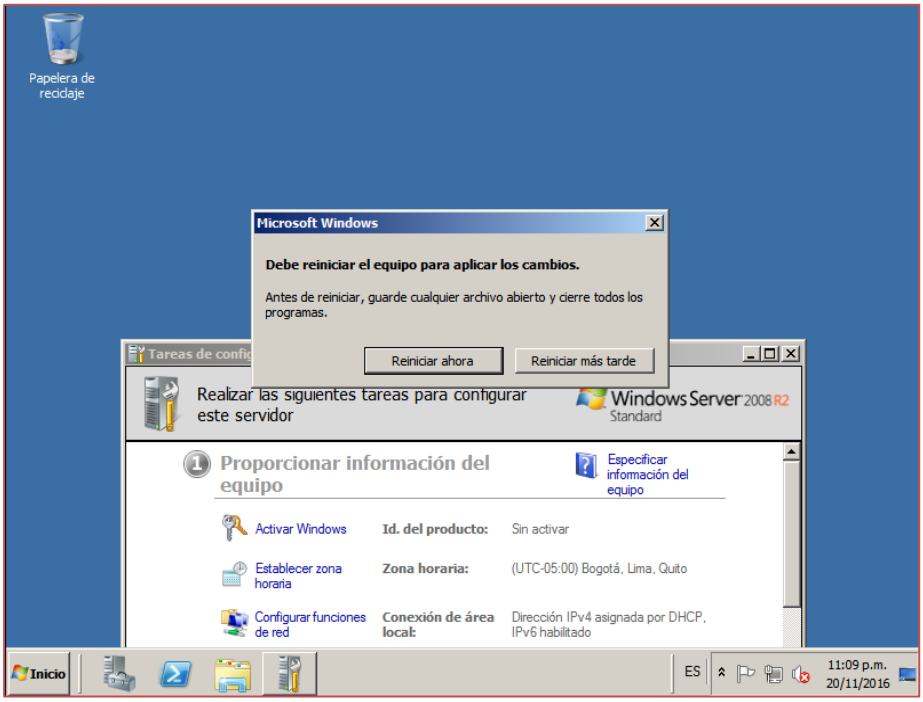


Figura 47: Instalación Paso 10
Elaborado: Por los autores

✓ Por ultimo ingresamos nuestra contraseña que asignamos anteriormente y el sistema estará listo.

Figura 48: Instalación Paso 11
Elaborado: Por los autores

- ✓ Por último se actualizara el sistema operativo por seguridad y quedara listo para instalar el TMG Forefront 2010.

Figura 49: Instalación Paso 12
Elaborado: Por los autores

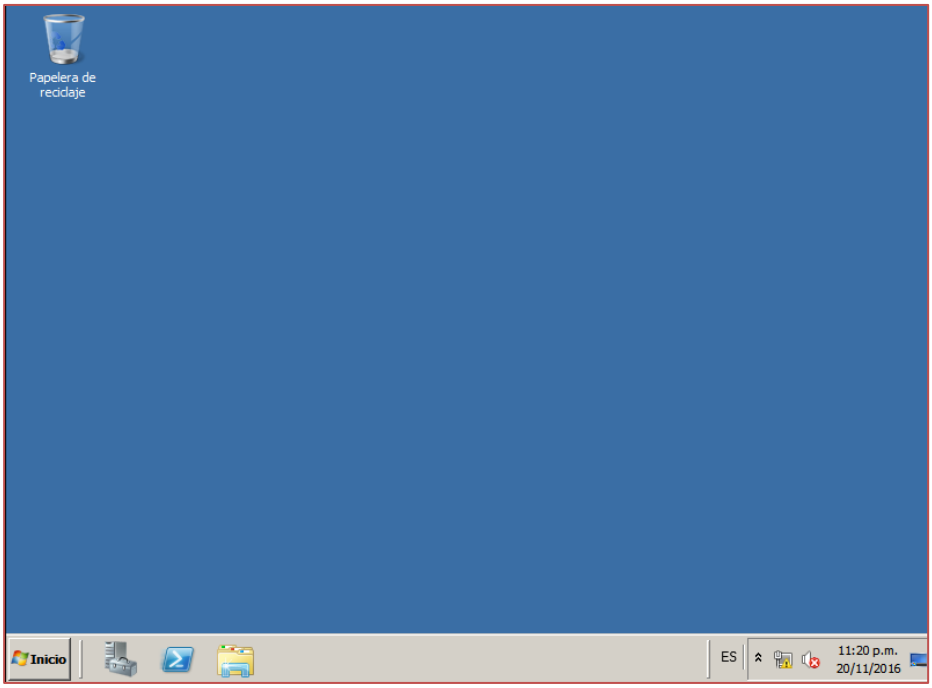


Figura 50: Instalación Paso 13
Elaborado: Por los autores

4.1.2 Implementación del Firewall

- ✓ Iniciamos el proceso de instalación del firewall ejecutando el instalador del TMG Forefront.

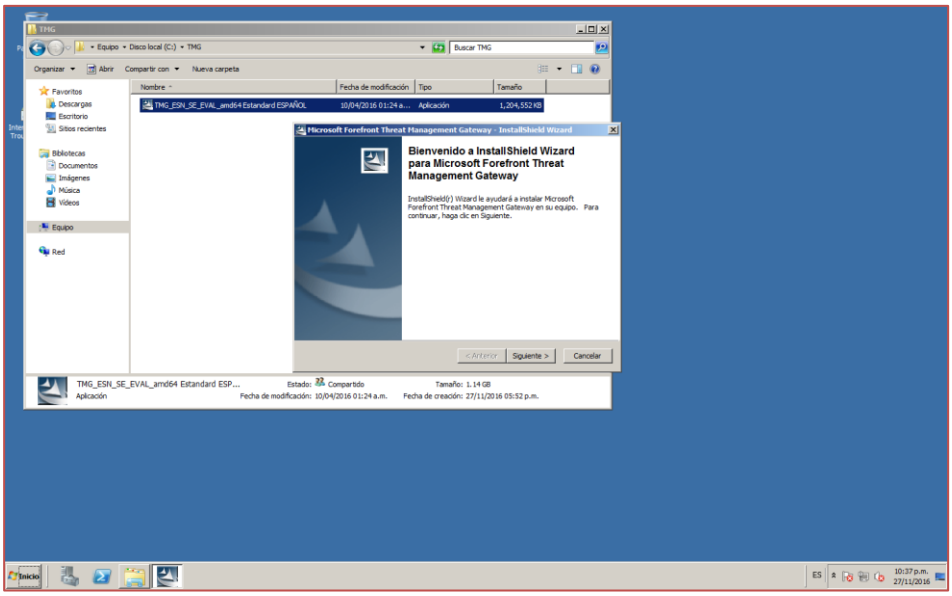


Figura 51: Ejecución del instalador del TMG
Elaborado: Por los autores

- ✓ Damos clic en el siguiente sin cambiar la ruta por defecto.

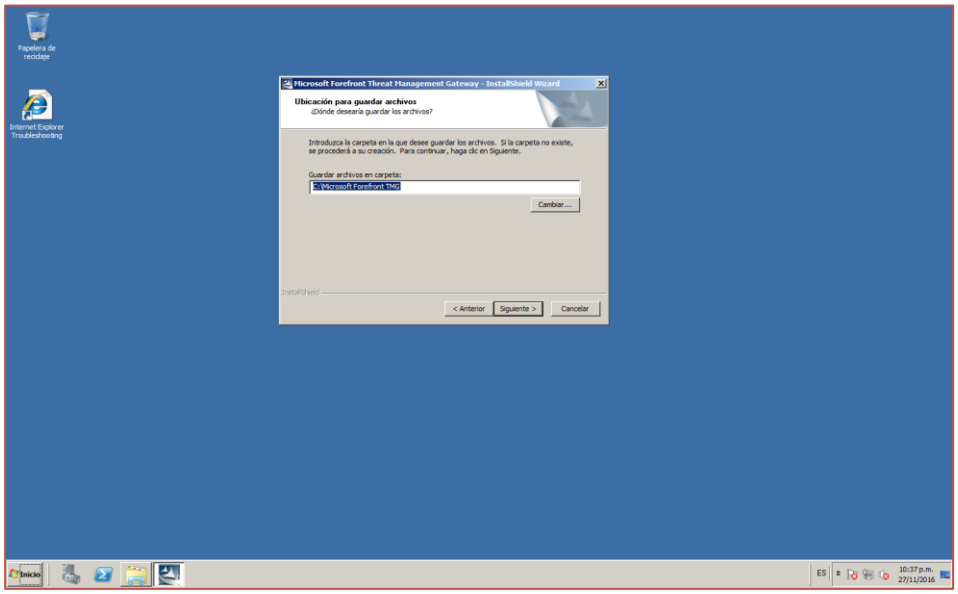


Figura 52: Ruta de instalación del TMG
Elaborado: Por los autores

✓ En la siguiente ventana vemos el progreso de pre - instalación.

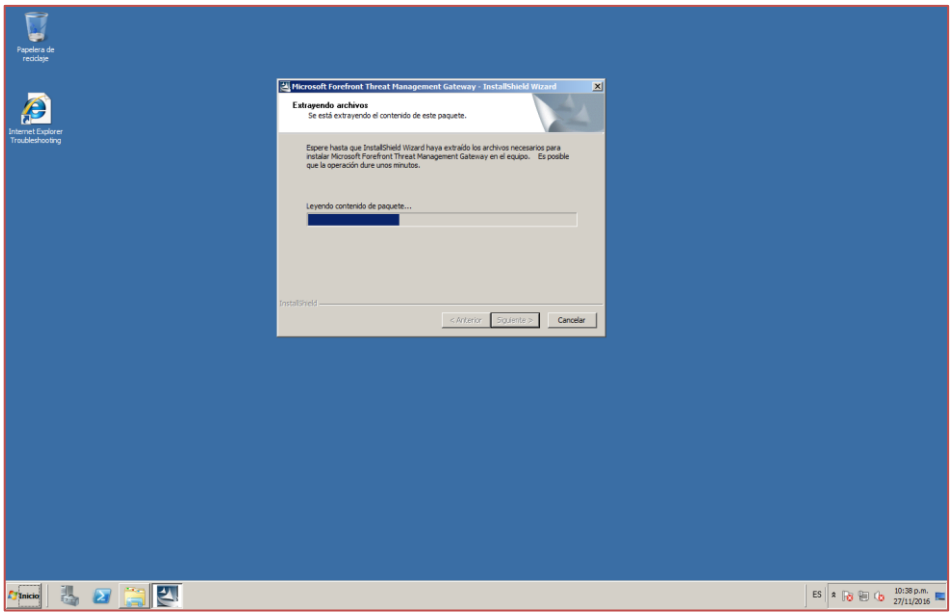


Figura 53: Progreso de pre - instalación
Elaborado: Por los autores

✓ Visualizamos la pantalla principal de instalación del TMG.

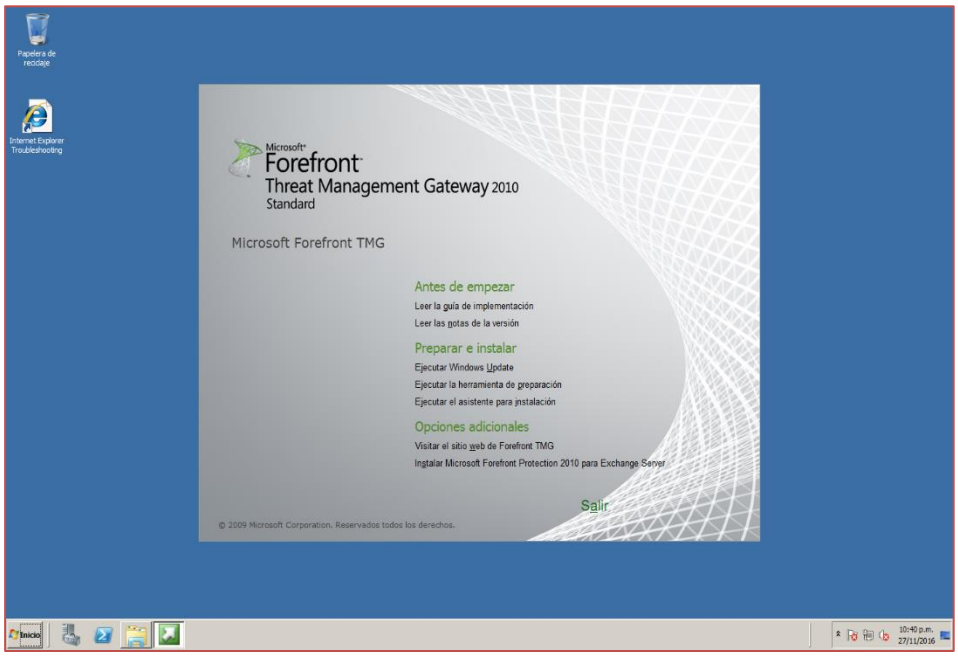


Figura 54: Pantalla principal de instalación del TMG
Elaborado: Por los autores

✓ Damos clic en herramientas de preparación.

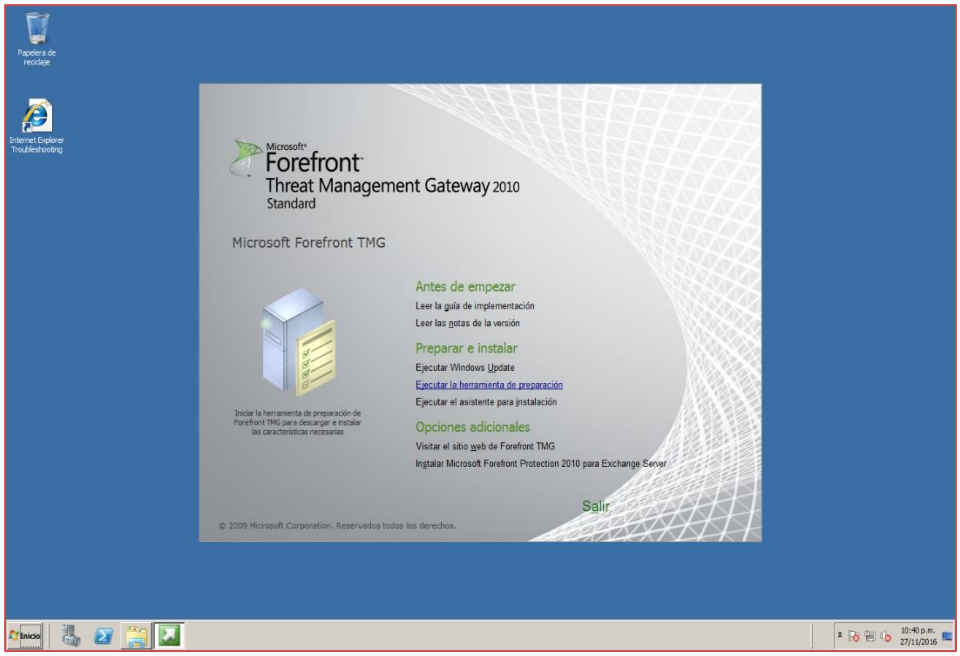


Figura 55: Herramienta de Preparación
Elaborado: Por los autores

✓ Damos clic en siguiente.

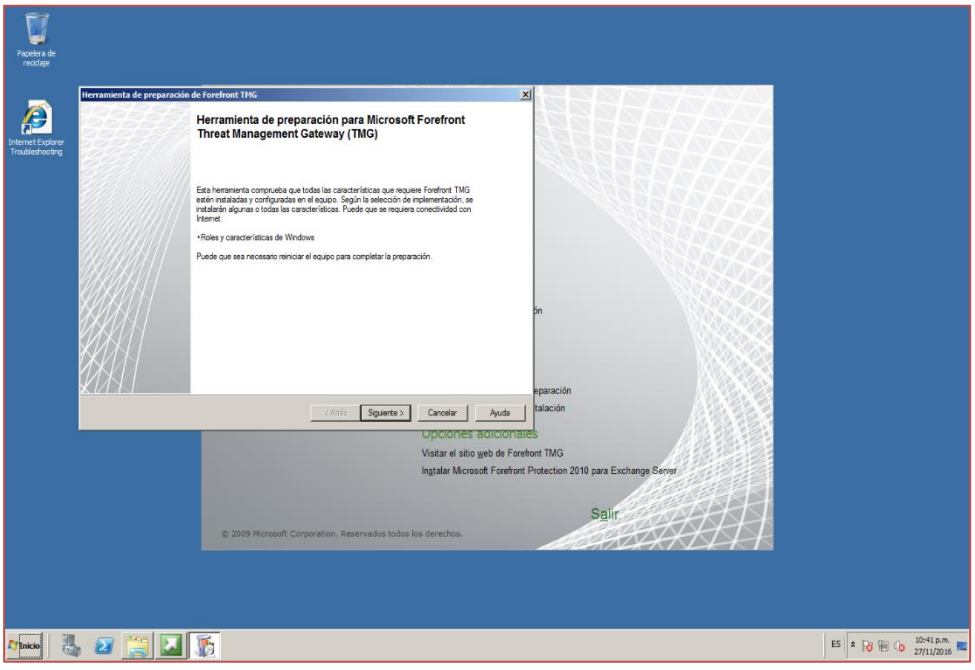


Figura 56: Herramienta de Preparación pasó 2
Elaborado: Por los autores

✓ Aceptamos y damos clic en siguiente.

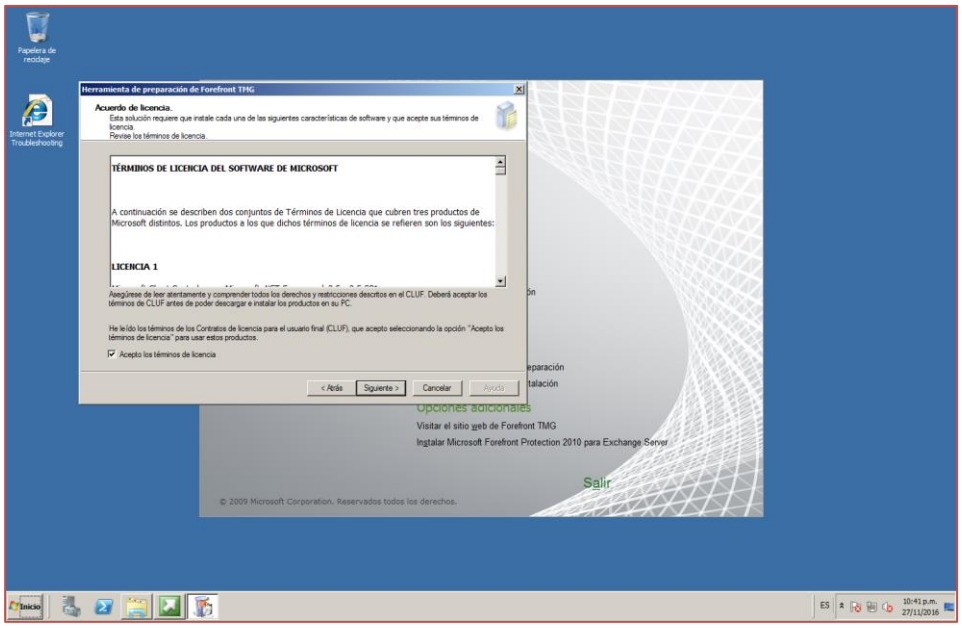


Figura 57: Confirmación de términos
Elaborado: Por los autores

✓ Se selecciona la opción de Servicios y Administración de Forefront TMG.

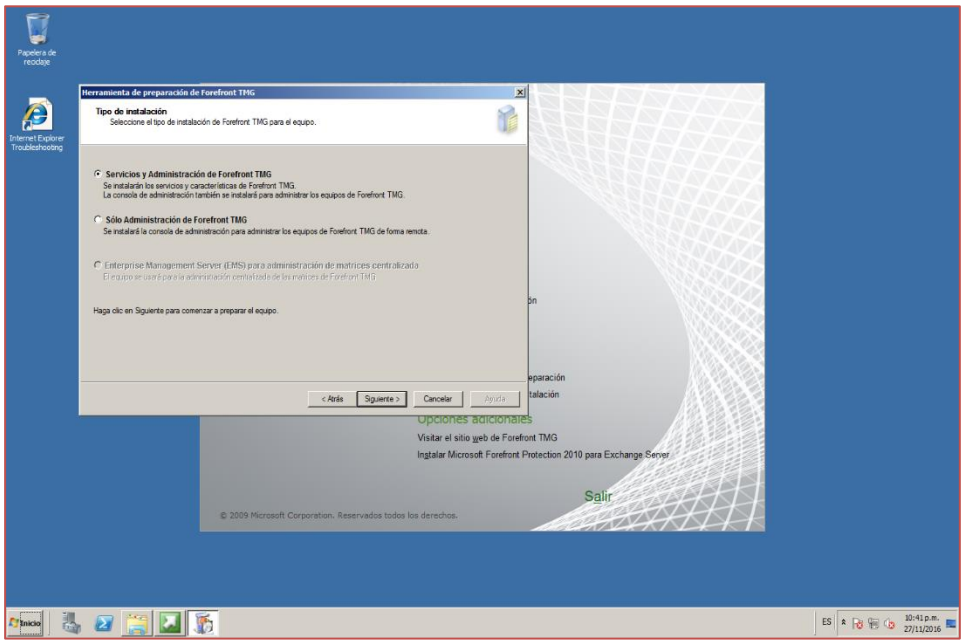


Figura 58: Selección de instalación
Elaborado: Por los autores

✓ Se visualiza el progreso de verificación de requisitos para la instalación.

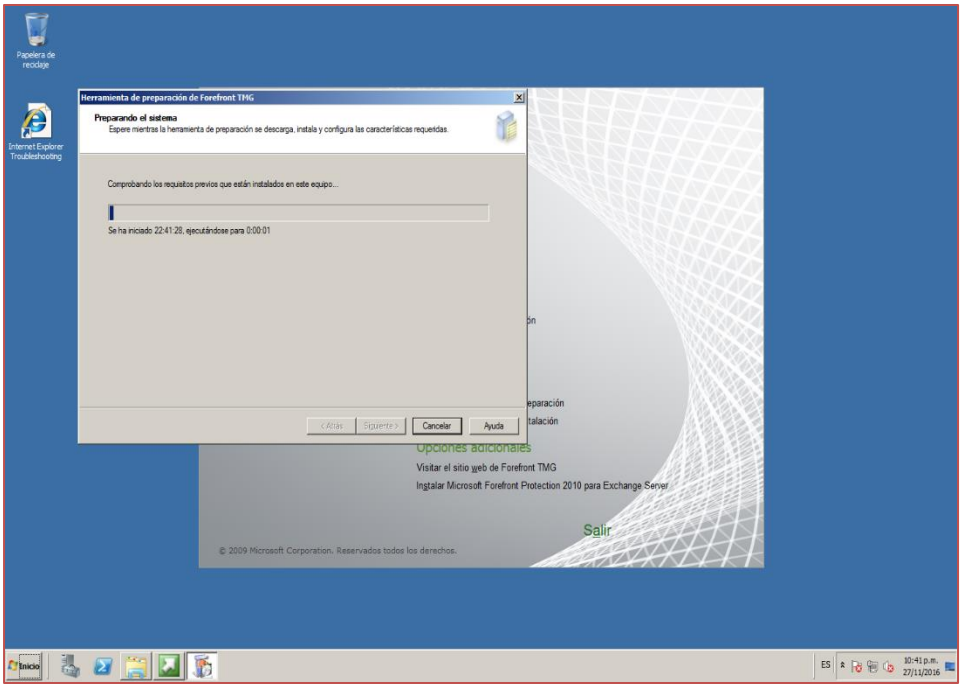


Figura 59: Verificación de requisitos
Elaborado: Por los autores

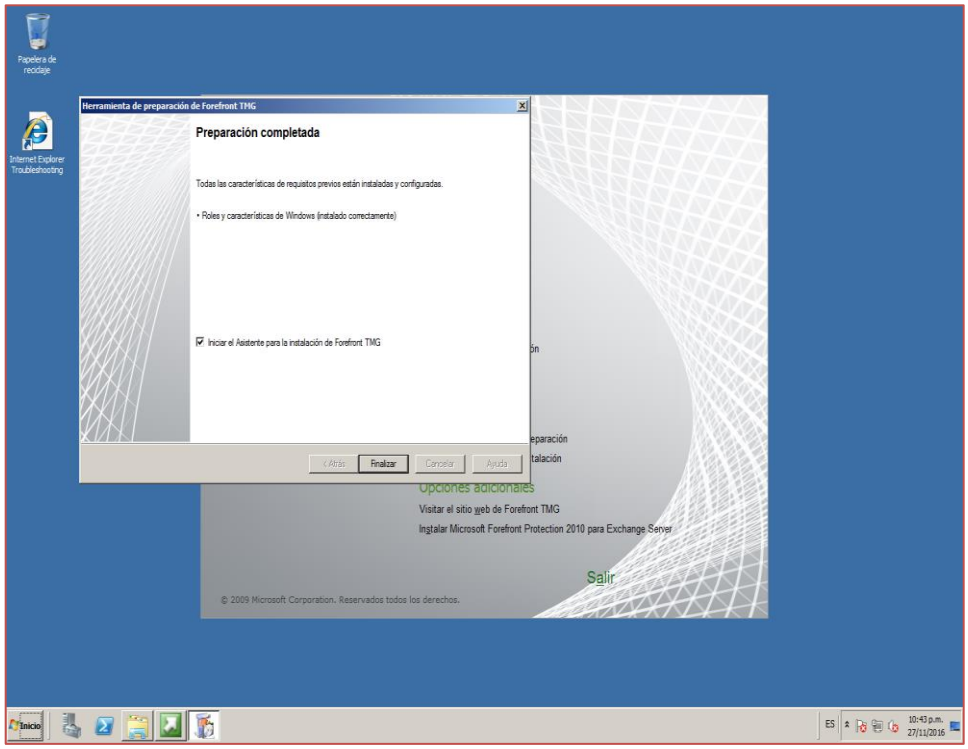


Figura 60: Finalización de preparación
Elaborado: Por los autores

✓ Se inicia el progreso de instalación del TMG dando clic en siguiente.

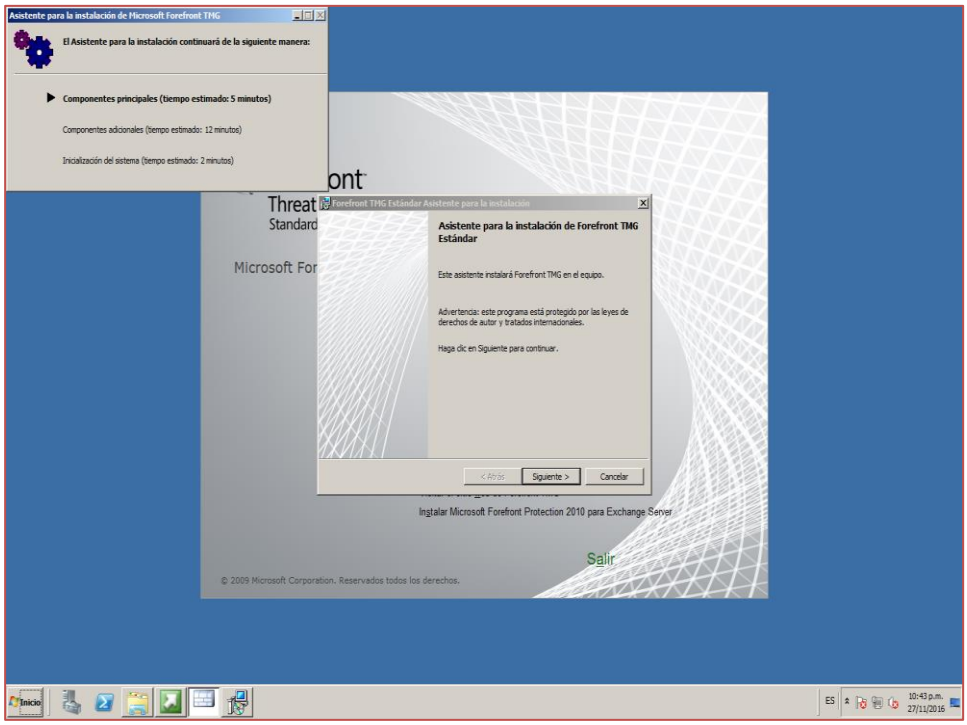


Figura 61: Asistente de instalación
Elaborado: Por los autores

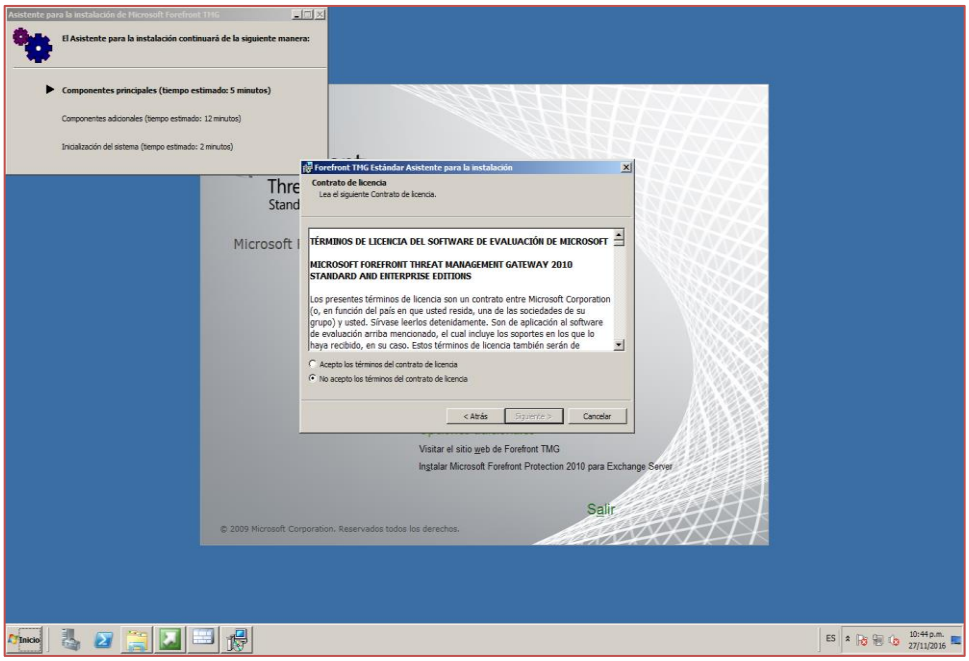


Figura 62: Confirmación de Términos
Elaborado: Por los autores

✓ Se ingresa el nombre del usuario, nombre de la empresa y key.

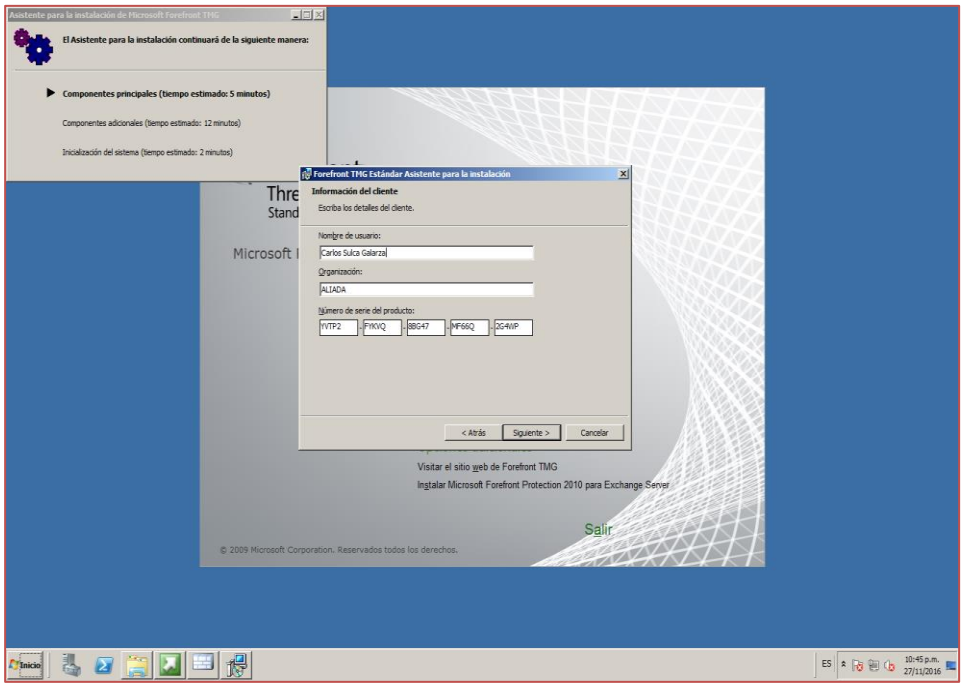


Figura 63: Ingreso de datos para la instalación
Elaborado: Por los autores

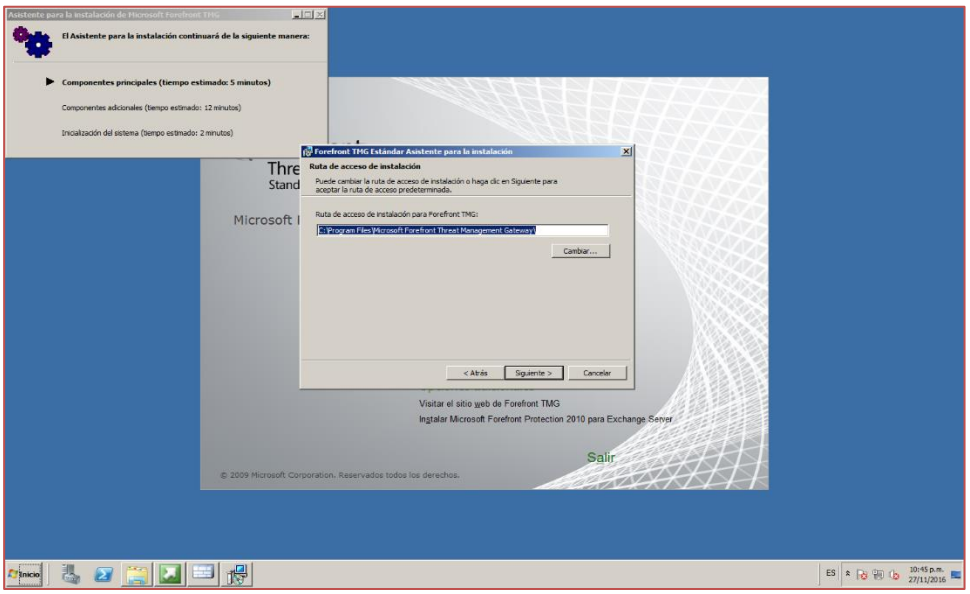


Figura 64: Ruta de instalación
Elaborado: Por los autores

✓ Definición de la red Interna.

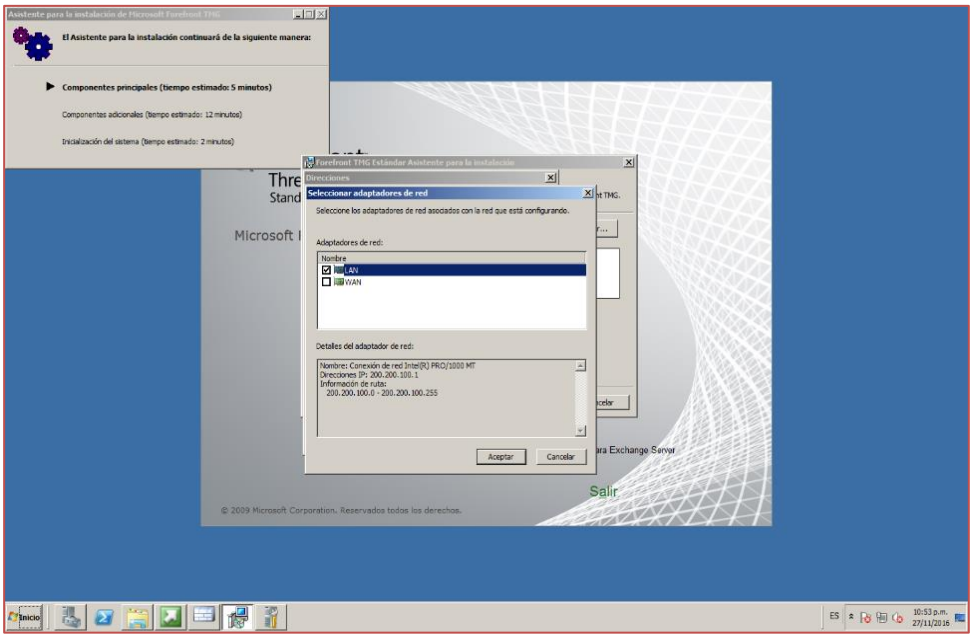


Figura 65: Definición de la red Interna
Elaborado: Por los autores

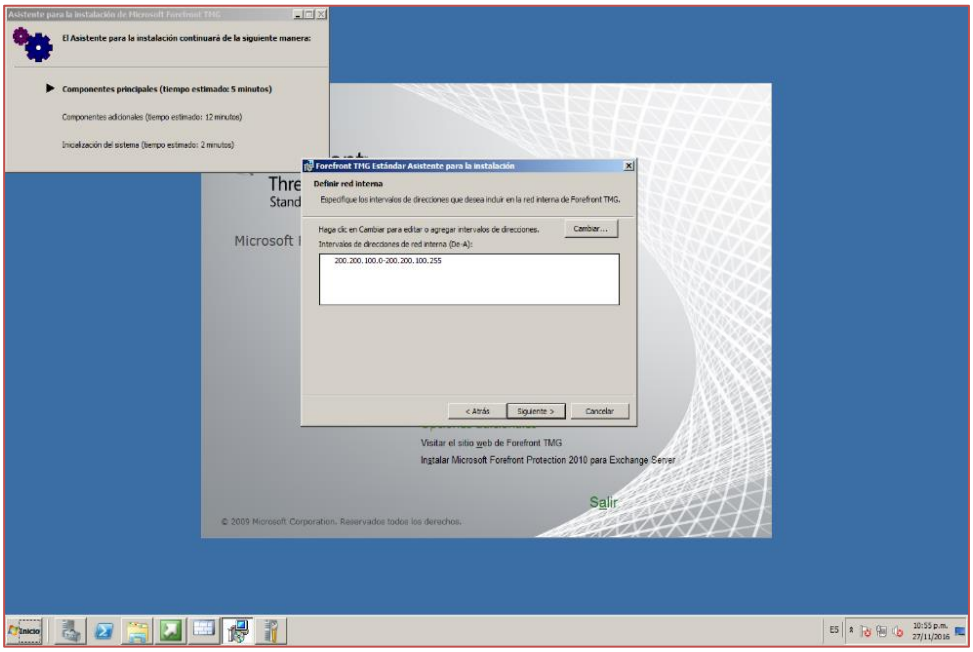


Figura 66: Red Interna
Elaborado: Por los autores

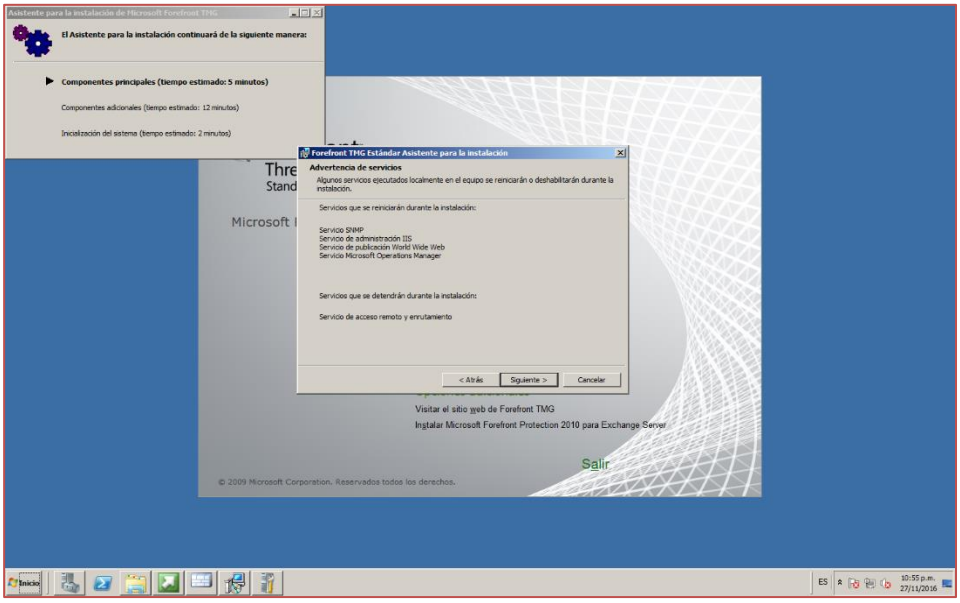


Figura 67: Servicios que se instalaran
Elaborado: Por los autores

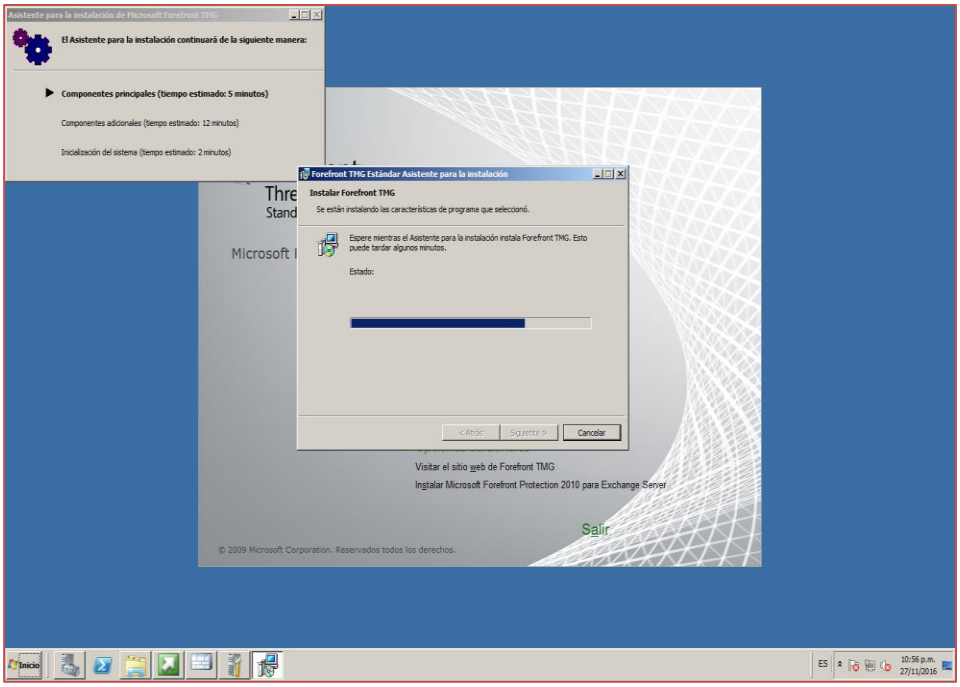


Figura 68: Progreso de instalación
Elaborado: Por los autores

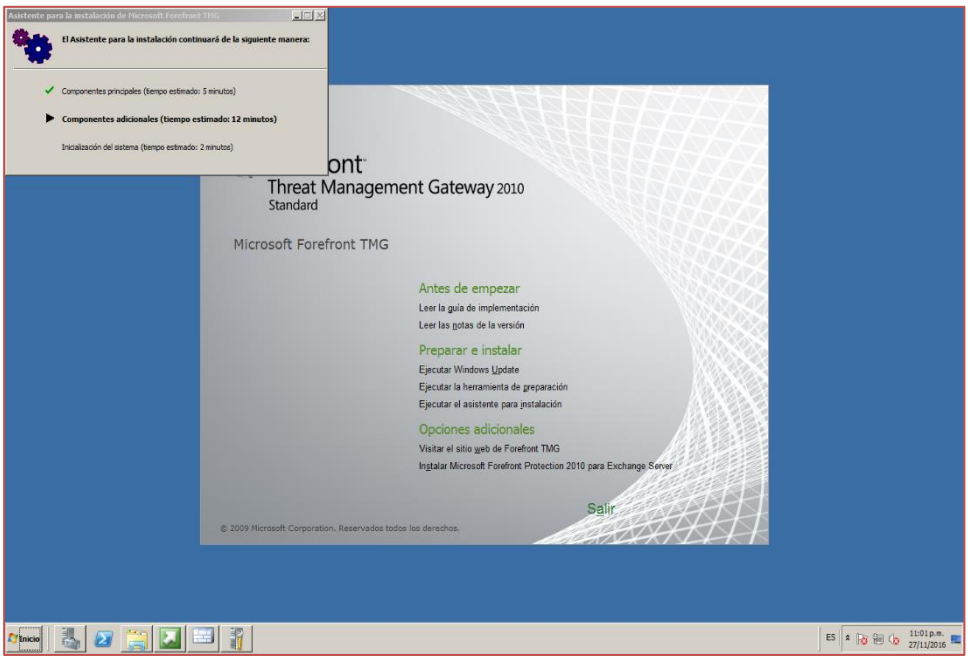


Figura 69: Verificación de componentes adicionales
Elaborado: Por los autores

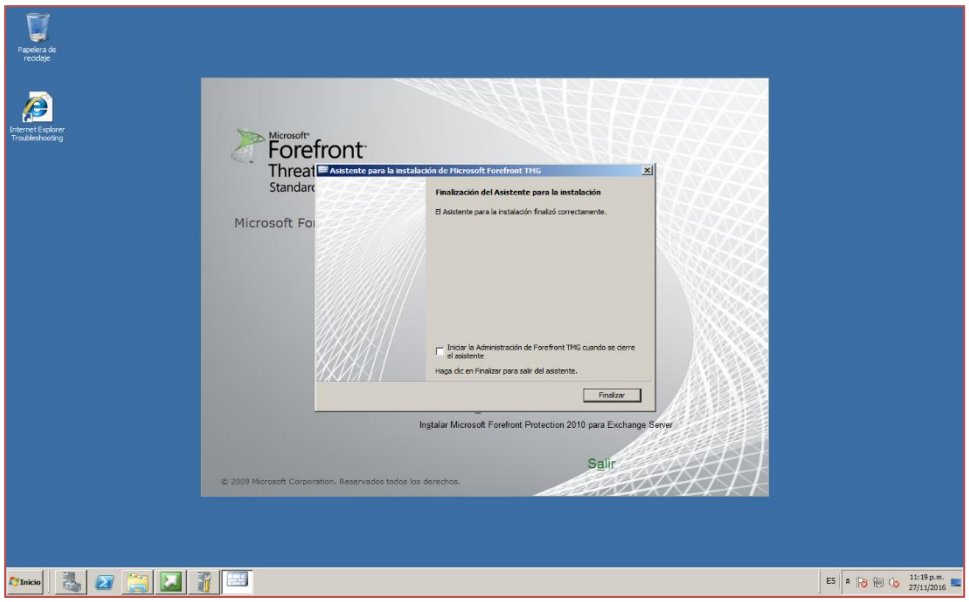


Figura 70: Finalización de la instalación
Elaborado: Por los autores

✓ Configuraciones de red.

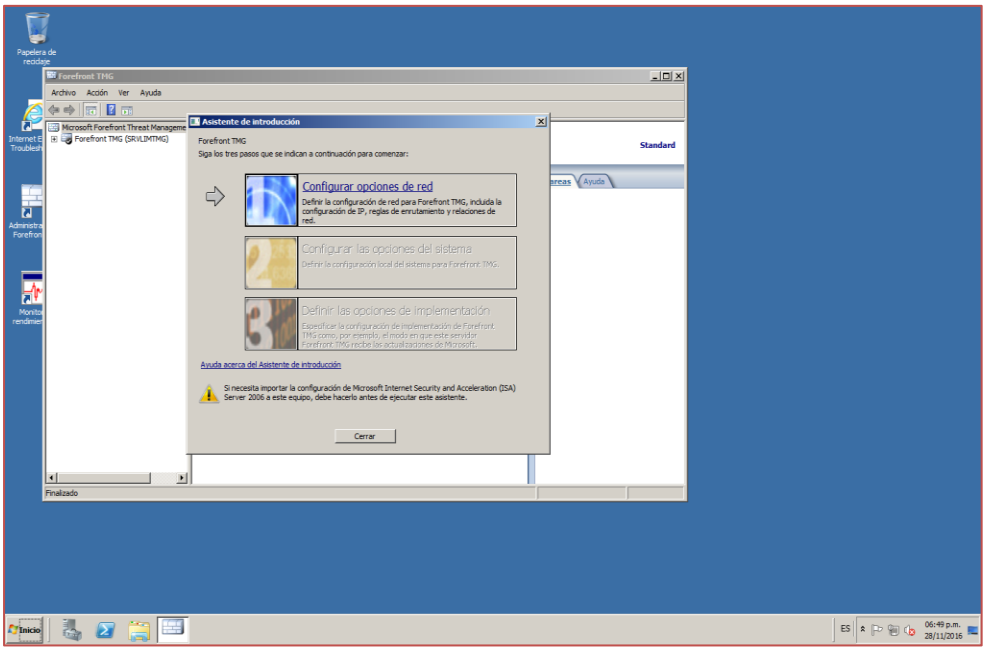


Figura 71: Configuración de Red
Elaborado: Por los autores

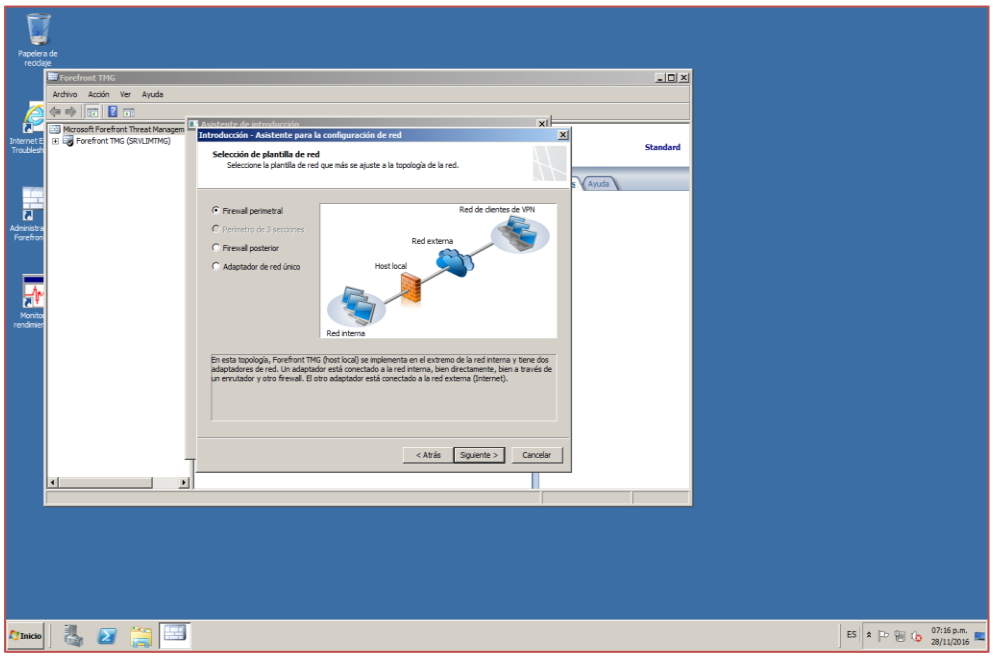


Figura 72: Elección del modo de trabajo del Firewall
Elaborado: Por los autores

✓ Configuración de la red Interna.

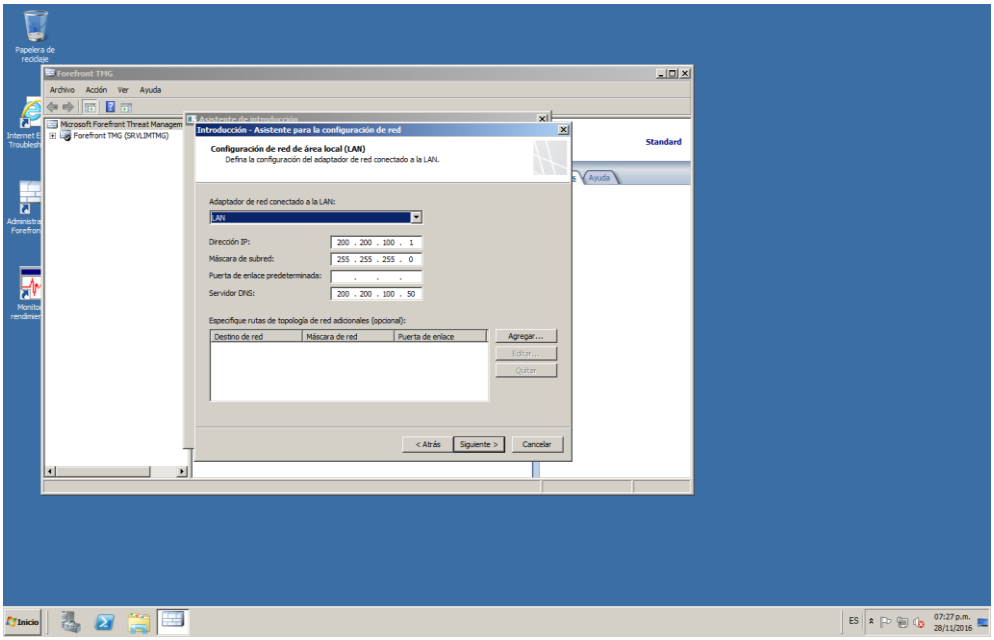


Figura 73: Configuración de la red interna
Elaborado: Por los autores

✓ Configuración de la red Externa.

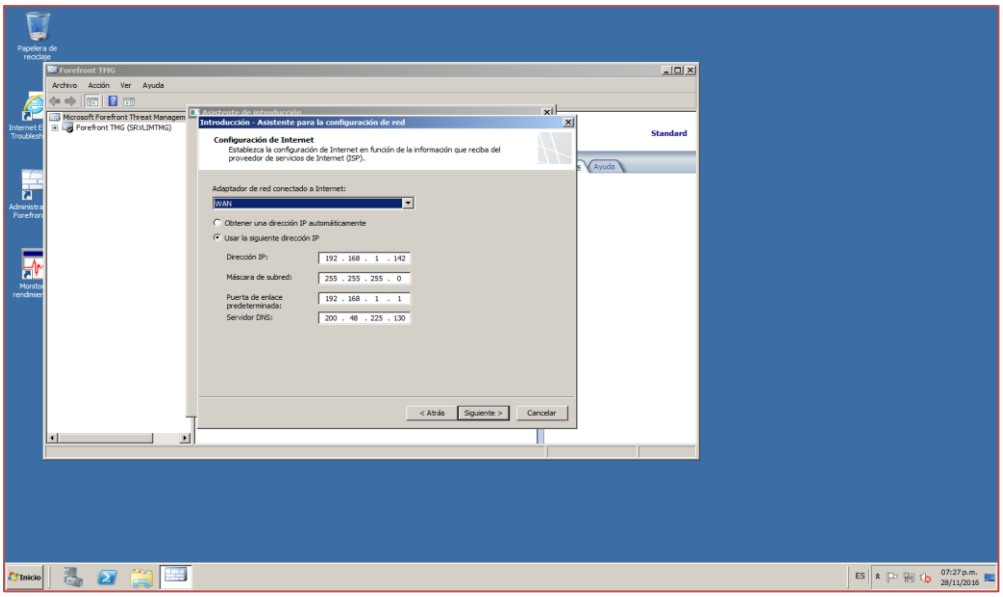


Figura 74: Configuración de la red externa

Elaborado: Por los autores

✓ Configuraciones del Sistema.

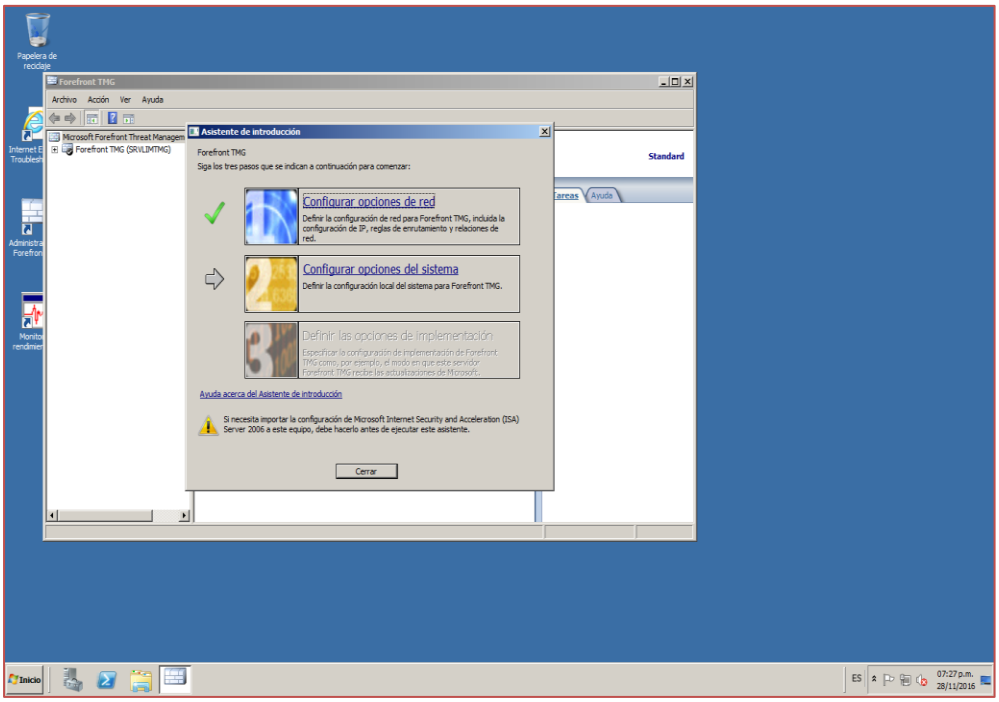


Figura 75: Configuraciones del sistema
Elaborado: Por los autores

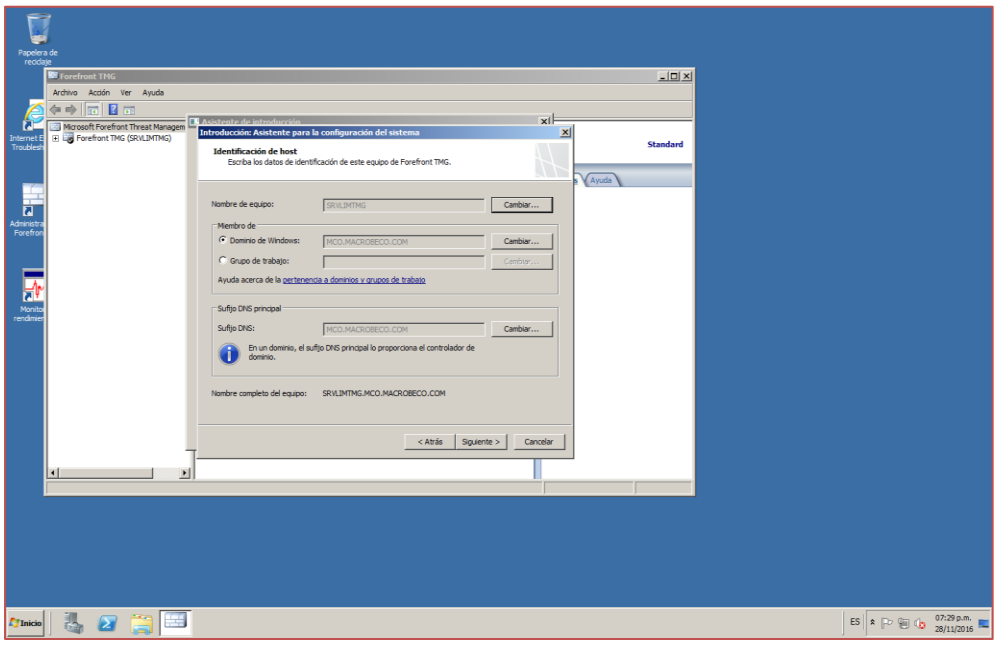


Figura 76: Configuraciones del dominio
Elaborado: Por los autores

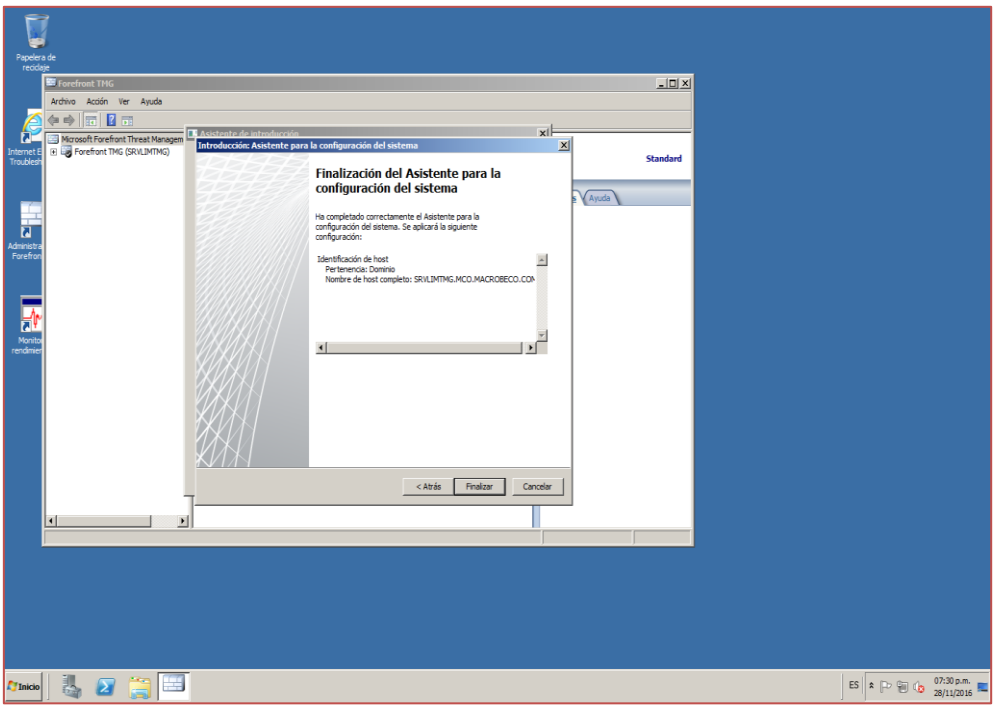


Figura 77: Finalización de la instalación y Configuración del Firewall

Elaborado: Por los autores

✓ Aplicación de Políticas de Seguridad.

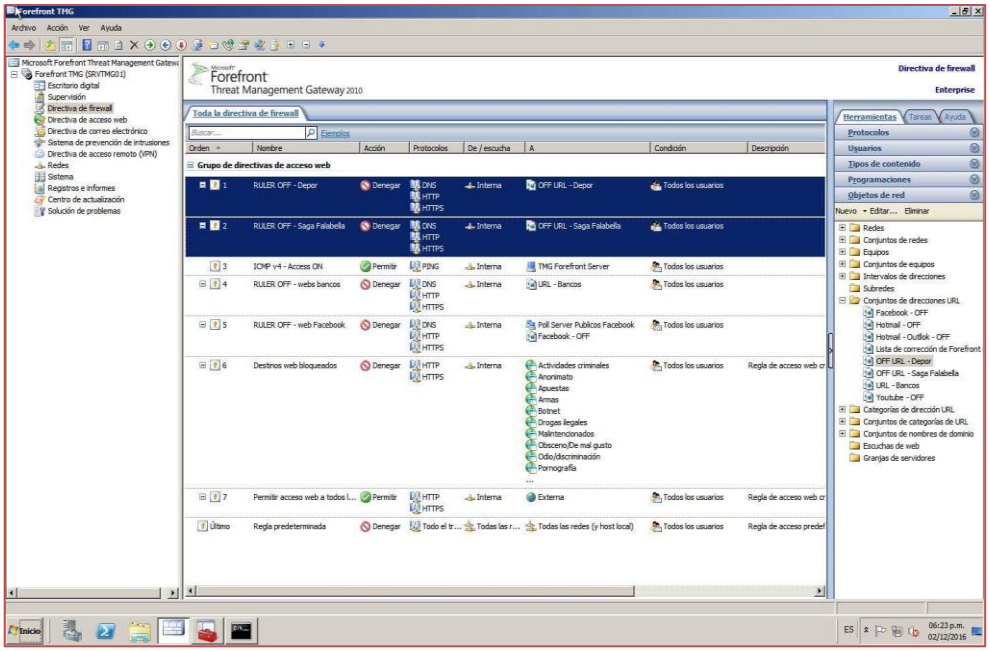


Figura 78: Políticas de Seguridad

Elaborado: Por los autores

En la imagen anterior se visualiza la aplicación de las políticas de seguridad, como se observa las páginas de **Depor, Falabella, Facebook, Bancos** están bloqueados para todos los usuarios.

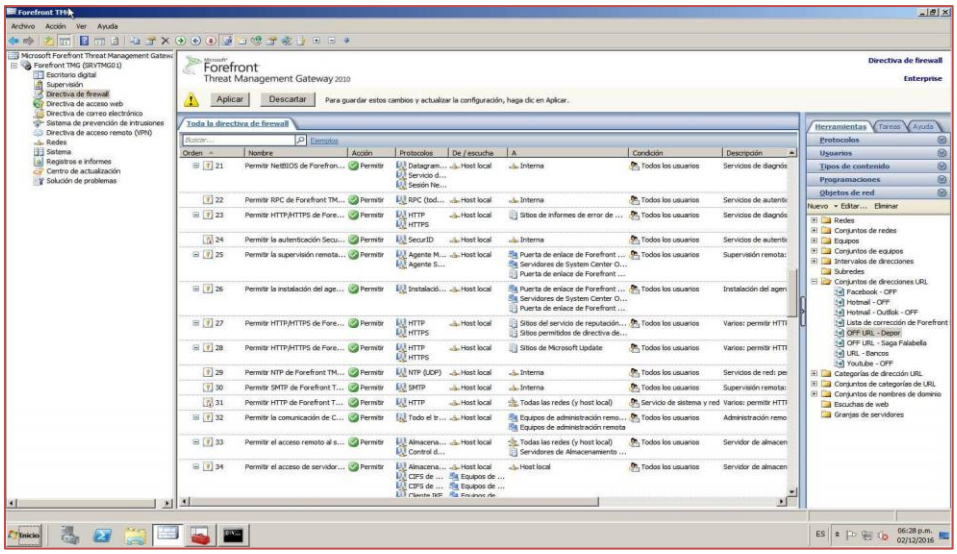


Figura 79: Políticas de Seguridad Adicionales
Elaborado: Por los autores

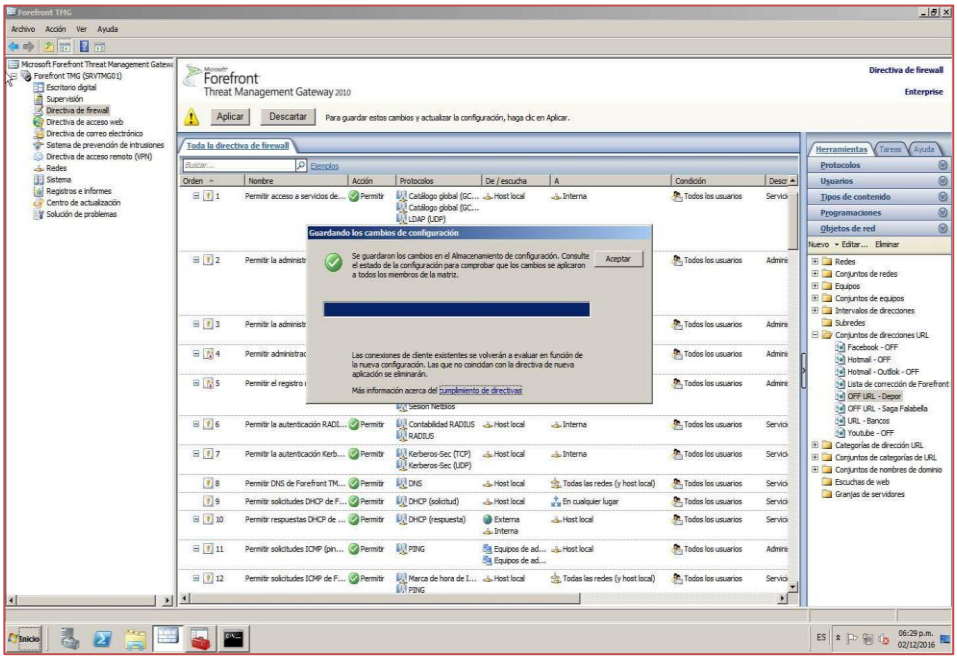


Figura 80: Guardado de Políticas de Seguridad
Elaborado: Por los autores

4.2 Fase de Operación

4.2.1 Pruebas de Protección

Se valida que el servicio de antivirus del Firewall está activo para brindar la protección ante ataques de virus informáticos.

✓ Verificación de la activación del servicio de antispam.

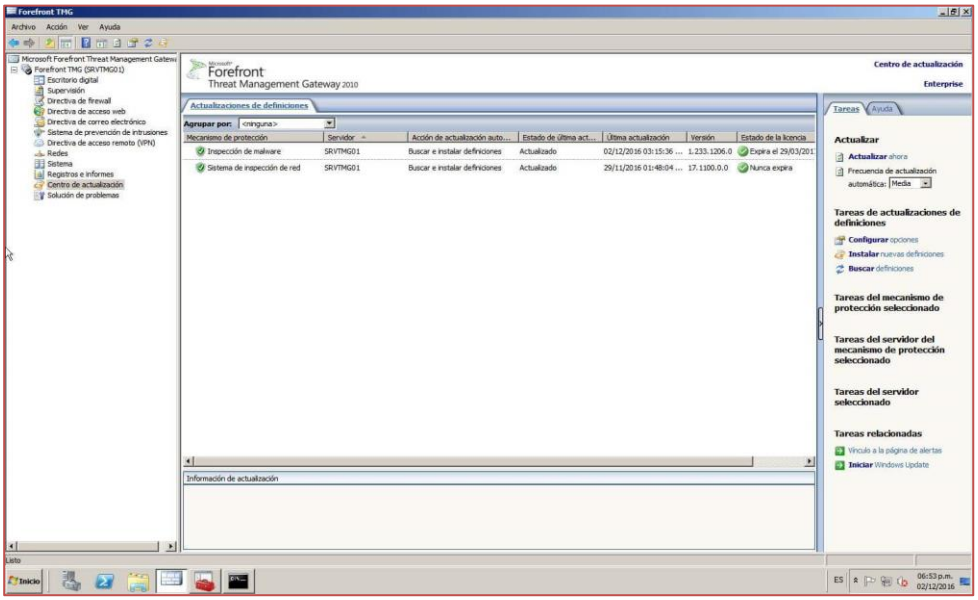


Figura 81: Verificación del Servicio Antispam
Elaborado: Por los autores

La siguiente imagen es una muestra de detección de un virus.

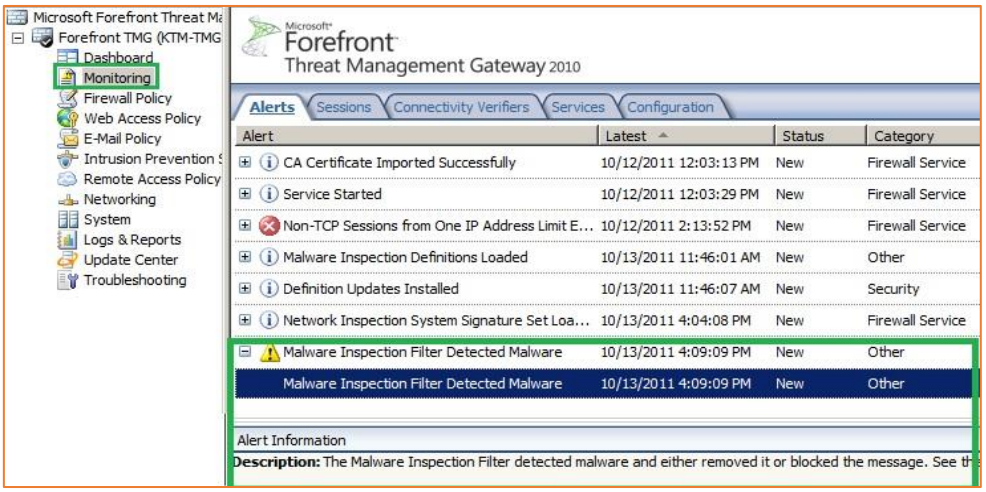


Figura 82: Virus detectado por Servicio Antispam
Elaborado: Por los autores

4.2.2 Pruebas de Ejecución de Políticas de Seguridad

Caso 1. Se valida el acceso libre a páginas deportivas como la página web www.depor.pe, se muestra el acceso a continuación.

Figura 83: Verificación de acceso libre a página Deportivas
Elaborado: Por los autores

Después de aplicado las políticas se verifican el bloqueo de la página web.

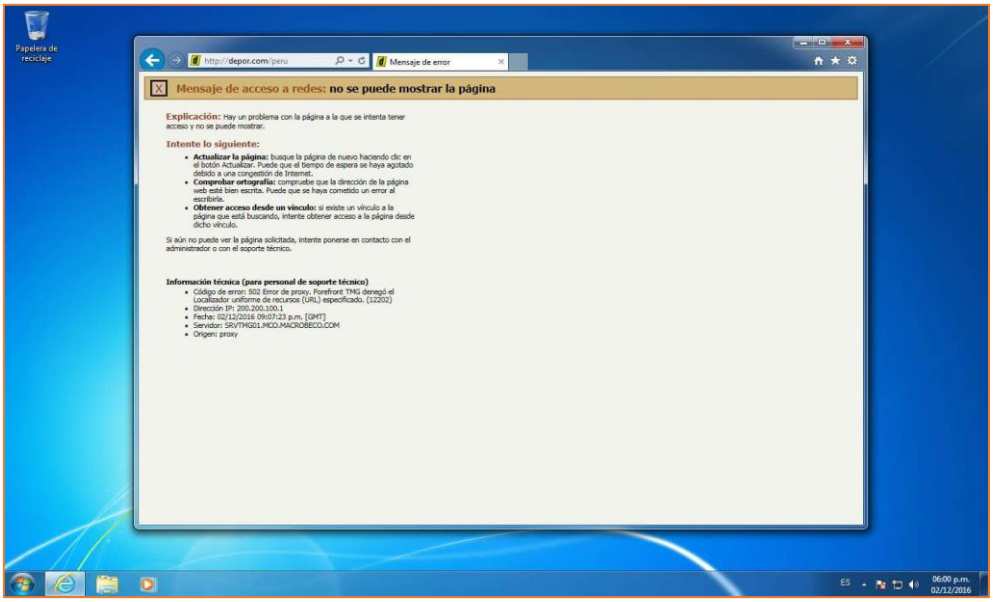


Figura 84: Verificación de políticas de seguridad
Elaborado: Por los autores

Caso 2. Se valida el acceso libre a páginas de comercio como la página web www.falabella.com.pe , se muestra el acceso a continuación.

Figura 85: Verificación de acceso libre a página de Comercio
Elaborado: Por los autores

Después de aplicado las políticas se verifican el bloqueo de la página web.

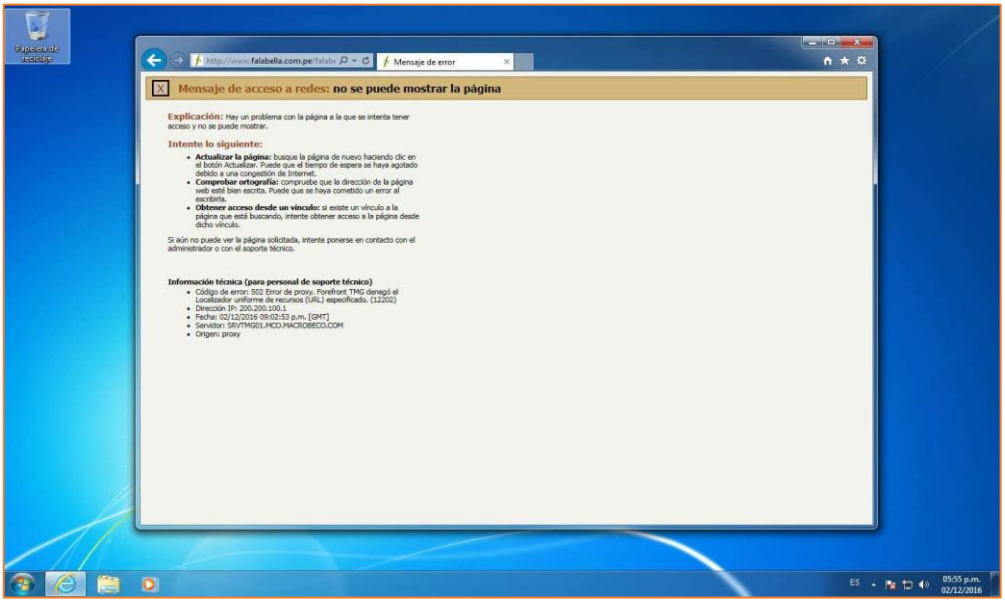


Figura 86: Verificación de políticas de seguridad
Elaborado: Por los autores

Caso 3. Se valida el bloqueo a la página de red social www.facebook.com.pe , se muestra el acceso a continuación.

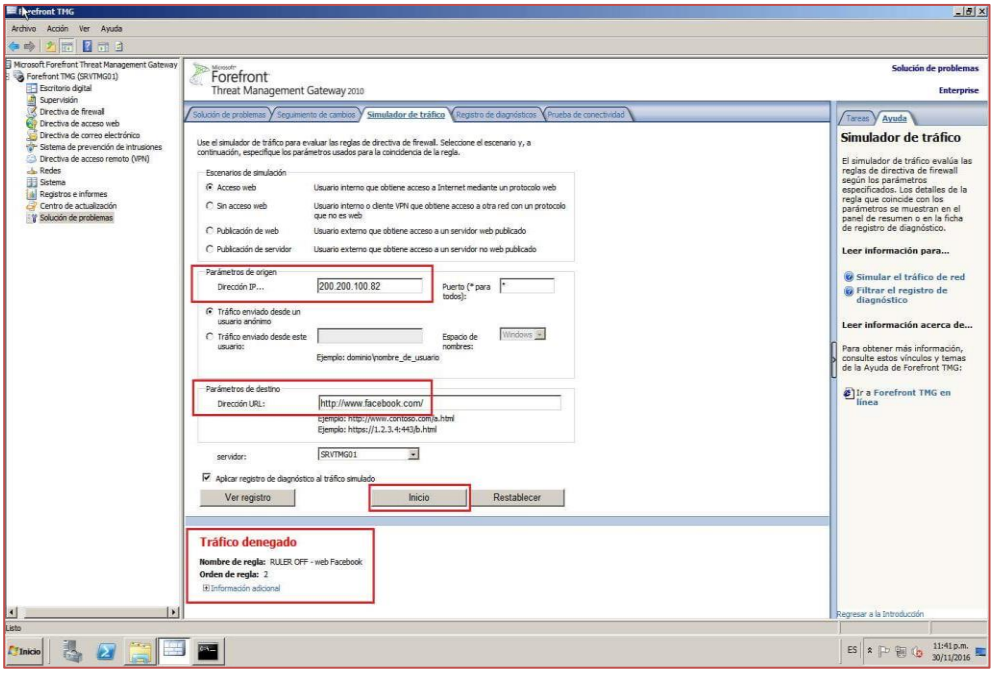


Figura 87: Validación de Políticas de Seguridad
Elaborado: Por los autores

4.2.3 Administración de Conexiones VPN

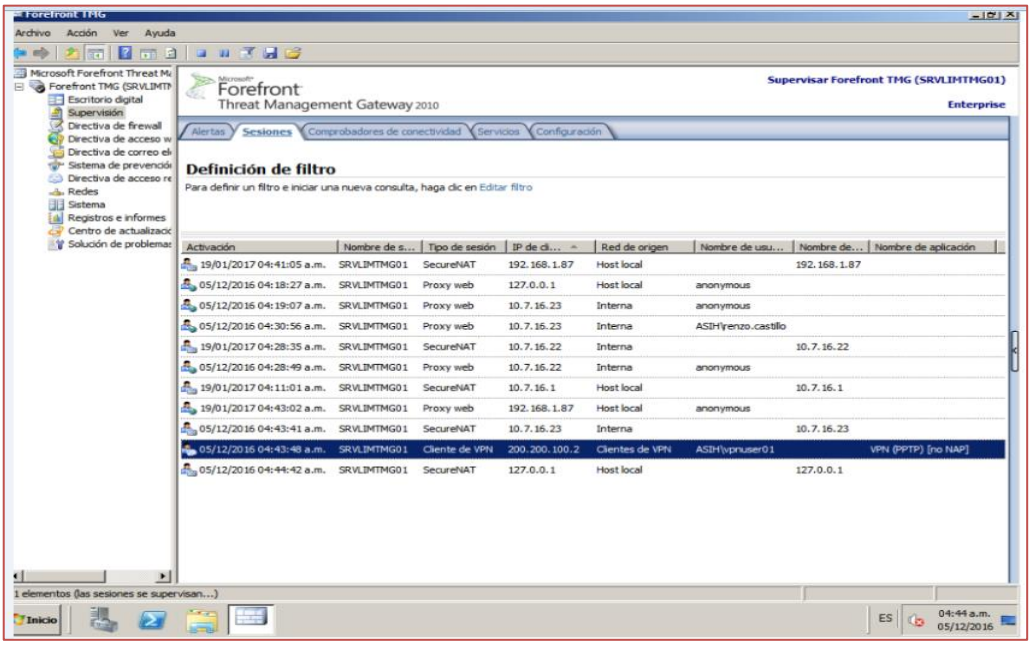


Figura 88: Validación de Conexión VPN
Elaborado: Por los autores

4.3 Fase de Optimización

4.3.1 Administración y Monitoreo de la red

Para tener una administración centralizada el firewall TMG Forefront permite gestionar fácilmente la aplicación de políticas de seguridad como también realizar un monitoreo en tiempo real de la navegación de los usuarios, facilitando la detección de vulnerabilidades en la gestión de políticas de seguridad, etc.

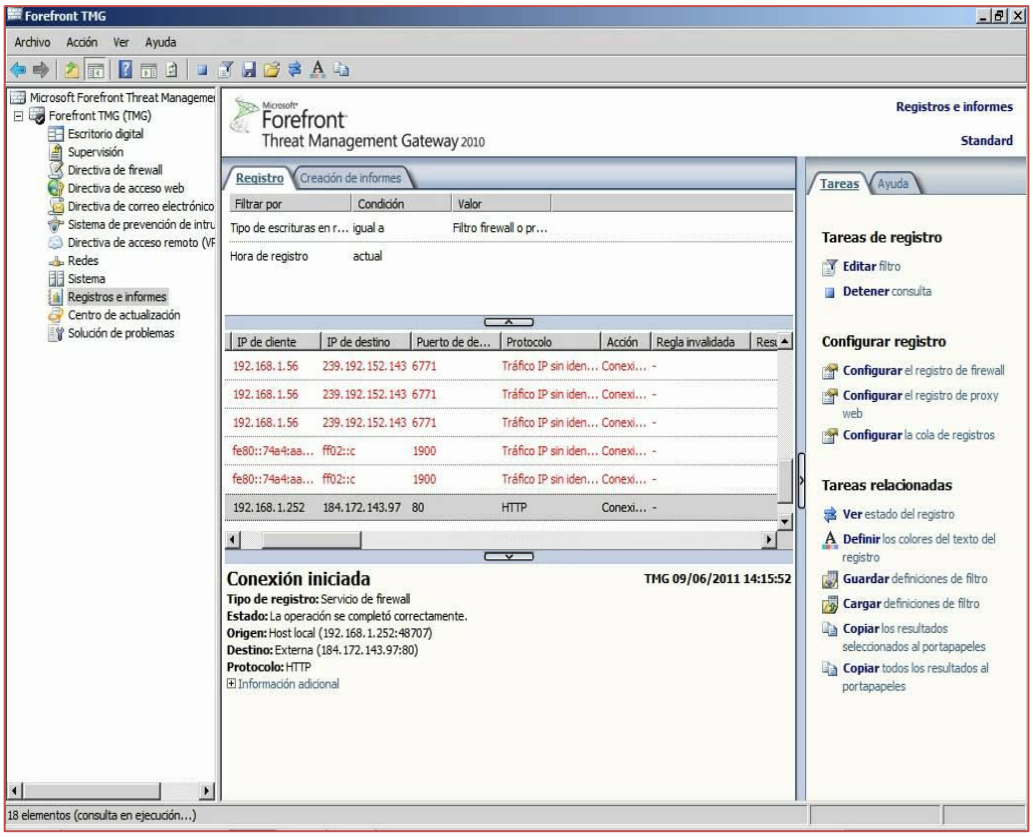


Figura 89: Monitoreo en tiempo real
Elaborado: Por los autores

El TMG Forefront también nos muestra un gráfico de picos de consumo de ancho de banda permitiéndonos visualizar de una manera dinámica el consumo del ancho de banda de internet.

✓ Verificación de la optimización del ancho de banda.

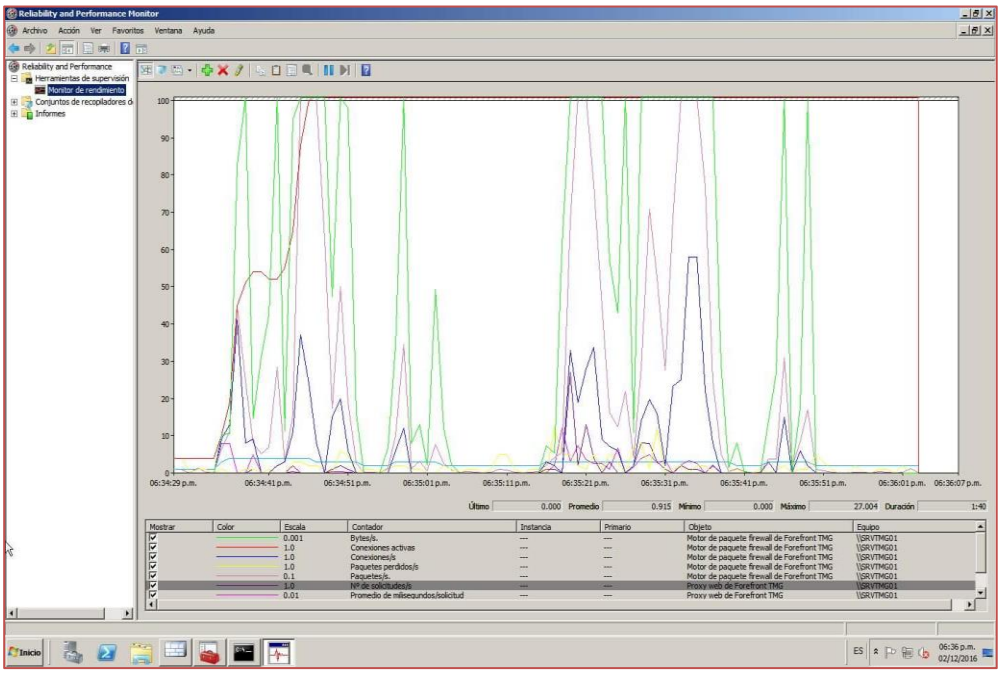


Figura 90: Verificación del Ancho de Banda
Elaborado: Por los autores

“IMPLEMENTACIÓN DE UN FIREWALL TMG FOREFRONT PARA LA SEGURIDAD PERIMETRAL DE LA RED DE DATOS DE LA CLÍNICA ALIADA”

Capítulo V: INTRODUCCIÓN A LA INVESTIGACIÓN CIENTIFICA

5.1 Introducción a la Investigación Científica

Según **Isaac Asimo**, la investigación científica, en su versión ideal, consiste en:

- Detectar la existencia de un problema.
- Separar luego y desechar los aspectos no esenciales.
- Reunir todos los datos posibles que incidan sobre el problema, mediante la observación simple y experimental.
- Elaborar una generalización provisional que los describa de la manera más simple posible: un enunciado breve o una formulación matemática. Esto es una hipótesis.
- Con la hipótesis no se pueden predecir los resultados de experimentos no realizados aún. Ver con ellos si la hipótesis es válida.
- Si los experimentos funcionan, la hipótesis sale reforzada y puede convertirse en una teoría o una ley natural.

Para **Mario Bunge**, la investigación científica, manifiesta que la ciencia es un estilo de pensamiento y de acción, y en toda creación humana, se tiene que distinguir en la ciencia el trabajo de investigación y su producto final, que es el conocimiento. Una clasificación de las ciencias propuesta por M. Bunge, es:

A) Ciencia Formal o Pura: Lógica y Matemática.

B) Ciencia Fáctica o Aplicada:

B.1 Ciencias Naturales: Física, Química, Biología, Psicología, etc.

B.2 Ciencias Sociales y Culturales: Sociología, Economía, Ciencia Política, Historia, etc.

CIENCIA	
Formal o Pura	**Fáctica o Aplicativa**
✓ No se ocupa de los hechos. ✓ Sus objetivos son formas e ideas. ✓ Sus enunciados son relacionados entre signos.	✓ Se ocupa de la realidad y sus hipótesis se adecúan a los hechos. ✓ Sus objetivos son materiales. ✓ Sus enunciados se refieren a sus sucesos y procesos.
MÉTODO	
La Lógica, para demostrar o probar rigurosamente los teoremas propuestos.	La observación y la experimentación, para verificar y confirmar si un enunciado es adecuado a su objeto.

Tabla 21: Diferencia entre Ciencia Formal y Fáctica

Elaborado: Por los autores

Según los Autores *"La investigación científica es el proceso que procura obtener información relevante para entender, verificar, corregir o aplicar el conocimiento.*

El investigador parte de planteamientos, proposiciones o respuestas en torno al problema que le ocupa planeando una metodología, recogiendo, registrando y analizando los datos obtenidos, y de no existir estos instrumentos el investigador debe crearlos."

Ambos conceptos sobre la investigación científica engrandecen el presente Proyecto brindando sólidos conocimientos para la formulación de la metodología Aplicativa la cual nos permitió realizar el proceso Experimental en la cual levantamos información referente al problema del Cliente generando diversas hipótesis más cercanas a la necesidad que cuenta el Cliente, esto nos permitirá tener una base sólida para la llevar acabo nuestro proyecto de implementación de firewall TMG Forefront sin inconvenientes.

5.2 Validación de Expertos

JUICIO DE EXPERTOS, PARA DETERMINAR LA APLICACION DE LA METODOLOGIA DE DESARROLLO

TABLA DE EVALUACION DE EXPERTOS

Apellidos y Nombres del Experto: Suyo Rojas Jean Pablo

Titulo y/o Grado:

Ph.D.. ( ) Doctor.... ( ) Magister....(X) Ingeniero.....( ) Otros.....especifique

Universidad que labora: Universidad Las Americas

Fecha: 01/12/16

TITULO DE TESIS

IMPLEMENTACIÓN DE UN FIREWALL CON TMG FOREFRONT PARA LA MEJORA DE GESTIÓN, ADMINISTRACIÓN Y SEGURIDAD PERIMETRAL DE LA RED DE DATOS DE LA CLÍNICA ALIADA

Tabla de Evaluación de Expertos para la elección de la metodología

En esta tabla de evaluación de expertos usted podrá calificar las metodologías relacionadas a esta investigación mediante una pequeña encuesta que tendrá que poner una calificación.

c	PREGUNTAS	METODOLOGIAS		
		CISCO	INEI	MICROSOFT
1	Mejor estructura metodológica	9	5	7
2	Permite un proceso fácil de adaptabilidad	9	3	8
3	Más enfocada a la escalabilidad	9	4	8
4	Asegura la flexibilidad en la red	9	5	6
	Total	36	17	29

Evaluar con la siguiente calificación:

1 – 3: Malo 4 – 6: Regular 7 – 10: Bueno

Firma del Experto

DNI: 43485095

JUICIO DE EXPERTOS, PARA DETERMINAR LA APLICACION DE LA METODOLOGIA DE DESARROLLO

TABLA DE EVALUACION DE EXPERTOS

Apellidos y Nombres del Experto: Ruiz Sanchez Félix Alexis

Titulo y/o Grado:

Ph.D.. ( ) Doctor.... ( ) Magister....(X) Ingeniero.....( ) Otros.....especifique

Universidad que labora: Las Américas

Fecha: 28/11/16

TITULO DE TESIS

IMPLEMENTACIÓN DE UN FIREWALL CON TMG FOREFRONT PARA LA MEJORA DE GESTIÓN, ADMINISTRACIÓN Y SEGURIDAD PERIMETRAL DE LA RED DE DATOS DE LA CLÍNICA ALIADA

Tabla de Evaluación de Expertos para la elección de la metodología

En esta tabla de evaluación de expertos usted podrá calificar las metodologías relacionadas a esta investigación mediante una pequeña encuesta que tendrá que poner una calificación.

N°	PREGUNTAS	METODOLOGIAS		
		CISCO	INEI	MICROSOFT
1	Mejor estructura metodológica	10	8	8
2	Permite un proceso fácil de adaptabilidad	7	6	7
3	Más enfocada a la escalabilidad	7	6	7
4	Asegura la flexibilidad en la red	9	8	7
	Total	33	28	29

Evaluar con la siguiente calificación:

1 – 3: Malo 4 – 6: Regular 7 – 10: Bueno

Firma del Experto

CIP: 124741

JUICIO DE EXPERTOS, PARA DETERMINAR LA APLICACION DE LA METODOLOGIA DE DESARROLLO

TABLA DE EVALUACION DE EXPERTOS

Apellidos y Nombres del Experto: PACHECO VERA CESAR ABRAHAM

Titulo y/o Grado:

Ph.D.. ( ) Doctor.... ( ) Magister....(X) Ingeniero.....( ) Otros.....especifique

Universidad que labora: UPA

Fecha: 09/01/17

TITULO DE TESIS

IMPLEMENTACIÓN DE UN FIREWALL CON TMG FOREFRONT PARA LA MEJORA DE GESTIÓN, ADMINISTRACIÓN Y SEGURIDAD PERIMETRAL DE LA RED DE DATOS DE LA CLÍNICA ALIADA

Tabla de Evaluación de Expertos para la elección de la metodología

En esta tabla de evaluación de expertos usted podrá calificar las metodologías relacionadas a esta investigación mediante una pequeña encuesta que tendrá que poner una calificación.

c	PREGUNTAS	METODOLOGIAS		
		CISCO	INEI	MICROSOFT
1	Mejor estructura metodológica	8	6	5
2	Permite un proceso fácil de adaptabilidad	9	5	3
3	Más enfocada a la escalabilidad	7	4	3
4	Asegura la flexibilidad en la red	7	5	4
	Total	31	20	15

Evaluar con la siguiente calificación:

1 – 3: Malo 4 – 6: Regular 7 – 10: Bueno

César Pacheco Vera

Firma del Experto

DNI: 42874679

5.3 Planteamiento del Problema

Actualmente con el desarrollo impulsivo de la tecnología a nivel global han surgido diversas soluciones que permiten a las personas comunicarse y desarrollarse en muchos ámbitos en todas las etapas de su vida, día a día estas nuevas tecnologías se actualizan y poco a poco desplazan y se imponen sobre las viejas, este cambio a su vez da lugar a circunstancias que llevan al mal uso de las tecnologías convergentes comprometiendo a la integridad de la información en el ámbito personal y corporativo.

ALIADA es un centro médico especializado en Oncología Integral constituido hace más de 21 años que maneja los más altos estándares internacionales en sus programas de prevención, diagnóstico y tratamiento del cáncer.

La problemática nace del uso que se le da a la tecnología, siendo más específico a los computadores, software e internet. Los usuarios, en este caso los empleados de la clínica Aliada, actualmente tienen la libertad de aprovechar un amplio abanico de comodidades tecnológicas en favor a las funciones que realizan como gestionar su trabajo dentro de la red interna como también a través de la red pública de internet. Esto puede suponer un problema muy relevante si no se cumplen ciertas medidas de seguridad para evitar las violaciones de datos que se puedan irrumpir en la red.

Actualmente la clínica Aliada no cuenta con una solución que permita proteger, gestionar y centralizar la seguridad perimetral y los accesos a nivel LAN y WAN por lo que pone en alto riesgo la confidencialidad de la información y los datos que puedan manejarse, así pues este proyecto se enfoca concretamente a brindar una solución a las necesidades expuestas bajo un escenario empresarial.

En las condiciones y el contexto planteado es obvia la importancia de encontrar una solución al problema de la seguridad, así pues con el estudio de diferentes Firewalls pretendemos implementar una solución que se adapte a los

requerimientos expuestos y nos brinde a su vez numerosas ventajas y propiedades de integración con las tecnologías que actualmente maneja todo el departamento de Sistemas de la clínica Aliada.

La solución que se brindara atacara las diversas necesidades de seguridad de la información dentro de la red perimetral como también tener una medida de control de autenticación de accesos que se pueda tener desde la red externa hacia la red interna, también tener un control sobre la navegación e ingreso a ciertos websites que pongan en riesgo la productividad del personal o la estabilidad de la red interna evitándose alguna manifestación de ataque desde la red externa por medio de hacker o un virus, spyware, malware etc. Otro problema a tratarse será la confidencialidad de la información puesto que actualmente el personal puede acceder libremente a sus correos personales creados en dominios públicos como Hotmail, Gmail, Yahoo, etc. Abriéndose una gran oportunidad para el tráfico ilícito de información interna. Para culminar se manifiesta en este documento la necesidad obligatoria de contar con la implementación y trabajo en la red de un dispositivo de seguridad que permita al área de sistemas mantener la seguridad y el control total sobre toda la infraestructura del parque tecnológico de la clínica Aliada.

5.4 Matriz de Consistencia

ANEXO 1: MATRIZ DE CONSISTENCIA

TÍTULO: IMPLEMENTACIÓN DE UN FIREWALL TMG FOREFRONT PARA LA SEGURIDAD PERIMETRAL DE LA RED DE DATOS DE LA CLÍNICA ALIADA

AUTORES: Carlos Iván Sulca Galarza, Miguel Ángel Dominguez Chávez, Renzo Giancarlo Castillo Palomino.

PROBLEMA	OBJETIVOS	HIPÓTESIS
PROBLEMA PRINCIPAL ¿Cuál es el efecto de la implementación de un Firewall TMG Forefront en la Seguridad perimetral de la red de datos de la Clínica Aliada? **PROBLEMAS SECUNDARIOS:** ¿Cuál es el efecto de la implementación de un Firewall TMG Forefront, en las políticas de seguridad de la red de datos de la Clínica Aliada? ¿Cuál es el efecto de la implementación de un Firewall TMG Forefront, ante posibles ataques de malware y spam en la red de datos de la Clínica Aliada? ¿Cuál es el efecto de la implementación de un Firewall TMG Forefront, en optimizar el ancho de banda de la red de datos de la Clínica Aliada? ¿Cuál es el efecto de la implementación de un Firewall TMG Forefront, en mejorar la calidad de los servicios de tecnologías de la información en la red de Datos de la Clínica Aliada?	**OBJETIVO GENERAL** Implementar un Firewall TMG Forefront para la seguridad perimetral de la red de datos de la Clinica Aliada. **OBJETIVOS ESPECÍFICOS** Implementar el firewall TMG Forefront para las políticas de seguridad en la red de datos de la Clínica Aliada. Implementar el firewall TMG Forefront para ataques de malware y spam en la red de datos de la Clínica Aliada. Implementar el firewall TMG Forefront y optimizar el ancho de banda para la red de datos de la Clínica Aliada. Implementar el firewall TMG Forefront y mejorar la calidad de los servicios de tecnologías de la información en la red de datos de la Clínica Aliada.	**HIPÓTESIS GENERAL** La implementação de un Firewall TMG Forefront mejora la seguridad perimetral de toda la red de datos de la Clínica Aliada? **HIPÓTESIS ESPECÍFICAS** La implementación del Firewall TMG Forefront mejora la gestión de políticas de seguridad para la red de datos de la Clínica Aliada? La implementación del Firewall TMG Forefront mejora la protección ante ataques de virus como malware y spam para la red de datos de la Clínica Aliada? La implementación del Firewall TMG Forefront mejorara el ancho de banda de la red de datos de la Clínica Aliada? La implementación del Firewall TMG Forefront mejorara los servicios de TI en la red de datos de la Clínica Aliada?

VARIABLES E INDICADORES

Variable Independiente: IMPLEMENTACIÓN DE UN FIREWALL TMG FOREFRONT

Dimensiones	Indicadores	Ítems	Niveles y rangos
Integridad	Casos de manipulación de información no autorizada.	1-3	SIEMPRE CASI SIEMPRE ALGUNAS VECES POCAS VECES NUNCA
Confidencialidad	Casos de divulgación de información no autorizada.	4-6	
Disponibilidad	Casos de problemas de servicios TI.	7-10	

Variable Dependiente: SEGURIDAD PERIMETRAL DE LA RED DE DATOS DE LA CLINICA ALIADA

Dimensiones	Indicadores	Ítems	Niveles y rangos
Políticas de Seguridad	Número de casos de usuarios que vulneren las políticas >1	11-13	SIEMPRE CASI SIEMPRE ALGUNAS VECES POCAS VECES NUNCA
Anti-Malware	Número de virus detectados en el Firewall >1	13-16	
Optimización de Ancho de Banda	Tiempo de respuesta en acceder a páginas web=5 segundos	16-19	
Calidad de los servicios de TI en los procesos de la Clínica	Tiempo de atención al paciente <180 segundos	20-22	

<table>
<tr>
<th>TIPO Y DISEÑO DE INVESTIGACIÓN</th>
<th>POBLACIÓN Y MUESTRA</th>
<th>TÉCNICAS E INSTRUMENTOS</th>
<th>ESTADÍSTICA DESCRIPTIVA E INFERENCIAL</th>
</tr>
<tr>
<td>TIPO: APLICADO
Por las características de la presente investigación reúne las condiciones metodológicas de una investigación tipo experimental. Se ejecutará a partir de una situación problemática real, abordándose con la construcción teórica en que se fundamenta para la elaboración y verificación de la hipótesis. El nivel de la investigación es explicativa y aplicada.
NIVEL: Explicativo.
DISEÑO: EXPERIMENTAL
El diseño de la investigación es experimental porque habrá manipulación de variables independientes y estas se miden o recolectan a través del tiempo en puntos o periodos especificados para hacer inferencias respecto al cambio en las variables dependientes.</td>
<td>POBLACIÓN:

Constituído por 60 personas.

TIPO DE MUESTRA: Censal.

TAMAÑO DE MUESTRA:

Grupo control: 30
Grupo experimental: 30
Total de muestra: 60

<table>
<tr><th>Perfil de Pers.</th><th>Número</th></tr>
<tr><td>Administrativos</td><td>20</td></tr>
<tr><td>Enfermeras</td><td>10</td></tr>
<tr><td>Cajeras</td><td>5</td></tr>
<tr><td>Médicos</td><td>21</td></tr>
<tr><td>Gerentes</td><td>4</td></tr>
<tr><td>Total de Censados</td><td>60</td></tr>
</table>
</td>
<td>Variable Independiente:

IMPLEMENTACIÓN DE UN FIREWALL TMG FOREFRONT

Instrumentos:

Autores: Carlos Iván Sulca Galarza, Miguel Ángel Domínguez Chávez, Renzo Giancarlo Castillo Palomino.

Año: 2016
Cuestionario: Diciembre – Enero 2017
Ámbito de Aplicación: Clínica Aliada
Forma de Administración: Directa

Variable Dependiente: SEGURIDAD PERIMETRAL DE LA RED DE DATOS DE LA CLINICA ALIADA

Técnicas: Prueba

Instrumentos:

Autores: Carlos Iván Sulca Galarza, Miguel Ángel Domínguez Chávez, Renzo Giancarlo Castillo Palomino.

Año: 2016
CheckList: Diciembre – Enero 2017
Âmbito de Aplicación: Clínica Aliada.
Forma de Administración: Directa</td>
<td>DESCRIPTIVA: De distribución de frecuencia, tablas de contingencia, figuras

DE PRUEBA:

Prueba hipótesis

Para Torres (1997) “La hipótesis es un planteamiento que establece una relación entre dos o más variables para explicar y, si es posible, predecir probabilísticamente las propiedades y conexiones internas de los fenómenos o las causas y consecuencias de un determinado problema” (p. 129)

U de Mann-Whitney o Prueba T
Aún falta ver cómo están distribuidos los datos.</td>
</tr>
</table>

Tabla 22: Matriz de Consistencia
Elaborado: Por los autores

5.5 Método de Investigación

Tipo de Investigación: Aplicativo

La investigación científica aplicada se propone transformar el conocimiento 'puro' en conocimiento útil. Tiene por finalidad la búsqueda y consolidación del saber y la aplicación de los conocimientos para el enriquecimiento del acervo cultural y científico, así como la producción de tecnología al servicio del desarrollo integral de las naciones. La investigación aplicada puede ser Fundamental o Tecnológica.

La aplicada fundamental, se entiende como aquella investigación relacionada con la generación de conocimientos en forma de teoría o métodos que se estima que en un período mediato podrían desembocar en aplicaciones al sector productivo.

La investigación aplicada tecnológica, se entiende como aquella que genera conocimientos o métodos dirigidos al sector productivo de bienes y servicios, ya sea con el fin de mejorarlo y hacerlo más eficiente, o con el fin de obtener productos nuevos y competitivos en dicho sector.

Por las características de la presente investigación reúne las condiciones metodológicas de una investigación tipo experimental. Se ejecutará a partir de una situación problemática real, abordándose con la construcción teórica en que se fundamenta para la elaboración y verificación de la hipótesis. El nivel de la investigación es explicativa y aplicada.

Nivel de Investigación: Explicativo

La Investigación Explicativa pretende establecer las causas de los eventos, sucesos o fenómenos que se estudian. Están dirigidos a responder por las causas de los eventos y fenómenos físicos o sociales. Su principal interés es explicar porque ocurre un fenómeno y en qué condiciones se manifiesta o porque se relacionan dos o más variables. Mediante este tipo de investigación que requiere la combinación de los métodos analítico y sintético, en conjunto con el deductivo y el inductivo, se trata de responder o dar cuenta del porqué del objeto que se investiga.

Diseño de Investigación: Experimental

El diseño experimental es una técnica estadística que permite identificar y cuantificar las causas de un efecto dentro de un estudio experimental. En un diseño experimental se manipulan deliberadamente una o más variables, vinculadas a las causas, para medir el efecto que tienen en otra variable de interés. El diseño experimental prescribe una serie de pautas relativas qué variables hay que manipular, de qué manera, cuántas veces hay que repetir el experimento y en qué orden para poder establecer con un grado de confianza predefinido la necesidad de una presunta relación de causa-efecto.

IMPLEMENTACIÓN DE UN FIREWALL TMG FOREFRONT PARA LA SEGURIDAD PERIMETRAL DE LA RED DE DATOS DE LA CLÍNICA ALIADA”

Capítulo VI: CONCLUSIONES

6.1 Conclusiones

- Mediante la implementación del Firewall TMG Forefront se espera minimizar los riesgos de ataques de malware y spam para toda la red de datos de la clínica Aliada.

- Mediante la implementación del Firewall TMG Forefront se espera mejorar la gestión de políticas de seguridad bajo la ISO 27001 (Seguridad de la Información) la cual nos facilitaría un estándar en la aplicación de políticas a los usuarios de la red de datos de la Clínica Aliada.

- Mediante la implementación del Firewall TMG Forefront se obtendrá un servicio de internet optimizado y veloz, estas mejoras se verán reflejadas al entrar el firewall a producción.

- La evaluación financiera del proyecto estima que nuestro cliente la Clínica Aliada se verá beneficiado en su gestión de seguridad produciendo un trabajo más eficaz de sus colaboradores y mejorando su Calidad de Servicio en todas las áreas de la empresa.

- Mediante la implementación del Firewall TMG Forefront se obtendrá brindar el servicio VPN para usuarios que requieran realizar trabajos desde cualquier ubicación fuera de la empresa, teniendo como uno requisito contar con internet.

6.2 Recomendaciones

- Se recomienda tener activo el servidor de Kaspersky, lo cual nos ayudaría a complementar la seguridad perimetral de la red de datos, formando una doble capa de seguridad fortaleciendo las defensas ante ataque de malware y spam.

- Se recomienda al área de Sistemas de la Clínica Aliada realizar una auditoría de permisos de accesos a páginas, uso de aplicaciones entre otros por lo menos cada 6 meses para llevar una mejor gestión de seguridad.

- Se recomienda al área de Sistemas de la Clínica Aliada realizar un test de performance del servicio de internet, para verificar su estado y medir la calidad de servicio que se brinda a los usuarios finales, si existen anomalías procederían a ejecutar un plan de acción para su corrección.

- Se recomienda al área de Sistemas de la Clínica Aliada proponer el desarrollo de un nuevo proyecto para implementar un firewall de contingencia, la cual ofrecería un beneficio importante a su empresa si hubiese caídas de internet con su proveedor.

- Se recomienda al área de Sistemas otorga accesos VPN a usuarios que necesiten urgentemente este servicio, lo ideal sería otorgarlo a usuarios VIP de la empresa.

ELABORACIÓN DE REFRENCIAS

Libros

Carlos Tori. (2008). Hacking Ético (1ra ed). Argentina.

Christos Kalloniatis. (2012). Security enhanced applications for information systems (1ra Ed). Croacia.

Claudio Hernández, (2001). Hackers 2 Los Piratas del chip y de internet. (1ra Ed). España.

Cisco. (2015). Cisco CCNA Exploration LAN Switching and Wireless (5ta Ed). Estados Unidos.

David B. Cross. (2010). Microsoft Forefront Threat Management Gateway (1ra Ed). Estados Unidos de America.

Iso. (2013). Information Technology-Security techniques-Information security Management systems (2da Ed). Suiza.

Libros en Versión Electrónica

International Organization for Standardization. (2017). Recuperado de**:** http:www.iso.org/iso/

Isc2. Certified Information Systems Security Professional. (2017). Recuperado de: https://www.isc2.org/cissp/default.aspx

Kaspersky. (2017). Recuperado de: https://support.kaspersky.com/kis2017

Anexos

1. Checklist

Plan de Actividades - ONCOCARE								
Item	Actividad	Descripción de la Actividad	Duración(min)	Personal Responsable	Pruebas de la Actividad	Resultado de la		Comentarios
						SI	NO	
1	1.- Reunion : Explicacion del Plan de Trabajo	1.1.- Se explico el plan de trabajo , las pruebas a realizar y la topologia final . Asi mismo algunos riesgos del trabajo a realizar sino se cumplen con el check list del Plan de trabajo .	0.4	Consultores	a) Se identifico riesgos y el impacto para el Negocio	X		
					b) Se identifico la importancia del Soporte de Claro para el retiro del NAT en el Router	X		
					c) Se identifico la importancia de crear la VLAN entre el Firewall y Switch Core propiedad del Cliente	X		
					d) Se identifico la importancia del Ruteo de la Ruta Cero hacia el Firewall en el Switch Core .	X		
2	2.- Validacion de Navegacion y Publicaciones	2.1 .- Se hara consultas a traves de un motor de busquedas desde navegador mozilla y/o Chrome	0.15	Consultores/Cliente	a) Se realizo pruebas de conectividad a distintas paginas local y externas .	X		
		2.2.- Test de Conectividad hacia INTERNET			b) Ping continuo al 8.8.8.8 y visualizar los tiempos de respuesta , elevado ?	X		
		2.2. Se validara desde INTERNET el acceso a la Publicacion .			b) Se logro visualizar el servicio Publicado .	X	X	
3	3.- Proveedor de Claro , retirara NAT del Router	3.1.- Se necesita retirar el NAT en el Router que da Salida a la LAN del ciente , el NATEO lo realizara el Firewall .	0.15	Cliente	a) Se configuro el NAT en el Firewall y no se tiene conflictos de IP .	X		
4	4.- Creacion de Vlans de Acceso en el Switch .	4.1.- Cliente debera configurar una Vlan de acceso y asignar un puerto en sus Switch	0.1	Cliente	a) Se visualiza el Puerto Activo y realiza pruebas de Ping y ARP	X		
5	5.- Asignacion de un Puerto en el Switch de Core para conexión del Firewall.	5.1 .- Cliente nos asignara un puerto en su Switch , para poder recibir las Vlans de sus Sedes Remotas .	0.1	Cliente	a) Se visualiza el Puerto Activo y realiza pruebas de Ping y ARP	X		
6	6.- Puesta en Produccion Firewall Fortinet	6.1.- Se pondra operativo el Firewall , se publicaran los servicios y navegacion de la LAN .	0.1	Consultores	a) Usuarios navegan con las restricciones de sus Perfiles	X		
7	7.- Validacion de los Servicios , Publicaciones y Navegacion de Usuarios	7.1.- Se debera validar la correcta navegacion de parte de los usuarios con los perfiles descritos en la plantilla .7.2.- Se debera validar las publicaciones desde INTERNET y correcto funcionamiento.	0.2	Consultores	a) Usuarios navegan con las restricciones de sus Perfiles			Si el resultado es "NO" , se debera aplicar Plan de Roollback.
8	8.- Rollback	8.1 .- Se desconectara el Firewall Fisicamente del Swicth Core y se realizara la conexión inicial entre Router y el Switch Core	0.3	Consultores	Navegacion de Usuarios			
		8.2.- Se volvera aplicar el NAT en el Router .		Cliente	Navegacion de Usuarios			
		8.3.- Se enrutara en el Switch Core la Ruta Cero hacia el Router .		Cliente	Navegacion de Usuarios			
		Total Horas :	1.5					

2. Kick Off del proyecto

CLIENTE	ONCOCARE		
Proyecto	1600615		
Código	Proyecto 1600615"|PER-000873033	Jefe de Proyecto:	Carlos Sulca
Fecha de seguimiento	15/12/2016	Fase actual del proyecto	Ejecución

A. Participantes del Proyecto

Nro.	PARTICIPANTES	Iniciales	Rol (1)	Asistió	Hora llegada
1	Carlos Sulca	CS	JP	Si	
2	Robert Cañari	RC	JP	SI	
3	Francisco Feliu	FF	DP	Si	

(1) Descripción de Roles

a. Jefe de Proyecto
b. Jefe de Proyecto (Oncocare)
c. Director del Proyecto (Oncocare)

B. Resumen del Proyecto a la fecha (Resumen ejecutivo)

% de Avance: *Valor real. Obtenido del cronograma de actividades.*		**Plazo Actual:** *Tiempo en días que dura el proyecto*	
Fecha Inicio:	21/11/2016	**Fecha Fin:**	14/03/2017

C. Actividades Realizadas

Revisión de los acuerdos de la semana anterior:	
Avance a la fecha:	- Kick off con cliente.
Hitos terminados:	
Entregables por vencer:	*Escenario a utilizarse*

D. Seguimiento de Compromisos y Stakeholders

Realizar seguimiento a los compromisos asumidos en el Proyecto y a las actividades planificadas en las cuales están involucrados los stakeholders. Si no existieran compromisos deberá documentarse la columna "Compromiso" poniendo "No existen observaciones".

Item	Fecha de Seguimiento	Compromiso	Responsable	Fec. Prog. Acción	Fec. Real Acción	Acción tomada	Estado [1]
1	20/02/2017	Definir diagrama a utilizarse	JP	13/02/2017			P

3. Acta de reunión

Acta de Reunión

Cliente: Robert Cañari Miranda RCM

Consultores TI : Carlos Sulca CS
Miguel Dominguez MD
Renzo Castillo RC

Referencia:

OBJETIVO
Implementar un Firewall TMG Forefront para seguridad Perimetral

ASUNTOS Y ACUERDOS	RESPONSABLE
Enviar la topología actual de la red LAN de Aliada	RCM
Enviar los requisitos para poder rediseñar la topología actual que cuenta Aliada	RC
Rediseñara la red LAN y se mostrara la nueva topología de Aliada	RC
Aceptará el nuevo diseño de la red LAN	RCM

ACTIVIDADES A REALIZAR	RESPONSABLE	FECHA	ESTADO
Enviar la topología actual de la red LAN de Aliada	RCM	29/12/2016	
Enviar los requisitos para poder rediseñar la topología actual que cuenta Aliada	RC	02/01/2017	
Rediseñara la red LAN y se mostrara la nueva topología de Aliada	RC	20/02/2017	
Confirmar cuando se entregara el equipo de seguridad en la sede de Aliada	CS	29/12/2016	

Autor del Acta:

Fecha de edición del acta 06/12/2016

Nota:

Rogamos nos hagan llegar sus comentarios y anotaciones en el plazo de 2 días tras la recepción de la presente acta. Transcurrido este período estimaremos correcta su forma y contenido. Gracias.

4. Cuestionario

CUESTIONARIO						
DIMENSIONES	INDICADORES	VALORES DE LA ESCALA				
		SIEMPRE	CASI SIEMPRE	ALGUNAS VECES	POCAS VECES	NUNCA
		5	4	3	2	1
INTEGRIDAD	**Casos de manipulación de información no autorizada**					
	1. ¿Cree usted que la información que trabaja en carpetas compartidas es correcta y no fue manipulada?					
	2. ¿Cree usted que la información que trabaja en su día a día es coherente?					
	3. ¿Cree usted que la información con la que trabaja en precisa y valida?					
CONFIDENCIALIDAD	**Casos de divulgación de información no autorizada**					
	4. ¿Cree usted que la información con la trabaja es de propiedad de la empresa?					
	5. ¿Cree usted que la información divulgada por algún personal debe ser sancionado?					
	6. ¿Cree usted que la información con la que trabaja puede ser de acceso libre a cualquier usuario?					
DISPONIBILIDAD	**Casos de problemas de servicios TI**					
	7. ¿Cree usted que los servicios de TI de la empresa facilitan su trabajo?					
	8. ¿Cree usted que los servicios de TI deben mejorar?					
	9. ¿Puede mencionar servicios de TI que fallen con frecuencia?					
	10. ¿Sus recursos compartidos suelen no estar disponibles?					
POLITICAS DE SEGURIDAD	**Número de casos de usuários que vulneren las políticas >1**					
	11. ¿Sabe que es la ISO 27001?					
	12. ¿Sabe en que se basa la seguridad de información?					
	13. ¿Cree usted que una capacitación de seguridad informática a nivel de usuario por parte de la Clínica le serviría para la mejora de sus funciones?					
ANTI-MALWARE	**Número de vírus detectados en el Firewall >1**					
	14. ¿Sabe usted protegerse de amenazas de internet?					
	15. ¿Cree usted que las computadoras de la clínica es indispensable tener un antivirus?					
	16. ¿Sabe que es un virus y cuál es su objetivo?					
OPTIMIZACION DEANCHO DE BANDA	**Tiempo de respuesta en acceder a páginas web=5 segundos**					
	17. ¿Usted cree que la velocidad del servicio de internet es óptima?					
	18. ¿Usted cree que su navegación por internet es segura?					
	19. ¿Puede indicar que páginas web necesita para sus labores?					
CALIDAD DE LOS SERVICIOS DE TI EN LOS PROCESO DE LA CLINICIA	**Tiempo de atención al paciente <180 segundos**					
	20. ¿Cree usted que los servicios de TI influyen en su rendimiento laboral?					
	21. ¿Cree usted que los servicios de TI mejoran la calidad de servicio?					
	22. ¿Cree usted que los servicios de TI deben mejorar?					