UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

TRABAJO DE GRADO PREVIO A LA OBTENCIÓN DEL

TÍTULO DE INGENIERA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

TEMA:

"GOBIERNO DE TI BASADO EN EL ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN (EGSI) EN EL HOSPITAL SAN LUIS DE OTAVALO"

AUTORA: CATHERINE LISETH LÓPEZ QUILUMBANGO

DIRECTORA: MSc. SANDRA KARINA NARVÁEZ PUPIALES

IBARRA – ECUADOR

2019

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTA DE INGENIERÍA EN CIENCIAS APLICADAS

CERTIFICACIÓN DEL DIRECTOR

La Srta. Catherine Liseth López Quilumbango, portadora de la cédula de identidad número: 100376918-7, ha trabajado en el desarrollo del proyecto de grado "**GOBIERNO DE TI BASADO EN EL ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN (EGSI) EN EL HOSPITAL SAN LUIS DE OTAVALO"**, previo a la obtención del título en Ingeniería en Electrónica y Redes de Comunicación realizado con interés profesional y responsabilidad, que certifico en honor a la verdad.

Ibarra, 16 de octubre del 2019

.....

MSc. Sandra Narváez

Directora de Trabajo de Grado

UNIVERSIDAD TÉCNICA DEL NORTE

BIBLIOTECA UNIVERSITARIA

AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

1. IDENTIFICACIÓN DE LA OBRA

En cumplimiento del Art. 144 de la Ley de Educación Superior, hago la entrega del presente trabajo a la Universidad Técnica del Norte para que sea publicado en el Repositorio Digital Institucional, para lo cual pongo a disposición la siguiente información:

DATOS DE CONTACTO			
CÉDULA DE IDENTIDAD:	100376918-7		
APELLIDOS Y NOMBRES:	LÓPEZ QUILUMBANGO CATHERINE LISETH		
DIRECCIÓN:	Imbabura – Antonio Ante		
E-MAIL:	cllopezq@utn.edu.ec		
TELÉFONO FIJO:	062-908-817	**TELÉFONO MÓVIL:**	0997165930

DATOS DE LA OBRA	
TÍTULO:	Gobierno de TI basado en el Esquema Gubernamental de Seguridad de la Información (EGSI) en el Hospital San Luis de Otavalo
AUTOR(ES):	LÓPEZ QUILUMBANGO CATHERINE LISETH
FECHA:	16 de Octubre del 2019
PROGRAMA:	■ Pregrado ☐ Posgrado
TÍTULO POR EL QUE OPTA:	Ingeniería en Electrónica y Redes de Comunicación
ASESOR/DIRECTOR:	MSc. Sandra Karina Narváez Pupiales

2. CONSTANCIA

La autora manifiesta que la obra objeto de la presente autorización es original y se desarrolló, sin violar derechos de autor de terceros, por lo tanto, la obra es original y que es la titular de los derechos patrimoniales, por lo que asume la responsabilidad sobre el contenido de la misma y saldrá en defensa de la Universidad en caso de reclamación por parte de terceros.

Ibarra, a los 16 días del mes de octubre del 2019

AUTORA:

.....

Firma

Nombre: Catherine Liseth López Quilumbango

Cédula: 100376918-7

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTA DE INGENIERÍA EN CIENCIAS APLICADAS

AGRADECIMIENTO

A Dios, mi familia, mis tutores, al personal del área de TI del Hospital San Luis de Otavalo, compañeros y a todos quienes hicieron esto posible.

Catherine López

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTA DE INGENIERÍA EN CIENCIAS APLICADAS

DEDICATORIA

A ti, a tu ausencia, a los años sin verte. A ti, que has sido mi mayor inspiración. Hoy la espera ha terminado, estoy a un paso de ti, y voy por ti.

Catherine López

RESUMEN

El presente proyecto consiste en diseñar un Gobierno de TI para el Hospital San Luis de Otavalo enfocado en la Seguridad de la Información el cual permite identificar los procesos que la Institución necesita mejorar con relación al uso de las TI y apoyar al cumplimiento de sus objetivos estratégicos; para ello se realiza el Análisis de Gestión de Riesgos según el estándar NTE INEN-ISO/IEC 27005:2012 donde se determinan los activos de información críticos, se identifican sus principales amenazas y vulnerabilidades, y a partir de los riesgos encontrados se formula una Política de Seguridad de la Información para reducir, controlar o mitigar cada riesgo encontrado.

La Política de Seguridad de la Información se elabora en base a las buenas prácticas del Esquema Gubernamental de Seguridad de la Información (EGSI) y el estándar NTE INEN/ISO 27799:2008, este es un documento de carácter obligatorio que reglamenta el uso adecuado de los equipos informáticos y la información contenida en ellos. Para implementar la Política se utilizarán recursos de hardware y software, de manera especial empleando soluciones basadas en software libre, Pfsense fue el sistema elegido para desempeñar el rol de firewall y brindar servicios como: DNS, Portal Cautivo, RADIUS, VPN y Proxy, optimizando la gestión de la red de datos, el control de accesos de usuarios y el monitoreo de tráfico.

Finalmente se elabora un análisis Costo-Beneficio donde se determina el presupuesto de los recursos que la Institución requiere para la implementación de los servicios propuestos y que contribuirán a que la Política de Seguridad de la Información se cumpla en su totalidad.

ABSTRACT

The present project consists of designing an IT Government for the San Luis de Otavalo Hospital focused on Information Security which allows to identify the processes that the Institution needs to improve in relation to the use of IT and support the fulfillment of its strategic objectives ; for this, the Risk Management Analysis is carried out according to the NTE INEN-ISO / IEC 27005: 2012 standard where critical information assets are determined, their main threats and vulnerabilities are identified, and from the risks found a Information Security Policy is formulated to reduce, control or mitigate every risk encountered.

The Information Security Policy is developed based on the good practices of the Esquema Gubernamental de Seguridad de la Información (EGSI) and the NTE INEN / ISO 27799: 2008 standard, this is a mandatory document that regulates the proper use of the computer equipment and the information contained therein. To implement the Policy, hardware and software resources will be used, especially using solutions based on free software, Pfsense was the system chosen to play the role of firewall and provide services such as: DNS, Captive Portal, RADIUS, VPN and Proxy, optimizing data network management, user access control and traffic monitoring.

Finally, a Cost-Benefit analysis is elaborated which determines the budget of the resources that the Institution requires for the implementation of the proposed services and that will contribute to the Information Security Policy being fully complied with.

INDICE DE CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

CAPÍTULO I: ANTECEDENTES

1.1 Problema

Estudios relacionados a las vulnerabilidades a los servicios de telecomunicaciones ejecutados tanto a nivel mundial como nacional, señalan que cerca del 50% de empresas sufrieron alguna brecha de seguridad, debido a que no cuentan con un proceso de gestión de incidentes (Deloitte, 2017), así como el peligro en el que recaen por propagaciones de varios tipos de malware, mencionando que en el país al menos 9 Instituciones han sido afectadas (Comercio, 2017); además de otros delitos registrados. Si bien esta es una visión general de la situación, a las entidades que conforman el Marco Administrativo Público Central, se les atribuye la implementación del Esquema Gubernamental de Seguridad de la Información (EGSI), que busca precisamente resguardar la seguridad informática adecuando políticas mediante el uso obligatorio de normativas técnicas. En este caso, las Instituciones del servicio de Salud Pública, que gestionan información sensible como registros médicos, historias clínicas, detalles de seguridad social de pacientes, etc., se convierten en un blanco atractivo para aquellos atacantes que indagan para obtener acceso a esta información altamente confidencial y actuar de acuerdo a sus propósitos, lo cual pone en riesgo los recursos informáticos y servicios de TI de dichas organizaciones.

En el Hospital San Luis de Otavalo la estructura de la red de datos, información, activos y recursos de red necesarios para brindar servicios y atención médica a los ciudadanos requieren una mejora en su gestión, en base a esta problemática se ve obligado a incluir las buenas prácticas del EGSI en sus actividades interinstitucionales y a través de la implementación de un Gobierno de TI proporcionar un conjunto de acciones a ser realizadas por el área de tecnologías en coordinación con la alta dirección para movilizar los recursos de la forma más eficiente en respuesta a requisitos regulatorios (Global, s.f.) y así elevar la seguridad informática en la Institución, asegurar la

preservación de la información de los pacientes y brindar servicios con garantías de calidad aportando a la creación de un entorno de atención sanitaria adecuado.

1.2 Objetivos

1.2.1 Objetivo General.

Diseñar un Gobierno de TI basado en el Esquema Gubernamental de la Seguridad de la Información (EGSI) en el Hospital San Luis de Otavalo.

1.2.2 Objetivos Específicos.

- Realizar una revisión de la estructura del EGSI y estándares que faciliten el diseño del Gobierno de TI afines a la seguridad informática en el sector salud.
- Analizar la situación actual del Hospital San Luis de Otavalo mediante un análisis de Gestión de Riesgos que posibilite determinar sus principales falencias a nivel informático estructural.
- Formular una Política de Seguridad de la Información a fin de mitigar o reducir los riesgos encontrados y que más se apeguen a los principios del EGSI.
- Implementar y socializar las políticas con el personal involucrado en la Seguridad de la Información con el objetivo de mejorar la gestión y desempeño de las TI en beneficio de los usuarios.
- Elaborar un análisis Costo - Beneficio de la implementación de políticas y procedimientos alineados a los objetivos estratégicos de la Institución.

1.3 Alcance

Con el objetivo de comprender acerca de la legislación del Estado en el marco de la Seguridad de la Información en Instituciones Públicas, se realizará un estudio de referencias afines

a los principios del EGSI y políticas propias del Ministerio de Salud Pública para obtener una perspectiva del punto de partida para el diseño del Gobierno de TI.

Se elaborará el diseño del Gobierno de TI enfocado en la Seguridad de la Información y se evaluará la situación actual del Hospital San Luis de Otavalo a través de un análisis de Gestión de Riesgos según las directrices del estándar NTE INEN-ISO/IEC 27005 para determinar las principales vulnerabilidades de los activos de información, este proceso se llevará a cabo a través de la elaboración de matrices de riesgos, documentando y detallando cada evento suscitado.

Una vez que se hayan determinado los principales riesgos relacionados con los activos de información se integrarán los controles y buenas prácticas del estándar (NTE INEN-ISO 27799 para la Gestión de la Seguridad de la Información en Sanidad) y del EGSI para formular las Política de Seguridad de la Información de la Institución a ser implementada.

La implementación de la Política de Seguridad de la Información puede efectuarse mediante socializaciones con los funcionarios, definición de procedimientos para desarrollar determinadas actividades e inclusive utilizando recursos de hardware y software para optimizar la estructura de la red de datos y mejorar la prestación de servicios en la Institución.

El análisis Costo - Beneficio tendrá un enfoque cuantitativo en cuestiones de cotizaciones para la adquisición de recursos informáticos necesarios para asegurar la confidencialidad, integridad y disponibilidad de la información.

1.4 Justificación

El Plan Nacional del Buen Vivir, en su objetivo tres promueve la mejora de la calidad de vida de los ciudadanos, lo cual implica colaborar para que los servicios públicos como la Salud, sean de calidad en todos sus aspectos, mejorando no solo las condiciones de vida de cada paciente,

sino también poniendo a salvo los recursos de TI, que son considerados herramientas esenciales para la prestación de servicios en beneficio de toda la población.

Debido a las incidencias y brechas de seguridad del Hospital San Luis de Otavalo se ve la necesidad de implementar estándares que responden al cumplimiento de las disposiciones propuestas por la Secretaría Nacional de la Administración Pública, partiendo del análisis de la realidad de la estructura de TI, determinando los principales riesgos que no contribuyen a llevar a cabo un mejoramiento, garantía de calidad y transparencia en la prestación adecuada de Servicios de Salud.

De esta manera, el presente proyecto contribuirá en beneficio del Hospital San Luis de Otavalo a mejorar la continuidad de los servicios, asegurar la información confidencial, cumplir con las directrices del EGSI, optimizar la gestión de los activos de TI identificando los posibles riesgos en la red y conocer las medidas a tomarse como respuesta ante los riesgos encontrados.

Por lo tanto, el Hospital San Luis de Otavalo prestará sus servicios cumpliendo con estándares que garanticen la seguridad de la información: integridad, confidencialidad y disponibilidad; con un Gobierno TI, todas las situaciones que debilitan la gestión interna de la Institución podrán ser identificadas y gestionadas adecuadamente y así generar confianza a la ciudadanía.

CAPÍTULO II: SEGURIDAD DE LA INFORMACIÓN, MARCOS DE CONTROL Y ESTÁNDARES PARA EL ÁMBITO LOCAL

El objetivo del presente capítulo es proveer un análisis introductorio capaz de ampliar el significado y propósito de la Seguridad de la Información en el sector salud, el Gobierno de TI, la Gestión de Riesgos y el Marco Legal que justifica el contexto del proyecto.

En primera instancia se definen a las Tecnologías de la Información (TI) y la Seguridad de la Información, el Gobierno de TI bajo el marco de referencia COBIT 5, la Gestión de Riesgos según el estándar NTE INEN ISO/IEC 27005:2012, la estructura del Esquema Gubernamental de Seguridad de la Información (EGSI) y el estándar NTE INEN ISO 27799:2008. Este conjunto de normativas se utilizará para obtener una base sólida sobre las mejores prácticas recomendadas para preservar la seguridad de la información enfocado a uno de los sectores más vulnerables a la pérdida de la confidencialidad, integridad y disponibilidad de la información, el sector salud.

2.1 Tecnologías de la Información (TI)

La manera en la cual la tecnología ha aportado en mejorar la calidad de vida de las personas es tan evidente al punto que hoy en día los gobiernos, empresas, sistemas, servicios y toda la sociedad se ha vuelto muy dependiente de ella convirtiéndose en un elemento imprescindible para el apoyo, sostenibilidad y crecimiento de los negocios, es decir, brindan valor a las empresas al automatizar los procesos y mejorar su productividad.

Según (Rajaraman, 2018) la Tecnología de la Información (TI) es la tecnología utilizada para organizar, almacenar o procesar datos que pueden usarse en aplicaciones específicas, esta información permite tomar decisiones e iniciar acciones.

2.2 Seguridad de la Información

La Seguridad de la Información es el conjunto de acciones o medidas que las organizaciones toman para proteger la confidencialidad, integridad y disponibilidad de los Sistemas de Información, sus principios son:

- **Confidencialidad:** Propiedad de la información que garantiza la conservación de la privacidad de los datos y acceso exclusivo para personal autorizado y con privilegios especiales.
- **Disponibilidad:** Propiedad de que la información se encuentra disponible contando con el acceso oportuno y confiable en todo momento a un servicio solicitado.
- **Integridad:** Propiedad de que la información se mantiene protegida garantizando su completitud y que se conserven las características que en un principio surgieron para sus propósitos.

2.3 Gobierno de TI

Partiendo de la gran demanda del uso de la tecnología surgió la necesidad de crear un instrumento capaz de reconocer el valor de las TI y en cómo pueden contribuir al cumplimiento de los objetivos estratégicos de las organizaciones.

> El gobierno de TI es parte integral de la junta directiva y de la dirección ejecutiva. Este es parte integral del gobierno corporativo y consiste en el liderazgo, los procesos y las estructuras que aseguran que las TI de la organización apoyen los objetivos y estrategias de la empresa. (ITGI, 2013, pág. 10)

El Gobierno de TI tiene como objetivo dirigir las TI para garantizar que cumplan con los siguientes objetivos:

- Alineación de las TI con la empresa para obtener los beneficios esperados.
- Maximización de beneficios a través del uso de las TI.
- Uso responsable de los recursos de las TI.
- Gestión adecuada de los riesgos relacionados con las TI.

El Gobierno de TI es un término trabajado por el IT Governance Institute ITGI (Instituto de Gobierno de TI), institución que se esfuerza en ayudar a líderes empresariales en su responsabilidad de lograr que las TI cumplan con los objetivos estratégicos, concienciando, orientando y proveyendo herramientas a directores y consejos administrativos para el buen manejo de las TI y mitigación de riesgos.

2.3.1 Marcos de Referencia (Frameworks).

Una organización puede implementar un Gobierno de TI adaptado a sus condiciones, los autores (Muñoz & Ulloa, 2011) indican que existe un número importante de marcos diseñados para dar soporte a la implementación de distintos aspectos del gobierno de TI; cada uno de ellos enfoca las prioridades en distintos aspectos del gobierno de TI, haciéndolos, en buena medida, complementarios.

En la Tabla 1 se revisan cinco marcos de control y estándares que apoyan al gobierno de las TI, donde se puede apreciar su enfoque en ciertas áreas del negocio tales como la gestión de procesos para los servicios de TI, seguridad de la información, inversiones en TI, etc.

Tabla 1. Marcos de control y estándares complementarios del Gobierno de TI

Área	COBIT	VAL IT	ITIL	ISO/IEC 38500	ISO/IEC 27002
Descripción	Ayuda a las empresas a crear el valor óptimo desde las TI manteniendo el equilibrio entre la generación de beneficios y la optimización de los niveles de riesgo y el uso de recursos.	Ayuda a las organizaciones a garantizar que logren un valor óptimo de las inversiones de negocio posibilitadas por TI a un coste económico, y con un nivel conocido y aceptable de riesgo.	Son recomendaciones para la correcta gestión de los departamentos TI y se especifican los procesos y procedimientos para ello, es como una manera de trabajar más ordenada y realmente dirigida a servir a negocio.	Provee a las organizaciones principios para evaluar, dirigir y monitorear el uso de las TI, que son la clave para saber dirigir y controlar la gestión interna de las organizaciones.	Provee un conjunto de objetivos de control y guías para iniciar, implementar, mantener, y mejorar la gestión de seguridad de la información en una organización. Cubre los requerimientos de seguridad que han salido de una evaluación de riesgos.
Función	Mapeo de procesos de TI	Marco de trabajo para generar valor de las inversiones del negocio posibilitadas por TI	Mapeo de la gestión de niveles de servicios de TI	Marco de principios para Gobernar las TI	Código de prácticas para la gestión de la seguridad de la información
Dominios, principios y procesos	5 dominios y 37 procesos	3 principios y 40 prácticas	27 procesos divididos en 5 fases	6 principios	14 cláusulas y 114 dominios de control de seguridad
Organismo que lo avala	ISACA (Asociación de Auditoría y Control de Sistemas de Información)	ITGI (Instituto de gobernanza de TI)	OCG (Oficina de Comercio Gubernamental)	ISO/IEC (Organismo Internacional de Normalización) / (Comisión	ISO/IEC (Organismo Internacional de Normalización) / (Comisión

Última versión	COBIT 5	Val IT Framework 2.0	ITIL v3	Electrotécnica Internacional) ISO/IEC 38500:2015	Electrotécnica Internacional) ISO/IEC 27002:2013
¿Para qué se implementa?	Gobierno de TI / Auditoria de sistemas de Información	Dirigir las inversiones del negocio que permiten las TI	Gestión de niveles de servicio de TI	Gobierno de gestión de procesos de TI	Gestión de seguridad de la información
¿Quiénes lo evalúan?	Organizaciones relacionadas con la consultoría y auditoría en TI	Organizaciones relacionadas con la consultoría y auditoría en TI	Organizaciones relacionadas con la consultoría y auditoría en TI	Organizaciones relacionadas con la consultoría y auditoría en TI	Organizaciones relacionadas con la consultoría y auditoría en TI

Fuente: Adaptado de (Agustín, 2015), (Muñoz & Ulloa, 2011), (ISACA, 2012)

La Tabla 1 permite comprender en qué se enfoca cada marco de control o estándar y de qué manera aportan a las organizaciones. COBIT 5 es el marco de control que engloba este conjunto de buenas prácticas y que consecuentemente será utilizado en el presente proyecto.

2.4 COBIT 5

COBIT (Objetivos de Control para la Información y las Tecnologías Relacionadas) es un marco de trabajo publicado en el año 2012 por ISACA (Asociación de Auditoría y Control de Sistemas de Información) que ayuda a las empresas a lograr sus objetivos a través del gobierno y gestión de las TI, maximizar beneficios, controlar niveles de riesgo y saber optimizar el uso de los recursos; es un marco de trabajo que funciona de un modo holístico, es decir, abarca a una empresa (independientemente de su tamaño o sector) de principio a fin (ISACA, 2012). COBIT 5 se construye en base a cinco principios, como lo describe la Figura 1.

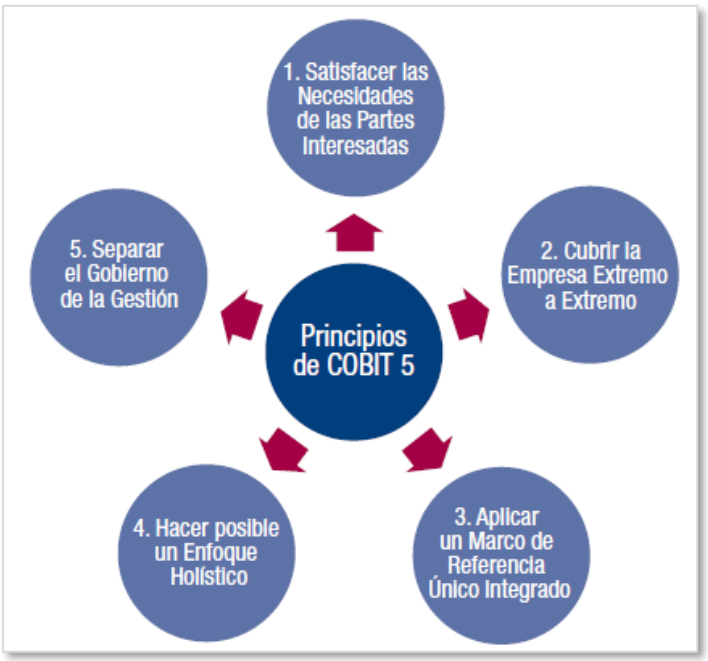


Figura 1. Principios de COBIT 5

Fuente: Recuperado de (ISACA, 2012)

2.4.1 Principios de COBIT 5.

Los siguientes literales describen los principios del Marco de Control COBIT 5 para el gobierno y gestión de las TI.

2.4.1.1 Satisfacer las necesidades de las partes interesadas.

COBIT 5 reconoce que las empresas existen para crear valor para sus partes interesadas, esto significa que, por ejemplo, si una empresa dedicada a la banca financiera busca atraer mayor cantidad de clientes, aplica una estrategia otorgando préstamos con un interés bajo; si una empresa dedicada a la venta de textiles busca atraer compradores de sus productos, aplica una estrategia de elevar ofertas, entre otros ejemplos.

COBIT 5 provee los procesos necesarios para mantener un equilibrio entre la realización de beneficios, optimización de riesgos y uso de recursos para que las empresas creen valor para las partes interesadas a través de las TI (ISACA, 2012), (Figura 2).

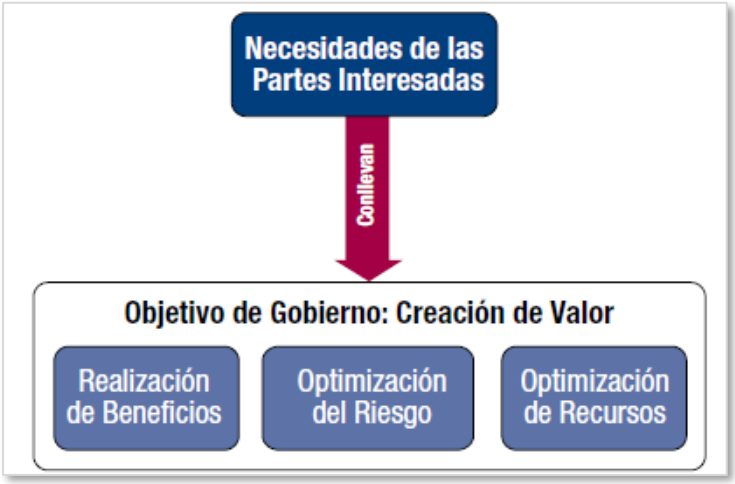


Figura 2. El objetivo de Gobierno: Creación de valor

Fuente: Recuperado de (ISACA, 2012)

2.4.1.2 Cubrir la Empresa Extremo a Extremo.

COBIT 5 visualiza a la información y las TI como un activo más de la empresa desde una perspectiva extremo a extremo, es decir, que el gobierno y gestión de dichos recursos requieren funciones y procesos adecuados donde quiera que la información sea

procesada. De acuerdo con la Figura 3, COBIT 5 contempla todos los servicios y procesos de TI internos y externos relevantes (ISACA, 2012).

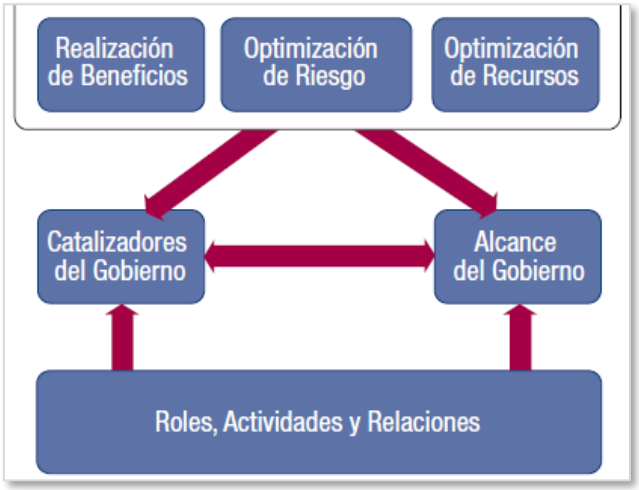


Figura 3. Componentes clave de un sistema de Gobierno

Fuente: Recuperado de (ISACA, 2012)

Un buen sistema de Gobierno además de crear valor para las partes interesadas se compone de Catalizadores de Gobierno, que son todos los recursos que organizan una empresa, como los marcos de referencia, procesos y prácticas, servicios, infraestructura de TI, personas e información; también necesita definir el alcance del sistema de Gobierno porque puede aplicarse a toda una empresa o parte de ella, así como los roles, actividades y relaciones de los involucrados en el Gobierno de TI.

2.4.1.3 Aplicar un Marco de Referencia Único e Integrado.

ISACA aporta al desarrollo de metodologías como COBIT, VAL IT, RISK IT, entre otros, que son marcos representativos y comúnmente utilizados para Gobernar las TI; COBIT 5 integra estos marcos, pero también puede unificarse con normas, guías y estándares relacionados con las TI. Por ello COBIT 5 es considerado un marco de referencia único e integrado.

2.4.1.4 Hacer posible un Enfoque Holístico.

COBIT 5 a través de sus catalizadores o recursos de TI (Figura 4) posibilita la implementación de un buen gobierno y gestión de TI para que las empresas logren sus metas y objetivos.

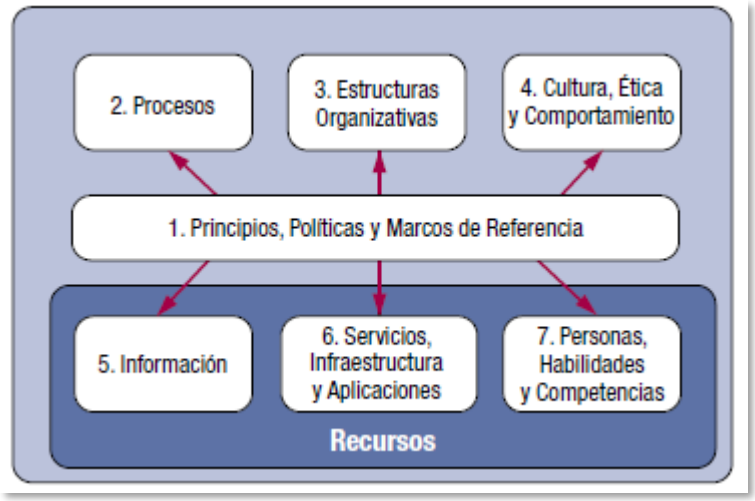


Figura 4. Catalizadores Corporativos de COBIT 5

Fuente: Recuperado de (ISACA, 2012)

- Los principios, políticas y marcos de referencia definen el comportamiento de una organización en base decisiones establecidas.
- Los procesos son prácticas que permiten lograr las metas empresariales.
- Las estructuras organizativas son quienes toman decisiones en una organización.
- La cultura, ética y comportamiento de los individuos son factores importantes para el éxito del gobierno y gestión de una empresa.
- La información es toda la información producida y utilizada por la empresa.
- Los servicios, infraestructuras y aplicaciones son los que proporcionan a la empresa servicios y tecnologías de procesamiento de la información.
- Las personas, habilidades y competencias son necesarias para poder completar de manera satisfactoria todas las actividades.

2.4.1.5 Separar el Gobierno de la Gestión.

COBIT 5 posiciona al gobierno y gestión en perspectivas diferentes debido a que sus propósitos, estructuras organizativas y actividades son distintas (Figura 5).

- **Gobierno:** El Gobierno se encarga de dirigir, orientar y supervisar a los cuerpos administrativos para que evalúen las necesidades de las partes interesadas de tal forma que se tomen decisiones que aseguren el logro de las metas institucionales.
- **Gestión:** La Gestión por su parte, son todas las actividades y prácticas como: planificación, construcción, ejecución y supervisión a realizarse como consecuencia de la toma de decisiones de Gobierno.

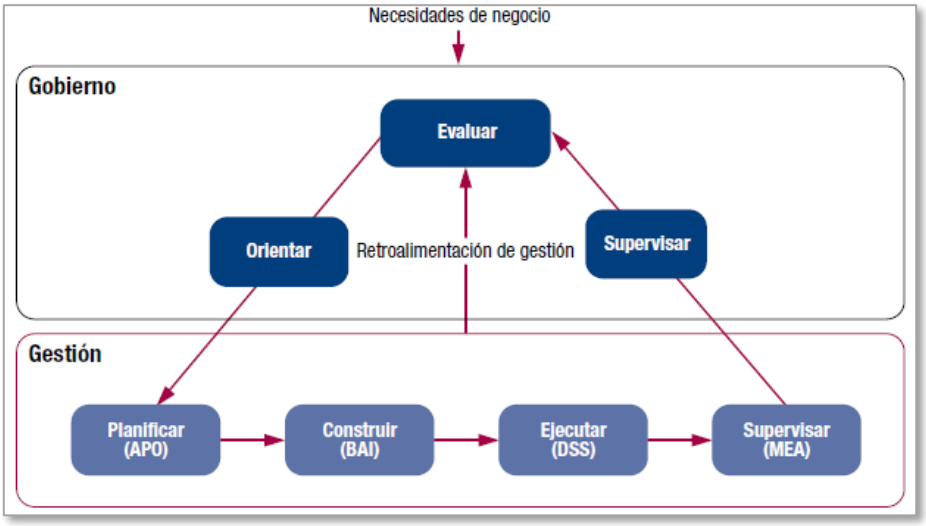


Figura 5. Áreas Clave de Gobierno y Gestión de COBIT 5

Fuente: Recuperado de (ISACA, 2012)

COBIT 5 señala que las empresas deben cubrir todas las metas de gobierno y gestión sin importar la cantidad de procesos que ejecute.

2.4.2 Cascada de metas de COBIT 5.

La cascada de metas de COBIT 5 es el mecanismo por el cual las empresas pueden personalizar a COBIT 5 y adaptarlo a su propio contexto y necesidades. Esta técnica permite “traducir metas corporativas de alto nivel en otras metas más manejables,

específicas, relacionadas con TI y mapeándolas con procesos y prácticas específicos" (ISACA, 2012).

Dicho en otras palabras, la cascada de metas de COBIT 5 es el resultado del mapeo de metas y procesos relacionados con las TI distribuidas en matrices que este marco de control provee.

2.4.3 Cuadro de Mando Integral (CMI).

El Cuadro de Mando Integral (CMI) es un sistema de control de gestión empresarial y va de la mano con la elaboración de la cascada de metas de COBIT 5 debido a que cada meta se agrupa en cuatro diferentes perspectivas. Este sistema inicia a partir de la idea de que la evolución de una empresa no solo debe fijar la mira en el ámbito financiero, sino que debería complementarse con otras medidas quizá intangibles como son la satisfacción del cliente, los procesos internos y la capacidad de innovar, que son fuentes principales para la ventaja competitiva.

"COBIT 5 utiliza el CMI debido a que estas cuatro perspectivas ayudan con sus indicadores a monitorizar si la empresa va a cumplir sus metas estratégicas considerando a las TI como parte de la organización" (Monfort, 2016). La Tabla 2 describe las cuatro perspectivas de COBIT 5.

Tabla 2. Perspectivas del Cuadro de Mando Integral

Perspectiva	Descripción
Financiera	Es importante tener información precisa y actualizada sobre el desempeño financiero de la empresa, no solo medidas tradicionales financieras como ganancias y crecimiento en las ventas, sino también otros aspectos relacionados al riesgo y el costo-beneficio.
Cliente	Es el cómo ve el cliente a la organización, y qué debe hacer ésta para mantenerlo como cliente. Si el cliente no está satisfecho, aun cuando las finanzas estén marchando bien, es un fuerte indicativo de problemas en el futuro.

Interna (Procesos del negocio)	Se refiere a los procesos internos que la organización debería mejorar para lograr sus objetivos y preguntarse: "Para satisfacer a los accionistas y clientes, ¿en qué procesos de negocio debemos sobresalir?".
Aprendizaje y crecimiento	Es el cómo puede la organización seguir mejorando para crear valor en el futuro, incluyendo aspectos como los objetivos y metas que se desean alcanzar, así como las iniciativas que se incluirán para alcanzar dichas metas.

Fuente: Adaptado de (Domínguez, 2015)

2.4.4 Dominios de COBIT 5.

COBIT 5 provee un conjunto de procesos los cuales representan a aquellos que generalmente se ejecutan en las pequeñas o grandes empresas en relación con las TI y que, dependiendo de su tamaño el número de procesos varía.

COBIT 5 enfatiza que cada organización puede personalizarlo a su contexto y no se debería utilizarlo de manera mecánica, debido a que es una guía que integra buenas prácticas acerca de cómo implementar y utilizar de mejor manera las TI y que como resultado sea posible soportar los objetivos de la empresa relacionadas con las TI.

Los procesos en este marco de referencia se encuentran sujetos a dos dominios principales que son el Gobierno y la Gestión (Tabla 3).

- Gobierno: Este dominio se conforma de 5 procesos de Gobierno donde se establecen prácticas de evaluación orientación y supervisión (EDM).
- Gestión: Está conformado de cuatro dominios de gestión y dentro de ellos se establecen prácticas sobre planificar, construir, ejecutar y supervisar.

Tabla 3. Procesos de TI COBIT 5

Procesos de Gobierno de las TI		
Evaluar, Orientar y Supervisar	EDM01	Asegurar el establecimiento y mantenimiento del Marco de Gobierno
	EDM02	Asegurar la entrega de beneficios
	EDM03	Asegurar la optimización del riesgo
	EDM04	Asegurar la optimización de los recursos

	EDM05	Asegurar la transparencia hacia las partes interesadas
Procesos de Gestión de las TI		
Alinear, Planificar y Organizar	APO01	Gestionar el marco de gestión de TI
	APO02	Gestionar la estrategia
	APO03	Gestionar la arquitectura empresarial
	APO04	Gestionar la innovación
	APO05	Gestionar el portafolio
	APO06	Gestionar el presupuesto y los costes
	APO07	Gestionar los recursos humanos
	APO08	Gestionar las relaciones
	APO09	Gestionar los acuerdos de servicio
	APO10	Gestionar los proveedores
	APO11	Gestionar la calidad
	APO12	Gestionar el riesgo
	APO13	Gestionar la seguridad
Construcción, Adquisición e Implementación	BAI01	Gestionar los programas y proyectos
	BAI02	Gestionar la definición de requisitos
	BAI03	Gestionar la identificación y construcción de soluciones
	BAI04	Gestionar la disponibilidad y la capacidad
	BAI05	Gestionar la introducción de cambios organizativos
	BAI06	Gestionar los cambios
	BAI07	Gestionar la aceptación del cambio y de la transición
	BAI08	Gestionar el conocimiento
	BAI09	Gestionar los activos
	BAI10	Gestionar la configuración
Entregar, dar Servicio y Soporte	DSS01	Gestionar las operaciones
	DSS02	Gestionar las peticiones y los incidentes del servicio
	DSS03	Gestionar los problemas
	DSS04	Gestionar la continuidad
	DSS05	Gestionar los servicios de seguridad
	DSS06	Gestionar los controles de los procesos del negocio
Supervisión, Evaluación y Verificación	MEA01	Supervisar, evaluar y valorar rendimiento y conformidad
	MEA02	Supervisar, evaluar y valorar el sistema de control interno

MEA03	Supervisar, evaluar y valorar la conformidad con los requerimientos internos

Fuente: Adaptado de (ISACA, 2012)

2.5 Introducción al Análisis de Riesgos

Uno de los principales recursos que deben ser protegidos en una organización es la información y el análisis de riesgos pretende identificar los elementos que componen los sistemas de información, como lo señala (Ortiz Beltrán, 2015), el análisis de riesgos consiste en el conocimiento profundo del comportamiento de los elementos de los sistemas como un requisito para decidir sobre la mejor manera de gestionar los recursos económicos, tecnológicos, humanos, etc. Para una mejor comprensión del contexto de la gestión de riesgos se definen los siguientes términos:

- **Activo:** Cualquier elemento que tiene valor para la organización, es un bien preciado y un recurso utilizado por la misma para fines del negocio o sustento.
- **Activos de información:** Todo aquello que tiene alta validez para las organizaciones y que puede contener algún tipo de información como puede ser bases de datos, contraseñas, números de cuentas, etc.
- **Activos Primarios:** Elementos por medio de los cuales una organización cumple con sus objetivos estratégicos.
- **Activos de soporte:** Son los que dan soporte a los activos primarios y se clasifican en activos de: hardware, software, redes, personal, ubicación o sitio.
- **Amenaza:** Origen de un acontecimiento no deseado y que “puede” afectar negativamente a los sistemas de información. “Puede”, ya que una amenaza en sí existe solamente cuando es aprovechada por una vulnerabilidad.

- **Gestión del riesgo:** Consiste en la capacidad de una organización de realizar acciones o crear estrategias para manejar adecuadamente los riesgos y establecer mecanismos para tratarlos.
- **Identificación del riesgo:** Proceso para encontrar, enumerar y caracterizar los elementos del riesgo.
- **Impacto:** Es la consecuencia de que una amenaza se materialice.
- **Vulnerabilidad:** Compromete a los sistemas de información, es una debilidad inherente que puede ser aprovechada por las amenazas.

2.5.1 Norma NTE INEN - ISO/IEC 27005:2012.

La Norma NTE INEN-ISO/IEC 27005:2012 aborda la Gestión de Riesgos de la Seguridad de la Información, para conocer acerca de su estructura se presenta un extracto de su contenido.

2.5.1.1 Objetivo.

Brinda directrices que permiten llevar a cabo una adecuada gestión de riesgos de la seguridad de la información, se compone de un conjunto de procesos expuestos de forma sistemática y organizada, sin embargo, "no brinda ninguna metodología específica para la gestión del riesgo de la seguridad de la información. Corresponde a la organización definir su enfoque para la gestión del riesgo" (INEN, 2012). La gestión del riesgo analiza lo que puede suceder y cuáles pueden ser las posibles consecuencias, antes de decidir lo que se debería hacer y cuándo hacerlo.

2.5.1.2 Estructura.

Su contenido inicia con información preliminar y definiciones relevantes, luego aborda el proceso de gestión del riesgo de la seguridad de la información y concluye con anexos y bibliografía. La Tabla 4 representa la estructura general de la norma.

Tabla 4. Estructura de la Norma NTE INEN - ISO/IEC 27005:2012

Núm.	Ítems
1.	Alcance
2.	Referencias normativas
3.	Términos y definiciones
4.	Estructura de esta norma
5.	Información general
6.	Visión general del proceso de gestión del riesgo de la seguridad de la información
7.	Establecimiento del contexto
8.	Valoración del riesgo de la seguridad de la información
9.	Tratamiento del riesgo de la seguridad de la información
10.	Aceptación del riesgo de la seguridad de la información
11.	Comunicación de los riesgos de seguridad de la información
12.	Monitoreo y revisión del riesgo de la seguridad de la información
	Anexo A (Informativo) Definición del alcance y los límites del proceso de gestión del riesgo de la seguridad de la información
	Anexo B (Informativo) Identificación y valoración de los activos y valoración del impacto
	Anexo C (Informativo) Ejemplos de amenazas comunes
	Anexo D (Informativo) Vulnerabilidades y métodos para la valoración de la vulnerabilidad
	Anexo E (Informativo) Enfoques para la valoración de riesgos en la seguridad de la información
	Anexo F (Informativo) Restricciones para la reducción de riesgos
	Bibliografía

Fuente: Adaptado de (INEN, 2012)

La presente norma no establece una metodología para llevar a cabo este proceso, pero “sirve para no tener dudas sobre los elementos que tienen que incluir las buenas metodologías de Análisis de Riesgos, por lo que desde este punto de vista puede constituirse como una metodología en sí misma” (ISO Tools Excellence, 2018). En la figura 6 se describe el proceso de la gestión de riesgos.

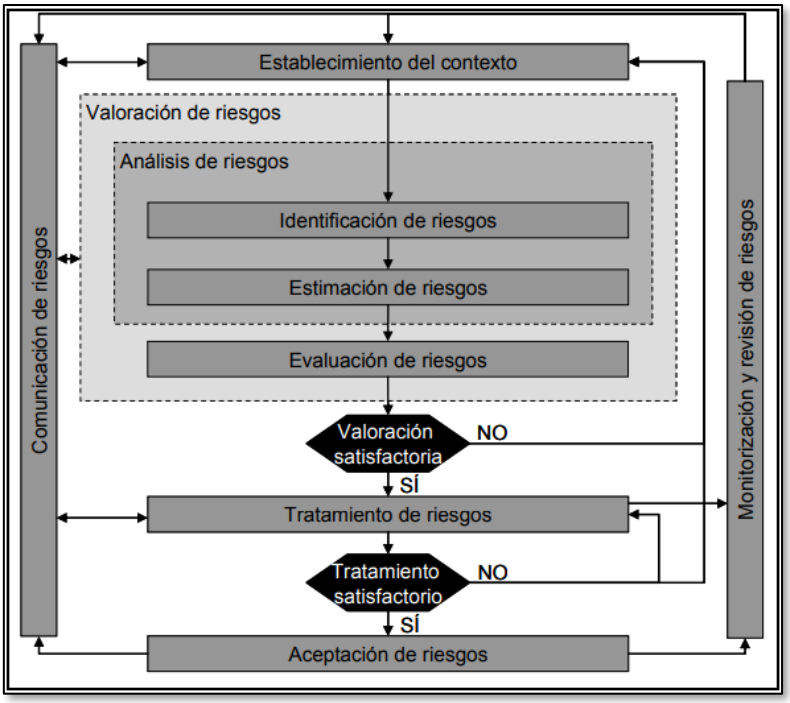


Figura 6. Proceso de Gestión de Riesgos de la Seguridad de la Información

Fuente: Recuperado de (INEN, 2012)

El establecimiento del contexto es el proceso donde se realiza un estudio de la estructura de la organización, se obtiene información pertinente y se definen de criterios claves para la valoración de los riesgos.

La valoración de riesgos es el proceso en el cual se analiza y recolecta información de los activos de información para poder valorarlos y determinar los activos críticos que serán considerados dentro del análisis de riesgos para estimar sus niveles de riesgo.

El tratamiento del riesgo son las medidas y acciones que han de tomarse para manejar los riesgos, como la selección de controles de seguridad apropiados para tratar dichos riesgos.

La aceptación del riesgo es formalizar la aprobación de las estrategias o planes de tratamiento de los riesgos tomando en cuenta cuestiones legales, reglamentarias, financieras, etc.

La comunicación del riesgo se trata de acordar formalmente la manera en que se gestionarán los riesgos considerando los criterios y puntos de vista de todas las partes interesadas, por ello es importante que exista una buena comprensión de las actividades que formarán parte del proceso de gestión de los riesgos.

El monitoreo y revisión es la identificación de los cambios y factores nuevos que pueden aparecer y llegar a modificar la valoración y tratamiento de los riesgos ya establecidos para verificar si los controles de seguridad, políticas y/o acciones seleccionadas mejoran la gestión de los riesgos en la seguridad de la información.

2.6 Esquema Gubernamental de Seguridad de la Información (EGSI)

En esta sección se realiza un análisis del Esquema Gubernamental de Seguridad de la Información (EGSI), documento que contiene directrices relacionadas con la Seguridad de la Información dirigidas a las entidades públicas del país.

2.6.1 Acuerdo Ministerial 166.

El presente acuerdo emitido la fecha del 19 de septiembre del 2013 dispone que todas las organizaciones que formen parte de la Administración Pública incorporen de manera obligatoria los estándares y/o referencias de la familia de Normas Técnicas Ecuatorianas NTE INEN-ISO/IEC 27000, basándose en sus lineamientos y buenas prácticas para la gestión de la Seguridad de la Información.

El artículo de 2 este Acuerdo señala que: “La implementación del EGSI se realizará en cada institución de acuerdo al ámbito de acción, estructura orgánica, recursos y nivel de madurez en gestión de Seguridad de la Información” (SNAP, 2012).

2.6.2 Contenido.

El EGSI establece un conjunto de directrices prioritarias para la Gestión de la Seguridad de la Información e inicia un proceso de mejora continua en las

instituciones de la Administración Pública. El EGSI no reemplaza a la norma INEN ISO/IEC 27002 sino que marca como prioridad la implementación de algunas directrices (SNAP, 2012, pág. 5).

La estructura del EGSI (Tabla 5) se compone de una sección introductoria que define el marco legal que lo sustenta, disposiciones generales, transitorias y derogatorias para finalmente concluir con el cuerpo principal del EGSI.

Tabla 5. Estructura del EGSI

Núm.	Cláusulas
1.	Política de seguridad de la información
2.	Organización de la seguridad de la información
3.	Gestión de los activos
4.	Seguridad de los recursos humanos
5.	Seguridad física y del entorno
6.	Gestión de comunicaciones y operaciones
7.	Control de acceso
8.	Adquisición, desarrollo y mantenimiento de sistemas de información
9.	Gestión de los incidentes de la seguridad de la información
10.	Gestión de la continuidad del negocio
11.	Cumplimiento

Fuente: Adaptado de (SNAP, 2012)

Según la Tabla 5, el EGSI posee 11 cláusulas y cada una contiene controles de seguridad, algunos son identificados como prioritarios mediante el símbolo (*). De manera general, el EGSI se compone de 11 cláusulas, 714 controles de seguridad y 107 controles prioritarios.

2.7 Norma NTE INEN - ISO 27799:2008

El sector salud maneja información sanitaria considerada de entre todos los tipos de datos personales como la más confidencial debido a que la salud física de un paciente

tiene una estrecha relación con la custodia de sus datos personales. Esta norma se utilizará en el presente proyecto al tratarse de una entidad de salud para este caso de estudio.

2.7.1 Objeto y campo de aplicación.

La (INEN, 2008) señala que esta norma internacional aplica la Norma ISO/IEC 27002 al dominio sanitario considerando cuidadosamente la aplicación apropiada de los controles de seguridad para los propósitos de proteger los datos personales sanitarios, para que los organismos de salud cumplan con requisitos especiales y únicos en su entorno, preservando la confidencialidad, integridad y disponibilidad de la información.

2.7.2 Estructura.

Se compone de una sección introductoria e informativa donde se abordan aspectos generales referentes a la seguridad de la información sanitaria, luego aborda directrices para la gestión de seguridad de la información en el ámbito sanitario y al final tres anexos con información de apoyo y bibliografía, como lo indica la Tabla 6.

Tabla 6. Estructura de la norma NTE INEN - ISO 27799:2008

Campos	Descripción
1.- Objeto y campo de aplicación	- Generalidades - Exclusiones del objeto y campo de aplicación
2.- Normas para la consulta	
3.- Términos y definiciones	- Términos sanitarios - Términos de seguridad de la información
4.- Términos abreviados	
5.- Seguridad de la información sanitaria	- Metas de la seguridad de la información sanitaria - Seguridad de la información dentro del gobierno de la información - Gobierno de la información dentro del gobierno corporativo y clínico - Información sanitaria a proteger - Amenazas y vulnerabilidades en la seguridad de la información sanitaria

6.- Plan de Acción práctico para implementar la norma ISO/IEC 27002	- Taxonomía de las Normas ISO/IEC 27002 e ISO/IEC 27001 - Compromiso de gestión para implementar la Norma ISO/IEC 27002 - Establecimiento, operación, mantenimiento y mejora del ISMS - Planificación: establecimiento del ISMS - Hacer: implementación y operación del ISMS - Comprobar: realizar seguimiento y revisar el ISMS - Acción: mantenimiento y mejora del ISMS
7.- Implicaciones sanitarias de la norma ISO/IEC 27002	- Generalidades - Políticas de seguridad de la información - Aspectos organizativos de la seguridad de la información - Gestión de activos - Seguridad de los recursos humanos - Seguridad física y del entorno - Gestión de comunicaciones y operaciones - Control de accesos - Adquisición, desarrollo y mantenimiento de los sistemas de información - Gestión de incidentes de seguridad de la información - Aspectos de seguridad de la información en la gestión de la continuidad del negocio - Cumplimiento
ANEXO A (Informativo) Amenazas a la seguridad de la información sanitaria	
ANEXO B (Informativo) Tareas y documentos relacionados con el sistema de gestión de seguridad de la información	
ANEXO C (Informativo) Beneficios potenciales y atributos necesarios de las herramientas de soporte	
BILBIOGRAFÍA	

Fuente: Adaptado de (INEN, 2008)

Nota: Para el desarrollo del presente proyecto se utilizará el apartado número 7 de la estructura de esta norma.

2.8 Comparación de las cláusulas del EGSI y NTE INEN-ISO 27799:2008

Una vez conocida la estructura del EGSI y la norma NTE INEN-ISO 27799:2008, es importante comparar las cláusulas que las componen y apreciar sus similitudes. La Tabla 7 brinda una comparativa de ambas normativas.

Tabla 7. Comparación de las cláusulas de seguridad de la información de las normativas EGSI y NTE INEN-ISO 27799:2008

Cláusulas EGSI	Cláusulas NTE ISO/IEC 27799:2008
	7.1 Generalidades
1. Política de seguridad de la información	7.2 Políticas de seguridad de la información
2. Organización de la seguridad de la información	7.3 Aspectos organizativos de la seguridad de la información
3. Gestión de los activos	7.4 Gestión de activos
4. Seguridad de los recursos humanos	7.5 Seguridad de los recursos humanos
5. Seguridad física y del entorno	7.6 Seguridad física y del entorno
6. Gestión de comunicaciones y operaciones	7.7 Gestión de comunicaciones y operaciones
7. Control de acceso	8. Control de accesos
8. Adquisición, desarrollo y mantenimiento de sistemas de información	9. Adquisición, desarrollo y mantenimiento de los sistemas de información
9. Gestión de los incidentes de la seguridad de la información	10. Gestión de incidentes de seguridad de la información
10. Gestión de la continuidad del negocio	11. Aspectos de seguridad de la información en la gestión de la continuidad del negocio
11. Cumplimiento	12. Cumplimiento

Fuente: Adaptado de (SNAP, 2012) y (INEN, 2008)

A continuación, se describe de manera general las cláusulas de ambas normativas.

- **Política de seguridad de la información:** Establece la aprobación de la Política de Seguridad de la Información en una Institución como un documento que define los lineamientos esenciales para garantizar la confidencialidad, integridad y disponibilidad de la información.

- **Organización de la seguridad de la información:** Define los responsables de velar por el cumplimiento de los lineamientos establecidos en la Política de Seguridad de la Información.
- **Gestión de los activos:** Aborda las acciones para el correcto manejo de los activos como su identificación, responsables de dicho activo, así como la clasificación de la información.
- **Seguridad de los recursos humanos:** Determina las funciones y responsabilidades del personal implicado en la seguridad de la información incluidas las condiciones antes, durante y después de su contrato laboral.
- **Seguridad física y del entorno:** Cubre aspectos relacionados con la protección física de todos los activos, así como de la seguridad de la información contenida en ellos.
- **Gestión de comunicaciones y operaciones:** Establece las medidas de seguridad para la información procesada en las redes, instalaciones o equipos que soportan su procesamiento, transporte, eliminación, etc.
- **Control de acceso:** Determina los límites de acceso a la información y a las áreas de procesamiento de la misma, regulando los permisos para acceder a los recursos de redes y servicios al personal autorizado.
- **Adquisición, desarrollo y mantenimiento de sistemas de información:** Establece los requisitos y especificaciones necesarias para la adquisición, desarrollo y mantenimiento de los Sistemas de Información.
- **Gestión de los incidentes de la seguridad de la información:** Abarca los procedimientos adecuados a realizar con el fin de responder ante eventualidades que pongan en riesgo a la información.

- **Gestión de la continuidad del negocio:** Determina las acciones para la planificación de la continuidad de los sistemas de información ante la materialización de incidentes en la seguridad de la información.
- **Cumplimiento:** Cubre aspectos para evitar el incumplimiento de las obligaciones y reglamentaciones legales relacionadas con la Seguridad de la Información.

2.9 Marco Legal Aplicado a la Seguridad de la Información

El Marco Legal constituye el conjunto de bases normativas sobre las cuales se sustenta el ejercicio de los derechos constitucionales y que, para fines del presente proyecto, justifica las represalias que los funcionarios son propensos a recibir si sus acciones representan un riesgo para la seguridad de la información.

2.9.1 La Constitución del Ecuador.

La Constitución del Ecuador es la Norma Jurídica Suprema de la República del Ecuador donde se cimentan las acciones de defensa que garantiza el Estado para reconocer los derechos de los ciudadanos y para el bien colectivo (Rojas, 2017). En este aspecto, la salud es uno de los derechos fundamentales y el Estado se compromete en promover un entorno adecuado para mejorar las condiciones de vida e interrelación con la sociedad capaz de preservar la integridad física de los ciudadanos, lo cual incluye la protección de su información personal.

2.9.2 La Administración Pública.

Comprende el conjunto de entidades que pertenecen al sector público del Estado, en el artículo 225 de la Constitución, según la (Asamblea Nacional de la República del Ecuador, 2008), el sector público lo constituyen los organismos de las funciones Ejecutiva, Legislativa, Judicial, Electoral y de Transparencia y Control Social, las instituciones del régimen autónomo descentralizado, las que son sustentadas económicamente por el Estado y prestan servicios públicos orientados a la colectividad y

beneficio de toda la población. El Hospital San Luis de Otavalo es una de las entidades que forma parte de la Administración Pública.

2.9.3 El Sistema Nacional de Salud.

"Organizado por el Estado y que se integra con las entidades públicas autónomas, privadas y comunitarias del sector salud, funcionará de manera descentralizada, desconcentrada y participativa" (Contraloría General del Estado, 2003, pág. 18). Estas dependencias serán las responsables de garantizar el acceso, prevención y promoción de la salud. El Ministerio de Salud Pública es el ente rector de la salud y aplicará normativas de cumplimiento obligatorio, creará los medios necesarios para gestionar adecuadamente los recursos provenientes del sector público en beneficio de la salud y generar planes o proyectos que ayuden a mejorar las condiciones de vida de la ciudadanía (Secretaría Técnica Plan Toda una Vida, 2015, pág. 4).

2.9.4 Ley Orgánica del Servicio Público.

La Ley Orgánica del Servicio Público es una "norma reglamentaria que permite una adecuada aplicación de los principios constitucionales y legales" (Ministerio de Finanzas, 2011, pág. 1) relacionado con el servicio público. Determina los deberes, derechos y prohibiciones de los/as servidores/as públicos acordados en los incisos e, f, y j del artículo 22 e indica que es su deber custodiar los recursos que le pertenecen al Estado como la preservación de documentación, herramientas, equipos y bienes confiados a su guarda y administración, brindar atención pública y asistencia permanente que garantice el derecho a los servicios públicos de calidad a la ciudadanía. Otra de sus obligaciones es "custodiar y cuidar la documentación e información que, por razón de su empleo, cargo o comisión tenga bajo su responsabilidad e impedir o evitar su uso indebido, sustracción, ocultamiento o inutilización" (Ministerio de Trabajo, 2011, pág. 15).

La presente Ley explica que los servidores/as públicos son responsables de entregar servicios de calidad con garantías de seguridad que velen por el cuidado, alteración, sustracción o pérdida de la información y recursos que constituyen elementos imprescindibles para el Estado y la prestación de servicios.

2.9.5 Ley Orgánica de Transparencia y Acceso a la Información Pública (LOTAIP).

La LOTAIP garantiza y norma el ejercicio del derecho fundamental de las personas a la información (CPCCS, 2018), donde uno de sus principales objetivos en relación con la seguridad de la información es garantizar la protección de la información personal en poder del sector público y/o privado (Ministerio de Educación, 2004), lo cual implica el cuidado de la información confidencial donde el artículo 6 señala que:

> Se considera información confidencial aquella información pública personal, que no está sujeta al principio de publicidad y comprende aquella derivada de sus derechos personalísimos y fundamentales, especialmente aquellos señalados en los artículos 23 y 24 de la Constitución Política de la República. El uso ilegal que se haga de la información personal o su divulgación dará lugar a las acciones legales pertinentes (Ministerio de Educación, 2004, pág. 3).

2.9.6 Ley Orgánica de Salud.

La Ley Orgánica de Salud en su artículo 1 señala que el Ministerio de Salud Pública se encargará de regular, vigilar y tomar las medidas destinadas a proteger la salud humana ante los riesgos y daños que pueden provocar las condiciones del ambiente (Secretaría Técnica Plan Toda una Vida, 2015). La presente Ley menciona sobre el derecho de los ciudadanos para recibir un servicio de salud organizado en cuestiones del manejo de su información tal como las historias clínicas, esto se especifica en el artículo 7 donde toda persona en referencia a la salud tiene derecho a:

> Tener una historia clínica única redactada en términos precisos, comprensibles y completos; así como la confidencialidad respecto de la información en ella contenida y a que se le entregue su epicrisis (Secretaría Técnica Plan Toda una Vida, 2015, pág. 5).

2.9.7 Ley de Derechos y Amparo al Paciente.

El Ministerio de Salud Pública a través de la presente Ley provee un conjunto de normativas que precautelan el derecho a la salud y vida de los pacientes, donde en términos de confidencialidad y derecho a la información están:

> Art. 4.- DERECHO A LA CONFIDENCIALIDAD. - Todo paciente tiene derecho a que la consulta, examen, diagnóstico, discusión, tratamiento y cualquier tipo de información relacionada con el procedimiento médico a aplicársele, tenga el carácter de confidencial (MSP, 2006, pág. 2).

> Art. 5.- DERECHO A LA INFORMACION. - Se reconoce el derecho de todo paciente a que, antes y en las diversas etapas de atención al paciente, reciba del centro de salud a través de sus miembros responsables, la información concerniente al diagnóstico de su estado de salud, al pronóstico, al tratamiento, a los riesgos a los que médicamente está expuesto (…) (MSP, 2006, pág. 2).

2.9.8 Reglamento de Información Confidencial en el Sistema Nacional de Salud.

Tiene como objetivo el manejo y gestión de la información confidencial de los pacientes desde el momento de la generación de la información hasta el evento de la muerte de la persona. Otro principio importante es el secreto médico o la responsabilidad de los médicos de guardar silencio sobre toda información que llegue a conocer sobre el/la usuario/a en el curso de su actuación profesional (MSP, 2015).

El artículo 7 del reglamento en cuestión define los documentos calificados como confidenciales para el sector de la salud a:

> Historias clínicas, resultados de exámenes de laboratorio, imagenología y otros procedimientos, tarjetas de registro de atenciones médicas con indicación de diagnóstico y tratamientos, siendo los datos consignados en ellos confidenciales (MSP, 2015, pág. 3).

La historia clínica es un documento médico legal que contiene detallada y ordenadamente todos los datos relativos a un paciente, incluyendo información de sus familiares, antecedentes, estado actual y evolución, además de los procedimientos y de los tratamientos recibidos, dicho documento sólo podrá ser manejado por personal de la cadena sanitaria: médicos, psicólogos, odontólogos, trabajadoras sociales, obstetrices, enfermeras, auxiliares de enfermería y personal de estadística; son requeridas claves de acceso personales para acceder a las historias clínicas dispuestas en formato electrónico; tanto el personal sanitario como la Institución en la que repose dicha información es responsable de su custodia física y del buen uso que se dé a la misma (MSP, 2015).

2.9.9 Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.

El objetivo de la presente Ley según el artículo 1 es regular los mensajes de datos, firma electrónica, servicios de certificación, contratación electrónica y telemática, prestación de servicios electrónicos, a través de redes de información, incluido el comercio electrónico y la protección a los usuarios de estos sistemas (OAS, 2002). La Tabla 8 resume las sanciones correspondientes a distintos delitos o infracciones informáticas contenidas en el artículo 58 de la presente Ley.

Tabla 8. Delitos y sanciones del Art. 58 de la Ley de Comercio electrónico, firmas electrónicas y mensajes de datos

Delitos de las infracciones informáticas	Pena privativa de libertad	Multa (Dólares americanos)
Violentar sistemas de seguridad para obtener acceso información protegida y vulnerar sistemas de información.	6 meses a 1 año	$500 a $100
Acceso a información que vulnere la seguridad nacional	1 a 3 años	$1000 a $1.500
Divulgación de información protegida	3 a 6 años	$2.000 a $10.000
Obtención y utilización no autorizada de información	2 meses a 2 años	$1.000 a $2.000

Fuente: Adaptado de (OAS, 2002)

De manera general, define en sus artículos las sanciones que se impondrán a los que violaren el derecho a la intimidad, en los términos establecidos en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos (OAS, 2002).

2.9.10 Código Orgánico Integral Penal (COIP).

El COIP fue aprobado como una herramienta jurídica en defensa de los derechos de la Constitución del Ecuador. La Sección Tercera sobre los delitos contra la seguridad de los activos de los sistemas de información y comunicación (Tabla 9), contiene 6 artículos que tratan sobre los delitos y sanciones que serían impuestas a los servidores/as públicos.

Tabla 9. Delitos y sanciones contra la seguridad de los activos de los sistemas de información y comunicación

Artículo	Delitos	Descripción	Sanciones
Art. 229	Revelación ilegal de base de datos	Revelación de información contenida en bases de datos o sistemas semejantes que violen la intimidad y privacidad de las personas.	3 a 5 años
Art. 230	Interceptación ilegal de datos	Interceptación de equipos informáticos, desarrollo de programas	3 a 5 años

		para evadir portales de acceso de origen; comercialización y distribución de información almacenada en medios electrónicos.	
Art. 231	Transferencia electrónica de activo patrimonial	Manipulación de sistemas informáticos para apropiación no consentida de un activo patrimonial.	3 a 5 años
Art. 232	Ataque a la integridad de sistemas informáticos	Supresión, destrucción o daño de los datos de sistemas los informáticos y sus componentes.	3 a 5 años
Art. 233	Delitos contra la información pública reservada legalmente	Revelación de información no autorizada y uso ilegítimo de la misma que comprometa la seguridad del Estado.	7 a 10 años e inhabilitación para ejercer un cargo o función pública por seis meses
Art. 234	Acceso no consentido a un sistema informático o de telecomunicaciones	Explotar ilegítimamente el acceso a un sistema informático	3 a 5 años

Fuente: Adaptado de (Ministerio de Defensa Nacional, 2014)

CAPÍTULO III: DISEÑO DEL GOBIERNO DE TI Y ANÁLISIS DE RIESGOS DEL HOSPITAL SAN LUIS DE OTAVALO

En el presente capítulo se realiza el diseño del Gobierno de TI por medio del marco de control COBIT 5 el cual permitirá alinear las metas corporativas, metas de TI y procesos de COBIT 5 con las metas del Hospital San Luis de Otavalo e identificar cuáles son los procesos que la Institución necesita mejorar para asegurar que las TI contribuyan al cumplimiento de sus objetivos estratégicos. Luego inicia la gestión de los procesos relacionados con la Seguridad de la Información resultantes del mapeo de procesos de COBIT 5, para ello se elabora un análisis de riesgos de la seguridad de la información en base a las directrices de la norma NTE INEN ISO/IEC 27005:2012 donde se identifican las amenazas, vulnerabilidades y riesgos de los activos de información resumida en la Matriz de Riesgos, la misma que posteriormente determinará la toma de decisiones para reducir o mitigar dichos riesgos. Durante el desarrollo de este proyecto se utilizarán las siglas HSLO para referir al Hospital San Luis de Otavalo y MSP al Ministerio de Salud Pública.

3.1 Estado de cumplimiento del EGSI

Dado que el Gobierno de TI se basa en el Esquema Gubernamental de Seguridad de la información, inicialmente es necesario conocer el nivel de cumplimiento de esta normativa en la Institución por medio de entrevistas al personal correspondiente, TIC, Talento Humano y Directivos. La Tabla 10 indica el porcentaje de cumplimiento por cláusulas del EGSI. Para más detalles revisar el Anexo A al final del documento.

Tabla 10. Nivel de cumplimiento del EGSI

Núm.	Cláusulas	% de cumplimiento
1.	Política de seguridad de la información	75%
2.	Organización de la seguridad de la información	91 %

3.	Gestión de los activos	80 %
4.	Seguridad de los recursos humanos	88 %
5.	Seguridad física y del entorno	77 %
6.	Gestión de comunicaciones y operaciones	88 %
7.	Control de acceso	69 %
8.	Adquisición, desarrollo y mantenimiento de sistemas de información	94 %
9.	Gestión de los incidentes de la seguridad de la información	100 %
10.	Gestión de la continuidad del negocio	80 %
11.	Cumplimiento	88 %
	Total	90.3 %

Fuente: Adaptado de (SNAP, 2012)

Seguidamente se justifica la calificación asignada a cada cláusula:

- Política de seguridad de la información: Tiene un nivel de cumplimiento del 75%, debido a que en la Institución existe una normativa interna denominada Política de uso de Servicios de Red y Recursos informáticos del MSP, pero no cubre todos los dominios de una Política de Seguridad de la Información.
- Organización de la seguridad de la información: En esta cláusula se cumple la mayoría de los dominios a excepción del control de Acuerdos de confidencialidad, documento que no está incluido dentro de los procesos internos.
- Gestión de los activos: Se tiene un control adecuado de los activos de información con custodios asignados para cada uno y un inventario actualizado de los mismos, sin embargo, no se han implementado procesos para clasificar la información.
- Seguridad de los recursos humanos: En esta cláusula el departamento de Talento Humano tiene claros los procedimientos para la gestión de contratación de nuevo personal y comunicación de responsabilidades a los funcionarios, antes, durante y al finalizar sus labores, sin embargo, no se ha incluido el acuerdo de confidencialidad al formalizar los contratos laborales.

- Seguridad física y del entorno: La Institución se esfuerza por precautelar la seguridad física de los recursos informáticos con las medidas de asignación de responsables de los activos, pero de manera física existen falencias especialmente en el cuarto de equipos debido a que no cuentan con sistemas de refrigeración y acceso físico adecuado y no se separan las líneas de cableado eléctrico y de datos correctamente, de manera que se necesita reforzar la seguridad física de los activos.
- Gestión de comunicaciones y operaciones: Existen procedimientos adecuados para la gestión de comunicaciones y operaciones incluyendo la documentación respectiva de los mismos mediante informes mensuales, sin embargo, la actualización de sistemas operativos, el control de conexión de dispositivos móviles, la ausencia de métodos de autenticación de acceso a las redes y una red plana sin segmentos lógicos son procesos que necesitan trabajarse y asegurar.
- Control de acceso: Esta es la cláusula con menor porcentaje de cumplimiento debido a que varios controles no se cumplen, como por ejemplo la ausencia de: perfiles de usuario para el acceso a servicios y recursos de red, mecanismos de encriptación para la transmisión de datos sobre la red, control de puertos, segmentos lógicos de red, control de tiempos de conectividad a la red, mecanismos de autenticación de usuarios, entre otros.
- Adquisición, desarrollo y mantenimiento de sistemas de información: Los responsables del área de TIC quienes monitorean el buen estado de los equipos informáticos tienen definidos los procesos para garantizar el cumplimiento de esta cláusula, pero no se han tomado medidas pertinentes con el manejo de información confidencial y cómo asegurarla.

- Gestión de los incidentes de la seguridad de la información: La política interna es una base para alertar a los funcionarios acerca del buen uso de los recursos y servicios informáticos, con una debida comunicación, capacitación y uso de herramientas tecnológicas es posible gestionar adecuadamente los incidentes en la seguridad de la información.
- Gestión de la continuidad del negocio: La institución cuenta con un generador eléctrico, sistemas UPS y servidores como backup para asegurar la continuidad de las actividades y prestación de servicios, sin embargo, no se realizan mapas de riesgos para identificar y priorizar riesgos para decidir sobre cómo tratarlos.
- Cumplimiento: El HSLO al ser una entidad pública se encuentra sujeta a la normativa legal y reglamentaria del Estado, en lo que respecta a la seguridad de los equipos informáticos, aún se necesitan tomar medidas para el uso de software propietario, como la adquisición de licencias corporativas, y así evitar posibles sanciones por violación de derechos de autor.

A partir del conocimiento del nivel de cumplimiento de esta normativa, ya se evidencia que existen ciertos procesos que necesitan gestionarse para que la Institución garantice que el EGSI se implementa e incluye dentro de los procesos y actividades de aseguramiento de los sistemas de información.

3.2 Diseño del Gobierno de TI

El diseño del Gobierno de TI para el HSLO se desarrolla en base a COBIT 5 donde se realiza un mapeo de objetivos dispuestos en matrices que provee este marco de control, con la finalidad de identificar los puntos débiles relacionados con la administración de las TI.

3.2.1 Estudio de la Institución.

En esta etapa se identifican los componentes estratégicos de la Institución, hacia dónde se dirige, sus metas, instalaciones físicas, capital humano, infraestructura de TI y cartera de servicios, es decir, ampliar esta información para conocer cómo opera internamente. En la Figura 7 se muestra una vista exterior frontal del Hospital San Luis de Otavalo.

Figura 7. Hospital San Luis de Otavalo

Fuente: Autoría propia

3.2.1.1 Antecedentes.

En 1923, Lucía Sornear una monja Superiora del Colegio Inmaculada organiza La liga de la caridad Pro Hospital de Otavalo y dentro de 1 año adquirió un lote de terreno para la construcción del Hospital. El sacerdote francés Bruning elaboró los planos en 1925 y finalmente se inaugura la obra el 6 de septiembre de 1953.

En la actualidad el HSLO ofrece el servicio de salud pública, pertenece a la Función Ejecutiva y su autoridad sanitaria es el MSP. El Decreto Ejecutivo N° 557 publicado en el Registro Oficial N° 290 en mayo del 2012 acuerda en su artículo 1 desconcentrar por distritos y circuitos a las casas de salud en todo el país, por lo cual al

HSLO se le denomina Distrito de Salud 10D02. La Institución se encuentra ubicada en la ciudad de Otavalo en las calles Sucre S/N y Estados Unidos.

3.2.1.2 Misión y Visión.

- **Misión:** El Hospital San Luis de Otavalo, presta servicios de salud con calidad y calidez en el ámbito de la asistencia especializada, a través de su cartera de servicios cumpliendo con la responsabilidad de promoción, prevención, recuperación, rehabilitación de la salud integral, docencia e investigación conforme a las políticas del MSP y el trabajo en red en el marco de la justicia y equidad social (MSP, 2012, pág. 5).
- **Visión:** Ser reconocido por la ciudadanía como un Hospital accesible que presta una atención de calidad que satisface las necesidades y expectativas de la población bajo principios fundamentales de salud pública y bioética, utilizando la tecnología y los recursos públicos de forma eficiente y transparente (MSP, 2012, pág. 5).

3.2.1.3 Valores.

Además de la entrega de servicios, creación de valor y cumplimiento de los objetivos estratégicos, los valores son fundamentales para la definición de la ética institucional que aporta en la calidad y calidez en la entrega oportuna de servicios (Figura 8).

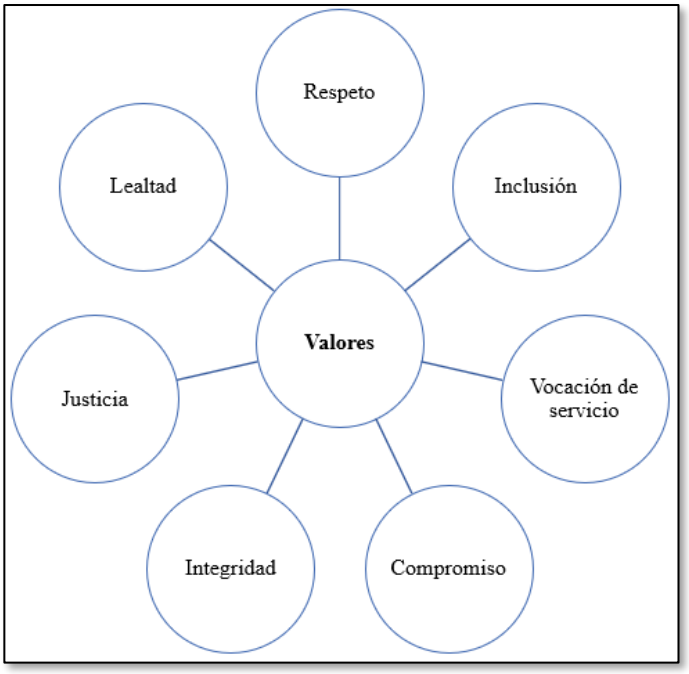


Figura 8. Valores del HSLO

Fuente: Coordinación General de Planificación HSLO

3.2.1.4 Objetivos estratégicos.

Los objetivos estratégicos (Tabla 11) tienen una estrecha relación con la misión y visión institucionales debido a que garantizan su cumplimiento.

Tabla 11. Objetivos Estratégicos de la Institución

Núm.	Objetivos
Objetivo 1	Garantizar la equidad en el acceso y gratuidad de los servicios.
Objetivo 2	Trabajar bajo los lineamientos del Modelo de Atención Integral de Salud de forma integrada y en red con el resto de las Unidades Operativas de Salud del MSP y otros actores de la red pública y privada complementaria que conforman el Sistema Nacional de Salud del Ecuador.
Objetivo 3	Mejorar la accesibilidad y el tiempo de espera para recibir atención, considerando la diversidad de género, cultural, generacional, socio económica, lugar de origen y discapacidades.
Objetivo 4	Involucrar a los profesionales en la gestión del hospital, aumentando su motivación, satisfacción y compromiso con la misión del hospital.

Objetivo 5	Garantizar una atención de calidad y respeto a los derechos de las y los usuarios, para lograr la satisfacción con la atención recibida.
Objetivo 6	Desarrollar una cultura de excelencia con el fin de optimizar el manejo de los recursos públicos, y la rendición de cuentas.

Fuente: Adaptado de (MSP, 2012)

3.2.1.5 Estructura organizacional de gestión por procesos.

Los procesos internos (Tabla 12) son los que permiten dar cumplimiento a la misión y responsabilidades del HSLO.

Tabla 12. Estructura organizacional de Gestión por Procesos HSLO

Proceso	Descripción
1. Proceso Gobernante	1.1 Gerencia Hospitalaria
2. Procesos Agregadores de Valor	2.1 Especialidades Clínicas y/o Quirúrgicas
	2.2 Gestión de Cuidados de Enfermería
	2.3 Gestión de Diagnóstico y Apoyo Terapéutico
	2.4 Gestión de Docencia e Investigación
3. Procesos Habilitantes de Asesoría	3.1 Gestión de Calidad
	3.2 Gestión de Planificación, seguimiento y evaluación de la gestión
4. Procesos Habilitantes de Apoyo	4.1 Gestión de Atención al usuario
	4.2 Gestión de Admisiones
	4.3 Gestión Administrativa – Financiera
	4.3.1 Gestión de Talento Humano
	4.3.2 Gestión Financiera
	4.3.3 Gestión Administrativa
	4.3.4 Gestión de Tecnologías de la Información y Comunicación

Fuente: Adaptado de (MSP, 2012)

3.2.1.6 Organigrama organizacional.

El Estatuto Orgánico de Gestión Organizacional por Procesos del Ministerio de Salud Pública sostiene que la estructura organizacional de las entidades de Salud tiene diferentes enfoques dependiendo del número de camas. El HSLO es considerado como un Hospital menor a 70 camas, por lo tanto, la estructura organizacional del HSLO es como se describe en la Figura 9.

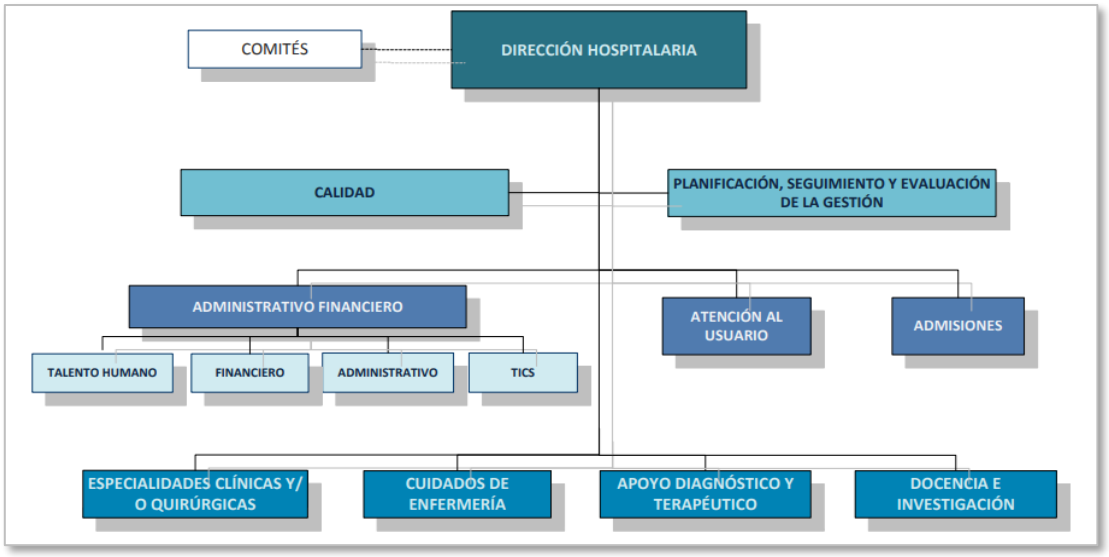


Figura 9. Organigrama organizacional del HSLO

Fuente: Recuperado de (MSP, 2012)

3.2.1.7 Instalaciones físicas.

Las instalaciones del HSLO se encuentran distribuidas según su estructura organizacional por oficinas y consultorios (Tabla 13). Las oficinas son las áreas donde los funcionarios realizan sus labores administrativas, mientras que en los consultorios los profesionales de salud prestan servicios de atención médica a los ciudadanos. Actualmente la Institución cuenta con 18 oficinas y 12 consultorios.

Tabla 13. Oficinas y consultorios del HSLO

Oficinas	Consultorios
Gestión TIC'S	Rehabilitación y Terapia Física
Farmacia	Odontología
Talento Humano	Consulta Externa y/o General
Gerencia	Psicología
Secretaría de Gerencia	Pediatría
Administración de caja	Ecografía
Gestión Financiera	Emergencia
Gestión SOAT	Gineco-Obstetricia
Gestión y Calidad de los Servicios	Laboratorio Clínico
Dirección Asistencial	Salud Ocupacional
Administrativo Zonal	Imagenología
Estadística	Cardiología
Trabajo Social	Quirófanos
Información	

Traumatología
Laboratorio Clínico
Servicios Institucionales

Fuente: Oficina de Gestión de Planificación HSLO

3.2.1.8 Capital Humano.

Dentro del HSLO los funcionarios desempeñan labores administrativas, médicas y de limpieza hospitalaria (Figura 14), la Institución cuenta con 252 funcionarios, recalcando que, al tratarse de un Hospital, el número de profesionales de salud varía y podría alterar la cantidad total de funcionarios.

Tabla 14. Capital humano del HSLO

Descripción	Total
Profesionales de Salud	140
Auxiliares laboratorio médico y enfermería	43
Personal de Nutrición	1
Personal Administrativo	29
Personal de Servicios	39
Total	252

Fuente: Oficina de Gestión de Planificación HSLO

3.2.1.9 Cartera de servicios.

Los servicios que la Institución ofrece son: Consulta Externa, Emergencia y Hospitalización (Tabla 15) centrados en la atención integral preventiva y curativa.

- En el área de Emergencia se provee atención inmediata a pacientes con cuadros de salud altamente sensibles según los protocolos de salud asignados por el MSP.
- En Consulta Externa se presta servicios médicos en sus distintas áreas de especialidad donde se diagnostica oportunamente a los pacientes.
- En el área de Hospitalización se brinda atención médica y cuidados básicos a pacientes que requieran seguimiento y que se encuentren en etapa de recuperación de su salud.

Tabla 15. Cartera de servicios del HSLO

Servicios	Especialidades	
Emergencia		
Consulta Externa	- Cirugía general	- Cardiología
	- Traumatología	- Nutrición
	- Gineco-obstetricia	- Estomatología
	- Pediatría	- Diagnóstico de rayos X
	- Neonatología	- Ecografía
	- Psicología	- Laboratorio clínico
	- Medicina Interna	- Rehabilitación
	- Psiquiatría	- Farmacia
Hospitalización	- Cirugía	- Traumatología
	- Pediatría	- Gineco-obstetricia
	- Medicina Interna	

Fuente: Coordinación General de Planificación HSLO

3.2.1.10 Unidad de Tecnologías de la Información y Comunicación (TIC).

La Unidad de Tecnologías de la Información y Comunicación del HSLO actualmente se ha convertido en el eje transversal de la gestión administrativa de la Institución y en gestor de apoyo tecnológico para sus actividades técnico-médicas. De acuerdo con el (MSP, 2012, pág. 40) los productos y servicios a su responsabilidad son:

- Mantenimiento de líneas de red y programas informáticos;
- Informes sobre las acciones preventivas y correctivas de software, hardware y redes de conectividad;
- Plan de mejoramiento de redes y plan de contingencias sobre respaldos de información;
- Correo institucional;
- Servicio de internet;
- Inventario de los equipos tecnológicos computacionales;
- Actas de la entrega recepción de los equipos adquiridos en coordinación con las áreas de Activos Fijos y Bodega;

- Informes de funcionamiento de los equipos adquiridos en coordinación con las áreas de Activos Fijos y Bodega;
- Traslado de equipos en coordinación con las áreas de Activos Fijos y Bodega.

En la actualidad, el área de TIC está a cargo de dos funcionarios: Ing. Manuel Guaján (Informático HSLO) y Tnlgo. Omar Albuja (Asistente de Sistemas).

3.2.1.11 Situación actual de la red de datos.

La red de datos de la Institución está conformada por equipos de conmutación en las capas de acceso y distribución, dispositivos finales como computadoras e impresoras, servidores que gestionan servicios propios para la Institución, una red inalámbrica constituida por siete Access Point y cableado estructurado categoría 5e (no certificado).

CNT (Corporación Nacional de Telecomunicaciones) es el proveedor del servicio de Internet entregando un enlace simétrico de 15 Mbps mediante fibra óptica, adicionalmente, ofrece un pool de cinco direcciones IP públicas. La característica de la red LAN (Red de área local) es que es plana, es decir sin segmentos lógicos de red. El estado del cableado estructurado no se encuentra en óptimas condiciones debido a que no se están cumpliendo con los estándares sugeridos.

En la Figura 10 se ilustra un diagrama topológico que representa a la red física de la red de datos actual y la interconexión de dispositivos a través de medios cableados e inalámbricos. La red interna o privada inicia desde la interfaz LAN del servidor Pfsense 1, en donde además de computadores e impresoras se encuentran dos servidores internos: Aplicaciones y FTP[1], mientras que los servidores: Zimbra, NextCloud y OTRS poseen direcciones IP públicas, para poder ser vistos y accedidos desde redes externas. El servidor Pfsense 2 por su parte, controla los accesos de los usuarios inalámbricos a determinados sitios web autorizados.

[1] Protocolo de Transferencia de Archivos

Los servidores Pfsense son los encargados de la seguridad perimetral los cuales representan al núcleo de la red, mientras que los conmutadores ubicados en el rack de equipos constituyen la capa de distribución debido a que a ellos se interconectan otros conmutadores que conforman la capa de acceso.

Nota: Por motivos de seguridad el direccionamiento IP no puede observarse en las topologías física y lógica de la red de datos.

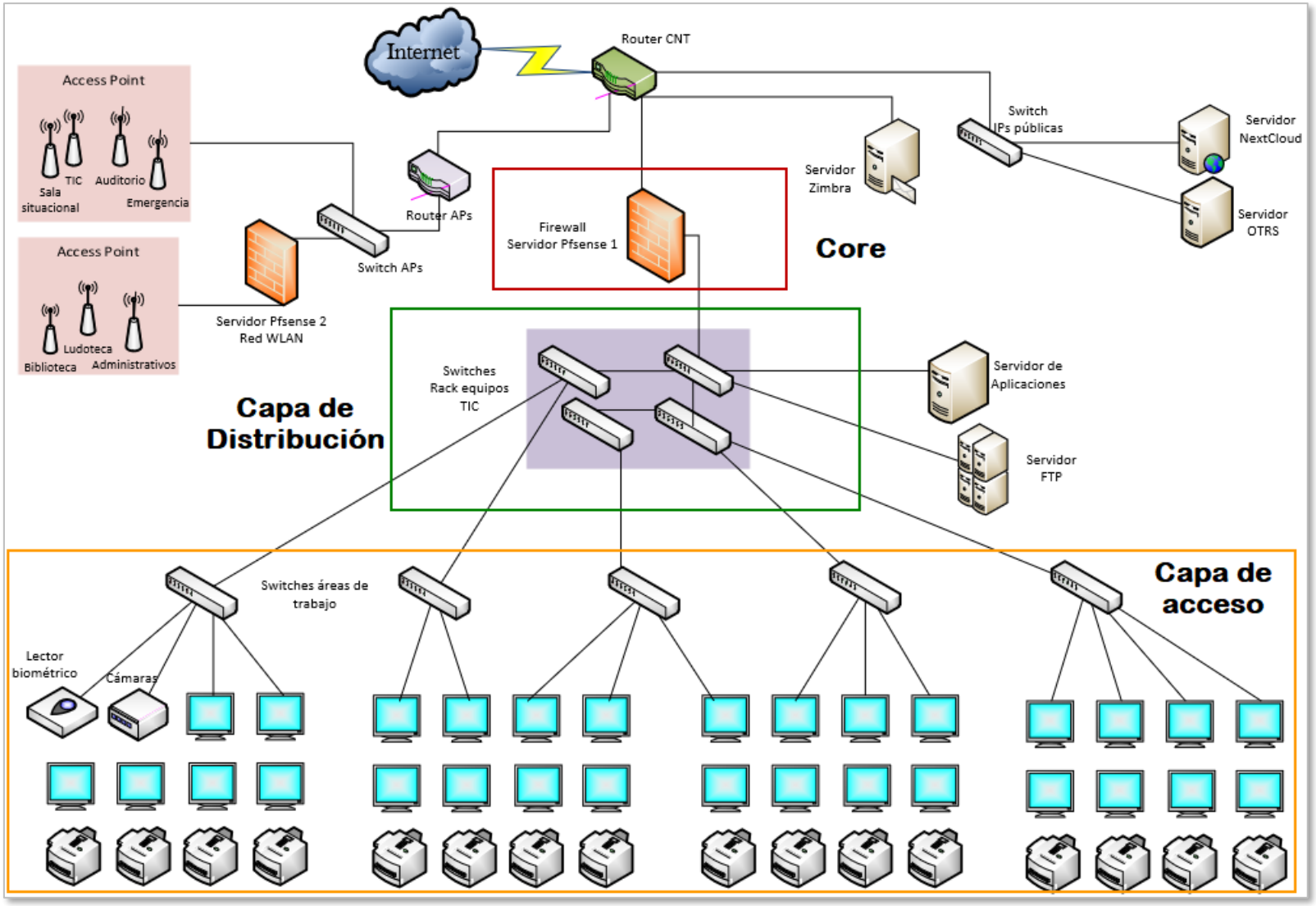


Figura 10. Topología Física de la Red de Datos HSLO

Fuente: Adaptado de Oficina de Gestión de TIC

En la Figura 11 se ilustra la topología lógica de la red de datos del HSLO, donde se detallan las áreas en las cuales se ubica cada conmutador de la capa de acceso. No existen puntos de red destinados para cada dispositivo final, es por ello que a partir de los puertos de los conmutadores de la capa de distribución se interconectan otros conmutadores de diferentes cantidades de puertos para abastecer la conexión a la red de datos a los dispositivos restantes.

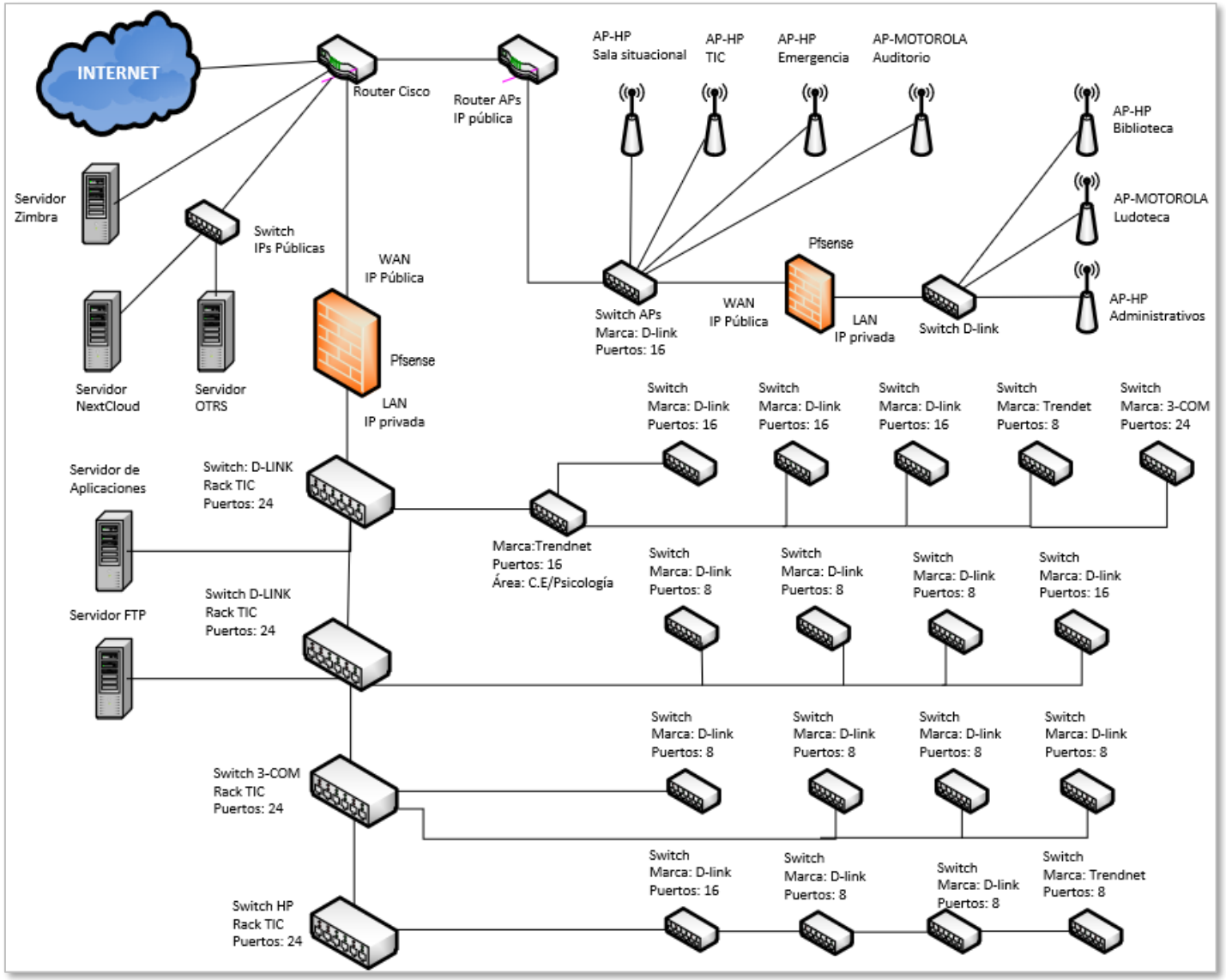


Figura 11. Topología Lógica de la Red de Datos del HSLO

Fuente: Adaptado de Oficina de Gestión de TIC

La oficina de Gestión de TIC comparte su espacio con el cuarto de equipos que junto con los computadores ubicados en las áreas de trabajo de cada funcionario conforman la red de datos de la Institución.

El rack que aloja a los principales equipos de comunicaciones es de 42 U (U=Unidades de Rack) y contiene: 1 servidor de correo institucional Zimbra, 2 servidores Pfsense, 1 servidor de Aplicaciones, 1 servidor FTP, 1 servidor OTRS, 1 servidor NextCloud, 4 Patch Panel de 24 puertos, 2 switches D-LINK DGS-1224T de 24 puertos, 1 switch HP V1910-24G de 24 puertos, 1 switch 3COM de 24 puertos, 1 UPS (Sistema de Alimentación Ininterrumpida), 1 router Cisco serie 800 (Propiedad del proveedor de Internet), Grabador de cámaras de videovigilancia. En la Figura 12 se puede apreciar la disposición del rack de equipos del área de TIC.

Figura 12. Cuarto de equipos

Fuente: Oficina de Gestión de TIC

3.2.2 Cascada de metas de COBIT 5.

Para iniciar la cascada de metas de COBIT 5 se procede a clasificar los objetivos estratégicos de la Institución según las cuatro perspectivas del CMI (Cuadro de Mando Integral) de COBIT 5 (Tabla 16).

Tabla 16. Clasificación de objetivos estratégicos del HSLO según perspectivas del CMI

Perspectiva	Objetivos estratégicos de la Institución
Financiera	• Garantizar la equidad en el acceso y gratuidad de los servicios
Cliente	• Mejorar la accesibilidad y el tiempo de espera para recibir atención, considerando la diversidad de género, cultural, generacional, socio económica, lugar de origen y discapacidades. • Garantizar una atención de calidad y respeto a los derechos de las y los usuarios, para lograr la satisfacción con la atención recibida.
Interna	• Desarrollar una cultura de excelencia con el fin de optimizar el manejo de los recursos públicos, y la rendición de cuentas.
Aprendizaje	• Trabajar bajo los lineamientos del Modelo de Atención Integral de Salud de forma integrada y en red con el resto de las Unidades Operativas de Salud del MSP y otros actores de la red pública y privada complementaria que conforman el Sistema Nacional de Salud del Ecuador. • Involucrar a los profesionales en la gestión del hospital, aumentando su motivación, satisfacción y compromiso con la misión del hospital.

Fuente: Adaptado de (MSP, 2012)

La primera matriz mapea los objetivos corporativos de COBIT 5 vs. los objetivos estratégicos de la Institución (Tabla 18), en ella se demuestra cómo los objetivos estratégicos de la Institución son soportados o tienen un mayor vínculo con las metas corporativas genéricas de COBIT 5, para valorar los resultados de la matriz se utilizan las ponderaciones señaladas en la Tabla 17.

Tabla 17. Ponderaciones para el mapeo de metas corporativas de COBIT 5 y objetivos estratégicos de la Institución

Escala		Descripción
P	Principal	Cuando existe una fuerte relación entre dichas metas corporativas.
S	Secundario	Cuando todavía hay un vínculo fuerte, pero menos importante, es decir, las metas corporativas de COBIT 5 son un soporte secundario para los objetivos estratégicos de la Institución.
N	Ninguno	Cuando las metas corporativas de COBIT 5 no tienen vínculo alguno o no soporta a los objetivos estratégicos de la Institución.

Fuente: Adaptado de (ISACA, 2012)

Nota: Esta primera matriz se elaboró juntamente con los principales directivos de la Institución, Jefe del área de Planificación y Gestión de Proyectos, Jefe del área de TIC y Director.

Tabla 18. Mapeo entre metas corporativas de COBIT 5 y objetivos estratégicos de la Institución

P=5 S=1 N=0		**OBJETIVOS ESTRATÉGICOS DE LA INSTITUCIÓN RELACIONADOS CON LOS OBJETIVOS CORPORATIVOS DE COBIT 5**	**Objetivos estratégicos de la Institución**						
			Garantizar la equidad en el acceso y gratuidad de los servicios	Mejorar la accesibilidad y el tiempo de espera para recibir atención, considerando la diversidad de género, cultural, generacional, socio económica, lugar de origen y discapacidades	Garantizar una atención de calidad y respeto a los derechos de las y los usuarios, para lograr la satisfacción con la atención recibida	Desarrollar una cultura de excelencia con el fin de optimizar el manejo de los recursos públicos, y la rendición de cuentas	Trabajar bajo los lineamientos del Modelo de Atención Integral de Salud de forma integrada y en red con el resto de las Unidades Operativas de Salud del Ministerio de Salud Pública y otros actores de la red pública y privada complementaria que conforman el sistema nacional de salud del Ecuador	Involucrar a los profesionales en la gestión del hospital, aumentando su motivación, satisfacción y compromiso con la misión del hospital	
FINANCIERA		**Objetivos corporativos de COBIT 5**	**FINANCIERA**	**CLIENTE**		**INTERNA**	**APRENDIZAJE**		**Total**
	1	Valor para las partes interesadas de las Inversiones de Negocio	S	P	P	P	P	S	22
	2	Cartera de productos y servicios competitivos	P	P	P	N	P	P	26
	3	Riesgos de negocio gestionados (salvaguarda de activos)	P	S	P	P	P	P	26
	4	Cumplimiento de leyes y regulaciones externas	P	P	S	N	P	S	18
	5	Transparencia financiera	N	N	S	S	N	S	3
CLIENTE	6	Cultura de servicio orientada al cliente	P	P	P	P	P	P	30
	7	Continuidad y disponibilidad del servicio de negocio	P	P	P	P	P	P	30
	8	Respuestas ágiles a un entorno de negocio cambiante	S	P	P	P	P	P	26
	9	Toma estratégica de Decisiones basada en Información	S	P	P	P	P	P	26

	10	Optimización de costes de entrega del servicio	P	S	P	P	S	P	22
INTERNA DE PROCESOS	11	Optimización de la funcionalidad de los procesos de negocio	P	P	S	S	P	P	22
	12	Optimización de los costes de los procesos de negocio	P	S	S	P	S	P	13
	13	Programas gestionados de cambio en el negocio	N	S	S	S	S	S	4
	14	Productividad operacional y de los empleados	P	S	S	P	P	P	22
	15	Cumplimiento con las políticas internas	P	P	P	P	P	P	30
APRENDIZAJE	16	Personas preparadas y motivadas	P	P	P	P	P	P	30
	17	Cultura de innovación de producto y negocio	P	P	S	P	N	P	21

Fuente: Adaptado de (ISACA, 2012)

De la primera matriz, se han considerado los objetivos con un valor superior a 25, que representan los objetivos corporativos de COBIT 5 de mayor utilidad para dar cumplimiento a los objetivos estratégicos institucionales y superar los inconvenientes relacionados con las TI (Tabla 19).

Tabla 19. Priorización de objetivos corporativos de COBIT 5

N°	Perspectiva	Objetivos coporativos de COBIT 5
1	Financiera	Cartera de productos y servicios competitivos
2	Financiera	Riesgos de negocio gestionados (salvaguarda de activos)
3	Cliente	Cultura de servicio orientada al cliente
4	Cliente	Continuidad y disponibilidad del servicio de negocio
5	Cliente	Respuestas ágiles a un entorno de negocio cambiante
6	Cliente	Toma estratégica de Decisiones basada en Información
7	Interna de procesos	Cumplimiento con las políticas internas
8	Aprendizaje	Personas preparadas y motivadas.

Fuente: Adaptado de (ISACA, 2012)

3.1.2.1 Mapeo de metas de TI con metas corporativas de COBIT 5.

Los objetivos corporativos de COBIT 5 resultantes ahora se mapean con los objetivos de TI de COBIT 5 (Tabla 20). Para esta matriz, se sumarán los valores de las filas que correspondan con las columnas de los objetivos corporativos resaltados para encontrar cuál objetivo u objetivos de TI de COBIT 5 soportan a los objetivos corporativos previamente seleccionados.

Nota: La matriz 20 se elabora en base a la matriz genérica de COBIT 5 y se califican o valoran utilizando las mismas ponderaciones mencionadas en la Tabla 17.

Tabla 20. Mapeo entre metas de TI con objetivos corporativos de COBIT 5

P=5 S=1		OBJETIVOS CORPORATIVOS DE COBIT 5 RELACIONADOS CON LOS OBJETIVOS DE TI DE COBIT 5	Objetivos corporativos de COBIT 5																	
			Valor para las partes interesadas de las Inversiones de Negocio	Cartera de productos y servicios competitivos	Riesgos de negocio gestionados (salvaguarda de activos)	Cumplimiento de leyes y regulaciones externas	Transparencia financiera	Cultura de servicio orientada al cliente	Continuidad y disponibilidad del servicio de negocio	Respuestas ágiles a un entorno de negocio cambiante	Toma estratégica de decisiones basada en Información	Optimización de costes de entrega del servicio	Optimización de la funcionalidad de los procesos de negocio	Optimización de los costes de los procesos de negocio	Programas gestionados de cambio en el negocio	Productividad operacional de los empleados	Cumplimiento con las políticas internas	Personas preparadas y motivadas	Cultura de innovación de producto y negocio	
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	
		Objetivos de TI de COBIT 5	**FINANCIERA**					**CLIENTE**					**INTERNA DE PROCESOS**					**APRENDIZAJE**		**Total**
FINANCIERA	1	Alineamiento de TI y la estrategia del negocio	P	P	S			P	S	P	P	S	P	S	P			S	S	23
	2	Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas			S	P											P			6
	3	Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI	P	S	S					S	S		S		P			S	S	5
	4	Riesgos de negocio relacionados con las TI gestionados			P	S			P	S		P			S		S	S		13

	5	Realización de beneficios del portafolio de Inversiones y Servicios relacionados con las TI	P	P				S		S		S	S	P		S			S	7
	6	Transparencia de los costes, beneficios y riesgos de la TI	S		S		P				S	P		P						2
CLIENTE	7	Entrega de servicios de TI de acuerdo a los requisitos del negocio	P	P	S	S		P	S	P	S		P	S	S			S	S	19
	8	Uso adecuado de aplicaciones, información y soluciones tecnológicas	S	S	S			S	S		S	S	P	S		P		S	S	6
INTERNA DE PROCESOS	9	Agilidad de las TI	S	P	S			S		P			P	-	S	S		S	P	13
	10	Seguridad de la información, infraestructuras de procesamiento y aplicaciones			P	P			P								P			15
	11	Optimización de activos, recursos y capacidades de las TI	P	S						S		P	S	P	S	S			S	2
	12	Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio	S	P	S			S		S		S	P	S	S	S			S	8
	13	Entrega de Programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad	P	S	P			S				S		S	P					7
	14	Disponibilidad de información útil y relevante para la toma de decisiones	S	S	S	S			P		P		S							12
	15	Cumplimiento de TI con las políticas internas			S	S											P			6
APRENDIZAJE	16	Personal del negocio y de las TI competente y motivado	S	S	P			S		S						P		P	S	12
	17	Conocimiento, experiencia e iniciativas para la innovación de negocio	S	P				S		P	S		S		S			S	P	13

Fuente: Adaptado de (ISACA, 2012)

De la Tabla 20 se han seleccionado aquellos objetivos de TI de COBIT 5 con valores superiores a 15 que son los más representativos y dan soporte a los objetivos corporativos de COBIT 5 como lo indica la Tabla 21.

Tabla 21. Priorización de objetivos de TI de COBIT 5

N°	Perspectiva	Objetivos de TI de COBIT 5
1	Financiera	Alineamiento de TI y la estrategia del negocio
2	Cliente	Entrega de servicios de TI de acuerdo a los requisitos del negocio
3	Interna de procesos	Seguridad de la información, infraestructuras de procesamiento y aplicaciones

Fuente: Adaptado de (ISACA, 2012)

3.2.3 Priorización de procesos de COBIT 5.

En esta etapa se identifican los procesos de TI de COBIT 5 que soportan a los objetivos de TI de COBIT 5 (Tabla 22) previamente priorizados con la finalidad de conocer cuáles procesos de TI permiten cumplir con los objetivos de TI. Para ello, se suman los valores de las filas que correspondan con las columnas de los objetivos de TI de COBIT 5 resultantes y así obtener los procesos con mayor puntuación y en los cuales la Institución debería trabajar para lograr un adecuado Gobierno y Gestión de las TI.

Nota: La siguiente matriz (Tabla 22) se elabora en base a la matriz genérica de COBIT 5 y para valorar los procesos de TI se utilizan las mismas ponderaciones mencionadas en la Tabla 17.

Como resultado de la Tabla 22 se tiene que los procesos que soportan o permiten alcanzar los objetivos de TI son los que tienen un mayor vínculo representados por los de puntuación más alta (Tabla 23).

Tabla 23. Procesos de TI de COBIT 5 resultantes para lograr los objetivos estratégicos de la Institución

N°	Dominio	Procesos de TI de COBIT 5
1	EDM01	Asegurar el establecimiento y mantenimiento del Marco de Gobierno
2	EDM02	Asegurar la entrega de beneficios
3	APO01	Gestionar el marco de gestión de TI
4	APO02	Gestionar la estrategia
5	APO03	Gestionar la arquitectura empresarial
6	APO08	Gestionar las relaciones
7	APO10	Gestionar los proveedores
8	APO12	Gestionar el riesgo
9	APO13	Gestionar la seguridad
10	BAI02	Gestionar la definición de requisitos
11	BAI06	Gestionar los cambios

Fuente: Adaptado de (ISACA, 2012)

Estas etapas desarrolladas son parte del diseño del Gobierno de TI para el Hospital San Luis de Otavalo, donde la técnica de la cascada de metas de COBIT 5 permitió alinear los objetivos estratégicos de la Institución con los objetivos y procesos de TI de COBIT 5, partiendo de una alineación de metas de alto nivel para luego decantar en metas relacionadas con las TI adaptadas a la realidad de la Institución y que ayudarán a un mejor desempeño de la misma.

El alcance del presente proyecto está enfocado en la Seguridad de la Información, motivo por el cual se gestionarán los Riesgos y la Seguridad de la información (Procesos APO12, APO13) que se obtuvieron como resultado de la cascada de metas de COBIT 5.

3.3 Análisis de Riesgos

El proceso del Análisis de Riesgos de la Seguridad de la Información comprende un conjunto de actividades a ser desarrolladas en base a las directrices de la normativa NTE INEN ISO/IEC 27005:2012.

3.3.1 Establecimiento del contexto.

El propósito de la gestión del riesgo de la Seguridad de la Información en el HSLO consiste en evaluar los riesgos asociados a los activos de información identificando sus principales amenazas y vulnerabilidades.

3.3.1.2 Criterios básicos.

Los criterios básicos son los que ayudarán a evaluar los riesgos y para efectos del presente proyecto se han definido los siguientes:

- Criterios para valorar los activos de información
- Criterios para valorar la probabilidad del escenario de incidente
- Criterios para valorar el impacto en el negocio
- Criterios para evaluar (valorar) el riesgo

3.3.1.3 Alcance y límites.

El alcance aborda a los activos de información del HSLO considerados dentro de la gestión del riesgo, esto incluye a la información en formato electrónico la cual es vital que permanezca disponible y se preserve su integridad y confidencialidad.

3.3.2 Valoración del riesgo.

La valoración del riesgo consiste en identificar a los activos de información a fin de proveer un mayor detalle sobre lo que ocurre con ellos, si existe una estructura organizacional adecuada, cual es el rol que desempeñan en la Institución y conocer su nivel de riesgo a través de la Matriz de Riesgos.

3.3.2.1 Identificación del riesgo.

Esta etapa consiste en la identificación de todos los activos de información dentro del alcance establecido y se realiza un listado con un nivel adecuado de detalle que proporcione información suficiente para la valoración del riesgo. Los activos de información se dividen en dos clases (Tabla 24).

Tabla 24. Clases de activos

Clase	Activos
Primarios	Procesos y actividades del negocio
	Información o datos
De soporte	Hardware
	Software
	Redes
	Personal
	Ubicación

Fuente: Adaptado de (INEN, 2012)

Los procesos y actividades, información o datos, constituyen la razón de ser de la Institución y por ello pertenecen a la clase de activos primarios como la Tabla 25 lo indica.

Tabla 25. Activos primarios del HSLO

Tipo	Activos	Descripción
Procesos y actividades del negocio	Servicio de Emergencia	Servicio de atención médica inmediata para pacientes en estado crítico o de alto riesgo.
	Servicio de Consulta Externa	Servicio de diagnóstico y seguimiento para pacientes en las diferentes especialidades de la Institución.
	Servicio de Hospitalización	Servicio de atención médica y cuidados básicos para pacientes en observación y que requieren tratamiento o seguimiento durante su recuperación.
Información o datos	Resultados de laboratorio clínico	Información personal de cada paciente sobre el análisis de sustancias corporales y diagnóstico de enfermedades.

	Información de las áreas administrativas	Información que se lleva sobre el control y organización de los recursos de la Institución.
	Historias clínicas	Información que contiene registros de las atenciones médicas que han recibido los pacientes y es un instrumento para futuros seguimientos.
	Archivos de trabajo del personal	Toda la documentación generada durante la jornada laboral de los funcionarios y que yace en sus ordenadores.
	Archivos de Imagenología	Conjunto de archivos generados por médicos especialistas en el área de imagenología de Rayos X.

Fuente: Oficina de Gestión de Planificación

Los activos de soporte son aquellos que dan soporte a los activos primarios y que se describen a continuación.

3.3.2.1.1 Hardware.

El hardware comprende los equipos informáticos que forman parte de la red de datos de la Institución.

- **Computadores portátiles y de escritorio:** Actualmente se utilizan dos tipos de Sistemas Operativos en los computadores de los usuarios: Windows y Linux, cada uno de ellos en distintas versiones, por ejemplo 7 y 8.1 para Windows mientras que en Linux se utiliza la versión Linux Mint 17 con un entorno gráfico de escritorio atractivo para los usuarios (Tabla 26). El listado detallado de los computadores se encuentra en el Anexo B al final del documento.

Tabla 26. Computadores portátiles y de escritorio

Tipo	**Sistema Operativo**	**Cantidad**	**Tiene licencia**	**Antivirus**
			Sí, No, NA	
Portátiles	Windows XP	1	No	1
	Windows 7	4	No	4
	Linux Mint 17	1	NA	1
Escritorio	Windows XP	1	No	1
	Windows 7	16	No	13
	Windows 8	9	No	9
	Windows 8.1 Pro	7	No	6
	Windows 10	1	No	1
	Linux Mint 17	77	NA	77
Total		118		114

Fuente: Oficina de Gestión de TIC

Existe un total de 118 computadores tanto de escritorio como portátiles, ninguno de los equipos con sistema operativo Windows posee licencia, por lo cual la Institución puede ser sancionada a causa del uso de software no propietario.

- **Servidores:** Son el conjunto de equipos que aloja distintas plataformas o aplicaciones para proveer servicios a la Institución, se ubican en el rack del cuarto de equipos del área de Gestión de TIC del HSLO y son administrados por los responsables de dicha área. La Tabla 27 describe a cada uno de ellos con sus respectivos detalles técnicos.

Tabla 27. Listado de servidores del HLSO

Servidor	Descripción	Marca	Procesador	RAM	Tamaño en Disco	Sistema Operativo	Licencia	Antivirus
Pfsense	Servidor utilizado como firewall perimetral, actualmente tiene implementado un servidor proxy modo no transparente para filtrado de sitios web mediante nombres de dominio.	LENOVO	Core I7	4 GB	1 TB	CentOS 7	NA	NO
Zimbra	Servidor de correo electrónico institucional.	HP	Core I7	4 GB	1 TB	CentOS 7	NA	NO
FTP	Servidor de archivos para la compartición de información generada en las áreas de Imagenología, Rayos X y Ecografía.	HP	Xeon	8 GB	2 TB	Windows Server 2008	NO	Nod 32 Antivirus
Aplicaciones	Soporta múltiples aplicaciones como las de las oficinas de Financiero, Activos Fijos, Bodega y Talento Humano.	HP	Xeon	4 GB	1 TB	Windows Server 2008	NO	NOD 32 Antivirus
NextCloud	Sistema de solicitud de tiquetes de código abierto utilizado para la solicitud de servicios interdepartamentales.	LENOVO	Core I7	4 GB	1 TB	CentOS 7	NA	NO
OTRS	Servidor de archivos semejante a Google Drive para el almacenamiento de información.	LENOVO	Core I7	4 GB	1 TB	CentOS 7	NA	NO

Fuente: Oficina de Gestión de TIC

- **Impresoras y copiadoras:** Permiten obtener de forma impresa la información generada por las/los funcionarios para fines laborales (Tabla 28). Se ubican en las distintas dependencias del HSLO y tienen a un responsable a cargo del activo, 20 de ellas poseen tarjetas de red, por lo cual tienen designada una dirección IP local.

Tabla 28. Listado de impresoras y copiadoras

Marca	Responsable	Ubicación	Tecnología de impresión
LEXMARK 611	López Maritza	Laboratorio Clínico	Láser
LEXMARK 611	Pomasqui Guido	Secretaría Dirección	Láser
LEXMARK 611	Montalvo Rodrigo	Admisiones	Láser
LEXMARK 611	Ayala Rocío	Quirófano	Láser
LEXMARK 611	Cabascango Carmen	Pediatría	Láser
LEXMARK 611	Chávez Olivia	Trabajo social	Láser
LEXMARK 611	Estrada Ángela	Emergencia	Láser
LEXMARK 611	Jácome Alexandra	Ginecología	Láser
LEXMARK 611	Teanga Juana	Consulta Externa	Láser
LEXMARK	Flores Leonel	Mantenimiento	Láser
XEROX		Medicina Interna	Multifunción
XEROX	Bracho Saskya	Consulta Externa	Multifunción
LEXMARK	Guaján Manuel	TIC	Láser
HP	Navarrete Nataly	Cirugía	Láser
HP	Pérez Luis	Farmacia	Láser
HP	Rhea Edwin	Bodega	Láser
HP	Rosero Eugenia	Compras Públicas	Láser
RICOH	Guevara Marco	Información	Multifunción
RICOH	Andrango Soledad	Administración	Multifunción
RICOH	Chamorro Yolanda	Talento Humano	Multifunción

Fuente: Oficina de Gestión de TIC

- **Biométricos:** El control de la entrada y salida de personal de manera continua es un proceso necesario para llevar registros de la permanencia de los funcionarios dentro de la Institución, los lectores biométricos se detallan en la Tabla 29.

Tabla 29. Listado de Biométricos

Nombre	Modelo	Marca	Ubicación	Responsable
Reloj Biométrico	STYLUS-980	BIOSYSTEM	Pasillo planta baja	Valladares Vanessa
Reloj Biométrico	STYLUS-980	BIOSYSTEM	Pasillo planta baja	Valladares Vanessa

Fuente: Oficina de Talento Humano

- **Sistema de Videovigilancia:** Este sistema consta de 16 cámaras colocadas en las distintas dependencias de la Institución, el videograbador STTV 800 STV cuenta con 2 TB de almacenamiento, se ubicado en el rack del cuarto de equipos del área de Gestión de TIC (Figura 13). Los responsables de dicha área son quienes administran este kit utilizado para la vigilancia y seguridad del HSLO.

Figura 13. Sistema de video vigilancia del HSLO

Fuente: Oficina de Gestión de TIC

- **Central Telefónica Analógica:** La Institución cuenta con una red de telefonía conmutada para la transmisión de voz (Figura 14), ubicada en la oficina de Estadística, está conformado por 16 terminales analógicos (Figura 15) distribuidos en las distintas áreas del Hospital.

Figura 14. Central telefónica analógica ubicada en oficina de Estadística

Fuente: Oficina de Estadística

Figura 15. Terminal analógico Panasonic

Fuente: Oficina de Gestión de TIC

- **Proyectores:** Son los dispositivos utilizados para la proyección de imágenes, audio y video para reuniones, charlas o videoconferencias que tienen lugar en la Sala de reuniones, Sala situacional o Biblioteca de la Institución. Son dos proyectores con los que cuenta el HSLO y son administrados e instalados por los responsables de la oficina de Gestión de TIC (Figura 16).

Figura 16. Proyector Sony

Fuente: Oficina de Gestión de TIC

3.3.2.1.2 Software.

Es el conjunto de programas o aplicaciones soportados por los equipos informáticos de la Institución y desempeñan tareas o procesos específicos, se describen en la Tabla 30.

Tabla 30. Listado de software del HSLO

Programa	Descripción	Licenciado
Fénix	Software de control de bienes	Sí
SOAT	Gestión de pacientes con accidentes de tránsito	Sí
Sistema de Laboratorio Clínico	Software utilizado para la presentación de resultados de laboratorio clínico	Sí
OVER TIME 2011 (Biométricos)	Control de asistencia de talento humano	Sí
SITAC	Software de facturación electrónica	Sí
Avast Antivirus	Software antivirus para sistema operativo Windows	No
ClamAV	Antivirus para software libre	
Eset NOD32	Antivirus para sistema operativo Windows	No
Avast Free	Antivirus para sistema operativo Windows	No
Avira	Antivirus para sistema operativo Windows	No

360 Total Security	Antivirus para sistema operativo Windows	No
Sistema operativo Windows	Sistema operativo instalado en determinados ordenadores para el soporte de aplicaciones específicas	No
Sistema operativo Centos 7	Sistema operativo utilizado en determinados servidores de la Institución	NA
Sistema operativo Linux Mint 17	Sistema operativo instalado en la mayor parte de computadores de escritorio de los funcionarios	NA
Ofimática Libre Office	Paquete de programas utilitarios de software libre	NA
Microsoft Office	Paquete de programas utilitarios de Windows	No

Fuente: Oficina de Gestión de TIC

3.3.2.1.3 Redes.

En esta sección se describen los equipos de redes para el enrutamiento, conmutación de paquetes y comunicación inalámbrica entre dispositivos, listados y detallados en la Tabla 31.

Tabla 31. Listado de equipos de redes de comunicación

Equipo	Marca	Núm. puertos	Velocidad de puerto	Ubicación
Access Point	HP	N/A	10/100/1000 Mbps	Gestión financiera/pasillo administrativo financiero
Access Point	HP	N/A	10/100/1000 Mbps	Emergencia
Access Point	HP	N/A	10/100/1000 Mbps	Sala de reuniones/Sala situacional
Access Point	HP	N/A	10/100/1000 Mbps	Medicina interna/Biblioteca
Access Point	HP	N/A	10/100/1000 Mbps	Sala de reuniones/Auditorio
Access Point	Motorola	N/A	10/100/1000 Mbps	Emergencia
Access Point	Motorola	N/A	10/100/1000 Mbps	Pediatría/Ludoteca
Switch	D-link	24	10/100/1000 Mbps	Gestión TIC/Rack
Switch	HP	24	10/100/1000 Mbps	Gestión TIC/Rack
Switch	D-link	16	10/100 Mbps	Emergencia
Switch	D-link	16	10/100 Mbps	Consulta externa y/o general
Switch	D-link	16	10/100 Mbps	Medicina interna/Cardiología

Switch	D-link	16	10/100 Mbps	Consulta externa y/o general
Switch	D-link	16	10/100 Mbps	Gestión TIC/Rack
Switch	D-link	16	10/100 Mbps	Gestión TIC/Rack
Switch	D-link	16	10/100 Mbps	Enfermería / pasillo Hospitalización
Switch	D-link	16	10/100 Mbps	Bodega
Switch	D-link	8	10/100 Mbps	Gestión Enfermería
Switch	D-link	8	10/100 Mbps	Estadística
Switch	D-link	8	10/100 Mbps	Servicios institucionales
Switch	D-link	8	10/100 Mbps	Gestión Financiera
Switch	D-link	8	10/100 Mbps	Quirófanos
Router	D-link	4	10/100 Mbps	Gestión TIC/Rack
Switch	D-link	8	10/100 Mbps	Odontología
Switch	D-link	8	10/100 Mbps	Laboratorio clínico
Switch	3com	24	10/100/1000 Mbps	Gestión TIC/Rack
Switch	Trendnet	8	10/100 Mbps	Laboratorio clínico
Switch	Trendnet	16	10/100 Mbps	Consulta externa y/o general
Switch	Trendnet	8	10/100 Mbps	Pediatría
Switch	D-link	24	10/100/1000 Mbps	Gestión TIC/Rack
Switch	3com	24	10/100/1000 Mbps	Gestión TIC/Rack
Switch	D-link	8	10/100 Mbps	Medicina interna/Biblioteca

Fuente: Oficina de Gestión de TIC

El listado de Personal e instalaciones físicas se encuentra en la sección 3.2.1.7 y 3.2.1.8 respectivamente.

3.3.2.2 Valoración de activos.

Los activos se valoran para evaluar las posibles consecuencias resultantes de la pérdida de la confidencialidad, integridad y disponibilidad, empleando criterios como: costo original, costo de reposición o renovación, reputación de una organización, etc. **(INEN, 2012)**. Los criterios que se han definido para valorar los activos del HSLO son:

- Interrupción en la prestación de servicios: Si el activo o la información contenida en él no está disponible, no se puede prestar adecuadamente los servicios.
- Costos de reparación o recuperación: Una falla o pérdida del activo físico implica costos de reparación o recuperación.

- Brechas en la seguridad de la información: se refiere a la pérdida de las propiedades de la información: confidencialidad, integridad y disponibilidad.

Los criterios descritos se los considera por ser los que representan mayor impacto, luego se definen las escalas a emplear, donde la norma menciona que una organización puede definir sus propios límites para valorar los activos como: bajo, medio o alto.

La Tabla 32 y Tabla 33 determinan las escalas que serán utilizadas para valorar los activos y el nivel de criticidad respectivamente.

Tabla 32. Escala de valoración de activos

Escala	Descripción
1	Bajo
2	Medio
3	Alto
NA	No aplica

Fuente: Autoría propia

Tabla 33. Nivel de criticidad del activo

Escala	Nivel de criticidad del activo
0-3	Bajo
4-6	Medio
7-9	Alto

Fuente: Autoría propia

La Tabla 34 de la valoración de los activos se realiza junto con los responsables del área de Gestión de TIC.

Tabla 34. Valoración de los activos de información del HSLO

Activos / Criterios	Interrupción en la prestación de servicios	Costos de reparación o recuperación	Brechas en la Seguridad de la Información	Resultado	Nivel de criticidad del Activo
Resultados de Laboratorio Clínico	3	3	3	9	Alta
Información de Áreas Administrativas	2	3	3	8	Alta
Historias Clínicas	3	3	3	9	Alta
Archivos de trabajo del personal	2	3	3	8	Alta
Archivos de Imagenología	2	3	3	8	Alta
Computadores portátiles y de escritorio	3	3	3	9	Alta
Servidores	3	3	3	9	Alta
Impresoras y copiadoras	2	3	1	6	Media
Biométricos	1	2	2	5	Media
Sistema de videovigilancia	1	3	1	5	Media
Central telefónica analógica	2	3	1	6	Media
Proyectores	1	3	1	5	Media
Software	3	2	3	8	Alta
Redes	3	3	3	9	Alta
Personal del HSLO	3	3	NA	6	Media
Oficinas y consultorios	3	3	NA	6	Media

Fuente: Oficina de Gestión de TIC

La Tabla 34 indica el listado de los activos de información del HSLO frente a los criterios que fueron definidos para valorarlos, aquellos con un nivel de criticidad alto son los implicados en la gestión del riesgo y que consecuentemente requieren de mayor cuidado. La Tabla 35 muestra los activos críticos sometidos en la gestión del riesgo.

Tabla 35. Activos sometidos a la gestión del riesgo

Tipo de Activo	Activos
Información o datos	Resultados de Laboratorio Clínico
	Información de Áreas Administrativas
	Historias Clínicas
	Archivos de trabajo del personal
	Archivos de Imagenología
Hardware	Computadores portátiles y de escritorio
	Servidores
Software	Software y aplicaciones del HSLO
Redes	Router
	Switches
	Access Point

Fuente: Autoría propia

3.3.2.3 Identificación de las amenazas.

Es importante identificar las amenazas que pueden causar daño a los activos de información tomando en cuenta su origen independientemente si se producen dentro o fuera de la Institución, ninguna de estas debe pasar por alto inclusive las inesperadas. La **(INEN, 2012)** provee un catálogo de amenazas comunes describiendo su origen y pueden ser del tipo: D (deliberadas), acciones deliberadas que tienen como objetivo los activos de información, A (accidentales), acciones humanas que pueden dañar accidentalmente los activos de información, E (ambientales) incidentes que no se basan en las acciones humanas y las amenazas humanas. El catálogo de amenazas comunes servirá como ejemplo para la elaboración de la matriz de riesgos de los activos de información críticos y se detalla en el Anexo C al final del documento.

3.3.2.4 Identificación de los controles existentes.

La (INEN, 2012) sugiere que se identifiquen los controles existentes para evitar trabajo o costos innecesarios, por ejemplo, en la duplicación de los controles, es decir, reconocer si dentro del HSLO existe una política o conjunto de políticas que tengan relación con la Seguridad de la Información y en efecto, el HSLO posee la política de Uso de Servicios de Red y Servicios Informáticos del Ministerio de Salud Pública de la Dirección Nacional de Tecnologías de la Información y Comunicaciones como documento para dar cumplimiento al correcto uso y manejo de los recursos y servicios de TI para las Instituciones que tienen al MSP como su autoridad sanitaria; sin embargo, debido al enfoque del presente proyecto hacen falta considerarse ciertos controles de Seguridad de la Información adicionales en relación a la informática sanitaria y políticas para asegurar los servicios, equipos informáticos y a la red de datos como tal. En el Anexo D al final del documento se encuentra un extracto de los Controles existentes en el HSLO.

3.3.2.5 Identificación de vulnerabilidades.

Deben identificarse las vulnerabilidades que pueden ser explotadas por las amenazas y que pueden causar daño a los activos de información. Cabe mencionar que una vulnerabilidad por sí sola no causa daño si no existe una amenaza presente para explotarla, la NTE INEN-ISO/IEC 27005:2012 también provee un catálogo de ejemplos de vulnerabilidades y que puede ser utilizada para asociarlas con los activos críticos. En el Anexo C al final del documento se detalla esta información.

3.3.2.6 Estimación del riesgo.

La NTE INEN ISO/IEC 27005:2012 no brinda una metodología específica para analizar los riesgos, sin embargo, incluye las características que toda metodología para la gestión de riesgos debería abordar, así que desde esta perspectiva esta norma se considera como una metodología en sí y cada organización puede definir su propio enfoque para

evaluar los riesgos. En el presente proyecto se utilizará la metodología cualitativa para estimar los riesgos.

La estimación cualitativa permite estimar y definir los riesgos por medio de estimaciones como: alta, media y baja, aunque también pueden definirse umbrales adicionales para esta actividad; facilita la comprensión de la estimación del riesgo de los activos y la toma de decisiones futuras permitiendo tener una percepción clara de lo que se está haciendo.

3.3.2.7 Valoración de la probabilidad del escenario de incidente.

Valorar la probabilidad del escenario de incidente es valorar la probabilidad de ocurrencia de las amenazas como lo describe la Tabla 36.

Tabla 36. Valoración de la probabilidad del escenario de incidente

Probabilidad	Descripción
Baja (improbable)	La probabilidad de ocurrencia de la amenaza es improbable.
Media (posible)	La probabilidad de ocurrencia de la amenaza es posible.
Alta (probable)	La probabilidad de ocurrencia de la amenaza es probable.

Fuente: Fuente: Adaptado de (INEN, 2012)

3.3.2.8 Valoración del impacto.

Valorar el impacto es valorar el grado de daño que ocasionaría a la Institución la materialización de las amenazas dando como resultado la pérdida de las brechas en la Seguridad de la Información (Tabla 37), pérdida de la continuidad de actividades para la entrega de servicios, pérdida de la reputación de la Institución o inclusive la pérdida de capital.

Tabla 37. Valoración del impacto en el negocio

Nivel	Descripción
Bajo	El impacto del riesgo es bajo.
Medio	El impacto del riesgo es medio.
Alto	El impacto del riesgo es alto.

Fuente: Adaptado de (INEN, 2012)

3.3.3 Evaluación del riesgo.

Posteriormente se evalúa el riesgo asignando un nivel a la probabilidad del escenario de incidente y al impacto que el riesgo ocasionaría a la Institución (Tabla 38); por ejemplo, si el impacto del riesgo es alto y la probabilidad de ocurrencia es baja, el valor del riesgo es Medio.

Tabla 38. Niveles de evaluación del riesgo

	Probabilidad del escenario de incidente	Baja (improbable)	Media (Posible)	Alta (Probable)
Impacto en el negocio	Bajo	Bajo	Medio	Medio
	Medio	Medio	Medio	Medio
	Alto	Medio	Medio	Alto

Fuente: Recuperado de (INEN, 2012)

La evaluación consiste en calificar el nivel del riesgo de los activos críticos a causa de la materialización de las amenazas. La Tabla 39 muestra el resultado de la matriz de riesgos de los computadores de escritorio y portátiles, donde se detallan sus principales amenazas y vulnerabilidades; mientras que para el resto de los activos críticos las matrices de riesgos se encuentran en el Anexo E al final del documento.

Tabla 39. Matriz de Riesgos de los computadores portátiles y de escritorio del HSLO

Tipo	Amenazas	Vulnerabilidades	Descripción del riesgo	Probabilidad de escenario de incidente	Impacto en el negocio	Valoración del riesgo
Daño físico	Fuego	Extintores caducados	Pérdida del activo por extintores caducados que imposibilitan la extinción del fuego en el activo	Bajo	Alto	Medio
	Polvo, corrosión, congelamiento	Activo susceptible a la humedad, polvo y suciedad	Obstrucción de paletas de los ventiladores de refrigeración de los equipos debido al polvo	Alto	Alto	Alto
Eventos naturales	Fenómenos climáticos	Aumento en la temperatura del activo	El activo puede destruirse a causa de tormentas eléctricas	Medio	Alto	Medio
			Sobrecalentamiento de los discos duros y fallas mecánicas por aumento de temperatura	Bajo	Alto	Medio
Compromiso de la información	Hurto del equipo, medios o documentos	Trabajo no supervisado del personal externo o de limpieza	Hurto o daño del activo debido a la falta de supervisión de personal externo o de limpieza	Medio	Medio	Medio
		Inventario de activos deficiente	Falta de actualización de datos en el inventario de activos	Medio	Medio	Medio
	Manipulación con hardware	Ingreso no controlado de dispositivos de almacenamiento	Infección del activo y pérdida de información a causa de virus, troyanos, código malicioso, etc.	Alto	Alto	Alto
Fallas técnicas	Mal funcionamiento del equipo	Finalización de la garantía del activo	Ante posibles fallas técnicas en el equipo no será posible solicitar uno nuevo	Bajo	Bajo	Bajo
		Equipos con sistema operativo desactualizado	Activo vulnerable fallas de rendimiento, funcionalidad y seguridad.	Alto	Alto	Alto

Compromiso de las funciones	Estructura de red poco segura	No existe una metodología de autenticación de usuarios para el acceso a la red de datos	Dificultad para controlar a los usuarios y monitorear el consumo de recursos en la red	Alto	Alto	Alto
	Sanciones a la Institución	Uso de sistema operativo propietario sin licencia	La Institución puede ser sancionada por violación de derechos de propiedad intelectual	Alto	Alto	Alto
Amenazas humanas	Ataques contra el sistema	Contraseñas del usuario del equipo y acceso a aplicaciones con niveles de seguridad bajos	Robo de credenciales y pérdida de información	Alto	Alto	Alto

Fuente: Autoría propia

La información que se muestra en la Tabla 39 fue proporcionada por el personal de TI, los resultados de las matrices de riesgos de los demás activos críticos también fueron obtenidos por información proporcionada por el personal de dicha área, utilizando herramientas de escaneo de puertos y visitas in situ, además, el conocimiento del nivel de cumplimiento de la normativa EGSI también contribuyó en la determinación de riesgos de los activos críticos.

El tratamiento para reducir, mitigar o minimizar los riesgos de los activos críticos en el presente proyecto se realiza a través del planteamiento de políticas de seguridad de la información.

CAPÍTULO IV: FORMULACIÓN E IMPLEMENTACIÓN DE POLÍTICAS Y PROCEDIMIENTOS DE SEGURIDAD DE LA INFORMACIÓN

El cuarto capítulo aborda la formulación e implementación de Políticas y procedimientos de Seguridad de la Información para el Hospital San Luis de Otavalo en base al Análisis de Riesgos de los activos críticos. La implementación de la Política de Seguridad de la Información se realiza mediante dos formas: procedimientos y soluciones basadas en software libre.

Los procedimientos se representan como diagramas de flujo que identifican un conjunto de actividades dispuestas de manera sistemática que deberán seguirse para lograr un propósito, en este caso, para dar cumplimiento a alguna política de seguridad de la información específica, así mismo, la implementación de Políticas a través de soluciones basadas en software libre quiere decir que se emplearán recursos tanto de hardware y/o software para optimizar la gestión de la red y asegurar la información confidencial, siempre y cuando dichos recursos se encuentren disponibles.

4.1 Definición de Política de Seguridad de la Información

Las políticas de Seguridad de la Información permiten establecer un vínculo de comunicación entre las decisiones del gobierno y poder transmitirlas hacia las distintas direcciones de la organización, por ello, facilitan la interacción entre el gobierno y gestión, donde el gobierno tiene la función de orientar mientras que la gestión se encarga de la ejecución de decisiones (Pillo, 2017).

> Uno de los componentes principales dentro de una estrategia de seguridad de la información en una organización es la Política de Seguridad. Este es un documento administrativo de alto nivel y de carácter obligatorio, en el cual se establecen los objetivos estratégicos y principios de seguridad de la información que deben ser seguidos en cualquier actividad que afecte el entorno de la

> organización y en donde se definen las responsabilidades y roles para todos los actores involucrados. Haciendo una comparación retórica, una política de seguridad de la información es a una organización lo que sería la Constitución (o Carta Magna) para un país (Acosta, 2016, pág. 1)

En el presente proyecto se ha definido inicialmente el uso de dos estándares: el Esquema Gubernamental de Seguridad de la Información (EGSI) y NTE INEN-ISO 27799:2008, los cuales proveen buenas prácticas para proteger la seguridad de la información, ambas poseen una fuerte estructura normativa que apoyará en la consolidación de la Política de Seguridad de la Información para el Hospital San Luis de Otavalo. A continuación, se describen las ventajas y desventajas que determinan su aplicación.

4.1.1 Ventajas.

- Las dos normativas se basan en las mejores prácticas proporcionadas por la ISO (Organización Internacional de Estandarización) reconocida a nivel nacional e internacional, son ampliamente utilizadas en numerosas organizaciones para distintos fines y sectores de la industria.
- Ambas son reconocidas y aceptadas en el país.
- Por su estructura se alinean con las fases de la Gestión del Riesgo de la Seguridad de la Información de la norma NTE INEN ISO/IEC 27005:2012.
- Sus cláusulas cubren y se adaptan a las condiciones y necesidades de las organizaciones.

4.1.2 Desventajas.

- No son certificables.
- No proporcionan una metodología de implementación.
- Acceder al estándar NTE INEN-ISO 27799:2008 requiere un costo.

4.2 Determinación de Políticas de Seguridad de la Información

Las matrices de riesgos de los activos críticos permitieron analizar las amenazas, vulnerabilidades y evaluar el nivel de riesgo de los mismos y, para su tratamiento, se formularán Políticas de Seguridad de la Información. La Tabla 40 muestra la Determinación de Políticas de Seguridad de la Información para los computadores portátiles y de escritorio del HSLO, mientras que para los demás activos de información críticos se detallan en el Anexo E al final del documento.

Tabla 22. Determinación de Políticas de Seguridad de la Información para los computadores de escritorio y portátiles

Amenazas	Vulnerabilidades	Valoración del riesgo	Políticas de Seguridad de la Información
Fuego	Extintores caducados	Medio	Protección contra amenazas externas y ambientales
Polvo, corrosión, congelamiento	Activo susceptible a la humedad, polvo y suciedad	Alto	Mantenimiento de equipos
Fenómenos climáticos	Aumento en la temperatura del activo	Medio	Protección contra amenazas externas y ambientales
Hurto del equipo, medios o documentos	Trabajo no supervisado del personal externo o de limpieza	Medio	Controles de acceso físico
	Inventario de activos deficiente	Medio	Inventario de activos
Manipulación con hardware	Ingreso no controlado de dispositivos de almacenamiento	Alto	Gestión de medios removibles
Mal funcionamiento del equipo	Finalización de la garantía del activo	Bajo	Mantenimiento de equipos
	Equipos con sistema operativo desactualizado	Alto	Mantenimiento de equipos
Estructura de red poco segura	No existe una metodología de autenticación de usuarios para el acceso a la red de datos	Alto	Control de acceso a la red de datos cableada

Sanciones a la Institución	Uso de sistema operativo propietario sin licencia	Alto	Derechos de propiedad intelectual
Ataques contra el sistema	Contraseñas de cuentas de usuario del equipo con niveles de seguridad bajo	Alto	Uso aceptable de los activos

Fuente: Adaptado de (SNAP, 2012)

Seguidamente se procede a elaborar el documento de la Política de Seguridad de la Información del Hospital San Luis de Otavalo (Tabla 41) que tendrá una estructura similar a la de los estándares anteriormente mencionados.

Tabla 41. Estructura de la Política de Seguridad de la Información del Hospital San Luis de Otavalo

Ítems principales
Introducción
Objetivos
Alcance
Sanciones
Sección I – Política de Seguridad de la Información
1.1 Compromiso de la máxima autoridad de la Institución con la Seguridad de la Información
Sección II - Organización de la Seguridad de la Información
2.1 Coordinación de la Gestión de la Seguridad de la Información
2.2 Acuerdos sobre Confidencialidad de la Información
Sección III – Gestión de Activos
3.1 Inventario de activos
3.2 Uso aceptable de los activos
3.3 Directrices de clasificación y etiquetado de la información
Sección IV – Seguridad de los Recursos Humanos
4.1 Selección del personal
4.2 Funciones y responsabilidades
Sección V – Seguridad física y del entorno
5.1 Protección contra amenazas externas y ambientales
5.2 Controles de acceso físico
5.3 Seguridad del cableado
Sección VI – Gestión de las Comunicaciones y Operaciones
6.1 Controles de seguridad perimetral
6.2 Política de la DMZ
6.3 Controles de acceso remoto
6.4 Controles de seguridad de servidores
6.5 Controles de acceso al servicio de Internet
6.6 Controles de acceso a la red inalámbrica

6.7 Controles de acceso a la red LAN
6.8 Controles contra código malicioso
6.9 Gestión de medios removibles
6.10 Mantenimiento de equipos
6.11 Documentación de procesos y actividades
Sección VII – Control de Acceso
7.1 Separación de las redes
Sección VIII – Gestión de la Continuidad del Negocio
8.1 Evaluación de Riesgos de la Seguridad de la información
Sección IX – Cumplimiento
9.1 Derechos de Propiedad Intelectual
9.2 Seguridad de registros en cada entidad
Glosario de Términos

Fuente: Adaptado de (SNAP, 2012), (INEN, 2012)

4.3 Política de Seguridad de la Información

A continuación, se elabora la Política de Seguridad de la Información del Hospital San Luis de Otavalo (Tabla 42).

Tabla 42. Política de Seguridad de la Información del Hospital San Luis de Otavalo

Ministerio de Salud Pública

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

HOSPITAL SAN LUIS DE OTAVALO

REVISIONES

Modificaciones	Nombre	Firma
Realizado por:	Catherine López	…….. Estudiante UTN
Revisado por:	Ing. Manuel Guaján	

			…….. Informático HSLO
	Aprobado por:	Dr. Juan Echeverría	…….. Director HSLO

INTRODUCCIÓN

La información constituye el activo más importante en una Institución, sea del tipo electrónica o física, requiere ser protegida al igual que los sistemas que la procesan en términos de confidencialidad, integridad y disponibilidad. El sector salud en comparación con otros sectores de la industria, gestiona un tipo de información particular que es la información sanitaria, considerada una de las más atractivas para los atacantes cibernéticos y desde esta perspectiva, el Hospital San Luis de Otavalo puede llegar a ser un blanco vulnerable y por ende exige que se realicen mayores esfuerzos para asegurar la información y a la Institución como tal.

El presente documento está elaborado en base al Análisis de Riesgos donde se identificaron las amenazas y vulnerabilidades de los activos de información críticos, tiene como objetivo proveer controles de seguridad a seguirse en cada actividad relacionada con el manejo de activos informáticos y manipulación de información, donde además se definen las responsabilidades de los involucrados, integrando las mejores prácticas sobre Seguridad de la Información recopiladas de estándares ampliamente utilizados y reconocidos a nivel nacional e internacional.

OBJETIVOS

Los objetivos de la presente Política de Seguridad de la Información son:

- Velar por el uso adecuado de la información y los medios que la procesan preservando su confidencialidad, integridad y disponibilidad.
- Garantizar el funcionamiento y continuidad de los servicios institucionales soportados por los sistemas de información a través de la gestión de los recursos humanos (capital humano) y las Tecnologías de la Información (recursos de TI).
- Dar seguimiento a las políticas propuestas, integrar mejoras o actualizarla ante el surgimiento de nuevas probabilidades de amenaza que puedan comprometer la seguridad de la información.
- Cumplir con estándares nacionales e internacionales que aseguren que los procesos relacionados con la Seguridad de la Información sean controlados de manera efectiva, elevando su compromiso con la seguridad de la ciudadanía.

ALCANCE

La Política de Seguridad de la Información al estar elaborada en base al análisis de riesgos de los activos de información críticos, se encuentra sujeta al personal que tiene a su alcance el manejo de recursos informáticos e información confidencial. La aplicación de la presente Política es de carácter obligatorio, exceptuando las circunstancias en las cuales no se cuente con los recursos necesarios, no obstante, el Comité de Seguridad de la Información, tiene la autoridad de modificar, eliminar una política puntual o anular todo el documento si las soluciones no llegan a ser suficientes para tratar algún riesgo.

SANCIONES

En base a la gravedad de incumplimiento de la Política de Seguridad de la Información sea por intenciones contrarias a la ética profesional, desconocimiento de su existencia, entre otros motivos, los funcionarios serán sancionados de acuerdo con la legislación vigente y en lo que estipulan las principales normativas del Estado respecto al uso de la información y recursos informáticos, estas son:

- Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos
- Código Orgánico Integral Penal
- Ley Orgánica de Transparencia y Acceso a la Información Pública
- Ley de Derechos y Amparo al Paciente

SECCIÓN I
POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

1.1 Compromiso de la máxima autoridad de la Institución con la Seguridad de la Información

Art. 1 La información y los sistemas que la procesan dentro de la Institución son propiedad de la misma y, por lo tanto, le pertenecen al Estado. La máxima autoridad de la Institución autorizará la implementación de la Política de Seguridad de la Información la cual establece lineamientos que apoyen en la preservación de la confidencialidad, integridad y disponibilidad de la información.

SECCIÓN II
ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

2.1 Coordinación de la Gestión de la Seguridad de la Información

Art. 2 Se conformará un Comité de Seguridad de la Información (CSI) integrado por los principales directivos de la Institución o por un comité ejecutivo existente.

Art. 3 El Comité de Seguridad de la Información designará un responsable de Seguridad del área de Tecnologías de la Información y Comunicación.

2.2 Acuerdos sobre Confidencialidad de la Información

Art. 4 Todo el personal sin excepción alguna oficializará un Acuerdo de Confidencialidad o No-Divulgación de la Información que tiene como objetivo consolidar el compromiso de cada funcionario de mantener la confidencialidad de la información y los recursos informáticos que la Institución le conceda.

SECCIÓN III
GESTIÓN DE ACTIVOS

3.1 Inventario de activos de información

Art. 5 Todos los activos de información de la Institución serán debidamente inventariados y clasificados según lo sugiere de la Norma Técnica Ecuatoriana INEN-ISO/IEC 27005:2012 como: activos primarios y de soporte, con un nivel adecuado de detalles y características que permitan identificar a dichos bienes.

a) Se clasificarán e inventariarán los activos primarios según su tipo:

- Procesos y actividades del negocio: Procesos estratégicos de la Institución y los servicios que brinda.

- Información o datos: Información dispuesta en formato físico o electrónico, documentación, manuales o archivos importantes.

b) Se clasificarán e inventariarán los activos de soporte según su tipo:

- Hardware: Todos los elementos físicos que dan soporte a los procesos.
- Software: Conjunto de programas, aplicaciones o herramientas necesarias para el funcionamiento de los equipos informáticos.
- Redes: Todos los dispositivos de telecomunicaciones que interconectan computadores o usuarios finales.
- Personal: Incluye a todo el personal de la Institución: profesionales de salud, auxiliares, administrativos, entre otros.
- Ubicación: Instalaciones de la Institución.

Nota: El inventario de activos deberá ser actualizado cuando existan cambios en el personal o cambios en los activos de información.

3.2 Uso aceptable de los activos

Art. 6 Se respetarán las disposiciones y se velará por el cumplimiento de la Política de Uso de Servicios de Red y Servicios Informáticos del Ministerio de Salud Pública.

3.3 Directrices de clasificación y etiquetado de la información

Art. 7 Se elaborará y aprobará un catálogo de clasificación de la información según se describen los siguientes niveles:

a) Pública: Toda información o documentación en poder de la Institución o generada por los funcionarios a través de los recursos del Estado.

b) Confidencial: Información que según el Reglamento de Información Confidencial del Sistema Nacional de Salud es: Historias clínicas, resultados de exámenes de laboratorio, imagenología y otros procedimientos, tarjetas de registro de atenciones médicas con indicación de diagnóstico y tratamientos.

c) De uso interno: Información que puede ser compartida entre los funcionarios dentro de la Institución.

Art. 8 El etiquetado o marcado de clasificación de la información se definirá en la esquina superior derecha de cada hoja de los documentos.

Art. 9 Se utilizarán mecanismos de cifrado (encriptación) para proteger la información sensible o crítica, bien sea durante su transporte o almacenamiento.

Art. 10 Se respetarán las disposiciones establecidas en el Art. 14 del Reglamento de Información Confidencial en el Sistema Nacional de Salud, el cual define que las personas autorizadas para el acceso a la información confidencial son: médicos, psicólogos, odontólogos, trabajadoras sociales, obstetrices, enfermeras, auxiliares de enfermería y personal de estadística.

SECCIÓN IV
SEGURIDAD DE LOS RECURSOS HUMANOS

4.1 Selección de Personal

Art. 11 Dentro del proceso interno para el contrato de profesionales de salud, se recopilará un número razonable de referencias domiciliarias y empleos previos y, de ser posible, llevar a cabo comprobaciones de actividades criminales pasadas como un

mecanismo adicional que ayuda en la determinación y selección de profesionales de salud idóneo.

4.2 Funciones y Responsabilidades

Art. 12 Cuando ingrese nuevo personal a la Institución, los responsables de Talento Humano informarán a la máxima autoridad la integración de dicho funcionario para que autorice al Responsable de Seguridad del área de TIC la habilitación de los privilegios de acceso respectivos a los Sistemas de Información.

Art. 13 Se rescindirá de manera inmediata los privilegios de acceso a los Sistemas de Información a funcionarios, estudiantes, pasantes, voluntarios, entre otros, cuando cualquiera de ellos se retire de la Institución de manera temporal o permanente, luego del cese de sus funciones, al ser notificado por despido, etc. y siempre que se perciba un incremento del riesgo por el mantenimiento de dicho privilegio.

SECCIÓN V
SEGURIDAD FÍSICA Y DEL ENTORNO

5.1 Protección contra amenazas externas y ambientales

Art. 14 Todas las áreas que alberguen equipos informáticos deberán permanecer dotadas de elementos de extinción de incendios, verificando su integridad y ubicación adecuada.

Art. 15 Se supervisará una vez por semana la integridad de los equipos de comunicaciones ubicados en áreas externas del cuarto de equipos.

5.2 Controles de acceso físico

Art. 16 El cuarto de equipos deberá adecuarse de sistemas de control de acceso físico, por ejemplo: identificación biométrica, lector de huellas dactilares, tarjetas inteligentes, entre otros, para restringir el acceso de personal no autorizado y evitar el robo de activos.

Art. 17 En las áreas donde se encuentren computadores y equipos de comunicaciones se supervisará la permanencia de personal externo y de limpieza, evitando abandonar el área mientras dicho personal finalice sus tareas.

5.3 Seguridad del cableado

Art. 18 Se velará por el estado del cableado estructurado verificando que se cumplan con estándares y normativas nacionales e internacionales con la finalidad de proteger los medios de comunicación.

Art. 19 Se supervisará el estado del cableado estructurado con una periodicidad de una vez al mes, corrigiendo fallas si es necesario, evitando el cruce con equipos, identificando y etiquetando correctamente cada punto de red hacia las áreas de trabajo de los funcionarios y equipos de comunicación.

SECCIÓN VI
GESTIÓN DE LAS COMUNICACIONES Y OPERACIONES

6.1 Controles de seguridad perimetral

Art. 20 Se implementará un firewall como mecanismo de seguridad perimetral de la red de datos de la Institución, será un dispositivo que contenga las características necesarias que le permitan segmentar la red de manera independiente manejando como mínimo tres interfaces de red: WAN, LAN y DMZ.

Art. 21 En el firewall perimetral se implementarán las principales reglas para permitir o denegar el tráfico entre las redes planteadas, verificando continuamente que las configuraciones y reglas establecidas cumplan con el propósito de proteger a los activos de información.

Art. 22 La administración del firewall perimetral estará a cargo únicamente del Responsable de Seguridad de la Información del área de TIC.

6.2 Política de la DMZ

Art. 23 Se implementará un segmento de red DMZ gestionado en el firewall perimetral donde serán colocados los servidores que requieran acceso interno y externo.

Art. 24 Se configurará esta zona de tal forma que no pueda alcanzar la red interna para protegerla en caso de que uno o varios de los servicios de la DMZ sean vulnerados.

6.3 Controles de acceso remoto

Art. 25 Siempre que los recursos lo permitan, se establecerán mecanismos de acceso remoto a los servicios internos mediante el redireccionamiento de puertos y/o implementación de redes privadas virtuales VPN.

Art. 26 Se asegurará que la implementación de VPNs limite el acceso solo a segmentos de red necesarios.

Art. 27 La implementación de redireccionamiento de puertos y VPN serán configuradas y administradas únicamente por el Responsable de Seguridad de la Información del área de TIC.

6.4 Controles de seguridad de los servidores

Art. 28 Se habilitará el acceso a los servidores de la Institución mediante la resolución de nombres de dominio.

Art. 29 Se habilitará el acceso externo e interno hacia los servicios institucionales a través de la habilitación de puertos seguros.

Art. 30 Se asegurará que el/los servidores que gestionen información confidencial utilicen puertos y protocolos seguros de tal forma que la información sensible no viaje de manera no cifrada.

6.5 Controles de acceso al servicio de Internet

Art. 31 Se implementará un mecanismo que permita controlar la conexión a Internet de los funcionarios de la red cableada a través de un Portal Cautivo.

Art. 32 La nomenclatura que será utilizada para la identificación de los funcionarios para la conexión a Internet es la siguiente:

a) Los nombres de usuario se estructurarán con la inicial del primer nombre y el apellido de cada funcionario; en caso de repetirse, se tomará la inicial del segundo nombre y el apellido.
b) La contraseña de cada usuario deberá ser robusta y se conformará por un mínimo 10 caracteres alfanuméricos.

Art. 33 Se socializará con los funcionarios la implementación del Portal cautivo recalcando la importancia de no seleccionar la opción “recordar contraseña” cuando los funcionarios ingresen al portal y aplicaciones en Internet.

Art. 34 El personal que no pertenezca a la Institución y requiera conexión a Internet deberá solicitarlo de manera formal, la máxima autoridad será quien lo apruebe y delegue al Responsable de Seguridad del área de TIC la habilitación del usuario respectivo.

Art. 35 Se prohibirá a todo el personal colocar de manera visible en pegatinas, documentos de texto o bloc de notas en las pantallas de los computadores personales las contraseñas de acceso a los Sistemas de Información en general. Estas credenciales son únicas y no deben ser compartidas.

6.6 Controles de acceso a la red inalámbrica

Art. 36 Se implementará un mecanismo de acceso a la red inalámbrica mediante el servicio RADIUS, donde los funcionarios deban autenticarse para conectarse a los distintos Access Point de la Institución.

Art. 37 La nomenclatura de los nombres de usuario será:

a) Los nombres de usuario se conformarán de la inicial del primer nombre seguido del apellido y los tres últimos dígitos de su cédula de identidad.
b) La contraseña de cada usuario deberá ser robusta y se conformará por un mínimo 10 caracteres alfanuméricos.

Art. 38 En la red inalámbrica se emplearán medidas para bloquear el acceso a portales, aplicaciones, servicios y webs sobre pornografía, violencia, racismo y todos aquellos sitios que vayan en contra de los intereses y reputación de la Institución.

Art. 39 Los funcionarios que requieran la habilitación de la red inalámbrica para una determinada área de la Institución deberán solicitarlo con anterioridad para que el responsable de seguridad del área de TIC lo autorice y gestione.

6.7 Controles contra código malicioso

Art. 40 Se mantendrán todos los sistemas operativos, antivirus y software contra código malicioso actualizados con las últimas versiones de seguridad disponibles con el objetivo de evitar deficiencias en el funcionamiento y proteger a los equipos de software malicioso.

Art. 41 Se actualizarán con las últimas versiones de seguridad disponibles a los navegadores de Internet de los computadores y protegerlos de malware, fallas de funcionamiento y mejorar el rendimiento de los mismos.

6.8 Mantenimiento de equipos

Art. 42 El responsable de Seguridad del área de TIC planificará la realización de mantenimientos preventivos y correctivos de manera periódica a los equipos y dispositivos de acuerdo a las especificaciones de los proveedores, comunicando con anterioridad a la máxima autoridad y funcionarios y conservando los registros de los eventos suscitados.

Art. 43 Los mantenimientos solamente podrá realizarlo el personal del área de TIC o personal calificado y autorizado por el responsable de seguridad del área de TIC.

6.9 Documentación de procesos y actividades

Art. 44 Los sistemas y/o activos de información que se encuentren operativos deberán contar con sus respectivos manuales de uso en los cuales se describa la estructura del sistema o del activo, características físicas y técnicas e instrucciones suficientes para que cualquier administrador y usuario pueda hacer uso de dicho sistema.

SECCIÓN VII

POLÍTICA DE CONTROL DE ACCESO

7.1 Separación de las redes

Art. 47 Se optimizará la gestión de la red LAN a través de la segmentación en dominios lógicos de red.

Art. 48 La separación de las redes (Vlan) se implementarán en base a la clasificación de la información almacenada o procesada en la red, según las funciones que ejecute el personal y/o dispositivos conectados a la red de datos, con el objetivo de proveer mayor seguridad a los activos de información.

Art. 49 Se aislará en un segmento de red específico a los funcionarios que gestionen información confidencial relacionada con los datos personales de los pacientes y se asegurará que solamente dicho personal tenga privilegios de acceso a los servidores dedicados a la gestión de información sanitaria.

Art. 50 Las Vlan serán configuradas y administradas únicamente por el Responsable de Seguridad de la Información del área de TIC.

SECCIÓN VIII
GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

8.1 Evaluación de Riesgos de la Seguridad de la Información

Art. 51 A todo el personal que se requiera su participación en la evaluación de riesgos deberá cooperar plenamente con las actividades que se necesiten llevar a cabo.

Art. 52 El proceso que el Comité de Seguridad de la Información desarrollará para gestionar los riesgos en la Seguridad de la Información será en base a la metodología propuesta por la Norma Técnica Ecuatoriana INEN-ISO/IEC 27005:2012 (Gestión del Riesgo de la Seguridad de la Información) a través de las siguientes actividades:

a) Se identificarán los activos de información de la Institución clasificándolos según su tipo (Ver Art. 6).
b) Se valorarán los activos de información en términos de: interrupción en la prestación de servicios, costos de reparación o recuperación del activo, brechas en la Seguridad de la Información, entre otros criterios adicionales.
c) Luego se identificarán las amenazas y vulnerabilidades de los activos de información, así como los controles existentes relacionados con la Seguridad de la Información.
d) Se establecerán escalas para la valoración de la probabilidad del escenario de incidente, el impacto en el negocio y el nivel del riesgo, todo ello plasmado o representado en la matriz de riesgos.
e) Como resultado de la matriz de riesgos se determinará el tratamiento que recibirán dichos riesgos asociados a los activos de información.

SECCIÓN IX
CUMPLIMIENTO

9.1 Derechos de Propiedad Intelectual

Art. 53 Se instalará software privativo siempre y cuando posea las respectivas licencias, mientras que se priorizará el uso e instalación de software libre en los equipos informáticos en conformidad con el Decreto Ejecutivo N° 1014.

9.2 Seguridad de registros en cada entidad

Art. 54 Se establecerán procedimientos para el almacenamiento y manipulación de la información electrónica y archivos de configuración de equipos de comunicaciones de

tal manera que se garantice su disponibilidad y legibilidad, especificando los períodos de retención y los medios de almacenamiento tales como: discos duros, DVDs, cintas magnéticas, servidores de archivos, entre otros.

GLOSARIO DE TÉRMINOS

- Activo de información: Cualquier cosa que tiene valor para la organización y que puede contener información valiosa para la misma.
- Sistema de Información: Conjunto de elementos organizados y que interactúan entre sí, procesan información de manera automatizada o manual.
- Confidencialidad: Propiedad de que la información no se ha puesto a disposición o revelado a individuos, entidades o procesos no autorizados.
- Integridad: Propiedad de que la información no ha sido alterada o destruida de forma no autorizada.
- Disponibilidad: Propiedad de la información de ser accesible y utilizable bajo demanda de una entidad autorizada.
- Riesgo: Combinación de la probabilidad de un evento y sus consecuencias.
- Amenaza: Causa potencial de un incidente no deseado, que puede dañar a un sistema u organización.
- Vulnerabilidad: Debilidad de los activos que puede ser aprovechado por una o más amenazas.

- DMZ: Zona desmilitarizada, red localizada entre la red Interna LAN y red externa WAN donde generalmente se alojan servicios, solo los servicios o puertos requeridos deben habilitarse en el firewall perimetral.
- VLAN: Son segmentos lógicos de una red, permiten flexibilidad, escalabilidad, seguridad y mejora la administración de la red.
- Norma NTE INEN-ISO/IEC 27005:2012: Es la Norma Técnica Ecuatoria preparada por el CTE (Comité Técnico Conjunto de Tecnología de la Información) en el año 2012, suministra directrices para la gestión del riesgo de la seguridad de la información.
- Norma NTE INEN-ISO 27799:2008: Es la Norma Técnica Ecuatoriana publicada por el Comité Técnico ISO/TC 215 para la informática sanitaria en el año 2008, contiene un conjunto de controles de seguridad para los propósitos de proteger los datos personales sanitarios.
- Seguridad de la Información: Hace referencia a la protección de la confidencialidad, integridad y disponibilidad de la información.
- Tecnologías de la Información: Tecnología que se utiliza para el procesamiento de información, datos procesados que permiten tomar decisiones e iniciar acciones.
- Planes de continuidad: Se enfoca en asegurar la continuidad del negocio ante la ocurrencia de incidentes inesperados con el objetivo de no detener la productividad de la Institución y que los acontecimientos afecten los menos posible.
- Acuerdo de Confidencialidad: Instrumento que afianza el compromiso de los funcionarios públicos con la Institución respecto al uso de recursos informáticos.

Fuente: Adaptado de (SNAP, 2012), (INEN, 2008)

La Política de Seguridad de la Información deberá ser revisada y aprobada por la máxima autoridad de la Institución, el Responsable de Seguridad de la Información del área de Gestión de TIC y socializada con el personal correspondiente.

4.4 Implementación de Políticas de Seguridad de la Información

El objetivo de esta sección es la implementación de la Política de Seguridad de la Información por medio de procedimientos y ejecución de soluciones basadas en software libre donde las TI desempeñan un papel fundamental en este propósito.

Cabe mencionar que la Política de Seguridad de la Información no podrá ser implementada en su totalidad debido a la falta de recursos y planificación previa para la aplicación de servicios. En el Anexo G al final del documento se encuentra un check list del cumplimiento de las políticas y medios utilizados para su ejecución.

4.4.1 Sección I – Política de Seguridad de la Información.

El artículo 1 de la Sección I señala que el documento de la Política de Seguridad de la Información deberá ser aprobado por la máxima autoridad de la Institución y que a su vez debe ser socializada con el personal pertinente. La Tabla 43 determina el procedimiento que deberá seguirse para la revisión, aprobación y socialización de la Política de Seguridad de la Información del HSLO con su respectivo diagrama de flujo (Figura 17) de las actividades a realizar.

Tabla 43. Procedimiento de revisión, aprobación y socialización de la Política de Seguridad de la Información del HSLO

SECCIÓN I – POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	
Procedimiento:	Revisión, Aprobación y Socialización de la Política de Seguridad de la Información
Objetivo:	Describir las actividades a seguir para la revisión, aprobación y difusión de la Política de Seguridad de la Información del Hospital San Luis de Otavalo y ponerla al alcance y conocimiento del personal involucrado.
Alcance:	La Política de Seguridad de la Información al ser un instrumento obligatorio se encuentra sujeta a todo el personal de la Institución, información y recursos informáticos.
Responsables:	• Director del HSLO • Comité de Seguridad de la Información (C.S.I) • Responsable de Seguridad de la Información del área de TIC • Funcionarios del HSLO

ACTIVIDAD	**DESCRIPCIÓN**
	Inicio del procedimiento
1	El Comité de Seguridad de la Información (C.S.I) revisa la Política de Seguridad de la Información del HSLO.
2	El director del HSLO revisa y aprueba la Política de S.I del HSLO.
3	El director del HSLO delega al C.S.I la difusión de la Política de S.I del HSLO.
4	El C.S.I convoca a todo el personal del HSLO a la socialización de la Política de S.I a través del correo electrónico institucional.
5	Los funcionarios reciben el correo enviado por el C.S.I y confirma su asistencia a la socialización.
Condición ¿El funcionario asiste a la socialización?	Si el funcionario asiste a la socialización continúa con la Actividad 6, caso contrario realiza Actividad 11.
6	El C.S.I comunica, difunde o socializa la Política de S.I del HSLO con el personal.

7	Los funcionarios tienen la libertad de realizar observaciones o solicitar modificaciones a la Política de S.I del HSLO.
8	El C.S.I realiza cambios en la Política de S.I sugeridos por el personal en caso de ser necesario.
9	Los funcionarios que asistieron a la socialización firman obligatoriamente el Acta de Asistencia con el objeto de evidenciar su presencia y participación.
10	El Responsable de S.I del área de TIC elabora un informe final acerca de lo tratado en la Socialización y se lo presenta al Director de la Institución.
11	El C.S.I transmite la Política de S.I a todo el personal del HSLO a través de distintos medios de comunicación.
12	Todo el personal tiene la obligación de ponerse al tanto e informarse sobre el contenido de la Política de S.I del HSLO.
13	El Responsable de S.I del área de TIC implementa las políticas de S.I.
	Fin del procedimiento

CONSTANCIAS
Revisado por: ……. Catherine López ESTUDIANTE UTN
Revisado y aprobado por: ……. Manuel Guaján INFORMÁTICO HSLO

Fuente: Autoría propia

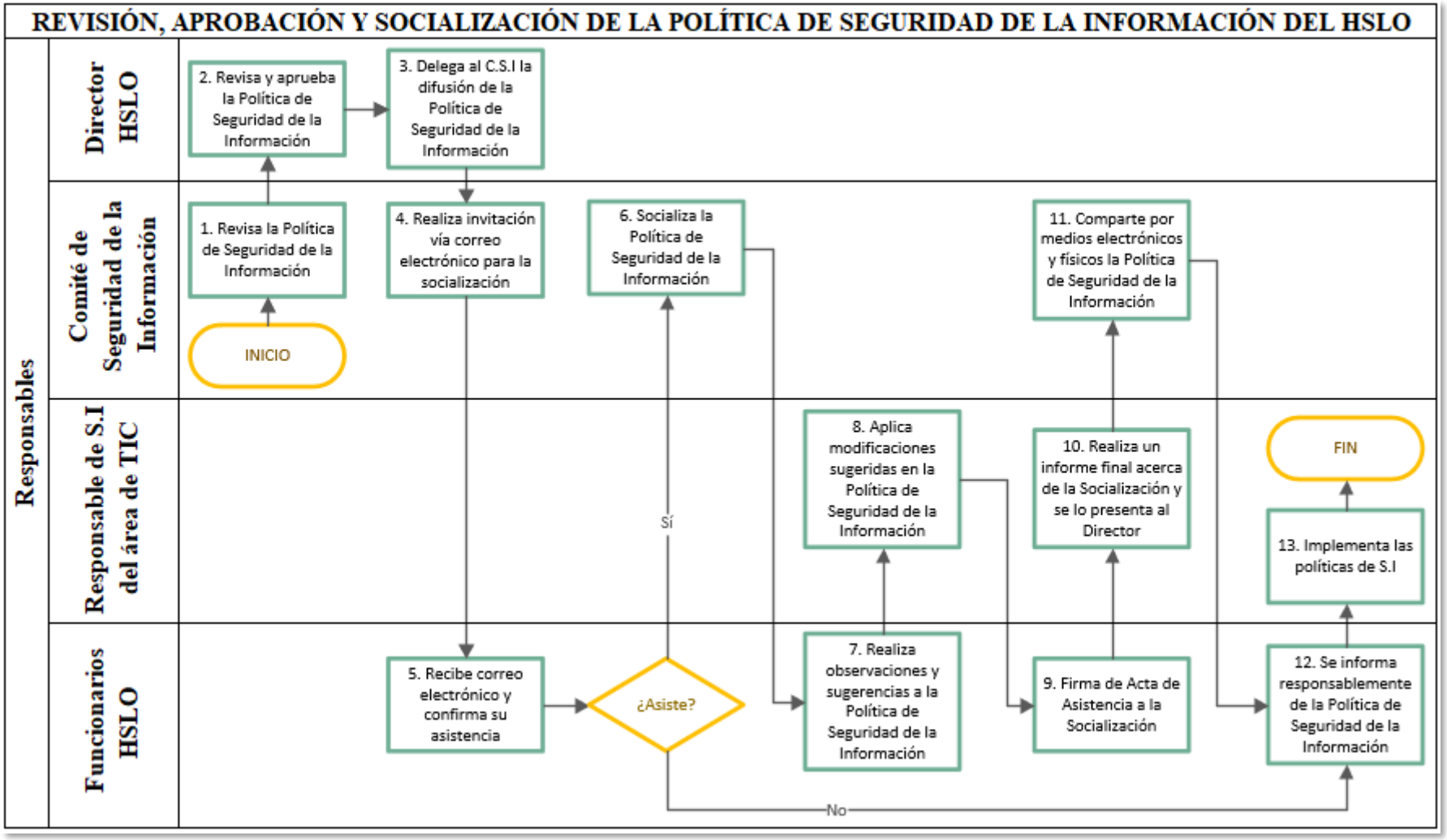


Figura 17. Diagrama de flujo del Proceso para la revisión, aprobación y socialización de la Política de Seguridad de la Información del HSLO

Fuente: Autoría propia

4.4.2 Sección II – Política de Seguridad de la Información.

Los artículos 2 y 3 referente a la coordinación de la gestión de la seguridad de la información se establece que se conforme un Comité de Seguridad de la Información y sean sus miembros quienes designen a un Responsable de Seguridad de la Información del área de TIC. Se ha elaborado un documento denominado Roles y Responsabilidades de la Seguridad de la Información (ver Anexo F) para oficializar este aspecto.

El artículo 4 menciona que todo el personal deberá oficializar el Acuerdo de Confidencialidad o No-Divulgación con el objetivo de afianzar su compromiso con la seguridad de la información. Este acuerdo se encuentra en el Anexo F al final del documento.

4.4.3 Sección III – Gestión de activos

El artículo 5 de esta sección trata acerca del inventario de activos de información en base a las directrices del estándar NTE INEN/ISO IEC 27005:2012, proceso que se lo realizó en el capítulo 3 del presente proyecto recomendando que el inventario se actualice cuando se presenten cambios de personal o en los activos.

El artículo 6 acerca del uso aceptable de los activos menciona que deben respetarse los lineamientos de la política existente, en la cual se establecen medidas para asegurar que se controlará el tráfico de la red evitando que los funcionarios utilicen los recursos informáticos para navegar en sitios web maliciosos; además se definen políticas para la creación de usuarios para el uso de correo electrónico institucional y la nomenclatura y niveles de seguridad de las contraseñas utilizadas para el acceso aplicaciones y servicios. Por lo tanto, estas disposiciones al estar descritas en la política existente, no se citan de nuevo en la Política de Seguridad de la Información para el HSLO.

Los artículos 7, 8, 9 y 10 establecen políticas que enfatizan la necesidad de clasificar la información que se gestiona en la Institución, este procedimiento lo indica la Tabla 44 y el diagrama de flujo (Figura 18) explica las actividades a seguir.

Tabla 44. Procedimiento para la Clasificación y etiquetado de la Información

Ministerio de Salud Pública

HOSPITAL SAN LUIS DE OTAVALO – DISTRITO 10D02

SECCIÓN III – GESTIÓN DE ACTIVOS

Procedimiento:	Procedimiento para la clasificación y etiquetado de la información
Objetivo:	Describir el procedimiento a seguir para clasificar y etiquetar la información.
Alcance:	El alcance de este procedimiento involucra a la información en formato electrónico.
Responsables:	• Responsable de S.I del área de TIC • Comité de Seguridad de la Información (C.S.I) • Funcionarios del HSLO

ACTIVIDAD	**DESCRIPCIÓN**
	Inicio del procedimiento
1	El C.S.I elabora un catálogo de información clasificada como pública o confidencial.
2	El C.S.I comparte el catálogo de información a todo el personal a través del correo electrónico institucional.
3	Los funcionarios etiquetan la información a su disposición según el catálogo recibido.
Condición ¿Gestiona información confidencial?	Si el funcionario gestiona información confidencial prosigue con la Actividad 4, caso contrario finaliza el procedimiento.

4	El Responsable de S.I del área de TIC instala el software para el cifrado de información AesCrypt en los ordenadores que lo requieran.
5	El/los funcionarios cifran la información etiquetada como confidencial cuando la transporte por medios digitales y/o al respaldarla en dispositivos de almacenamiento físicos.
	Fin del procedimiento

CONSTANCIAS
Realizado por:
…….
Catherine López
ESTUDIANTE UTN
Revisado y aprobado por:
…….
Manuel Guaján
INFORMÁTICO HSLO

Fuente: Autoría propia

Diagrama de flujo:

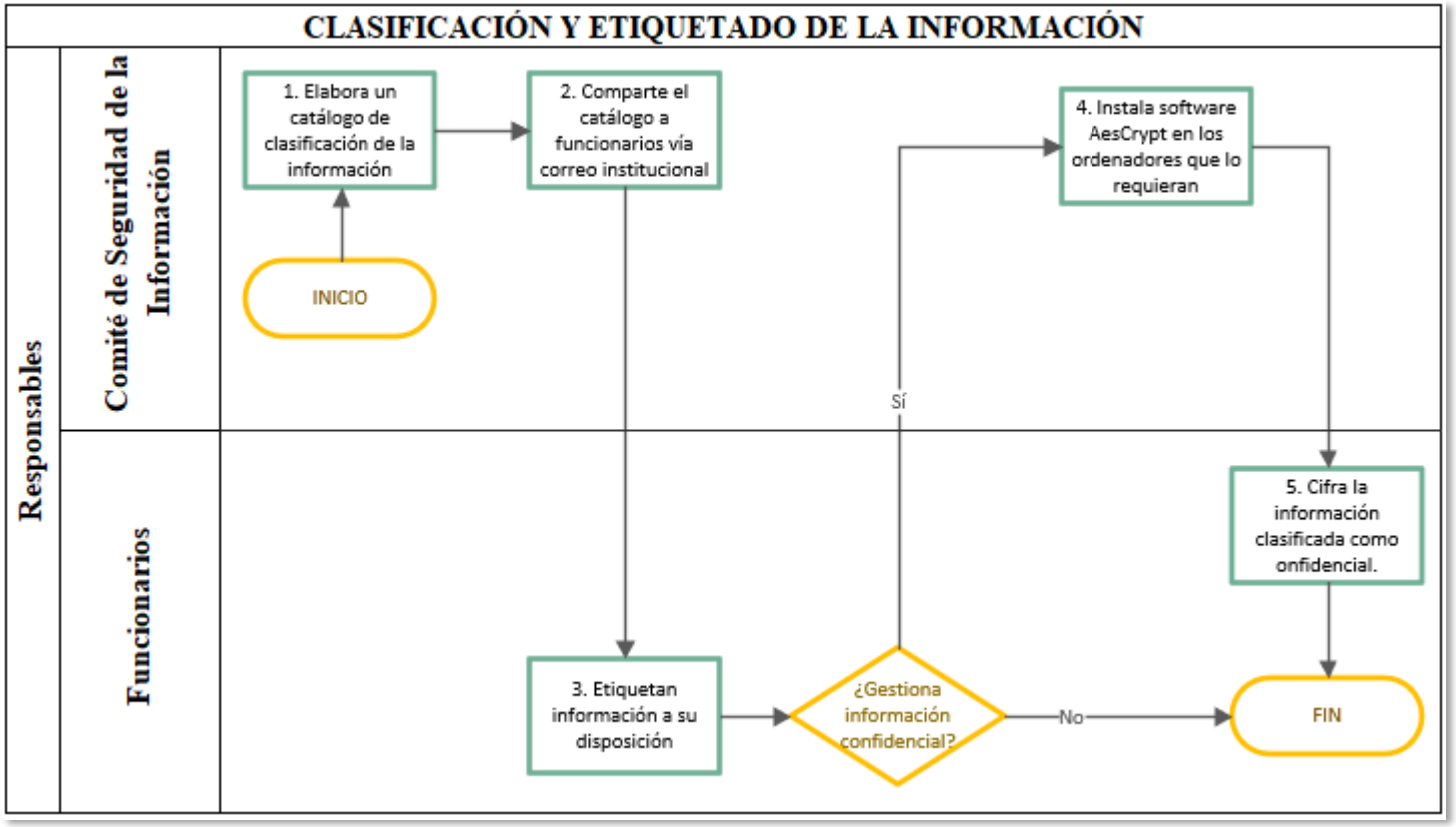


Figura 18. Diagrama de Flujo del procedimiento de clasificación y etiquetado de información

Fuente: Autoría propia

La herramienta que facilitará el cifrado de información confidencial es AESCrypt.

AESCrypt es un software de código abierto para el cifrado de información proporcionando un nivel alto de seguridad debido a que usa el algoritmo AES[2] con cifrado de 256 bits. Garantiza que la información sea protegida al asignar una contraseña para cada archivo o documento electrónico y, mientras más compleja sea, mejor será el cifrado.

Debido a la naturaleza de la información que se maneja en el HSLO, AESCrypt incrementará la seguridad de la información clasificada como confidencial a través del cifrado. La Figura 19 muestra cómo AESCrypt genera un archivo cifrado con extensión (.aes) el cual puede abrirse solamente si se introduce la contraseña inicialmente asignada.

Figura 19. Generación de archivo cifrado con AESCrypt

Fuente: Captura de Pantalla AESCrypt

Características:

- Es gratuito.
- Es compatible con Windows, Linux, MacOs.
- Cifra información sensible o confidencial.
- El consumo de recursos en el equipo es mínimo ocupando un tamaño en disco de 392 KB y 1,5 MB en la memoria RAM.

[2] Estándar de Cifrado Avanzado

El manual de instalación de AESCrypt se encuentra en el Anexo H al final del documento.

4.4.4 Sección IV – Seguridad de los Recursos Humanos

El artículo 11 referente a la selección de personal, la NTE INEN ISO/IEC 27799:2008 sugiere que se recopile un número considerable de referencias domiciliarias de los funcionarios, sobre todo de los profesionales de salud debido a los frecuentes cambios y rotaciones y de ser posible, llevar a cabo comprobaciones de actividades criminales pasadas, estos controles tienen como fin de evaluar de manera más objetiva a los aspirantes a funcionarios. El proceso para efectuar esta actividad se indica en la Tabla 45 y en el diagrama de flujo como lo interpreta la Figura 20.

Tabla 45. Procedimiento para la selección de personal y formalización del Acuerdo de Confidencialidad

Ministerio de Salud Pública

HOSPITAL SAN LUIS DE OTAVALO – DISTRITO 10D02

SECCIÓN II – ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	
Procedimiento:	Procedimiento para la selección de personal y formalización del Acuerdo de Confidencialidad
Objetivo:	Describir el procedimiento a seguir para formalizar el Acuerdo de Confidencialidad de la Información al nuevo y actual personal del HSLO.
Alcance:	Este procedimiento se encuentra sujeto tanto al personal nuevo como a los actuales funcionarios.
Responsables:	• Director del HSLO • Personal de Talento Humano (TT. HH) • Aspirantes

- Responsable de Seguridad de la Información del área de TIC

ACTIVIDAD	**DESCRIPCIÓN**
	Inicio de procedimiento
1	El responsable de Talento Humano convoca a los aspirantes a funcionarios para el HSLO.
2	El/los aspirantes asisten a la Institución y se dirigen a la oficina de Talento Humano.
3	El responsable de Talento Humano realiza la entrevista al aspirante el cual debe proveer toda la información necesaria la cual permita solventar todas las interrogantes posibles.
Condición ¿El aspirante cumple requisitos?	Si la información proporcionada por el aspirante satisface los requisitos establecidos por Talento Humano continúa con la Actividad 4, caso contrario se retorna a la Actividad 1.
4	Talento Humano formaliza el contrato laboral con el aspirante y le informa acerca del Acuerdo de Confidencialidad o No Divulgación de la Información.
5	Talento Humano informa al aspirante la existencia del Acuerdo de Confidencialidad o No Divulgación de la Información.
6	El aspirante lee y firma el Acuerdo de Confidencialidad o No Divulgación de la Información, comprometiéndose con el cuidado de los activos de información del HSLO.
7	Talento Humano informa al Director del HSLO la integración de un nuevo funcionario.
8	El Director autoriza al Responsable de la S.I del área de TIC que conceda privilegios de acceso a los Sistemas de Información al aspirante.
9	El Responsable de la S.I del área de TIC informa y otorga al aspirante los privilegios de acceso a los Sistemas de Información correspondientes.
	Fin del procedimiento.

CONSTANCIAS
Realizado por: ……. Catherine López ESTUDIANTE UTN
Revisado y aprobado por: ……. Manuel Guaján INFORMÁTICO HSLO

Fuente: Autoría propia

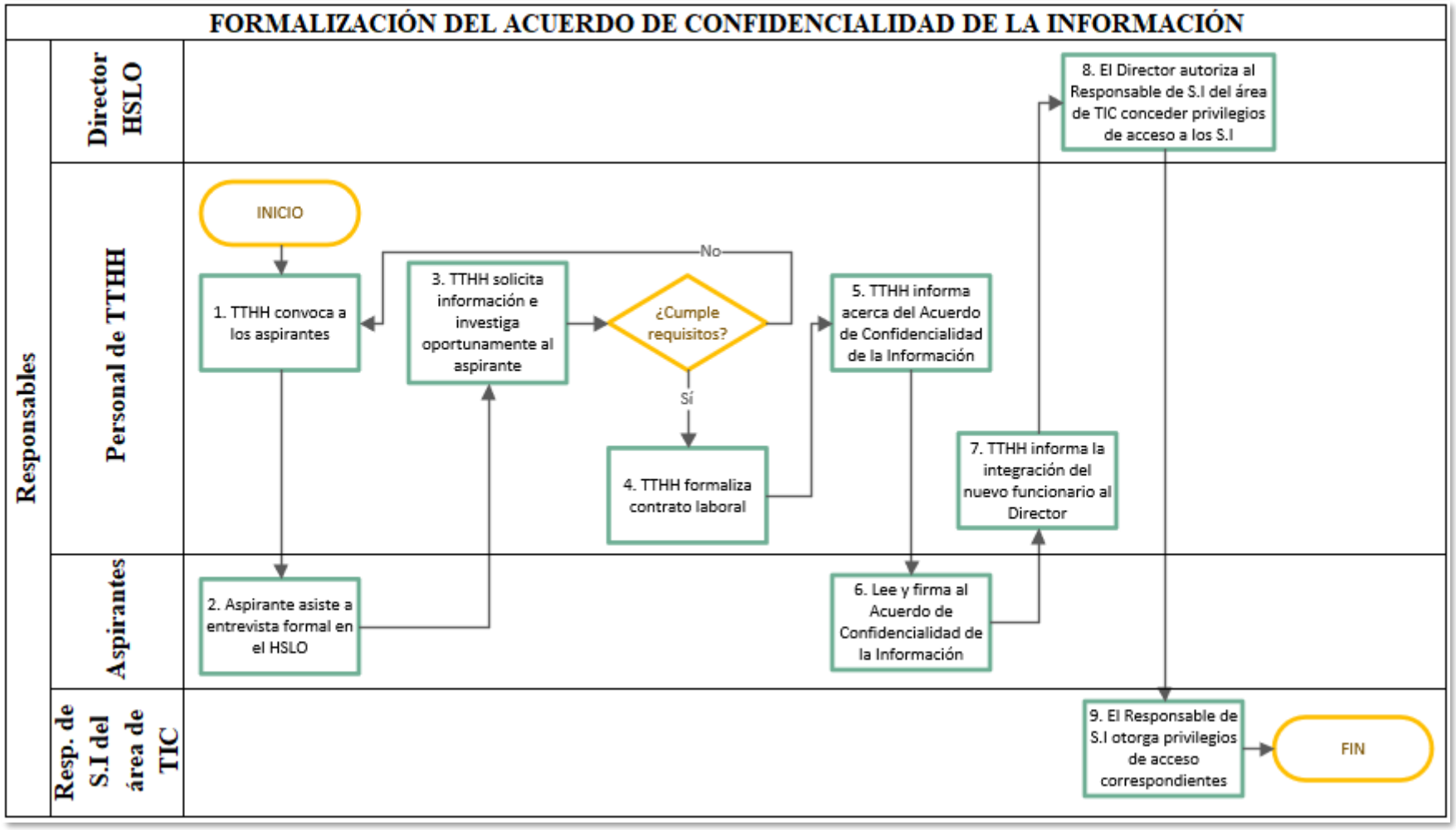


Figura 20. Diagrama de Flujo del procedimiento de selección de personal y oficialización del Acuerdo de Confidencialidad

Fuente: Autoría propia

Los artículos 12 y 13 trata acerca de las funciones y responsabilidades del personal, donde las políticas mencionan que una vez que los funcionarios sean contratados, el jefe de Talento Humano debe informar a la máxima autoridad la integración del nuevo personal para que autorice al responsable de la Seguridad del área de TIC la habilitación de sus privilegios de acceso a los sistemas de información. Asimismo, estos privilegios serán retirados una vez que los funcionarios cesen su contrato, esto aplica para pasantes, estudiantes, auxiliares, etc.

4.4.6 Sección V – Seguridad física y del entorno

En esta sección según el análisis de riesgos se enfatiza la importancia de asegurar los equipos informáticos, es decir, no sólo requieren protegerse a nivel de software sino a nivel físico, por ello se sugiere que cada área en la que se encuentren estos activos posea elementos de extinción de incendios y que se verifique la integridad de los mismos una vez por semana. En el Anexo J al final del documento se encuentra una cotización de precios y recursos necesarios para solventar este riesgo.

El artículo 16 hace referencia a la seguridad física del cuarto de equipos, el cual no cuenta con sistemas de control de acceso físico para evitar accesos no autorizados a esta área crítica de la Institución, de igual manera en el Anexo J consta la cotización para la adquisición de este sistema.

Por su parte, el artículo 17 sugiere que se vigile la permanencia de usuarios externos en las áreas que contienen sistemas de información, una advertencia que no está de más mencionarla debido a la gran afluencia de ciudadanos en la Institución.

Los 18 y 19 acerca de la seguridad del cableado menciona que este recurso requiere permanecer en óptimas condiciones debido a que representa el medio físico por el cual se efectúan las comunicaciones.

Cabe mencionar que la nomenclatura del etiquetado de cableado estructurado, según la normativa de etiquetado de cableado estructurado ANSI[3]/TIA[4]/EIA[5] 606A se define como sigue (Tabla 46).

Tabla 46. Nomenclatura de etiquetado de cableado estructurado

Cuarto de Telecomunicaciones	
fs	f= Caracter alfanumérico del piso donde se ubica el cuarto de equipos. s= Caracter alfanumérico con un identificador único del cuarto de equipos.
Enlaces horizontales	
fs - an	fs= Identificador del cuarto de equipos a= Uno o dos caracteres alfanuméricos que identifiquen al Patch Panel. n= Hasta cuatro caracteres alfanuméricos que identifiquen el número de puerto del Patch Panel.

Fuente: Adaptado de (ITCA)

Las etiquetas deben colocarse en ambos extremos de los cables y posicionarlas en forma horizontal de tal forma que sean visibles y legibles, un ejemplo de etiqueta que identifica al puerto 3 del Patch Panel B ubicado en el primero piso del cuarto de equipos:

1A – B03

A causa de que el estado del cableado en la Institución necesita una reestructuración, en el Anexo J se realiza una cotización de todos los implementos que permitirán llevar a cabo este proceso.

4.4.7 Sección VI – Gestión de las comunicaciones y operaciones

En esta sección intervienen un conjunto de procedimientos a ejecutarse para suplir políticas por medio del uso de recursos de hardware y software y que tienen una relación

[3] Instituto Nacional Americano de Estándares
[4] Asociación de Industrias de Telecomunicaciones
[5] Asociación de Industrias Electrónicas

directa con la red de datos de la Institución y debido a las falencias encontradas en ella, se plantea realizar un rediseño en su estructura.

4.4.7.1 Planteamiento del Rediseño de la Red de Datos del HSLO.

A través de esta actividad pueden cumplirse los controles de los artículos 20, 21 y 22 de la Política de Seguridad de la Información del HSLO.

Realizar un rediseño de la red de datos no pretende juzgar o desvalorar a la red actual, más bien el objetivo es optimizarla, brindar una estructura más segura, flexible y mejor administrada para reducir aquellos riesgos que atenten contra la confidencialidad, integridad y disponibilidad de los equipos informáticos y la información contenida en ellos, además se enfoca en proveer mayor seguridad a los servidores y dispositivos de la red de datos a través de la implementación de un firewall basado en el software Pfsense.

El rediseño se efectuará utilizando el simulador de redes GNS3 para representar de manera virtual los dispositivos que conforman la red de datos y realizar pruebas necesarias que constituyen la implementación del Firewall.

- **GNS3:** Es un Simulador gráfico de redes que, al igual que los softwares VMWare o VirtualBox permiten virtualizar varios tipos de sistemas operativos dentro de un entorno virtual en un computador. GNS3 por su parte también emula hardware de los dispositivos de enrutamiento de la marca Cisco con sus respectivos sistemas operativos, por lo tanto, su entorno gráfico facilita el dimensionamiento de topologías de red.

GNS3 para su funcionamiento se basa en los componentes Dynamips y Dynagen. Dynamips es el software que permite la emulación de IOS del hardware Cisco, mientras que Dynagen es la herramienta de configuración de Dynamips, con una interfaz de

administración en modo texto que habilita funciones como iniciar, detener, capturar tráfico de servicios, entre otros (Rocha, 2019).

4.4.7.1.1 Firewall.

Conocido también como cortafuegos, es un dispositivo de software o hardware capaz de discernir el tráfico entrante o saliente que atraviesa una red mediante la configuración de reglas que determinan si se permiten o se deniegan los paquetes en función de los filtros establecidos.

Es utilizado principalmente para asegurar los dispositivos de red de una organización tales como servidores y computadores con el objetivo de evitar ataques externos, denegación de servicios y reducir los peligros de los accesos no deseados; suelen ser situados entre la red interna y el nodo o router de frontera del proveedor de Internet, de tal forma que todo el tráfico deba atravesar el firewall antes de ingresar a la red (Lancho, 2017).

4.4.7.1.2 Pfsense.

Es un software comúnmente utilizado como enrutador y firewall, de código abierto basado en FreeBSD, característica que le permite ser instalado en computadores de distintas capacidades o en servidores; posee una atractiva interfaz web para la administración del sistema, implementación de reglas, monitoreo de la red, entre otros, donde sus principales características son: Balanceo de carga, Firewall, NAT (Traducción de direcciones de red), Portal Cautivo, Servidor VPN (Red privada virtual), Servidor DHCP (Protocolo de configuración dinámica de host), Servidor DNS (Sistema de nombres de dominio), Servidor Proxy entre otras. Varias organizaciones en el mundo han confiado en Pfsense para asegurar las redes, debido a su flexibilidad y confiabilidad comprobada, y que actualmente se encuentra operativo en el HSLO con una excelente acogida.

La Tabla 47 indica los requisitos mínimos de hardware para la instalación de Pfsense.

Tabla 47. Requisitos mínimos de hardware para Pfsense

Componente	Descripción
Velocidad CPU	600 MHz o más rápido
Memoria RAM	512 MB o más
Tamaño en Disco	4 GB o más, puede ser Disco Duro HDD o disco de estado sólido SDD.
Tarjetas de red	Una o más compatibles con el equipo
Unidad de arranque	USB o CD/DVD-ROM

Fuente: Adaptado de (Netgate, 2019)

El planteamiento del rediseño de la red de datos consta de lo siguiente:

- Un diseño basado en el uso de Pfsense como sistema perimetral o firewall, con tres tarjetas de red, una para la red WAN[6], LAN[7] y también para crear una red DMZ[8] donde se colocarán los servidores que actualmente no atraviesan un firewall y que son vulnerables a ataques externos.
- Segmentación de la red LAN en redes Vlan[9] para facilitar la administración de la red, proveer mayor seguridad y flexibilidad, reducir los dominios de difusión, optimizar el consumo del ancho de banda disponible y mejorar el rendimiento.
- Aprovechamiento del potencial de los equipos existentes, 4 de sus switches ubicados en el rack son administrables con capacidades de conmutación y enrutamiento y que pueden usarse para la declaración y troncalización de redes Vlan, siempre y cuando el cableado estructurado se encuentre en óptimas condiciones.

[6] Red de área amplia
[7] Red de área local
[8] Zona Desmilitarizada
[9] Red de área local virtual

- Creación de una VPN con el objetivo de gestionar de manera remota los servidores internos estableciendo una conexión segura entre los extremos de la red.
- Implementación de un servidor DNS para acceder a los servicios de la Institución a través de la resolución de nombres de dominio en lugar de direcciones IP.
- Implementación de un Servidor Proxy para controlar el tráfico entrante y saliente a través de la categorización de sitios web permitidos y no permitidos a los cuales los funcionarios pueden navegar en Internet.
- Configuración de un Portal Cautivo como método de autenticación de usuarios para el acceso a la red cableada.
- Implementación de un servidor Radius como mecanismo de autenticación de usuarios para el acceso a la red inalámbrica.

4.4.7.1.3 Direccionamiento IP.

Con Pfsense será posible obtener una gestión centralizada de la red que estará conformada de tres segmentos WAN, LAN y DMZ que se describen a continuación:

- Zona LAN: Es la red interna LAN del HSLO en donde se encuentran todos los equipos de la red local tales como computadores, cámaras, impresoras, etc.
- Zona DMZ: Esta zona debe ser independiente del resto para poder controlar el tráfico y peticiones realizadas tanto por los usuarios internos como desde redes externas hacia los servidores de la Institución.
- Zona WAN: Es la interfaz que se enlaza con el enrutador de borde CNT para la salida hacia Internet.

La dirección IP que será colocada en la interfaz WAN en la topología de red simulada es 192.168.137.98/24, en la interfaz DMZ se coloca la dirección IP 192.168.4.1/24 y, finalmente en la interfaz de la red LAN se configuran las redes Vlan con su respectivo direccionamiento.

La Tabla 48 indica el direccionamiento IP de la red LAN segmentada en redes Vlan, la cual se ha desarrollado de acuerdo al número de hosts internos existentes y considerando un incremento de usuarios en un 20%.

En el rediseño se emplea un modelo en capas o niveles que según lo indica (Ariganello, 2016) tiene como objetivo simplificar el diseño, implementación y administración de las redes, acelerando la convergencia, manteniendo aislados posibles problemas por capas y reduciendo la sobrecarga de los dispositivos. La capa de acceso tiene un nexo directo con los equipos de los usuarios y soporta tecnologías como Ethernet y Wireless, la capa de distribución es el punto de concentración de los dispositivos de acceso y enrutará el tráfico entre las Vlan, mientras que la capa de núcleo recibe las peticiones de los usuarios procesadas a nivel de capa de distribución y enruta el tráfico hacia los servicios solicitados.

La Figura 21 representa el rediseño de la red de datos del HSLO con una estructura por niveles, en la red LAN se encuentran las redes Vlan y en la DMZ determinados servidores.

Tabla 48. Direccionamiento IP de Vlan

VLAN	Nombre	Red	Hosts necesarios	Hosts disponibles	Máscara de Subred	Rango de direcciones IP	Dir. Broadcast
10	Administrativos	192.168.10.0	65	126	255.255.255.128	192.168.10.1 - 192.168.10.126	192.168.10.127
20	Doctores	192.168.20.0	57	62	255.255.255.192	192.168.20.1 - 192.168.20.62	192.168.20.63
30	Impresoras	192.168.30.0	24	30	255.255.255.224	192.168.30.1 - 192.168.30.30	192.168.30.31
40	TIC	192.168.40.0	10	14	255.255.255.240	192.168.40.1 - 192.168.40.14	192.168.40.15
50	WLAN	192.168.50.0	9	14	255.255.255.240	192.168.50.1 - 192.168.50.14	192.168.50.15
60	Aplicaciones	192.168.60.0	8	14	255.255.255.240	192.168.60.1 - 192.168.60.14	192.168.60.15
70	Invitados	192.168.70.0	3	6	255.255.255.248	192.168.70.1 - 192.168.70.6	192.168.70.7
80	Gerentes	192.168.80.0	3	6	255.255.255.248	192.168.80.1 - 192.168.80.6	192.168.80.7
90	Servidores	192.168.90.0	3	6	255.255.255.248	192.168.90.1 - 192.168.90.6	192.168.90.7

Fuente: Autoría propia

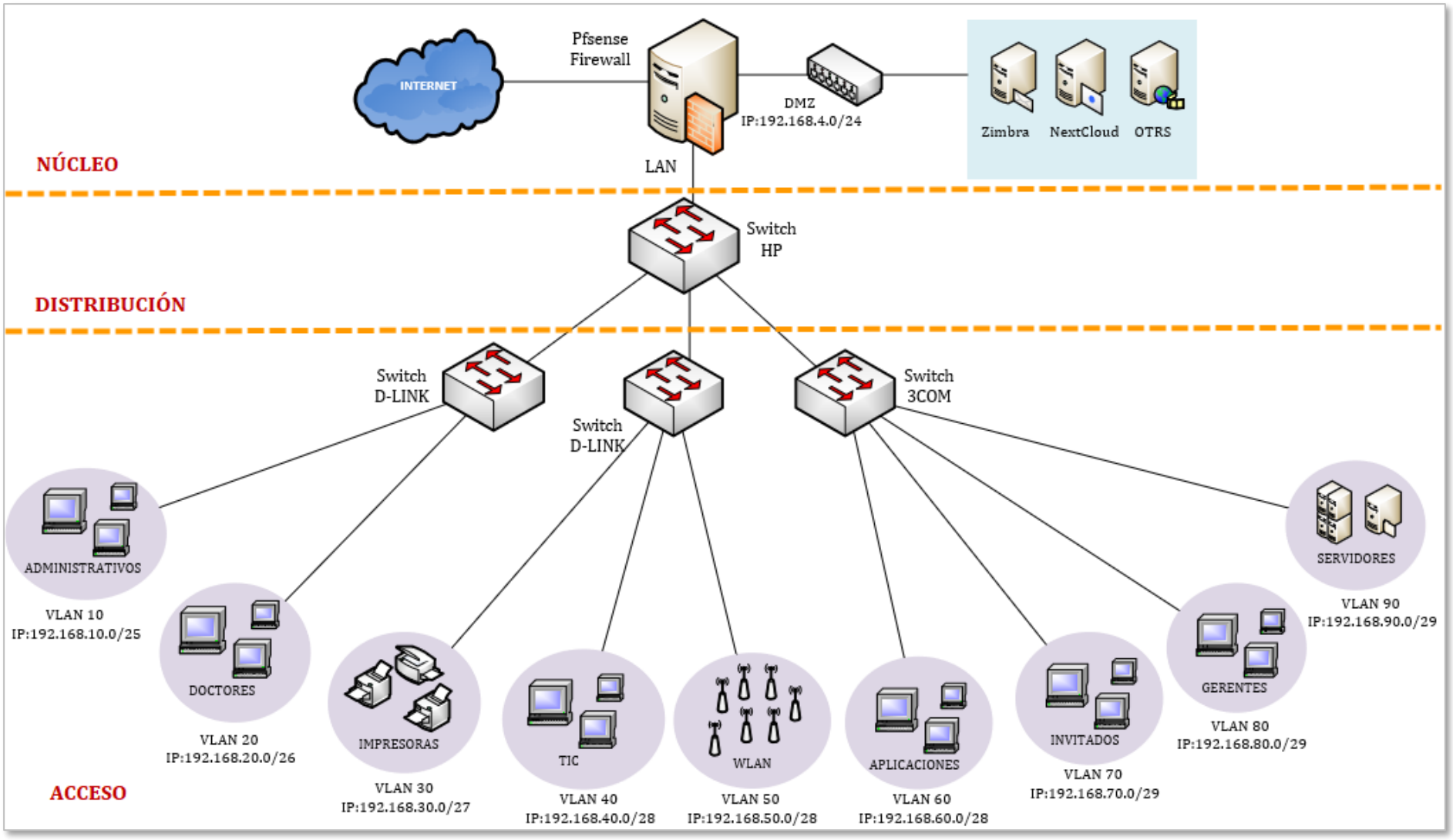


Figura 21. Rediseño de la red de datos del HSLO
Fuente: Autoría propia

Nota: La Vlan Aplicaciones pertenecen a un grupo de usuarios unicos que requieren acceso a uno de los servidores internos ubicados en la Vlan servidores, en ésta última se colocarán aquellos servidores de uso interno, en este caso SFTP y Aplicaciones.

Para desarrollar la simulación en GNS3 se han virtualizado los dispositivos descritos en la Tabla 49.

Tabla 49. Descripción de servicios virtualizados en GNS3

Dispositivo	Ubicación	Sistema operativo	RAM	Disco Duro
Servidor Zimbra	DMZ	Centos 7	2 GB	32 GB
Servidor NextCloud	DMZ	Centos 7	2 GB	8 GB
Servidor SFTP	Vlan Servidores	Ubuntu 14.04	1 GB	10 GB
Pfsense	Firewall	Centos 7	2 GB	25 GB
Servidor DNS	WAN	Centos 7	1 GB	8 GB
PC 1	Vlan Doctores	Linux Mint 19	1 GB	16 GB
PC 2	Vlan Administrativos	Linux Mint 19	1 GB	16 GB
PC 3	Vlan Aplicaciones	Windows 7	1 GB	20 GB
Switch Cisco	LAN	Cisco IOS c3725	134.2 MB	

Fuente: Autoría propia

El dimensionamiento de la topología de red realizada en GNS3 en el presente proyecto se observa en la Figura 22. Se han simulado algunas Vlan donde a cada una se ha conectado uno o dos hosts con sistema operativo Windows o Linux para realizar pruebas de conectividad respectivas.

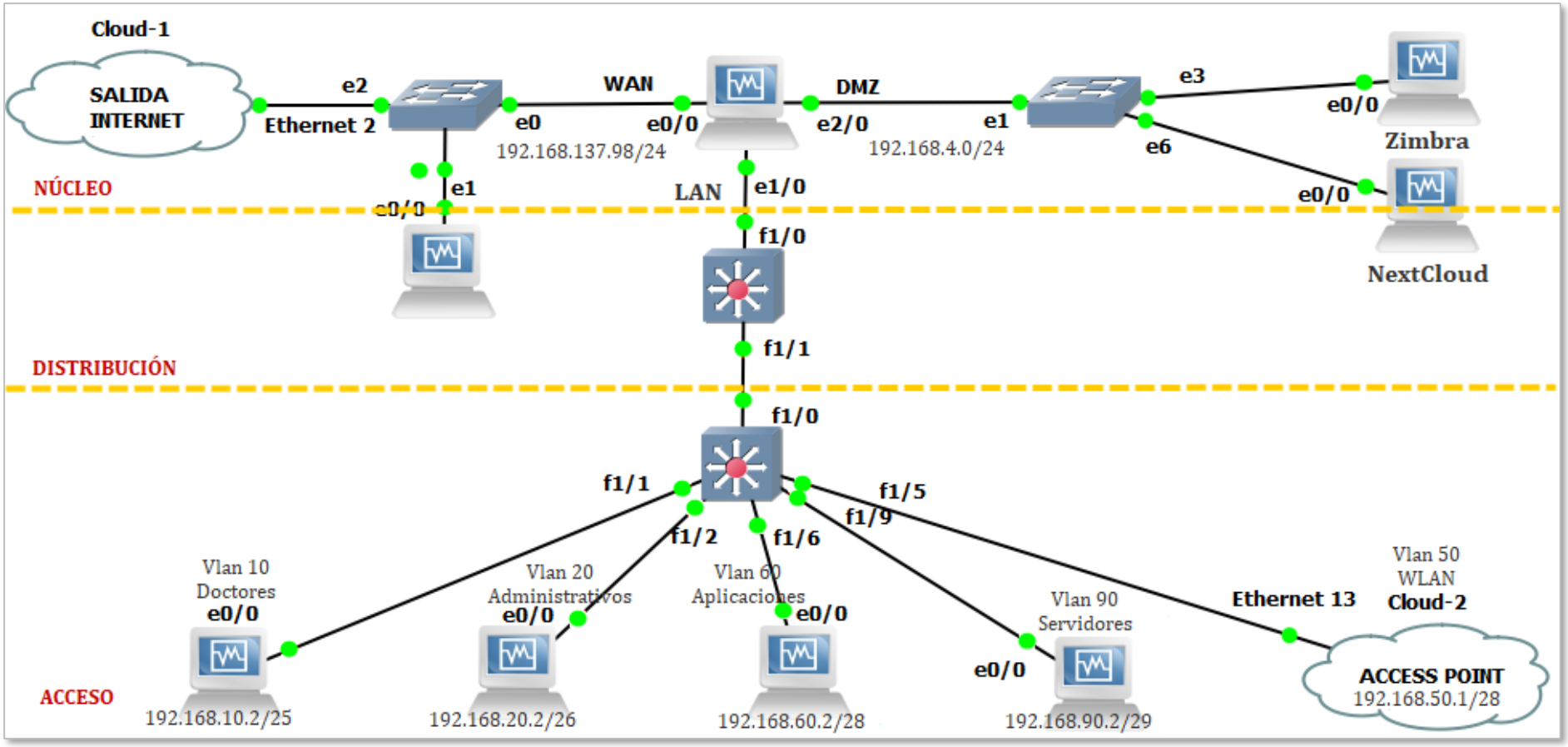


Figura 22. Topología de red simulada en GNS3

Fuente: Captura de pantalla GNS3

A la tarjeta de red de la DMZ de Pfsense se ha conectado un switch para que a este se conecten los servidores.

En la interfaz LAN de Pfsense se ha conectado un switch de capa 3, es decir que tiene características de un conmutación de paquetes y habilitará la comunicación entre las Vlan. Este switch debe conectarse con Pfsense por medio de un puerto configurado en modo troncal por donde transitarán las Vlan.

Para la comprobación de la red inalámbrica, se ha conectado un puerto del switch que pertenece a la Vlan WLAN a un adaptador de red USB – Ethernet que a su vez se conecta físicamente a la WAN de un access point desde el cual se recibirán las peticiones de usuarios de la red inalámbrica.

En la interfaz WAN de Pfsense se ha colocado un servidor DNS con el propósito de simmular un proveedor del servicio de hosting para registrar un dominio que se colocará en esta interfaz de Pfsense y de esta manera realizar peticiones desde usuarios externos a los servidores ubicados en la DMZ por medio de un nombre de dominio en lugar de una dirección IP.

4.4.7.1.4 Configuración de las Reglas de la DMZ.

Por medio de la configuración de reglas de la DMZ puede cumplirse el artículo 23 de la política la cual menciona que se establezca un segmento de red DMZ en donde se coloquen a los servidores de la Institución, a su vez permitirá cumplir con el artículo 24 recalcando que esta zona se crea con el objetivo principal de proteger a los dispositivos de la red interna.

- **DMZ:** Es la abreviatura de Zona Desmilitarizada conocida también como red perimetral. Consiste en una porción de red corporativa ubicada entre la Intranet e Internet. Proporciona una capa adicional de seguridad al asegurar que una red

interna no sea explotada directamente por nodos y redes externas. Una red DMZ tiene acceso limitado a la red interna, por lo que es imposible para un atacante violar la seguridad interna de una organización (Dadheech, Choudhary, & Bhatia, 2018).

La idea general es colocar los servidores públicos en el segmento DMZ para que la red interna y confiable se separe de la red no confiable (Figura 23). Ahora, si una parte malintencionada de alguna manera obtiene acceso a un servidor dentro de la DMZ, solo afectará a los servidores de la red DMZ, mas no a los de la red privada.

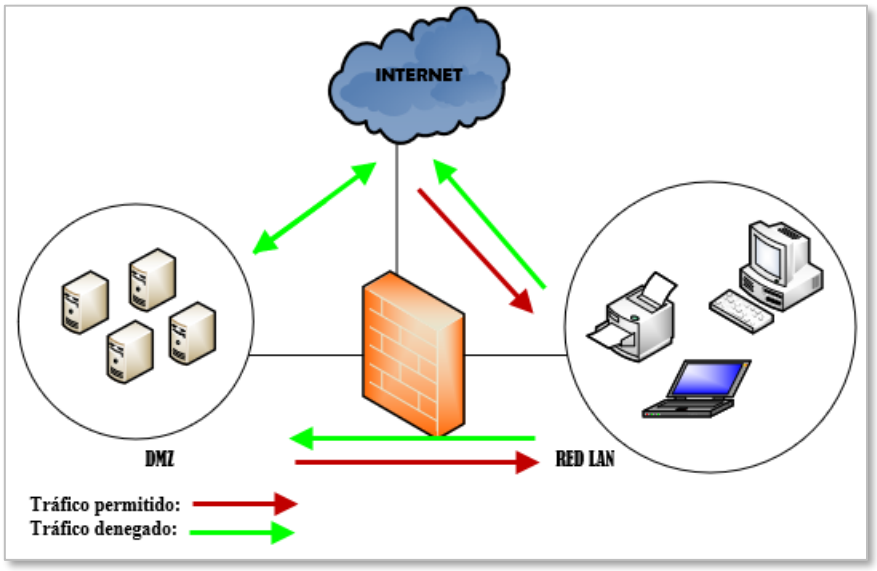


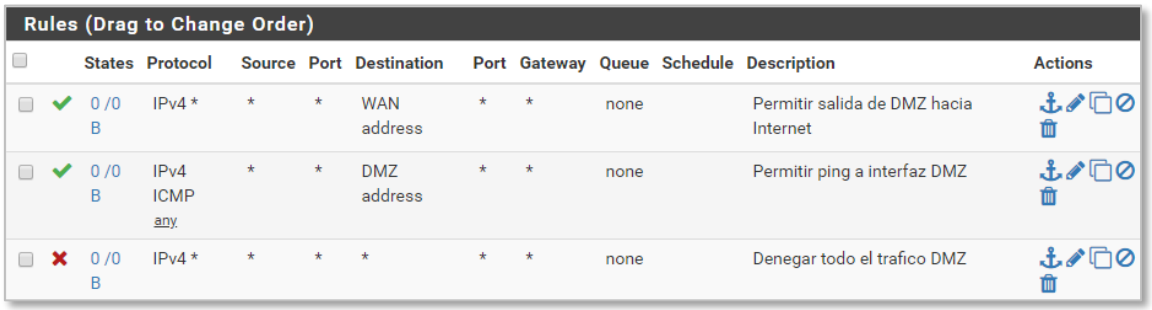
Figura 23. Diagrama de red común con DMZ

Fuente: Adaptado de redescisco.net

En la simulación, en la red DMZ se ubicarán los servidores de la Institución cuyo acceso será debidamente controlado y autorizado por el firewall. Por el contrario, en la arquitectura anterior, los usuarios desde Internet podían acceder a los servidores Zimbra, OTRS y NextCloud por su IP pública, el cambio radica en que ahora se colocarán en este segmento de red privado. Generalmente no se permite la conexión directa desde / hacia la red interna hacia / desde Internet, pero en este caso Pfsense actuará como un enrutador entre las tres redes propuestas.

En la interfaz DMZ se configuran las siguientes reglas:

- Una regla para habilitar que la DMZ tenga salida hacia Internet, para lo cual se dirige todo el tráfico de esta zona hacia la interfaz WAN (Figura 24), así, cuando se vean vulnerados los servidores por atacantes externos, la red LAN permanecerá protegida.
- Una regla para habilitar el ping dentro de la misma DMZ hacia la interfaz de dicha zona con el objetivo de comprobar conectividad.
- Una regla que deniegue todo y solo se permita el tráfico necesario.



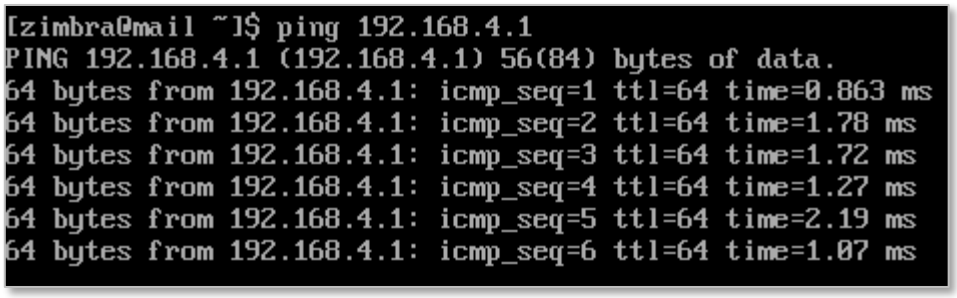
Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✔	0 /0 B	IPv4 *	*	*	WAN address	*	*	none		Permitir salida de DMZ hacia Internet	
✔	0 /0 B	IPv4 ICMP any	*	*	DMZ address	*	*	none		Permitir ping a interfaz DMZ	
✖	0 /0 B	IPv4 *	*	*	*	*	*	none		Denegar todo el trafico DMZ	

Figura 24. Configuración de las reglas de la DMZ

Fuente: Captura de pantalla Pfsense

Desde uno de los servidores ubicados en la DMZ se realiza un ping hacia la propia interfaz DMZ para comprobar conectividad (Figura 25).



```
[zimbra@mail ~]$ ping 192.168.4.1
PING 192.168.4.1 (192.168.4.1) 56(84) bytes of data.
64 bytes from 192.168.4.1: icmp_seq=1 ttl=64 time=0.863 ms
64 bytes from 192.168.4.1: icmp_seq=2 ttl=64 time=1.78 ms
64 bytes from 192.168.4.1: icmp_seq=3 ttl=64 time=1.72 ms
64 bytes from 192.168.4.1: icmp_seq=4 ttl=64 time=1.27 ms
64 bytes from 192.168.4.1: icmp_seq=5 ttl=64 time=2.19 ms
64 bytes from 192.168.4.1: icmp_seq=6 ttl=64 time=1.07 ms
```

Figura 25. Prueba de ping hacia Gateway de la DMZ

Fuente: Captura de pantalla servidor Zimbra

Igualmente, desde el mismo servidor ubicado en la DMZ se intenta hacer un ping hacia un host del segmento LAN (Figura 26), donde se comprueba que esta acción no se ejecuta, porque Pfsense será quien enrute el tráfico.

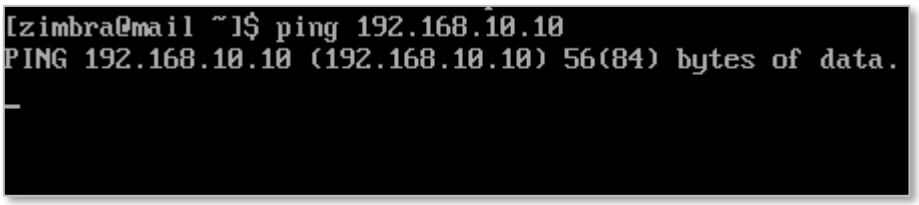


Figura 26. Prueba de ping desde DMZ hacia host LAN

Fuente: Captura de pantalla servidor Zimbra

4.4.7.1.5 VPN con Pfsense.

El objetivo de crear una red VPN por medio de Pfsense es para proveer una conexión segura extremo a extremo desde redes externas o Internet hacia un segmento de la red de datos del HSLO, con esta medida se cumplen los artículos 25, 26 y 27 de la Política de Seguridad de la Información.

- **VPN**: Una VPN (Red Privada Virtual) establece un canal seguro lógico para la comunicación entre dos entidades a través de Internet mediante un método de tunelización que encapsula el datagrama IP en un protocolo de tunelización, ocultando así los datos originales de intrusos o piratas informáticos. Establece virtualmente un enlace punto a punto o multipunto entre las partes que se comunican, tanto en el extremo de transmisión como en el de recepción, a través de una red de comunicación pública o compartida (Kuldeep & Gupta, 2016).

VPN utiliza distintos protocolos de encapsulación para la tunelización donde cada uno exige ciertos requisitos del sistema y niveles de seguridad. La Tabla 50 describe a cada protocolo con sus principales ventajas y desventajas.

Tabla 50. Ventajas y desventajas de los protocolos VPN

Protocolo	Ventajas	Desventajas
PPTP (Protocolo de tunelización punto a punto)	- Rápido - Usa cifrado estándar MS-CHAPv1-v2 - Mayor soporte de conexiones PPTP - No es seguro	-Problemas de seguridad -Soporta solo un túnel a la vez para cada usuario -Sin funciones de autenticación y cifrado
L2TP/Ipsec (Protocolo de túnel de capa 2/Protocolo IP seguro)	- Compatible con estándares de cifrado AES y 3DES - Admite múltiples túneles simultáneamente. - Compatibilidad multiplataforma	- Problemas de rendimiento - Soporta menos conexiones L2TP en el servidor VPN
SSTP (Protocolo de tunelización de sockets seguros)	- Seguridad en el cifrado - Usa estándar de cifrado SSL v3 (Protocolo de canal seguro)	- Mejor rendimiento en dispositivos propiedad de Microsoft
OpenVPN (VPN de código abierto)	- Rápido y muy seguro - Compatibilidad multiplataforma - Plataforma de código abierto - Compatible con varios algoritmos de cifrado - Usa protocolos SSL[10]/TLS[11]	- Requiere uso de cliente OpenVPN - Difícil configuración - Necesita mejoras para clientes móviles
IKEv2/Ipsec (Protocolo de intercambio de claves de Internet/Protocolo IP seguro)	- Admite variedad de estándares de cifrado - Es estable y muy rápido - Mejor rendimiento en dispositivos móviles	- Compatibilidad limitada de plataformas - Difícil configuración del servidor - Protocolo no es de código abierto

Fuente: Adaptado de (Bozovic, 2019)

En el presente proyecto se ha optado por implementar una VPN utilizando el protocolo OpenVPN por sus beneficios: es criptográficamente seguro, es la opción más amigable con el firewall, utiliza protocolos TCP o UDP y no se ve afectado por ninguna función NAT, con TLS se mitiga gran parte del peligro de divulgarse las claves

[10] Capa de sockets seguros
[11] Seguridad en la capa de transporte

compartidas, requiere el uso de certificados para el acceso remoto así como la autenticación de usuarios y es compatible con varios sistemas operativos.

En la Figura 27 se puede apreciar la manera en que establecerá un túnel de conexión segura el administrador de la red de la Institución con el servidor VPN en Pfsense.

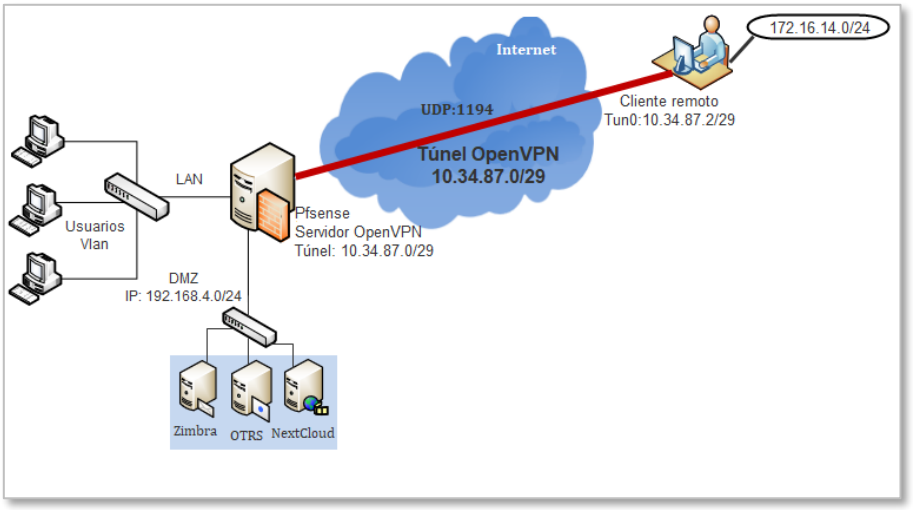


Figura 27. Servidor VPN con Pfsense

Fuente: Autoría propia

Una VPN es una función incorporada en Pfsense, OpenVPN es un servidor y cliente VPN de código abierto multiplataforma que emplea protocolos SSL/TLS que operan en la capa de transporte y establecen una conexión segura desde una extensión de una red LAN sobre redes externas o Internet, donde el tráfico que atraviesa este túnel viaja de manera encriptada proveyendo mayor seguridad en las comunicaciones.

La configuración del servidor VPN desde Pfsense consta de los siguientes pasos:

- Crear de una entidad certificadora que valide la emisión de certificados.
- Crear un certificado interno para el servidor VPN.
- Configurar el servidor OpenVPN habilitando el puerto de comunicación UDP 1194.

- Definir un segmento de red que se asignará a la VPN.
- Establecer la red alcanzable para la VPN o el extremo de conexión del túnel.
- Crear usuarios con privilegios de acceso a la VPN.
- Instalar el cliente exportador de llaves de usuario.
- Exportar la llave de usuario.
- Comprobación de funcionamiento de la VPN.

Una vez que este procedimiento se realice se exportará la llave del cliente, la cual contiene identificaciones numéricas y permisos respectivos para establecer conexión con la VPN. Desde el host de un usuario con sistema operativo Windows (Figura 28) que tenga instalada la herramienta OpenVPN GUI puede autenticarse introduciendo la contraseña de su llave.

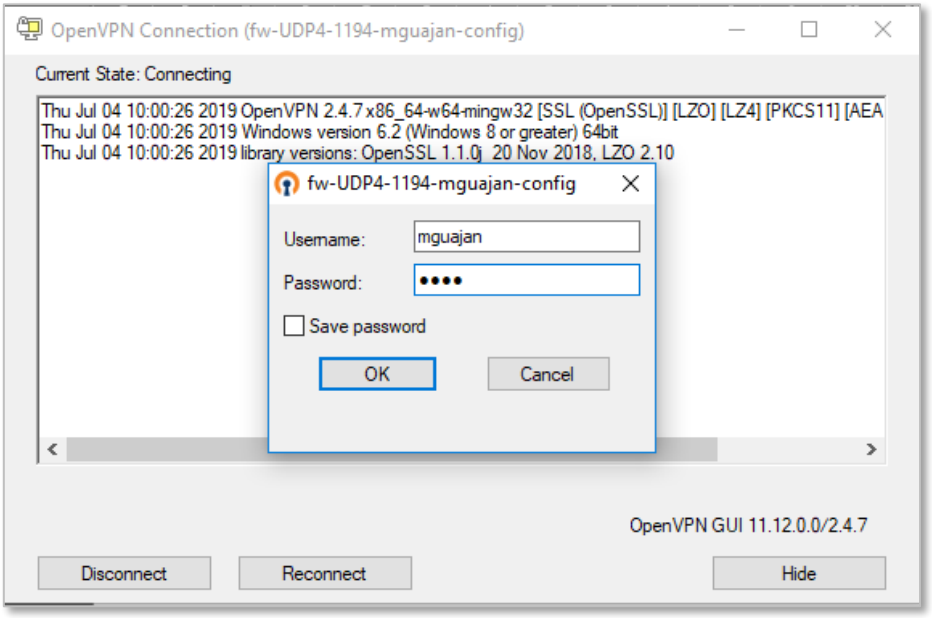


Figura 28. Autenticación de cliente Windows con OpenVPN

Fuente: Captura de pantalla usuario Windows

El host del usuario desde Internet al autenticase en la VPN automáticamente crea una nueva interfaz virtual TAP capaz de crear un túnel de red en el equipo y permite la encapsulación de paquetes Ethernet, es decir, en la capa de enlace y opera como si

estuviera dentro de la red interna. En la Figura 29 se observa que dicha interfaz genera una dirección IP dentro del segmento asignado a la VPN desde un host externo.

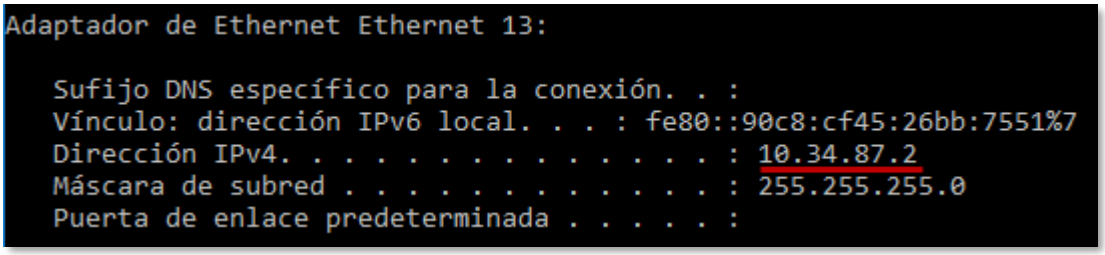


Figura 29. Creación de interfaz TAP en host Windows

Fuente: Captura de pantalla usuario VPN

De manera similar, para crear un puente con la VPN desde un host Linux se utilizará la línea de comandos. Al abrir un terminal en Linux Mint se introduce el comando mostrado en la Figura 30 y luego se coloca la clave de la llave respectiva.

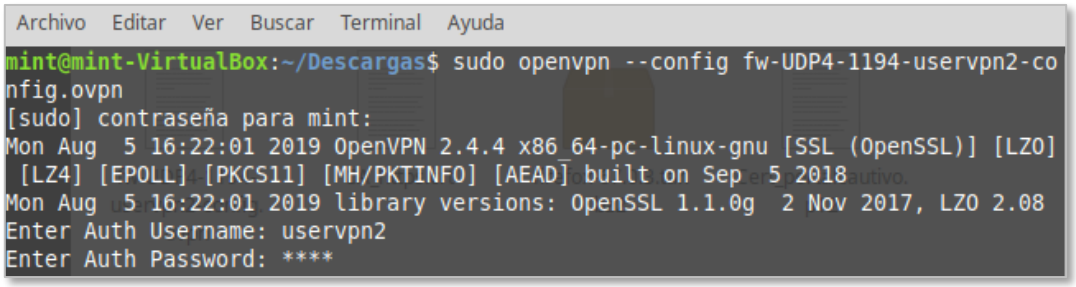


Figura 30. Autenticación de cliente Linux a red VPN

Fuente: Captura de pantalla usuario Linux

Y finalmente en este host también se crea la interfaz TAP con su respectiva dirección IP.

Nota: La información acerca de la implementación de OpenVPN en Pfsense se amplía en el Anexo I al final del documento.

4.4.7.1.6 Servidor DNS en Pfsense.

La tecnología DNS facilitará la interpretación de direcciones IP de las redes en nombres de dominio, por medio de la configuración de este servicio se cumplirán los artículos 28, 29 y 30 de la Política de Seguridad de la Información.

- **DNS:** El objetivo de los nombres de dominio es proporcionar un mecanismo para nombrar recursos de tal manera que se puedan utilizar en diferentes hosts, redes, familias de protocolos, Internet y organizaciones administrativas, en definitiva, un DNS permite solicitar la dirección de algún host con algún nombre de dominio en particular (IETF, 1987).

DNS es una función que también viene incorporada en Pfsense, permite resolver una dirección IP a un nombre de dominio o viceversa. Desde Pfsense se configura el Resolvedor DNS que gestiona las solicitudes DNS de los clientes y entrega las consultas a un servidor DNS (Figura 31), opera en la capa de aplicación del modelo OSI[12] a través del puerto UDP 53.

[12] Interconexión de sistemas abiertos

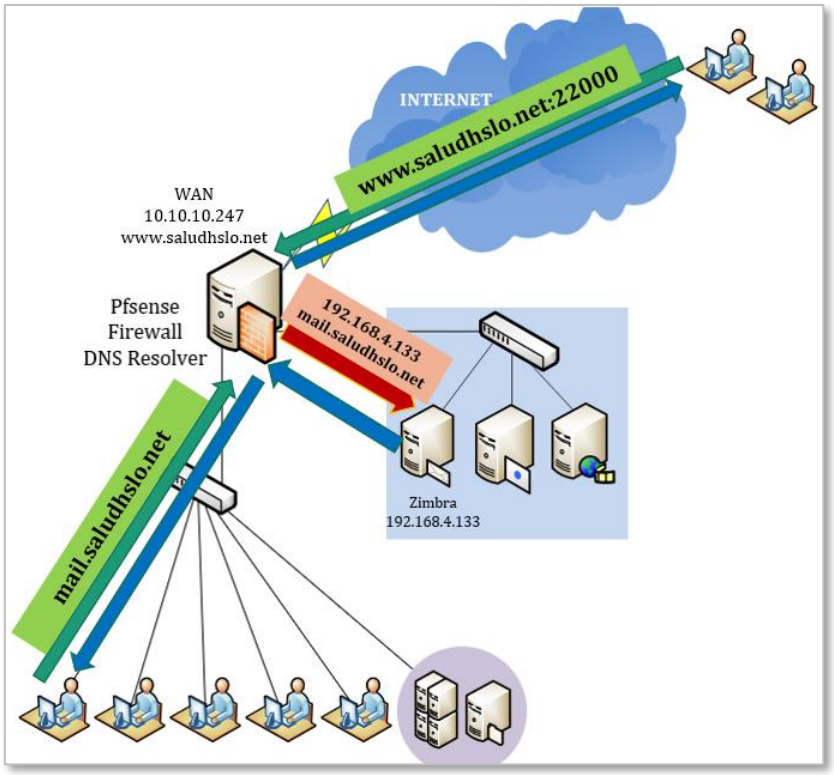


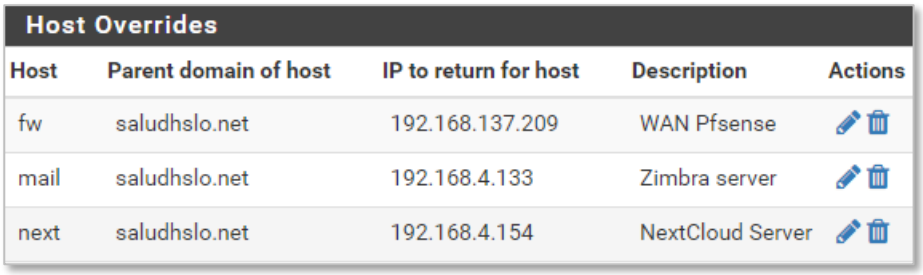
Figura 31. Servidor DNS con Pfsense

Fuente: Autoría propia

Los pasos a seguir para la configuración del DNS Resolver son:

- Habilitación del Resolvedor DNS.
- Establecimiento del puerto UDP 53.
- Selección de las interfaces que a través del DNS responderán las peticiones de los clientes.
- Habilitación de resolución de nombres de dominio para clientes OpenVPN.
- Creación de los registros de direcciones IP que serán resueltos a un nombre de dominio.
- Creación de los registros de nombres de dominio que serán resueltos a las direcciones IP respectivas.

Desde Pfsense se habilita el Resolvedor DNS donde se gestionan las anulaciones de hosts como lo indica la Figura 32, es necesario agregar un nombre a una dirección de red determinada.



Host Overrides

Host	Parent domain of host	IP to return for host	Description	Actions
fw	saludhslo.net	192.168.137.209	WAN Pfsense	
mail	saludhslo.net	192.168.4.133	Zimbra server	
next	saludhslo.net	192.168.4.154	NextCloud Server	

Figura 32. Configuración de dominios de hosts

Fuente: Captura de pantalla Pfsense

Con el Resolvedor DNS los funcionarios de la red interna y externa podrán acceder a los servidores de la Institución sin la necesidad de memorizar una dirección IP y realizarlo a través de un nombre que lo identifique, por ejemplo, en la Figura 33 se accede al servidor SFTP ubicado en la Vlan Servidores desde un usuario de otra Vlan por medio del dominio sftp.saludhslo.net.

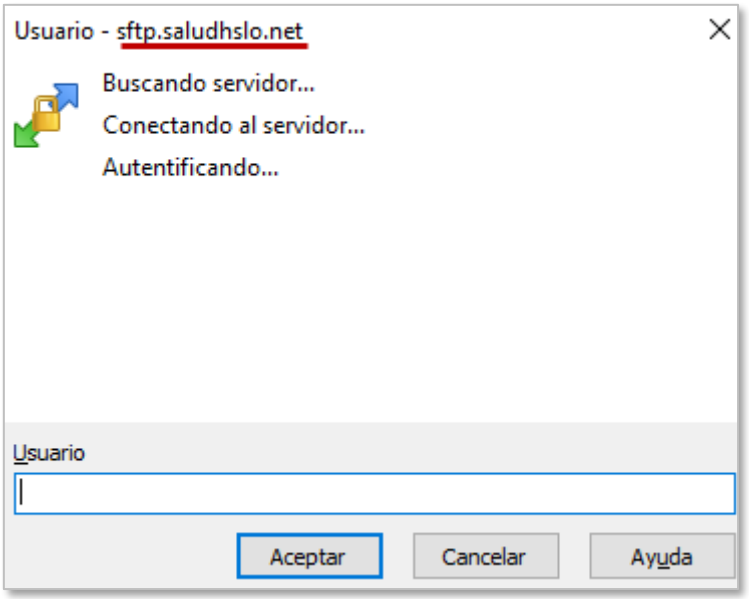


Figura 33. Acceso a servidor SFTP por nombre de dominio

Fuente: Captura de pantalla cliente WinSCP

Nota: Por motivos demostrativos el dominio utilizado es saludhslo.net, sin embargo, si el servicio DNS llegara a implementarse en el entorno real, el dominio a utilizarse sería hslo.gob.ec.

Las solicitudes de acceso a los servicios de la Institución desde redes externas se realizará a través del dominio https://www.saludhslo.net, por la razón de que los servicios se sitúan en una red interna y segmento de red distinto, es así que el tráfico generado desde redes externas necesariamente debe atravesar el Firewall, el cual con la configuración de reglas de NAT habilitará la traducción de direcciones externas a la dirección correspondiente del servicio solicitado. Asimismo, se configuran protocolos y puertos para acceder a los servidores para diferenciarlos, los números de puerto deben ser preferencialmente mayores a 1024.

En la Figura 34 se observa que para acceder por nombre de dominio hacia la administración de Pfsense desde Internet se realiza mediante el nombre www.saludhslo.net:10000.

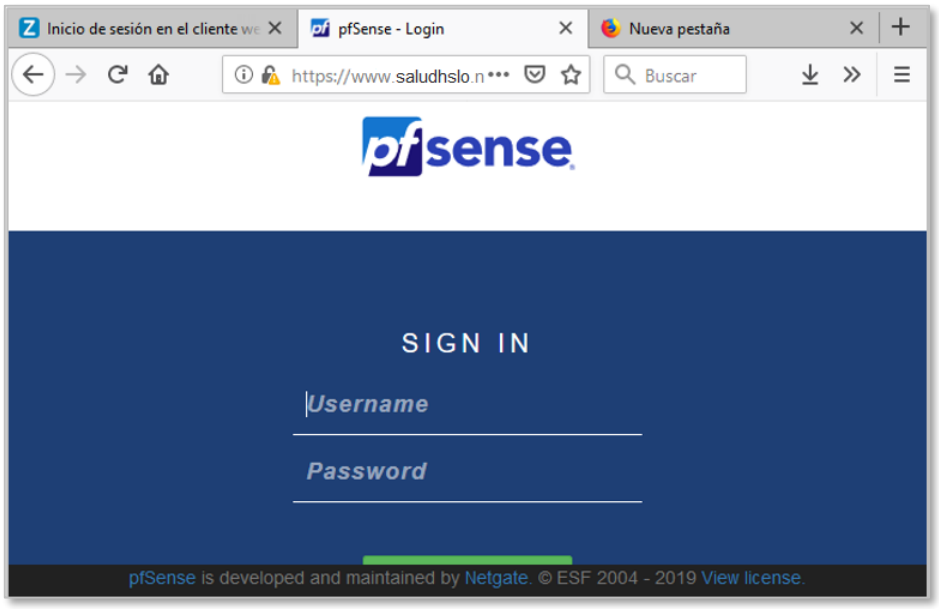


Figura 34. Acceso externo a administración de Pfsense por DNS

Fuente: Captura de pantalla Pfsense

Se ha demostrado que es posible acceder a los servidores tanto desde redes internas como externas, sin embargo, la seguridad es un factor crucial, por ello se recomienda utilizar canales seguros para el envío y recepción de información.

Específicamente para el servicio de correo electrónico, la información transmitida a través del cliente web de Zimbra viaja de manera no encriptada y cualquier atacante podría intervenir las comunicaciones y robar información, una alternativa a esto es utilizar clientes de correo para acceder a las cuentas de Zimbra, para ello se utilizará el cliente de correo electrónico de Linux Thunderbird para el envío y recepción de correo electrónicos sobre canales seguros utilizando los protocolos POP3 y SMTP con los puertos 995 y 587 respectivamente. En la Figura 35 el cliente Thunderbird se configura para la cuenta de un usuario en específico.

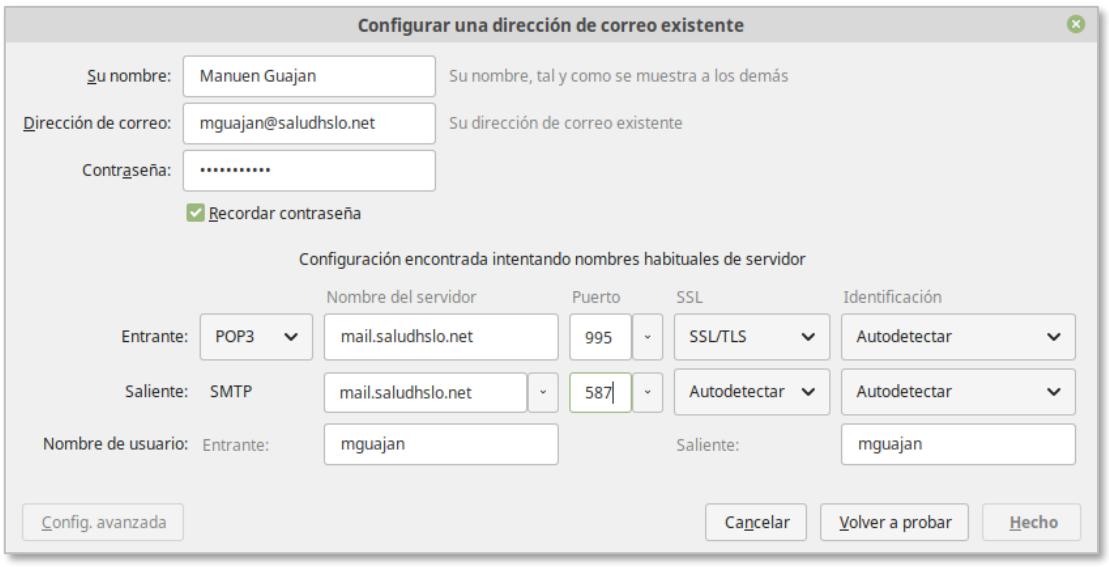


Figura 35. Configuración de cliente Zimbra en Thunderbird

Fuente: Captura de pantalla Thunderbird

De manera similar, la Figura 36 indica la configuración de un usuario Zimbra desde el cliente Outlook de Microsoft para hosts Windows.

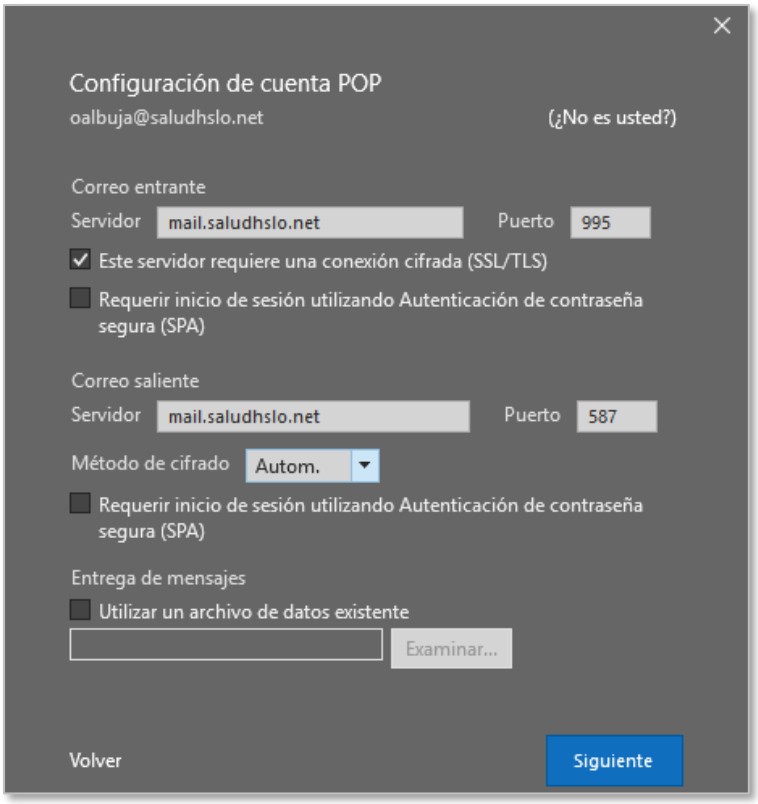


Figura 36. Configuración de cliente Zimbra en Outlook

Fuente: Captura de pantalla Outlook

Cabe mencionar que para que sea posible el acceso externo hacia los servidores institucionales ubicados en la DMZ, se requiere que Pfsense posea un dominio propio, esto puede llevarse a cabo a través de la compra del servicio de hosting a cualquier proveedor, que en este caso será CNT, empresa que en la actualidad lo provee. El nuevo dominio puede tener la siguiente nomenclatura: www.hslo.gob.ec en el entorno real.

Nota: La información acerca de la implementación del servidor DNS en Pfsense se amplía en el Anexo I al final del documento.

4.4.7.1.7 Portal Cautivo.

La configuración del mecanismo de control de acceso a la red mediante Portal Cautivo permite dar cumplimiento a los artículos 31, 32, 33, 34 y 35 respectivamente de la Política de Seguridad de la Información.

- **Portal Cautivo:** Es una aplicación que vigila el tráfico http y hace que los usuarios primero atraviesen por una página inicial que requiere una autenticación especial que les conceda acceso a Internet. Este servicio es comúnmente implementado en aeropuertos, parques, hoteles, proveedores de servicios de Internet, entre otros. Como (Netgate, 2019) señala, la función de Portal cautivo de Pfsense redirige a los usuarios a una página web alojada en el firewall antes de permitir el acceso a Internet. Desde esta página, se puede obligar a los usuarios a autenticarse antes de otorgarles acceso.

Se implementará un Portal Cautivo con el objetivo mejorar el control de la actividad de los usuarios administrando sus privilegios de acceso a Internet, de tal forma que aquellos usuarios que no pertenezcan a la Institución y requieran hacer uso de dicho recurso necesitarán la aprobación de la máxima autoridad para que sea quien autorice al Responsable de la Seguridad del área de TIC la habilitación de los permisos respectivos, con estas medidas se cumple la Política de Seguridad de la Información y se evita el acceso a la red a personas no autorizadas.

El Portal Cautivo actúa como un servidor de autenticación de usuarios que opera en la capa 3 del modelo OSI y este mecanismo se utilizará para administrar el acceso a la red para los usuarios de la red cableada, de tal forma que bloqueará el acceso a la red mientras no se autentiquen. El modo de operación del Portal Cautivo desde Pfsense se explica a continuación (Figura 37).

- Los usuarios abren un navegador intentando acceder a un sitio web e implícitamente se realiza una solicitud http o https.

- El Portal Cautivo desde Pfsense intercepta la solicitud https o http y redirecciona automáticamente esta solicitud hacia la página de inicio de sesión del portal cautivo donde los usuarios deben autenticarse.
- El Portal Cautivo valida los datos de entrada de los usuarios contra la base de datos de usuarios del Portal Cautivo.
- Cuando el usuario se haya validado contra la base de datos de usuarios del portal, el servidor otorgará acceso a Internet y mostrará como página de inicio a la del Ministerio de Salud Pública.

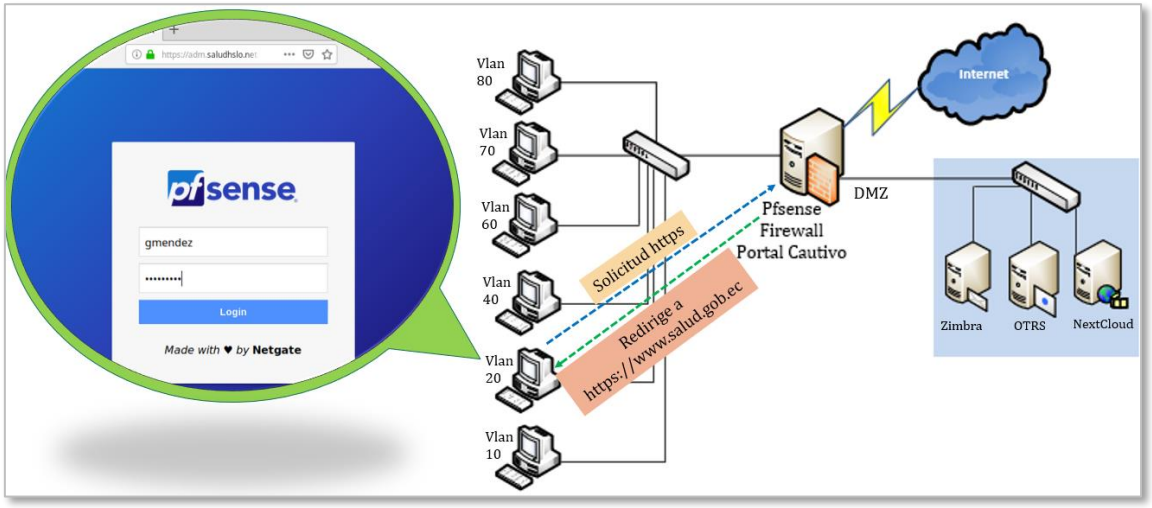


Figura 37. Autenticación de usuarios Portal Cautivo - Pfsense

Fuente: Autoría propia

El Portal Cautivo viene integrado a Pfsense por lo cual no es necesario descargar un paquete adicional, el procedimiento de configuración del Portal Cautivo consta de:

- Crear una zona para el Portal Cautivo.
- Identificar las interfaces que estarán activas para esa zona.
- Establecer un tiempo de inactividad después del cual los usuarios se desconectarán y deberán volver a iniciar sesión.

- Luego se habilita el inicio de sesión https con el propósito de transmitir las credenciales de acceso de los usuarios a través de una conexión https y evitar que esa información sea interceptada por espías.
- Especificar el nombre del servidor https, este nombre será usado en la solicitud del formulario https que hará aparecer el navegador, por lo tanto, este nombre debe coincidir con el establecido en el certificado SSL.
- Definir un certificado SSL, de lo contrario debe ser creado.
- El siguiente paso es crear un grupo y los usuarios que tendrán privilegios de acceso al Portal Cautivo.

Se comprueba desde un cliente interno el acceso al Portal Cautivo (Figura 38), al iniciar un explorador de Internet cualquiera se muestra automáticamente la ventana de inicio de sesión desde la cual los usuarios deben autenticarse con sus credenciales.

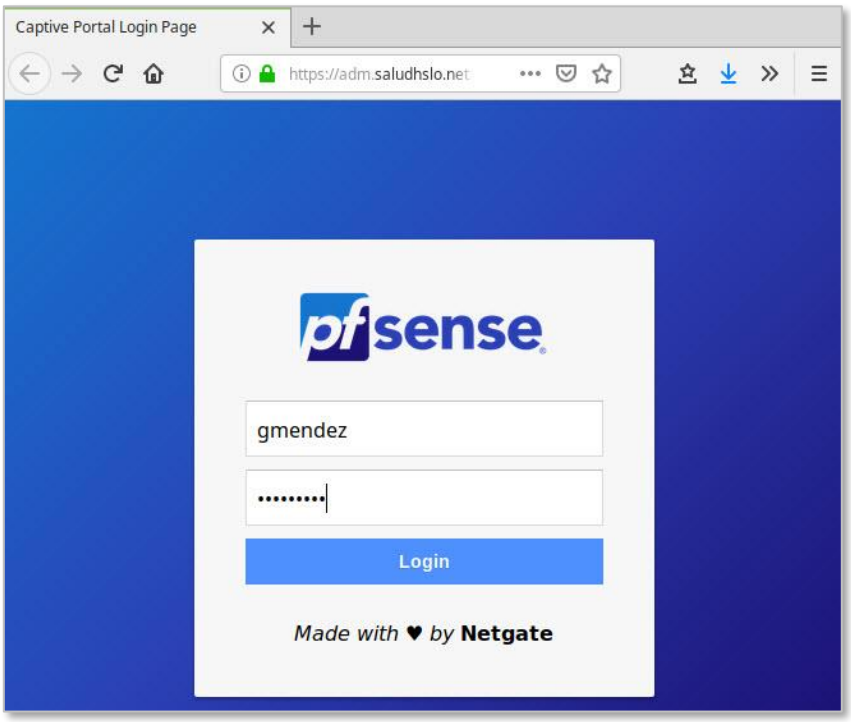


Figura 38. Página de inicio de sesión al Portal Cautivo

Fuente: Captura de pantalla servidor Zimbra

Simultáneamente, Pfsense facilita el monitoreo de los usuarios autenticados en el Portal Cautivo detallando la dirección IP del usuario, la dirección MAC del equipo, el nombre de usuario que lo identifica y la fecha y hora en que se autenticó; desde el menú Estado – Portal Cautivo es posible visualizarlo. La Figura 39 fue obtenida desde Pfsense en la Institución que por motivo de cumplimiento de la política interna se implementó.

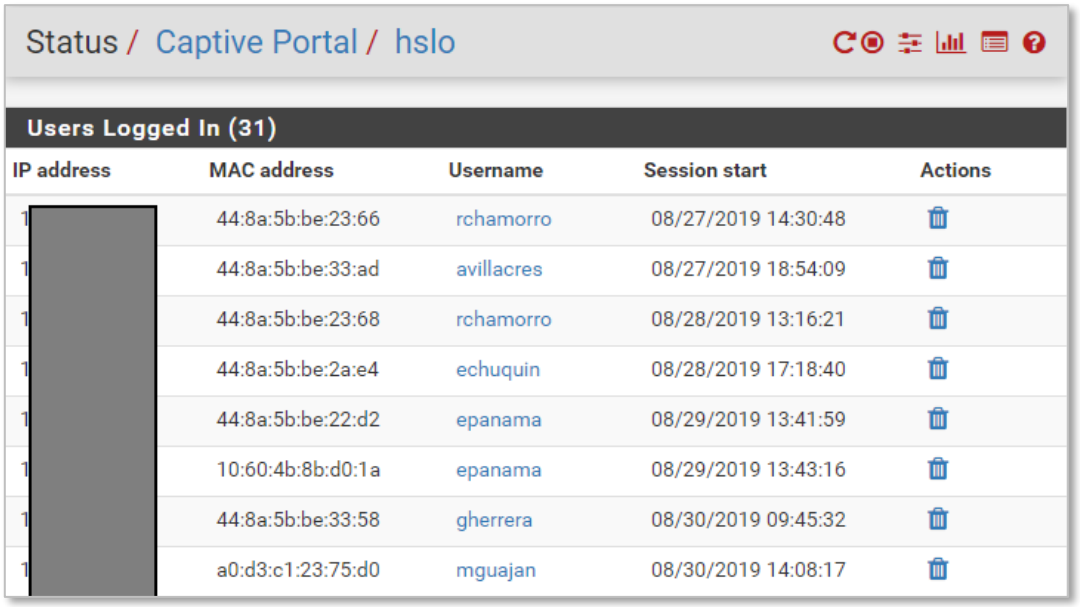


Figura 39. Usuarios autenticados con Portal Cautivo – Pfsense en el HSLO

Fuente: Captura de pantalla Pfsense

Cabe mencionar que en Pfsense el Portal Cautivo no está habilitado para operar paralelamente con un Servidor Proxy en modo No Transparente como el que inicialmente se encontraba implementado en la red de la Institución, por ello, es necesario configurar un Servidor Proxy en modo Transparente.

Nota: La información acerca de la configuración del Portal Cautivo en Pfsense se amplía en el Anexo I al final del documento.

4.4.7.1.8 Servidor Proxy.

Esta sección se presenta como un mecanismo que limite a los funcionarios la navegación en sitios web contrarios a los intereses de la Institución y es un complemento

importante al funcionamiento del Portal Cautivo configurado en Pfsense, además, permite dar cumplimiento a la política interna del HSLO.

- **Servidor Proxy**: Actúa como un escudo que protege y oculta a dispositivos internos de una red externa, envía y recibe paquetes encapsulados de aplicaciones específicas y escucha el tráfico a través del puerto 3128, cuando hay un servidor proxy en la red, el acceso a Internet se canaliza a través de él. Son útiles en redes con gran densidad de usuarios, debido a que las solicitudes que realizan se almacenan en la memoria caché del servidor proxy, de tal modo que no tiene que volver a realizar dichas solicitudes porque ya se encuentran aprendidas y almacenadas. En un proxy pueden aplicarse filtros para bloquear el acceso a determinados sitios web.

Un servidor Proxy funciona como un enlace que interconecta a usuarios internos con hosts externos, decidiendo qué tráfico se permite u obstruye según las reglas establecidas, toma las solicitudes de hosts internos y las envía a un destino en Internet. El modo de operación de un servidor proxy según lo señala (Cengace learning, 2010) es:

- Un host interno solicita acceso a un sitio web.
- La solicitud pasa por el servidor proxy, diagnostica el encabezado y contenido del paquete y lo compara con las reglas predefinidas.
- El servidor proxy reconstruye el paquete de datos con una dirección IP de origen diferente.
- El servidor proxy transmite el paquete hacia el destino y oculta al host real que realizó la solicitud.
- Las respuestas del destino se envían al servidor proxy verificando el paquete según las reglas predefinidas.

- El servidor proxy reconstruye el paquete de respuesta y se lo entrega al host de origen.

Una ilustración de la manera en que un servidor Proxy opera en la red interna se muestra en la Figura 40.

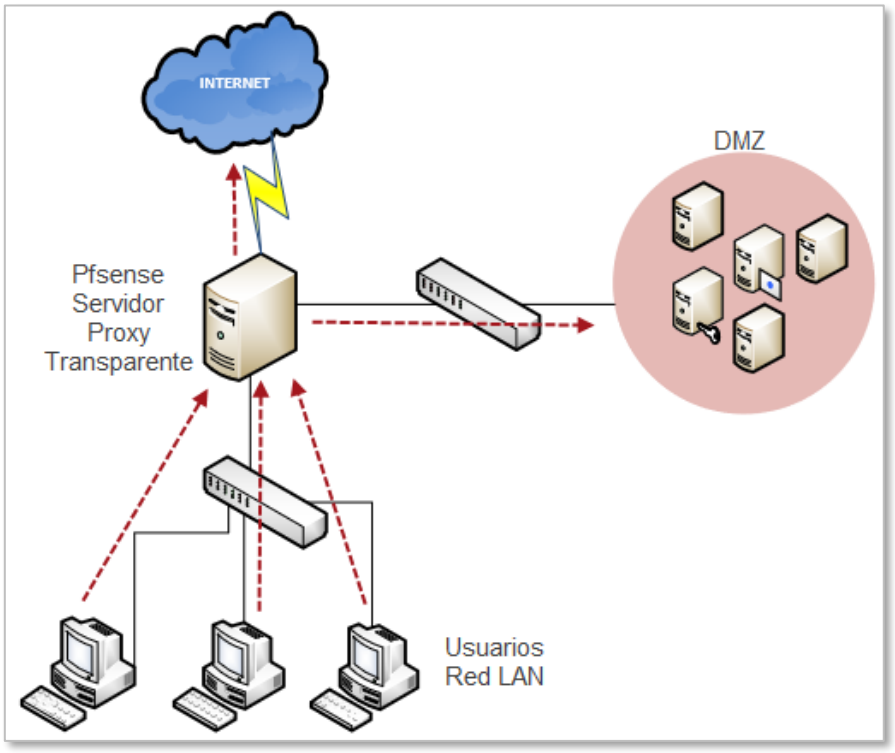


Figura 40. Servidor proxy protegiendo usuarios locales

Fuente: Adaptado de (Cengace learning, 2010)

Un servidor Proxy controla el tráfico en distintos modos y para efectos de este proyecto, se mencionan a los del tipo transparente y no transparente.

El Servidor Proxy en modo No Transparente es aquel en el cual los hosts internos conocen la existencia del servidor proxy y se requiere colocar el puerto 3128 en los hosts clientes, mientras que un servidor proxy en modo Transparente es aquel que cuando un host realiza peticiones hacia Internet no requiere que se configure a los hosts con el puerto 3128, lo realiza automáticamente, la desventaja es que no permite detectar tráfico HTTPS.

El Proxy no viene integrado a Pfsense, por lo que el paquete Squid Proxy debe ser descargado. Adicionalmente, se instalan los paquetes SquidGuard Proxy y LightSquid Proxy, el primero se encarga de filtrar contenido categorizado a través de las denominadas listas negras y blancas donde se introducen URLs o sitios web hacia los cuales se permiten o no las peticiones de los clientes, mientras que el segundo es un paquete que facilita el monitoreo de los accesos de los clientes a través del servidor proxy, presenta registros diarios, semanales y mensuales.

Estos tres paquetes operan simultáneamente y mejoran la gestión del Proxy. En la Figura 41 se puede apreciar al servidor Proxy en operación, donde se observa que una vez que los usuarios inicien sesión en el Portal Cautivo, se les permitirá o denegará el acceso a determinados sitios en Internet.

Squid Access Table

Squid - Access Logs

Fecha	J	Estado	Dirección	Usuario	Destino
17.07.2019 00:25:28	192.168.1.52	TCP_TUNNEL/200	www.salud.gob.ec:443	mguajan	190.152.52.202
17.07.2019 00:25:28	192.168.1.52	TCP_TUNNEL/200	www.presidencia.gob.ec:443	mguajan	190.152.52.202
17.07.2019 00:25:07	192.168.1.52	TCP_TUNNEL/200	sgrdacaa.msp.gob.ec:443	mguajan	181.112.138.227
17.07.2019 00:25:07	192.168.1.52	TCP_TUNNEL/200	sgrdacaa.msp.gob.ec:443	mguajan	181.112.138.227
17.07.2019 00:25:07	192.168.1.52	TCP_TUNNEL/200	sgrdacaa.msp.gob.ec:443	mguajan	181.112.138.227
17.07.2019 00:25:07	192.168.1.52	TCP_TUNNEL/200	sgrdacaa.msp.gob.ec:443	mguajan	181.112.138.227
17.07.2019 00:25:07	192.168.1.52	TCP_TUNNEL/200	sgrdacaa.msp.gob.ec:443	mguajan	181.112.138.227
17.07.2019 00:25:07	192.168.1.52	TCP_TUNNEL/200	sgrdacaa.msp.gob.ec:443	mguajan	181.112.138.227
17.07.2019 00:22:47	192.168.1.52	TCP_MISS/400	http://instagram.com/favicon.ico	mguajan	192.168.10.1
17.07.2019 00:22:47	192.168.1.52	TCP_MISS/400	http://instagram.com/	mguajan	192.168.10.1

Figura 41. Monitoreo de tráfico de usuarios

Fuente: Captura de pantalla Pfsense

Cuando las solicitudes de los usuarios sean analizadas por el Proxy, según las políticas establecidas, los navegadores web visitados mostrarán mensajes que informan que no se puede establecer conexión con algún sitio solicitado. La Figura 42 indica el resultado que se obtiene al intentar acceder a un sitio Web no permitido por el servidor.

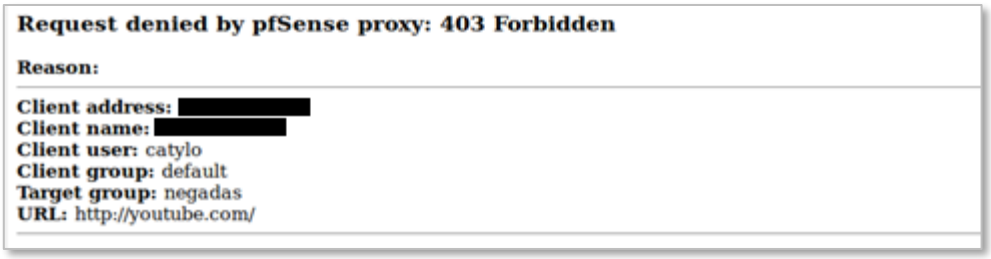


Figura 42. Acceso denegado por servidor Proxy para un host interno

Fuente: Captura de pantalla usuario Windows

Nota: La información acerca de la implementación y configuración del servidor Proxy en Pfsense se amplía en el Anexo I al final del documento.

4.4.7.1.9 Servidor Radius.

Mediante la implementación de un servidor Radius gestionado desde Pfsense se suplirán los artículos 36, 37,38 y 39 respectivamente de la Política de Seguridad de la Información.

- **Radius**: (Servicio de usuario de marcación de autenticación remota) es un protocolo ampliamente utilizado en entornos de red, facilita una administración centralizada de la información de autenticación de usuarios y ofrece un nivel de protección contra atacantes y espías. RADIUS es actualmente el estándar de facto para la autenticación remota.

Según (Rigney, Rubens, Simpson, & Willens, 1997) indican, RADIUS maneja un esquema cliente-servidor que opera como se explica:

- Cuando un cliente, en este caso NAS[13] está configurado para usar el protocolo RADIUS se espera que los usuarios presenten sus solicitudes de inicio de sesión.
- El NAS se autentica con el servidor RADIUS enviando un mensaje “Access-Request” que contiene atributos como el nombre y contraseña del usuario, así

[13] Servidor de acceso a la red

como el ID[14] del cliente y el puerto al que accede y si existe una contraseña de por medio se oculta usando un algoritmo de encriptación.

- El mensaje “Acess-Request” se entrega al servidor RADIUS y es enviado varias veces hasta obtener una respuesta.
- Cuando el servidor RADIUS reciba el “Acess-Request”, valida al NAS por medio de la llave secreta compartida.
- El servidor RADIUS consulta en una base de datos de usuarios para saber si coincide con la información de la solicitud, verificando requisitos para validar al usuario.
- Si no existen coincidencias, el servidor RADIUS responde con el mensaje “Access-Reject”.
- Si las condiciones son válidas, el servidor RADIUS responde con un “Access-Challenge”, un desafío al cual debe responder el usuario.
- El NAS responde al desafío volviendo a enviar el “Access-Request” original del usuario.
- El servidor RADIUS responde a la solicitud con un “Access-Permit”, “Access-Reject” o un nuevo “Access-Challenge”.
- Si todas las condiciones se cumplen, se emite la respuesta “Access-Accept” y un conjunto de valores de configuración del usuario.

Varios mecanismos de autenticación de usuarios son admitidos por el protocolo RADIUS cuando éste recibe la información proporcionada por el usuario, estos son: PPP[15], PAP[16], CHAP[17], etc.

[14] Identificador
[15] Protocolo punto a punto
[16] Protocolo de autenticación de contraseña
[17] Protocolo de autenticación por desafío mutuo

En el presente proyecto se utiliza Pfsense para la implementación de un servidor RADIUS debido a que permite una gestión centralizada de usuarios en la red, no consume demasiados recursos del sistema, es fácil de administrar si se tienen grandes cantidades de usuarios y no existe la necesidad de crear un servidor RADIUS externo.

En este escenario (Figura 43), el servidor RADIUS es el servidor de autenticación, mientras que el NAS es o son los puntos de acceso inalámbricos. Este mecanismo se utilizará para autenticar usuarios de la red inalámbrica, en específico, de la Vlan WLAN.

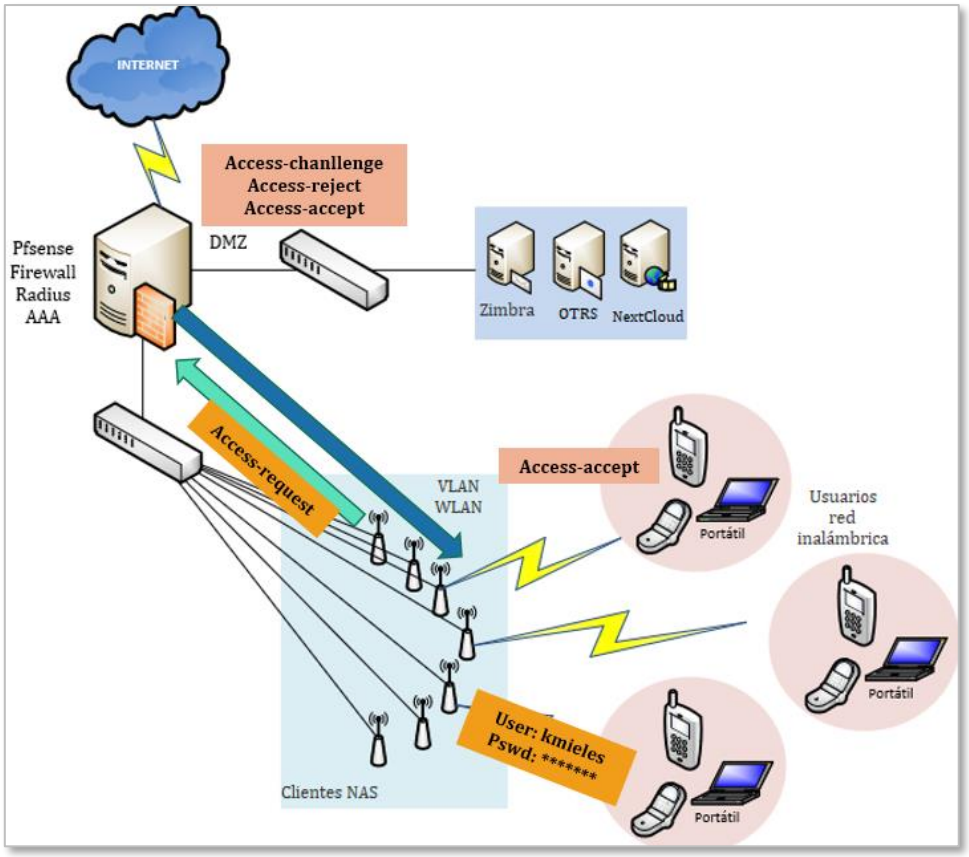


Figura 43. Funcionamiento del servidor RADIUS en Pfsense

Fuente: Autoría propia

El procedimiento de implementación del servidor RADIUS en Pfsense consta de:

- Descarga del paquete Freeradius3.
- Configuración de las interfaces de escucha para el servidor Radius.

- Adición y configuración del cliente NAS, donde se establece la clave secreta compartida con el servidor RADIUS.
- Creación y configuración de cuentas de usuarios y sus credenciales de acceso.
- Configuración de dispositivos que actuarán como clientes y asociarlos con el servidor RADIUS.
- Comprobar la autenticación de usuarios a la red.

En la Figura 44 capturada desde un dispositivo móvil que simula a un usuario, es posible verificar que se muestra información de una solicitud de acceso, se introducen las credenciales de autenticación del usuario “kmieles” para ser autenticado y así el servidor RADIUS conceda el permiso para acceder a los recursos de la red.

Figura 44. Autenticación de usuario en servidor RADIUS

Fuente: Captura de pantalla usuario Android

En la Figura 44 se observa que el método de autenticación utilizado el PEAP el cual es un Protocolo de Autenticación Extensible Protegido que tiene sus ventajas en

comparación a otros métodos de autenticación, donde la autenticación se efectúa en un túnel TLS, es decir que está cifrado en ambos extremos, la identidad de los usuarios se asegura y no requiere la creación de certificados por cliente sino solo en el servidor (Vallejos, 2019, págs. 29-31).

Desde Pfsense se verifica la autenticación del usuario ingresando al menú Servicios – Registros del Sistema como lo indica la Figura 45.

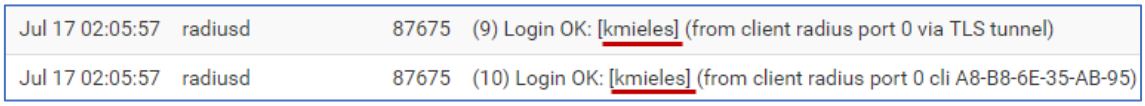
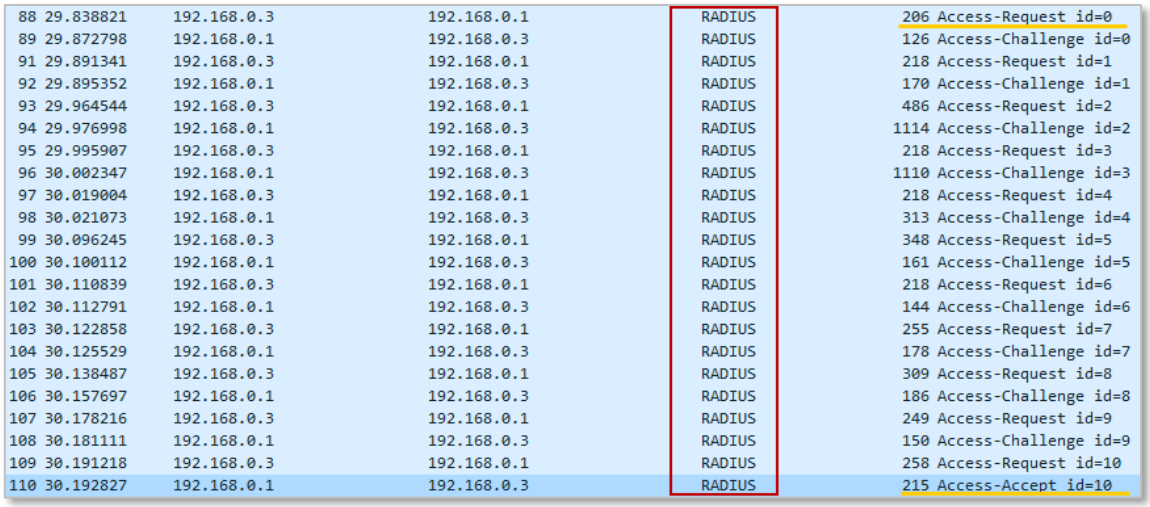


Figura 45. Verificación de autenticación de usuario en servidor Radius

Fuente: Captura de pantalla Pfsense

Adicionalmente se realiza una captura de paquetes con el software Wireshark[18] (Figura 46) para consolidar la negociación entre el cliente NAS y el servidor RADIUS para la autenticación de usuarios.



88	29.838821	192.168.0.3	192.168.0.1	RADIUS	206 Access-Request id=0
89	29.872798	192.168.0.1	192.168.0.3	RADIUS	126 Access-Challenge id=0
91	29.891341	192.168.0.3	192.168.0.1	RADIUS	218 Access-Request id=1
92	29.895352	192.168.0.1	192.168.0.3	RADIUS	170 Access-Challenge id=1
93	29.964544	192.168.0.3	192.168.0.1	RADIUS	486 Access-Request id=2
94	29.976998	192.168.0.1	192.168.0.3	RADIUS	1114 Access-Challenge id=2
95	29.995907	192.168.0.3	192.168.0.1	RADIUS	218 Access-Request id=3
96	30.002347	192.168.0.1	192.168.0.3	RADIUS	1110 Access-Challenge id=3
97	30.019004	192.168.0.3	192.168.0.1	RADIUS	218 Access-Request id=4
98	30.021073	192.168.0.1	192.168.0.3	RADIUS	313 Access-Challenge id=4
99	30.096245	192.168.0.3	192.168.0.1	RADIUS	348 Access-Request id=5
100	30.100112	192.168.0.1	192.168.0.3	RADIUS	161 Access-Challenge id=5
101	30.110839	192.168.0.3	192.168.0.1	RADIUS	218 Access-Request id=6
102	30.112791	192.168.0.1	192.168.0.3	RADIUS	144 Access-Challenge id=6
103	30.122858	192.168.0.3	192.168.0.1	RADIUS	255 Access-Request id=7
104	30.125529	192.168.0.1	192.168.0.3	RADIUS	178 Access-Challenge id=7
105	30.138487	192.168.0.3	192.168.0.1	RADIUS	309 Access-Request id=8
106	30.157697	192.168.0.1	192.168.0.3	RADIUS	186 Access-Challenge id=8
107	30.178216	192.168.0.3	192.168.0.1	RADIUS	249 Access-Request id=9
108	30.181111	192.168.0.1	192.168.0.3	RADIUS	150 Access-Challenge id=9
109	30.191218	192.168.0.3	192.168.0.1	RADIUS	258 Access-Request id=10
110	30.192827	192.168.0.1	192.168.0.3	RADIUS	215 Access-Accept id=10

Figura 46. Captura de paquetes protocolo Radius

Fuente: Captura de pantalla Wireshark

Nota: La información acerca de la implementación del servidor RADIUS en Pfsense se amplía en el Anexo I al final del documento.

[18] Analizador de protocolos de red

4.4.8 Sección VII – Control de acceso

4.4.8.1 Creación de Vlans.

Las Vlans se crean con el propósito de segmentar la red plana existente para colocar en cada uno de ellos a los dispositivos y usuarios según sus funciones, con esta medida será posible dar cumplimiento a los artículos 43, 44, 45 y 46 de la Política de Seguridad de la Información.

- **Vlan:** Son un grupo de dispositivos situados en diferentes redes de área local que tienen la capacidad de comunicarse entre sí en una misma red o con dispositivos de otras redes como si todos estuvieran en la misma LAN física. Las Vlan pueden basarse en direcciones MAC, direcciones IP, puertos, protocolos o una combinación de estos aspectos.

En la Tabla 51 se discuten algunos beneficios de las Vlan.

Tabla 51. Beneficios de las Vlan

Aspecto	Descripción
Escalabilidad	Capacidad de agregar, mover y cambiar redes simplemente configurando los puertos de los conmutadores y asignando clientes a diferentes Vlan.
Seguridad	Mayor control de los puertos de los conmutadores y de los dispositivos que tienen permitido conectarse, restringen el tráfico sensible originado en un departamento empresarial.
Ahorro de costos	Se reducen los costos de expansión de las redes, eliminando la necesidad de equipos, cables o enrutadores adicionales.
Eficiencia	Capacidad de utilizar mejor el ancho de banda y recursos.
Facilidad de solucionar problemas	Facilidad de observar las actividades de las Vlan. Por lo tanto, los problemas de red se pueden rastrear, identificar y rectificar con facilidad.
Integridad	Los segmentos lógicos dividen un conmutador físico y separa hosts que no deben acceder entre sí. Esto asegura que los datos no se vean comprometidos cuando se manejan.
Grupos de trabajo virtuales	Permite la creación de grupos de trabajo virtuales que ayudan a disminuir el tráfico de la red.

Fuente: Adaptado de (Mehdizadeha & Suinggi, 2017)

Una de las características de Pfsense es que admite la creación de Vlans. Se decide por la implementación de Vlans en la red de datos del HSLO debido a que existe un único segmento LAN, lo cual significa que todos los dispositivos comparten el ancho de banda disponible y como consecuencia de esto, es posible que se generen colisiones cuando tratan de comunicarse al mismo tiempo. Por lo tanto, por medio de la implementación de Vlans, un único dominio de colisión se divide en dominios de colisión más pequeños y de esta manera se optimiza el uso del ancho de banda ya que permite dedicarlo a cada segmento de red.

En la Figura 47 se muestran las Vlan creadas en Pfsense, para lo cual se han organizado grupos tanto para el personal según sus funciones y para el conjunto de dispositivos conectados a la red de datos: WLAN, doctores, administrativos, impresoras, invitados, provisional, gerentes y TIC; las Vlans creadas pueden ser observadas directamente desde la consola de Pfsense.

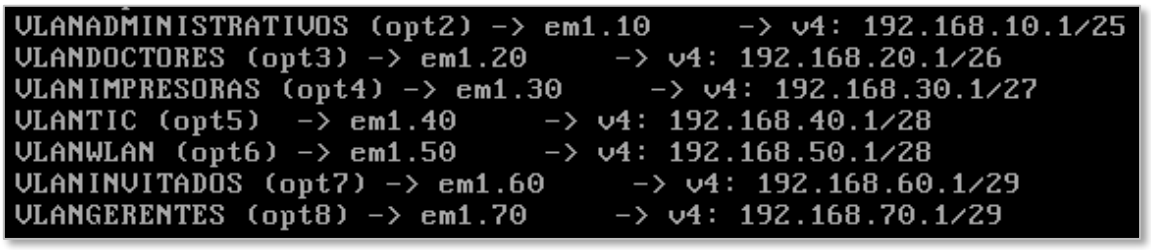


Figura 47. Vlans creadas en Pfsense

Fuente: Captura de pantalla Pfsense

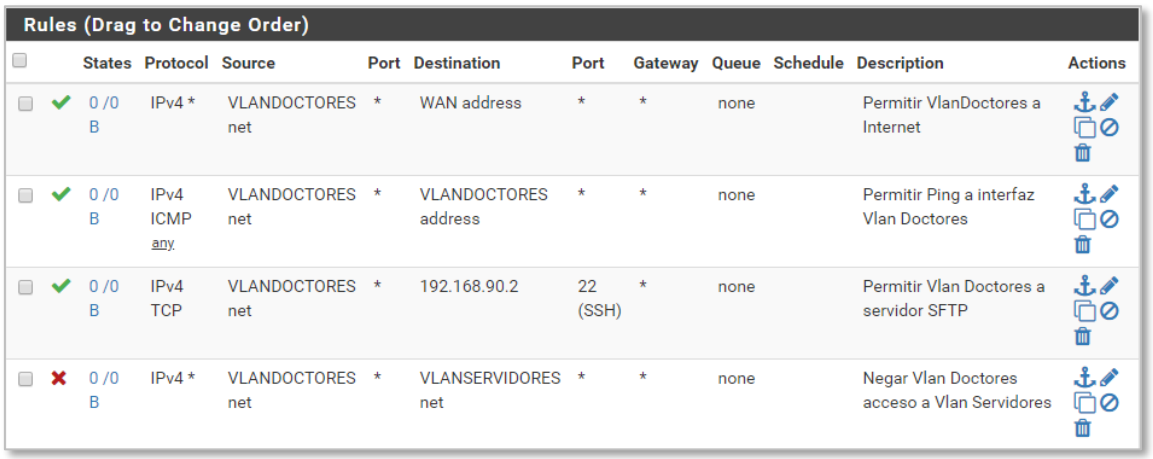
Adicionalmente, se considera la condición en la que se encontraba el servidor FTP[19] en el caso de no existir segmentos lógicos de red, donde cualquier usuario podía establecer una conexión con él. Este servidor es únicamente dedicado para el almacenamiento de información de Imagenología o Rayos X, es decir, información confidencial de los pacientes. Para elevar la seguridad del servidor se establece una regla

[19] Protocolo de transferencia de archivos

que habilite el paso de este tráfico solamente a la Vlan Doctores, mientras que a los usuarios de las demás Vlans se les limita estos permisos.

Desde la configuración de reglas del firewall en Pfsense, se crea una regla que bloquee el acceso al servidor SFTP[20] a los segmentos que no pertenezcan a la Vlan Doctores, en la Figura 48 se crea y aplica esta regla a esta Vlan.

La interfaz desde la cual los paquetes coincidirán con la regla es la interfaz de la Vlan Doctores, de igual manera coincidirá con cualquier protocolo en la versión IPv4, la interfaz y puerto de origen configurado es la red de la Vlan Doctores, debido a que coincidirá con cualquier paquete proveniente de ella, mientras que en el destino se coloca la dirección IP del servidor SFTP.



Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓	0 /0 B	IPv4 *	VLANDOCTORES net	*	WAN address	*	*	none		Permitir VlanDoctores a Internet	
✓	0 /0 B	IPv4 ICMP any	VLANDOCTORES net	*	VLANDOCTORES address	*	*	none		Permitir Ping a interfaz Vlan Doctores	
✓	0 /0 B	IPv4 TCP	VLANDOCTORES net	*	192.168.90.2	22 (SSH)	*	none		Permitir Vlan Doctores a servidor SFTP	
✗	0 /0 B	IPv4 *	VLANDOCTORES net	*	VLANSERVIDORES net	*	*	none		Negar Vlan Doctores acceso a Vlan Servidores	

Figura 48. Regla de restricción de acceso al servidor SFTP

Fuente: Captura de pantalla Pfsense

Nota: Es muy importante tomar en cuenta el orden en el que se configuran las reglas, las coincidencias se efectúan desde arriba hacia abajo.

[20] Protocolo seguro de transferencia de archivos

Una vez aplicada la regla se comprueba mediante un ping que solamente desde cualquier host ubicado en la Vlan Doctores (Figura 49) será posible acceder al servidor SFTP.

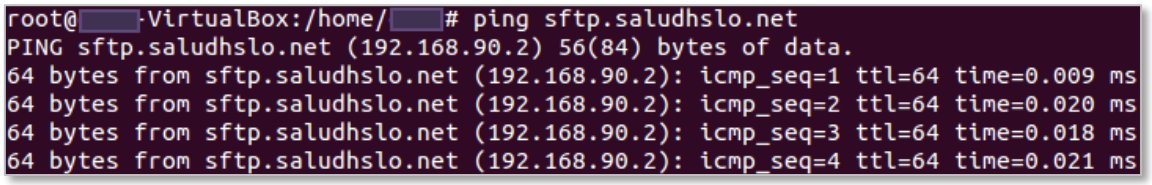


Figura 49. Ping desde un host de la Vlan doctores hacia servidor SFTP

Fuente: Captura de pantalla usuario Linux Mint

Nota: La información acerca de la implementación de Vlan en Pfsense se amplía en el Anexo I al final del documento.

4.4.9 Sección VIII: Gestión de la Continuidad del Negocio

Esta sección resalta la importancia de realizar un Análisis de Gestión de Riesgos, proceso que a inicios del desarrollo del presente proyecto se realizó, sin embargo, esta actividad debe actualizarse continuamente para el descubrimiento de nuevas amenazas de riesgo, con esta medida se cumplirá con los artículos 51 y 52 de la Política de Seguridad de la Información. El procedimiento a seguir se indica en la (Tabla 52) y en el diagrama de flujo (Figura 50).

Tabla 52. Procedimiento de Evaluación de Riesgos de la Seguridad de la Información

Ministerio de Salud Pública	
HOSPITAL SAN LUIS DE OTAVALO – DISTRITO 10D02	
SECCIÓN VIII – GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	
Procedimiento:	Proceso para realizar la Evaluación de Riesgos de la Seguridad de la Información

Objetivo:	Describir las actividades a seguir para desarrollar la Evaluación de Riesgos de la Seguridad de la Información
Alcance:	Activos de información (hardware y software) e información electrónica
Responsables:	• Comité de Seguridad de la Información (C.S.I) • Responsable de S.I del área de TIC

ACTIVIDAD	**DESCRIPCIÓN**
	Inicio de procedimiento
1	Los responsables del proceso tienen a su alcance la norma NTE INEN-ISO/IEC 27005:2012 para informarse acerca del procedimiento de Evaluación de Riesgos.
2	Los responsables del proceso inicialmente identifican todos los activos de información de la Institución.
3	Los responsables del proceso realizan la valoración de los activos de información donde identifica los activos críticos.
4	Los responsables del proceso identifican los principales riesgos de los activos de información derivados de las amenazas y vulnerabilidades.
5	Los responsables del proceso valoran los riesgos de los activos de información que dan como resultado en la Matriz de Riesgos.
6	Los responsables del proceso una vez evaluados los riesgos determinan el tratamiento que recibirán para reducir, mitigar o eliminarlos.
Condición ¿La Política de S.I. requiere cambios?	Si la evaluación de riesgos desencadena un conjunto de nuevas prácticas a realizarse y por ende, la Política de S.I necesita cambios, se procede con la actividad 7, caso contrario el proceso de Evaluación de Riesgos finaliza.
7	Los responsables del proceso actualizan la Política de S.I con los parámetros necesarios.
Condición ¿La implementación de la Política necesita recursos?	Si para implementar las nuevas directrices de la Política de S.I y reducir los riesgos encontrados se necesitan de recursos económicos proseguir con la actividad 8, caso contrario con la actividad 9.

8	Los responsables del proceso realizan un análisis Costo/Beneficio.
9	Los responsables del proceso implementan las políticas propuestas.
	Fin del procedimiento.

CONSTANCIAS
Realizado por:
…… Catherine López ESTUDIANTE UTN
Revisado y aprobado por:
…… Manuel Guaján INFORMÁTICO HSLO

Fuente: Autoría propia

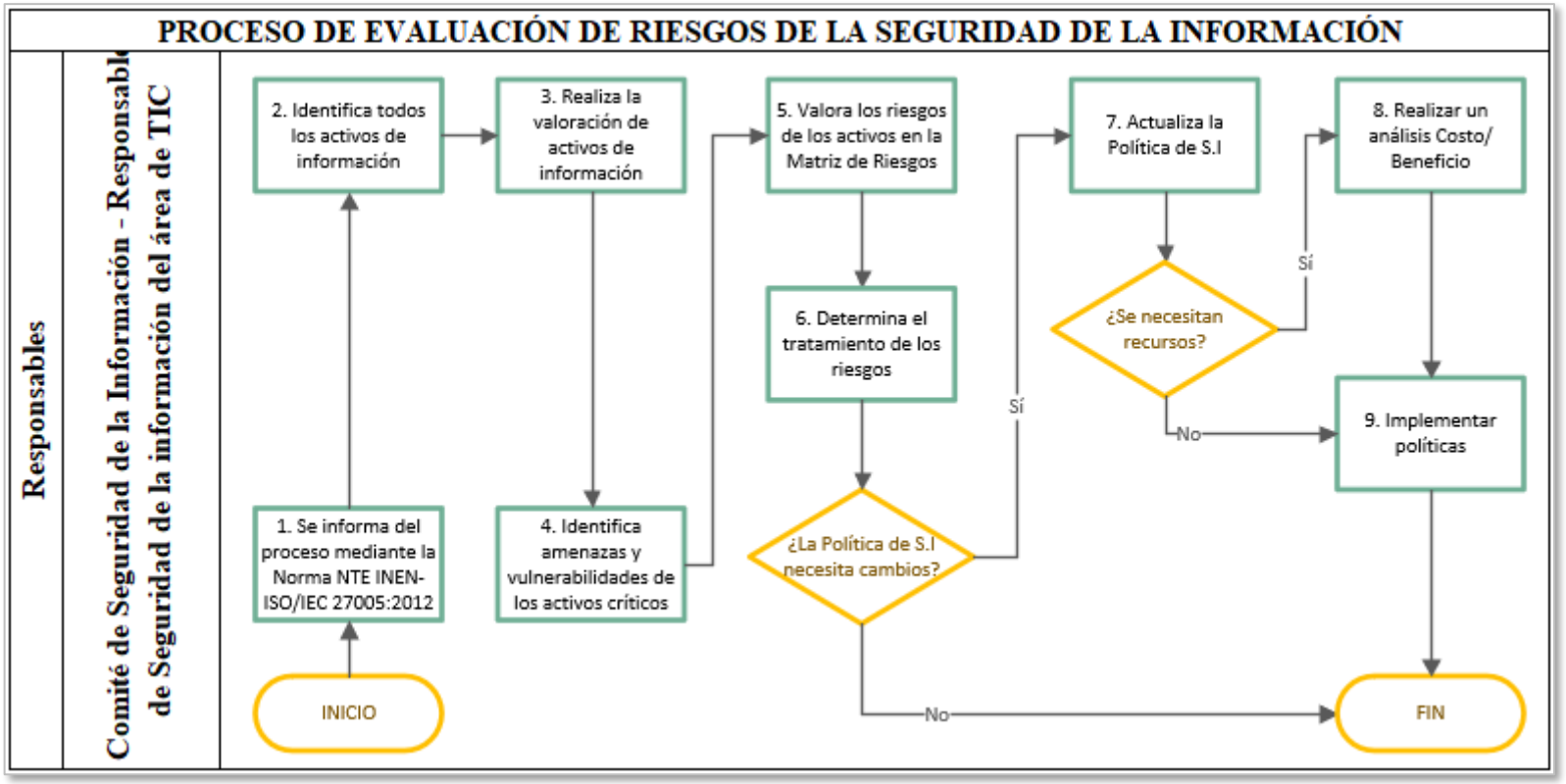


Figura 50. Diagrama de flujo del procedimiento de Evaluación de Riesgos de la Seguridad de la Información

Fuente: Autoría propia

4.4.9 Sección IX: Cumplimiento

Dentro de esta sección que trata acerca del cumplimiento de reglamentaciones impuestas por el Estado o por la autoridad sanitaria nacional MSP, no está de más recordar que para evitar uno de los gastos en la compra de licencias para sistemas operativos propietario, la Institución se encuentra en toda su libertad de acatar con las disposiciones del Decreto Ejecutivo N° 1014 e implementar software libre como sistema operativo en los equipos de la Institución, esta es una recomendación explicada en el artículo 53 de la Política de Seguridad de la Información. La Tabla 53 expone un conjunto de procedimientos a seguir para efectuar esta actividad y en la Figura 51 un diagrama de flujo respectivo.

Tabla 53. Procedimiento de uso de software propietario sin licencia

Ministerio de Salud Pública

HOSPITAL SAN LUIS DE OTAVALO – DISTRITO 10D02

SECCIÓN IX – CUMPLIMIENTO	
Procedimiento:	Procedimiento de uso de software propietario sin licencia
Objetivo:	Describir las actividades a seguir para la adquisición de licencias de software propietario o migración a sistema operativo gratuito.
Alcance:	Se aplica para los computadores y/o servidores con software propietario instalado.
Responsables:	• Comité de Seguridad de la Información (C.S.I) • Responsable de S.I del área de TIC • Responsable de oficina Administrativo-Financiero
ACTIVIDAD	**DESCRIPCIÓN**
	Inicio de procedimiento

1	El C.S.I delega a Responsable de S.I del área de TIC identificar la cantidad de equipos con software propietario sin licencia
2	El Responsable de S.I del área de TIC identifica en inventario de activos los equipos sin licencia.
3	El Responsable de S.I del área de TIC elabora una cotización de precios para la adquisición de licencias.
4	El Responsable de S.I del área de TIC presenta cotización a oficina de Administrativo-Financiero.
Condición ¿Hay recursos para la compra de licencias?	Si existen recursos destinados para la adquisición de licencias proseguir con la actividad 5, caso contrario con la actividad 7.
5	Si existen los recursos para la compra, la oficina de Administrativo-Financiero gestiona la adquisición de las licencias
6	El Responsable de S.I del área de TIC instala el sistema operativo con la licencia respectiva, continúa con la actividad 9.
7	Si no existen recursos disponibles para la compra de licencias, el Responsable de S.I del área de TIC inicia proceso de transición de software propietario a software libre en los equipos.
8	El Responsable de S.I del área de TIC capacita a los funcionarios acerca del uso del nuevo sistema operativo.
9	El Responsable de S.I del área de TIC documenta los procesos realizados.
	Fin del procedimiento.

CONSTANCIAS

Realizado por:

…….

Catherine López

ESTUDIANTE UTN

Revisado y aprobado

por:

…….

Manuel Guaján

INFORMÁTICO HSLO

Fuente: Autoría propia

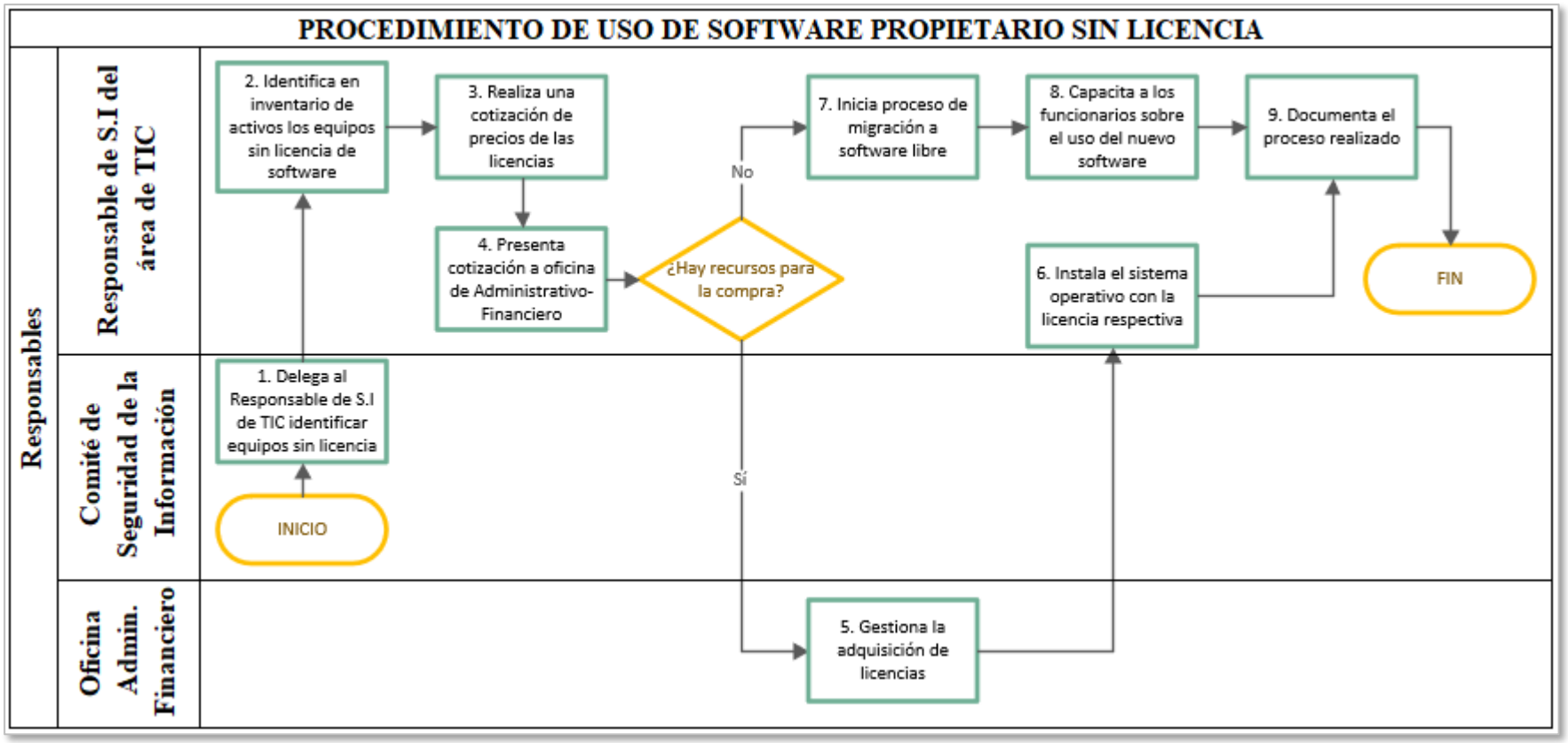


Figura 51. Procedimiento de uso de software propietario sin licencia

Fuente: Autoría propia

Para cumplir con el artículo 54 de la política en la cual se sugiere encontrar las maneras y los medios respectivos para asegurar la disponibilidad de la información, puede efectuarse bien sea con el respaldo de información en servidores de archivos o en dispositivos de almacenamiento externo, esta última opción se discute en el Anexo J al final del documento. Para culminar con la implementación de políticas, los manuales desarrollados serán entregados al Responsable de la Seguridad del área de TIC.

4.5 Análisis de los servicios implementados en Pfsense en el entorno real.

No todos los servicios pudieron implementarse en la actual red de datos de la Institución por los siguientes motivos:

- El estado del cableado estructurado no está debidamente organizado, por lo cual se requiere una reestructuración del mismo y evitar inconvenientes en la puesta en marcha de los servicios.
- El Firewall Pfsense está implementado en un computador, con buenas características para operar como un ordenador, sin embargo, un firewall debe ser un dispositivo creado específicamente para dichos fines, por lo que si se implementasen todos los servicios en el computador actual, podría llegar a disminuir el rendimiento de la red.

En el entorno real se implementó un Servidor Proxy en modo Transparente, Portal Cautivo y VPN en Pfsense para dar cumplimiento a políticas y necesidades internas, estos servicios actualmente operativos permitirán analizar el nivel de rendimiento del equipo.

La actividad del sistema de Pfsense se puede monitorear desde la consola la cual arroja información cada segundo acerca del uso de la memoria, procesos, subprocesos, tiempos de ejecución y todo aquello que consume recursos del CPU.

La ecuación 1 permite obtener el valor del consumo máximo del CPU medido en porcentajes (Solano, 2017), la cual se utilizará para cada resultado obtenido.

%CPU=%user+%system+%interrupt [%] (Ec. 1)

Cabe mencionar que Pfsense utiliza el Mebibyte como unidad de medida de los datos de almacenamiento de la memoria RAM y swap. La equivalencia es 1 MiB = 1.04858 MB.

Al introducir el comando top se obtuvieron los siguientes datos de las Figuras 52, 53 y 54 respectivamente.

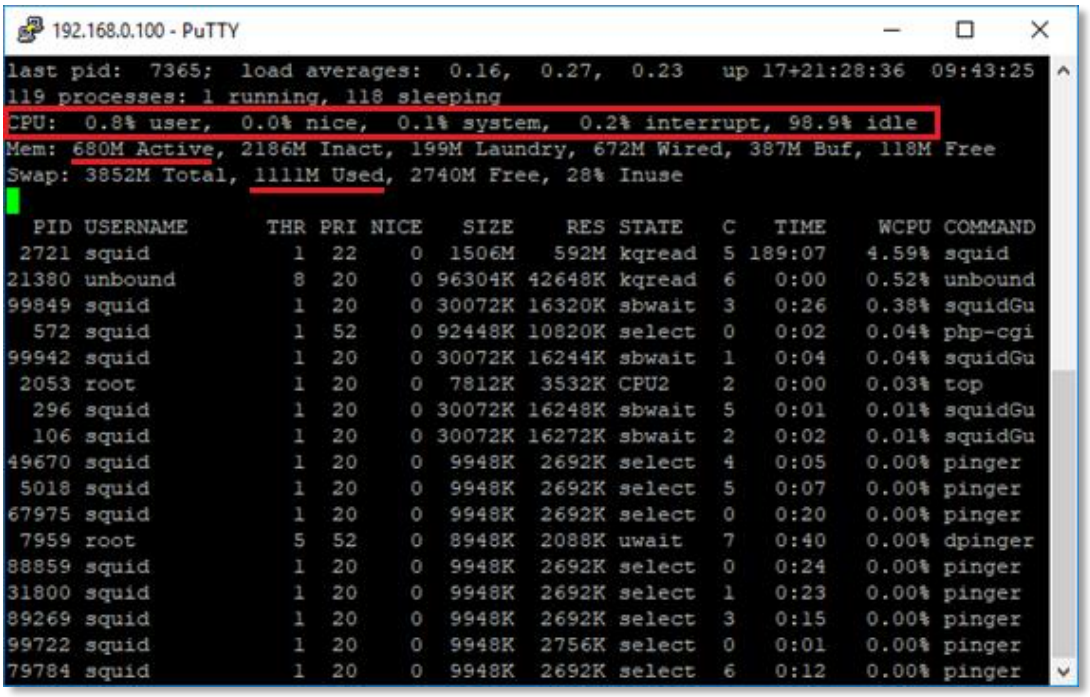


Figura 52. Captura 1: Actividad del sistema Pfsense-entorno real

Fuente: Captura de pantalla Pfsense

Consumo de CPU:

- %CPU= 0.8%+0.1%+0.2% =1.1%

Consumo de memoria RAM:

- 680 MiB = 713 MB

Consumo de memoria SWAP:

- 1111 MiB = 1165 MB

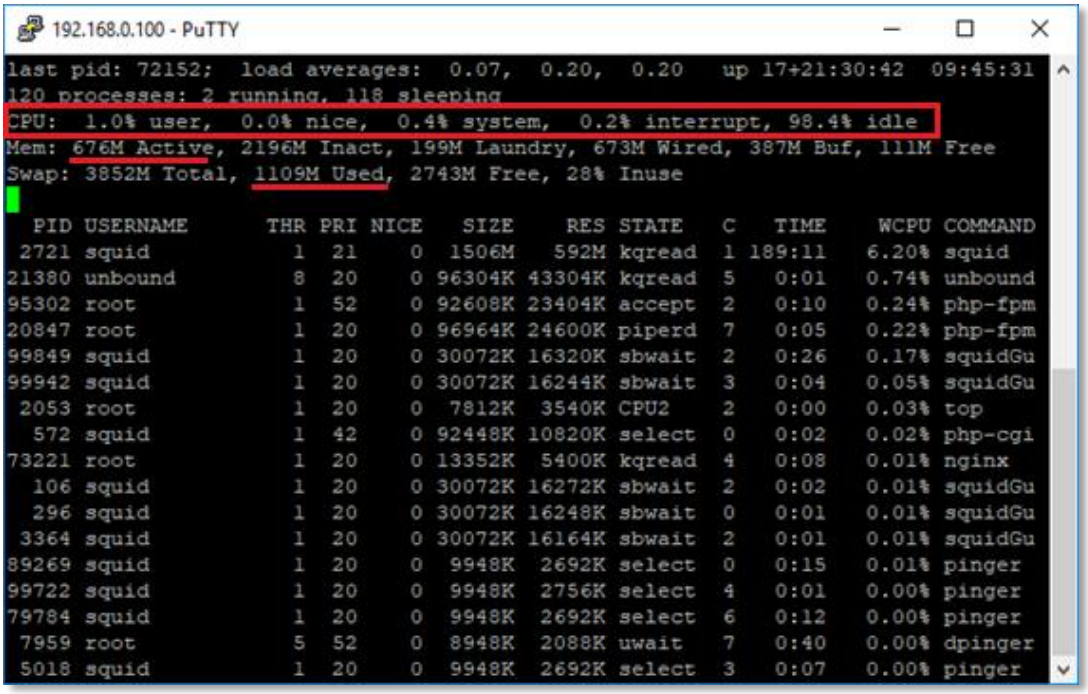


Figura 53. Captura 2: Actividad del sistema Pfsense-entorno real

Fuente: Captura de pantalla Pfsense

Consumo de CPU:

- %CPU= 1.0%+0.4%+0.2% =1.6%

Consumo de memoria RAM:

- 676 MiB = 709 MB

Consumo de memoria SWAP:

- 1109 MiB = 1163 MB

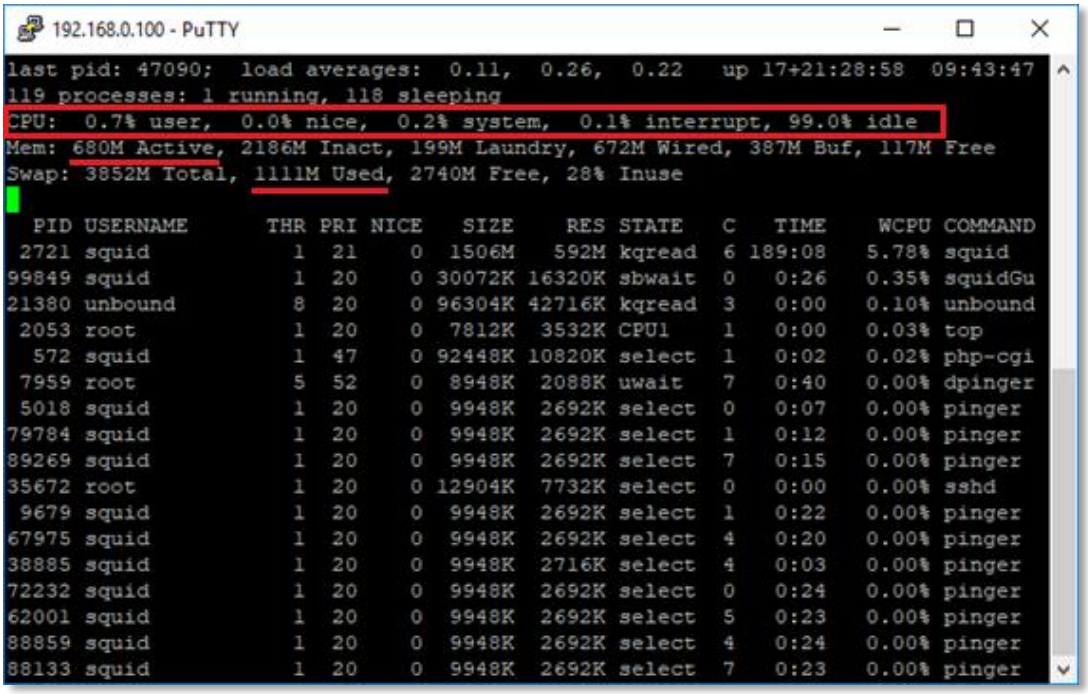


Figura 54. Captura 3: Actividad del sistema Pfsense-entorno real

Fuente: Captura de pantalla Pfsense

Consumo de CPU:

- %CPU= 0.7%+0.2%+0.1% =1%

Consumo de memoria RAM:

- 680 MiB = 713 MB

Consumo de memoria SWAP:

- 1111 MiB = 1165 MB

De los resultados anteriores se deduce lo siguiente:

- Con los servicios implementados, el consumo del CPU alcanza un aproximado de 1.23%.
- Los servicios implementados consumen 713 MB de la memoria RAM, constatando que más de la mitad de la memoria no se utiliza.
- El consumo de la memoria swap alcanza un poco más de 1 GB, esta indica el espacio usado para el intercambio de información del sistema.

- Los procesos de los servicios Squid y Squidguard consumen un promedio de 5.52% y 0.08% de la capacidad del CPU respectivamente, ejecutando tareas de análisis de tráfico entrante y saliente en una red donde existen aproximadamente 110 usuarios conectados a la red de datos y acceso a determinados sitios web en Internet, estos valores son relativamente bajos para la cantidad de usuarios activos que Pfsense gestiona.
- El consumo del CPU por el uso del Portal Cautivo y VPN no se indica debido a que es una tarea que se ejecuta en el momento de la autenticación de usuarios y no representa mayor diferencia en el rendimiento del equipo.

Nota: Esta información se obtuvo en horas laborables en la mañana donde el tráfico de la red es comúnmente más alto.

Adicionalmente, el tablero de Pfsense (Figura 55) reporta información del sistema similar a la obtenida desde la consola.

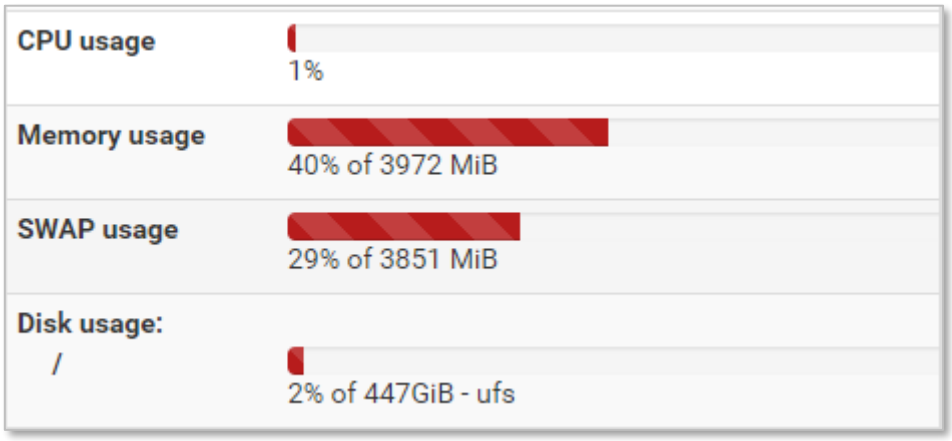


Figura 55. Reporte del estado del Sistema Pfsense-entorno real

Fuente: Captura de pantalla Pfsense

Pfsense permite además visualizar el estado del consumo del ancho de banda por interfaz, desde el menú Estado en la pestaña Gráfico de Tráfico se observa que, de los 15 Mbps del enlace entregado por el proveedor de Internet a la Institución, existen picos que

llegan hasta los 6 Mbps como lo indica la Figura 56 obtenida en horas de la tarde donde aún se reporta tráfico.

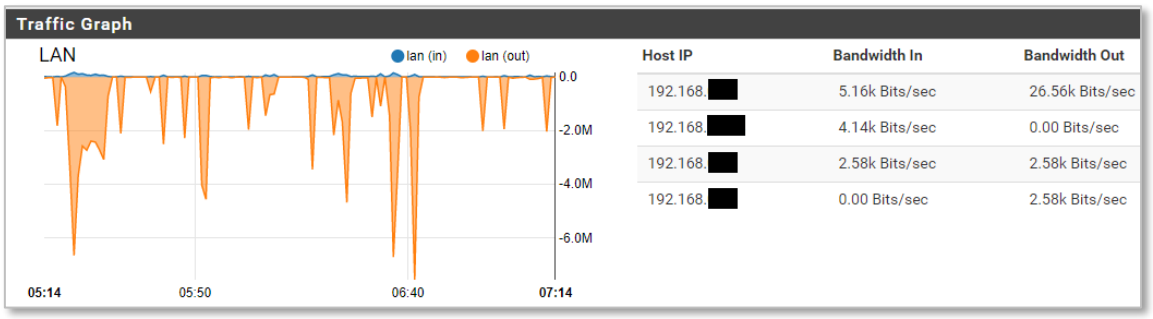


Figura 56. Ancho de banda de interfaz LAN- entorno real

Fuente: Captura Pfsense

Como se observa, la capacidad del enlace no ha llegado a saturarse por completo.

Del análisis anterior se puede concluir que el equipo en el que se encuentra implementado Pfsense cumple con las características necesarias para operar sin problemas con los servicios actuales, Pfsense no consume gran cantidad de recursos y los resultados del análisis son favorables en vista de que la velocidad de las dos interfaces de red es de 1 Gigabit Ethernet.

4.6 Análisis de los servicios simulados en Pfsense.

El rediseño de la red de datos del Hospital San Luis de Otavalo y los servicios anteriormente planteados son una propuesta que puede ser implementada a futuro. El equipo en el que se instale Pfsense deberá contar con las capacidades necesarias que eviten comprometer su rendimiento cuando se implementen los servicios: DNS, VPN, Proxy, Portal Cautivo y Radius.

En la simulación, se genera tráfico desde uno de los usuarios ubicados en la red interna para analizar el comportamiento de Pfsense con JMeter (Figura 57), es una herramienta de testing que permitirá simular la generación de peticiones a aplicaciones como HTTP, FTP, LDAP, etc. A partir de estas pruebas se obtendrá información referente

al estado del sistema de tal forma que se asemeje al entorno real. El escenario consiste en 140 usuarios que realizan peticiones al servicio de correo institucional Zimbra.

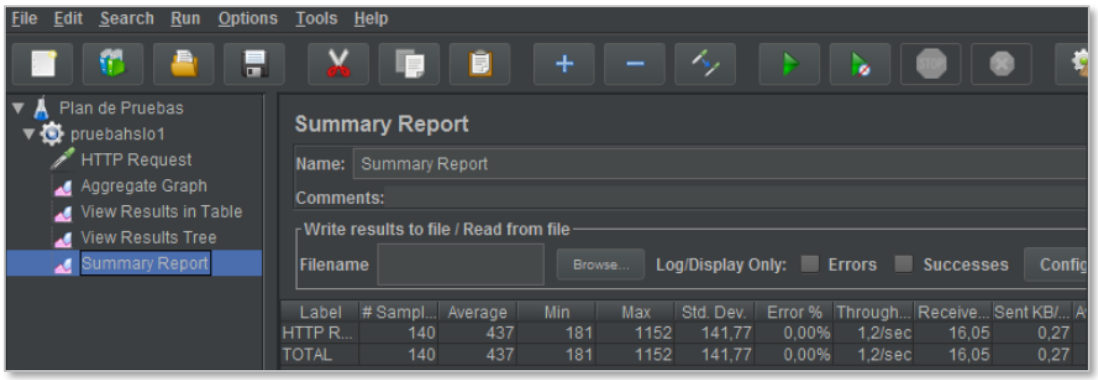


Figura 57. Peticiones de 140 usuarios realizadas en JMeter

Fuente: Captura JMeter

JMeter reporta que el tiempo promedio de respuesta de cada petición realizada fue de 0.437 segundos, que el servidor manejó 1.2 solicitudes por segundo (rendimiento), que se recibieron aproximadamente 16.05 Kb/s de información y se enviaron 0.27 Kb/s.

Con el tráfico generado y con todos los servicios activos, desde la consola de Pfsense con el comando top se observa el comportamiento del servidor, las Figuras 58, 59 y 60 devuelven los datos mostrados, calculando valores similares al proceso anterior.

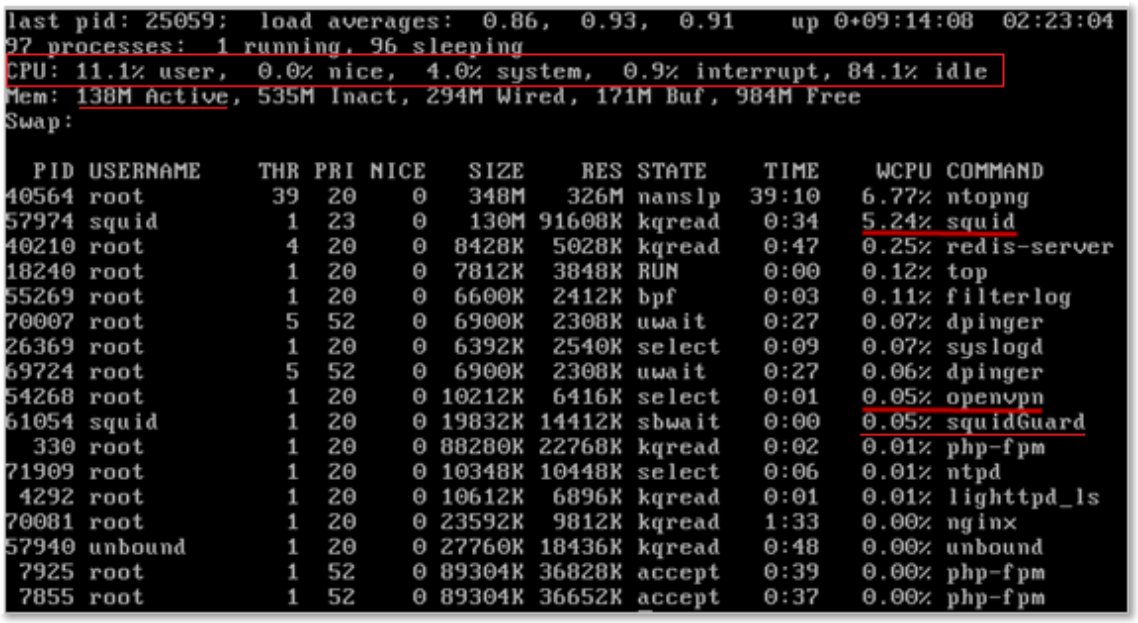


Figura 58. Captura 1: Actividad del sistema Pfsense – entorno de pruebas

Fuente: Captura Pfsense

Consumo del CPU:

- %CPU= 11.1%+4.0%+0.9% =16%

Consumo de memoria RAM:

- 132 MiB = 138 MB

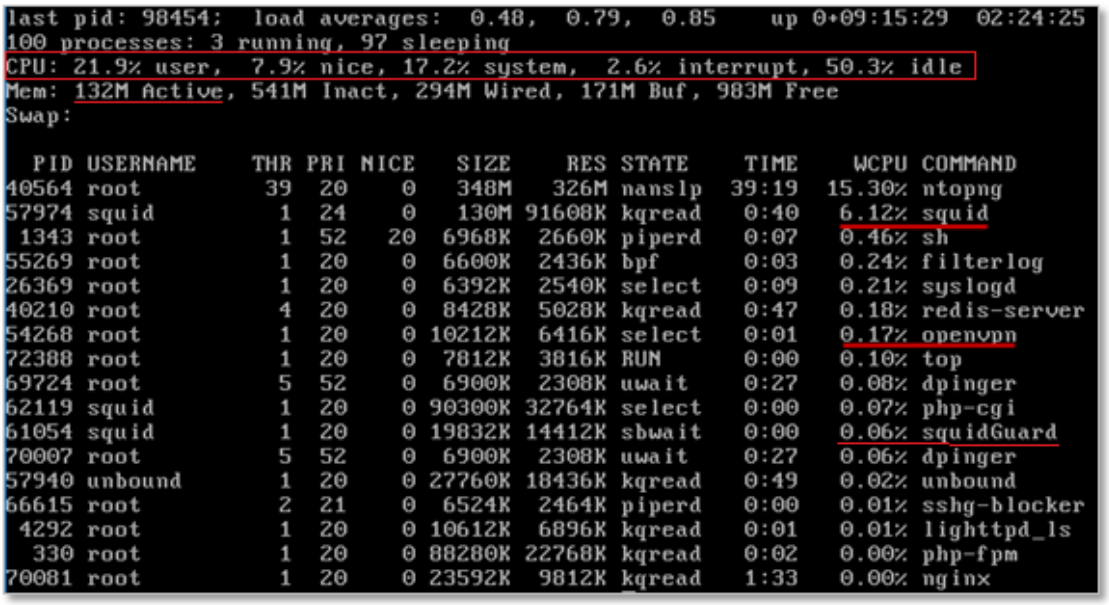


Figura 59. Captura 2: Actividad del sistema Pfsense – entorno de pruebas

Fuente: Captura Pfsense

Consumo del CPU:

- %CPU= 21.9%+17.2%+2.6% = 41.7%

Consumo de memoria RAM:

- 132 MiB = 138 MB

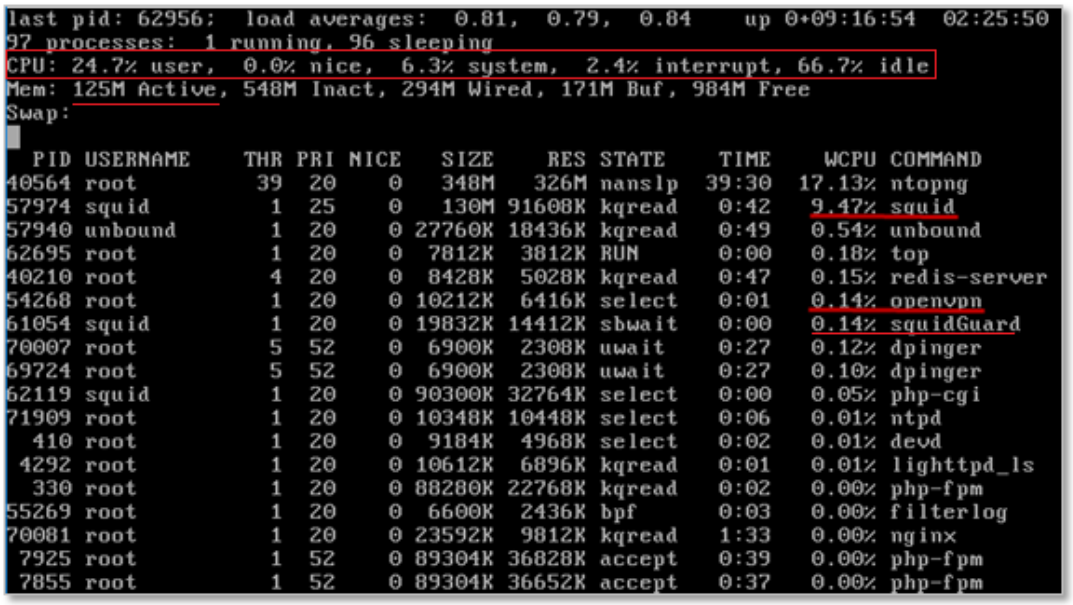


Figura 60. Captura 3: Actividad del sistema Pfsense – entorno de pruebas

Fuente: Captura Pfsense

Consumo del CPU:

- %CPU= 24.7%+6.3%+2.4% = 33.4%

Consumo de memoria RAM:

- 125 MiB = 132 MB

  De los resultados obtenidos se deduce lo siguiente:

- Con todos los servicios activos, el rendimiento del CPU llegó hasta un 41.7%.
- Se consume un promedio de 132 MB de memoria RAM están en uso y aún queda espacio disponible.
- Los procesos de los servicios que se pudieron visualizar: Squid, OpenVPN y SquidGuard consumieron un promedio de 6.94%, 0.12% y 0.08% respectivamente de la capacidad del CPU.
- El consumo del CPU por el uso del Portal Cautivo y Radius no se muestra debido a que es una tarea que se ejecuta en el momento de la autenticación de usuarios y no representa mayor diferencia en el rendimiento del equipo.

El tablero de Pfsense también reporta información del estado del sistema (Figura 61), similar a la obtenida desde la consola, donde se observa que, en efecto, el consumo del CPU incrementó.

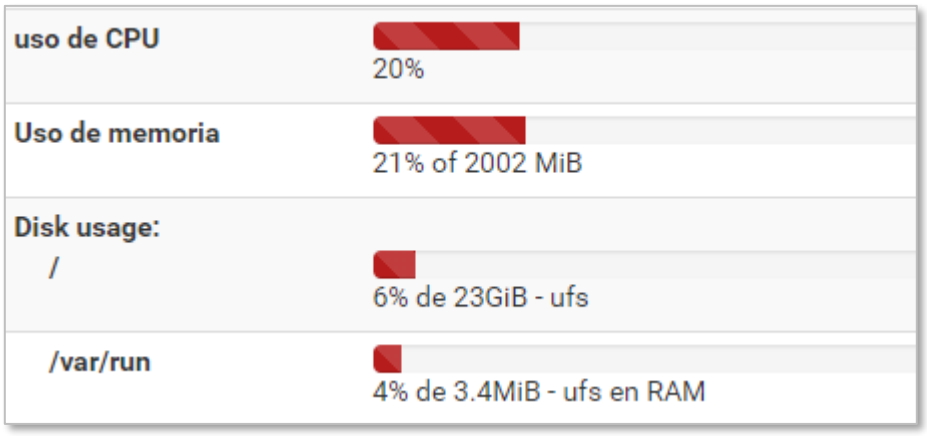


Figura 61. Reporte del sistema Pfsense-entorno de pruebas

Fuente: Captura Pfsense

Se visualiza el consumo del ancho de banda de la interfaz que corresponde a la Vlan Administrativos (Figura 62) y desde la cual se generaron las peticiones; en el menú Estado - Gráfico de Tráfico se observa que, de los 800Kbps de la capacidad de esta interfaz, existen picos que alcanzan los 50 Kbps como lo indica la siguiente imagen.

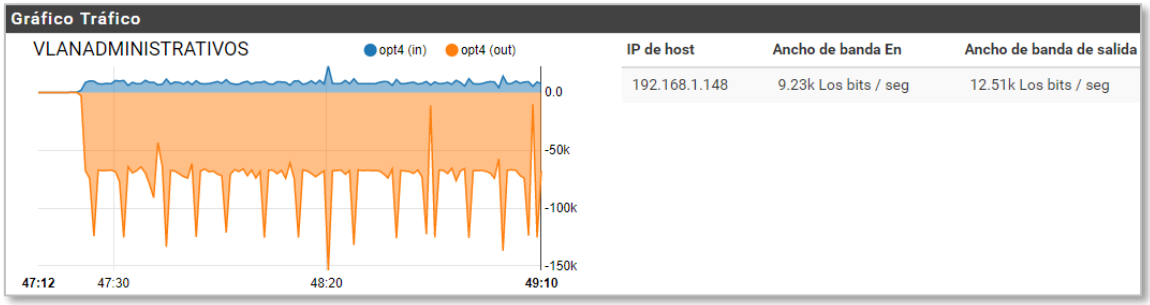


Figura 62. Ancho de banda de interfaz LAN- entorno de pruebas

Fuente: Captura Pfsense

Del análisis realizado en el ambiente de pruebas se concluye que Proxy es uno de los servicios que más recursos consume en el equipo y en comparación con el entorno real este parámetro se mantiene, por el contrario, el consumo del CPU incrementó, aunque

no ha llegado a sobrepasar el 50% de uso, lo cual indica que aún con todos los servicios implementados el rendimiento del equipo puede permanecer estable.

Cabe mencionar que el equipo Firewall perimetral en la Institución es un computador, pero este dispositivo debe ser capaz de atender estas peticiones y muchas más en caso de incrementar el número de usuarios y estar diseñado de una arquitectura de alto rendimiento para proveer los diferentes servicios a la red de datos sin saturar o limitar su desempeño.

Se elabora la Tabla 54 con los requerimientos más importantes que deberá tener el hardware para el Firewall.

Tabla 54. Requerimientos para el hardware Pfsense del HSLO

Componente	Descripción
Velocidad del Procesador	2 GHz o más
Memoria RAM	8 GB o más
Tamaño en Disco	1 TB o más
Número de tarjetas de red	3 o más
Velocidad de tarjetas de red	1/10/100 Gbps

Fuente: Autoría propia

Pfsense al basarse en FreeBSD puede ser implementado en cualquier dispositivo con requerimientos mínimos de hardware como se indicó en la Tabla 47, pero para que las Políticas de Seguridad de la Información propuestas sean implementadas efectivamente se recomiendan dos opciones: adquirir un equipo servidor para el Firewall en el cual se instale el software Pfsense, o en su caso, adquirir el hardware directamente de los desarrolladores de Pfsense. La Tabla 55 compara ambas soluciones para determinar cuál sería la adecuada.

Tabla 55. Comparativa entre servidor y hardware Pfsense

Servidor	Hardware Pfsense
Comúnmente poseen 2 tarjetas de red	Posee más de 2 tarjetas de red
Velocidad de las interfaces a 1 Gbps	Velocidades de 1/10/100 Gbps
Ocupan mayor espacio	Tamaño reducido, equipo de sobremesa

Se puede instalar cualquier sistema operativo	Posee a Pfsense y todas sus funciones como sistema operativo
Servidor que puede soportar varios tipos de servicios	Equipo creado netamente para cumplir funciones de firewall

Fuente: Autoría propia

Ante esta comparativa, es evidente que un sistema perimetral tendrá un mejor desempeño si es un dispositivo creado propiamente para realizar esta función y el hardware de Pfsense posee grandes ventajas frente a un servidor. A continuación, la Tabla 56 describe a los productos Firewall de Netgate con sus respectivas características.

Tabla 56. Dispositivos Netgate Pfsense Security Gateway

Productos	**Tamaño empresa**	**Procesador**	**Memoria RAM**	**Opciones de almacenamiento**	**Puertos**	**Costo**
SG-1100	Pequeña sucursal	ARM 1.2 GHz 2 núcleos	1GB DDR4	Flash de 8GB	3x 1GbE	$ 159,00
SG-3100	Pequeña sucursal	ARMv7 1.6 GHz 2 núcleos	2GB DDR4	Flash de 8GB	6x 1GbE	$ 349,00
SG-5100	Pequeñas y medianas	Intel Atom 2.2 GHz 4 núcleos	4GB DDR4	Flash de 8GB	6x 1GbE	$ 699,00
XG-7100	Medianas y grandes	Intel Atom 2.2 GHz 4 núcleos	8GB DDR4	Flash de 32 GB SSD de 256GB	2x 10GbE 8x 1GbE	$ 849,00
XG-7100 1U	Medianas y grandes	Intel Atom 2.2 GHz 4 núcleos	8GB DDR4	Flash de 32 GB SSD de 256GB	2x 10GbE 8x 1GbE	$ 999,00
XG-7100 1U HA	Medianas y grandes	Intel Atom 2.2 GHz 4 núcleos	8GB DDR4	Flash de 32 GB SSD de 256GB	2x 10GbE 8x 1GbE	$ 2.523,00
XG-1537 1U	Medianas y grandes	Intel Xeon 1.7 GHz 8 núcleos	8GB DDR4	SSD de 256GB	2x 10GbE 2x 1GbE	$ 1.949,00
XG-1537 1U HA	Medianas y grandes	Intel Xeon 1.7 GHz 8 núcleos	8GB DDR4	SSD de 256GB	2x 10GbE 2x 1GbE	$ 3.898,00
XG-1541 1U	Medianas y grandes	Intel Xeon 2.1 GHz 8 núcleos	16GB DDR4	SSD de 150GB	2x 10GbE 2x 1GbE	$ 2.649,00

XG-1541 1U HA	Medianas y grandes	Intel Xeon 2.1 GHz 8 núcleos	16GB DDR4	SSD de 150GB	2x 10GbE 2x 1GbE	$ 5.298,00

Fuente: Adaptado de (Netgate, 2019)

La Tabla 56 puede tomarse como referencia para la selección del hardware Pfsense adecuado para la Institución.

4.5 Análisis Costo – Beneficio

El análisis costo - beneficio se refiere al presupuesto de los recursos y medios que se necesitarán para la implementación de la Política de Seguridad de la Información, cabe mencionar que dicha implementación no generará ingresos económicos a la Institución, más bien, el beneficio se manifestará al evitar futuras pérdidas de información y daño de los equipos informáticos a causa de los riesgos.

4.5.1 Costos.

Una de las razones por las cuales se deja como propuesta el rediseño de la red de datos sin lograr su implementación total es debido al estado del cableado estructurado que necesita una reestructuración y que perjudica la implementación de Vlans y la gestión de la red como tal.

Dentro de la política de seguridad también se considera la protección física de los activos críticos alojados en el rak de equipos: servidores, switches, routers, etc., que se encuentran operando con normalidad, sin embargo, el área que los alberga carece de métodos de control de acceso físico que eviten robos e ingreso de personal no autorizado, igualmente, requiere adecuarse como mínimo de sistemas de refrigeración, ventilación, climatización, control de humedad, entre otros., para no sobrecalentar los equipos que a su vez incrementan el consumo de energía eléctrica.

De la Tabla 56 se ha seleccionado a uno de los equipos hardware Pfsense que cumple con las características que pueden satisfacer las necesidades de la red de datos de

la Institución. Uno de los riesgos encontrados en el análisis de riesgos fue la falta de medios destinados al almacenamiento de copias de respaldo del sistema por motivos de seguridad, por lo cual se consideran dentro de los costos.

En lo que se refiere a la política sobre derechos de propiedad intelectual, se toma en cuenta la cantidad de computadores y servidores con sistema operativo Windows (propietario), estos equipos deben tener la licencia respectiva para autorizar su uso dentro de la Institución y evitar sanciones.

En la Tabla 57 se elabora un cálculo estimado de precios de los recursos de hardware y software que la Institución requiere para implementar la Política de Seguridad de la Información, estos valores son parte de una propuesta que puede ser discutida con el personal correspondiente y que podría variar según la elección de los proveedores.

Tabla 57. Hardware y software estimado para la implementación de la Política de Seguridad de la Información

Hardware			
Descripción	**Cantidad**	**Valor U.**	**Valor total**
Cableado estructurado	1	$ 12,750,00	$ 12,106,6
Sistema de enfriamiento para el rack de equipos	1	$ 800,00	$ 800,00
Kit de control de acceso físico	1	$ 118,75	$ 118,75
XG-7100 1U Pfsense Security Gateway	1	$ 999,00	$ 999,00
Disco duro externo Toshiba	5	$ 65,00	$ 325,00
Total			$ 14.350,35
Software			
Descripción	**Cantidad**	**Valor U.**	**Valor total**
Licencias de sistema operativo propietario	33	$ 199,00	$ 6.567,00
Total			$ 6.567,00

Fuente: Anexo J – Cotización de recursos

El costo final es el resultado de la suma del presupuesto requerido para la implementación de la Política de Seguridad de la Información; cabe mencionar que, para dar cumplimiento a la política sobre el acceso a los servicios de la Institución a través de un nombre de dominio, la Institución debe solicitar el servicio de registro de nombre de dominio a su proveedor de Internet CNT. Todos los recursos mencionados permitirán elevar los niveles de seguridad de los activos críticos y la información que procesan (Tabla 58).

Tabla 58. Costos finales

Descripción	Valor total
Costos de Hardware	$ 14.350,35
Costos de Software	$ 6.567,00
Servicio de registro de dominio CNT (precio anual)	$ 35,00
Asesoramiento para la implementación de servicios	$ 1.280,00
Total	$ 22.232,35

Fuente: Anexo J – Cotización de recursos

Nota: En el Anexo J al final del documento se proveen mayores detalles acerca de los recursos mencionados.

4.5.2 Beneficio.

El Hospital San Luis de Otavalo podrá beneficiarse a partir de la implementación del presente proyecto con una estructura de red de datos más segura y flexible, segura en cuanto a la protección de los dispositivos de red y comunicaciones e información electrónica, y flexible en cuanto a la mejora en la administración de los equipos informáticos, todo ello a través de un conjunto de procedimientos y políticas que claramente deben ser entendidas tanto por los responsables del área de TIC, principales directivos de la Institución y por todos los funcionarios.

Los beneficios para los administradores de la red de datos serán:

- Estructura de red de datos mejor organizada.
- Facilidad de monitoreo de accesos de usuarios internos.
- Capacidad de controlar el flujo de datos entre las redes internas con la externa.
- Reducción de riesgos de servidores expuestos a redes externas.

Los beneficios para los funcionarios de la Institución serán:

- Mejor seguridad de la información contenida en los equipos informáticos a su cargo.
- Menos probabilidades de sufrir infecciones causadas por virus informáticos.
- Disponibilidad de servicios.

Los ciudadanos que acuden al Hospital San Luis de Otavalo también se beneficiarán con:

- Seguridad en cuanto a la confidencialidad e integridad de su información personal.
- Recibir una mejor atención debido a que los servicios informáticos permanecerán disponibles para que los profesionales de salud puedan llevar a cabo registros médicos e historias clínicas de los pacientes.

Finalmente, el Hospital San Luis de Otavalo se convertirá en un referente para otras casas de salud de la zona norte del país en cuanto a la gestión de los recursos de TI para garantizar la seguridad de la información, ubicándose entre los primeros en tomar acciones que aporten en la optimización de la atención en beneficio de los ciudadanos.

5. CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

- Con el marco de trabajo COBIT 5 se logró diseñar el Gobierno de TI para el Hospital San Luis de Otavalo a través de la aplicación de la técnica de la cascada de metas de COBIT 5 que consiste en alinear los objetivos estratégicos de la Institución con los objetivos, metas y procesos de TI propios de este marco de trabajo y que permitió determinar los procesos de TI que, en cuestiones de la Gestión de Riesgos y Seguridad de la Información, la Institución necesita mejorar; para ello, COBIT 5 como un marco integrador, se apoyó en otras normativas gubernamentales con un conjunto de buenas prácticas para mejorar aspectos específicos sobre la seguridad de la información.
- La norma NTE INEN-ISO/IEC 27005:2015 permitió desarrollar el análisis de Gestión de Riesgos de la Seguridad de la Información de manera sistemática mediante lineamientos que explican cómo realizar la identificación de activos, el conocimiento de políticas existentes, la determinación de criterios para la valoración de activos y riesgos que, finalmente fueron expuestos en la matriz de riesgos, cuya información constituye el punto de partida para el tratamiento de las principales amenazas y vulnerabilidades asociadas con los activos de información críticos.
- Como resultado del proceso de Análisis de Riesgos de la Seguridad de la Información los principales riesgos que se pudieron evidenciar fueron: un estado desorganizado del cableado estructurado, seguridad de acceso físico deficiente, fallas en el funcionamiento del servidor Proxy No Transparente en Pfsense, una red plana sin segmentos de red lógicos o perfiles de usuarios, ausencia de mecanismos de encriptación de información confidencial, ausencia de

mecanismos de autenticación de usuarios a la red, servidores internos vulnerables, puertos abiertos innecesarios, servidores con accesos remotos desprotegidos, uso de software propietario sin licencia y desactualizados, red poco escalable, entre otros; y que sin embargo, con los recursos informáticos existentes fue posible mejorar la seguridad de la red de datos y a la información como tal.

- La solución para minimizar o reducir los riesgos presentes en la actual red de datos de la Institución fue por medio de la formulación la Política de Seguridad de la Información, un documento de alto nivel con medidas que exigen la importancia de proteger el activo más importante de esta casa de salud que es la información, y en especial, la información personal de los pacientes que a su vez es procesada por los equipos informáticos; se elaboró a partir de la inclusión del conjunto de buenas prácticas recomendadas por el Esquema Gubernamental de Seguridad de la Información (EGSI), así como de la normativa NTE INEN-ISO 27799:2008 con aspectos específicos sobre la protección de la información en el ámbito sanitario.
- La formulación de la Política de Seguridad de la Información se llevó a cabo mediante el establecimiento de procedimientos para tratar aspectos como la socialización de la Política de Seguridad de la Información, la formalización del acuerdo de Confidencialidad de la Información, el proceso a seguir para la gestión de riesgos e identificación de nuevas amenazas de riesgo y el procedimiento para la adquisición de licencias para uso de software propietario; adicionalmente, para mitigar los riesgos a nivel informático se utilizaron herramientas basadas principalmente en el uso de software libre para dar cumplimiento a políticas de seguridad específicas.

- Se planteó un rediseño de la red de datos actual teniendo como base al firewall Pfsense, este software gratuito permitió establecer mecanismos para implementar políticas para reducir riesgos claves tales como: la ausencia de mecanismos de autenticación a la red de datos por medio de un Portal Cautivo y la autenticación de usuarios a la red inalámbrica con la implementación de un servidor Radius, una red plana con alto tráfico de broadcast a partir de la creación de Vlans, las fallas en el bloqueo de sitios web no autorizados a través de un servidor Proxy Transparente, mejorar la seguridad de los servidores con la integración de una nueva Zona Desmilitarizada y demás riesgos que pueden solventarse con la aplicación correcta de reglas de firewall, es decir, elevar el nivel de protección de la red de datos implementando funciones y servicios que caracterizan a Pfsense para el control de tráfico que atraviesa la red interna y externa.
- La Política de Seguridad de la Información se implementó parcialmente en el entorno real dejando operativos a los servicios: Proxy Transparente, Portal Cautivo y VPN, debido al estado del cableado estructurado de la red de datos de la Institución y al computador en el que se encuentra instalado Pfsense que no cumple con los requisitos para actuar propiamente como un firewall, es por eso que el rediseño de la red de datos y servicios se deja como una propuesta que puede ser implementada a futuro por medio de los recursos de hardware y software planteados para cumplir con la totalidad de la Política de Seguridad de la Información.
- El software Pfsense ofrece una gran ventaja para la Institución porque es un sistema completo, seguro y fácil de administrar, sobre todo, permite implementar varios servicios en un solo dispositivo, reduciendo la necesidad de destinar un

equipo físico para cada servicio y por ende se minimiza las inversiones en recursos informáticos.

- En el análisis costo-beneficio se elaboró una estimación del presupuesto de los recursos que la Institución necesita adquirir para elevar los niveles de seguridad de la infraestructura informática, presupuesto que no debería considerarse como un gasto sino como una inversión y comprender que las tecnologías de la información (TI) son en la actualidad y a futuro un el eje transversal para la gestión administrativa de la Institución y gestores de apoyo tecnológico para sus actividades técnico-médicas.

5.2 Recomendaciones

- En un inicio los administradores del área de TIC del Hospital San Luis de Otavalo no se encontraban familiarizados con las normativas que el Estado ecuatoriano establece referente a la Gestión de la Seguridad de la Información, por ello se recomienda que se instruyan y se capaciten sobre las mejores prácticas definidas particularmente en el Esquema Gubernamental de Seguridad de la Información y en las normativas NTE INEN-ISO/IEC 27005:2012 y NTE INEN-ISO 27799:2008, que son estándares nacionales recomendados para su aplicación en las entidades que forman parte de la administración pública del país.
- La normativa NTE INEN-ISO/IEC 27005:2012 al constituirse como el estándar principal sobre el cual se basan otras metodologías de gestión de riesgos de la seguridad de la información, no presenta una metodología clara para ejecutar dicho proceso, motivo por lo cual se sugiere utilizar cualquiera de las existentes y que persigan el mismo principio.
- Aunque existe una política sobre la seguridad de los equipos informáticos, esta se encuentra sujeta a todas las entidades que conforman el Sistema Nacional de

Salud, es decir, no está adaptada al entorno real de la Institución, por lo tanto, es recomendable la formulación e implementación de una Política de Seguridad propia donde se definan los lineamientos y procedimientos necesarios para reducir los riesgos presentes y que afectan directamente a los activos críticos.

- El software Pfsense ofrece una gestión centralizada de la red de datos y por ello se recomienda realizar respaldos o copias de seguridad diarios de las configuraciones del sistema y una supervisión periódica del sistema eléctrico o sistema de alimentación ininterrumpida UPS para evitar fallas o pérdida de disponibilidad de los servicios.
- En el caso de que la Institución no cuente con el presupuesto para invertir en la adquisición de los recursos propuestos, se recomienda que, para disminuir costos en la compra de licencias de software para Windows, se considere la sustitución de dicho sistema operativo con software libre, capacitando oportunamente a los usuarios acerca del uso del mismo.
- La protección de la información debe ser compromiso de todos los funcionarios del Hospital San Luis de Otavalo, cada colaborador debe tomar conciencia acerca del daño potencial que puede provocar a los activos de información a su cargo si cometen actos indebidos que los pongan en riesgo, por ello es necesario motivar al personal a tomar la iniciativa y capacitarse en temas de seguridad de la información y atender cualquier duda, inquietud o desconocimiento que necesite aclararse.

6. REFERENCIAS BIBLIOGRÁFICAS

Acosta, D. (2016). Vulnerando la Política de Seguridad de la Información por diversión y dinero. Colombia.

Agustín, Z. (2015). *Cuadro comparativo de normas y estándares de TI*. Obtenido de Cuadro comparativo de normas y estándares de TI: https://agustinzaidti.wordpress.com/2014/09/20/cuadro-comparativo-de-normas-y-estandares-ti/

Ariganello, E. (2016). *Guía de estudio para la certificación CCNA Routing and Switching.* Madrid: Ra-Ma.

Asamblea Nacional de la República del Ecuador. (2008). CONSTITUCIÓN DE LA REPÚBLICA DEL ECUADOR. Obtenido de https://www.asambleanacional.gob.ec/sites/default/files/private/asambleanacional/filesasambleanacionalnameuid-29/2018-08-01-constitucion-reformada.pdf

Bozovic, N. (24 de Julio de 2019). *Wich VPN Protocol you should use? - Five common VPN protocols explained and compared*. Obtenido de https://www.technadu.com/vpn-protocols/8436/

Cengace learning. (2010). *Network Defense Perimeter Defense Mechanism.*

Comercio, E. (10 de Febrero de 2017). *Kaspersky detectó malware que ha infectado bancos de todo el mundo, entre esos de Ecuador*. Obtenido de https://www.eluniverso.com/vida-estilo/2017/02/10/nota/6041425/kaspersky-detecto-malware-que-ha-infectado-bancos-todo-mundo

Contraloría General del Estado. (6 de Noviembre de 2003). Constitución Política de la República del Ecuador. Obtenido de http://www.contraloria.gob.ec/documentos/normatividad/ConPolRep.pdf

CPCCS. (2018). *Transparencia LOTAIP*. Obtenido de Transparencia LOTAIP: http://www.cpccs.gob.ec/es/transparencia-lotaip/

Dadheech, K., Choudhary, A., & Bhatia, G. (2018). De-Militarized Zone: A next Level to Network Security. *IEEE Xplore Compliant*, 2.

Deloitte. (2017). *Seguridad de la Información en Ecuador*. Obtenido de https://www2.deloitte.com/content/dam/Deloitte/ec/Documents/deloitte-analytics/Estudios/SeguridadInformacion2017.pdf

Domínguez, J. (2015). Panorama General de COBITv5 y Balanced Score Card. Obtenido de https://ingenieriayeducacion.files.wordpress.com/2013/05/panorama-general-de-cobitv5-y-balanced-score-card.pdf

Global, U. (s.f.). *Gobierno IT*. Obtenido de http://www.tcpsi.com/servicios/gobierno_ti.htm

IETF. (November de 1987). Domain names - Implementation and specification.

INEN. (2008). *NORMA TÉCNICA ECUATORIANA NTE INEN-ISO 27799.* Quito.

INEN. (2012). *NORMA TÉCNICA ECUATORIANA NTE INEN-ISO/IEC 27005:2012.* Quito.

ISACA. (2012). *COBIT 5 Spanish*. Obtenido de http://www.isaca.org/COBIT/Pages/COBIT-5-spanish.aspx

ISACA. (2012). Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa. Estados Unidos. Obtenido de https://articulosit.files.wordpress.com/2013/07/cobit5-framework-spanish.pdf

ISO Tools Excellence. (8 de Febrero de 2018). *¿Cómo analizar los riesgos? Con ISO 27005 o con MAGERIT*. Obtenido de ¿Cómo analizar los riesgos? Con ISO 27005 o con MAGERIT: https://www.pmg-ssi.com/2018/02/riesgos-iso-27005-magerit/

ITGI. (2 de Octubre de 2013). *Board Briefing on IT Governance, 2nd Edition.* Obtenido de Board Briefing on IT Governance, 2nd Edition: https://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Board-Briefing-on-IT-Governance-2nd-Edition.aspx

Kuldeep, K., & Gupta, H. (5 de Marzo de 2016). A new approach for the security of VPN. India. Obtenido de https://dl.acm.org/citation.cfm?id=2905219

Lancho, Á. (2017). *Sistema Cortafuegos de Alta disponibilidad con Pfsense.* Universidad Politécnica de Madrid, Madrid.

Mehdizadeha, A., & Suinggi, K. (2017). Virtual Local Area Network (VLAN): Segmentation and Security. *Researchgate,* 78.

Ministerio de Defensa Nacional. (10 de Febrero de 2014). Código Orgánico Integral Penal, COIP. Obtenido de https://www.defensa.gob.ec/wp-content/uploads/downloads/2018/03/COIP_feb2018.pdf

Ministerio de Educación. (18 de Mayo de 2004). Ley Orgánica de Transparencia y Acceso a la Información Pública. Obtenido de http://www.oas.org/juridico/PDFs/mesicic5_ecu_ane_cpccs_22_ley_org_tran_acc_inf_pub.pdf

Ministerio de Finanzas. (24 de Marzo de 2011). Reglamento General a la Ley Orgánica del Servicio Público. Obtenido de http://www.ueb.edu.ec/sitio/images/PDF/LEYES/REGLAMENTO_LEY_SERVICIO_PUBLICO.pdf

Ministerio de Trabajo. (24 de Marzo de 2011). Ley Orgánica del Servicio Público LOSEP. Obtenido de https://www.telecomunicaciones.gob.ec/wp-content/uploads/2017/05/LEY-ORGANICA-DEL-SERVICIO-PUBLICO.pdf

Monfort, R. (2016). COBIT 5 y el Cuadro de Mando Integral como herramientas de Gobierno de TI. *Trabajo de Fin de Grado.* Universidad Politécnica de Valencia, España. Obtenido de https://riunet.upv.es/bitstream/handle/10251/72620/MONFORT%20-%20COBIT%205%20y%20el%20Cuadro%20de%20Mando%20Integral%20como%20herramientas%20de%20Gobierno%20de%20TI.pdf?sequence=2

MSP. (22 de Diciembre de 2006). Ley de Derechos y Amparo al Paciente. Obtenido de https://www.salud.gob.ec/wp-content/uploads/downloads/2014/09/Normativa-Ley-de-Derechos-y-Amparo-del-Paciente.pdf

MSP. (31 de Julio de 2012). Estatuto Orgánico de Gestión Organizacional por Procesos de los Hospitales del Ministerio de Salud Pública. Quito. Obtenido de http://instituciones.msp.gob.ec/somossalud/images/guia/documentos/estatuto_de_hosp_acuerdo.pdf

MSP. (24 de Enero de 2015). Reglamento de Información Confidencial en el Sistema Nacional de Salud. Obtenido de http://instituciones.msp.gob.ec/cz6/images/lotaip/Enero2015/Acuerdo%20Ministerial%205216.pdf

Muñoz, I., & Ulloa, G. (2011). Gobierno de TI – Estado del arte. *S&T*.

Netgate. (2019). *Captive Portal*. Obtenido de https://docs.netgate.com/pfsense/en/latest/book/captiveportal/index.html

Netgate. (2019). *Minimum Hardware Requirements*.

Netgate. (2019). *Productos Pfsense*. Obtenido de https://www.pfsense.org/products/

OAS. (17 de Abril de 2002). LEY DE COMERCIO ELECTRÓNICO, FIRMAS ELECTRÓNICAS Y MENSAJES DE DATOS. Obtenido de https://www.oas.org/juridico/spanish/cyb_ecu_ley_comelectronico.pdf

Ortiz Beltrán, F. (2015). HACKING ÉTICO PARA DETECTAR FALLAS EN LA SEGURIDAD INFORMÁTICA DE LA INTRANET DEL GOBIERNO PROVINCIAL DE IMBABURA E IMPLEMENTAR UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI), BASADO EN LA NORMA ISO/IEC 27001:2005. *(Tesis de Grado).* Universidad Técnica del Norte, Ibarra.

Pillo, D. (2017). Propuesta de un modelo de Gobierno de Tecnología de la Información para hospitales públicos. Caso: Hospital General Docente de Calderón. *(Tesis de Maestría).* Universidad de las Américas, Quito.

Planificación HSLO. (2018). *Plan Estratégico Institucional.* HSLO, Otavalo.

Rajaraman, V. (2018). *Introduction to Information Technology.* India: PHI Learning Private Limited.

Rigney, Rubens, Simpson, & Willens. (1997). Remote Authentication Dial In User Service (RADIUS).

Rocha, M. (2019). Instructivo Dynamips-Dynagen-GNS3. Uruguay.

Rojas, F. (2017). *La Razón*. Obtenido de La Consitución: http://www.la-razon.com/opinion/columnistas/Constitucion_0_2730926884.html

Secretaría Técnica Plan Toda una Vida. (20 de Marzo de 2015). Ley Orgánica de Salud. Obtenido de https://www.todaunavida.gob.ec/wp-content/uploads/downloads/2015/04/SALUD-LEY_ORGANICA_DE_SALUD.pdf

SNAP. (15 de Junio de 2012). EGSI - Esquema Gubernamental de Seguridad de la Información. Ecuador.

Solano, E. (2017). *Diseño de un Cloud privado para ofrecer infraestructura como servicio de máquinas virtuales, utilizando la plataforma OpenStack para la Facultad de Ingeniería en Ciencias Aplicadas (FICA) de la Universidad Técnica del Norte.* UTN, Ibarra.

Vallejos, M. (2019). *Diseño de Sistema de Seguridad a nivel de capa de enlace de datos en redes cableadas mediante el estándar IEEE 802.1x en la LAN de la Universidad Técnica del Norte.* Universidad Ténica del Norte, Ibarra.

MINISTERIO DE **SALUD**

Coordinación Zonal 1 - Salud
Hospital San Luis de Otavalo

EL GOBIERNO DE TODOS

Otavalo, 17 de julio 2019

Señores.

A quien corresponda.

Presente.

CERTIFICADO

Se certifica que la Srta. Catherine Liseth Lòpez Quilumbango con Cédula de Identidad Nro. 1003769187, estudiante de la Carrera de Ingeniería Electrónica y Redes de Comunicación de la Universidad Técnica del Norte, realizó la socializaciòn de los resultados del Proyecto de Tesis Titulado "Gobierno de TI Basado en el Esquema Gubernamental de Seguridad de la Información (EGSI) en el Hospital San Luis de Otavalo, 2019", el día miércoles 10 de Julio del año en curso, culminado con el Proyecto antes mencionado.

Particular que informo para fines pertinentes.

Atentamente.

HOSPITAL SAN LUIS DE OTAVALO
Carmen Cabascango
LICENCIADA EN ENFERMERÍA
REG SENESCYT 1015-13-1189639

Dr. Juan Echeverría
Director del Hospital
San Luis de Otavalo

Lic. Carmen Cabascango
Responsable Unidad de
Docencia e investigación

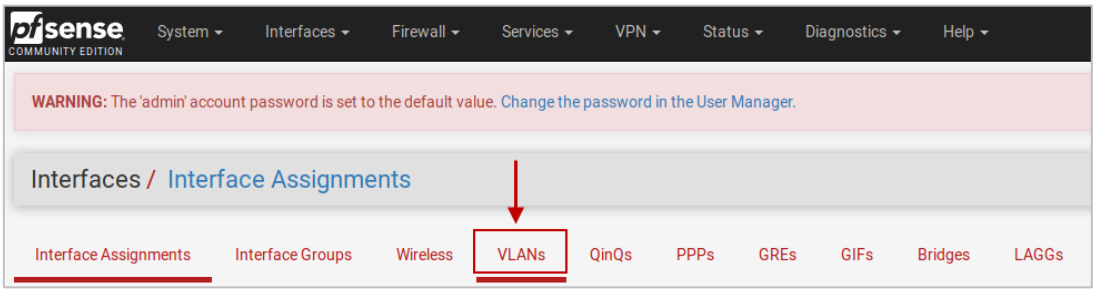
ANEXOS

I.1 Manual de implementación de Vlans en Pfsense

El siguiente manual tiene como objetivo presentar el procedimiento a seguir para la creación y configuración de Vlans en el software Pfsense. El primer paso es acceder a la interfaz web de Pfsense introduciendo las credenciales correspondientes.

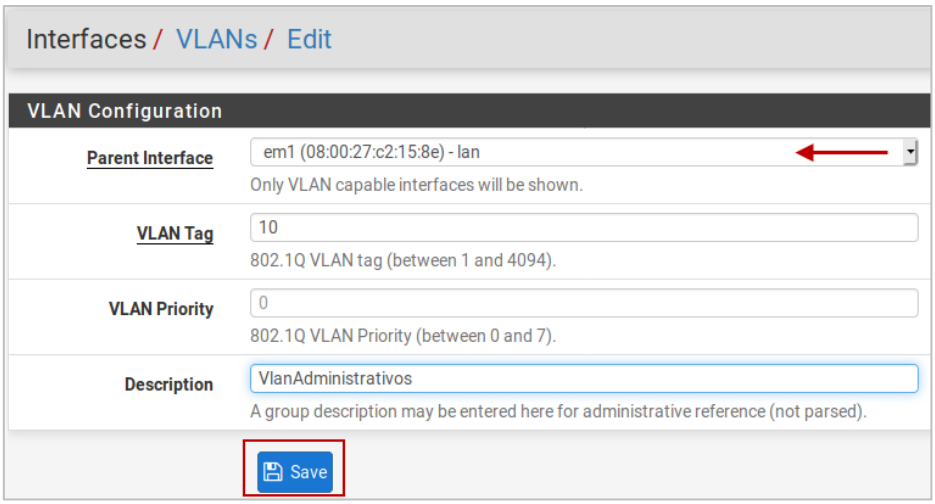
Creación de VLANs

Una vez que se acceda a Pfsense, en la ventana inicial ingresar al menú Interfaces en la pestaña Interface Assignments, luego seleccionar la opción VLANs para crearlas.



Para crear una Vlan, hacer clic en el botón Add y posteriormente llenar los siguientes campos indicados:

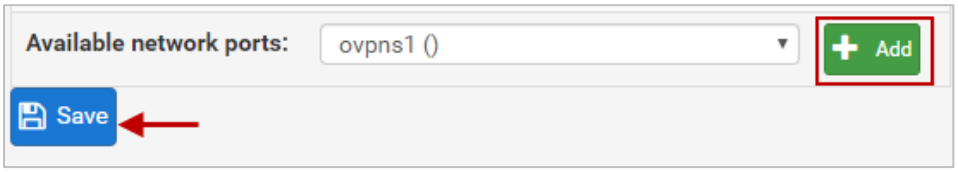
- Seleccionar la interfaz física en la cual se van a crear la Vlan.
- Insertar un número de identificación de la Vlan entre (1-4094).
- Colocar una descripción que identifique a la Vlan.
- Guardar los cambios.



La captura de pantalla anterior indica el proceso para crear una Vlan con un nombre y un número de identificación, el mismo proceso debe repetirse para crear las Vlan establecidas de acuerdo con la tabla de direccionamiento.

Asignación de Vlans a interfaces

Posteriormente, en la pestaña Interface Assignments se procede a añadir cada Vlan a una interfaz, en este caso se asigna a la interfaz opt que tendrá el mismo comportamiento que las demás interfaces opt asignadas a la red LAN, WAN o DMZ, por ello necesitan configurarse, colocar reglas de firewall y activar servicios de ser el caso. En la ventana que se muestra, hacer clic en Add para agregar una Vlan a la interfaz y guardar.

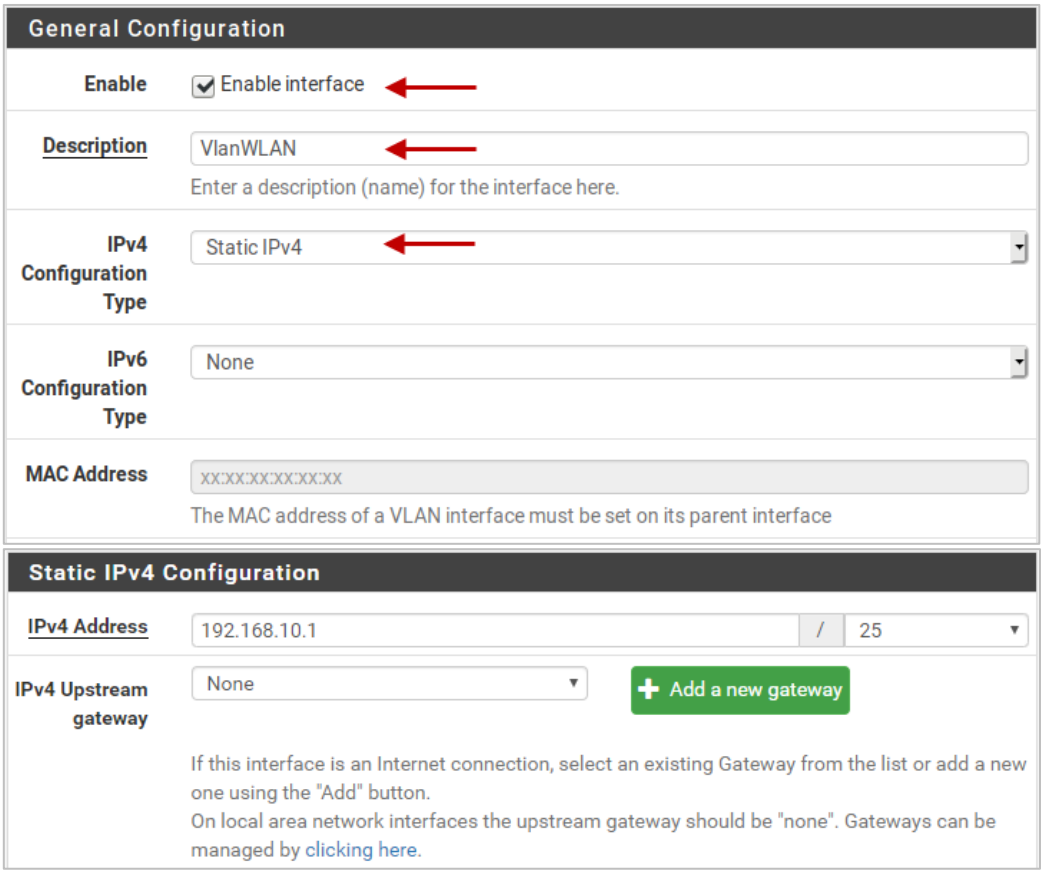


Seguidamente, seleccionar la nueva interfaz para configurar la Vlan y realizar lo siguiente:

- Seleccionar la pestaña para habilitar la interfaz.
- Colocar un nombre que describa a la interfaz.

- Seleccionar el tipo de configuración de la dirección IP de dicha interfaz, en este caso la configuración será de manera estática.
- En la sección Static IPv4 Configuration colocar la dirección IP correspondiente a cada Vlan con su respectiva máscara de subred, guiándose de la tabla de direccionamiento inicial.
- Guardar los cambios.

Nota: Los demás campos pueden omitirse.

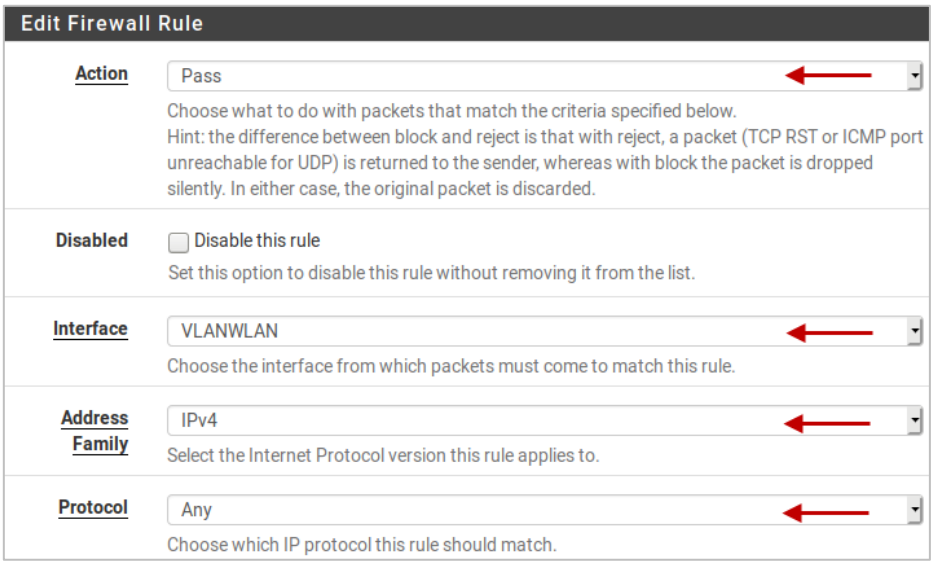


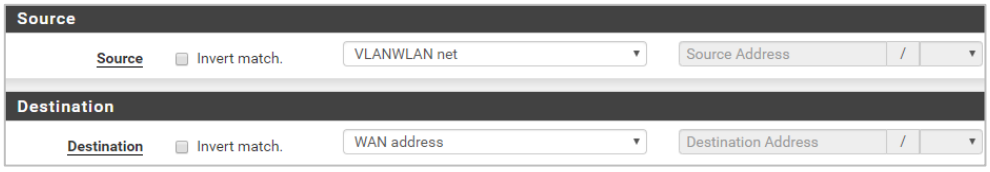
Con la ayuda de la tabla de direccionamiento se colocan las direcciones IP correspondientes para cada Vlan. El mismo procedimiento se repite para asignar las Vlans restantes a una interfaz.

Cuando todas las Vlans se hayan configurado adecuadamente Pfsense almacena esta información.

Configuración de reglas para las Vlan

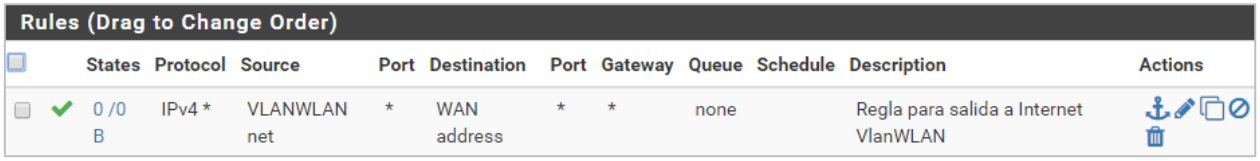
Ahora, al dirigirse al menú Firewall - Rules se observa que se han generado nuevas pestañas que corresponden a las interfaces de las Vlans creadas y se configuran como si fuesen interfaces físicas. Ahora se editan las reglas del Firewall para cada una de ellas. En la siguiente Vlan se crea la regla para permitir salida hacia internet a través de la WAN.





Nota: El procedimiento para editar y configurar las reglas de cada Vlan es similar.

Finalmente se ha creado la regla establecida para la Vlan WLAN del proceso anterior.



Como se mencionó anteriormente, 3 de los switches de la Institución son administrables, y pueden ser aprovechados para crear Vlan y organizar de mejor manera

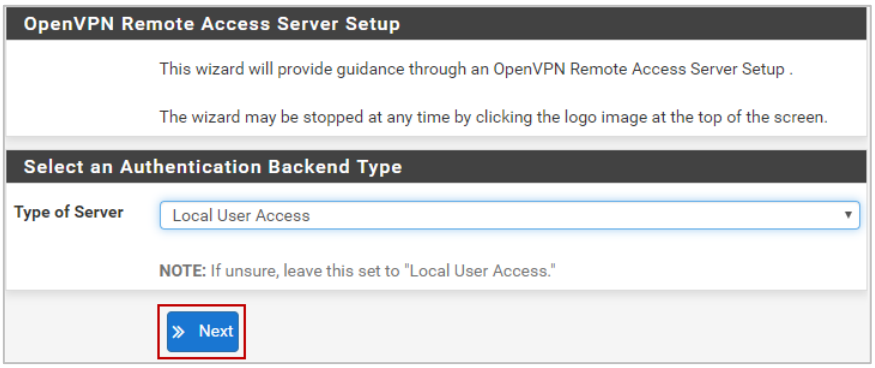
la red de datos de la Institución siempre y cuando esté acompañado de un cableado estructurado en buenas condiciones.

I.2 Manual de configuración de OpenVPN en Pfsense

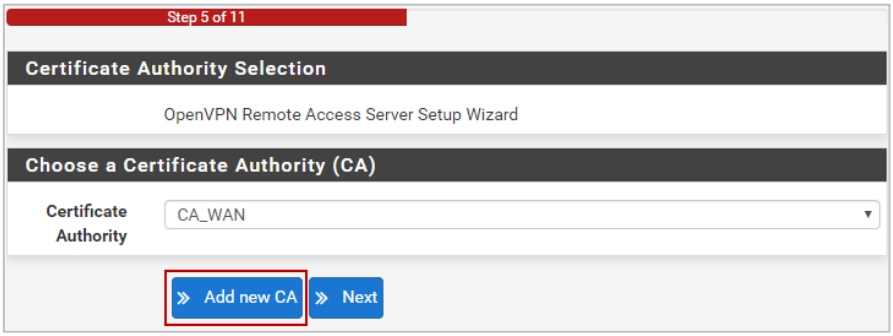
El objetivo de crear una conexión mediante VPN es habilitar un acceso seguro para configurar los servidores internos de la Institución desde redes externas.

Configuración inicial de OpenVPN

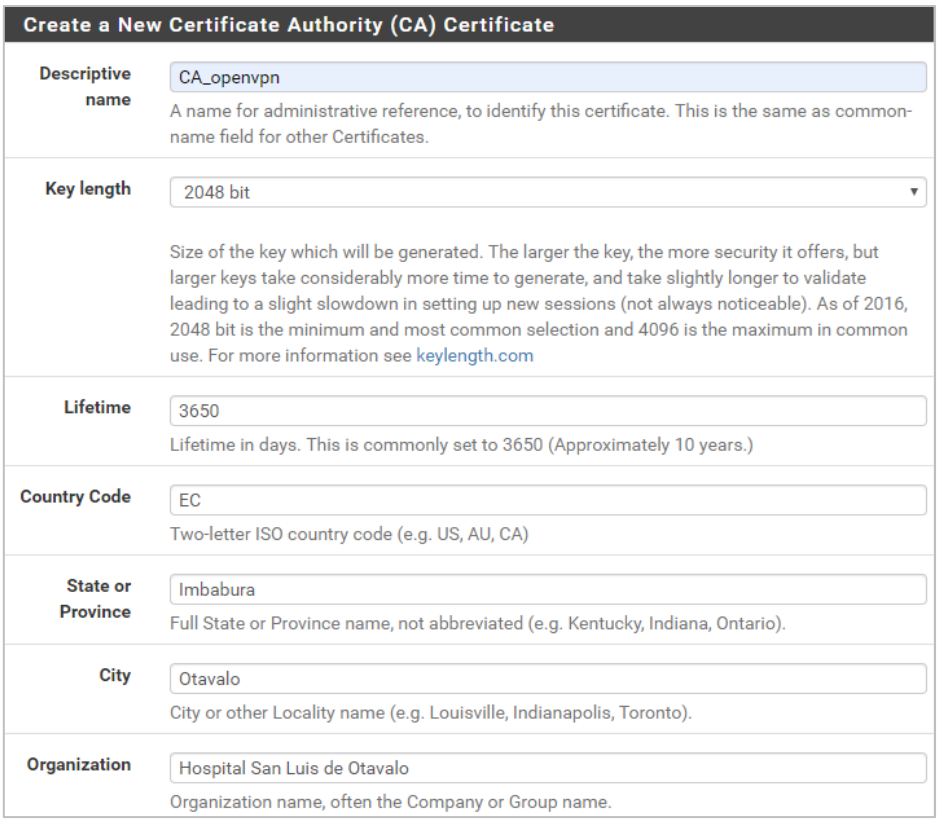
Desde Pfsense, acceder al menú VPN – OpenVPN. Hacer clic en la pestaña Wizards desde donde se inicia la creación y configuración de la VPN. Clic en Next.



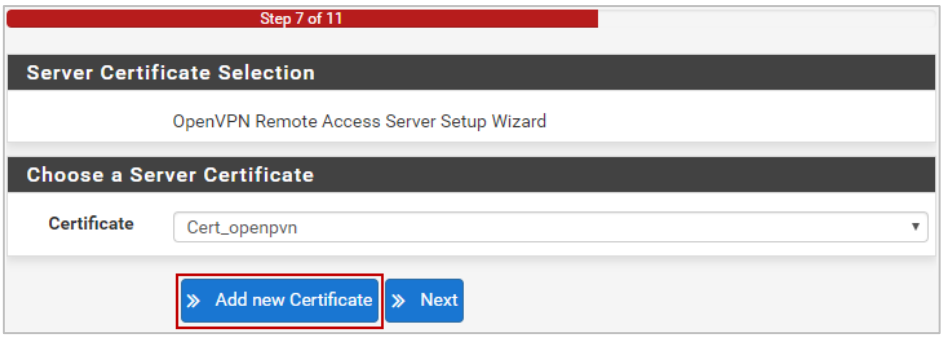
En la siguiente ventana, clic en el botón Add new CA, desde el cual se creará una Autoridad Certificadora para validar la VPN.



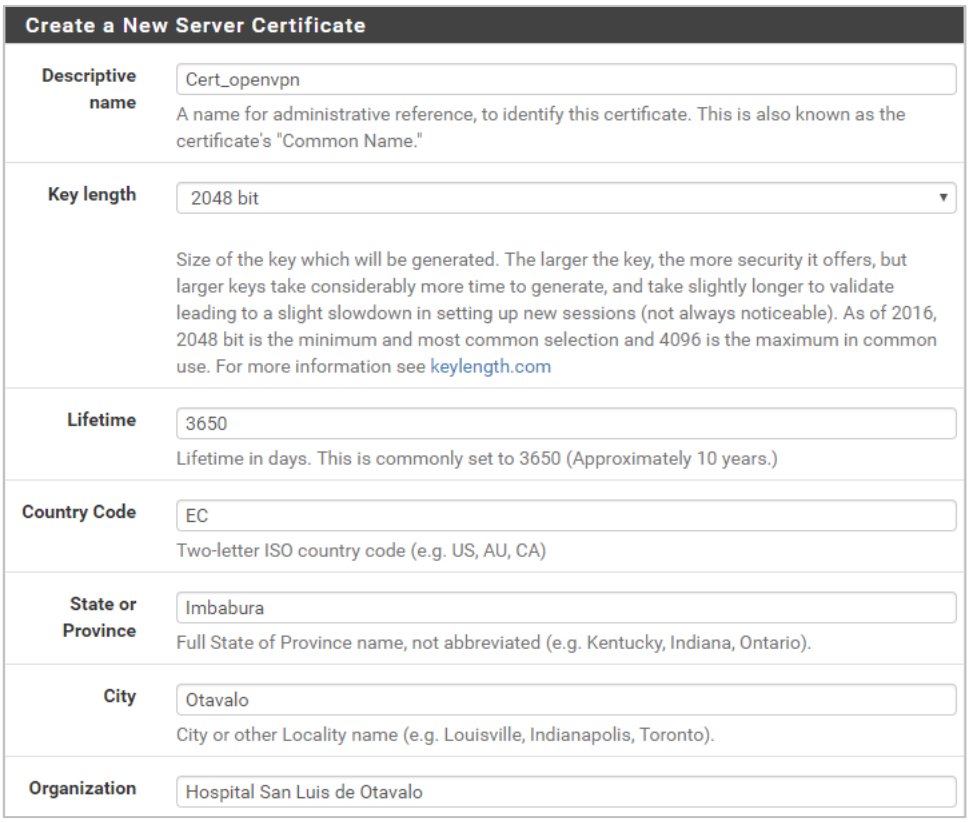
En esta ventana introducir los siguientes datos que identifican a la Institución. Guardar los cambios y clic en Next.



Seguidamente, se pedirá seleccionar un certificado para la VPN, para ello hacer clic en Add new Certificate



Introducir los mismos campos que identifican a la Institución. Guardar los cambios y clic en Next.



Posteriormente, se configura la VPN llenando los campos con la siguiente información:

En la sección General OpenVPN Server Information:

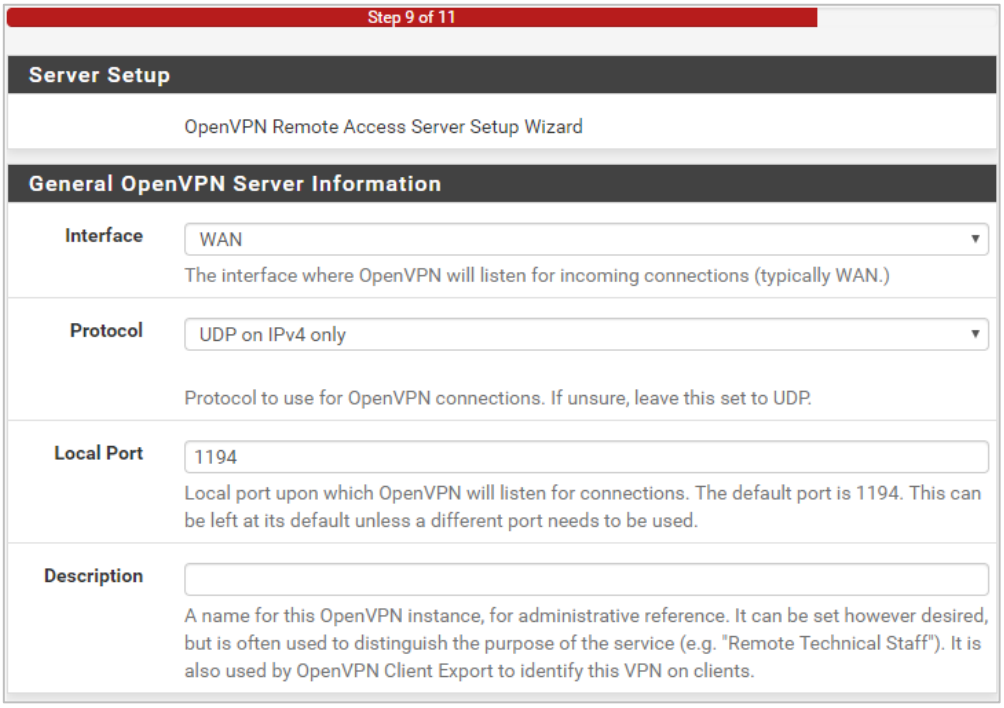
- Seleccionar la interfaz desde la cual la VPN escuchará las conexiones entrantes.
- Seleccionar el protocolo que se utilizará para las conexiones VPN, en este caso UDP.
- Seleccionar el puerto local en el que OpenVPN escuchará las conexiones. El puerto predeterminado es 1194, se puede dejar en su valor predeterminado a menos que se necesite utilizar un puerto diferente.

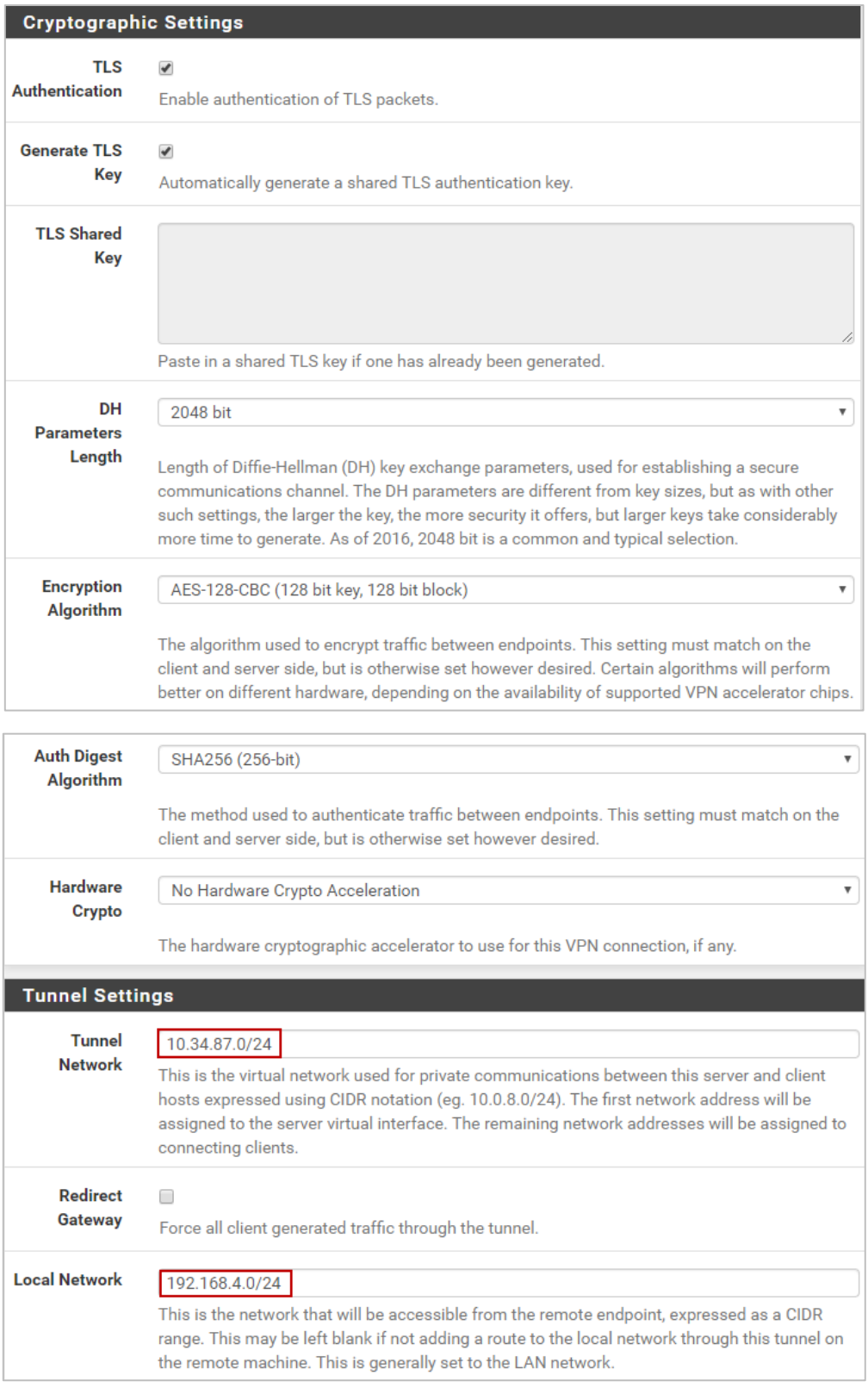
En la sección Tunnel Settings configurar lo siguiente:

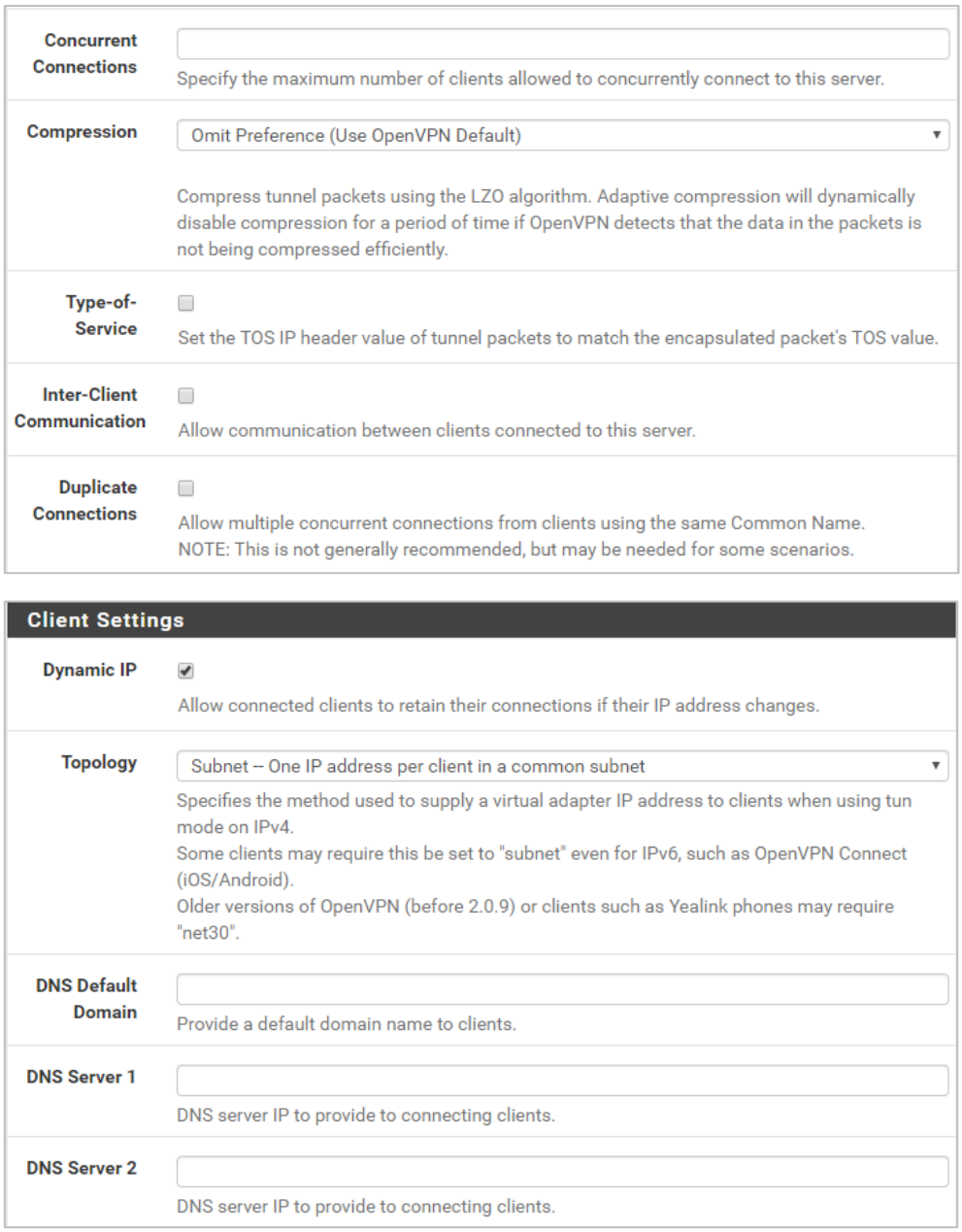
- En el campo Tunnel Network introducir una dirección de red que será utilizada para las comunicaciones entre el servidor OpenVPN y los hosts del cliente expresados mediante la notación CIDR (por ejemplo, 10.0.8.0/24). La primera

dirección de red se asignará a la interfaz virtual del servidor. Las direcciones de red restantes se asignarán a clientes de conexión.

- En el campo Local Network se introducen las redes locales que serán accesibles para los clientes VPN, estas rutas se envían a los clientes que se conectan al servidor.

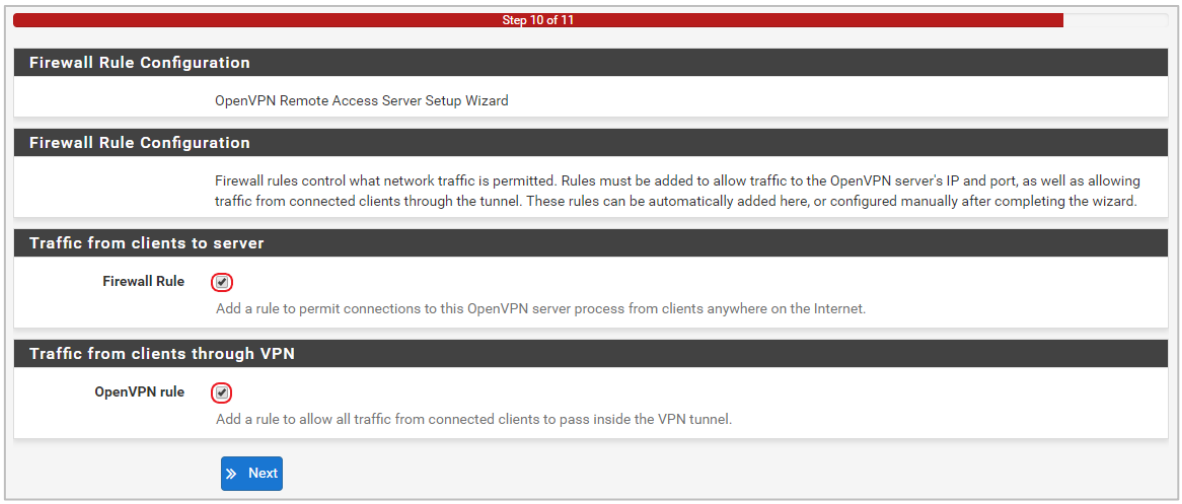



Cryptographic Settings
TLS Authentication
Enable authentication of TLS packets.
Generate TLS Key
Automatically generate a shared TLS authentication key.
TLS Shared Key
Paste in a shared TLS key if one has already been generated.
DH Parameters Length
2048 bit
Length of Diffie-Hellman (DH) key exchange parameters, used for establishing a secure communications channel. The DH parameters are different from key sizes, but as with other such settings, the larger the key, the more security it offers, but larger keys take considerably more time to generate. As of 2016, 2048 bit is a common and typical selection.
Encryption Algorithm
AES-128-CBC (128 bit key, 128 bit block)
The algorithm used to encrypt traffic between endpoints. This setting must match on the client and server side, but is otherwise set however desired. Certain algorithms will perform better on different hardware, depending on the availability of supported VPN accelerator chips.
Auth Digest Algorithm
SHA256 (256-bit)
The method used to authenticate traffic between endpoints. This setting must match on the client and server side, but is otherwise set however desired.
Hardware Crypto
No Hardware Crypto Acceleration
The hardware cryptographic accelerator to use for this VPN connection, if any.
Tunnel Settings
Tunnel Network
10.34.87.0/24
This is the virtual network used for private communications between this server and client hosts expressed using CIDR notation (eg. 10.0.8.0/24). The first network address will be assigned to the server virtual interface. The remaining network addresses will be assigned to connecting clients.
Redirect Gateway
Force all client generated traffic through the tunnel.
Local Network
192.168.4.0/24
This is the network that will be accessible from the remote endpoint, expressed as a CIDR range. This may be left blank if not adding a route to the local network through this tunnel on the remote machine. This is generally set to the LAN network.

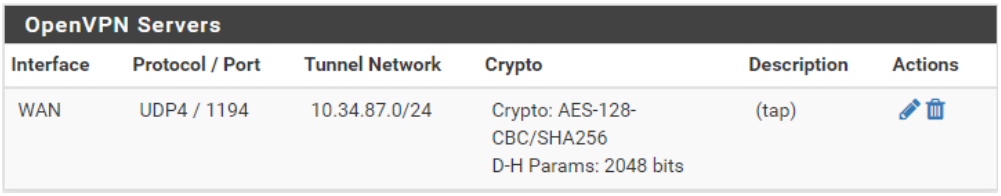


Luego de configurar la VPN, clic en Next y activar las dos pestañas que se indican:

- La pestaña Firewall Rule creará una regla para permitir la conexión al servidor OpenVPN desde clientes en cualquier lugar de Internet.
- La pestaña de OpenVPN rule agregará una regla para permitir que todo el tráfico de los clientes conectados pase dentro del túnel VPN.



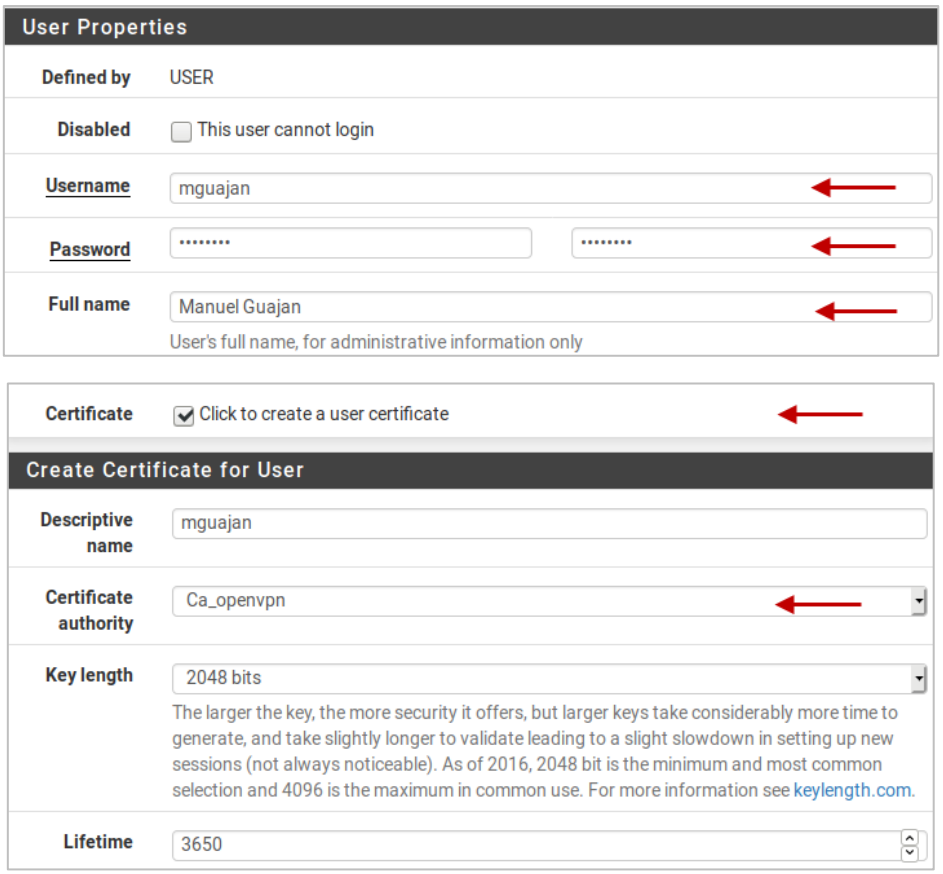
Con los pasos mencionados se finaliza la configuración de OpenVPN.



Creación de usuarios para OpenVPN

Posteriormente se crean los usuarios que podrán conectarse a la VPN al verificar la autenticidad de su identidad utilizando sus contraseñas y certificados anteriormente creados. En la pestaña System - User Manager, seleccionar Users - Add. En esta ventana, como ejemplo, se crea un usuario con privilegios de acceso a la VPN llenando los siguientes campos:

- Colocar un nombre de usuario.
- Agregar una contraseña de usuario y confirmarla.
- Colocar el nombre completo del usuario.
- Activar la pestaña Certificate.
- Seleccionar el certificado creado para que este usuario tenga privilegios de acceso a la VPN.
- Guardar los cambios.

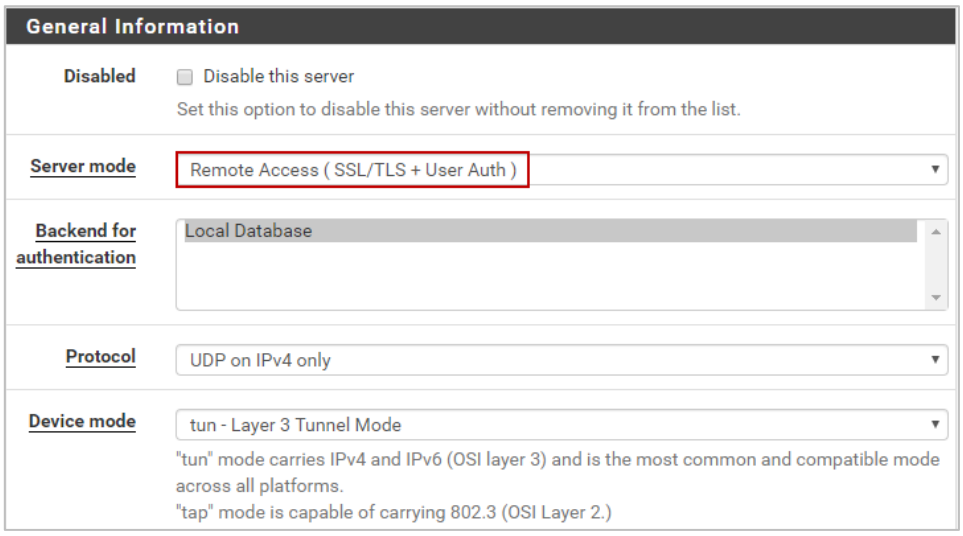


Nota: En este ejemplo, se ha generado un usuario para que pueda acceder a la VPN, si se requiere compartir dicho privilegio a más de un usuario, debe seguirse el mismo procedimiento.

El siguiente paso en la ventana de Información general configurar lo siguiente:

- El modo de servidor especifica como se conectarán los clientes al servidor, por lo que se sugiere elegir la opción Acceso remoto (SSL/TLS + User Auth) que es la opción más segura con los beneficios de SSL/TLS y requiere de un nombre de usuario y contraseña del cliente al conectarse.
- En protocolo, seleccionar UDP ya que es la opción más rápida para ejecutar OpenVPN, TCP hace que el rendimiento disminuya en conexiones con mucha carga de paquetes.
- En modo del dispositivo indica el modo de túnel, se puede elegir entre un túnel IP (controlador TUN) y un túnel Ethernet (controlador TAP), el túnel IP también se

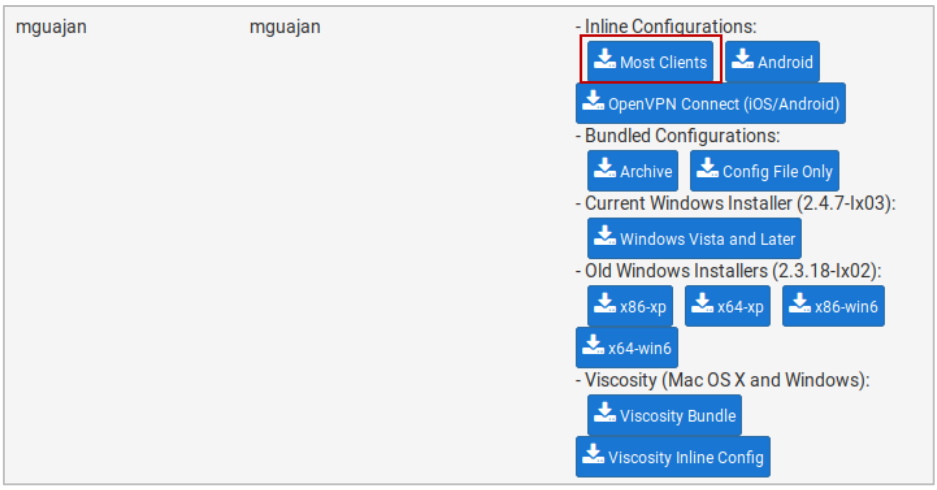
conoce como modo de enrutamiento, y el túnel Ethernet como modo puente. Es preferible elegir el modo de túnel IP (configuración predeterminada) a menos que se necesite pasar tráfico Ethernet dentro del túnel.



Exportación del certificado VPN de usuario

Una vez creado el/los usuarios correspondientes, se genera un certificado correspondiente a cada uno de ellos para autenticarse en la VPN y que deben ser descargados. Para ello, es necesario descargar un nuevo paquete desde Pfsense que permita exportar dichos certificados. Desde la pestaña System – Package Manager, descargar el paquete openvpn-client-export:

Proceder con la descarga del certificado desde la pestaña OpenVPN - Client Export, buscando el archivo del usuario respectivo. Pfsense permite descargar los certificados según los tipos de archivos que se deseen, en este caso, descargar el formato Most Clients.

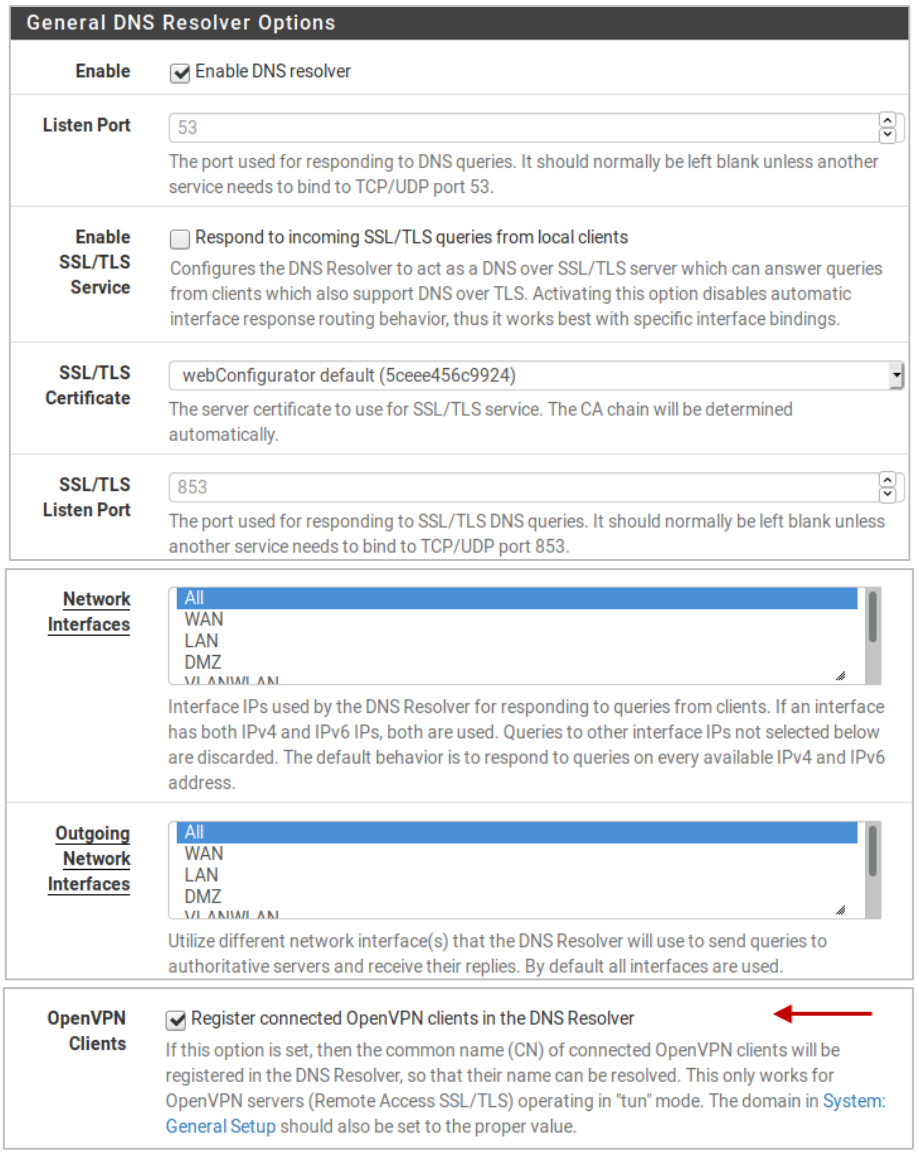


I.3 Manual de configuración del Resolvedor DNS en Pfsense

El presente anexo indica los pasos a seguir para la configuración del Servidor de Resolución de Dominios DNS en Pfsense. El servidor DNS se configura con la finalidad de acceder a los servicios de la Institución mediante nombres de dominio en lugar de una dirección IP.

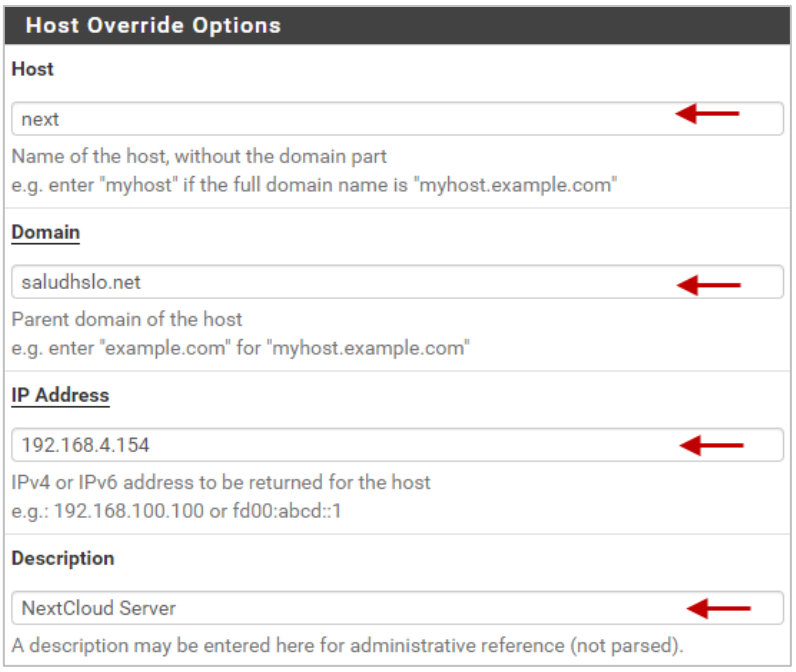
Pfsense también provee la función de configurar un servidor DNS, desde el menú Service seleccionar DNS Resolver -General Settings y configurar los siguientes parámetros:

- Habilitar el Resolvedor DNS.
- Seleccionar el puerto usado para resolver las peticiones DNS será el 53.
- Seleccionar las interfaces desde las cuales se responderán las peticiones de los clientes, en este caso se seleccionan todas las interfaces con la opción All.
- Habilitar la pestaña para que las peticiones DNS realizadas desde clientes OpenVPN puedan resolverse.

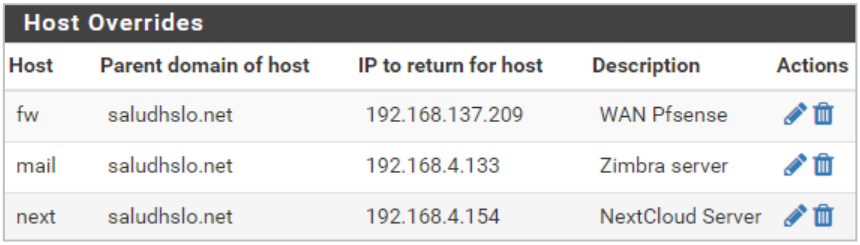


En la sección Host Override Options se colocan las descripciones tanto de las direcciones IP como de los dominios de los servicios que el servidor DNS resolverá.

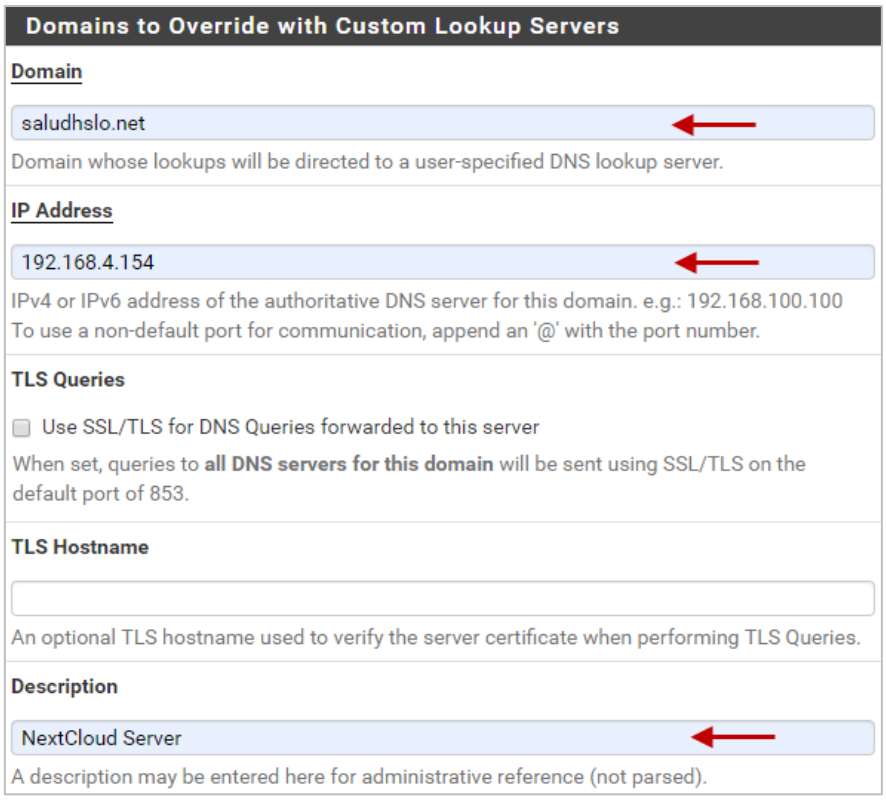
- Colocar un nombre de host exceptuando la parte del dominio.
- Colocar el dominio principal del host.
- Colocar la dirección IP correspondiente al servicio.
- Colocar una descripción del servicio como una referencia (opcional).
- Guardar los cambios.



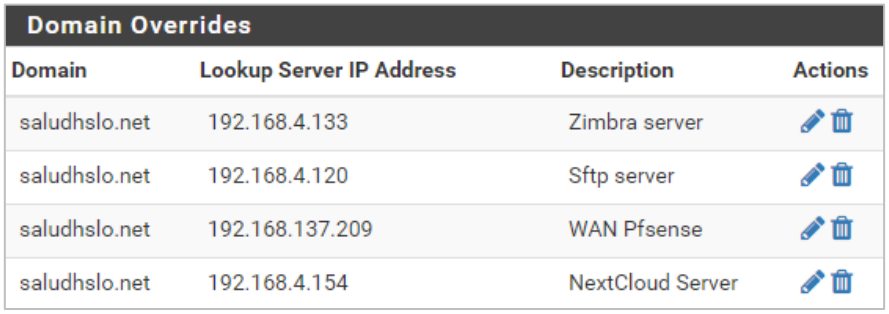
Nota: Los datos introducidos para resolver un servicio se realizará de manera similar si se desean agregar más hosts.



Colocar los dominios cuyas búsquedas se dirigirán al servidor de búsqueda DNS especificado por el usuario.



Y finalmente se tienen los dominios establecidos en el Servidor DNS.

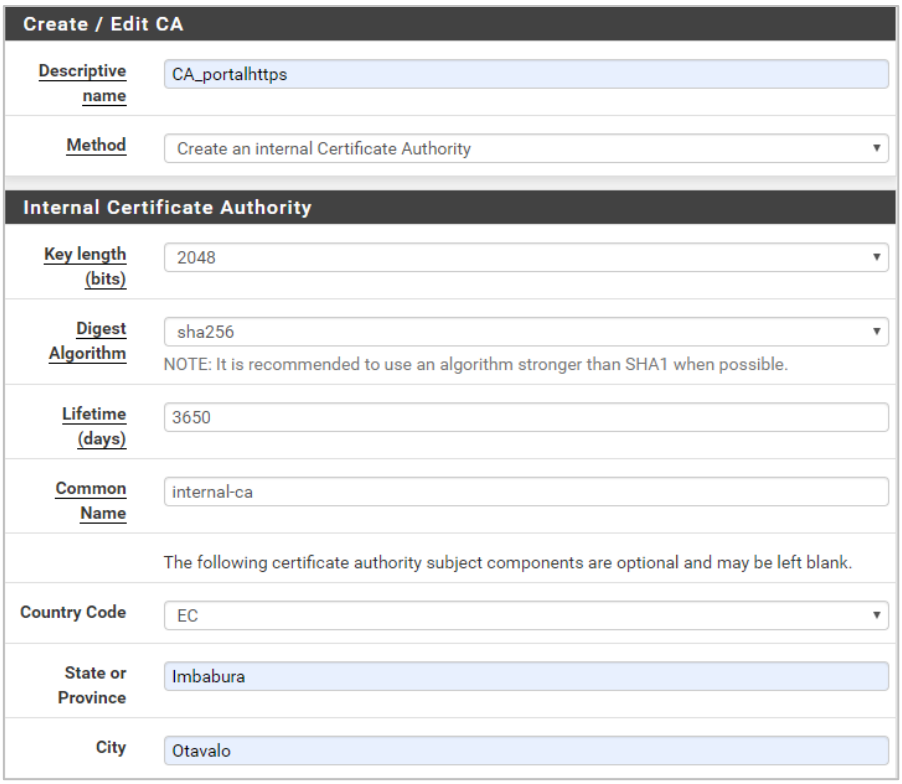


I.4 Manual de configuración del Portal Cautivo en Pfsense

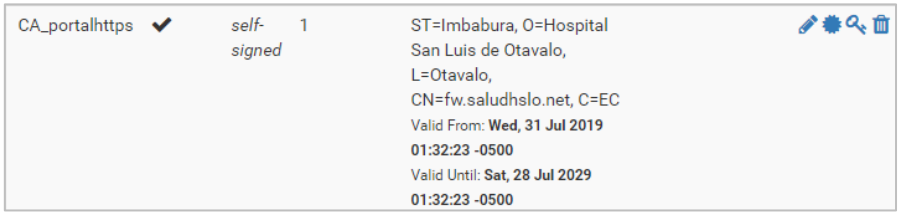
En el presente Anexo se explica el procedimiento a seguir para la creación y configuración del Portal Cautivo con Pfsense.

Creación de certificado SSL para Portal Cautivo

Ingresar al menú System en la pestaña Certificate Manager y crear una Autoridad Certificadora, llenando los campos con información que describa a la Institución.

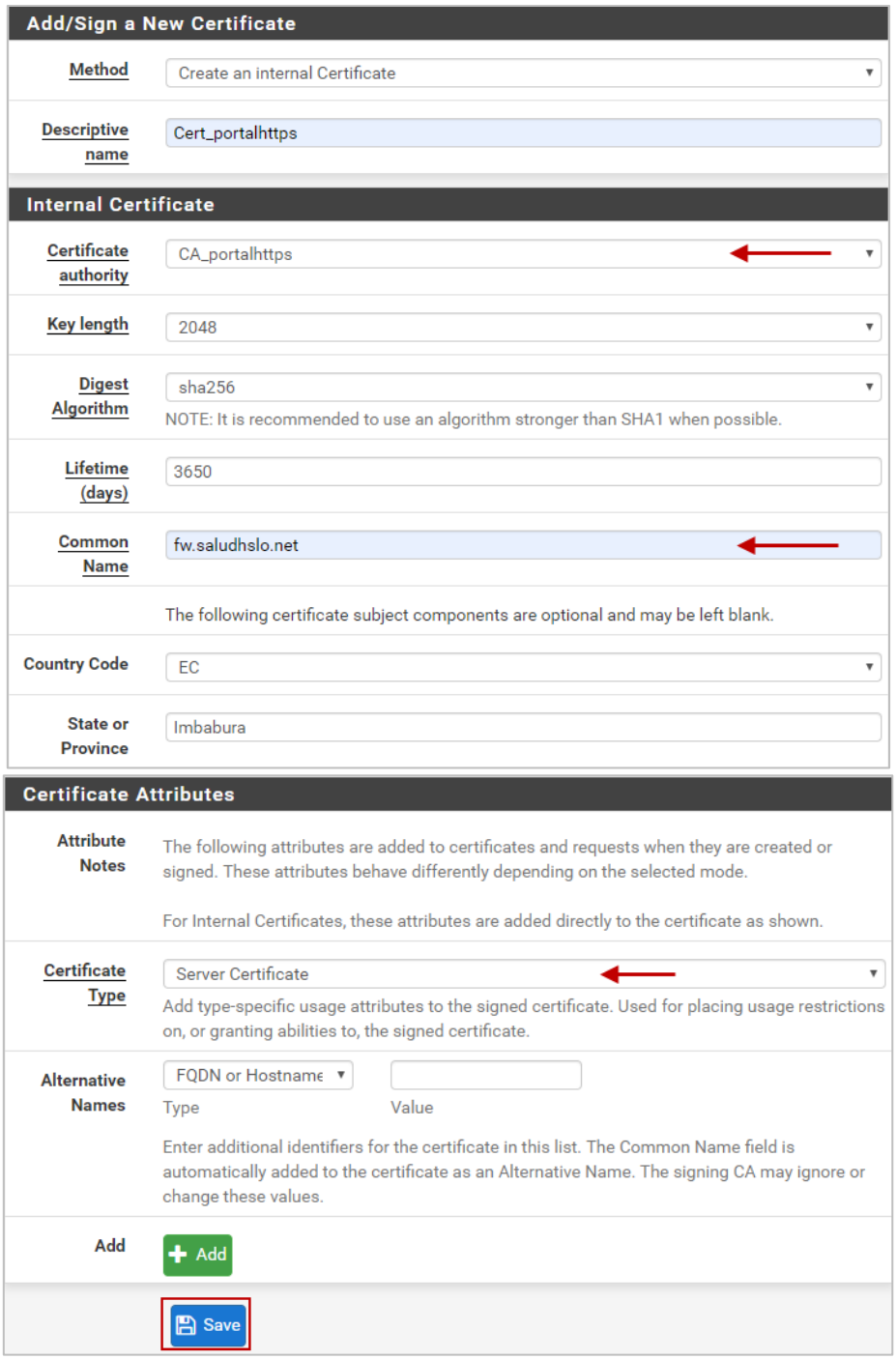


Cuando se hayan completado los campos respectivos se creará la Autoridad Certificadora.

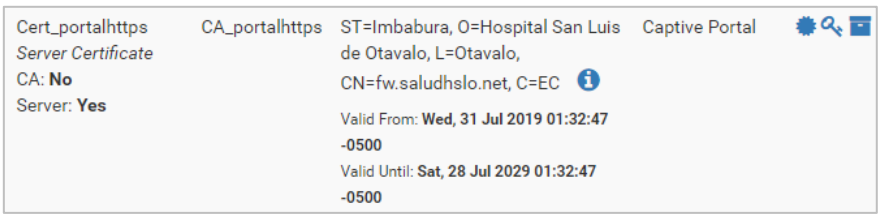


De la misma manera crear un Certificado SSL para el Portal Cautivo, en la misma pestaña, seleccionar Certificates y llenar los mismos campos, pero adicionalmente:

- Seleccionar la autoridad certificadora creada anteriormente.
- En common name colocar el dominio de Pfsense.
- En certificate type, seleccionar el tipo certificado de servidor.



Y el certificado se crea.



Creación de zona para Portal Cautivo

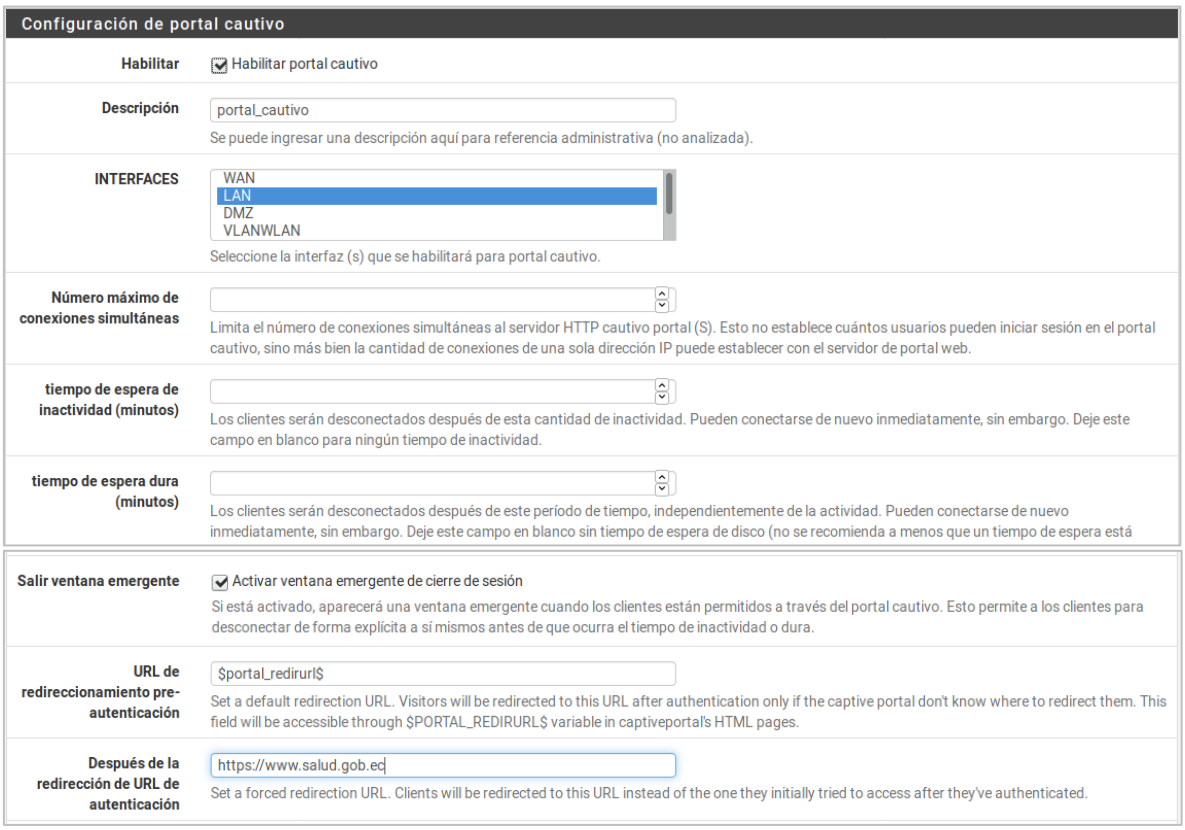
Dirigirse a la pestaña Servicios – Portal Cautivo. En esta ventana, colocar un nombre a la zona del Portal Cautivo y una descripción.

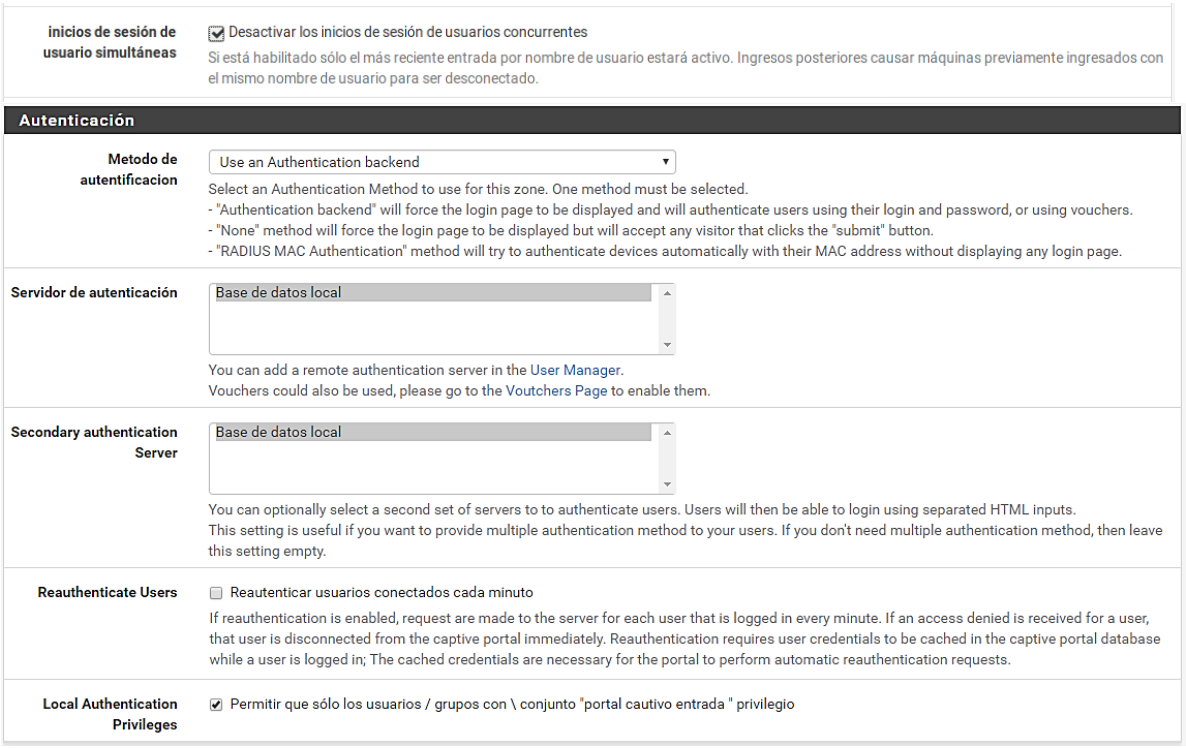
Una vez creada la zona, pulsar en el ícono del lápiz para configurarla y en la siguiente ventana, se configuran ciertos parámetros según los requerimientos deseados, o bien, los campos pueden ser omitidos.

- Habilitar la casilla del Portal Cautivo.
- Seleccionar la interfaz a la cual se habilitará el Portal Cautivo, en este caso, se habilita el portal cautivo para las VLANS Doctores y Administrativos.
- Habilitar la ventana emergente de cierre de sesión.
- Establecer una página web o URL (Localizador Uniforme de Recursos) a la cual serán redireccionados una vez autenticados los usuarios, en este caso será la página inicial del Ministerio de Salud Pública.
- Deshabilitar la casilla de inicio de sesión de usuarios concurrentes para evitar que los usuarios inicien sesión en varios equipos a la vez.

En la sección **Autenticación**, configurar lo siguiente:

- Seleccionar un método de autenticación, para este caso, se utilizará "**Authentication backend**" que forzará a los usuarios a atravesar una página en la cual iniciar sesión con un usuario y contraseña para navegar por Internet.
- Como la autenticación de usuarios será de forma local, seleccionar "**Base de Datos Local"**.
- Seleccionar la opción de Privilegios de Autenticación Local solamente a usuarios o grupos que tienen privilegios de acceso al Portal Cautivo.

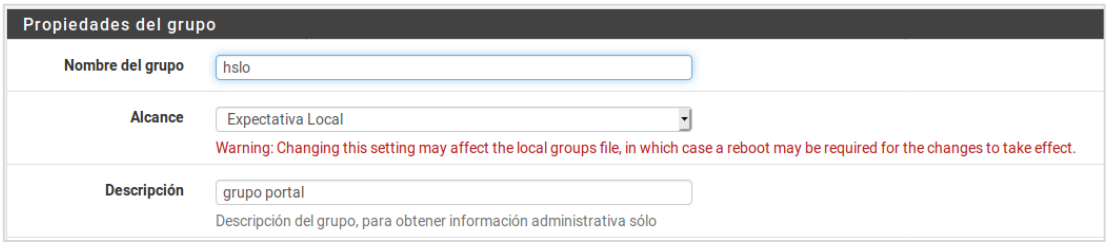




Nota: Para que se active la ventana emergente, se debe permitir o habilitar en cada navegador de los equipos cliente las ventanas emergentes.

Creación de grupo y usuarios del Portal Cautivo

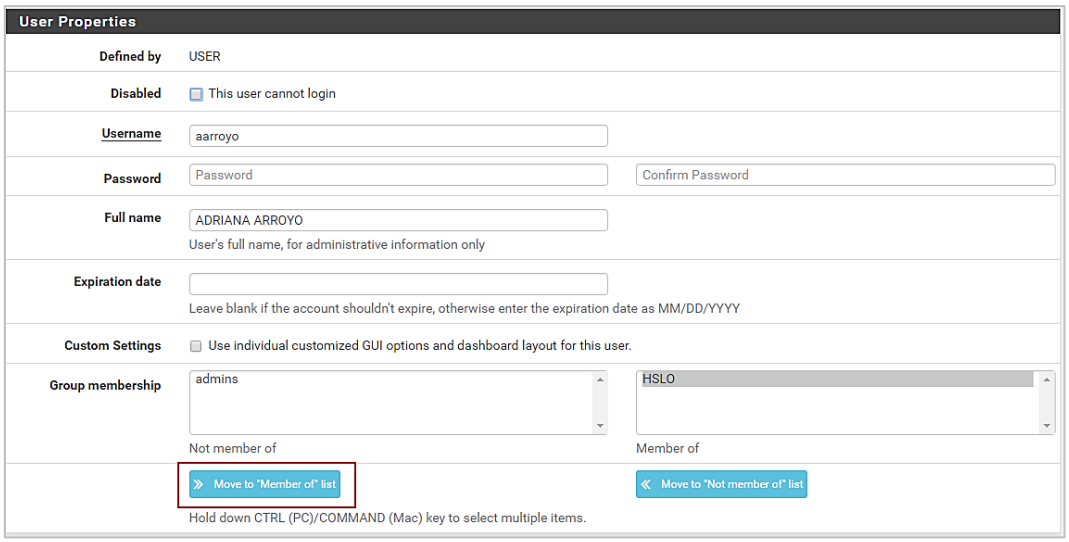
Seguidamente se crea un grupo que contenga la cantidad de usuarios que se necesiten. Para ello, dirigirse a la pestaña System – User Management. En la sección "Propiedades del grupo", colocar un Nombre y Descripción al grupo a ser creado y guardar los cambios.



Desde la pestaña Users**,** añadir usuarios realizando lo siguiente:

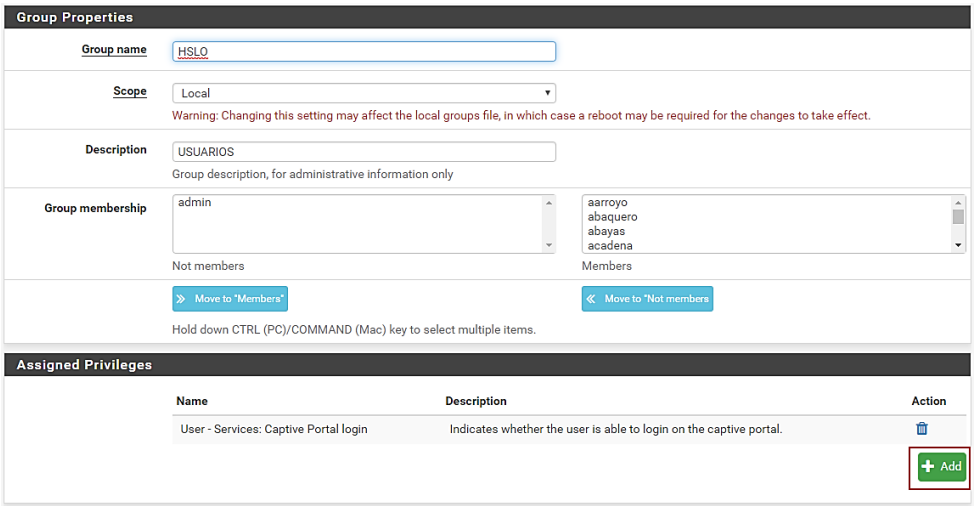
- Colocar un nombre de usuario.
- Asignar una contraseña y confirmar contraseña.

- Colocar el Nombre completo del usuario.
- Mover al usuario a la lista o grupo anteriormente creado.
- Guardar los cambios.



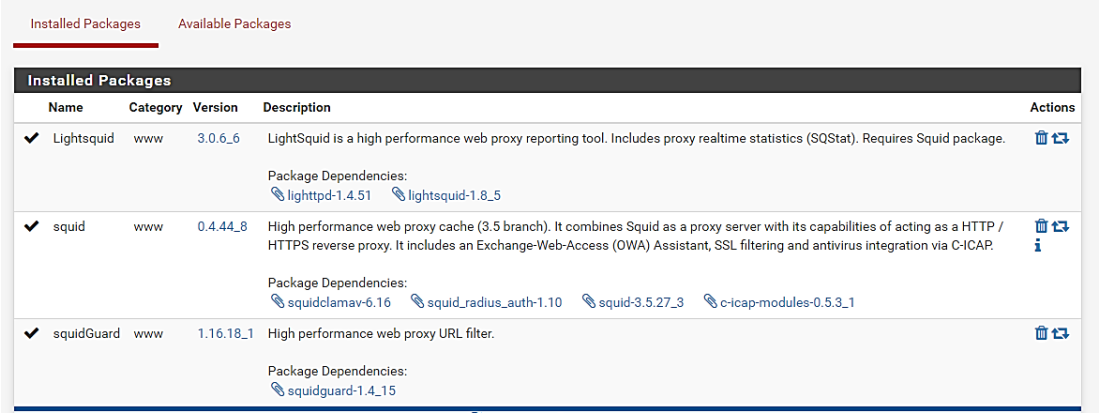
Nota: Se repite el mismo procedimiento para crear más usuarios.

Volver a la configuración del Grupo del Portal Cautivo y en la sección “Asigned Privileges”, seleccionar “User – Services Captive Portal Login” para habilitar a los usuarios el privilegio de acceso al Portal Cautivo.



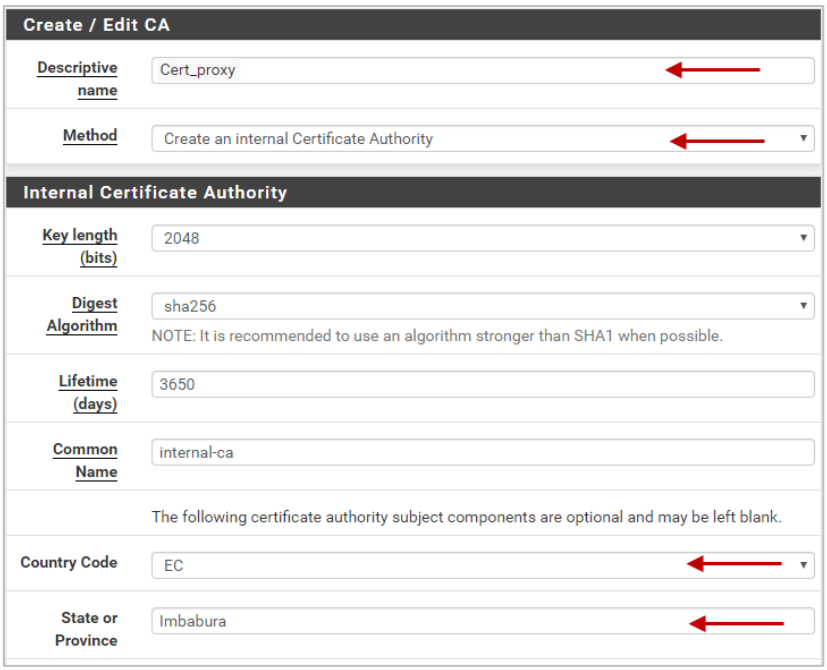
I.5 Manual de configuración del servidor Proxy en Pfsense

Desde la pestaña System – Package Manager descargar los paquetes: Proxy, Squidguard Proxy y Lightsquid, son tres paquetes que trabajan en conjunto y permitirán obtener una mejor administración del Servidor Proxy.



Es necesario crear un certificado para que le Servidor Proxy pueda filtrar contenido https. Desde la pestaña System - Certificate Manager, seleccionar CAs - Add, donde se llenan los siguientes campos:

- Colocar un nombre para el Certificado.
- Seleccionar la opción “Crear Autoridad Certificadora Interna”.
- Elegir el código del país (opcional).
- Escribir el nombre de la provincia (opcional)
- Guardar los cambios.

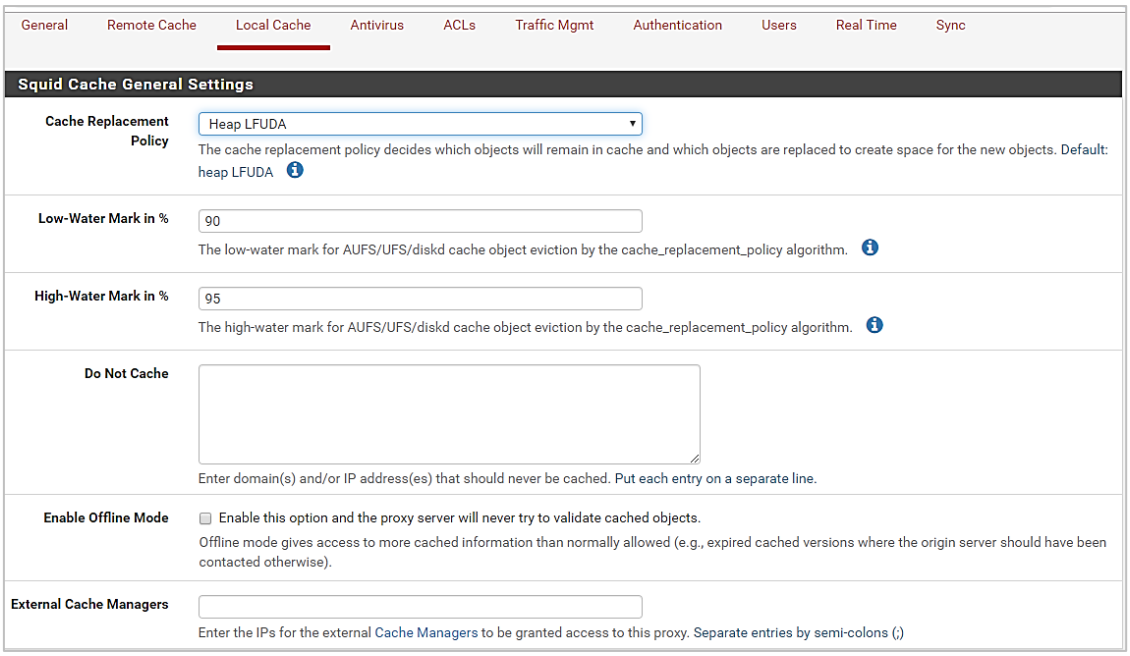


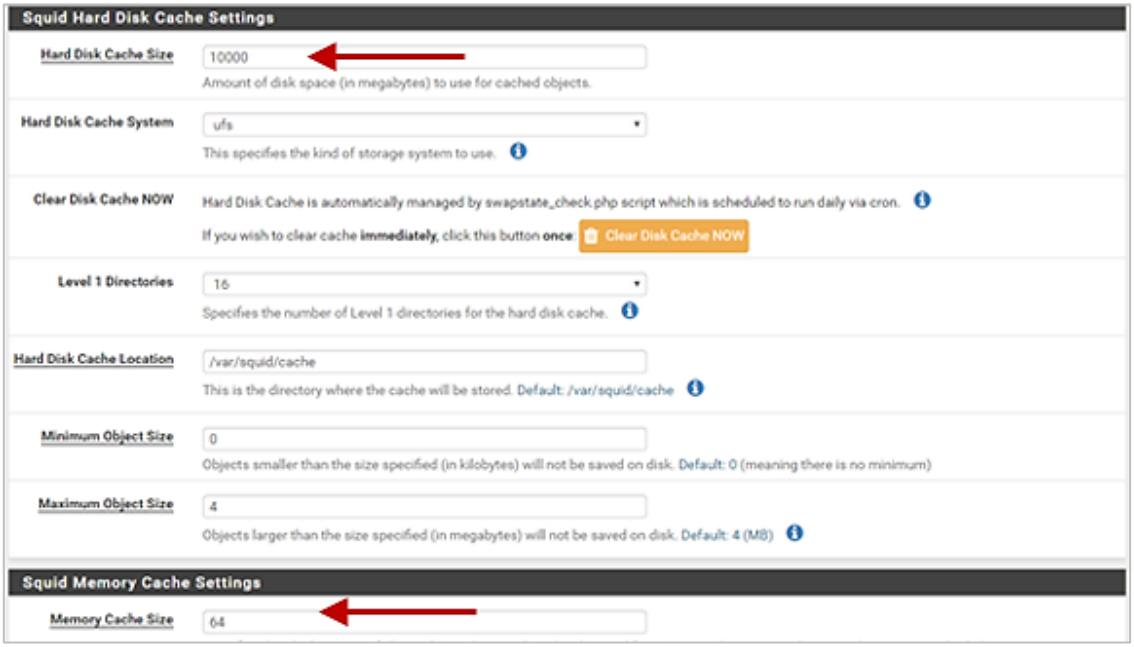
Finalmente se crea el certificado para el Servidor Proxy.

Ahora, se procede a configurar el Servidor Proxy, desde la pestaña Servicios - Proxy Server. En primer lugar, seleccionar Local Caché**,** donde se determinan los recursos utilizados o el espacio de almacenamiento reservado para la memoria caché del servidor Proxy donde se realiza lo siguiente:

- Establecer un tamaño de espacio de disco reservado para el caché.
- Establecer un tamaño para la memoria caché.
- Guardar los cambios.

Nota: Los demás campos se pueden omitir.



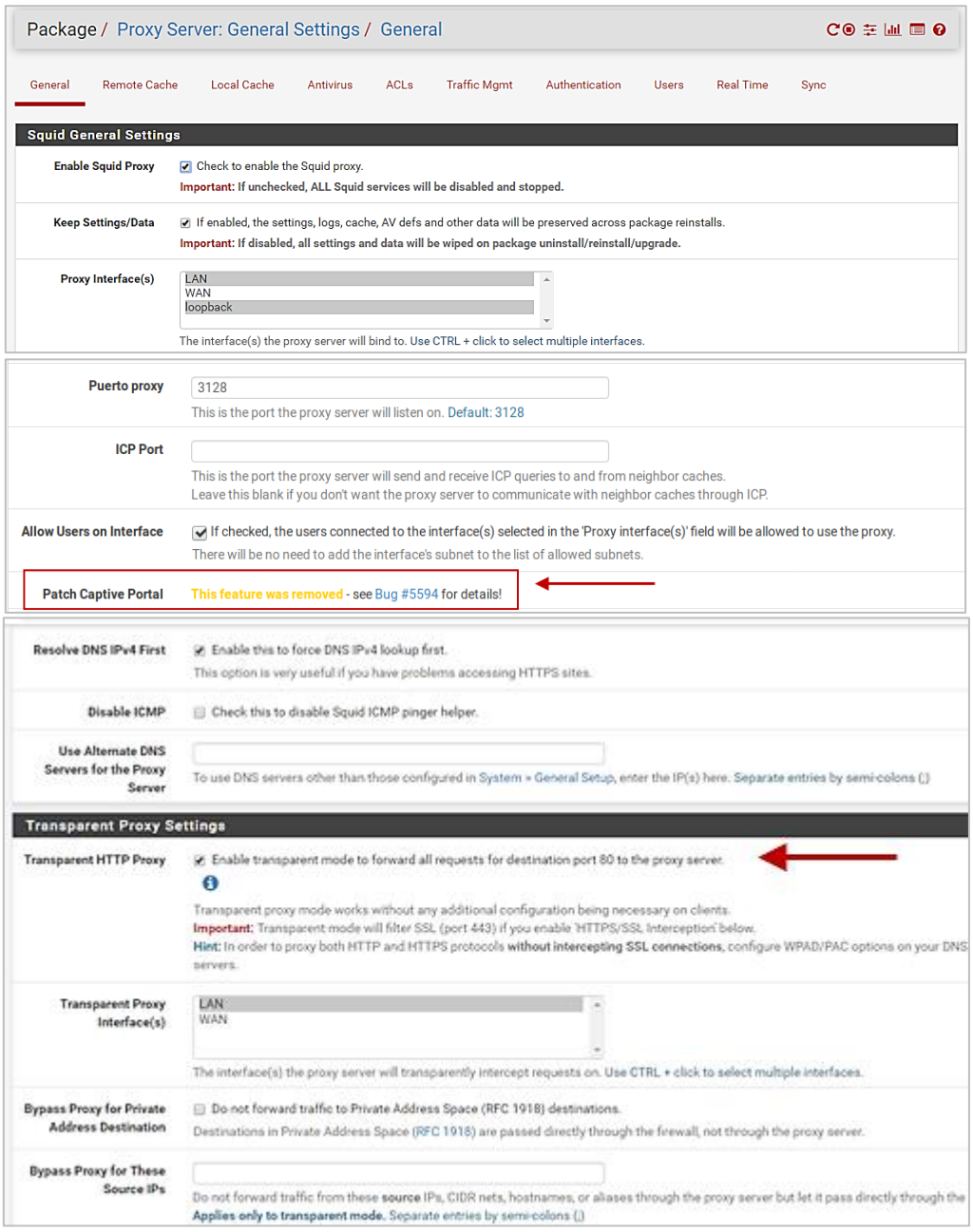


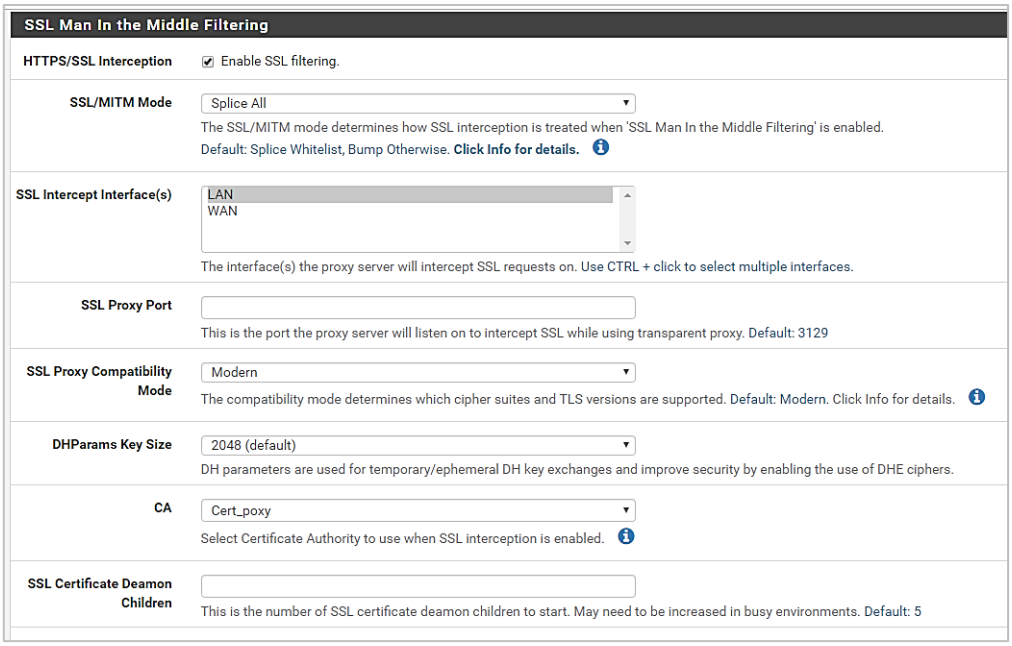
En a la pestaña General realizar las siguientes modificaciones:

- Habilitar la casilla del Servidor Proxy.
- Seleccionar las interfaces para las cuales se habilitará el Servidor Proxy.
- Habilitar la casilla de Proxy en modo Transparente.
- En la sección SSL Man in the Middle, activar la casilla “Enable SSL filtering” para filtrar contenido https.

- En la opción CA seleccionar el nombre del certificado previamente creado.
- Guardar los cambios.

  Nota: Los demás campos pueden omitirse.

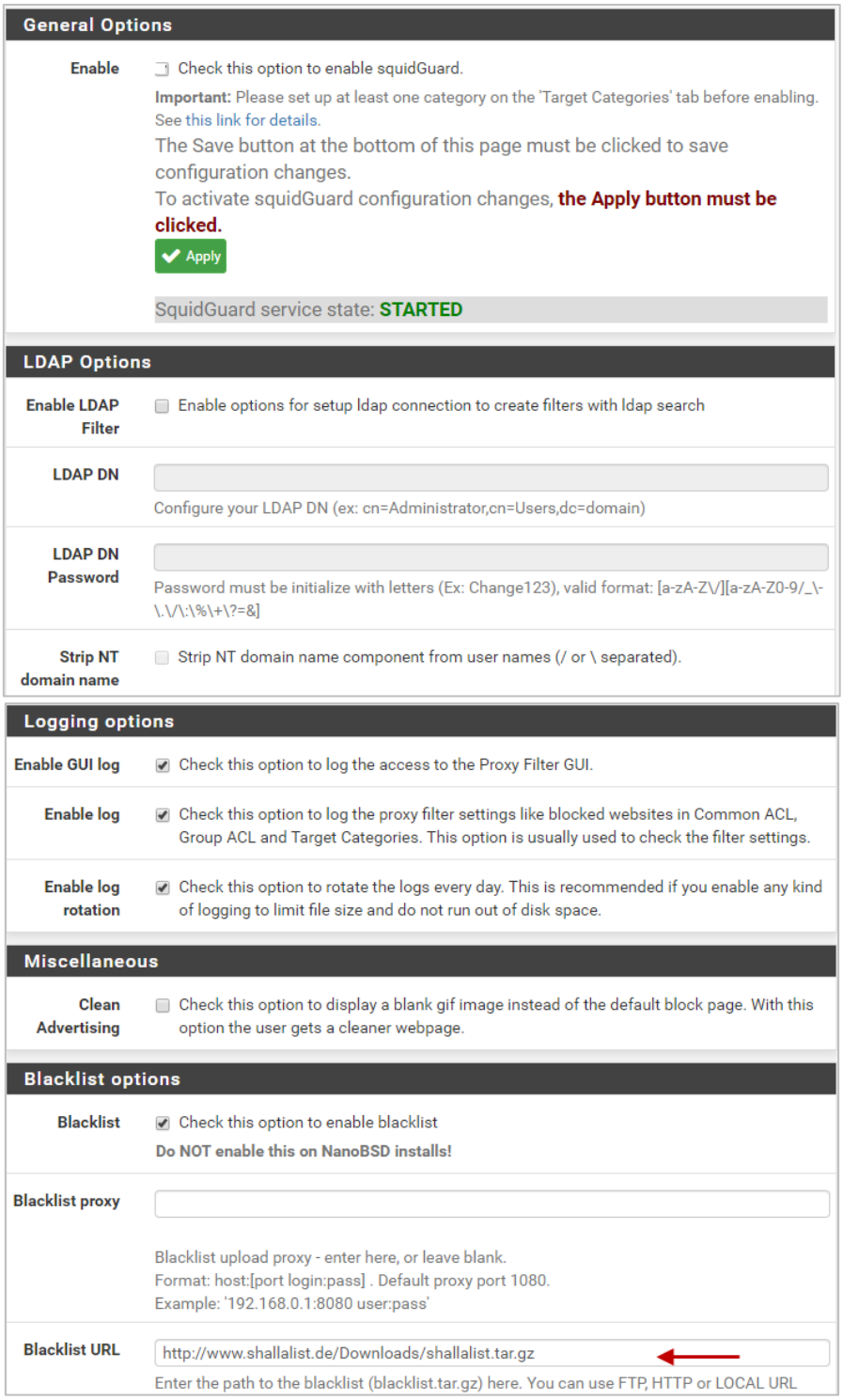




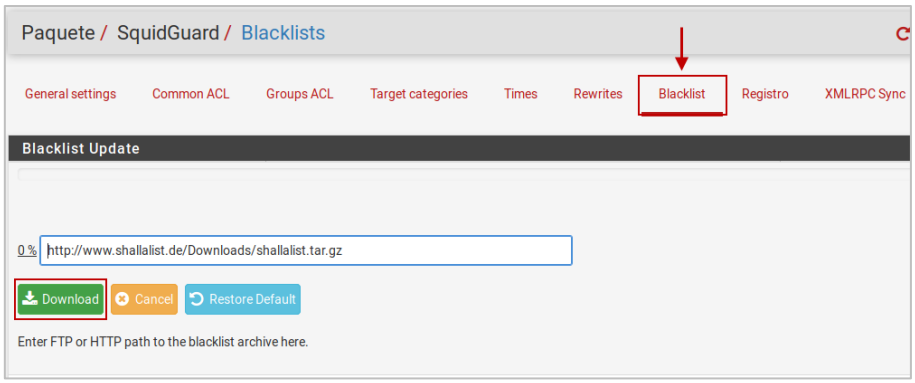
- **SquidGuard Proxy**

SquidGuard es un paquete de Pfsense capaz de filtrar contenido a través de las denominadas listas negras y blancas donde se introducen URLs o sitios web hacia los cuales se permiten o no las peticiones. En la pestaña General Settings realizar las siguientes modificaciones:

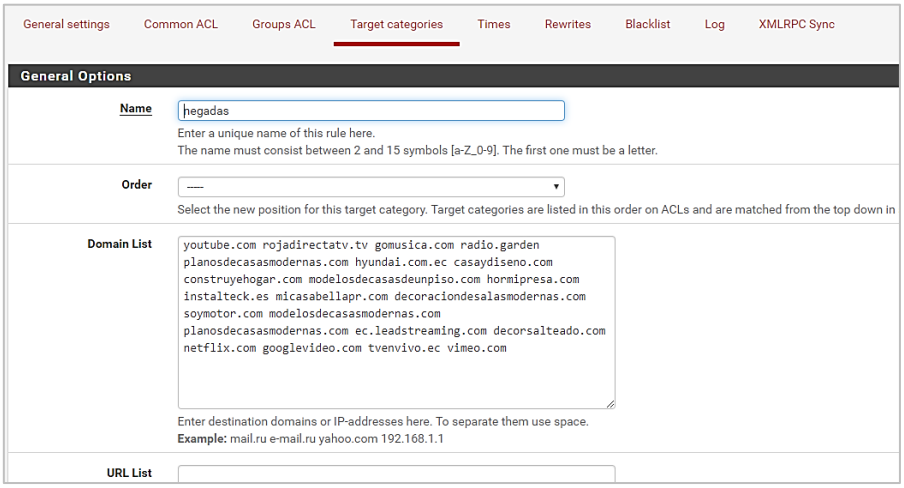
- Habilitar las casillas de la sección Loggin Options para registrar los accesos o peticiones realizadas por los usuarios.
- Antes de habilitar SquidGuard, en Blacklist Options introducir un enlace para que Pfsense descargue un grupo clasificado de sitios web pertenecientes a las listas negras: http://www.shallalist.de/Downloads/shallalist.tar.gz.
- Guardar los cambios.

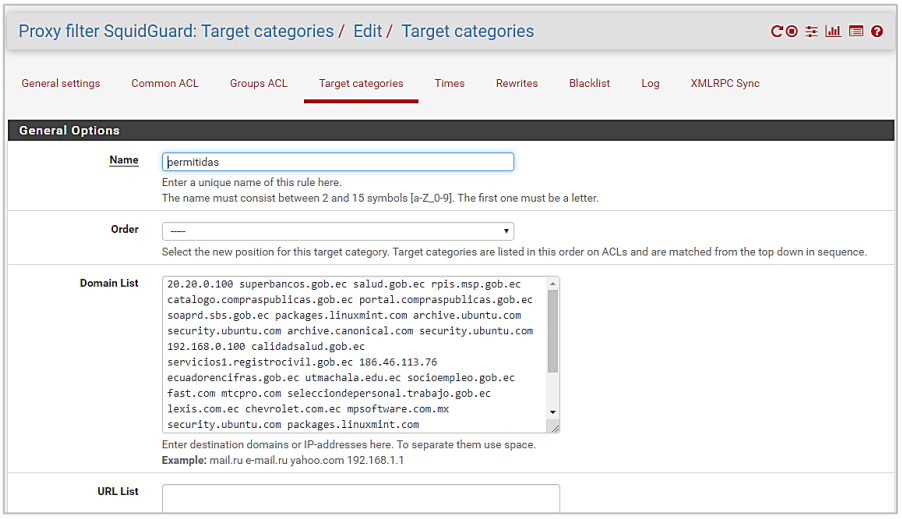


Desde la pestaña Blacklist se procede con la descarga de la lista negra.

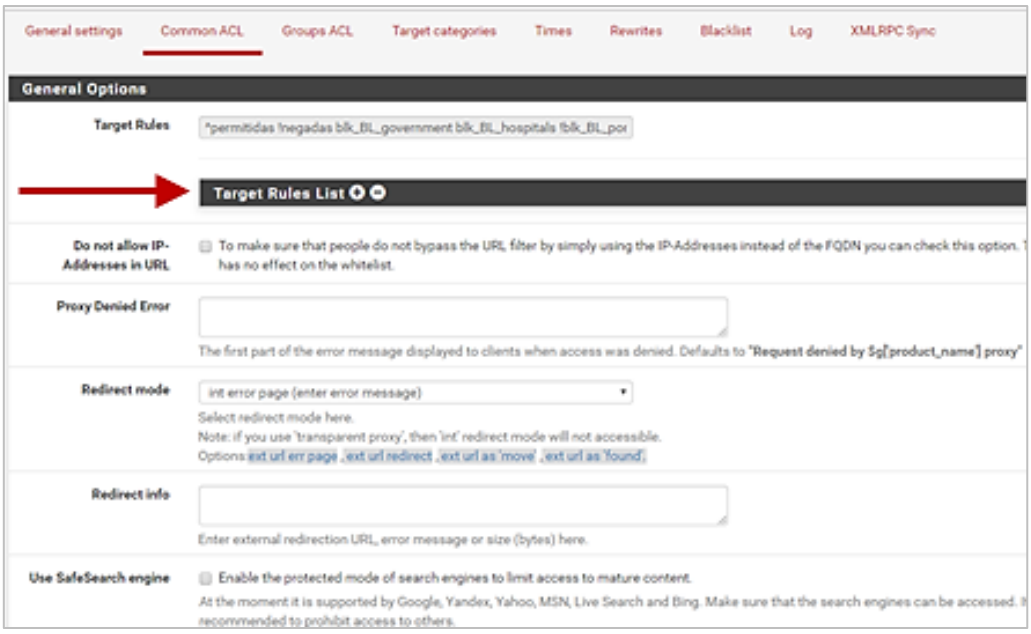


Desde la pestaña Target Categories se crearán categorías donde se añaden direcciones IP, nombres de dominio o sitios web, en este caso se crea una categoría para contenido restringido y otra para contenido permitido.

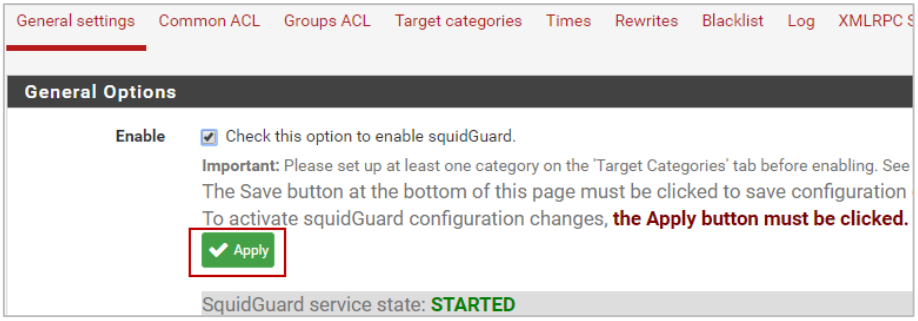




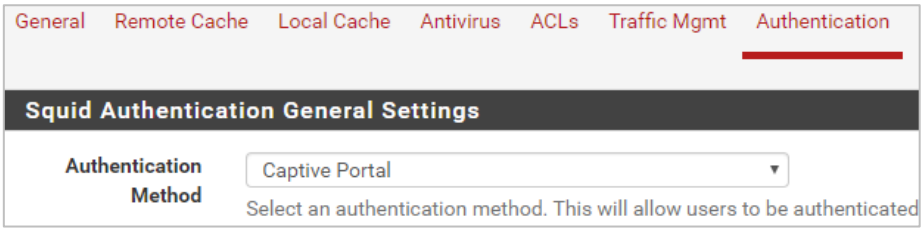
En la pestaña Common ACL se permiten o deniegan los sitios web que se descargaron a través del enlace de la lista negra.



Una vez realizados los cambios anteriormente realizados, retornar a la pestaña General Settings para habilitar SquidGuard Proxy.



Finalmente, ingresar a la configuración del servidor Proxy y en la pestaña Authentication habilitar autenticación del Proxy mediante Portal Cautivo.



Finalmente es posible visualizar el tráfico al cual accede cada usuario autenticado a través del portal cautivo en la pestaña Servicios – Proxy Server – Real Time.

Squid Access Table

Squid - Access Logs

Fecha	J	Estado	Dirección	Usuario	Destino
17.07.2019 00:25:28	192.168.1.52	TCP_TUNNEL/200	www.salud.gob.ec:443	mguajan	190.152.52.202
17.07.2019 00:25:28	192.168.1.52	TCP_TUNNEL/200	www.presidencia.gob.ec:443	mguajan	190.152.52.202
17.07.2019 00:25:07	192.168.1.52	TCP_TUNNEL/200	sgrdacaa.msp.gob.ec:443	mguajan	181.112.138.227
17.07.2019 00:25:07	192.168.1.52	TCP_TUNNEL/200	sgrdacaa.msp.gob.ec:443	mguajan	181.112.138.227
17.07.2019 00:25:07	192.168.1.52	TCP_TUNNEL/200	sgrdacaa.msp.gob.ec:443	mguajan	181.112.138.227
17.07.2019 00:25:07	192.168.1.52	TCP_TUNNEL/200	sgrdacaa.msp.gob.ec:443	mguajan	181.112.138.227
17.07.2019 00:25:07	192.168.1.52	TCP_TUNNEL/200	sgrdacaa.msp.gob.ec:443	mguajan	181.112.138.227
17.07.2019 00:25:07	192.168.1.52	TCP_TUNNEL/200	sgrdacaa.msp.gob.ec:443	mguajan	181.112.138.227
17.07.2019 00:22:47	192.168.1.52	TCP_MISS/400	http://instagram.com/favicon.ico	mguajan	192.168.10.1
17.07.2019 00:22:47	192.168.1.52	TCP_MISS/400	http://instagram.com/	mguajan	192.168.10.1

I.6 Manual de configuración del servidor Radius en Pfsense

El presente manual muestra las actividades a seguir para la implementación del método de acceso Radius de capa 2 en la red cableada e inalámbrica.

- **Descarga del paquete Radius**

En Pfsense no viene integrado Freeradius por lo cual es necesario descargar el paquete desde el menú Sistema – Gerente de empaquetación.

- **Configuración FreeRadius**

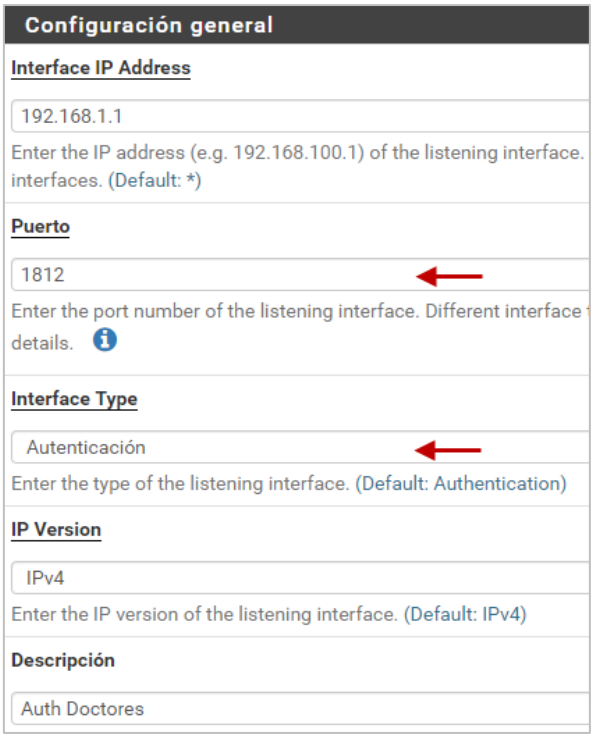
Ingresar al menú Servicios-FreeRadius-Interfaces, donde se crearán interfaces para que el servidor Radius escuche en el puerto 1812, 1813 y 1816 respectivamente,

donde se coloca en cada interfaz la dirección del Gateway de la Vlan en la cual se desea que el servidor Radius escuche.

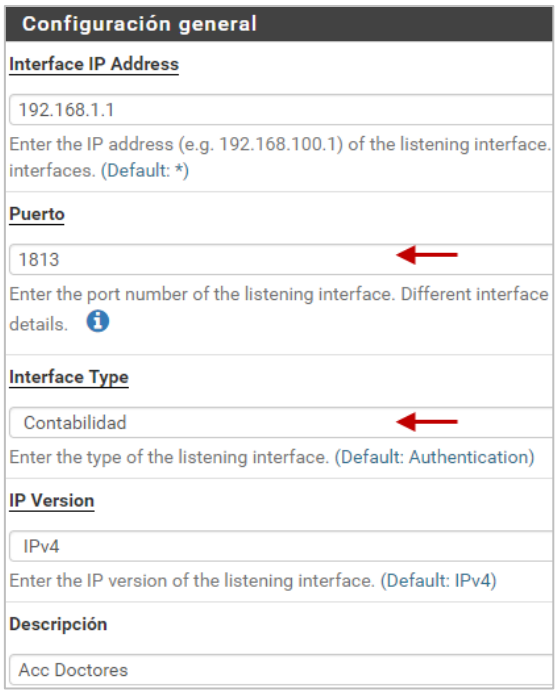
192.168.1.1	1812	auth	ipaddr	Auth Doctores	
192.168.1.1	1813	acct	ipaddr	Acc Doctores	
192.168.1.1	1816	status	ipaddr	Est Doctores	

Cada interfaz se configura de la siguiente manera.

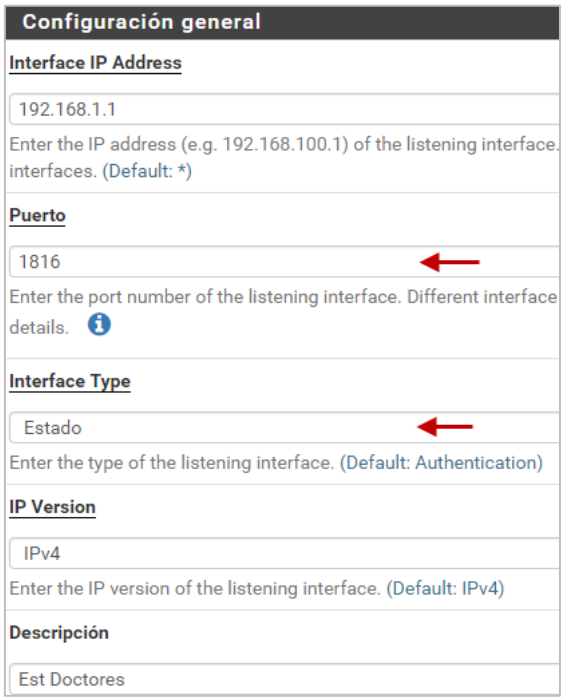
- Para la interfaz de autenticación:



- Para la interfaz de Contabilidad:



- Para la interfaz de Estado:

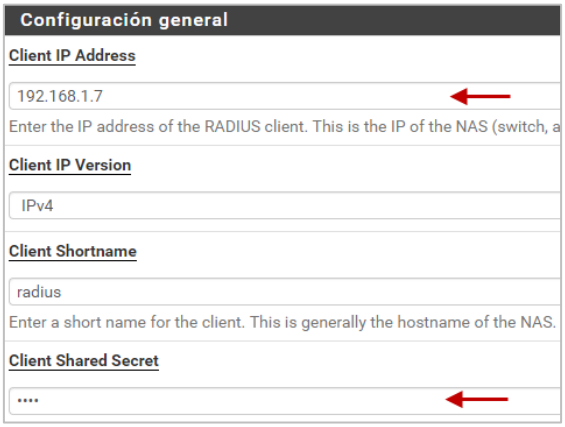


Luego, se configura un servidor NAS que corresponde a una dirección IP cualquiera del rango disponible de la Vlan

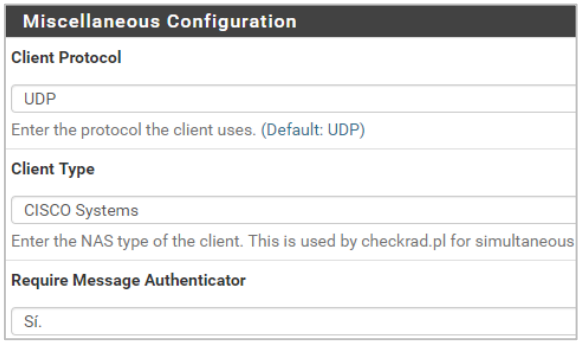
Client IP Address	Client IP Version	Client Shortname	Client Protocol	Client Type	Require Message Authenticator	Max Connections	Description	
192.168.0.3	ipaddr	radius	udp	other	no	16		
192.168.1.7	ipaddr	radius	udp	cisco	yes	16		

Se configura de la siguiente manera:

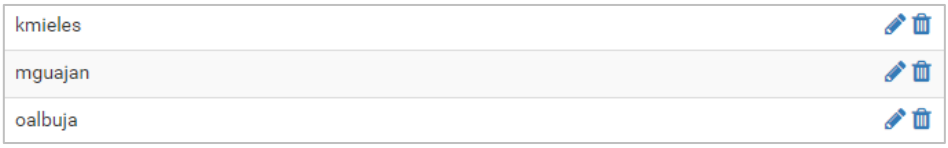
- Colocar la IP del NAS (almacenamiento conectado en red)
- Seleccionar la versión IPv4.
- Colocar un nombre al cliente NAS.
- Introducir una contraseña secreta compartida del cliente Radius, es la contraseña que el NAS (router, punto de acceso, etc.) necesita para comunicarse con el servidor Radius.



En la siguiente sección seleccionar el tipo de cliente NAS y habilitar la autenticación de mensajes en la solicitud de acceso.

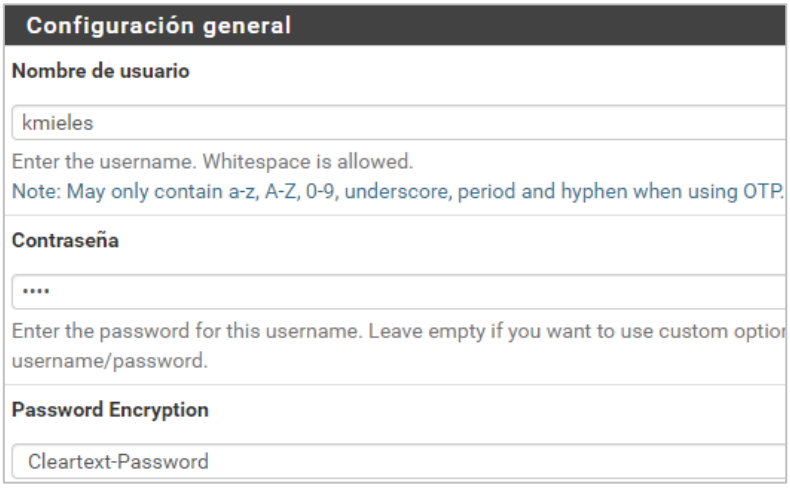


Crear usuarios para la autenticación por Radius.



Cada cliente se crea de la siguiente manera:

- Colocar un nombre
- Asignar una contraseña
- Seleccionar la encriptación en texto plano.
- Guardar.



Desde Pfsense, en el menú Servicios-Registros del Sistema-Generales es posible verificar la autenticación de los usuarios a través del servidor Radius. Este es un tipo de autenticación de capa 2 de acceso a la red.