UNIVERSIDAD CATÓLICA SANTO TORIBIO DE MOGROVEJO

FACULTAD DE INGENIERÍA

ESCUELA DE INGENIERÍA DE SISTEMAS Y COMPUTACIÓN

IMPLEMENTACIÓN DE UN SERVICIO DE RED GNU/LINUX PARA MEJORAR LA GESTIÓN DE ACCESO A LOS SERVICIOS DE RED E INTERNET PARA LAS AGENCIAS EN LAS ZONAS RURALES EN LA EMPRESA EDPYME ALTERNATIVA

TESIS PARA OPTAR EL TÍTULO DE
INGENIERO DE SISTEMAS Y COMPUTACIÓN

AUTOR

DANIEL RODOLFO PÉREZ TESÉN

ASESOR

HUILDER JUANITO MERA MONTENEGRO

https://orcid.org/0000-0001-6830-5415

Chiclayo 2020

IMPLEMENTACIÓN DE UN SERVICIO DE RED GNU/LINUX PARA MEJORAR LA GESTIÓN DE ACCESO A LOS SERVICIOS DE RED E INTERNET PARA LAS AGENCIAS EN LAS ZONAS RURALES EN LA EMPRESA EDPYME ALTERNATIVA

PRESENTADA POR:

DANIEL RODOLFO PÉREZ TESÉN

A la Facultad de Ingeniería de la

Universidad Católica Santo Toribio de Mogrovejo

para optar el título de

INGENIERO DE SISTEMAS Y COMPUTACIÓN

APROBADA POR**:**

Marlon Eugenio Vílchez Rivas
PRESIDENTE

Héctor Zelada Valdivieso
SECRETARIO

Huilder Juanito Mera Montenegro
ASESOR

DEDICATORIA

“Para mi esposa Maribel e hijas Angell y Daniela, porque gracias a ellas he ido logrando mis metas y objetivos paso a paso y, nunca han dejado de demostrarme su cariño, aliento y comprensión.”

“Para mis queridos padres Antonio y Aquilina y mis hermanos que siempre me han apoyado y aconsejado para no renunciar ante las adversidades.

EPIGRAFE

"Si quieres ser sabio, aprende a interrogar razonablemente, a escuchar con atención, a responder serenamente y a callar cuando no tengas nada que decir"

Jhon Wolfang Goethe

"La inteligencia consiste no sólo en el conocimiento, sino también en la destreza de aplicar los conocimientos en la práctica"

Aristóteles

AGRADECIMIENTOS

“A Dios todopoderoso, porque sin él nada soy y con él todo lo puedo.

A la empresa Edpyme Alternativa, en representación del Sr. Fernando Bautista, por darme la oportunidad de aplicar este proyecto, y a nuestro asesor por darnos el tiempo necesario para realizar esta tesis.

RESUMEN

El presente trabajo de investigación tiene como objetivo principal mejorar la gestión y optimizar los recursos de red e internet para las zonas semi rurales y rurales de la empresa Edpyme Alternativa, entidad financiera dedicada a prestar servicios y productos micro financieros para la pequeña y micro Empresa, usando para ello infraestructura tecnológica y herramientas GNU/LINUX, para mantener la continuidad operativa y que está al alcance de las necesidades de la empresa

La estrategia de Edpyme Alternativa, para los siguientes tres años reposa sobre tres pilares fundamentales: crecimiento rural y consolidación urbana, fortalecimientos de procesos y sistemas de control y fortalecimiento del equipo de trabajo.

Teniendo en cuenta estas estrategias es que Edpyme alternativa en su afán de expandir nuevos mercados financieros en las zonas rurales y con ello apoyar con la formalización y desarrollo de micro empresas, expande su nicho de mercado hacia estas zonas donde los proveedores grandes de servicios de internet local como Claro, Bitel y Telefónica del Perú, no cuentan con una infraestructura como del tipo de redes tipo MPLS o privadas y solo cuentan con acceso a Internet público. Estas sedes se vuelven vulnerables ante la amenaza de los piratas informáticos que utilizan diferentes métodos de sabotaje para intentar encontrar equipos desprotegidos.

La implementación de este servicio de red, se realizó en base a los indicadores de crecimiento y disponibilidad de los servicios informáticos que tiene Edpyme alternativa, por el cual se realizó la recolección de datos con el propósito de conocer el proceso de otorgamiento de créditos y cuáles eran sus limitaciones y situación problemática que afrontaba en estas zonas semi rurales y rurales.

El trabajo de investigación permitió demostrar que la variable crecimiento de cartera y costos operativos calculados por mes se puede mejorar implementando el servicio de red GNU/LINUX para mantener la continuidad operativa y ayudar a alcanzar las metas y objetivos de Edpyme Alternativa.

PALABRAS CLAVE:
GNU/LINUX, costos operativos, Red privada MPLS.

ABSTRACT

The main objective of this research work is to improve management and optimize network and internet resources for semi-rural - rural areas of the company Edpyme Alternative, a financial entity dedicated to providing micro-financial services and products for small and micro companies. using technological infrastructure and GNU / LINUX tools, to maintain operational continuity and that is within the reach of the company's needs

The strategy of Edpyme Alternative, for the next three years rests on three fundamental pillars: rural growth and urban consolidation, strengthening of processes and control systems and strengthening of the work team.

Considering these strategies is that Edpyme alternative in its eagerness to expand new financial markets in rural areas and thereby support with the formalization and development of micro enterprises, expands its niche market to these areas where large local internet service providers such as Claro, Bitel and Telefonica In Peru, they do not have an infrastructure such as MPLS or private networks and only have public Internet access. These venues become vulnerable to the threat of hackers using different sabotage methods to try to find unprotected computers.

The implementation of this network service, was based on the indicators of growth and availability of computer services that has alternative Edpyme, by which the data collection was carried out in order to know the process of granting credits and which were its limitations and problematic situation that faced in these semi-rural and rural areas.

The research work showed that the variable portfolio growth and operating costs calculated per month can be improved by implementing the GNU / LINUX network service to maintain operational continuity and help achieve the goals and objectives of Edpyme Alternative.

KEYWORDS:
GNU / LINUX, operating costs, MPLS private network.

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

I. INTRODUCCIÓN

En el mundo globalizado, la inclusión financiera es un factor clave para reducir la pobreza e impulsar la prosperidad de las naciones, es por ello que significa, para personas y empresas, tener acceso a productos financieros que satisfagan sus necesidades y que sean prestados de manera responsable y sostenible.

De acuerdo a la información del GBM (Grupo Banco Mundial) [1], la inclusión financiera se está convirtiendo en una prioridad para el desarrollo a nivel mundial, es por esta razón que el Grupo de los Veinte (G-20) se comprometió a promover la inclusión financiera en todo el mundo y reafirmó su compromiso de aplicar los principios de alto Nivel del G-20 para la Inclusión Financiera Digital. Desde el 2010, más de 55 países se han comprometido a implementar la inclusión financiera, y más de 30 de ellos han puesto en marcha o están preparando una estrategia nacional al respecto. Las investigaciones realizadas en el GBM indican que el ritmo y el impacto de las reformas aumentan cuando un país aplica una estrategia nacional de inclusión financiera. Los países que han logrado más avances con miras a la inclusión financiera son los que han creado un entorno normativo y reglamentario propicio, y han fomentado la competencia permitiendo a las instituciones bancarias y no bancarias innovar y ampliar el acceso a servicios financieros. Sin embargo, la creación de este espacio innovador y competitivo debe ir acompañada de reglamentaciones y medidas de protección del usuario apropiadas para garantizar la prestación responsable de servicios financieros. Es decir, garantizar que el acceso y los servicios financieros lleguen a las poblaciones difíciles de alcanzar, como las mujeres y los pobres de las zonas rurales.

Esta inclusión facilita que las instituciones financieras puedan llegar a los segmentos que tradicionalmente han sido desatendidos por la banca tradicional. Esto es particularmente importante para las Edpyme, que atienden a clientes de bajos ingresos, pero que realizan transacciones con mayor frecuencia y administran montos de dinero más bajos.

De acuerdo a la información publicada por banco mundial [1], en México el gobierno ha dado prioridad a la inclusión financiera, herramienta crucial para reducir la pobreza y promover la prosperidad compartida, esto ha sido uno de los principales desafíos de cara al desarrollo. En 2011, alrededor de 71 millones de mexicanos, 65% de una población total de 112 millones, carecía de acceso a un servicio financiero formal, tema especialmente crítico en áreas rurales, donde 78% de los municipios no tenía un solo punto de servicios para residentes que quisieran realizar un depósito, retirar dinero, consultar saldo s o realizar pagos. Apenas 13,6% de la población adulta tenía una cuenta de ahorro formal en contraste con el 33,6% de promedio regional. Asimismo, y particularmente en áreas rurales, un número significativo de prestadores de servicios disponibles operaban entidades de ahorro y crédito no autorizadas ni reguladas. Sin garantías de depósito los ahorros en estas entidades estaban en riesgo y solo ofrecían acceso limitado a servicios financieros apropiados e idóneos.

En el ámbito nacional [2] tal como lo indica un estudio sobre inclusión financiera elaborado por la SBS, La inclusión social es una de las prioridades del Estado Peruano y en el logro de este objetivo, la inclusión financiera constituye un instrumento clave, en la medida que conlleva una serie de beneficios para quienes pueden acceder y usar los servicios financieros. Entre otras ventajas, la inclusión financiera permite a la población mayor eficiencia y eficacia en la realización de sus transacciones financieras, en el financiamiento de sus actividades productivas,

en la administración de sus recursos y en la gestión de los riesgos que enfrentan. Por ello, y ante la necesidad de articular las políticas y acciones desplegadas por diversas instancias del Estado en favor de la inclusión financiera, en febrero de 2014, se constituyó formalmente la Comisión Multisectorial de Inclusión Financiera. A nivel nacional en la zona urbana, el grado de conocimiento de los canales de atención del sistema financiero es alto: alrededor de 93% de la población señaló conocer las oficinas, 82% afirmó conocer los cajeros automáticos y 78% los agentes, pero se reduce en el ámbito rural, sobre todo en el caso de los cajeros automáticos y agentes. A pesar de que los agentes han sido el canal que más se ha expandido en los últimos años, solo 40% de la población en el ámbito rural señaló conocerlos, lo que reflejaría la baja penetración y poca difusión de este canal en dicha zona.
En relación al acceso a los créditos del sistema financiero, el 14% de la población a nivel nacional solicitó al menos un crédito en alguna institución financiera durante el 2014 (ver Gráfico N°01). Dicho porcentaje se reduce a 11% en el ámbito rural y a 10% en el grupo más pobre. Por el contrario, se eleva a 15% en el ámbito urbano, principalmente por el mayor porcentaje de la población que solicitó al menos un crédito del Sistema Financiero en las grandes ciudades urbanas.

Para nuestro proyecto de tesis, se presenta a la empresa Edpyme Alternativa, que es una entidad financiera para la pequeña y micro empresa y que es supervisada por la Superintendencia de Banca, Seguros y AFP, y en su afán de crecimiento sostenido y del logro de sus objetivos institucionales, ha expandido con énfasis su mercado en las zonas semi rurales y rurales de la zona Nororiente, donde el acceso al crédito por parte de las grandes financieras nacionales y extranjeras es casi nulo. A razón de esta problemática es que esta afrontado el reto de incluir a los pobladores de estas zonas lejanas rurales que trabajan en el ámbito de la pequeña empresa, agricultura, ganadería, apicultura, etc.

Conociendo estas realidades a nivel internacional y nacional para lograr este objetivo las gerencias respectivas vienen implementando nuevas agencias y oficinas informativas para atender y promover la formalización de las pymes mediante el acceso al crédito en las zonas rurales. Es en estas zonas donde el medio de acceso a una plataforma tecnológica de red segura (MPLS o redes privadas) que permitan acceder a los sistemas de información de la institución son inviables, debido al alto costo de implementación por parte de los proveedores de servicios. Cabe precisar que en estas zonas solo se encuentra tecnología inalámbrica, como radio enlaces, VSAT e internet del tipo hogar.
Así mismo para que el personal de créditos pueda alcanzar sus metas y objetivos de crecimiento de cartera necesitan información en línea, tales como filtros, reportes de deudas, tipos de negocio, estimaciones de crecimiento tanto a nivel de agricultura como ganadería. Por lo cual usan la información proporcionada en internet y la red de datos de acceso al sistema para realizar evaluaciones correctas, descartando operaciones inusuales como es el lavado de activos y así mitigar la morosidad y reducir las provisiones por mala calidad de cartera que se pueda presentar en estos créditos.
Uno de los problemas más comunes es el indebido uso que se le da a la tecnología existente en estas sedes, como es el uso de los computadores y el acceso a internet, los colaboradores de Edpyme alternativa tienen la libertad de aprovechar la tecnología en favor de sus objetivos, pero muchas veces se realizan de manera

inapropiada o indebida. Sumado a esto el no tener acceso a los sistemas informáticos de la institución.

Es conocido que conectarse a internet y acceder a una red de datos en un entorno empresarial sin un servidor de seguridad incrementa la vulnerabilidad de la información lo que provoca pérdidas económicas como de reputación, es por ello que un servidor de seguridad mitiga el riesgo y protege la integridad de la información.

Actualmente en estas zonas la conexión a internet se realiza directamente con un equipo de comunicación de datos "DCE" (Modem Router) del proveedor de servicios, sin la ayuda de un servicio de seguridad que sirva de intermediario entre el DCE y la red local, la cual estamos expuestos a carencia de controles de acceso a la web y sus contenidos, lo que ocasionan el uso e instalaciones indiscriminadas de contenidos dañinos para el tráfico de red, falta de administración y gestión adecuada de contenidos, al no contar con un servidor de seguridad en estas zonas se incrementa la vulnerabilidad de los sistemas de información.

Lo indicado anteriormente dificulta el logro de los objetivos que se encuentran detallados dentro del plan estratégico Anual 2019-2020 de la Edpyme Alternativa y que es de conocimiento de todo el personal de la institución

Por lo antes mencionado en la presente tesis se ha planteado la siguiente formulación del problema ¿De qué manera se podría mejorar la gestión de acceso a la red de datos e Internet, para las agencias en zonas rurales de la empresa Edpyme Alternativa?, en el desarrollo de la misma se ha determinado que se demostrará el alcance de la propuesta a través de la hipótesis que indica que con la implementación de un servicio de red GNU/Linux, se mejorara la gestión de acceso a la red e internet reflejada en la reducción del índice de morosidad por debilidad en filtros y otros indicadores necesarios para el otorgamiento de un crédito.

Para esta tesis se ha planteado como objetivo general la implementación de un servicio de red GNU/Linux para mejorar la gestión de acceso a los servicios de red e internet para las agencias en las zonas rurales en la empresa Edpyme alternativa y para la contrastación de la hipótesis se ha planteado los siguientes objetivos específicos como:

- Reducir gradualmente el índice de morosidad, reflejado en un menor deterioro de la cartera de créditos.
- Reducir el importe provisionado por cartera morosa, lo que permitirá un mayor importe en ingresos.
- Reducir los costos operativos, principalmente los generados por los préstamos en situación de morosidad y el depender de una sede remota para el crecimiento de estas sedes rurales.
- Incrementar la rentabilidad de la empresa (ROE) reflejado en la mejora de indicadores mensuales de rentabilidad.

Esta investigación se respalda en el logro social ya que con el uso de herramientas GNU/LINUX facilita el acceso a los servicios de información para el personal de la empresa lo que a su vez permitirá brindar un mejor servicio a los clientes. Por otro lado, el desarrollo de este proyecto abre la posibilidad de desarrollar nuevos productos no financieros como son las ventas de seguros, SOAT, pago de servicios básicos como Luz, agua, teléfonos, transacciones, giros, etc.

La tecnología usada permitirá mejorar el proceso de negocios logrando la disponibilidad de la información en el momento oportuno. En el aspecto

económico consideramos que el proyecto es viable desde este punto debido a que no se requerirá una mayor inversión en la adquisición de equipos de última generación, siendo solo necesario que el equipo cuente con la capacidad necesaria de hardware para instalar la aplicación. Por otro lado, el uso de software libre en el desarrollo de la solución no representará inversión en compra de licencias. Este proyecto incidirá en mejorar la gestión de acceso a los recursos de red de la institución. Como resultado de esta mejora se proyecta la reducción de indicadores de mora lo que a su vez repercutirá en la disminución de provisiones y gastos operativos reflejados en el incremento de utilidades.

II. MARCO TEÓRICO

2.1 ANTECEDENTES DE LA INVESTIGACIÓN

Antecedente # 01: Según Molina [3], el principal problema de la empresa editora El comercio planta Norte, en la ciudad de Chiclayo, se basaba principalmente en un desorden de la aplicabilidad de los recursos de la red, lo que hacía que sus procesos se vean interrumpidos constantemente generando demoras en sus operaciones y por consecuencia pérdida de tiempo y elevación de costos operativos, para ello se planteó la propuesta de la Segmentación de redes virtuales y la priorización del ancho de banda con QOS para la mejora del rendimiento y mejorar la seguridad en la red LAN.
Para realizar este proyecto Molina, hace un inventario inicial de los equipos de comunicación existentes y redefine la nueva segmentación de la red, dando prioridad a las áreas principales, instala cortafuegos y prioriza el ancho de banda haciendo más productiva la red LAN. Así mismo se ha Implementado mecanismos para autenticación de los accesos a servicios y recursos de red a través de roles y perfiles de usuario, como RADIUS que trabaja con Active Directory, lográndose un mejor nivel de seguridad, dado que los filtros son más rigurosos gracias a las capas de seguridad que brinda este protocolo.
Con estas acciones el logro obtenido es mejorar los recursos de red, haciendo un tráfico más seguro y ahorro en costos operativos.

Antecedente # 02: Según [4], la principal problemática de la empresa TERRACARGO S.A.C., era el aislamiento que tenían entre la oficina principal y las sucursales, ya que los procesos eran manuales y no se obtenía información en línea, siendo una desventaja tanto para para los colaboradores como para los usuarios.
Para ello se ha implementado un diseño de la una red VPN para unir la sede principal con las sedes remotas a través de mecanismos de seguridad que brinden seguridad, disponibilidad e integridad de los sistemas informáticos. Para ello hace una investigación del mejor protocolo y del tipo de VPN a usar, usando software libre como principal soporte.
Con este proyecto usando software libre el costo de la implementación tenía un bajo costo, considerando el crecimiento de esta empresa y logrando los objetivos esperados.

Antecedente # 03: Según [5] , en su tesis de la universidad del Altiplano en Puno, nos muestra un modelo de sistema criptográfico de seguridad para las redes de comunicaciones, con la finalidad de asegurar la confidencialidad de las redes de comunicaciones, ya que las mimas estaban expuestas a riesgos como denegación de servicios, observación y modificación no autoriza, para ello se basó en herramientas VPN de software libre VPN, usando protocolos SSL con autentificación certificada entre cliente y servidor mediante un algoritmos de criptografía asimétrica.
Con estos modelos se puede tener un alcance de los diferentes protocolos y la forma de diseñar una criptografía segura para la transmisión de datos por las redes.
Con este proyecto se planteó como objetivo fundamental “Modelar el sistema criptográfico de seguridad para las redes de comunicaciones” para proteger y tomar medidas de seguridad restringiendo los datos, cumpliendo con las

políticas de seguridad, mecanismos consistentes y las prácticas que lo regulan.

Antecedente # 04: Según [6], en su investigación de tesis Repotenciación de un sistema Firewall de código abierto, hacen un análisis de los diferentes protocolos y tipos de VPN.
Así mismo hace la elección del software libre ClearOs, PFsense y Zentyal, con la finalidad de probar su funcionalidad y reforzar la detección y control de las vulnerabilidades que pueden estar expuestas y que pueden ser usadas en las instituciones públicas como privadas.
De acuerdo a la evaluación de los resultados se ha podido determinar que el desempeño de cada uno de los firewalls de software libre, es directamente proporcional a la aplicabilidad que se necesita. Dentro de este análisis se ha logrado dar una mejor puntación a la herramienta ClearOS de RED HAT y que es comparable con Zentyal de la distro Debian.
Luego de haber seleccionado esta herramienta ClearOS, realiza un análisis para repotenciar este firewall y realizando las recomendaciones necesarias para instalar esta herramienta.

2.2 BASES TEÓRICO CIENTÍFICAS

2.2.1 GNU/LINUX.

El proyecto GNU/LINUX se inicia con el principal objetivo de crear un sistema operativo completamente libre, fue diseñado para ser totalmente compatible con UNIX. El término GNU proviene de «GNU No es Unix». Se pronuncia en una sola sílaba: ñu.
Su creador Richard Stallman escribió el anuncio inicial del Proyecto GNU en setiembre de 1983 una versión extendida denominada el Manifiesto de GNU y fue publicada en setiembre de 1985 siendo traducido a diversos idiomas.

2.2.1.1 SOFTWARE LIBRE.

De acuerdo a la publicación en internet [7] para asegurar que el software GNU permaneciera libre para que los usuarios pudieran "Ejecutarlo, Copiarlo, Modificarlo y Distribuirlo", el proyecto debía ser liberado bajo una licencia diseñada para garantizar esos derechos al tiempo que evitase restricciones posteriores de los mismos. La idea se conoce en Ingles como copyleft 'copia permitida' (en clara oposición a copyright 'derecho de copia') y está contenida en la Licencia General Publica de GNU (GPL). Stallman introdujo la definición de free software (software libre) que desarrollo para otorgar libertad a los usuarios y para restringir las posibilidades de apropiación del software.
El software libre da la libertad de los usuarios de ejecutar, copiar, distribuir, estudiar, cambiar y mejorar el software. Explícitamente se refiere a cuatro tipos de libertades para los usuarios del software:

- La libertad de ejecutar el programa, para cualquier propósito (libertad 0).
- La libertad de estudiar cómo trabaja el programa, y adaptarlo a sus necesidades (libertad 1). El acceso al código fuente es una condición necesaria.

- La libertad de redistribuir copias para que pueda ayudar al prójimo (libertad 2).
- La libertad de mejorar el programa y publicar sus mejoras y versiones modificadas en general, para que se beneficie toda la comunidad (libertad 3). El acceso al código fuente es una condición necesaria.

2.2.1.2 CATEGORÍAS.

Como se menciona en la publicación de internet gnu.org **[8]**. Existen las siguientes categorías.

- **Software de fuente abierta 'Open Source'.** Es el término con el que se conoce al software distribuido y desarrollado libremente. Fue utilizado por primera vez en 1998 por algunos usuarios de la comunidad del software libre, tratando de usarlo como reemplazo al ambiguo nombre original en inglés del software libre (free software). Open Source se centra en el potencial de realización de software de alta calidad, pero esquiva las ideas de libertad, comunidad y principio. Es un movimiento más pragmático, se enfoca más en los beneficios prácticos como acceso al código fuente que en aspectos éticos o de libertad que son tan relevantes en el Software Libre. Su premisa es que, al compartir el código, el programa resultante tiende a ser de calidad superior al software propietario, es una visión técnica. Obviamente para lograr calidad técnica lo ideal es compartir el código, pero no estás obligado a hacerlo.
- **Software de dominio público.** El software de dominio público es aquel que no tiene derechos de autor (no está protegido con copyright), Lo que significa que algunas copias o versiones que se han modificado pueden no ser libres en absoluto. El termino Dominio público es un término legal cuyo significado se precisa "sin copyright, sin derechos de autor".
- **Software protegido con copyleft.** El software protegido con copyleft es software libre cuyos términos de distribución garantizan que las copias tengan el mismo término de distribución, es decir que no se permiten a los desarrolladores agregar algunas modificaciones adicionales cuando estos redistribuyen o modifican el software. Esto significa que cada copia del software, aun si ha sido modificado, debe ser software libre. Esto protege el programa y sus versiones modificadas contra algunas de las formas más comunes de convertirlo en software privativo.
- **Software libre no protegido con copyleft.** El software libre no protegido con copyleft viene desde el autor con autorización para redistribuir y modificar, así como para añadirle restricciones adicionales. Si un programa es libre pero no tiene copyleft, es posible que

algunas copias o modificaciones no sean libres en absoluto. Una empresa de software puede compilar el programa, con o sin modificaciones, y distribuir el archivo ejecutable como software privativo. Un ejemplo de ellos es el Sistema X Windows.

- **Software GNU.** Software GNU es software que es liberado bajo el auspicio del Proyecto GNU. La mayoría del software GNU está protegido con copyleft, pero no todos; sin embargo, todo el software GNU debe ser software libre.
- **Software propietario.** El software propietario es software que no es libre. Su uso, redistribución o modificación está prohibida, o requiere que se solicite autorización o esta tan restringida que no pueda hacerla libre de un modo efectivo.
- **Freeware.** El término freeware no tiene una definición claramente aceptada, pero se usa generalmente para referirse a paquetes en los cuales se permite la redistribución, pero no la modificación (y su código fuente no está disponible). Estos paquetes no son software libre.
- **Shareware.** El término shareware se refiere al software del que se permite redistribuir copias, pero quien continúa a utilizar una copia debe pagar para obtener la licencia. El software shareware no es software libre, ni siquiera semi libre, por dos razones: Para la mayoría de los programas shareware, el código fuente no está disponible, por lo tanto, no se pueden modificar. El software shareware no viene con permiso para hacer una copia e instalarlo sin pagar la licencia, ni siquiera para las personas que participan en actividades sin fines de lucro. En la práctica, los usuarios suelen ignorar los términos de distribución y lo hacen de todos modos, aunque las condiciones no lo permiten.
- **Software comercial.** El software comercial es software que está siendo desarrollado por una entidad que tiene la intención de generar ganancias económicas mediante el uso del software. Comercial y propietario no son equivalentes. La mayoría del software comercial es propietario, pero hay software libre comercial y hay software no libre no comercial. Por ejemplo, GNU Ada fue desarrollado por una empresa. Se distribuye siempre bajo los términos de la GNU GPL, y cada una de las copias es software libre, pero los desarrolladores venden servicios de soporte. Cuando los vendedores hablan con los posibles clientes, estos a veces dicen, «Nosotros nos sentiríamos más seguros con un compilador comercial». Los vendedores responden, «GNU Ada es un compilador comercial, aunque sea software libre».

2.2.1.3 LICENCIAS.

Existen 3 tipos de licencias de software libre:

- **Licencia pública general de GNU (GPL).** La Licencia Pública General de GNU, llamada comúnmente GNU GPL, la usan la mayoría de los programas de GNU y más de la mitad de las aplicaciones de software libre. El texto de la Licencia Pública General de GNU está en cuatro formatos: HTML, texto plano, Texinfo y LaTeX. Estos documentos no están maquetados para publicarlos por sí solos, sino que están pensados para ser incluidos en otro documento.
- **Licencia pública general reducida de GNU (LGPL).** La Licencia Pública General Reducida de GNU la usan algunas, pero no todas, las bibliotecas GNU. Esta licencia fue llamada en un principio GPL para bibliotecas, pero le cambiamos el nombre debido a que animaba a la gente a emplear esta licencia más de lo debido. El texto de la Licencia Pública General Reducida de GNU, está en tres formatos: HTML, texto plano y Texinfo.
- **Licencia de documentación libre de GNU.** La Licencia de Documentación Libre de GNU es una forma de copyleft para ser usada en un manual, libro de texto u otro documento que asegure que todo el mundo tiene la libertad de copiarlo y redistribuirlo, con o sin modificaciones, de modo comercial o no comercial. El texto de la Licencia Libre de Documentación de GNU está en tres formatos: HTML, texto plano, Texinfo y LaTeX. Estos documentos no están maquetados para publicarlos por sí solos, sino que están pensados para ser incluidos en otro documento.

2.2.1.4 IMPACTO DEL SOFTWARE LIBRE EN LAS ENTIDADES DEL ESTADO.

Según el INEI [9], en la actualidad, la mayoría de las aplicaciones del software se han centrado en ambientes empresariales, la popularización del uso del internet ha obligado a los países a aplicar estas tecnologías en ambientes de tipo social como la Educación, la sistematización de las empresas del gobierno, los manejos de comunidades remotas, el comercio, etc. Todo esto tendrá un impacto enorme en la sociedad debido a que la masificación es de grandes proporciones.

Razones que han generado el impacto de GNU/LINUX:

- El sistema operativo GNU/LINUX nos permite con libertad ejecutar el programa, con cualquier propósito. Modificar el programa para adaptarlo a sus necesidades, redistribuir copias, distribuir versiones modificadas del programa. De tal manera que la comunidad pueda beneficiarse con sus mejoras.
- Como solución económica, rentable, poderosa, estable, robusta y segura. permite aplicar estas tecnologías en todo tipo de organizaciones. La masificación es de grandes proporciones.

- Grandes empresas fabricantes de hardware y software vienen adaptando software libre a sus productos, garantizando a nivel mundial su uso. Tales como IBM, Compaq, Intel, entre otras.
- Desde el punto de vista educativo, el desarrollo de sistemas informáticos utilizando software libre permitirá crear una base de desarrolladores de aplicaciones y herramientas GNU/LINUX, y con el apoyo de las universidades se crearía una sinergia muy importante.

2.2.1.5 LICENCIA PÚBLICA GENERAL Y LA LEGISLACIÓN PERUANA.

De acuerdo al texto publicado por la secretaria del gobierno nacional PCM [10], la licencia GPL (General Public License) a pesar de haber sido escrita con una aproximación desde el punto de vista de la legislación anglosajona, tiene una perfecta validez en el ámbito peruano, pues está amparado por los acuerdos internacionales que regulan la aplicación de las leyes de derecho de autor en el Perú.

En la actualidad el gobierno peruano con el decreto Supremo N.º 051-2018-PCM, que crea el Portal de software Público Peruano establece disposiciones adicionales sobre el software Público Peruano. En la cual declara al Estado Peruano en proceso de modernización en sus diferentes instancias, dependencias, entidades, organizaciones y procedimientos, con la finalidad de mejorar la gestión pública y contribuir al fortalecimiento de un Estado moderno. Así mismo mediante Decreto Supremo N° 066-2011-PCM se aprueba el Plan de Desarrollo de la Sociedad de la Información en el Perú. La Agenda Digital Peruana 2.0, que tiene como uno de sus objetivos el indicado en el numeral 7 por el cual se busca "Promover una Administración Pública de calidad orientada a la población", estableciendo como una de sus estrategias "Adecuar la normatividad necesaria para el despliegue del gobierno electrónico", lo que implica contar con un Repositorio Nacional de Software y Procesos que permita a las instituciones del Estado centralizar el código fuente del software y procesos de gestión de propiedad estatal, que servirán para su reutilización e implementación en las entidades que lo requieran, contribuyendo al despliegue del gobierno electrónico de manera rápida y eficiente.

2.2.2 PLATAFORMA LINUX.

De acuerdo a lo publicado por Michael K. Johnson [11] Existen buenas razones para optar por la plataforma Linux debido a que el sistema ofrece estabilidad, seguridad, velocidad y alta performance, usando menos recursos del hardware instalado. Como relevancia importante es la disponibilidad del código fuente lo que proporciona a esta plataforma un alto nivel de independencia y flexibilidad, debido a que los desarrolladores no están vinculados a los productores de software, sino que es posible hacer adaptaciones y extensiones de acuerdo a sus necesidades tecnológicas. En el campo informático existe gran variedad

de aplicaciones libres de uso comercial para Linux. Como las conocidos Gestores de Bases de Datos "MYSQL, POSTGREST ". Suites Ofimáticas como Apache Office. Open Office y manejadores de servicios como: ClearOS, Nagios, Apache, etc.

2.2.2.1 LINUX COMO SISTEMA OPERATIVO.

Linux es un sistema operativo diseñado en la actualidad por cientos de programadores de todo el planeta, siendo el principal responsable del proyecto es Linus Torvalds. Torvalds comenzó a trabajar en su propio núcleo del sistema operativo, lo que eventualmente se convirtió en el núcleo de Linux, comenzó el desarrollo del núcleo de Linux en MINIX y las aplicaciones escritas para MINIX también se usaron en Linux. Posteriormente, Linux maduró y desarrollo un núcleo solido el cual tuvo lugar en sistemas Linux. Su objetivo inicial es propulsar el software de libre distribución junto con su código fuente para que pueda ser modificado por cualquier persona, dando rienda suelta a la creatividad. El hecho de que el sistema operativo incluya su propio código fuente expande enormemente las posibilidades de este sistema.

2.2.2.2 CARACTERÍSTICAS DE LINUX.

Las principales características de Linux son:

- **Multitarea**, es decir varios programas (procesos) ejecutándose al mismo tiempo.
- **Multiusuario**, varios usuarios en la misma máquina al mismo tiempo.
- **Multiplataforma**, corre en muchos fabricantes de CPU distintas, no sólo Intel, Funciona en modo protegido 386.
- **Protección de la memoria entre procesos,** de manera que uno de ellos no pueda colgar el sistema.
- **Carga de ejecutables por demanda:** Linux sólo lee de disco aquellas partes de un programa que están siendo usadas actualmente.
- **Política de copia en escritura para la compartición de páginas entre ejecutables;** esto significa que varios procesos pueden usar la misma zona de memoria para ejecutarse. Cuando alguno intenta escribir en esa memoria, la página (4Kb de memoria) se copia a otro lugar. Esta política de copia en escritura tiene dos beneficios: aumenta la velocidad y reduce el uso de memoria.
- **Memoria virtual usando paginación (sin intercambio de procesos completos) a disco:** una partición o un archivo en el sistema de archivos, o ambos, con la posibilidad de añadir más áreas de intercambio sobre la marcha (se sigue denominando intercambio, es en realidad un intercambio de páginas). Un total de 16 zonas de intercambio de 128Mb de tamaño máximo pueden ser usadas en un momento dado con un límite teórico de 2Gb para intercambio.
- **La memoria se gestiona como un recurso unificado para los programas de usuario y para el caché de disco**, de tal

forma que toda la memoria libre puede ser usada para caché y éste puede a su vez ser reducido cuando se ejecuten grandes programas.

- **Librerías compartidas de carga dinámica (DLL's) y librerías estáticas**; también por supuesto. realizan volcados de estado (Core dumps) para posibilitar los análisis post-mortem, permitiendo el uso de depuradores sobre los programas no sólo en ejecución sino también tras abortar éstos por cualquier motivo.
- Casi totalmente compatible con POSIX, System V y BSD a nivel fuente.
- Compatible con SCO, SVR3 y SVR4 a nivel binario.
- Pseudo terminales (pty's).
- Emulación de 387 en el núcleo, de tal forma que los programas no tengan que hacer su propia emulación matemática. Cualquier máquina que ejecute Linux parecerá dotada de coprocesador matemático. Por supuesto, si tu ordenador ya tiene una FPU (unidad de coma flotante), será usada en lugar de la emulación, pudiendo incluso compilar tu propio kernel sin la emulación matemática y conseguir un pequeño ahorro de memoria.
- Consolas virtuales múltiples: varias sesiones de login a través de la consola entre las que se puede cambiar con las combinaciones adecuadas de teclas (totalmente independiente del hardware de video). Se crean dinámicamente y puedes tener hasta 64.
- Acceso transparente a particiones MS-DOS WINDOWS (o a particiones OS/2 FAT32, NTFS) mediante un sistema de archivos especial: no se necesita ningún comando especial para usar la partición MS-DOS WINDOWS, parece un sistema de archivos normal de Unix.
- Sistema de archivos especial llamado UMSDOS que permite que Linux sea instalado en un sistema de archivos DOS.
- Soporta protocolos TCP/IP, incluyendo ftp, telnet, NFS, etc.
- Soporta los protocolos AppleTalk disponible en el actual núcleo de desarrollo.
- Software cliente y servidor NetWare disponible en los núcleos de desarrollo.

2.2.2.3 DISTRIBUCIONES DE LINUX.

De acuerdo a la publicación de Yubal FM en el portal Xataka Basics [12], son conocidas en la comunidad de software libre como “distro”, que son distribuciones basadas en el núcleo Linux. Estas distribuciones incluyen habitualmente bibliotecas, herramientas del proyecto GNU y el sistema de ventanas X Window System. Dependiendo del tipo de usuarios a los que la distribución va a ser dirigida se incluye también otro tipo de software como procesadores de texto, hoja de cálculo, reproductores multimedia, herramientas administrativas, etc.

En el caso de incluir herramientas del proyecto GNU, se denomina distribución GNU/Linux. Existen multitud de versiones del Sistema Operativo Linux algunas son con derecho de pago y otras son gratuitas. Aunque Windows y MacOs son mucho más populares que Linux, este sistema operativo también es muy utilizado en todo el mundo. Una de sus grandes ventajas frente a los otros dos es que está basado en software libre, en código abierto. Es posible instalarlo cuantas veces se requiera en una computadora de forma gratuita y personalizarlo como se desea.

Imagen N° 1: Distribuciones Linux
Fuente: https://www.redeszone.net/2015/12/12/las-distribuciones-linux-mas-buscadas-de-2015/

- **MANDRIVA LINUX**.: Creada por Gaël Duval en 1998. Con el nombre de Mandrake Linux, es fundamentalmente una distribución orientada al escritorio. Sus características más apreciadas son su ultra actualizado software, su excelente suite de administración del sistema DrakConf (Centro de Control de Mandriva), la excelente implementación de su edición de 64-bit y su extenso soporte de internacionalización. En la actualidad Mandriva Linux ha ido perdiendo protagonismo debido al surgimiento de otras distribuciones amigables que se han puesto a la par de Mandriva, y debido a su mala reputación de servicio al cliente y de ciertas decisiones controversiales de la compañía han alejado a un gran sector de la base de usuarios de la distribución
  Página oficial: https://www.openmandriva.org/
- **SUSE LINUX:** Fue creada en 1992 por los alemanes Roland Dyroff, Thomas Fehr, Hubert Mantel y Burchard Steinbild quienes lanzaron el proyecto bajo el nombre de SuSE “Software und System Entwicklun” ((Desarrollo de Sistemas y de Software). Al comienzo, la naciente empresa solía vender discos informáticos los cuales contenían la versión alemana de Linux-Slackware, pero no pasó mucho tiempo hasta Linux-SuSE se transformará en una distribución independiente a través de su versión 4.2 lanzada en mayo de 1996. En los siguientes años, los desarrolladores adoptaron el formato de paquetes RMP e introdujeron YaST, una amigable herramienta gráfica de administración. Cuenta con lanzamientos frecuentes,

excelentes publicaciones y documentación, y una amplia disponibilidad. En la actualidad SUSE fue comprado por Novell, Inc. a finales del 2003. Amplios cambios en el desarrollo, de licencia y disponibilidad de Linux SUSE fueron aplicados casi de inmediato, YaST fue lanzado bajo Licencia General Pública, las imágenes ISO fueron distribuidas libremente desde servidores públicos y lo más significativo fue que el desarrollo de la distribución fue por primera vez abierto para todo público. Desde el lanzamiento del proyecto open SUSE y la versión 10.0 en octubre del 2005, la distribución a llegado a ser completamente libre en todo sentido.
Página oficial: http://www.opensuse.org/es/

- **DEBIAN LINUX:** Debian GNU/Linux fue anunciada por primera vez en 1993. Su fundador, Ian Murdock, ideó la creación de un proyecto no comercial desarrollado por cientos de voluntarios en su tiempo libre. El desarrollo de Debian se realiza en tres ramales principales (o cuatro si se incluye la ultra actual rama "experimental") de niveles de estabilidad creciente: "unstable" (también conocido como "sid"), "testing" y "stable". Esta integración y estabilización progresiva de paquetes y componentes, junto a los sólidos y probados mecanismos de control de calidad, le han dado a Debian la reputación de ser una de las distribuciones más probadas y libres de errores de la actualidad. Página oficial: http://www.debian.org/

- **GENTOO LINUX:** El concepto de Gentoo Linux fue ideado alrededor del año 2000 por Daniel Robbins, formalmente un desarrollador de Stampede Linux y FreeBSD. Fue la exposición del autor a FreeBSD y su funcionalidad “autobuild” llamada “ports”, que lo inspiró a incorporar alguno de los principios de manejo de software de FreeBSD a Gentoo bajo el nombre de “portage”. La idea fue desarrollar una distribución de Linux que permita a los usuarios compilar el kernel de Linux y aplicaciones desde el código fuente directamente en sus propias computadoras, entonces manteniendo un sistema altamente optimizado y siempre actualizado. Para cuando el proyecto liberó la versión 1.0 en marzo 2002, el manejo de paquetes de Gentoo era considerado una alternativa superior a algunos sistemas de manejo de paquetes en binario, especialmente el entonces ampliamente utilizado RPM.
Página oficial: http://www.gentoo.org/
- **UBUNTU:** Es un sistema operativo de código abierto para computadores. Es una distribución de Linux basada en la arquitectura de Debian. Actualmente corre en computadores de escritorio y servidores, en arquitecturas Intel, AMD y ARM. Su patrocinador, Canonical, es una compañía británica propiedad del empresario sudafricano Mark

Shuttleworth. Ofrece el sistema de manera gratuita, y se financia por medio de servicios vinculados al sistema operativo y vendiendo soporte técnico. Además, al mantenerlo libre y gratuito, la empresa es capaz de aprovechar los desarrolladores de la comunidad para mejorar los componentes de su sistema operativo. Extraoficialmente, la comunidad de desarrolladores proporciona soporte para otras derivaciones de Ubuntu, con otros entornos gráficos, como Kubuntu, Xubuntu, Ubuntu MATE, Edubuntu, Ubuntu Studio, Mythbuntu, Ubuntu GNOME y Lubuntu. Está orientado al usuario promedio, con un fuerte enfoque en la facilidad de uso y en mejorar la experiencia del usuario. Estadísticas web sugieren que la cuota de mercado de Ubuntu dentro de las distribuciones Linux es, aproximadamente, del 49 %, y con una tendencia a aumentar como servidor web. Canonical, además de mantener Ubuntu, también provee una versión orientada a servidores, Ubuntu Server, una versión para empresas, Ubuntu Business Desktop Remix, una para televisores, Ubuntu TV, otra versión para tabletas Ubuntu Tablet, también Ubuntu Phone y una para usar el escritorio desde teléfonos inteligentes, Ubuntu for Android. Cada seis meses se publica una nueva versión de Ubuntu. Esta recibe soporte por parte de Canonical durante nueve meses por medio de actualizaciones de seguridad, parches para bugs críticos y actualizaciones menores de programas. Las versiones LTS (Long Term Support), que se liberan cada dos años, reciben soporte durante cinco años en los sistemas de escritorio y de servidor.
Página oficial: http://www.ubuntu.com/

- **RED HAT:** Red Hat Software Inc. fue fundada en el año 1994 por Bob Young y Marc Ewing. En agosto de 1999. Es una distribución Linux que llegó a ser una de las más populares en los entornos de usuarios domésticos hasta el 22 de septiembre de 2003 cuando los proyectos Fedora y Red Hat se fusionaron. En septiembre de 2003, Red Hat decidió concentrar sus esfuerzos de desarrollo en la versión corporativa de su distribución y delegó la versión común a Fedora Core, un proyecto abierto independiente de Red Hat, pero patrocinado por la empresa. Fue la primera distribución en usar RPM como su formato de paquete, y fue la que sirvió de punto de partida para otras distribuciones. Red Hat es instalado con un ambiente gráfico llamado Anaconda, diseñado para su fácil uso por novatos. También incorpora una herramienta llamada Lokkit para configurar las capacidades de Cortafuegos. En la actualidad es un sistema operativo de pago que destaca en estabilidad y flexibilidad.
  Página oficial: https://www.redhat.com/en

- **FEDORA:** Es una distribución Linux para propósitos generales mantenida por la empresa Red Hat basada en RPM, que se caracteriza por ser un sistema estable, la cual es mantenida gracias a una comunidad internacional de ingenieros, diseñadores gráficos y usuarios que informan de fallos y prueban nuevas tecnologías. Cuenta con el respaldo y la promoción de Red Hat. El proyecto no busca sólo incluir software libre y de código abierto, sino ser el líder en ese ámbito tecnológico. Algo que hay que destacar es que los desarrolladores de Fedora prefieren hacer cambios en las fuentes originales en lugar de aplicar los parches específicos en su distribución, de esta forma se asegura que las actualizaciones estén disponibles para todas las variantes de Linux.
  Página oficial: https://getfedora.org/

- **CentOS:** Se trata de una distribución derivada del código de Red Hat Enterprise Linux (RHEL), trabajando de manera similar, y cuyo objetivo es ofrecer al usuario un software de "clase empresarial" gratuito. Se define como robusto, estable y fácil de instalar y utilizar. Desde la versión 5, cada lanzamiento recibe soporte durante diez años, por lo que la actual versión 7 recibirá actualizaciones de seguridad hasta el 30 de junio de 2024. La actual versión 7.0 de CentOS (enero 2017) se basa en el núcleo de Linux 3.10.0, incluyendo la extensión de seguridad mencionada anteriormente SELinux, y ha implementado GCC (GNU Compiler Collection). Esta colección contiene el compilador para los lenguajes de programación más importantes, como por ejemplo C, C++ y Java. Esta distribución de Linux también es compatible con Hyperthreading (la división de un procesador en dos procesadores virtuales para aumentar el rendimiento), Plug and Play, Bluetooth y la sexta versión del protocolo de Internet (IPv6).
  Página oficial: https://www.centos.org/

- **ClearOS:** Anteriormente llamado ClarkConnect. Es una distribución GNU/Linux basada en Fedora y Red Hat; su creación proviene de ClearOS Enterprise, la cual creo la Clear Foundation organizadora y desarrolladora de esta distribución, donde su entorno de escritorio predeterminada puede ser KDE o GNOME. Es un sistema operativo orientado a Pymes (pequeñas y medianas empresas), con lo que cuenta con todo el software necesario para su funcionamiento y gestión. ClearOS es una solución poderosa como servidor de internet, se instala bajo su misma plataforma Linux la cual ya trae incluida dentro de la solución. Al igual que con otros sistemas GNU/Linux, ClearOS está virtualmente libre de virus y spyware.

Servicios, módulos y utilidades: Entre los principales servicios de este aplicativo están:

- ✓ Escaneo de virus y spam a través de la verificación del tráfico http, así como imap, pop y smtp.
- ✓ Filtrado de contenidos y protocolos a través de Proxy de una manera realmente fácil y rápida.
- ✓ Firewall sencillo y detección de intrusos mediante Snort
- ✓ Servidor LDAP con autenticación de SAMBA (SMB) como PDC (controlador primario de dominio).
- ✓ Sistema de impresión CUPS (Sistema de impresión común de Unix) y recursos compartidos (sistema de ficheros e impresoras) a través de SAMBA.
- ✓ Servidor FTP (ProFTPD), WEB (apache 2 con módulo de php) y MySQL con administración a través del proyecto phpMyAdmin.
- ✓ Servidor de correo electrónico (POSTFIX) con soporte de captura de correo de otras cuentas (Maildrop), SMTP, POP y WebMail.
- ✓ Sistema de backup de configuración del servidor (tanto local como remotamente en el servidor del proyecto).
- ✓ DHCP y DMZ
- ✓ Informes de errores sobre cada uno de los servicios.
- ✓ Bandwith Manager: Velocidad de Carga y Descarga, establece las velocidades de la red
- ✓ Mail Scanning, antivirus para el servicio de correo

Para activar algunos servicios, es necesario crear una cuenta en www.clearcenter.com. Si optamos por crear una cuenta con suscripción, tendremos algunas características más (como la VPN con IP dinámica o un espacio de almacenamiento para Backups).

Página oficial: https://www.clearos.com/

Imagen N° 2: Pantalla del Sistema operativo ClearOS
Fuente: https://www.clearcenter.com/products/clearos-7-business-new

2.2.3 LA SEGURIDAD DE LA INFORMACION

De acuerdo al artículo publicado por Ing. Maurice Frayssinet [13] La seguridad de la información es el conjunto de políticas, procedimientos, organización, acciones y demás actividades, orientadas a proteger la información de un amplio rango de amenazas. La seguridad de la información pretende proteger a la información de riesgos que atenten contra su:

- Confidencialidad: Solo acceden quienes están autorizados
- Disponibilidad: La información es accedida cuando sea requerida por el negocio
- Integridad: La información y sus procesos son exactos y completos.

Por lo tanto, la seguridad de la información debe considerarse un proceso de gestión y no un proceso tecnológico. Existen otros aspectos a los que la seguridad de la información también debe proteger, tales como:

- **Privacidad:** La información es accedida solo por el propietario de la información o excepcionalmente por quien él autorice.
- **Autenticidad:** La información accedida es auténtica

- **Autenticación:** Función de la seguridad de la información que permite asegurar que quien accede a la información es quien dice ser.

El concepto de seguridad de la información no debe ser confundido con el de seguridad informática, ya que este último sólo se encarga de la seguridad en el medio informático, pero la información puede encontrarse en diferentes medios o formas, y no solo en medios informáticos.

En los momentos actuales, donde el desarrollo tecnológico crece a ritmo exponencial, los procesos de negocio de las organizaciones, cada vez más cuentan con una alta dependencia de las tecnologías de la información y de las comunicaciones, Sin embargo, al mismo tiempo, estas tecnologías exponen a la información de las organizaciones a nuevos riesgos de seguridad. Por otro lado, la información como otros activos importantes del negocio, tiene gran valor para la organización y requiere de una protección adecuada.

Asimismo, la información adopta diversas formas:

- Impresa o escrita en papel.
- Almacenada electrónicamente
- Transmitida por correo electrónico
- Mostrada en video
- Hablada en conversación

La información debe protegerse cualquiera que sea la forma que tome o los medios por los que se comparta o almacene.

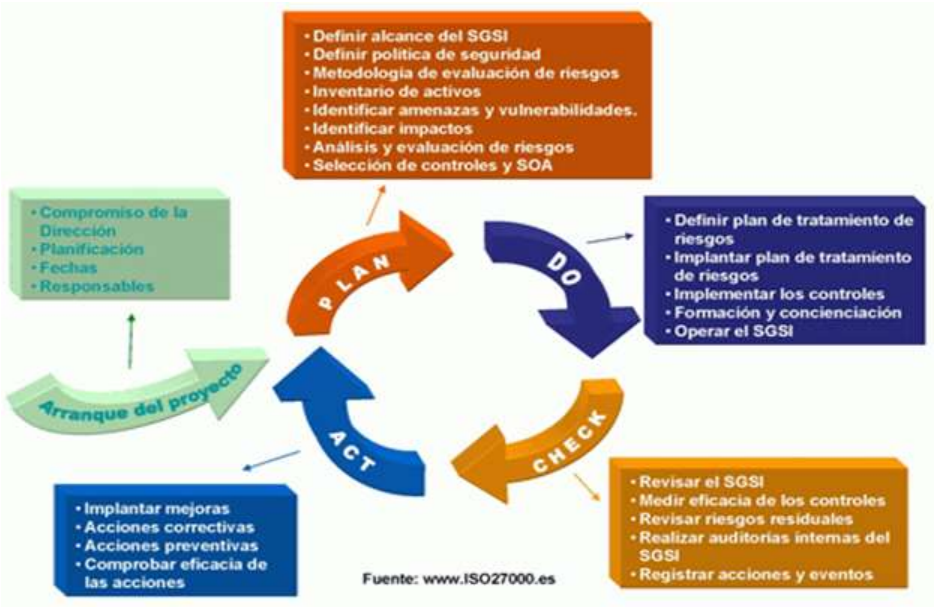


Imagen N° 3: Procesos ISO 27000-27002
Fuente: http://www.iso27000.es

2.2.3.1 ESTÁNDARES DE SEGURIDAD DE LA INFORMACIÓN - ISO 27000.

De acuerdo a la publicación Web por Neira, Agustín López [14] los estándares de la seguridad de información fueron publicados el 1 de mayo de 2009, revisada con una segunda edición de 01 de diciembre de 2012, una tercera edición de 14 de enero de 2014 y una cuarta en febrero de 2016. ISO 27000 es un conjunto de estándares internacionales sobre la Seguridad de la Información. Esta norma proporciona una visión general de las normas que componen la serie 27000, indicando para cada una de ellas su alcance de actuación y el propósito de su publicación. Recoge todas las definiciones para la serie de normas 27000 y aporta las bases de por qué es importante la implantación de un SGSI, una introducción a los Sistemas de Gestión de Seguridad de la Información, una breve descripción de los pasos para el establecimiento, monitorización, mantenimiento y mejora de un SGSI (la última edición no aborda ya el ciclo Plan-Do-Check-Act para evitar convertirlo en el único marco de referencia para la mejora continua).

Un Sistema de Gestión de la Seguridad de la Información es un conjunto de políticas y procedimientos que sirven para estandarizar la gestión de la Seguridad de la Información.

La familia ISO 27000 contiene un conjunto de buenas prácticas para el establecimiento, implementación, mantenimiento y mejora de Sistemas de Gestión de la Seguridad de la Información.

Los pilares principales de la familia 27000 son las normas 27001 y 27002. La principal diferencia entre estas dos normas, es que 27001 se basa en una gestión de la seguridad de forma continuada

apoyada en la identificación de los riesgos en el tiempo. En cambio, 27002, es una mera guía de buenas prácticas que describe una serie de objetivos de control y gestión que deberían ser perseguidos por las organizaciones.

a) **ISO/IEC 27001:** Es el conjunto de requisitos para implementar un SGSI. Publicada el 15 de octubre de 2005, revisada el 25 de septiembre de 2013. Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información. Tiene su origen en la BS 7799-2:2002 y es la norma certificable. En su Anexo A, enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002:2005, para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI; a pesar de no ser obligatoria la implementación de todos los controles enumerados en dicho anexo, la organización deberá argumentar sólidamente la no aplicabilidad de los controles no implementados.
b) **ISO/IEC 27002:** Publicada desde el 1 de Julio de 2007, es el nuevo nombre de ISO 17799:2005, manteniendo 2005 como año de edición. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable. Actualmente, la última edición de 2013 este estándar ha sido actualizada a un total de 14 Dominios, 35 Objetivos de Control y 114 Controles.
c) **ISO/IEC 27003:** Publicada el 01 de febrero de 2010 y actualizada el 12 de abril de 2017. No certificable. Es una guía que se centra en los aspectos críticos necesarios para el diseño e implementación con éxito de un SGSI de acuerdo ISO/IEC 27001. Describe el proceso de especificación y diseño desde la concepción hasta la puesta en marcha de planes de implementación, así como el proceso de obtención de aprobación por la dirección para implementar un SGSI. Tiene su origen en el anexo B de la norma BS 7799-2 y en la serie de documentos publicados por BSI a lo largo de los años con recomendaciones y guías de implantación.
d) **ISO/IEC 27004:** Publicada el 15 de diciembre de 2009 y revisada en diciembre de 2016. No certificable. Es una guía para el desarrollo y utilización de métricas y técnicas de medida aplicables para determinar la eficacia de un SGSI y de los controles o grupos de controles implementados según ISO/IEC 27001
e) **ISO/IEC 27005:** Publicada la tercera edición en julio de 2018 con actualizaciones respecto a requisitos de norma ISO/IEC 27001:2013. No certificable. Proporciona directrices para la gestión del riesgo en la seguridad de la información. Apoya los conceptos generales especificados en la norma ISO/IEC 27001 y está diseñada para ayudar a la

aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos.

f) **ISO/IEC 27006:** Publicada en segunda edición el 1 de diciembre de 2011 (primera edición del 1 de marzo de 2007) y revisada el 30 de septiembre de 2015. Especifica los requisitos para la acreditación de entidades de auditoría y certificación de sistemas de gestión de seguridad de la información. Es una versión revisada de EA-7/03 (Requisitos para la acreditación de entidades que operan certificación/registro de SGSIs) que añade a ISO/IEC 17021 (Requisitos para las entidades de auditoría y certificación de sistemas de gestión) los requisitos específicos relacionados con ISO 27001:2005 y los SGSIs. Es decir, ayuda a interpretar los criterios de acreditación de ISO/IEC 17021 cuando se aplican a entidades de certificación de ISO 27001, pero no es una norma de acreditación por sí misma.

g) **ISO/IEC 27007:** Publicada el 14 de noviembre de 2011 y revisada el 09 de octubre de 2017. No certificable. Es una guía de auditoría de un SGSI, como complemento a lo especificado en ISO 19011. En España, esta norma no está traducida.

h) **ISO/IEC TR 27008:** Publicada el 15 de octubre de 2011. No certificable. Es una guía de auditoría de los controles seleccionados en el marco de implantación de un SGSI. En España, esta norma no está traducida. El original en inglés puede adquirirse en iso.org. Actualmente en proceso de revisión para su actualización.

i) **ISO/IEC 27009:** Publicada el 15 de junio de 2016. No certificable. define los requisitos para el uso de la norma ISO/IEC 27001 en cualquier sector específico (campo, área de aplicación o sector industrial). El documento explica cómo refinar e incluir requisitos adicionales a los de la norma ISO/IEC 27001 y cómo incluir controles o conjuntos de control adicionales a los del Anexo A.

j) **ISO/IEC 27010:** Publicada el 20 de octubre de 2012 y revisada el 10 de noviembre de 2015. Consiste en una guía para la gestión de la seguridad de la información cuando se comparte entre organizaciones o sectores. ISO/IEC 27010:2012 es aplicable a todas las formas de intercambio y difusión de información sensible, tanto pública como privada, a nivel nacional e internacional, dentro de la misma industria o sector de mercado o entre sectores. En particular, puede ser aplicable a los intercambios de información y participación en relación con el suministro, mantenimiento y protección de una organización o de la infraestructura crítica de los estados y naciones. Actualmente en proceso de revisión para su actualización.

k) **ISO/IEC 27031:** Publicada el 01 de marzo de 2011. No certificable. Es una guía de apoyo para la adecuación de las tecnologías de información y comunicación (TIC) de una

organización para la continuidad del negocio. El documento toma como referencia el estándar BS 25777.

l) **ISO/IEC 27032:** Publicada el 16 de Julio de 2012. Proporciona orientación para la mejora del estado de seguridad cibernética, extrayendo los aspectos únicos de esa actividad y de sus dependencias en otros dominios de seguridad, concretamente: Información de seguridad, seguridad de las redes, seguridad en Internet e información de protección de infraestructuras críticas (CIIP). Cubre las prácticas de seguridad a nivel básico para los interesados en el ciberespacio. Esta norma establece una descripción general de Seguridad Cibernética, una explicación de la relación entre la ciberseguridad y otros tipos de garantías, una definición de las partes interesadas y una descripción de su papel en la seguridad cibernética, una orientación para abordar problemas comunes de Seguridad Cibernética y un marco que permite a las partes interesadas a que colaboren en la solución de problemas en la ciberseguridad.

m) **ISO/IEC 27033:** Norma dedicada a la seguridad en redes, consistente en 6 partes: 27033-1, conceptos generales (Publicada el 15 de diciembre de 2009 y revisada el 10 de octubre de 2015); 27033-2, directrices de diseño e implementación de seguridad en redes (Publicada el 27 de julio de 2012); 27033-3, escenarios de referencia de redes (Publicada el 3 de diciembre de 2010); 27033-4, aseguramiento de las comunicaciones entre redes mediante gateways de seguridad (Publicada el 21 de Febrero de 2014); 27033-5, aseguramiento de comunicaciones mediante VPNs (Publicada el 29 de Julio de 2013); 27033-6, securización de redes IP wireless (Publicada en Junio de 2016).

n) **ISO/IEC 27034:** Norma dedicada la seguridad en aplicaciones informáticas, consistente en 7 partes: 27034-1, conceptos generales (Publicada el 21 de noviembre de 2011); 27034-2, marco normativo de la organización (Publicada el 15 de agosto de 2015); 27034-3, proceso de gestión de seguridad en aplicaciones (publicada en mayo 2018); 27034-4, validación de la seguridad en aplicaciones (en fase de desarrollo); 27034-5, estructura de datos y protocolos y controles de seguridad de aplicaciones (Publicada el 09 de octubre de 2017); 27034-6, guía de seguridad para aplicaciones de uso específico (Publicada en octubre de 2016); 27034-7, marco predictivo de en la seguridad (publicada en mayo 2018).

o) **ISO/IEC 27035:** Publicada el 17 de agosto de 2011. Proporciona una guía sobre la gestión de incidentes de seguridad en la información. Consta de 3 partes: 27035-1, Principios en la gestión de incidentes (Publicada en noviembre de 2016); 27035-2, guías para la elaboración de un plan de respuesta a incidentes (Publicada en noviembre

de 2016); 27035-3, guía de operaciones en la respuesta a incidentes.

p) **ISO/IEC 27037:** Publicada el 15 de octubre de 2012. Es una guía que proporciona directrices para las actividades relacionadas con la identificación, recopilación, consolidación y preservación de evidencias digitales potenciales localizadas en teléfonos móviles, tarjetas de memoria, dispositivos electrónicos personales, sistemas de navegación móvil, cámaras digitales y de video, redes TCP/IP, entre otros dispositivos y para que puedan ser utilizadas con valor probatorio y en el intercambio entre las diferentes jurisdicciones.

q) **ISO/IEC 27039:** Publicada el 11 de febrero de 2015. Es una guía para la selección, despliegue y operativa de sistemas de detección y prevención de intrusión (IDS/IPS). Existe una (corrección al contenido inicial de 28 de abril de 2016).

2.2.4 RED PRIVADA VIRTUAL (VPN).

La seguridad siempre es un motivo de preocupación cuando se utiliza Internet pública para los procesos del negocio en las empresas. Es por ello que las redes virtuales privadas (VPN) se usan para garantizar la seguridad de los datos a través de Internet. Una VPN se utiliza para crear un túnel privado a través de una red pública. Se puede proporcionar seguridad a los datos mediante el uso de cifrado en este túnel a través de Internet y con autenticación para proteger los datos contra el acceso no autorizado.

Tal como lo indica Vásquez, Virgilio [15] en su tesis “Implementación De Una Red Privada Virtual (VPN) Bajo Software Libre”, Virtual Prívate Network (VPN) es una tecnología de red que permite una extensión segura de la red local (LAN) sobre una red pública o no controlada como Internet, mediante un proceso de encapsulación y de encriptación, de los paquetes de datos a distintos puntos remotos mediante el uso de infraestructuras públicas de transporte. Permite que la computadora en la red envíe y reciba datos sobre redes compartidas o públicas como si fuera una red privada. VPN ofrece una solución de bajo costo para implementar la red a larga distancia al basarse sobre Internet, además de ofrecer autenticación de usuarios o equipos a través de cifrados, firmas digitales o claves de acceso para una identificación inequívoca; ofreciendo integridad, garantizando que los datos enviados por el emisor sean exactos a los que se reciben, y confidencialidad, esto definido por el cifrado que usa ya que nada de lo transmitido sea interceptado o interpretada por nadie más que emisor y destino.

Las soluciones de hardware casi siempre ofrecen mayor rendimiento y facilidad de configuración, aunque no tienen la flexibilidad de las versiones por software. Dentro de esta familia tenemos a los productos de Fortinet, Sonic WALL, WatchGuard, Nortel, Cisco, Linksys, Netscreen (Juniper Networks), Symantec, Nokia, U.S. Robotics, D-link, Mikrotik, etc.

Las aplicaciones VPN por software son las más configurables y son ideales cuando surgen problemas de interoperabilidad en los modelos anteriores. Obviamente el rendimiento es menor y la configuración más delicada, porque se suma el sistema operativo y la seguridad del equipo en general. Aquí tenemos por ejemplo a las soluciones nativas de Windows, GNU/Linux y los Unix en general. Por ejemplo, productos de código abierto como OpenSSH, OpenVPN y FreeS/Wan.
En ambos casos se pueden utilizar soluciones de firewall («cortafuegos» o «barrera de fuego»), obteniendo un nivel de seguridad alto por la protección que brinda, en detrimento del rendimiento.

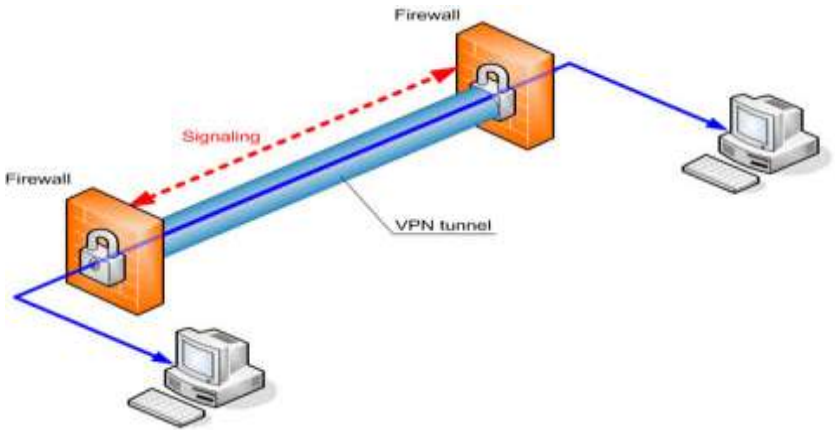


Imagen N° 4: Esquema de Red VPN
Fuente: https://www.profesionalreview.com/2016/06/06/que-es-una-vpn-y-para-que-sirve

2.2.4.1 BENEFICIOS DE LAS VPN:

Los beneficios de tener una VPN como red segura son:

- **Ahorro de costos:** Permiten que las organizaciones utilicen un transporte externo de Internet para conectar oficinas y usuarios remotos al sitio principal; por lo tanto, se eliminan los costosos enlaces WAN dedicados
- **Escalabilidad:** Permiten que las organizaciones utilicen la infraestructura de Internet dentro de los ISP y los dispositivos, lo que facilita la tarea de agregar nuevos usuarios. Por lo tanto, las organizaciones pueden agregar una gran cantidad de capacidad sin necesidad de aumentar considerablemente la infraestructura.
- **Compatibilidad:** Permiten que los trabajadores móviles y los empleados a distancia aprovechen la conectividad por banda ancha como DSL o VSAT, para acceder a las redes de sus organizaciones. La conectividad por banda ancha proporciona flexibilidad y eficacia, también proporcionan una solución rentable para conectar oficinas remotas.
- **Seguridad:** Permiten incluir mecanismos de seguridad que proporcionan el máximo nivel de seguridad mediante protocolos de cifrado y autenticación avanzados que protegen los datos contra el acceso no autorizado.

2.2.4.2 PROTOCOLOS.

El protocolo estándar por defecto es el IPSEC, pero también están PPTP, L2F, L2TP, SSL/TLS, SSH, etc. Cada uno con sus ventajas y desventajas en cuanto a seguridad, facilidad, mantenimiento y tipos de clientes soportados. Actualmente hay una línea de productos en crecimiento relacionada con el protocolo SSL/TLS, que intenta hacer más amigable la configuración y operación de estas soluciones.

a) **IPSec:** Es un conjunto de estándares para incorporar seguridad en IP, actúa a nivel de capa de red, protegiendo y autenticando los paquetes IP entre los equipos participantes de la red. Proporciona confidencialidad, integridad y autenticación a través de algoritmos de cifrado, hash, llaves públicas y certificados digitales. IPSec tiene tres grandes componentes, dos protocolos de seguridad, como son Autenticación de cabecera IP (AH) y Carga de seguridad de encapsulado (ESP); y uno de seguridad de llaves, Intercambio de llaves de Internet (IKE).

b) **PPTP:** Point-to-Point Tunneling Protocol fue desarrollados por ingenieros de Ascend Communications, U.S. Robotics, 3Com Corporation, Microsoft, y ECI Telematics para proveer entre usuarios de acceso remoto y servidores de red una red privada virtual. PPTP fue diseñado para permitir a los usuarios conectarse a un servidor RAS desde cualquier punto en Internet para tener la misma autenticación, encriptación y los mismos accesos de LAN como si discaran directamente al servidor.

c) **L2TP:** Layer-2 Tunneling Protocol (L2TP) facilita el entunelamiento de paquetes PPP a través de una red de manera tal que sea lo más transparente posible a los usuarios de ambos extremos del túnel y para las aplicaciones que éstos corran. L2TP utiliza dos tipos de mensajes: de control y de datos. Los mensajes de control son usados para el establecimiento, el mantenimiento y el borrado de los túneles y las llamadas. Utilizan un canal de control confiable dentro de L2TP para garantizar el envío. Los mensajes de datos encapsulan los marcos PPP y son enviados a través del túnel.

d) **SSL y TLS;** SSL significa Secure Sockets Layer y TLS es la abreviatura de Transport Layer Security. Ambas funcionan como un protocolo, utilizadas para crear una conexión VPN. Se trata de una conexión de VPN donde el navegador web funciona como cliente, y el acceso del usuario está restringido a aplicaciones específicas en lugar de poder acceder a toda la red. El protocolo SSL y TLS se utiliza principalmente en sitios web de compras y proveedores de servicios. Una VPN SSL y TLS te brinda una sesión segura desde el navegador de tu PC hacia el servidor de la aplicación. Esto se debe a que los navegadores web cambian a SSL fácilmente y casi no

requieren ninguna acción por parte del usuario. Los navegadores ya vienen con SSL y TLS integrado. Las conexiones SSL tienen https al inicio de la dirección URL en lugar de http.

2.2.4.3 TIPOS DE VPN.

Básicamente existen cuatro arquitecturas de conexión VPN:

- Tunneling,
- Punto a Punto,
- Acceso Remoto,
- VPN Interna (Over LAN)

a) **Tunneling:** La técnica de tunneling consiste en encapsular un protocolo de red sobre otro, creando un túnel dentro de una red de computadoras. El establecimiento de dicho túnel se implementa incluyendo una PDU (unidades de datos de protocolo) determinada dentro de otra PDU con el objetivo de transmitirla desde un extremo al otro del túnel sin que sea necesaria una interpretación intermedia de la PDU encapsulada. De esta manera se encaminan los paquetes de datos sobre nodos intermedios que son incapaces de ver en claro el contenido de dichos paquetes. El túnel queda definido por los puntos extremos y el protocolo de comunicación empleado, que, entre otros, podría ser SSH. Básicamente, esta técnica consiste en abrir conexiones entre dos máquinas por medio de un protocolo seguro, SSH (Secure SHell), a través de las cuales se realiza las transferencias inseguras, que pasarán de este modo a ser seguras, siendo la conexión segura el túnel por el cual se envían los datos para que nadie más aparte de los interlocutores que se sitúan a cada extremo del túnel, pueda ver dichos datos. Este tipo de técnica requiere de forma imprescindible tener una cuenta de acceso seguro en la máquina con la que se quiere comunicar los datos. Una vez autenticados tienen un nivel de acceso muy similar al que tienen en la red local de la empresa. Muchas empresas han reemplazado con esta tecnología su infraestructura dial-up (módems y líneas telefónicas).

b) **Punto a Punto:** Está basado en las conexiones desde un eje central (Sede principal de la empresa) o componente central VPN y los servidores de otras oficinas que estén remotas. Se conectan a internet solo utilizando internet de los proveedores de servicios, en definitiva, es medida de ahorro en cables y conexiones físicas o denominados conexiones punto a puntos tradicionales, sobre todo si se encuentran ubicadas en diversos estados del país o incluso fuera de él. El equipo central vpn, que posee un vínculo a Internet permanente, acepta las conexiones vía Internet provenientes de los sitios y establece el "túnel" vpn. Los servidores de las sucursales se conectan a Internet utilizando los servicios de

su proveedor local de Internet, típicamente mediante conexiones de banda ancha.

c) **VPN de acceso remoto:** Considerado como el más común en este momento es la conexión remota de un usuario o grupo de usuarios desde sitios externos de la empresa utilizando el internet como modo de acceso. Pare el acceso se debe contar del lado de la VPN un servidor que puede ser de hardware o software y por el lado del cliente tenemos que contar con el protocolo de la VPN instalada. Una vez autenticados tienen un nivel de acceso muy similar al que tienen en la red local de la empresa.

d) **VPN over LAN:** Es un esquema realmente desconocido pero muy útil y potente; consiste en establecer redes privadas virtuales dentro de una misma red local. El objetivo último es aislar partes de la red y sus servicios entre sí, aumentando la seguridad. Una aplicación muy típica de este modelo se utiliza para aumentar la seguridad en redes de acceso inalámbrico, separándolas así de la red física para evitar posibles fugas de información o accesos no autorizados. Un ejemplo es la conexión a redes Wifi haciendo uso de túneles cifrados IPSec o SSL que además de pasar por los métodos de autenticación tradicionales (WEP, WPA, direcciones MAC, etc.) agregan las credenciales de seguridad del túnel VPN creado en la LAN interna o externa.

2.2.5 FIREWALL.

Como lo indica en un artículo web del portal Cisco [16]Un firewall es un dispositivo de seguridad de red que monitorea el tráfico de red entrante y saliente y decide si permite o bloquea el tráfico específico en función de un conjunto definido de reglas de seguridad. Los cortafuegos han sido una primera línea de defensa en seguridad de red durante más de 25 años. Establecen una barrera entre las redes internas seguras y controladas que pueden ser confiables y no confiables fuera de las redes, como Internet. Un firewall puede ser hardware, software o ambos

La ubicación habitual de un firewall es el punto de conexión de la red interna de la organización con la red exterior, que normalmente es Internet; de este modo se protege la red interna de intentos de acceso no autorizados desde Internet, que puedan aprovechar vulnerabilidades de los sistemas de la red interna. También es frecuente conectar al firewall una tercera red, llamada zona desmilitarizada o DMZ, en la que se ubican los servidores de la organización que deben permanecer accesibles desde la red exterior. Un firewall correctamente configurado añade protección a una instalación informática, pero en ningún caso debe considerarse como suficiente. La Seguridad informática abarca más ámbitos y más niveles de trabajo y protección.

2.2.5.1 TIPOS DE FIREWALL.

Los más conocidos son:

a) **Cortafuegos proxy:** Un firewall proxy sirve como puerta de enlace de una red a otra para una aplicación específica. Los servidores proxy pueden proporcionar funcionalidades adicionales, como el almacenamiento en caché de contenido y la seguridad al evitar conexiones directas desde fuera de la red. Sin embargo, esto también puede afectar las capacidades de rendimiento y las aplicaciones que pueden soportar.

b) **Firewall de inspección con estado:** Ahora considerado como un firewall "tradicional", un firewall de inspección con estado permite o bloquea el tráfico según el estado, el puerto y el protocolo. Supervisa toda la actividad desde la apertura de una conexión hasta que se cierra. Las decisiones de filtrado se toman en base tanto a las reglas definidas por el administrador como al contexto, que se refiere al uso de información de conexiones anteriores y paquetes que pertenecen a la misma conexión.

c) **Firewall de gestión unificada de amenazas (UTM):** Un dispositivo UTM generalmente combina, de manera poco flexible, las funciones de un firewall de inspección con estado con prevención de intrusiones y antivirus. También puede incluir servicios adicionales y, a menudo, gestión en la nube. Los UTM se centran en la simplicidad y la facilidad de uso.

d) **Firewall de próxima generación (NGFW):** Los firewalls han evolucionado más allá del simple filtrado de paquetes y la inspección de estado. La mayoría de las empresas están implementando firewalls de próxima generación para bloquear las amenazas modernas, como el malware avanzado y los ataques de la capa de aplicación.

e) **Firewall de capa de red o de filtrado de paquetes.:** Funciona a nivel de red (nivel 3) de la pila de protocolos (TCP/IP) como filtro de paquetes IP. A este nivel se pueden realizar filtros según los distintos campos de los paquetes IP: dirección IP origen, dirección IP destino. A menudo en este tipo de firewall se permiten filtrados según campos de nivel de transporte (nivel 4) como el puerto origen y destino, o a nivel de enlace de datos (nivel 2) como la dirección MAC.

f) **Firewall de capa de aplicación:** Trabaja en el nivel de aplicación (nivel 7) de manera que los filtrados se pueden adaptar a características propias de los protocolos de este nivel. Por ejemplo, si se trata de tráfico HTTP se pueden realizar filtrados según la URL a la que se está intentando acceder. Un firewall a nivel 7 de tráfico HTTP es normalmente denominado Proxy y permite que los computadores de una organización entren a internet de una forma controlada.

g) **Firewall personal:** Es un caso particular de firewall que se instala como software en un computador, filtrando las comunicaciones entre dicho computador y el resto de la red y viceversa, también lo pueden contener los sistemas operativos o antivirus.

Según la definición de Gartner, Inc., un firewall de próxima generación debe incluir:

- Capacidades de firewall estándar como inspección con estado
- Prevención de intrusiones integrada
- Conocimiento y control de aplicaciones para ver y bloquear aplicaciones riesgosas actualizando las rutas para incluir futuras fuentes de información
- Técnicas para abordar las amenazas de seguridad en evolución.

Si bien estas capacidades se están convirtiendo cada vez más en el estándar para la mayoría de las empresas, los NGFW pueden hacer más.

2.2.5.2 FUNCIONAMIENTO DE UN FIREWALL.

Un firewall funciona como una barrera entre internet u otras redes públicas y nuestra computadora. Todo el tipo de tráfico que no esté en la lista permitida por el firewall, no entra ni sale de la computadora. Para ello, un sistema de firewall contiene un conjunto de reglas predefinidas que permiten:

- Autorizar una conexión (Allow)
- Bloquear una conexión (Deny)
- Redireccionar un pedido de conexión sin avisar al emisor (Drop).

El conjunto de estas reglas permite instalar un método de filtración dependiente de la política de seguridad adoptada por la organización. Se distinguen habitualmente dos tipos de políticas de seguridad que permiten:

- Permitir únicamente las comunicaciones autorizadas explícitamente: "Todo lo que no es autorizado explícitamente está prohibido".
- Impedir cualquier comunicación que fue explícitamente prohibida.

El primer método es el más seguro, pero requiere de una definición precisa de las necesidades de comunicación de toda la red.

2.2.5.3 VENTAJAS DE UN FIREWALL.

Un firewall es como un cuello de botella por el que todo el tráfico de Internet entrante y saliente debe pasar, permitiéndote controlar el tráfico. Un buen cortafuegos bien configurado y administrado evita en gran medida que los hackers lo superen y por supuesto nos ayuda a mantener a salvo los datos confidenciales de la empresa. En pocas palabras un firewall trabaja como un policía identificando cada paquete de información antes de que este le permita el acceso.

Algunas de las ventajas se detallan a continuación:

a) **Protege de intrusiones:** El acceso a ciertos segmentos de la red de una organización, sólo se permite desde máquinas autorizadas de otros segmentos de la organización o de Internet.
b) **Protección de información privada:** Permite definir distintos niveles de acceso a la información de manera que en una organización cada grupo de usuarios definido tendrá acceso sólo a los servicios y la información que le son estrictamente necesarios.
c) **Optimización de acceso:** Identifica los elementos de la red internos y optimiza que la comunicación entre ellos sea más directa. Esto ayuda a reconfigurar los parámetros de seguridad.

2.2.5.4 LIMITACIONES DE UN FIREWALL.

Como se indica en su artículo Arenas, José [17]Se menciona 6 limitaciones que se deben tener en cuenta:

a) Un firewall no puede protegerse contra aquellos ataques que se efectúen fuera de su punto de operación.
b) El firewall no puede protegerse de las amenazas a que está sometido por traidores o usuarios inconscientes.
c) El firewall no puede prohibir que los traidores o espías corporativos copien datos sensibles en disquetes o tarjetas PCMCIA y sustraigan éstas del edificio.
d) El firewall no puede proteger contra los ataques de Ingeniería social
e) El firewall no puede protegerse contra los ataques posibles a la red interna por virus informáticos a través de archivos y software. La solución real está en que la organización debe ser consciente en instalar software antivirus en cada máquina para protegerse de los virus que llegan por medio de disquetes o cualquier otra fuente.
f) El firewall no protege de los fallos de seguridad de los servicios y protocolos de los cuales se permita el tráfico.

2.2.5.5 POLÍTICAS DEL FIREWALL.

Hay dos políticas básicas en la configuración de un firewall y que cambian radicalmente la filosofía fundamental de la seguridad en la organización:

a) **Política restrictiva:** Se deniega todo el tráfico excepto el que está explícitamente permitido. El firewall obstruye todo el tráfico y hay que habilitar expresamente el tráfico de los servicios que se necesiten.
b) **Política permisiva:** Se permite todo el tráfico excepto el que esté explícitamente denegado. Cada servicio potencialmente peligroso necesitará ser aislado básicamente caso por caso, mientras que el resto del tráfico no será filtrado.

La política restrictiva es la más segura, ya que es más difícil permitir por error tráfico potencialmente peligroso, mientras que en la política permisiva es posible que no se haya contemplado algún caso de tráfico peligroso y sea permitido por defecto.

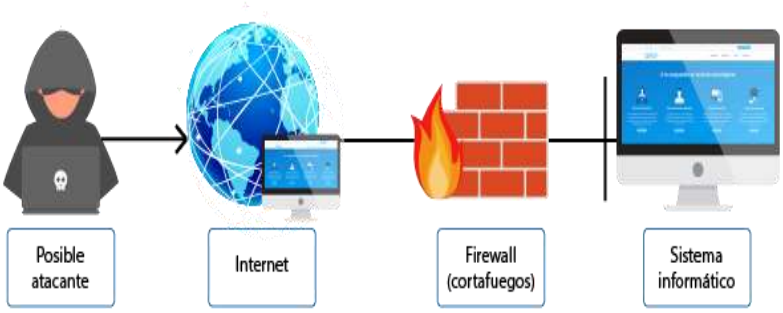


Imagen N° 5: Esquema de un firewall
Fuente: https://antiun.com/firewall/

2.2.6 TECNOLOGÍA DE SWITCHES - CISCO.

De acuerdo a la academia Netacad del portal web Cisco [18], Las soluciones de switching de Cisco ofrecen una valiosa ventaja estratégica a las redes de cualquier tamaño y en cualquier sector. Los avances tecnológicos en los que ha innovado Cisco impulsan la productividad de las empresas, fomentan la excelencia operativa, y aumentan el valor comercial de la red y de los recursos conectados. Las plataformas de hardware extensibles y los servicios de switching inteligentes hacen realidad de expandir las redes sin fronteras de forma segura, confiable y transparente. Las soluciones de switching de Cisco pueden personalizarse según los requisitos técnicos y presupuestarios.

Las redes siempre deben ser confiables, protegidas y listas para afrontar nuevos desafíos. Las soluciones de switching de Cisco están diseñadas para brindar acceso e intercambios que son:

- **Seguros:** protegen la información personal y comercial, las identidades e interacciones de los usuarios, y las conexiones y recursos de la red no sólo es fundamental, sino que a menudo es una exigencia legal
- **Confiables:** reduce el costoso tiempo de inactividad de la red. Hardware redundante, actualizaciones de software en servicio (ISSU), diagnósticos en línea genéricos (GOLD) y mecanismos de recuperación automatizados son sólo algunos ejemplos de las capacidades de switching de Cisco que permiten mantener los niveles de servicio de la red
- **Transparentes:** las organizaciones conectadas a la red necesitan redes que crezcan con ellas. Las soluciones de switching de Cisco se adaptan fácilmente a los nuevos requisitos mediante hardware escalable, servicios integrados, asistencia líder de la industria, sistemas abiertos, e innovación tecnológica continua

2.2.6.1 CONCEPTOS BÁSICOS DE SWITCHING.

Se usan para conectar varios dispositivos en una misma red diseñada correctamente, y son los responsables de controlar el flujo de datos en la capa de acceso y de dirigirlo a los recursos conectados en red. Los switching funcionan en la capa de acceso donde los dispositivos de red cliente se conectan directamente a la red, esta es una de las áreas más vulnerables de la red, ya que está muy expuesta al usuario. Se deben configurar para que sean resistentes a los ataques de todo tipo y, al mismo tiempo, protejan los datos de los usuarios y permitan que haya conexiones de alta velocidad. La seguridad de puertos es una de las características de seguridad que proporcionan los switching administrados por Cisco.
Los switching LAN mantienen una tabla que usan para determinar cómo reenviar el tráfico a través del switch.

2.2.6.2 CONFIGURACIÓN BÁSICA DE LOS SWITCH CISCO.

- Para el acceso a la administración remota de un switch Cisco, se debe configurar una dirección IP y una máscara de subred y para administrar un switch desde una red remota, se debe configurar con un Gateway predeterminado.
- Esta configuración se realiza es una interfaz virtual del switch “SVI”, la cual no es un puerto físico del switch.
- SVI es un concepto relacionado con las VLAN.
- Las VLAN son grupos lógicos numerados a los que se pueden asignar puertos físicos.
- Los parámetros de configuración aplicados a una VLAN también se aplican a todos los puertos asignados a esa VLAN.
- De manera predeterminada, el switch está configurado para que el control de la administración del switch se realice mediante la VLAN 1.
- Todos los puertos se asignan a la VLAN 1 de manera predeterminada. Por motivos de seguridad, se recomienda usar una VLAN de administración distinta de la VLAN 1.

Imagen N° 6: Configuración básica de un switch
Fuente: cisco.netacad.net/Academy

2.2.6.3 SEGURIDAD DE PUERTOS.

Como recomendación se deben proteger todos los puertos (interfaces) del switch antes de implementar el dispositivo para que empiece a funcionar en la red. Una forma de proteger los puertos es mediante la implementación de una característica denominada "seguridad de puertos". La seguridad de puerto limita la cantidad de direcciones MAC válidas permitidas en el puerto. Se permite el acceso a las direcciones MAC de los dispositivos legítimos, mientras que otras direcciones MAC se rechazan.

La seguridad de puertos se puede configurar para permitir una o más direcciones MAC. Si la cantidad de direcciones MAC permitidas en el puerto se limita a una, solo el dispositivo con esa dirección MAC específica puede conectarse correctamente al puerto. Si se configura un puerto como seguro y se alcanza la cantidad máxima de direcciones MAC, cualquier intento adicional de conexión de las direcciones MAC desconocidas genera una violación de seguridad.

La característica de seguridad de puertos no funciona hasta que se habilita la seguridad de puertos en la interfaz mediante el comando *switchport port-security.*

a) **Tipos de direcciones MAC seguras:** Existen varias maneras de configurar la seguridad de puerto. El tipo de dirección segura se basa en la configuración e incluye lo siguiente:
b) **Direcciones MAC seguras estáticas:** Son direcciones MAC que se configuran manualmente en un puerto mediante el comando: ***switchport port-security mac-address dirección-mac*.** Las direcciones MAC configuradas de esta forma se almacenan en la tabla de direcciones y se agregan a la configuración en ejecución del switch.
c) **Direcciones MAC seguras dinámicas:** Son direcciones MAC detectadas dinámicamente y se almacenan solamente en la tabla de direcciones. Las direcciones MAC configuradas de esta manera se eliminan cuando el switch se reinicia.
d) **Direcciones MAC seguras persistentes:** Son direcciones MAC que pueden detectarse de forma dinámica o configurarse de forma manual, y que después se almacenan en la tabla de direcciones y se agregan a la configuración en ejecución. Para configurar una interfaz a fin de convertir las direcciones MAC detectadas dinámicamente en direcciones MAC seguras persistentes y agregarlas a la configuración en ejecución, debe habilitar el aprendizaje por persistencia. El aprendizaje por persistencia se habilita en una interfaz mediante el comando switchport port-security mac-address sticky. Cuando se introduce este comando, el switch convierte todas las direcciones MAC detectadas dinámicamente en direcciones MAC seguras persistentes, incluso las que se detectaron dinámicamente antes de que se habilitara el aprendizaje por persistencia. Todas las

direcciones MAC seguras persistentes se agregan a la tabla de direcciones y a la configuración en ejecución. También se pueden definir manualmente mediante el comando switchport port-security mac-address sticky dirección-mac, todas las direcciones especificadas se agregan a la tabla de direcciones y a la configuración en ejecución.

Si se guardan las direcciones MAC seguras persistentes en el archivo de configuración de inicio, cuando el switch se reinicia o la interfaz se desactiva, la interfaz no necesita volver a aprender las direcciones. Si no se guardan las direcciones seguras persistentes, estas se pierden. Si se inhabilita el aprendizaje por persistencia mediante el comando no switchport port-security mac-address sticky, las direcciones MAC seguras persistentes siguen formando parte de la tabla de direcciones, pero se eliminan de la configuración en ejecución.

Un método simple que se usa para contribuir a la seguridad de la red ante accesos no autorizados es inhabilitar los puertos del switch que no se utilizan. Es aconsejable inhabilitar los puertos que no se utilizan. Se debe verificar los puertos que no se utilizan y se emita el comando shutdown de Cisco IOS para deshabilitar el puerto que no se usara. Si más adelante se debe reactivar un puerto, este se puede habilitar con el comando no shutdown.

```
Switch# configure terminal
Switch(config)#interface fa 0/"Número de Puerto"
Switch(config-if)#no shutdown
Switch(config-if) #shutdown
```

En la siguiente figura n°07, muestra el resultado de esta configuración.

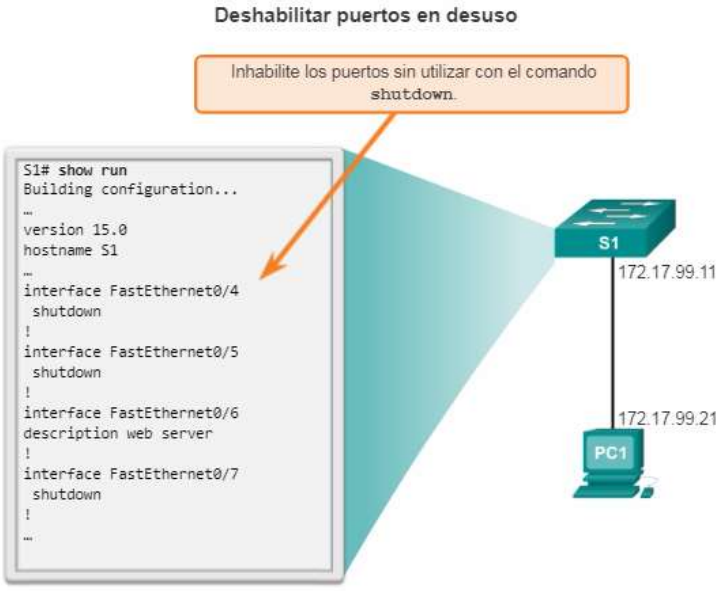


Imagen N° 7: Seguridad de puertos
Fuente: cisco.netacad.net/Academy

Para realizar cambios de configuración a varios puertos de un switch es sencillo. Si se debe configurar un rango de puertos, use el comando interface range.

> Switch(config)# interface range "escriba el módulo/primer-número – último-número"

El proceso de habilitación e inhabilitación de puertos puede llevar mucho tiempo, pero mejora la seguridad de la red y vale la pena el esfuerzo.

2.2.6.4 VLAN (Red de área local virtual).

El rendimiento de la red es un factor importante en la productividad de una organización. Una de las tecnologías que contribuyen a mejorar el rendimiento de la red es la división de los grandes dominios de difusión en dominios más pequeños. La función de proporcionar acceso a una LAN suele reservarse para los switch de capa de acceso. Se puede crear una red de área local virtual (VLAN) en un switch de capa 2 para reducir el tamaño de los dominios de difusión, similares a los dispositivos de capa 3. Por lo general, las VLAN se incorporan al diseño de red para facilitar que una red dé soporte a los objetivos de una organización. Si bien las VLAN se utilizan principalmente dentro de las redes de área local conmutadas, las implementaciones modernas de las VLAN les permiten abarcar redes MAN y WAN.

a) **Beneficios de una VLAN.** Los principales beneficios de utilizar las VLAN son los siguientes:
   - **Seguridad:** Los grupos que tienen datos sensibles se separan del resto de la red, lo que disminuye las posibilidades de que ocurran violaciones de información confidencial.
   - **Reducción de costos:** El ahorro de costos se debe a la poca necesidad de actualizaciones de red costosas y al uso más eficaz de los enlaces y del ancho de banda existentes.
   - **Mejor rendimiento:** La división de las redes planas de capa 2 en varios grupos de trabajo lógicos (dominios de difusión) reduce el tráfico innecesario en la red y mejora el rendimiento.
   - **Dominios de difusión reducidos:** La división de una red en redes VLAN reduce la cantidad de dispositivos en el dominio de difusión.
   - **Mayor eficiencia del personal de TI:** Las VLAN facilitan el manejo de la red debido a que los usuarios con requerimientos similares de red comparten la misma VLAN.

b) **Segmentación de VLAN:** Las VLAN proporcionan la segmentación y la flexibilidad organizativa, es una manera de agrupar dispositivos dentro de una LAN como si

estuvieran conectados al mismo cable. Las VLAN se basan en conexiones lógicas, en lugar de conexiones físicas. Las VLAN permiten que el administrador divida las redes en segmentos según factores como la función, el equipo del proyecto o la aplicación, sin tener en cuenta la ubicación física del usuario o del dispositivo. Los dispositivos dentro de una VLAN funcionan como si estuvieran en su propia red independiente, aunque compartan una misma infraestructura con otras VLAN. Cualquier puerto de switch puede pertenecer a una VLAN, y los paquetes de unidifusión, difusión y multidifusión se reenvían y saturan solo las estaciones terminales dentro de la VLAN donde se originan los paquetes.

Cada VLAN se considera una red lógica independiente, y los paquetes destinados a las estaciones que no pertenecen a la VLAN se deben reenviar a través de un dispositivo que admita el routing. Las VLAN habilitan la implementación de las políticas de acceso y de seguridad según grupos específicos de usuarios. Cada puerto de switch se puede asignar a una sola VLAN

c) **Tipos de VLAN:** Existen diferentes tipos de redes VLAN, algunos tipos de VLAN se definen según las clases de tráfico y según la función específica que cumplen.
   - **VLAN de datos:** Es una VLAN configurada para transportar tráfico generado por usuarios. Las VLAN de datos se usan para dividir la red en grupos de usuarios o dispositivos.
   - **VLAN predeterminada:** Todos los puertos de switch se vuelven parte de la VLAN predeterminada después del arranque inicial de un switch que carga la configuración predeterminada. Los puertos de switch que participan en la VLAN predeterminada forman parte del mismo dominio de difusión. Esto admite cualquier dispositivo conectado a cualquier puerto de switch para comunicarse con otros dispositivos en otros puertos de switch. La VLAN predeterminada para los switch Cisco es la VLAN 1.
   - **VLAN nativa:** Una VLAN nativa está asignada a un puerto troncal 802.1Q. Los puertos de enlace troncal 802.1Q admiten el tráfico proveniente de muchas VLAN (tráfico con etiquetas), así como el tráfico que no proviene de una VLAN (tráfico sin etiquetar). El tráfico con etiquetas hace referencia al tráfico que tiene una etiqueta de 4 bytes insertada en el encabezado de la trama de Ethernet original, que especifica la VLAN a la que pertenece la trama. El puerto de enlace troncal 802.1Q coloca el tráfico sin etiquetar en la VLAN nativa, que es la VLAN 1 de manera predeterminada. Una VLAN nativa funciona

como identificador común en extremos opuestos de un enlace troncal.

- **VLAN de administración:** Una VLAN de administración es cualquier VLAN que se configura para acceder a las capacidades de administración y configuración de un switch. La VLAN 1 es la VLAN de administración de manera predeterminada en los Switch.
  Para crear la VLAN de administración, se asigna una dirección IP y una máscara de subred a la interfaz virtual de switch (SVI) de esa VLAN, lo que permite que el switch se administre mediante HTTP, Telnet, SSH o SNMP. Dado que en la configuración de fábrica de un switch Cisco la VLAN 1 se establece como VLAN predeterminada, la VLAN 1 no es una elección adecuada para la VLAN de administración.

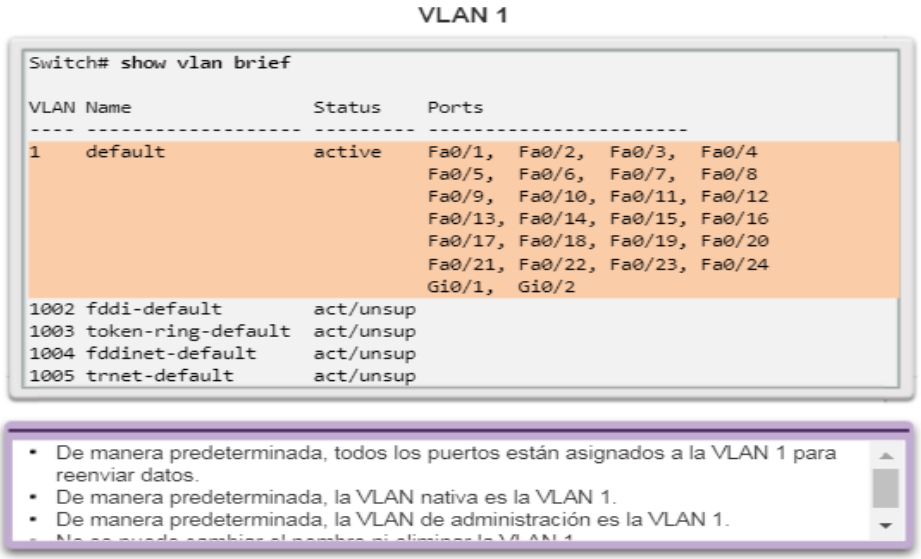


Imagen N° 8: VLAN en un switch CISCO
Fuente: Cisco.netacad.net/Academy

d) Creación de una VLAN. Para la creación de una VLAN en un Switch Cisco se utiliza el siguiente comando:

S1(config)# vlan *"# nro. de VLAN"*

Luego de crear una VLAN, el siguiente paso es asignar puertos a la VLAN. Un puerto de acceso puede pertenecer a una sola VLAN por vez; una excepción a esta regla es un puerto conectado a un teléfono IP, en cuyo caso, hay dos VLAN asociadas al puerto: una para voz y otra para datos.
El comando ***switchport mode access*** es optativo, pero se aconseja como práctica recomendada de seguridad.

Con este comando, la interfaz cambia al modo de acceso permanente.
El comando switchport access vlan fuerza la creación de una VLAN si es que aún no existe en el switch.
Se puede cambiar la pertenencia de puertos de una VLAN con el comando:

no switchport access vlan

No es necesario eliminar primero un puerto de una VLAN para cambiar su pertenencia de VLAN. Cuando se vuelve a asignar la pertenencia de VLAN de un puerto de acceso a otra VLAN existente, la nueva pertenencia de VLAN simplemente reemplaza la pertenencia de VLAN anterior.

Creación de una VLAN

Comandos de IOS de un switch Cisco	
Ingrese al modo de configuración global.	`S1# configure terminal`
Cree una VLAN con un número de ID válido.	`S1(config)#vlan id-vlan`
Especifique un nombre único para identificar la VLAN.	`S1(config-vlan)#name nombre-vlan`
Vuelva al modo EXEC privilegiado.	`S1(config-vlan)# end`

Imagen N° 9: Creación de una VLAN
Fuente: cisco.netacad.net/Academy

Asignación de puertos a las VLAN

Comandos de IOS de un switch Cisco	
Ingrese al modo de configuración global.	`S1# configure terminal`
Ingrese al modo de configuración de interfaz para la SVI.	`S1(config)# interface id_interfaz`
Establezca el puerto en modo de acceso.	`S1(config-if)# switchport mode access`
Asigne el puerto a una VLAN.	`S1(config-if)# switchport access vlan id_vlan`
Vuelva al modo EXEC privilegiado.	`S1(config-if)# end`

Imagen N° 10: Asignación de puertos a una VLAN
Fuente: cisco.netacad.met/Academy

e) Enrutamiento entre VLAN.

Se utilizan enlaces troncales para transportar información de varias VLAN entre dispositivos. Sin embargo, debido a que estas VLAN segmentan la red, es necesario un proceso de capa 3 para permitir que el tráfico pase de un segmento de red a otro.

Este proceso de routing de capa 3 puede implementarse utilizando un router o una interfaz de switch de capa 3. El uso de un dispositivo de capa 3 proporciona un método para controlar el flujo de tráfico entre segmentos de red, incluidos los segmentos de red creados por las VLAN.

2.2.6.5 FUNCIONAMIENTO Y CONFIGURACIÓN DEL SWITCHING DE CAPA 3.

En los comienzos de las redes conmutadas, el switching era rápido (corría a la velocidad del hardware, es decir que la velocidad era equivalente al tiempo físico que tomaba recibir las tramas y reenviarlas a otros puertos) y el routing era lento (debía procesarse mediante software). Esto hizo que los diseñadores de redes ampliaran la porción conmutada de la red al máximo posible.

El acceso, la distribución y las capas de núcleo solían configurarse para comunicarse en la capa 2, pero esta topología generaba problemas de bucles. Para resolver estos problemas, se utilizaron tecnologías de árbol de expansión a fin de prevenir los bucles sin necesidad de renunciar a la flexibilidad y la redundancia de las conexiones entre switch. Sin embargo, a medida que las tecnologías de redes evolucionaron, el routing se volvió más rápido y económico.

Hoy en día, el routing se puede llevar a cabo a la velocidad del hardware. Una consecuencia de esta evolución es que el routing se puede transferir a las capas de núcleo y de distribución sin afectar el rendimiento de la red.

La mayoría de las redes empresariales utilizan switch multicapa para obtener altas velocidades de procesamiento de paquetes con switching basado en hardware. Los switch de capa 3 suelen tener un rendimiento de switching de paquetes en el orden de los millones de paquetes por segundo (pps), mientras que los router tradicionales proporcionan switching de paquetes en el orden de 100 000 a más de 1 millón de pps. Todos los switch multicapa Catalyst admiten los siguientes tipos de interfaces de capa 3:

- **Puerto enrutado:** una interfaz puramente de capa 3 similar a la interfaz física de un router IOS de Cisco.
- **Interfaz virtual del switch (SVI):** una interfaz VLAN virtual para routing entre VLAN. En otras palabras, las SVI son las interfaces VLAN enrutadas de manera virtual.

Todos los switch Cisco Catalyst de capa 3 admiten protocolos de routing, pero varios modelos de switch Catalyst requieren un software mejorado para admitir características específicas de protocolos de routing. Muchos usuarios están en VLAN separadas,

y cada VLAN suele ser una subred distinta. Por lo tanto, resulta lógico configurar los switch de distribución como Gateway de capa 3 para los usuarios de la VLAN de cada switch de acceso. Esto significa que cada switch de distribución debe tener direcciones IP que coincidan con la VLAN de cada switch de acceso. Los puertos de capa 3 (enrutados) se suelen implementar entre la capa de distribución y la capa de núcleo.

2.2.6.5.1 Motivos para configurar una SVI.

Se detallan los siguientes motivos.

- Para proporcionar un Gateway a una VLAN a fin de poder enrutar el tráfico dentro o fuera de esa VLAN.
- Para proporcionar conectividad IP de capa 3 al switch.
- Para admitir las configuraciones de puente y de protocolo de routing.

2.2.6.5.2 Alcance de redes remotas.

Un router puede descubrir redes remotas de dos maneras:

- **Manualmente:** las redes remotas se introducen de forma manual en la tabla de rutas por medio de rutas estáticas.
- **Dinámicamente:** las rutas remotas se descubren de forma automática mediante un protocolo de routing dinámico.

2.2.6.6 ROUTING ESTÁTICO.

El routing estático proporciona algunas ventajas en comparación con el routing dinámico, como:

- Las rutas estáticas son más seguro: no se anuncian a través de la red.
- Las rutas estáticas usan menos recursos del router: consumen menos ancho de banda que los protocolos de routing dinámico.
- No se utiliza ningún ciclo de CPU para calcular y comunicar las rutas.
- La ruta que usa una ruta estática para enviar datos es conocida.

El routing estático tiene tres usos principales:

- Facilita el mantenimiento de la tabla de routing en redes más pequeñas en las cuales no está previsto que crezcan significativamente.
- Proporciona routing hacia las redes de rutas internas y desde estas. Una red de rutas internas es aquella a la cual se accede a través un de una única ruta y cuyo router no tiene otros vecinos.
- Utiliza una única ruta predeterminada para representar una ruta hacia cualquier red que no tenga una coincidencia más específica con otra ruta en la tabla de routing. Las rutas

predeterminadas se utilizan para enviar tráfico a cualquier destino que esté más allá del próximo router ascendente.

Las rutas estáticas se suelen utilizar en los siguientes casos:

- Para conectarse a una red específica
- Para proporcionar un Gateway de último recurso para una red de rutas internas
- Para reducir el número de rutas anunciadas mediante el resumen de varias redes contiguas como una sola ruta estática
- Para crear una ruta de respaldo en caso de que falle un enlace de la ruta principal

Un administrador de red puede configurar una ruta estática de forma manual para alcanzar una red específica. A diferencia de un protocolo de routing dinámico, las rutas estáticas no se actualizan automáticamente, y se deben volver a configurar de forma manual cada vez que cambia la topología de la red. Una ruta estática no cambia hasta que el administrador la vuelve a configurar en forma manual.

2.2.6.6.1 Configuración de rutas estáticas IPv4

Las rutas estáticas se configuran con el comando *ip route* de configuración global. La sintaxis del comando es la siguiente:

Router(config)# ip route ***dirección-red*** ***máscara-subred*** ***dirección-ip*** ***interfaz de salida***

Se requieren los siguientes parámetros para configurar el routing estático:

- Dirección de red: Dirección de red de destino de la red remota que se agrega a la tabla de routing, también llamada “prefijo”.
- Máscara subred: Máscara de subred, o simplemente máscara, de la red remota que se agrega a la tabla de routing. La máscara de subred puede modificarse para resumir un grupo de redes.

Además, deberá utilizarse uno de los siguientes parámetros o ambos:

- Dirección IP: Dirección IP del router de conexión que se va a utilizar para reenviar el paquete a la red de destino remota. Se la suele denominar “siguiente salto”.
- Interfaz-salida: interfaz de salida que se va a utilizar para reenviar el paquete al siguiente salto.

Imagen N° 11: Sintaxis del comando IP ROUTE
Fuente: cisco.netacad.met/Academy

2.2.6.6.2 Configuración de rutas predeterminadas IPv4.

Una ruta predeterminada es una ruta estática que coincide con todos los paquetes. En lugar de almacenar todas las rutas para todas las redes en la tabla de routing, un router puede almacenar una única ruta predeterminada que represente cualquier red que no esté en la tabla de routing.

Los routers suelen utilizar rutas predeterminadas configuradas de forma local, o bien, descubiertas por otro router, mediante un protocolo de routing dinámico. Una ruta predeterminada se utiliza cuando ninguna otra ruta de la tabla de routing coincide con la dirección IP de destino del paquete. Es decir, si no existe una coincidencia más específica, entonces se utiliza la ruta predeterminada como el gateway de último recurso.

El comando para una ruta estática predeterminada es similar a la sintaxis del comando de cualquier otra ruta estática, con la excepción de que la dirección de red es 0.0.0.0 y la máscara de subred es 0.0.0.0. La sintaxis del comando básico de una ruta estática predeterminada es la siguiente:

ip route 0.0.0.0 0.0.0.0 { dirección-ip | interfaz-salida }

Imagen N° 12: Configuración De Ruta Estática Predeterminada
Fuente: cisco.netacad.met/Academy

2.2.6.6.3 Configuración de rutas estáticas flotantes.

Las rutas estáticas flotantes son rutas estáticas que tienen una distancia administrativa mayor que la de otra ruta estática o la de rutas dinámicas. Son muy útiles para proporcionar un respaldo a un enlace principal. De manera predeterminada, las rutas estáticas tienen una distancia administrativa de 1, lo que las hace preferibles a las rutas descubiertas mediante protocolos de routing dinámico. Por ejemplo, las distancias administrativas de algunos protocolos de routing dinámico comunes son las siguientes:

- ✓ **EIGRP = 90**
- ✓ **IGRP = 100**
- ✓ **OSPF = 110**
- ✓ **IS-IS = 115**
- ✓ **RIP = 120**

La distancia administrativa de una ruta estática se puede aumentar para hacer que la ruta sea menos deseable que la ruta de otra ruta estática o una ruta descubierta mediante un protocolo de routing dinámico. De esta manera, la ruta estática "flota" y no se utiliza cuando está activa la ruta con la mejor distancia administrativa. Sin embargo, si se pierde la ruta de preferencia, la ruta estática flotante puede tomar el control, y se puede enviar el tráfico a través de esta ruta alternativa. Una ruta estática flotante se puede utilizar para proporcionar una ruta de respaldo a varias interfaces o redes en un router. También es independiente de la encapsulación, lo que significa que puede utilizarse para reenviar paquetes desde cualquier interfaz, sin importar el tipo de encapsulación.

Es importante tener en cuenta que el tiempo de convergencia afecta una ruta estática flotante. Una ruta que pierde y restablece una conexión de manera continua puede hacer que la interfaz de respaldo se active innecesariamente.
Para configurar rutas estáticas IPv4, se utiliza el comando ip route de configuración global y se especifica una distancia administrativa. Si no se configura ninguna distancia administrativa, se utiliza el valor predeterminado (1).

Imagen N° 13: Esquema de una ruta Estática Flotante
Fuente: cisco.netacad.met/Academy

Imagen N° 14: Configuración de una Ruta Estática Flotante
Fuente: cisco.netacad.met/Academy

2.2.6.6.4 Comandos para la verificación de una ruta estática.

Para verificar las rutas estáticas son los siguientes:

- Ping
- Traceroute
- show ip route
- show ip interface brief
- show cdp neighbors detail
- show ip route static

III. MATERIALES Y MÉTODOS

3.1 TIPO DE ESTUDIO Y DISEÑO DE CONTRASTACIÓN DE HIPÓTESIS

Está investigación por su propia naturaleza es Descriptiva/Aplicada y con un diseño cuasi experimental, debido a que se aplican los indicadores a un área determinada de la organización.

Para el diseño de la contrastación de la hipótesis se utiliza el método de Diseño con un grupo único con medición antes y después, que consiste en:

- Realizar una medición previa de la variable dependiente a ser utilizada antes de la aplicación de la variable independiente.
- La aplicación de la variable dependiente.
- Una nueva medición de la variable dependiente después de la aplicación de la variable independiente.

3.2 POBLACIÓN YMUESTRA

La población a investigar para este proyecto serían los colaboradores del área de negocios de Edpyme Alternativa de las zonas alejadas, ya que ellos son afectados por no tener la información en línea de manera segura que ayude a lograr los objetivos específicos y cumplir con la estimación de crecimiento de acuerdo al plan institucional de la empresa.

Como la población es un aproximado de 10 colaboradores distribuidos en las diferentes sedes de las zonas rurales, se toma como muestra el total de los trabajadores para la presente investigación.

3.3 HIPOTESIS

Con la implementación de un servicio de red GNU/Linux se mejorará la gestión de acceso a la red de datos e internet para las agencias en las zonas rurales en la empresa Edpyme Alternativa.

3.4 VARIABLES

Se consideran las siguientes variables.

- **Variable Independiente.**
  Implementación de un servicio de red GNU/Linux
- **Variable Dependiente.**
  Gestión de acceso a la red de datos e internet.

3.5 INDICADORES

Variables	Dimensión	Indicadores	Medida o Instrumento	Unidad de Medida
Servicio de Red GNU/Linux	Seguridad	Numero de hosts permitidos	Reportes del servicio instalado	% de Accesos
		Número de hosts denegados		
	Gestión de Costos	Gastos en equipos de comunicación	Costos operativos por sedes	Soles
		Gastos en Infraestructuras de red tipo MPLS		
Gestión de acceso a la red de datos e internet.	Comunicación	Número de sedes interconectadas	Entrevista	% de sedes
		Trafico de red	Reportes del servicio instalado	paquetes de Información
	Trafico	Caídas del servicio de Internet	Reportes del servicio instalado	Tiempo

Tabla 1: Indicadores

3.6 MÉTODOS, TÉCNICAS E INSTRUMENTOS DE RECOLECCIÓN DE DATOS

3.6.1 MÉTODOS.

El método a utilizar en la presente investigación, es el Científico debido a que se ejecuta a raíz de una situación problemática real, abordándose con la construcción teórica en que se fundamenta para la elaboración y verificación de la hipótesis. Al mismo tiempo, se presenta la teoría, referente al problema. se recolecta información de cada variable, explorando y describiendo las características relevantes enfocadas al problema.

3.6.2 TÉCNICAS.

Las técnicas para la recolección de datos que se utilizan en el presente estudio son:

- **La Encuesta:** Se define como un procedimiento que consiste en hacer las mismas preguntas, a una parte de la población, que previamente fue definida y determinada a través de procedimientos estadísticos de muestreo.
- **La Entrevista.** Es un procedimiento similar a la encuesta con la diferencia que las preguntas se desarrollan de forma oral obteniendo las respuestas de igual forma.

Con estas técnicas se ha logrado conocer información de determinados hechos a través de las opiniones de grupos o individuos con presencia del investigador responsable de recolectar la información.
La encuesta se aplicó a los colaboradores de las sedes rurales, mientras que la entrevista fue aplicada a la Gerencia de Negocios, Oficial de seguridad de la Información y a responsable de oficina de Sedes rurales.

3.6.3 INSTRUMENTOS.

Como instrumentos tenemos el cuestionario y la guía de preguntas como instrumentos para la recolección de los datos. El cuestionario, contiene preguntas cerradas y categorizadas. Las razones que justifican dicha elección se derivan de las ventajas proporcionadas por este instrumento; haciéndose más fácil la posterior tabulación e interpretación de los resultados.
La guía de preguntas, consta de una serie de interrogantes dirigidas a la gerencia o “responsable del negocio”, con el objeto de obtener información referente a la disponibilidad de adoptar o no, esta solución.

3.7 PROCEDIMIENTO

3.7.1 DETERMINAR LA SITUACIÓN ACTUAL.

Se ha recopilado toda la documentación sobre el diagrama de la red existente en Edpyme Alternativa, para poder tener un conocimiento real y un criterio concreto del estado y su funcionamiento del mismo.
Esta información nos servirá para conocer los niveles de seguridad que se tiene con las sedes existentes y la interconexión hacia la sede central donde se encuentran los servicios de TI.

La estructura de la red actual de Edpyme Alternativa, está administrada principalmente por dos proveedores ISP como son CLARO Y BITEL, ofreciendo un servicio del tipo MPLS, donde cada proveedor cuenta con una cabecera en la sede Central y la sede alterna y un equipo cliente en agencias.

Para las sedes rurales no existe conectividad hacia la sede principal, solo usan el Internet de algún proveedor ISP como, Claro, telefónica, Bitel, VSAT, sin un control centralizado de accesos no existe una administración centralizada de usuarios, por lo que se asume que todo usuario en estas zonas es administrador de la máquina que utiliza.

3.7.2 REDISEÑO DE LA RED.

Los cambios en la configuración de red pueden generar un riesgo alto para la empresa y así mismo resultar muy costosos si no se hace con la debida planificación e identificando los riesgos asociados. Esta nueva configuración implica modificaciones en los equipos conectados, tales como ordenadores, routers y otros.

Para ello se instalará un servidor demo el cual nos servirá para realizar pruebas de interconectividad, acceso a la red LAN mediante la conexión VPN site to site, generar reportes del uso del Internet como el consumo por sitio Web y porcentajes de descargas a nivel de usuario, con estos reportes podremos determinar las medidas de seguridad y establecer nuevas normas regulatorias sobre el uso del Internet para estas zonas rurales.

3.7.3 IMPLEMENTACIÓN.

Con los resultados de determinar la situación actual y el rediseño de la red se iniciará la implementación configurando el servidor con las soluciones de: VPN, Firewall, Control de Ancho de banda, proxy Spam, Filtro de Contenidos, Detección de Intrusos IDS y Prevención de Intrusos IPS, se realizarán distintas pruebas con cada servicio configurado lo cual garantizará el correcto funcionamiento del proyecto.

3.7.4 PRUEBAS DE FUNCIONALIDAD.

Se realizarán las pruebas necesarias para asegurar la funcionalidad de cada uno de los servicios implementados, con la finalidad de que cada uno de los servicios funcione de forma adecuada de acuerdo a las necesidades de Edpyme Alternativa.

IV. RESULTADOS

Para la aplicación del servicio de red GNU/LINUX, aplicable para mejorar la gestión de acceso a la red de datos e internet en las zonas rurales, se tuvo como referencia la metodología planteada por el área de Tecnologías de la Información de la empresa Edpyme Alternativa.

4.1 FASE I: RECOPILACIÓN DE INFORMACIÓN ACERCA DE LA RED

De acuerdo al esquema de red de Edpyme Alternativa, se verifica que la interconexión entre la sede principal que se ubica en Chiclayo donde se encuentran los servicios de información del sistema Core del negocio y las sedes situadas en las diferentes regiones del norte peruano como Lambayeque, Piura, La Libertad, Cajamarca, Amazonas y San Martin, se realiza mediante la red MPLS que es brindada por los proveedores CLARO y BITEL. Estas sedes se interconectan con la sede principal mediante una red VPN del tipo site to site a la cabecera central en la sede principal y en caso de que la red MPLS se corte, de manera transparente y automática las sedes buscan una segunda ruta hacia la sede alterna que se ubica en la ciudad de Olmos, donde se encuentra el servidor de base de datos alterno del sistema, con lo que se tiene alta disponibilidad de los servicios.

El acceso a los servicios de información como navegación a Internet y servicio de correo se realiza a través de un equipo firewall gestionado por CLARO, para lo cual el acceso a estos servicios de red se controla por su segmento de red IP y por perfiles de usuario los cuales son: perfil Operativo, perfil administrativo, perfil de control e invitados.

Así mismo se verifica que no existe interconexión entre las sedes remotas en las zonas rurales, semi rurales y la sede principal. Estas sedes se encuentran aisladas dentro de la red de Edpyme Alternativa, por consiguiente, estas sedes no tienen acceso al sistema Core del negocio (sistema NetBank) lo que es una fuerte limitante para que los colaboradores de esta zona puedan desarrollar su trabajo y apoyar con los objetivos de crecimiento de la institución. Estas sedes acceden a Internet de manera libre y no cuentan con ningún de sistema de seguridad (Firewall, Controles de acceso, contenido, etc.) que evite que el personal en estas sedes se distraiga y no se dedique de manera exclusiva a su labor diaria para lo cual fue contratado.
También se ha tomado en cuenta que dentro del POA 2017-2018 aprobado por el Directorio de Edpyme Alternativa en enero 2017, se considera la expansión y crecimiento de la institución con énfasis en zonas rurales.

4.1.1 DIAGRAMA ACTUAL DE LA RED DE EDPYME ALTERNATIVA.

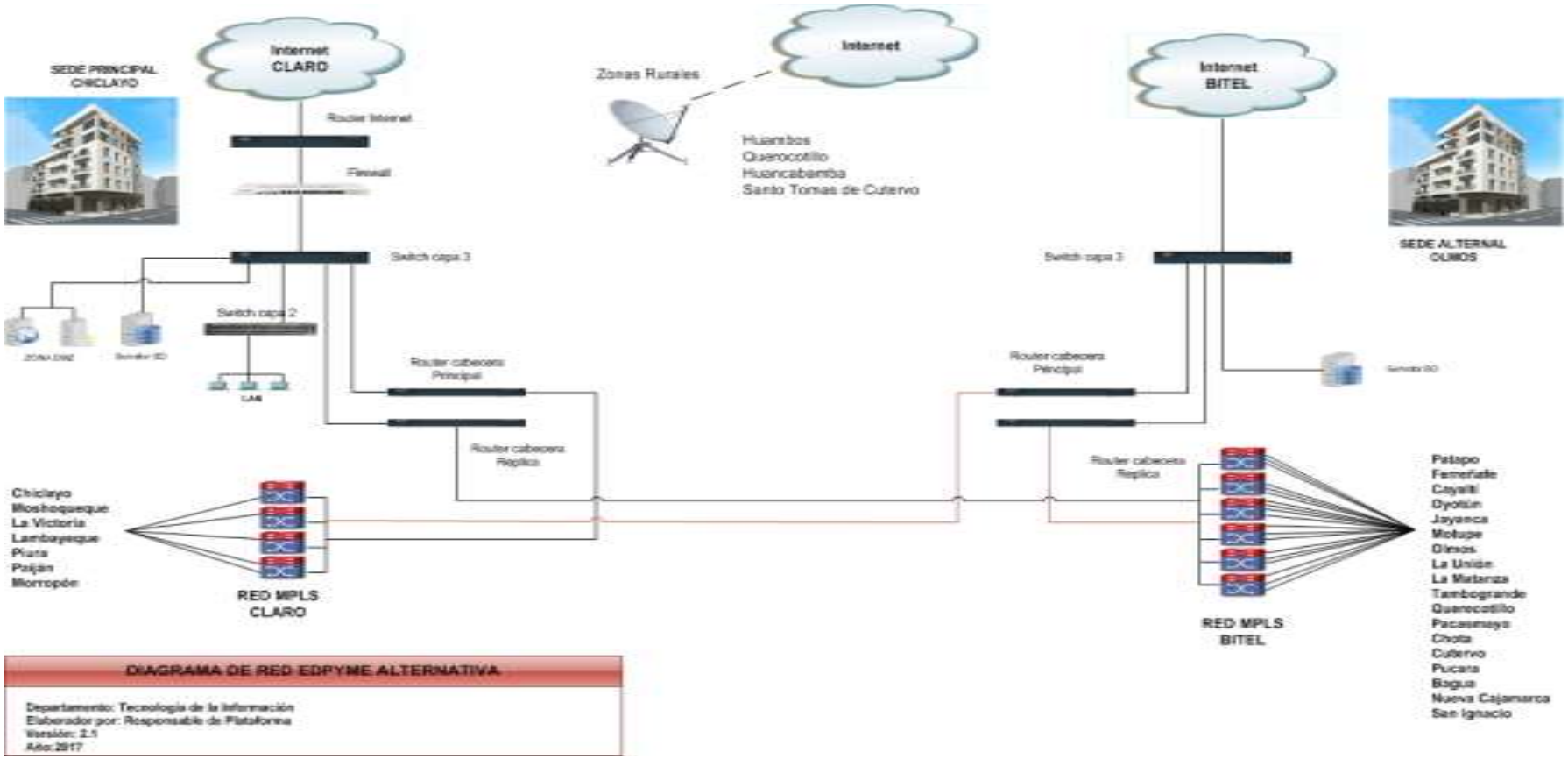


Imagen N° 15: Diagrama de Red de Edpyme Alternativa
Fuente: MAPRO TI – Edpyme Alternativa

4.2 FASE II: ANALISIS DE LOS REQUERIMIENTOS

Para el presente proyecto el análisis de los requerimientos se basará en los siguientes puntos.

- Requisitos para instalar el servicio de accesos a la red e internet mediante el uso de la herramienta GNU/Linux Clear OS 7.0
- Establecer el dimensionamiento actual de los equipos de comunicación existentes.

4.2.1 REQUISITOS GENERALES PARA INSTALAR EL SERVICIO DE RED E INTERNET GNU/LINUX CLEAROS 7.0.

Para este proyecto se detallan a continuación los requisitos generales para la implementación de la herramienta GNU/Linux Clear OS 7.0

- Equipos servidores de gama baja o compatibles (Para Sede principal, alterna y sede remotas).
- Conexión a Internet de Banda Ancha (mínimo 512 kbps) que puede ser redes inalámbricas, ADSL o VSAT.
- Red de área local (LAN) en la sede a implementar
- Lectora CD/DVD conteniendo la imagen de disco de ClearOS 7.0 Community.
- Opcional se puede adquirir la Licencia Bussines edition para soporte.
    -

4.2.1.1 Requisitos mínimos de hardware.

Para este proyecto nos hemos basado en las recomendaciones indicadas en el portal web de la comunidad CLEAROS.

HARDWARE BASE	
PROCESADOR/CPU	Soporte hasta cuatro procesadores - Pentium®, Celeron®, AMD Athlon®; 32-bit o 64-bit
MEMORIA/RAM	Se recomienda al menos 1 GB
DISCO DURO	Se recomienda al menos 10 GB
UNIDAD ÓPTICA/CD-ROM	Se requiere únicamente para la instalación
TARJETA VIDEO	Cualquier tarjeta de video
TARJETA DE SONIDO	No requerida
PERIFÉRICOS	
MOUSE	Sólo requerido para la instalación
MONITOR Y TECLADO	Sólo requerido para la instalación
RED	
CONEXIÓN A INTERNET	Ethernet, cable, DSL, VSAT
TARJETAS DE RED	Dos tarjetas de red, para el modo de puerta de enlace.

Tabla 2: Requerimientos mínimos

Nota: el servidor luego de la instalación no necesita teclado, mouse ni monitor, ya que se comportará como un servidor no dedicado.

4.2.1.2 Directrices de hardware:

Estas guías que se presentan son necesarias para estimar el tipo de hardware que se requiere para el proyecto a instalar. Por lo que es

necesario tener en cuenta que el hardware requerido depende de cómo se use el software. Como ejemplo, un uso continuo del filtro de contenido, generación de reportes y almacenamiento de logs se necesita una mejor performance del equipo de cómputo que el mantener corriendo el propio servicio VPN/Firewall.

RAM Y CPU	5 usuarios	5-25 Usuarios	25-50 Usuarios	50-250 Usuarios	250+ Usuarios
Procesador CPU	Bajo Consumo	Básico	Doble Núcleo	Cuatro Núcleos	Múltiple Núcleo
Memoria RAM	1-2 GB	2-4 GB	4-8 GB	8-16 GB	16-32 GB
Almacenamiento					
Disco Duro	La instalación y los registros requieren 2 GB. Recomendamos 20 GB o más: el almacenamiento opcional adicional depende de usted				
RAID	Recomendado para sistemas de misión crítica (Correo Electrónico, Web).				

Tabla 3: Directrices de Hardware

Los requerimientos descritos en este documento son sólo guías para el usuario y son los recomendados por la comunidad ClearOS. La institución o el usuario final es el que decide qué tipo de equipo de acuerdo a sus necesidades prefiere disponer para su implementación. Para el presente proyecto se presentó dos propuestas de hardware que a continuación se detallan, en ambos casos se realizaron las pruebas y rindieron de acuerdo a la necesidad de la empresa.

- **Propuesta N°01.**
  Equipo servidor de nivel de entrada con rendimiento y confiabilidad, El servidor HPE ProLiant ML30 Gen9 proporciona rendimiento a nivel de servidor en un tamaño silencioso y compacto que es fácil de implementar para una pequeña empresa. Diseñado para emplearse como servidor, lo cual es una ventaja en cuestión de desempeño y confiabilidad.

HP ProLiant ML30 Gen9	
PROCESADOR/CPU	Intel(R) Xeon(R) CPU E5-2600 v3 Series
MEMORIA RAM	**4 GB DDR4 2133MHz**
DISCO DURO	1 TB SATA
TARJETA VIDEO	INCLUIDA
Tarjeta de Red	**02** puertos de 1GB - HPE 332I Network Adapter incluido

Tabla 4 : Propuesta de servidor N°01

Precio de Mercado: USS 715.00
Especificaciones técnicas completas, ver Anexo1

- **Propuesta N°02**

  Se puede usar equipos de escritorio compatibles ensamblados localmente que puede tomar el rol de servidor, pero optando por instalar una fuente de energía con capacidad real considerando que va a estar encendida 24 horas del día durante todo el año y adicionando una tarjeta de red adicional del modelo TPLINK TG3468 ya que el servidor trabajara como VPN, Firewall y Gateway.

PC COMPATIBLE DE ESCRITORIO	
Mainboard	Asus o Intel
Procesador	Intel® Core® i5 de última generación o AMD equivalente
Memoria RAM	4 GB, DDR4 2133MHz Kingston
Almacenamiento	02 discos duros de TB SATA - Wester Digital Black
Tarjeta de Video	Integrada
Tarjeta de Red	02 TPLINK TG3468 10/100/1000 mbps

Tabla 5: Propuesta de Servidor N°02

Precio de Mercado: USS 465.00

4.2.2 CONSIDERACIONES PARA LA IMPLEMENTACIÓN DEL SOFTWARE CLEAROS 7.0.

Se tendrá que tener en cuenta los siguientes servicios a configurar para asegurar la funcionabilidad, disponibilidad e integridad de los sistemas de información en las sedes rurales, donde se viene expandiendo la empresa Edpyme Alternativa.

a) **Balanceo de carga y failover:** Es necesario obtener alta disponibilidad de las conexiones de internet, para Edpyme Alternativa es primordial y de acuerdo a los contratos establecidos con los proveedores de telecomunicaciones en estas sedes es un dilema evaluar el costo/beneficio de los servicios brindados. Para ello implantamos el servicio de balanceo de carga que nos permite establecer las peticiones de internet puedan ser distribuidas en varios dispositivos y así mismo permite tolerancia a fallos en las conexiones de Internet, de modo que siempre se cuenten con al menos una conexión, ofreciendo continuidad del negocio.

b) **Administración centralizada del ancho de banda:** Se ha establecido realizar la asignación de cuotas límites para subidas y descargas de archivos. El rendimiento de las aplicaciones a través de Internet o de la Red de Área interna (LAN) resulta crítico para la institución. Así mismo el correo electrónico, las descargas peer-to-peer y el uso de Internet compiten por los recursos y pueden afectar al rendimiento de aplicaciones críticas. Las Soluciones de Bandwidth Management de ClearOS son dispositivos de

gestión del tráfico de aplicaciones que nos proporcionan visibilidad hacia estos problemas y la capacidad de resolverlos. Basado en la inteligencia a nivel de aplicación de estos equipos, que supervisan, controlan y aceleran el tráfico en la red, proporcionando así una elevada calidad de servicio a las aplicaciones críticas y permitiendo alinear los recursos de red de la organización con las necesidades del negocio.

c) **Filtrado de contenido web:** El Filtro de Contenido WEB, bloquea sitios que no están permitidos por las políticas de seguridad de la empresa, aumentando la productividad del personal y mitigando la posibilidad de infección. Sus funciones básicas son:
   - Controlar y restringir la navegación en una computadora específica.
   - Definir filtros y los aplicarlos por niveles de usuarios de la institución.
   - Bloquear páginas Web con temas específicos tales como: sexo, violencia, drogas, compras, música, juegos, azar, redes sociales, etc., que no significan productividad para la Edpyme Alternativa.
   - Delimitar el tiempo máximo de navegación en Internet, aplicando cuotas para cada usuario de acuerdo al perfil que desempeña en la institución.

d) **Aceleración web proxy:** Se configurará el módulo de servidor Proxy de la herramienta ClearOS como un equipo intermediario situado entre el sistema del usuario e Internet, para registrar el flujo de información de cada usuario, teniendo así el control total del uso del Internet dentro de la Institución. El Proxy guarda en la memoria caché las páginas Web a las que acceden los sistemas de la red. Cuando un sistema solicita la misma página Web, el servidor Proxy utiliza la información guardada en la memoria caché en lugar de recuperarla del proveedor de contenidos. De esta forma, se accede con más rapidez a las páginas Web, se implementará listas de accesos a Web permitidas ACL.

e) **Modulo centralizado antispam y antivirus:** Se encargará de proteger a la red interna verificando datos entrantes y salientes de internet, lo que permite no solo evitar ataques informáticos sino también detectar los equipos dentro de la red local que estén infectados. Así mismo se configurará para escanear el correo durante el manejo de la mensajería y realizará las funciones definidas por las reglas configuradas por el administrador. Para aplicaciones comerciales, Clear Center ofrece reglas de spam adicionales que se actualizan continuamente como un servicio.

f) **Módulo de seguridad contra ataques indeseados y controles de acceso IDS (sistema de detección de intrusos):** Es un Firewall basado en estándares Iptables, configurable de acuerdo a las necesidades de la red local de la empresa. El contar con un servicio de firewall y no un IDS genera con frecuencia un sentido falso de seguridad a la empresa. Aunque los firewalls y otros controles pueden bloquear el acceso no autorizado a los recursos de la red, tienen limitaciones en su capacidad para protegerse de un ataque de Negación de Servicio (DoS), Caballos de Troya, gusanos y demás ataques maliciosos que son más frecuentes. El uso del IDS en la red ayudará básicamente a que el atacante no pueda lanzar una amenaza que pueda penetrar eficazmente las redes protegidas por esta capa adicional de seguridad. Un cambio o aumento repentino en la actividad de los puertos puede indicar un posible ataque, aunque pasaría desapercibido si únicamente se cuenta con un firewall para la protección en el perímetro. El IDS monitorea y analiza constantemente los incidentes que ocurren en un sistema o red informáticos en busca de actividades sospechosas (señales preliminares como rastreos de equipos host o análisis de puertos) o ataques directos que lo alertan en tiempo real para que tome decisiones inmediatas.

g) **Módulo de seguridad para prevención de ataques indeseados y controles de acceso (prevención de intrusos - IPS):** Es un dispositivo que ejerce el control de acceso en una red informática para proteger a los sistemas computacionales de ataques y abusos. La tecnología de Prevención de Intrusos es considerada por algunos como una extensión de los Sistemas de Detección de Intrusos (IDS), pero en realidad es otro tipo de control de acceso, más cercano a las tecnologías cortafuegos. Los IPS fueron inventados de forma para resolver ambigüedades en el monitoreo pasivo de redes de computadoras, al situar sistemas de detecciones en la vía del tráfico. Los IPS presentan una mejora importante sobre las tecnologías de firewall tradicionales, al tomar decisiones de control de acceso basados en los contenidos del tráfico, en lugar de direcciones IP o puertos. También es importante destacar que los IPS pueden actuar a nivel de equipo, para combatir actividades potencialmente maliciosas.

h) **Servicio de servidor firewall perimetral:** Es un dispositivo que filtra el tráfico entre redes. En general se debe verlo como una caja con dos o más interfaces de red en la que se establecen reglas de filtrado con las que se decide si una conexión determinada puede establecerse o no. Sus funciones básicas son:

- Habilitar el acceso a puertos de administración a determinadas IPS privilegiadas.
- Enmascarar el tráfico de la red local hacia el exterior.
- Denegar el acceso desde el exterior a puertos de administración y a todos los que no estén dentro de las reglas marcadas por la institución.

i) Servicio de acceso Virtual Private Network (VPN): Nos va a Permitir la conexión en red de estas oficinas con nuestros sistemas de información tanto en la sede central como réplica, se configurará para crear un túnel entre cliente y servidor estableciendo una comunicación segura usando el protocolo OPEN VPN utilizando como medio el Internet. Este protocolo Ofrece una encriptación segura de 256 bits y es compatible con la mayoría de sistemas operativos de ordenadores de escritorio, ofrece la máxima seguridad en la creación del túnel de datos entre cliente y servidor y los datos se autentican usando certificados digitales. Este protocolo es extremadamente rápido y confiable en redes de trabajo de alta latencia y ofrece control de integridad de datos de su tráfico para asegurar que no han sido manipulados en tránsito.
Se configurará un túnel tanto para enlazar al centro de datos principal como al alterno.

4.3 FASE 3: DISEÑO E IMPLEMENTACIÓN PARA EL SERVICIO DE RED GNU/LINUX

Para el presente proyecto se instalará, implementará, documentará y pondrá en marcha los servicios de VPN, Firewall, filtro de contenido, control de ancho de banda, detección de intrusos, prevención de intrusos y proxy utilizando para ello el Software ClearOS versión 7.0.
Se realizarán las pruebas correspondientes para asegurar su funcionamiento en línea, con lo cual dispondremos de confidencialidad, Integridad y Disponibilidad de los servicios que requiere la empresa Edpyme Alternativa para el logro de los objetivos de acuerdo a su Plan operativo Anual 2018-2020**.**
Para ello se elabora el diseño de la propuesta para las sedes en zonas rurales la cual quedaría de la siguiente manera.

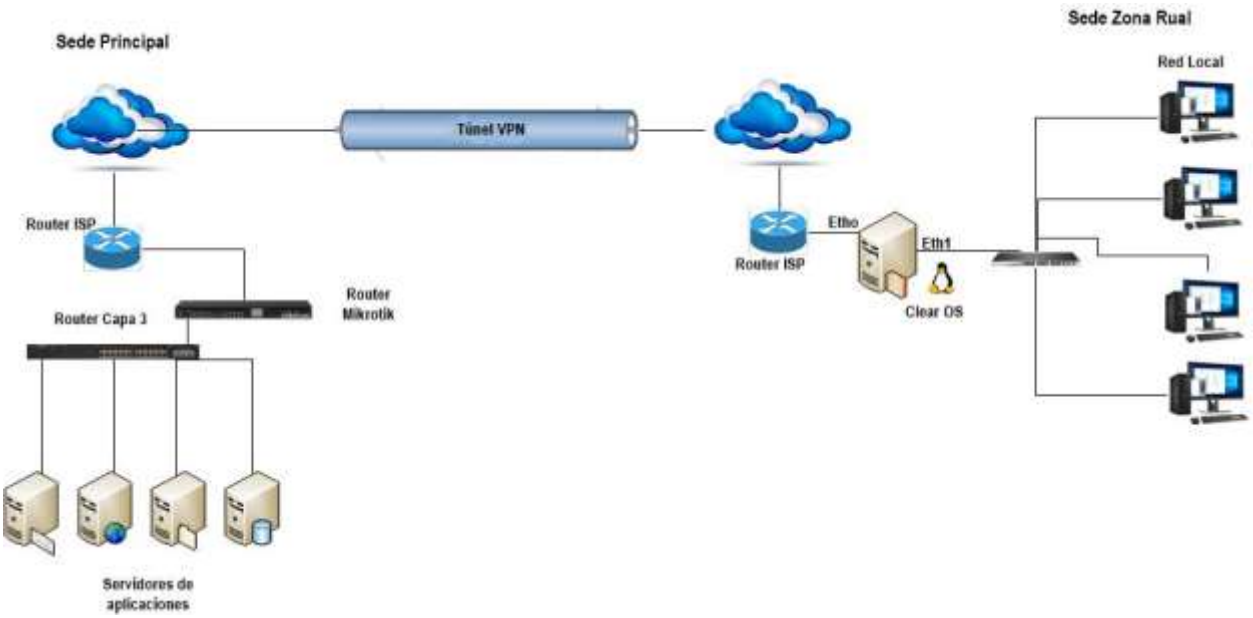


Imagen N° 16: Diagrama de Red – Conexión Sede Santo Tomas de Cutervo
Fuente: Área de TI – Edpyme Alternativa

La sede a implementar en el presente proyecto será la sede rural que se ubica en el distrito de Santo tomas de Cutervo, perteneciente a la Provincia de Cutervo en el Departamento de Cajamarca. De acuerdo como se muestra el plano de la ubicación de la oficina, esta sede tendrá como máximo 14 colaboradores entre Analistas de créditos, Servicio de Créditos, Caja, impresoras en red, servicio de video conferencia y Administrador. Los cuales van a necesitar del acceso a la red VPN de Alternativa para acceder a los servicios de información como Sistema, Navegación Web y Correo electrónico, utilizando para ello el servicio de ClearOS 7.0.

Para ello dentro de la distribución del plano de esta sede se ha acondicionado un espacio de aproximadamente 2*2 mts2, donde se alojará el servidor ClearOS y los equipos de comunicación como Switch y Modem/Router del Proveedor de servicios de Internet (ISP).
En esta área se acondicionará 01 Servidor HP o compatible instalado en un gabinete de piso de 24 RU y tendrá su respectiva protección eléctrica como: Línea estabilizada, backup de energía, filtro de trasientes tipo A, y pozo a tierra que cumplan de acuerdo a los códigos nacionales de electricidad CNE.

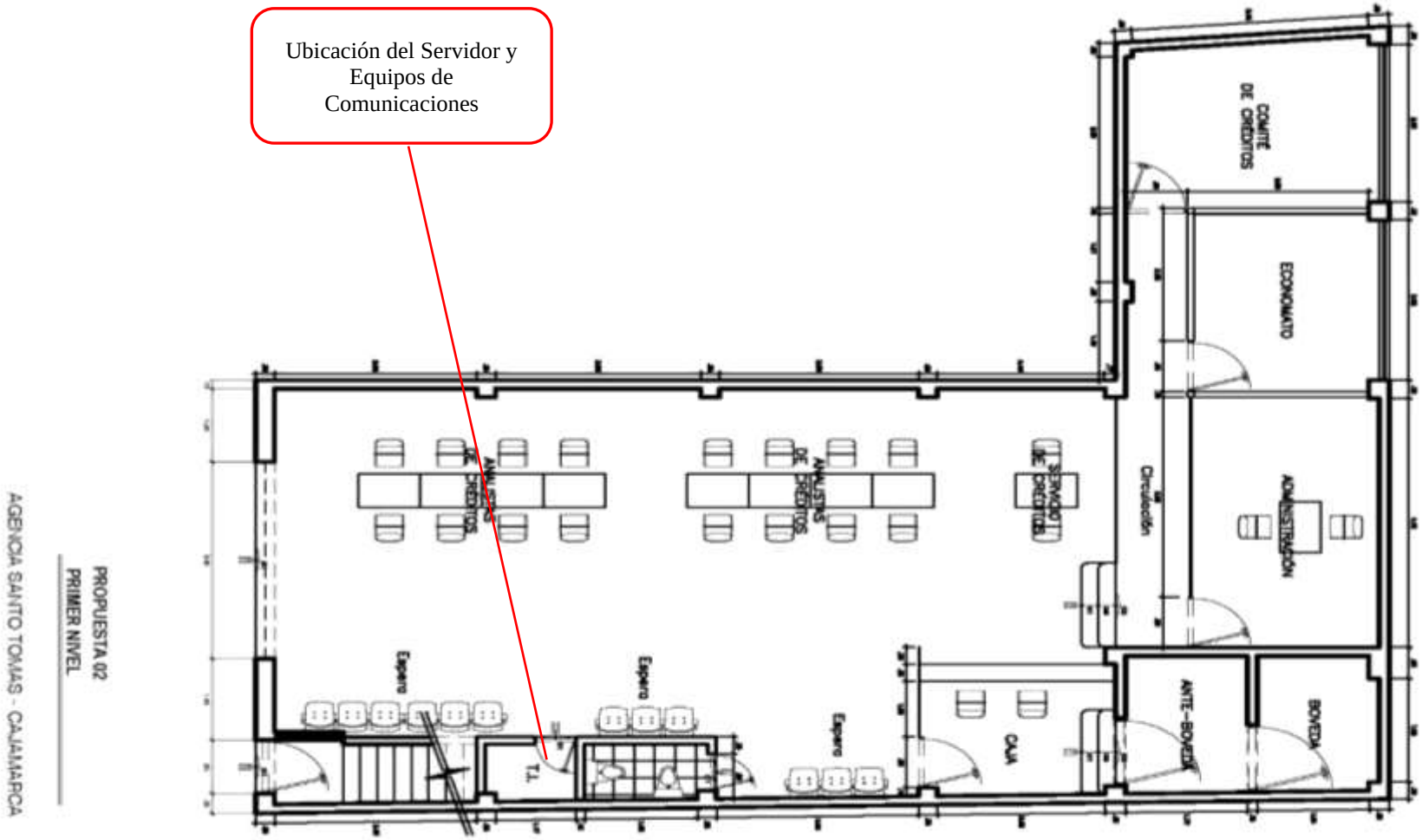


Imagen N° 17: PLANO DE SEDE RURAL – SANTO TOMAS DE CUTERVO
Fuente: Área de Administración – Edpyme Alternativa

4.4 FASE 4: REDISEÑO DE LA RED

4.4.1 DIMENSIONAMIENTO DE LOS EQUIPOS DE COMUNICACIÓN EXISTENTES.

Para enlazar este servicio con la red existente se va a adicionar algunas configuraciones en los equipos de comunicación con las que cuenta funcionando la red de Edpyme Alternativa de acuerdo a su diagrama de red existente.

Estos equipos a configurar son 02 Switch Catalyst 3650 Capa 3 de 24 puertos de la marca Cisco y que se encuentran ubicados en la sede principal y Olmos. Ambos tienen las mismas características técnicas y que se resumen en la siguiente tabla.

TIPO	MARCA	MODELO	DETALLE	VERSION DE IOS	UBICACIÓN
SWITCH Capa 3	Cisco	Catalyst 3650 Series	24 puertos 10/100/1000	03.03.04SE RELEASE SOFTWARE (fc3) (universalk9)	Sede Principal
SWITCH Capa 3	Cisco	Catalyst 3650 Series	24 puertos 10/100/1000	03.03.04SE RELEASE SOFTWARE (fc3) (universalk9)	Sede Olmos (contingencia)

Tabla 6: Dimensionamiento de equipos de comunicación

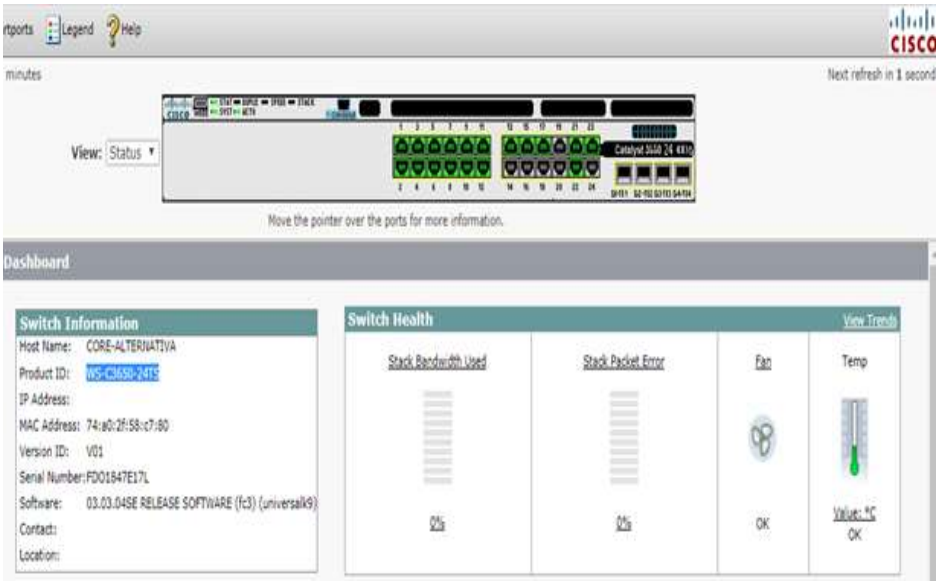


Imagen N° 18: Equipo Cisco Capa 3 Catalyst 3650
Fuente: Área de TI – Edpyme Alternativa

4.4.2 CONFIGURACIÓN DE LOS EQUIPOS SWITCH CISCO Y ROUTING MIKROTIK EXISTENTES.

Para el presente proyecto se va a configurar los equipos de comunicación existentes el acceso para establecer rutas estáticas para que los usuarios de las sedes en la zona rural, puedan acceder también a los sistemas de información.

4.4.2.1 CONFIGURACIÓN DEL SWITCH CAPA 3 CISCO:

Esta configuración se va realizar primero a los Switch capa 3 de la sede principal como la de Olmos que es donde se encuentra el centro de datos alterno, para que ante alguna contingencia no se pierda la continuidad operativa**.**

Nota: Antes de realizar cualquier cambio debemos realizar una **copia de seguridad** de la configuración existente para ello realizamos los siguientes pasos:

- Ingresamos mediante el cable consola o por el puerto de red que contiene la interface administrativa del Switch Cisco, utilizando para ello la herramienta libre tftpd32, con la cual establecemos una sesión Telnet con el que podemos conectarnos al Switch Cisco.
- Ingresamos nuestras credenciales y digitamos el siguiente comando:

  Router#copy running-config tftp
- Con este comando nos pedirá la dirección IP de la Pc de donde tenemos instalado el programa tftp instalado y luego nos pedirá el nombre del archivo para guardar.

a) Rutas a Adicionar: Cisco Capa 3 – Sede Principal:

En primer lugar, se creará una VLAN para este servidor, con la finalidad de separar las conexiones y tener mejor control de las peticiones que vengan desde la red VPN de la herramienta ClearOS, para ello utilizamos los siguientes comandos.

enable
conf term
vlan 60
name VPN-rural
end
configure term
interface fa 0/20
switchport mode access
switchport access vlan60
no shutdown
end
interface vlan60
ip address 192.168.99.98 255.255.255.252
end

Luego se agregarán estas rutas que sirven para que todos los paquetes que salgan de la red de Edpyme Alternativa sean canalizados a través de la red VPN del servidor ClearOS.

- **Rutas para clientes individuales**
  ip route 172.18.0.0 255.255.0.0 192.168.99.98

- **Rutas para clientes en sedes zonas rurales (Ruta Ficticia)**
  ip route 192.168.117.0 255.255.255.0 192.168.98.99

b) Cisco Capa 3 – Sede Olmos Replica o Contingencia:

Se creará una VLAN para este servidor con el mismo fin de la configuración anterior.
enable
conf term
vlan 60
name VPN-rural
end
configure term
interface fa 0/20
switchport mode access
switchport access vlan60
no shutdown
end
interface vlan60
ip address 192.168.9.99 255.255.255.252
end
También se adicionará las siguientes rutas

- **Rutas para clientes individuales"**
  ip route 172.18.0.0 255.255.0.0 192.168.9.99

- **Rutas para clientes en sedes**
  ip route 192.168.117.0 255.255.255.0 192.168.9.99

4.4.2.2 CONFIGURACIÓN DEL SERVIDOR VPN MIKROTIK

En el equipo VPN MIKROTIK, tanto de la oficina principal se creará las credenciales de acceso para los servicios VPN de ClearOS instalados en las distintas sedes rurales donde se expande Edpyme Alternativa, para ello se va a configurar lo siguiente:

- Primero se va crear una regla adicional en /IP / firewall /crear nueva regla > para habilitar el puerto TCP 1194 (ovpn MIKROTIK solo funciona con TCP).
- Se crean los certificados de autenticidad de la siguiente manera:
  /certificate add name=ca-template common-name=CA-%MikroTik Identity% key-usage=key-cert-sign,crl-sign
  /certificate add name=server-template common-name=SERVER
  /certificate add name=client-%Client Name%-template common-name=client-%Client Name%
- Luego se procede a firmar los certificados
  /certificate sign ca-template ca-crl-host=%MikroTik Local IP% name=CA-%MikroTik Identity%

/certificate sign ca=CA-%MikroTik Identity% server-template name=SERVER
/certificate sign ca=CA-%MikroTik Identity% client-%Client Name%-template name=client-%Client Name%

- Luego se exporta los certificados de autenticidad creados con el protocolo open VPN.
- Habilitar OVPN Y configurarlo de la siguiente manera.
  /PPP /interface /OVPN Server. (Ver Figura N°20)
- En /PPP /secret crear un nuevo secret y definir los siguientes parámetros de acuerdo a la figura N°21.

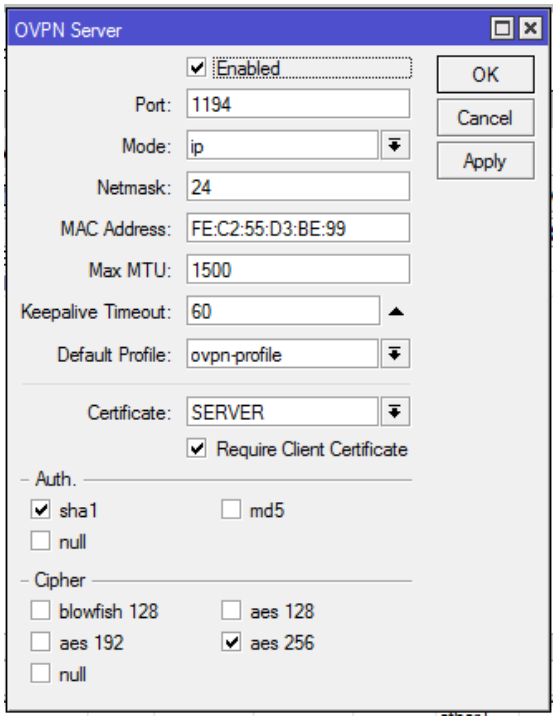


Imagen N° 19: Configuración VPN MIKROTIK
Fuente: Área de TI – Edpyme Alternativa

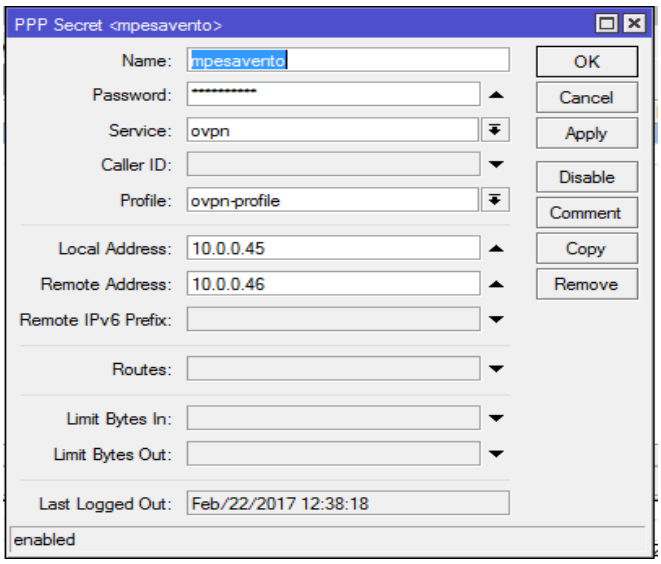


Imagen N° 20: Configuración VPN MIKROTIK

4.5 FASE 4: IMPLEMENTACIÓN UN SERVIDOR CLEAROS CON HERRAMIENTAS DE OPTIMIZACIÓN Y ADMINISTRACIÓN DE INTERNET.

Para el presente proyecto se ha instalado el paquete de software libre CLEAROS en su versión 7.0, de la cual se ha configurado los siguientes servicios:

4.5.1 SERVICIO PROXY.

Se configura este servicio por la interfaz de administración basada en gráficos, con la finalidad de almacenar una lista de páginas web permitidas visitadas que usara el personal de negocios con la finalidad que al acceder sea más rápida la navegación, para ello establecemos los siguientes parámetros:

- **Puerto:** De modo predeterminado, SQUID utilizará el puerto 3128 para atender peticiones, aunque puede configurarse para que use cualquier otro. Para incrementar la seguridad, se vinculará el servicio a una IP a la que sólo se pueda acceder desde la red autorizada.

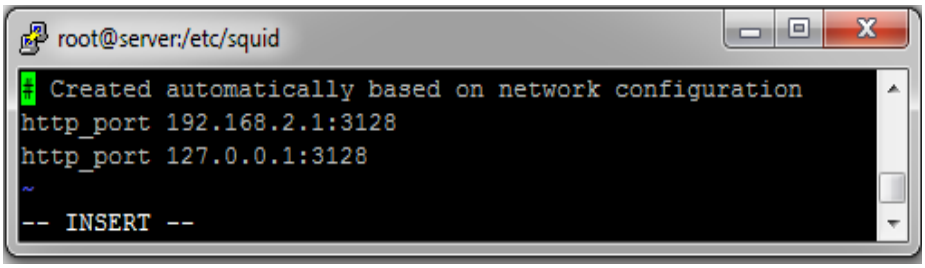


Imagen N° 21: Configuración del servició SQUID - ClearOS, configuración de puertos.

- **Cache de almacenamiento:** Se fijará el espacio en disco que se usará para almacenar las páginas visitadas. Por defecto SQUID usa 100Mb, como límite para el tamaño del caché, pero en este caso se lo fijará en 2000Mb o 2 Gb.
- **Lista de controles de acceso – ACL:** Se crearon listas de control de acceso que abarque a toda la red local o quienes tienen permiso de navegar o no, el control individual se hará por IP. Cada una de las ACL's tendrá asociadas reglas de control que regularán esta actividad. Es decir, definirán unas listas, por una parte, estableciendo reglas específicas para cada una de ellas, se creará la ACL que dirá cuando es necesario usar password para poder navegar. Se ha creado el ACL para el control de navegación por horarios, con el periodo de tiempo denominado Horario Normal, que pertenece al horario de lunes a viernes de 07:00am a 15:00pm, y el otro periodo, que pertenece al horario del fin de semana de 07:00am a 01:00pm, que se denominará Horario Fin Semana.

  Una vez creados los periodos de tiempo se crearán las listas de control de acceso correspondientes a cada periodo.

Para los periodos Horario Normal y Fin de semana se creará el ACL con las siguientes características

- Nombre del ACL.
- Tipo de ACL: Permitido (se pondrán las reglas que se definirán para el efecto).
- Periodo de tiempo:
- Restricciones: Within time restrictions (dentro de las restricciones de tiempo).
- Método de Identificación: Group user (grupos de usuarios).

- **Políticas y reglas de control de acceso:** Se aplican a las listas de control de acceso creadas

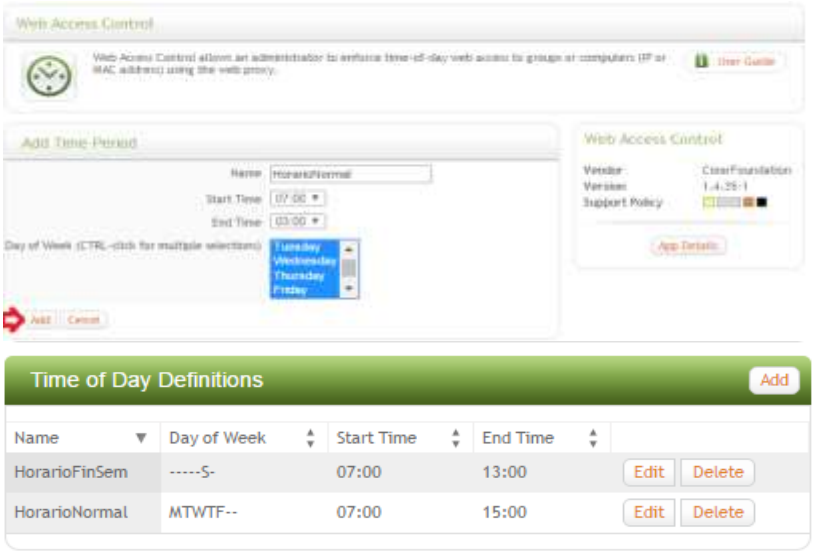


Imagen N° 22: El Servicio SQUID - ClearOS, configuración de horarios.

4.5.2 FILTRO DE CONTENIDO.

Para asegurar una navegación limpia de los usuarios del área de negocios, se realiza mediante la herramienta DansGuardian, la cual tiene la particularidad de trabajar conjuntamente con el servidor proxy Squid.
DansGuardian se encuentra en el intermedio de comunicación entre el navegador web del cliente y el servidor proxy, de esta manera intercepta y modifica toda la petición que se realiza y que el servidor deba atender.

- **Configuración de la lista exceptioniplist.** En este archivo se almacena la lista de direcciones IP de clientes que no usarán el filtro y tendrán acceso libre a internet.
- **Configuración de la lista bannedphraselist:** Contiene la lista de frases prohibidas. Las frases pueden contener espacios para obtener mayor beneficio del filtrado. Esta es la parte más útil de DansGuardian y filtrará más páginas que combinando los filtros de imagen y url juntos. También puede usarse combinaciones de frases, que, de ser encontradas en una página, serán bloqueadas. En este caso se usarán servidores de blacklist existentes y que continuamente se están actualizando. En nuestro caso hemos usado servidores que en listan y clasifican listas negras a nivel

mundial. Para que sea más efectivo el control es mejor buscar una base de datos donde estén las paginas peligrosas por categorías, se descarga una lista de páginas prohibidas de la página http://urlblacklist.com, la que se descomprimirá en el archivo de configuración: /etc/dansguardian-av/list/blacklist/, para permitir tener de forma automática la actualización de las páginas.

- **Configuración de lista bannedmimetypelist:** Contiene una lista de tipos MIME prohibidos (Multipurpose Internet Mail Extensions), si una URL retorna un tipo MIME, incluida en esta lista, DansGuardian lo bloqueará. Esta es una forma interesante de bloquear aplicaciones no deseadas, por ejemplo, videos, música, aplicaciones zip, etc.

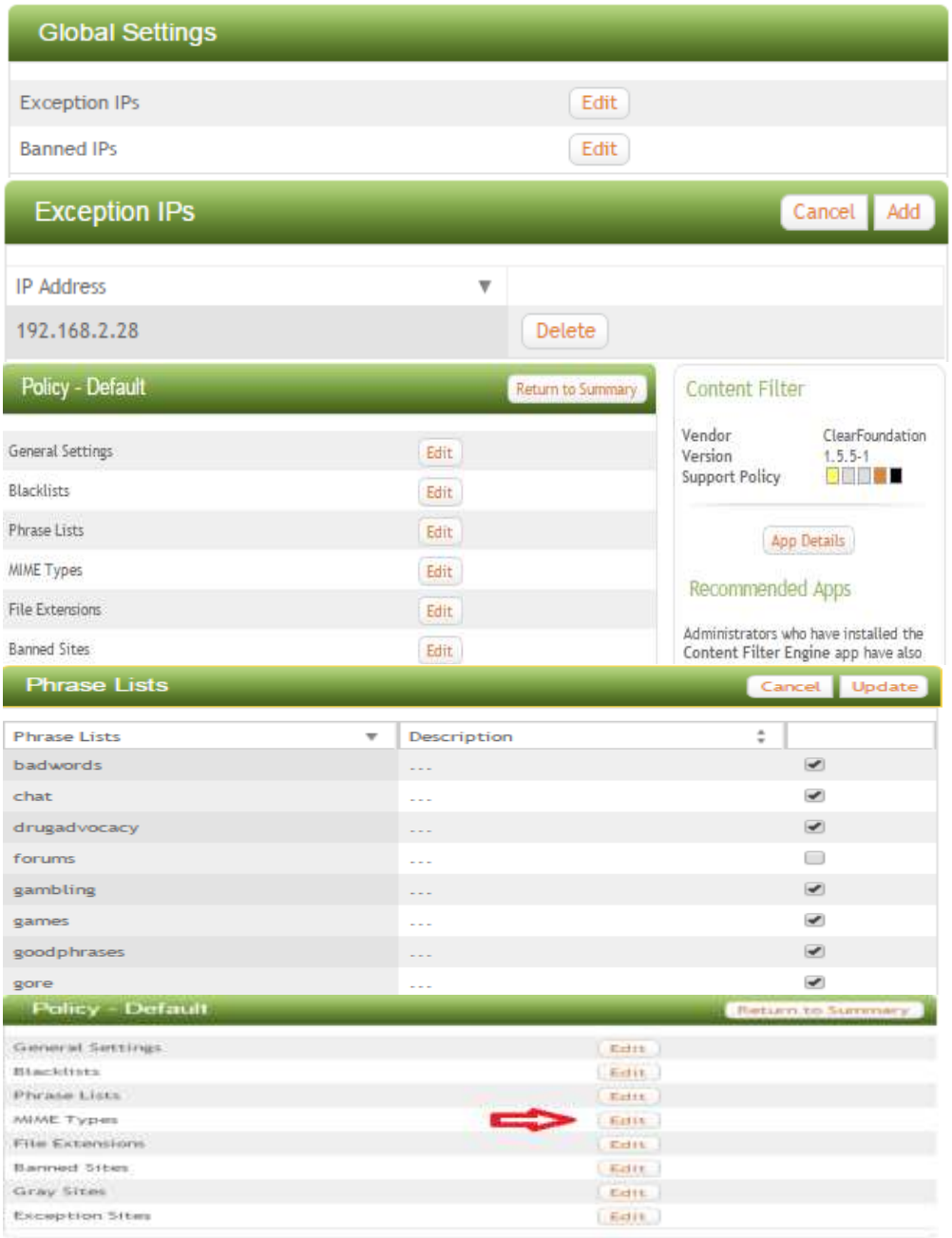


Imagen N° 23: Tabla gráfica de filtro de contenido- ClearOS

4.5.3 EL SERVICIO FIREWALL.

Para asegurar el acceso a los sistemas de información solo por personal de Edpyme Alternativa, mediante IP permitidas, se ha configurado este servicio a través del fichero de configuración IPTABLES, con esto se conseguirá mitigar incidentes de seguridad en los sistemas de información.

En el archivo IPTABLES se crean reglas, dirigiendo a cada una de ellas diferentes características que deben cumplir todos los paquetes que entren o salgan del área perimetral del servidor. Además, para cada regla se especifica y se aplica una acción. Las reglas tienen un orden, y cuando se recibe o se envía un paquete, las reglas se verifican en orden hasta que las condiciones que pide una de ellas se cumplen en el paquete, y la regla se activa aplicando sobre el paquete la acción que se haya especificado.

En nuestro caso se ha configurado y usado las siguientes acciones, por ejemplo:

- **Permite el tráfico de internet:**
  iptables -A INPUT –s 192.168.2.0/24 -i eth1 -j ACCEPT
- **Prevenir ataques DDOS:**
  - ✓ Eliminado el ping
    iptables -A INPUT -s 0.0.0.0/0 -i eth0 -p icmp --icmp-type echo-request -j DROP
  - ✓ Limitando conexiones múltiples
    iptables -A INPUT -p tcp --dport 80 -m limit --limit 25/minute --limit-burst 100 -j ACCEPT
- **Permitimos reenvió de paquetes:**
  iptables -A FORWARD -i eth0 -o eth1 -j ACCEPT
- **Enmascaramiento de la red local:**
  iptables -t nat -A POSTROUTING –s 192.168.2.0/24 -o eth0 -j MASQUERADE
- **Apertura realizamos la redirección de puertos:**
  - ✓ Abrimos el puerto 587 SMTP
    iptables -A FORWARD -i eth1 -o eth0 -s 192.168.2.0/24 -d mail.munipicsi.gob.pe -p tcp --dport 587 -j ACCEPT
  - ✓ Abrimos el pop3
    iptables -A FORWARD -i eth0 -o eth1 -s 192.168.2.0/24 -d mail.munipicsi.gob.pe -p tcp --dport 110 -j ACCEPT
- **No se admiten más redirecciones:**
  iptables -A FORWARD -i eth0 -j DROP
  iptables -A FORWARD -s 192.168.2.0/24 -i eth1 -j REJECT

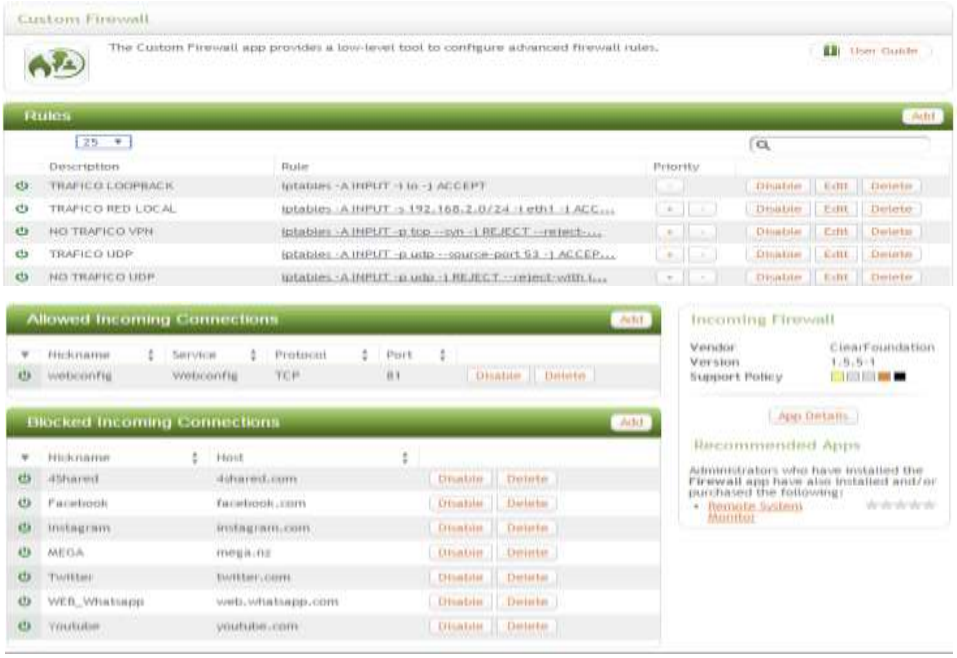


Imagen N° 24: Servicio Firewall- ClearOS

Estas reglas usadas, deben ser bien analizadas y realizar todas las pruebas correspondientes, ya que puede ser causa de problemas si no se fijan con detalle las reglas.

4.5.4 SERVICIO DE DETECCIÓN DE INTRUSOS.

Para este servicio se usa el paquete SNORT, que es un SNIFFER que se encarga de rastrear los paquetes que circulan por la red y al encontrar un paquete sospechoso (según reglas previamente definidas), lo visualiza en una base de datos mediante MySQL.

Imagen N° 25: Reglas del Sistema de detección de intrusos- ClearOS

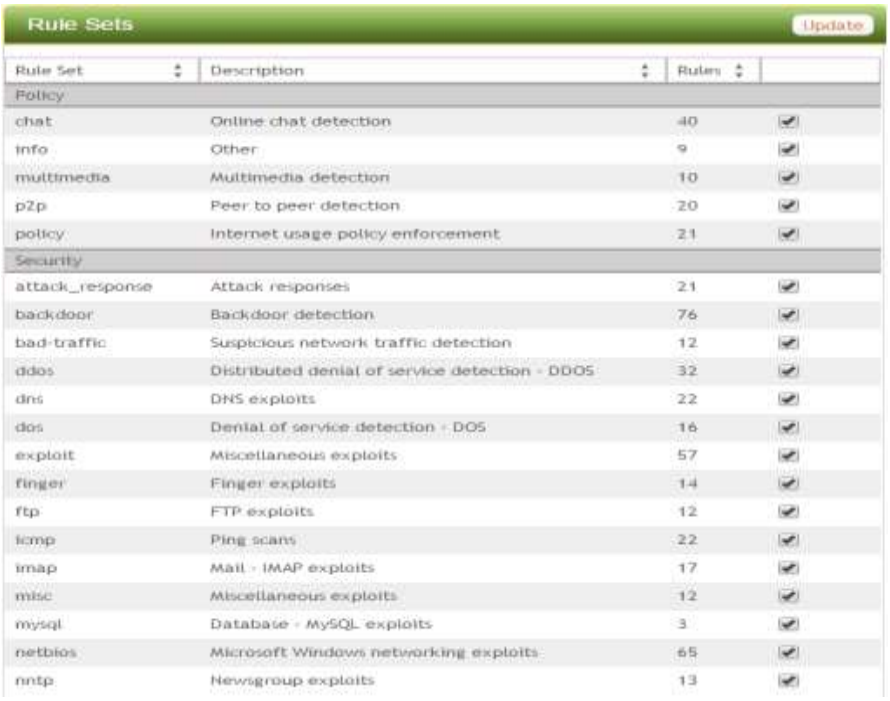


Imagen N° 26: Sistema de detección de intrusos- ClearOS

De manera predeterminada se descargan reglas establecidas por la comunidad desde el site oficial de la aplicación (https://www.snort.org/).

4.5.5 SERVICIO DE CONTROL DE ANCHO DE BANDA

Se establece en la opción Network, Bandwidth donde se debe agregar el ancho de banda que tiene contratada con el ISP que se haya contratado en la zona, para este caso es un servicio ADSL de 6Mbps.

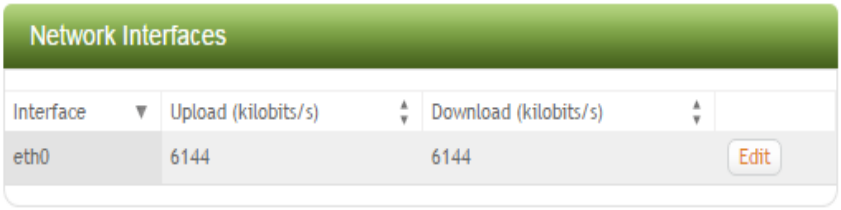


Imagen N° 27: Control de ancho de banda- ClearOS

a) Configuración de reglas globales de bandwidth controller:

Se configura para controlar el ancho de banda en el tamaño de los paquetes de entrada y salida en lo que a correo electrónico se refiere; para ello como política de seguridad de la información existente en la empresa, se establece configurar como un máximo de 1024 kbps para el protocolo de recepción de mail pop3 y 2048 kbps para el protocolo de envió de mail SMTP.

Este ancho de banda es para toda la institución, ya que se considera que el correo electrónico en un porcentaje mayor

a 90% es dirigido dentro de la institución por lo que no necesita para su flujo salir a internet.

b) Configuración de reglas avanzadas para bandwidth controller:

Como regla ya establecida dentro de las políticas de seguridad de Edpyme Alternativa, se establece controlar el ancho de banda de cada uno de los usuarios que acceden al servicio a internet a 512 kbps sin excepción.

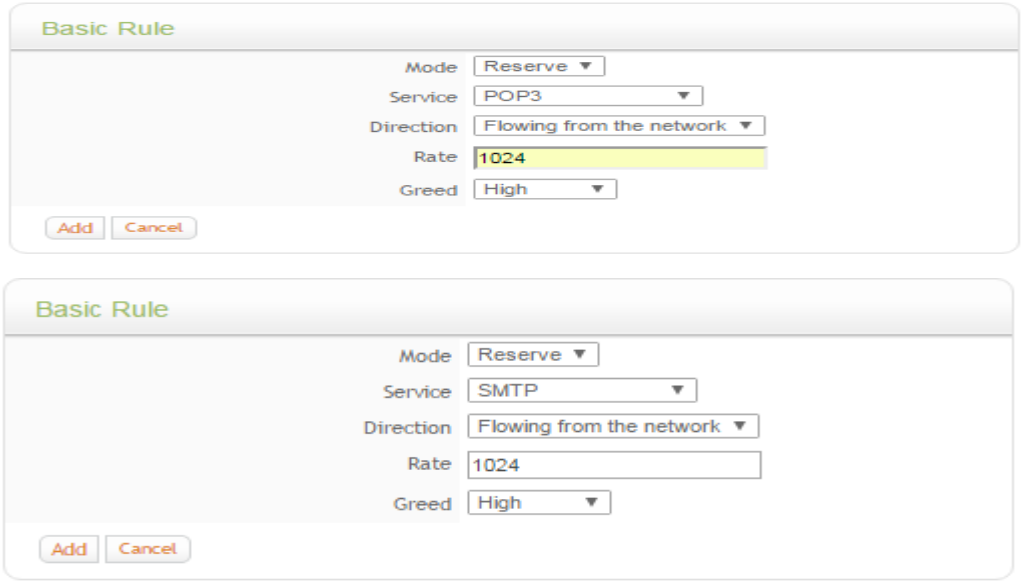


Imagen N° 28: Control de ancho de banda- ClearOS

4.5.6 SERVICIO DE VPN – OPEN VPN.

El servidor OpenVPN de CLEAROS, es una forma segura y rentable de proporcionar acceso VPN a los recursos en la red.

a) Antes de configurar OPEN VPN se debe agregar la siguiente regla para permitir el acceso VPN por el puerto UDP 1194, de acuerdo como lo muestra la figura 30.

b) Luego se debe agregar en la interface de CLEAROS en la opción security and keys, las credenciales ya creadas en el servidor VPN tanto de la cabecera de la oficina principal como la de Olmos.

c) Se debe agregar las subredes para atravesar el túnel al parámetro EXTRALANS en /etc/clearos/network.conf separados por espacios

EXTRALANS = "192.168.25.0/23 172.20.0 / 24"

d) luego de instaladas las credenciales se procede a crear el usuario que se conectara a la red OPEN VPN, los usuarios deben estar configurados con acceso OpenVPN y Certificado de seguridad (figura 319).

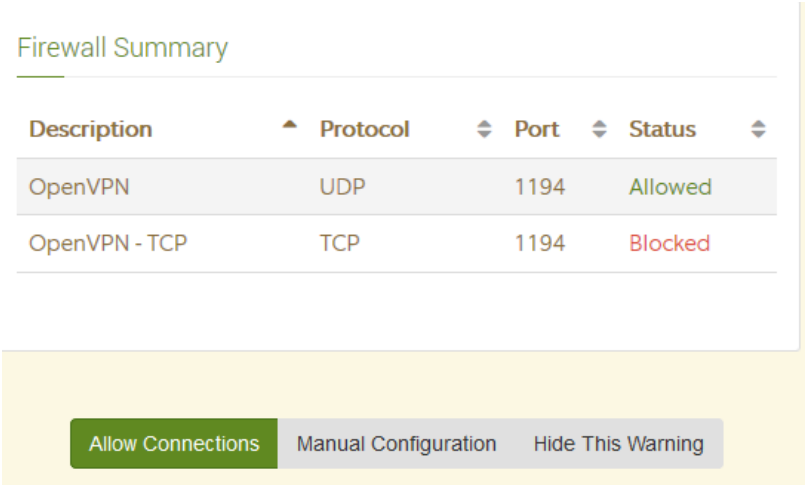


Imagen N° 29: Habilitar regla firewall para OPEN VPN- ClearOS

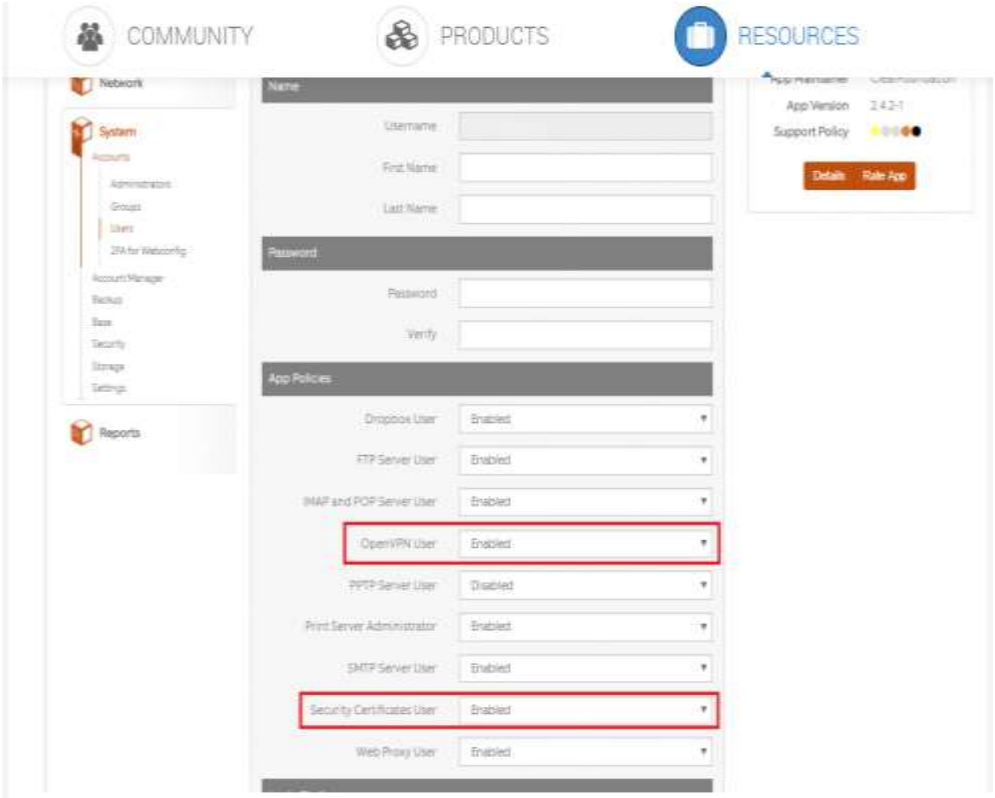


Imagen N° 30: Agregar usuarios para OPEN VPN- ClearOS

4.6 FASE 6: DISEÑO FINAL DE LA SOLUCIÓN

Con estas configuraciones se permite el acceso a los servicios de información de Edpyme Alternativa, para este caso se ha tomado como referencia la sede Santo Tomas de Cutervo. Así mismo el acceso se plasma de la siguiente

manera en el siguiente diagrama, como quedaría la implementación final luego de instalado todo el proyecto:

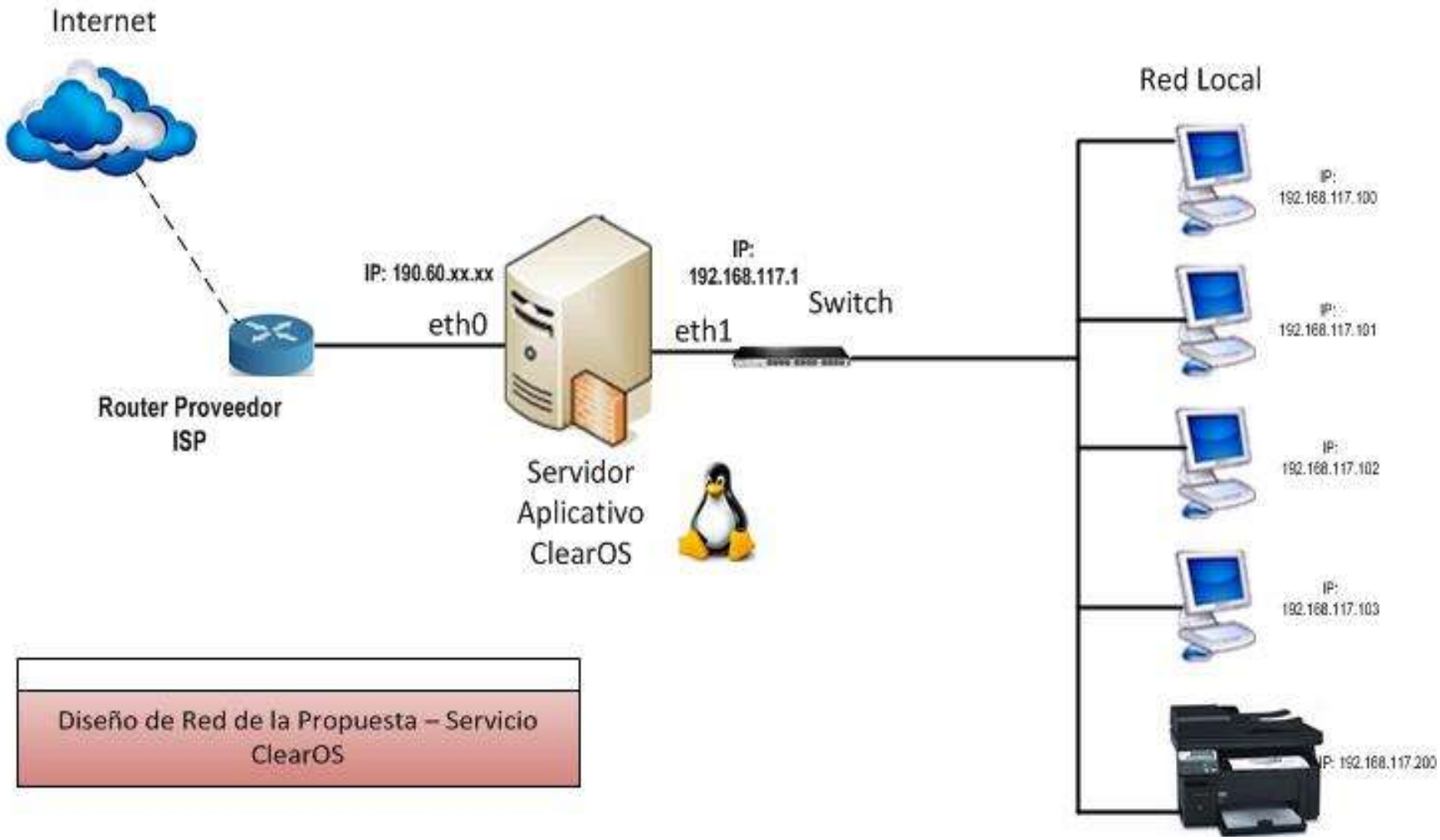


Imagen N° 31: Diagrama de Red para sedes
Fuente: Propia

V. DISCUSIÓN

En el desarrollo de esta investigación se logró comprobar la necesidad que tienen las empresas no solo en el sector micro financiero, sino también de los diferentes sectores comerciales, la necesidad de mantener sus sistemas de información interconectados para el cumplimiento de sus objetivos institucionales, enviando y recibiendo información, en algunos casos por medios de transporte de comunicación de internet no seguros, sobre todo como los que se encuentran en las zonas geográficas donde las tecnologías de comunicaciones no tienen alcance.

Esto con lleva a mencionar lo dicho por Tomas C. (2008) en su tesis de "Servicio VPN de acceso remoto basado en SSL mediante Open VPN" [19] que "Las comunicaciones a través de las redes de información resultan de vital importancia para un gran número de empresas y organizaciones. Para llegar a su destino, ese tráfico debe atravesar, muy a menudo, una infraestructura de redes públicas (como Internet), lo que lo hace vulnerable a los ataques de usuarios mal [19]intencionados".

Teniendo en cuenta estas vulnerabilidades que día a día se hacen más frecuentes, resulta entonces imprescindible poseer con herramientas avanzadas que permitan proteger el contenido de dicho tráfico. Para asegurar tanto su privacidad, Integridad y confiabilidad en las comunicaciones de extremo a extremo. Debido a esta necesidad es que esta investigación se enfocó, al emplear una herramienta basada en software libre aplicada a una empresa del rubro micro finanzas, para lo cual ha quedado demostrado que, con el uso de estas herramientas de software libre, se optimiza y se asegura la conectividad y la seguridad de los sistemas de información de la empresa Edpyme alternativa.

En la siguiente figura se resume del tráfico de la red en la sede rural Santo tomas de Cutervo, donde se puede verificar que se ya se puede controlar el ancho de banda y se da prioridad a los sistemas de información de Edpyme Alternativa. En la gráfica se ve el pico de consumo al mediodía, que es usual, ya que a esa hora se generan los desembolsos vía corresponsalía.

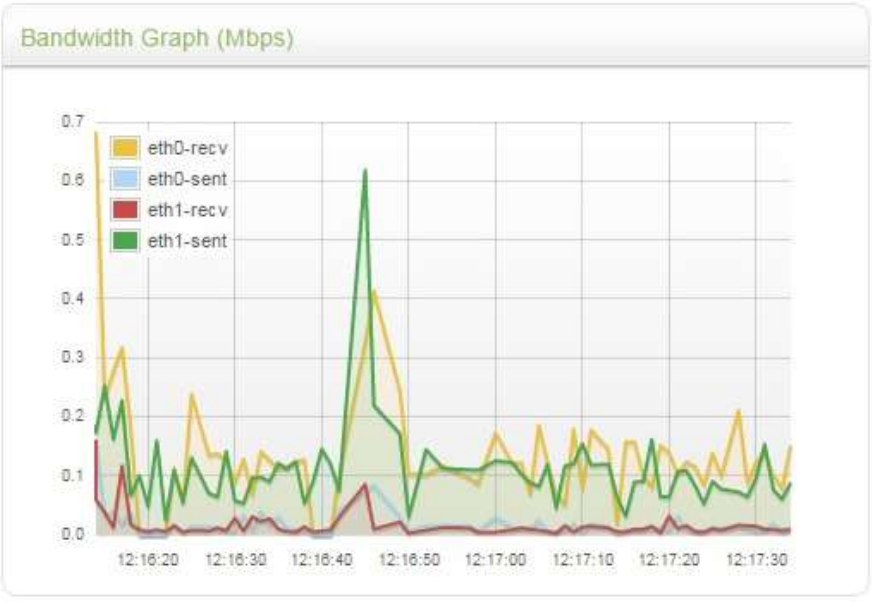


Imagen N° 32: Control de ancho de banda

En la siguiente figura se puede mapear y dar seguimiento a los sitios web más visitados, con lo cual se puede determinar el uso adecuado que se le está dando a internet y si los colaboradores están usando de manera adecuada los servicios de información.

Imagen N° 33: Listado de páginas web visitadas

En la siguiente imagen se muestra a los usuarios reflejados por sus IP, con mayor número de peticiones realizadas en internet, con el cual se puede controlar y mejorar el uso a los sistemas de información.

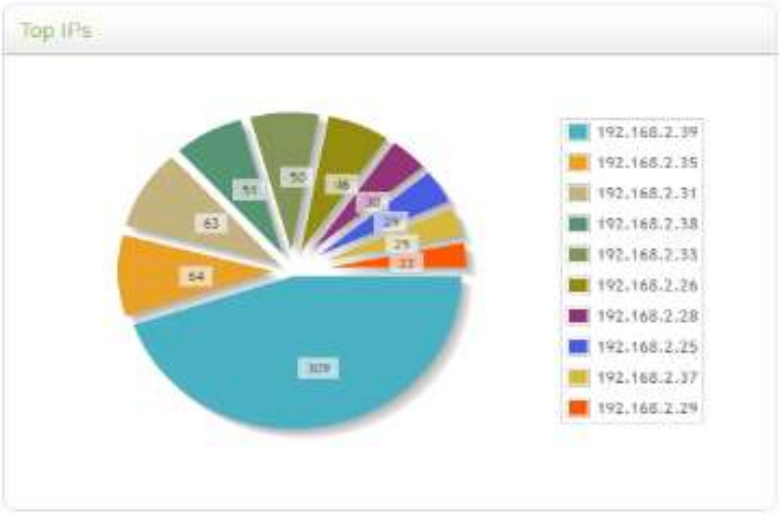
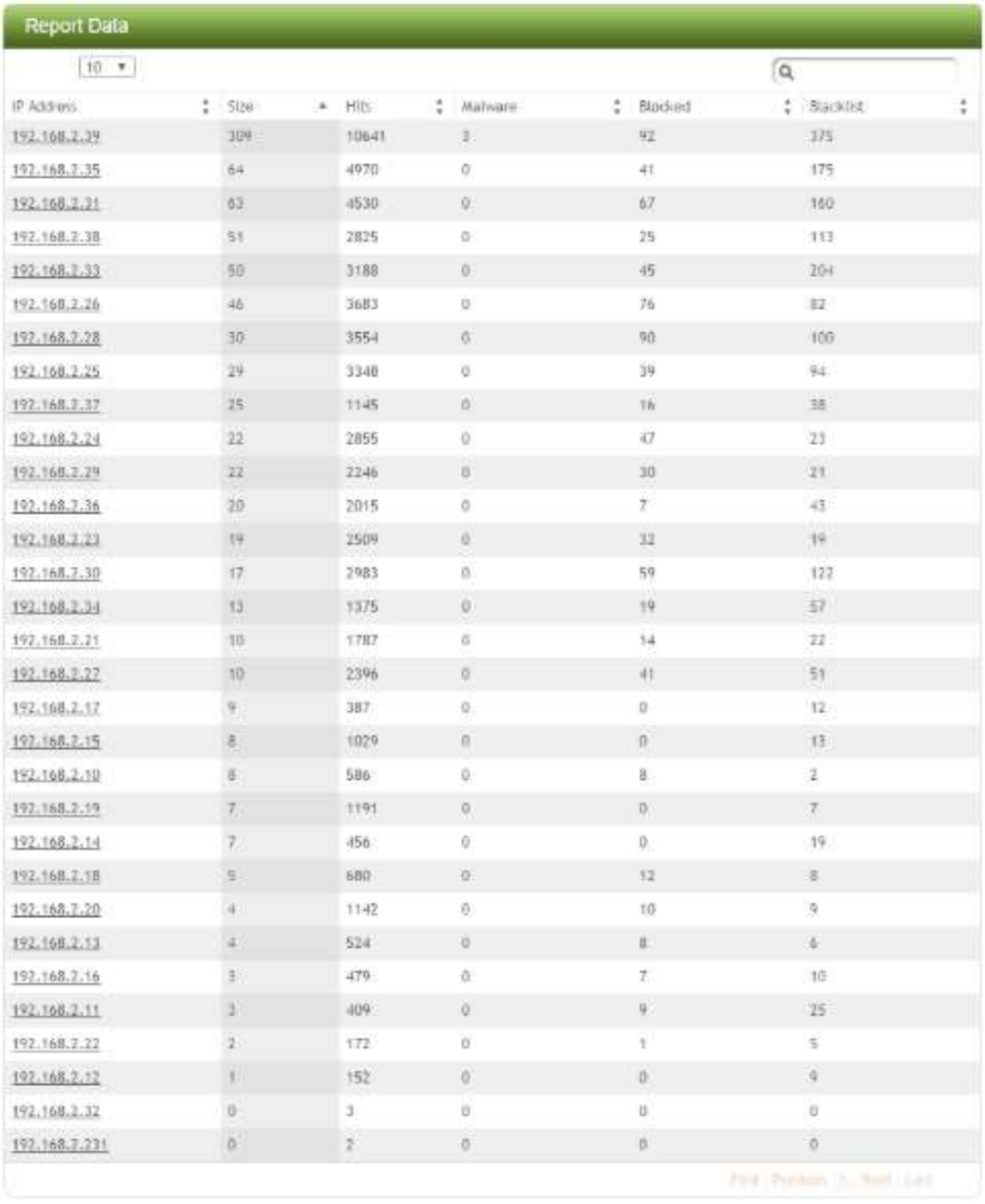


Imagen N° 34: PCS con mayor petición de acceso a los sistemas de información

En la siguiente imagen, se muestra los usuarios que dan mal uso a los sistemas de información y se detalla en el reporte las páginas bloqueadas, con este reporte se realiza las correcciones necesarias al personal para asegurar la operatividad del negocio.



Report Data

10

IP Address	Size	Hits	Malware	Blocked	Blacklist
192.168.2.39	309	10641	3	92	375
192.168.7.35	64	4970	0	41	175
192.168.2.31	63	4530	0	67	160
192.168.2.38	51	2825	0	25	113
192.168.2.33	50	3188	0	45	204
192.168.2.26	46	3683	0	76	82
192.168.7.28	30	3554	0	90	100
192.168.2.25	29	3348	0	39	94
192.168.7.37	25	1145	0	16	38
192.168.2.24	22	2855	0	47	23
192.168.2.29	22	2246	0	30	21
192.168.7.36	20	2015	0	7	43
192.168.2.23	19	2509	0	32	19
192.168.7.30	17	2983	0	59	122
192.168.2.34	13	1375	0	19	57
192.168.7.21	10	1787	0	14	22
192.168.2.27	10	2396	0	41	51
192.168.2.17	9	387	0	0	12
192.168.2.15	8	1029	0	0	13
192.168.2.10	8	586	0	8	2
192.168.2.19	7	1191	0	0	7
192.168.2.14	7	456	0	0	19
192.168.2.18	5	680	0	12	8
192.168.7.20	4	1142	0	10	9
192.168.2.13	4	524	0	8	6
192.168.7.16	3	479	0	7	10
192.168.2.11	3	409	0	9	25
192.168.7.22	2	172	0	1	5
192.168.2.12	1	152	0	0	9
192.168.2.32	0	3	0	0	0
192.168.7.231	0	2	0	0	0

Imagen N° 35: Monitoreo de PCS con páginas bloqueadas

En los resultados que se describen en las imágenes con la implementación del servicio GNU/LINUX, se ha logrado asegurar los puntos de atención de las zonas rurales con la sede principal donde se encuentran los sistemas de información de manera segura, confidencial y sobre todo inalterables. Elevando el rendimiento del personal de negocios en la colocación segura de los créditos y atendiendo de manera oportuna a los clientes.

Con el presente proyecto se apoya en el objetivo institucional que es lograr un mayor crecimiento a través de una mayor presencia en el sector Rural, un fortalecimiento de nuestras operaciones en el sector Urbano y una diversificación de servicios.

De acuerdo a los resultados obtenidos luego de la implementación del proyecto, se puede evidenciar la accesibilidad de manera segura de los servicios de los sistemas de información existente en Edpyme alternativa, necesarios para el logro de los objetivos de la institución remarcados en el POA 2018 – 2019

DISTRIBUCIÓN PRODUCTOS %	Crecimiento al 2019 - I	Nro. de Clientes	Crecimiento al 2019 - II	Nro. de Clientes	2020	Nro. de Clientes
PYME	32.00%	20	31.00%	30	30.00%	40
RURAL	31.00%	20	32.50%	30	33.50%	40
AGRICOLA	9.00%	20	9.00%	30	9.00%	40
VEHICULAR	2.00%	5	3.00%	8	3.50%	12
MEJORANDO CASA	13.00%	15	14.50%	25	14.50%	35
CREDISERVICIO	7.00%	8	8.00%	15	7.50%	20
CONSUMO	6.00%	8	2.00%	15	2.00%	20
Total	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%

Tabla 7: Crecimiento actual de la cartera de créditos y número de clientes
FUENTE: Plan Operativo Institucional 2019 - 2021

En la siguiente imagen se muestra el posicionamiento de acuerdo a estadísticas de la SBS entre el año 2018 y el 2019, en el territorio nacional.

Distribución de Oficinas por Zona Geográfica de las Entidades de Desarrollo a la Pequeña y Micro Empresa

(Al 31 de Diciembre de 2018)

Empresas	Amazonas	Ancash	Apurimac	Arequipa	Ayacucho	Cajamarca	Callao	Cusco	Huanuco	Ica	Junin	La Libertad	Lambayeque	Lima	Loreto	Piura	Puno	San Martin	Tacna	Tumbes	Ucayali	TOTAL
EDPYME ALTERNATIVA	1	-	-	-	-	6	-	-	-	-	-	2	10	-	-	5	-	1	-	-	-	25
EDPYME CREDIVISION	-	-	-	-	-	-	-	4	-	-	-	1	-	1	-	-	-	-	-	-	-	6
EDPYME MARCIMEX S.A.	-	3	-	-	1	2	-	-	1	3	-	8	3	5	2	8	-	4	-	1	1	42
EDPYME MICASITA	-	-	-	-	-	-	-	-	-	-	-	-	-	1	-	-	-	-	-	-	-	1
EDPYME ACCESO CREDITICIO	-	-	-	1	-	-	-	-	-	1	-	1	1	2	-	1	-	-	-	-	-	7
EDPYME INVERSIONES LA CRUZ	-	3	-	4	-	-	4	1	-	3	1	4	3	46	3	12	1	1	-	1	3	90
EDPYME BBVA CONSUMER FINANCE	-	-	-	-	-	-	-	-	-	-	-	-	-	1	-	-	-	-	-	-	-	1
EDPYME GMG	-	1	1	4	1	1	2	3	1	4	1	3	2	18	-	4	1	1	1	1	1	51
EDPYME SANTANDER	-	-	-	-	-	-	-	-	-	-	-	-	-	1	-	-	-	-	-	-	-	1
TOTAL EDPYMES	**1**	**7**	**1**	**9**	**2**	**9**	**6**	**8**	**2**	**11**	**2**	**19**	**19**	**75**	**5**	**30**	**2**	**7**	**1**	**3**	**5**	**224**

Nota: Información obtenida del Anexo No. 10; Depósitos, Colocaciones y Personal por Oficinas.

Imagen N° 36: Distribución por zonas geográficas año 2018
Fuente: http://www.sbs.gob.pe/app/stats_net/stats/EstadisticaBoletinEstadistico.aspx?p=5#

Distribución de Oficinas por Zona Geográfica de las Entidades de Desarrollo a la Pequeña y Micro Empresa

(Al 30 de Noviembre de 2019)

Empresas	Amazonas	Ancash	Apurimac	Arequipa	Ayacucho	Cajamarca	Callao	Cusco	Huanuco	Ica	Junin	La Libertad	Lambayeque	Lima	Loreto	Piura	Puno	San Martin	Tacna	Tumbes	Ucayali	TOTAL
EDPYME ALTERNATIVA	1	-	-	-	-	7	-	-	-	-	-	2	10	-	-	8	-	3	-	-	-	31
EDPYME CREDIVISION	-	-	-	-	-	-	-	4	-	-	-	1	-	1	-	-	-	-	-	-	-	6
EDPYME PROGRESO S.A.	-	3	-	-	1	2	-	-	1	3	-	7	3	5	2	8	-	4	-	1	1	41
EDPYME MICASITA	-	-	-	-	-	-	-	-	-	-	-	-	-	1	-	-	-	-	-	-	-	1
EDPYME ACCESO CREDITICIO	-	-	-	1	-	-	-	-	-	1	-	1	1	2	-	1	-	-	-	-	-	7
EDPYME INVERSIONES LA CRUZ	-	3	-	4	-	-	4	1	-	3	1	5	4	46	3	14	-	1	-	1	4	94
EDPYME BBVA CONSUMER FINANCE	-	-	-	-	-	-	-	-	-	-	-	-	-	1	-	-	-	-	-	-	-	1
EDPYME GMG	-	1	1	4	1	1	2	3	1	4	1	3	2	18	-	4	1	1	1	1	1	51
EDPYME SANTANDER	-	-	-	-	-	-	-	-	-	-	-	-	-	1	-	-	-	-	-	-	-	1
TOTAL EDPYMES	**1**	**7**	**1**	**9**	**2**	**10**	**6**	**8**	**2**	**11**	**2**	**19**	**20**	**75**	**5**	**35**	**1**	**9**	**1**	**3**	**6**	**233**

Nota: Información obtenida del Anexo No. 10; Depósitos, Colocaciones y Personal por Oficinas.

Imagen N° 37: Distribución por zonas geográficas año 2019

Fuente: http://www.sbs.gob.pe/app/stats_net/stats/EstadisticaBoletinEstadistico.aspx?p=5#

En las siguientes imágenes, de acuerdo a información de la SBS, se muestra el crecimiento de los créditos desembolsado en zonas rurales en los años 2018 y 209, donde se aprecia un incremento de 226 créditos para Agricultura, ganadería, caza y silvicultura.

Nuevos créditos corporativos, a grandes, medianas, pequeñas y micro empresas
por sector económico y Entidad de Desarrollo de la Pequeña y Microempresa
Desembolsados en el mes de Diciembre de 2018
(En miles de soles)

Empresas	Agricultura, Ganadería, Caza y Silvicultura			Minería			N° des
	N° de Nuevos Créditos desembolsados	Monto de Nuevos Créditos desembolsados en M.N. (miles de S/)	Monto de Nuevos Créditos desembolsados en M.E. (miles de $.)	N° de Nuevos Créditos desembolsados	Monto de Nuevos Créditos desembolsados en M.N. (miles de S/)	Monto de Nuevos Créditos desembolsados en M.E. (miles de $.)	
EDPYME Alternativa	954	3,995	-	1	7	-	
EDPYME Acceso Crediticio	-	-	-	-	-	-	
EDPYME Credivisión	327	1,024	-	2	9	-	
EDPYME Micasita	-	-	-	-	-	-	
EDPYME Marcimex	-	-	-	-	-	-	
EDPYME Inversiones La Cruz	-	-	-	-	-	-	
EDPYME BBVA Consumer Finance	-	-	-	-	-	-	
EDPYME GMG	-	-	-	-	-	-	
EDPYME Santander	2	107	-	-	-	-	
TOTAL EDPYMES	1,283	5,126	-	3	16	-	

Nota: Información obtenida del Anexo N° 3: Stock y Flujo Crediticio por Tipo de Crédito y Sector Económico.
Las definiciones de los tipos de crédito se encuentran en el Numeral 4 del Capítulo I del Reglamento para la Evaluación y Clasificación del Deudor y la Exi
http://intranet1.sbs.gob.pe/idxall/seguros/doc/resolucion/11356-2008.r.doc

Imagen N° 38: Número de Desembolsos por tipo de créditos
Fuente: http://www.sbs.gob.pe/app/stats_net/stats/EstadisticaBoletinEstadistico.aspx?p=5#

Fuente: http://www.sbs.gob.pe/app/stats_net/stats/EstadisticaBoletinEstadistico.aspx?p=5#

Nuevos créditos corporativos, a grandes, medianas, pequeñas y micro empresas por sector económico y Entidad de Desarrollo de la Pequeña y Microempresa

Desembolsados en el mes de Noviembre de 2019

(En miles de soles)

Empresas	Agricultura, Ganadería, Caza y Silvicultura			Minería		
	N° de Nuevos Créditos desembolsados	Monto de Nuevos Créditos desembolsados en M.N. (miles de S/)	Monto de Nuevos Créditos desembolsados en M.E. (miles de $.)	N° de Nuevos Créditos desembolsados	Monto de Nuevos Créditos desembolsados en M.N. (miles de S/)	Monto de Nuevos Créditos desembolsados en M.E. (miles de $.)
EDPYME Alternativa	1,180	5,157	-	2	50	-
EDPYME Acceso Crediticio		-	-	-	-	-
EDPYME Credivisión	204	824	-	-	-	-
EDPYME Micasita	-	-	-	-	-	-
EDPYME Progreso	-	-	-	-	-	-
EDPYME Inversiones La Cruz	1	1	-	-	-	-
EDPYME BBVA Consumer Finance	1	-	14	-	-	-
EDPYME GMG	-	-	-	-	-	-
EDPYME Santander	-	-	-	-	-	-
TOTAL EDPYMES	1,386	5,982	14	2	50	-

Nota: Información obtenida del Anexo N° 3: Stock y Flujo Crediticio por Tipo de Crédito y Sector Económico.

Las definiciones de los tipos de crédito se encuentran en el Numeral 4 del Capítulo I del Reglamento para la Evaluación y Clasificación del Deudor y la E

http://intranet1.sbs.gob.pe/idxall/seguros/doc/resolucion/11356-2008.r.doc

Imagen N° 39: Número de créditos desembolsado año 2019

Fuente: http://www.sbs.gob.pe/app/stats_net/stats/EstadisticaBoletinEstadistico.aspx?p=5#

Créditos Directos Corporativos, a Grandes, a Medianas, a Pequeñas y a Microempresas por Sector Económico y EDPYME

Al 31 de Diciembre de 2018

(En miles de nuevos soles)

Sector Económico	EDPYME Alternativa	EDPYME Acceso Crediticio	EDPYME Credivisión	EDPYME Micasita	EDPYME Marcimex	EDPYME Inversiones La Cruz	EDPYME BBVA Consumer Finance	EDPYME GMG	EDPYME Santander	TOTAL EDPYMES
Agricultura, Ganadería, Caza y Silvicultura	30,781	180	7,024	-	8	1	147	-	427	38,569
Pesca	626	421	-	-	-	-	180	-	-	1,227
Minería	146	66	29	-	-	29	246	-	144	660
Industria Manufacturera	7,852	4,144	607	-	18	2	1,445	-	1,366	15,434
Electricidad, Gas y Agua	-	66	4	-	-	-	-	-	401	470
Construcción	2,274	1,777	594	9,353	3	-	1,332	-	945	16,278
Comercio	43,999	26,977	12,353	-	115	-	7,427	-	3,878	94,748
Hoteles y Restaurantes	6,770	90	487	-	-	-	1,322	-	171	8,840
Transporte, Almacenamiento y Comunicaciones	10,816	522,848	940	-	3	-	2,766	-	2,314	539,685
Intermediación Financiera	-	56	24	-	-	1	146	-	53	279
Actividades Inmobiliarias, Empresariales y de Alquiler	2,905	1,755	118	-	33	15	6,011	-	3,934	14,772
Administración Pública y de Defensa	12	98	58	-	-	-	-	-	161	330
Enseñanza	194	43	146	-	-	-	287	-	97	768
Servicios Sociales y de Salud	267	291	58	-	-	-	464	-	211	1,291
Otras Actividades de Servicios Comunitarios	1,032	1,844	2,523	-	-	77	2,008	-	1,997	9,481
Hogares Privados c/serv. Doméstico y Organos Extraterritoriales	74	132	27	-	-	-	8	-	19,263	19,505
CREDITOS CORPORATIVOS, A GRANDES, A MEDIANAS, A PEQUEÑAS Y A MICROEMPRESAS	**107,749**	**560,786**	**24,993**	**9,353**	**181**	**125**	**23,790**	**-**	**35,361**	**762,338**

Nota: Información obtenida del Anexo 3 - Stock y flujo crediticio por tipo de crédito y sector económico.

Nota: Las definiciones de los tipos de crédito se encuentran en el Numeral 4 del Capítulo I del Reglamento para la Evaluación y Clasificación del Deudor y la Exigencia de Provisiones, aprobado mediante Resolución SBS N° 11356-2008

Imagen N° 40: Créditos Directos 2018

Fuente: http://www.sbs.gob.pe/app/stats_net/stats/EstadisticaBoletinEstadistico.aspx?p=5#

Créditos Directos Corporativos, a Grandes, a Medianas, a Pequeñas y a Microempresas por Sector Económico y EDPYME

Al 30 de Noviembre de 2019

(En miles de nuevos soles)

Sector Económico	EDPYME Alternativa	EDPYME Acceso Crediticio	EDPYME Credivisión	EDPYME Micasita	EDPYME Progreso	EDPYME Inversiones La Cruz	EDPYME BBVA Consumer Finance	EDPYME GMG	EDPYME Santander	TOTAL EDPYMES
Agricultura, Ganadería, Caza y Silvicultura	34,571	156	6,768	-	8	6	189	-	349	42,047
Pesca	659	143	-	-	-	-	137	-	71	1,011
Minería	222	63	44	-	-	-	175	-	110	614
Industria Manufacturera	8,805	4,945	601	-	18	-	1,847	-	1,889	18,106
Electricidad, Gas y Agua	-	66	-	-	-	-	160	-	323	549
Construcción	2,581	1,638	553	8,513	3	-	1,915	-	1,634	16,837
Comercio	50,598	8,844	12,018	-	111	-	6,288	-	5,443	83,302
Hoteles y Restaurantes	6,775	90	685	-	-	-	1,213	-	255	9,018
Transporte, Almacenamiento y Comunicaciones	10,721	708,408	865	-	3	-	2,824	-	2,284	725,104
Intermediación Financiera	-	-	2	-	-	8	139	-	30	179
Actividades Inmobiliarias, Empresariales y de Alquiler	3,341	1,056	141	-	33	-	5,792	-	3,536	13,900
Administración Pública y de Defensa	23	69	102	-	-	-	-	-	110	305
Enseñanza	161	54	133	-	-	-	261	-	10	620
Servicios Sociales y de Salud	494	164	75	-	-	-	438	-	321	1,492
Otras Actividades de Servicios Comunitarios	1,025	831	2,335	-	-	30	1,468	-	2,309	7,998
Hogares Privados c/serv. Doméstico y Organos Extraterritoriales	77	95	22	-	-	-	2	-	20,220	20,417
CREDITOS CORPORATIVOS, A GRANDES, A MEDIANAS, A PEQUEÑAS Y A MICROEMPRESAS	**120,052**	**726,622**	**24,345**	**8,513**	**177**	**45**	**22,847**	**-**	**38,897**	**941,498**

Nota: Información obtenida del Anexo 3 - Stock y flujo crediticio por tipo de crédito y sector económico.
Nota: Las definiciones de los tipos de crédito se encuentran en el Numeral 4 del Capítulo I del Reglamento para la Evaluación y Clasificación del Deudor y la Exigencia de Provisiones, aprobado mediante Resolución SBS N° 11356-2008

Imagen N° 41: Créditos Directos 2019
Fuente: http://www.sbs.gob.pe/app/stats_net/stats/EstadisticaBoletinEstadistico.aspx?p=5#

VI. CONCLUSIONES

De acuerdo a la investigación desarrollada y a los resultados obtenidos, se llegó a las siguientes conclusiones:

1. De acuerdo al plan operativo institucional POA 2018-2019, con la aplicación de esta herramienta en las zonas rurales se mantiene el índice de morosidad controlado en 4.62 % sobre la cartera vigente, ya que los analistas tienen en sus manos la información necesaria para los filtros adecuados (Imagen 42).
2. El mantener la morosidad controlada se ve reflejado en el importe que se provisiona por cartera morosa al 2019 (Imagen 43 – circulo de color rojo) comparado con lo provisionado al 2018 (Imagen 44 – circulo de color rojo).
3. Se reduce el costo operativo, ya que no las sedes rurales no dependen de una agencia matriz para producir sus utilidades (Imagen 43 y 42– círculo de color verde).
4. El resultado neto del ejercicio 2019 de acuerdo a la publicación de la SBS en el 2019 fue de 3,146 (Imagen 43 marcado de color azul) en comparación con el año 2018 (Imagen 44 marcado de color azul).
5. Así mismo. el hacer uso de las herramientas libres GNU/ LINUX, nos proporciona seguridad y permite acceder la información de manera óptima y eficaz, accediendo a diferentes recursos entre las agencias y oficinas informativas de la institución de manera directa y nos asegura una vía de acceso que sirva como soporte para enlazar futuras implementaciones tecnológicas, las cuales se pueden enlazar garantizando la mejora del proceso de acceso a los servicios de los sistemas de información y el acceso a datos de la corporación entre sedes.

Morosidad según tipo y modalidad de crédito de las Entidades de Desarrollo de la Pequeña y Microempresa*

Al 30 de Noviembre de 2019

(En porcentaje)

Concepto	EDPYME Alternativa	EDPYME Acceso Crediticio	EDPYME Credivisión	EDPYME Micasita	EDPYME Progreso	EDPYME Inversiones La Cruz	EDPYME BBVA Consumer Finance	EDPYME GMG	EDPYME Santander	TOTAL EDPYMEs
Créditos corporativos										
Tarjetas de crédito										
Descuentos										
Préstamos										
Factoring										
Arrendamiento financiero y Lease-back *										
Comercio exterior										
Otros 1/										
Créditos a grandes empresas				-					-	-
Tarjetas de crédito										
Descuentos										
Préstamos									-	-
Factoring										
Arrendamiento financiero y Lease-back *										
Comercio exterior										
Otros 1/				-						-
Créditos a medianas empresas	-	3.86	-	-		1.88	11.34		11.92	4.29
Tarjetas de crédito										
Descuentos										
Préstamos	-	4.78	-			1.88	11.34		11.92	**5.32**
Factoring		3.44								**3.44**
Arrendamiento financiero y Lease-back *		-								-
Comercio exterior										
Otros 1/				-						-
Créditos pequeñas empresas	4.69	4.04	0.84	-	100.00	-	11.00		13.16	4.77
Tarjetas de crédito										
Descuentos										
Préstamos	4.69	4.05	0.84		100.00	-	11.00		13.16	**4.82**
Factoring		-								-
Arrendamiento financiero y Lease-back *										
Comercio exterior										
Otros 1/				-						-
Créditos a microempresas	4.57	4.63	8.68		100.00		20.50		13.04	5.31
Tarjetas de crédito										
Descuentos										
Préstamos	4.57	4.63	8.68		100.00		20.50		13.04	**5.31**
Factoring										
Arrendamiento financiero y Lease-back *										
Comercio exterior										
Otros 1/										
Créditos de consumo	3.11	6.65			4.67	5.87	3.23	13.18	1.68	3.75
Tarjetas de crédito										
Préstamos	3.11	6.65			4.67	8.92	3.23	13.18	1.68	**3.59**
Préstamos revolventes						8.70		13.13		**12.23**
Préstamos no revolventes	3.11	6.65			4.67	13.45	3.23	100.00	1.68	**3.21**
Préstamos autos		7.50			2.30		2.92		1.48	**2.90**
Arrendamiento financiero y Lease-back *										
Pignoraticios						5.56				**5.56**
Otros 1/		-								-
Créditos hipotecarios para vivienda				1.91						1.91
Préstamos				2.57						**2.57**
Préstamos Mivivienda				1.84						**1.84**
Otros 1/										
Total Créditos Directos	4.23	4.62	7.19	1.82	4.99	5.87	3.58	13.18	2.43	3.97

Imagen N° 42: Índice de Morosidad al 2019

Fuente: http://www.sbs.gob.pe/app/stats_net/stats/EstadisticaBoletinEstadistico.aspx?p=5#

Estado de Ganancias y Pérdidas por Entidad de Desarrollo de la Pequeña y Microempresa

Al 30 de Noviembre de 2019

(En Miles de Soles)

	Alternativa		
	MN	ME	TOTAL
INGRESOS FINANCIEROS	**51 136**	**65**	**51 201**
Disponible	19	65	84
Fondos Interbancarios	-	-	-
Inversiones	-	-	-
Créditos Directos	51 085	( )	51 084
Ganancias por Valorización de Inversiones	-	-	-
Ganancias por Inversiones en Subsidiarias, Asociadas y Negocios Conjuntos	-	-	-
Diferencia de Cambio	-	-	-
Otros	32	0	32
GASTOS FINANCIEROS	**10 510**	**609**	**11 119**
Obligaciones con el Público	-	-	-
Fondos Interbancarios	-	-	-
Adeudos y Obligaciones Financieras	10 453	639	11 092
Obligaciones en Circulación no Subordinadas	-	-	-
Pérdida por Valorización de Inversiones	-	-	-
Pérdida por Inversiones en Subsidiarias, Asociadas y Negocios Conjuntos	-	-	-
Primas al Fondo de Seguro de Depósitos	-	-	-
Diferencia de Cambio	56	(30)	27
Otros	-	-	-
MARGEN FINANCIERO BRUTO	**40 626**	**(544)**	**40 082**
PROVISIONES PARA CRÉDITOS DIRECTOS	**5 045**	**( )**	**5 045**
MARGEN FINANCIERO NETO	**35 581**	**(544)**	**35 037**
INGRESOS POR SERVICIOS FINANCIEROS	**468**	**-**	**468**
Cuentas por Cobrar	0	-	0
Créditos Indirectos	-	-	-
Fideicomisos y Comisiones de Confianza	-	-	-
Ingresos Diversos	468	-	468
GASTOS POR SERVICIOS FINANCIEROS	**239**	**38**	**278**
Cuentas por Pagar	-	-	-
Créditos Indirectos	-	-	-
Fideicomisos y Comisiones de Confianza	-	-	-
Gastos Diversos	239	38	278
UTILIDAD (PÉRDIDA) POR VENTA DE CARTERA CREDITICIA	**11**	**-**	**11**
MARGEN OPERACIONAL	**35 820**	**(582)**	**35 238**
GASTOS ADMINISTRATIVOS	**30 465**	**721**	**31 187**
Personal	23 228	31	23 259
Directorio	600	4	604
Servicios Recibidos de Terceros	6 136	685	6 821
Impuestos y Contribuciones	502	1	503
MARGEN OPERACIONAL NETO	**5 355**	**(1 303)**	**4 051**
PROVISIONES, DEPRECIACIÓN Y AMORTIZACIÓN	**1 171**	**(1)**	**1 170**
Provisiones para Créditos Indirectos	-	-	-
Provisiones por Pérdida por Deterioro de Inversiones	-	-	-
Provisiones para Incobrabilidad de Cuentas por Cobrar	0	(1)	(1)
Provisiones para Bienes Realizados, Recidos en Pago y Adjudicados	(16)	-	(16)
Otras Provisiones	70	-	70
Depreciación	1 096	-	1 096
Amortización	20	-	20
OTROS INGRESOS Y GASTOS	**(13)**	**13**	**0**
RESULTADO ANTES DEL IMPUESTO A LA RENTA	**4 172**	**(1 289)**	**2 882**
IMPUESTO A LA RENTA	1 025	-	1 025
RESULTADO NETO DEL EJERCICIO	**3 146**	**(1 289)**	**1 857**
Tipo de Cambio Contable: S/ 3.396			

Imagen N° 43: Estado de Ganancias y pérdidas año 2019

Fuente: http://www.sbs.gob.pe/app/stats_net/stats/EstadisticaBoletinEstadistico.aspx?p=5#

Estado de Ganancias y Pérdidas por Entidad de Desarrollo de la Pequeña y Microempresa

Al 31 de Diciembre de 2018

(En Miles de Soles)

Actualizado al 06/05/2019

	Alternativa		
	MN	ME	TOTAL
INGRESOS FINANCIEROS	**50 747**	**70**	**50 817**
Disponible	33	70	103
Fondos Interbancarios	-	-	-
Inversiones	-	-	-
Créditos Directos	50 670	0	50 671
Ganancias por Valorización de Inversiones	-	-	-
Ganancias por Inversiones en Subsidiarias, Asociadas y Negocios Conjuntos	-	-	-
Diferencia de Cambio	-	-	-
Otros	44	-	44
GASTOS FINANCIEROS	**11 535**	**415**	**11 951**
Obligaciones con el Público	-	-	-
Fondos Interbancarios	-	-	-
Adeudos y Obligaciones Financieras	11 523	425	11 948
Obligaciones en Circulación no Subordinadas	-	-	-
Pérdida por Valorización de Inversiones	-	-	-
Pérdida por Inversiones en Subsidiarias, Asociadas y Negocios Conjuntos	-	-	-
Primas al Fondo de Seguro de Depósitos	-	-	-
Diferencia de Cambio	12	(10)	2
Otros	-	-	-
MARGEN FINANCIERO BRUTO	**39 212**	**(345)**	**38 866**
PROVISIONES PARA CRÉDITOS DIRECTOS	**4 623**	**(1)**	**4 622**
MARGEN FINANCIERO NETO	**34 589**	**(344)**	**34 245**
INGRESOS POR SERVICIOS FINANCIEROS	**525**	-	**525**
Cuentas por Cobrar	0	-	0
Créditos Indirectos	-	-	-
Fideicomisos y Comisiones de Confianza	-	-	-
Ingresos Diversos	525	-	525
GASTOS POR SERVICIOS FINANCIEROS	**290**	**29**	**319**
Cuentas por Pagar	-	-	-
Créditos Indirectos	-	-	-
Fideicomisos y Comisiones de Confianza	-	-	-
Gastos Diversos	290	29	319
UTILIDAD (PÉRDIDA) POR VENTA DE CARTERA CREDITICIA	**31**	-	**31**
MARGEN OPERACIONAL	**34 855**	**(373)**	**34 482**
GASTOS ADMINISTRATIVOS	**29 865**	**772**	**30 637**
Personal	22 776	26	[illegible]
Directorio	586	3	589
Servicios Recibidos de Terceros	5 961	743	6 703
Impuestos y Contribuciones	542	1	543
MARGEN OPERACIONAL NETO	**4 991**	**(1 146)**	**3 845**
PROVISIONES, DEPRECIACIÓN Y AMORTIZACIÓN	**1 655**	**1**	**1 656**
Provisiones para Créditos Indirectos	-	-	-
Provisiones por Pérdida por Deterioro de Inversiones	-	-	-
Provisiones para Incobrabilidad de Cuentas por Cobrar	9	1	10
Provisiones para Bienes Realizados, Recidos en Pago y Adjudicados	(6)	-	(6)
Otras Provisiones	334	-	334
Depreciación	1 228	-	1 228
Amortización	90	-	90
OTROS INGRESOS Y GASTOS	**(70)**	**(21)**	**(91)**
RESULTADO ANTES DEL IMPUESTO A LA RENTA	**3 266**	**(1 167)**	**2 099**
IMPUESTO A LA RENTA	866	-	866
RESULTADO NETO DEL EJERCICIO	**2 400**	**(1 167)**	**1 233**

Tipo de Cambio Contable: S/ 3.373

Imagen N° 44: Estado de Ganancias y pérdidas año 2018
Fuente: http://www.sbs.gob.pe/app/stats_net/stats/EstadisticaBoletinEstadistico.aspx?p=5#

VII. RECOMENDACIONES

1. Se recomienda este proyecto de investigación como propuesta de solución para las micro empresas, ya que esta solución brinda ventajas, tales como: Estable, Robusto y configurable a las necesidades de las empresas; y tiene como ventaja que es libre y es escalable.
2. Realizar capacitaciones informativas, con la finalidad de generar una cultura de prevención sobre la seguridad de la información a los colaboradores de Edpyme Alternativa.

VIII. REFERENCIAS BIBLIOGRÁFICAS

BIBLIOGRAFIA Y LINKOGRAFÍA

[1] Banco Mundial, «https://www.bancomundial.org/es/results/2018/07/02/profundizar-la-inclusion-financiera-en-areas-rurales-de-mexico,» [En línea].

[2] SBS - Informe, «https://www.sbs.gob.pe/Portals/0/jer/ESTUDIOS-SOBRE-INCLUSI%C3%93N-FINANCIERA/Informe-de-Resultados.pdf,» [En línea].

[3] J. M. Ruiz, «Propuesta de Segmentación de Redes Virtuales y priorización del ancho de banda con QOS para la mejora del redimiento y seguridad de la red LAN en la empresa Editora EL Comercio Planta Norte,» 2012.

[4] G. L. A. Vieyra Dioses y M. A. Díaz Llatance, «Diseño de una red privada virtual para interconectar las sucursales de la empresa Terracargo S. A. C.,» 2016.

[5] T. Mamani Tito, «Modelo De Sistema Criptográfico De Seguridad Para Las Redes De Comunicaciones En La Región Puno,» 2014.

[6] P. J. Zambrano Rodriguez y M. P. Sanchez Aguayo, «Repotenciación de un sistema de firewall de código abierto basado en funcionalidades de plataforma propietaria,» 2013.

[7] Gnu Org, 2004 Junio 2017. [En línea]. Available: https://www.gnu.org/philosophy/free-sw.es.html. [Último acceso: 2019].

[8] webmasters@gnu.org, «GNU operating System,» Free Software Foundation, Inc., 15 09 2019. [En línea]. Available: https://www.gnu.org/philosophy/free-sw.es.html. [Último acceso: 5 10 2019].

[9] INEI, «Guia para la migración de software libre en las entidades públicas,» Colección Metodologia Informatica, Lima, 2002.

[10] «Secretaría de Gobierno Digital SEGDI-PCM,» Julio 2019. [En línea]. Available: https://www.softwarepublico.gob.pe/index.php/es/software-publico-es/marco-legal-es. [Último acceso: octubre 2019].

[11] E. S. R. Michael K. Johnson, Introduction to Linux: A Collection of Linux HOWTOs, iUniverse, 2000.

[12] Xataka, «Xataka Basics,» setiembre 2018. [En línea]. Available: https://www.xataka.com/basics/distribuciones-gnu-linux-para-encontrar-que-mejor-se-adapta-a-tu-escritorio. [Último acceso: Octubre 2019].

[13] I. M. F. Delgado, «Oficina Nacional de Gobierno Electrónico e Informática,» 2019. [En línea]. Available: https://www.gobiernodigital.gob.pe/docs/ISO_27001_v011.pdf. [Último acceso:

Octubre 2019].

[14] A. L. Neira, «ISO 27000.es,» 2012. [En línea]. Available: http://iso27000.es/iso27000.html. [Último acceso: Octubre 2019].

[15] V. A. VÁSQUEZ, Chiclayo, IMPLEMENTACIÓN DE UNA RED PRIVADA VIRTUAL (VPN).

[16] Cisco, «Cisco,» 2019. [En línea]. Available: https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html . [Último acceso: Octubre 2019].

[17] J. C. M. Arenas, «pymsol.es,» 2018. [En línea]. Available: https://firewalls-hardware.com/blog/. [Último acceso: Octubre 2019].

[18] Cisco, «Cisco,» 2019. [En línea]. Available: https://www.netacad.com/. [Último acceso: Junio 2019].

[19] J. J. T. Cánovas, «Servicio VPN de acceso remoto basado en SSL mediante OpenVPN,» Cartagena, 2008.

[20] F. y. N. G. Markus, Beginning OpenVPN 2.0.9: Build and integrate Virtual Private Networks using, 2009.

[21] V. M, «Desarrollo de una virtual private network (vpn) para la interconexión de una empresa con sus sucursales en provincias. Facultad de ingeniería de sistemas e informática.,» 2003.

[22] webmasters@gnu.org, [En línea]. Available: https://www.gnu.org/philosophy/categories.es.html. [Último acceso: Octubre 2019].

IX. ANEXOS

ANEXO 01: GRÁFICOS

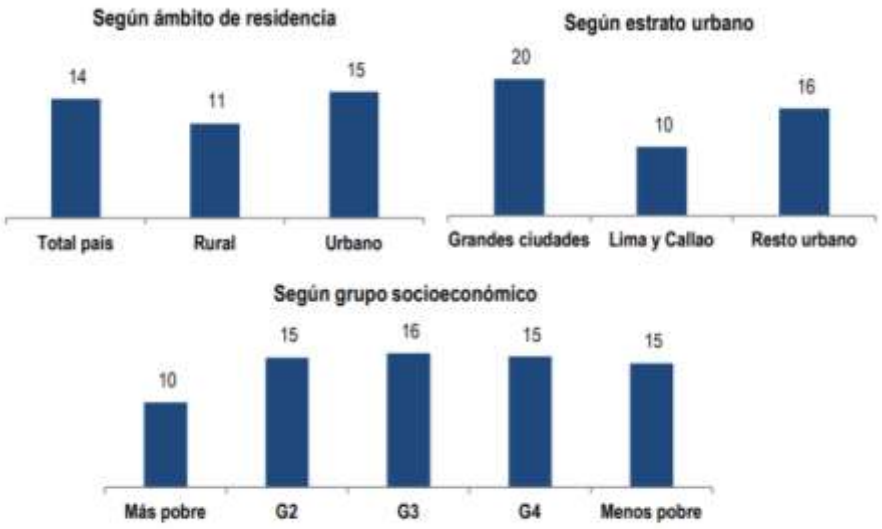


Gráfico N°01: Población que solicitó algún crédito en el Sistema Financiero durante el 2014
Fuente: Encuesta Nacional de Demanda de Servicios Financieros y Nivel de Cultura Financiera en el Perú

ANEXO 02: PROPUESTA DE IMPLEMENTACIÓN

PROPUESTA 01: HP PROLIANT ML10 SERVERS
HP ProLiant ML10 E3-1220v2 1P 2GB-U B110i 300W PS Entry Server/S-Buy(737649-S01) Especificaciones

- **Características del sistema**
  - ✓ Procesador: Intel® Xeon® E3-1220 v2 (4 core, 3.1 GHz, 8MB, 69W)
  - ✓ Número de procesadores: 1
  - ✓ Núcleo de procesador disponible: 4
  - ✓ Factor de forma (configuración completa): 4U
  - ✓ Tipo de fuente de alimentación:
    Kit de fuente de alimentación integrada de fábrica 300W de salida múltiple
  - ✓ Slots de expansión:
    (4) PCIe; Para detalles descripciones hacen referencia a la QuickSpec
- **Memoria**
  - ✓ Memoria, estándar: 2GB (1x2GB) UDIMM
  - ✓ Ranuras de memoria: 4 ranuras DIMM
  - ✓ Tipo de memoria: 1R x8 PC3-12800E-11
- **Almacenamiento**
  - ✓ Discos duros incluidos: No incorpora discos duros
  - ✓ Soporta hasta (4) unidades de LFF SATA
  - ✓ Sin conexión en caliente, según el modelo
- **Tarjetas controladoras**
  - ✓ El controlador de red:
    Adaptador Ethernet 1Gb NC112i 1 puerto por controlador
  - ✓ Controlador de almacenamiento:
    (1) Smart Array B110i SATA RAID
- **Dimensiones y peso**
  - ✓ Dimensiones (W x D x H) : 36.39 x 16.5 x 38.1 cm (14.3 x 6.5 x 15 in)
  - ✓ Peso : 5.94kg (13.08 lb)
- **Administración de servidores**
  - ✓ Administración de infraestructura
  - ✓ Estándar iLO, Insight Control

SERVIDOR DISCO DURO
HP 1 TB 3 G SATA 7,2 K rpm LFF (3,5 pulgadas) de la línea media del enchufe sin conexión en caliente, 1 año garantía del disco duro (507772-B21) Precio: $ 269

- ❖ **Visión de conjunto**
  - ✓ 1TB 3G LFF (3,5 pulgadas) de la línea media no conectable en caliente
- ❖ **Características**
  - ✓ Mayor fiabilidad de la unidad de la línea media de aproximadamente dos veces mayor que la de las unidades de entrada basados en un <40% de carga de trabajo. Reduce el costo sin sacrificar la fiabilidad con los discos duros de clase empresarial en el más bajo $ / GB
- ❖ **Especificaciones**
  - ✓ Peso: 1,36 kg
  - ✓ Dimensiones mínimas (W x D x H): 4 x 5.75 x 1.028 cm
  - ✓ (1) 1TB LFF (3,5 pulgadas) de la línea media no conectable en caliente

- ✓ HP Price: $269.00
- ✓ MFG #507772-B21

Valor: US$ 599+ US$ 269= US$ 868
** El valor es aproximado y puede variar en cualquier momento. Este valor proviene de la página oficial HP (http://www8.hp.com).

PROPUESTA 02: DELL OptiPlex 745

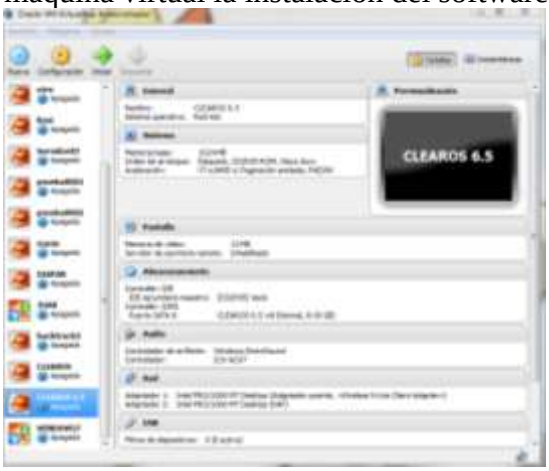
❖ **Especificaciones**

- **Características del sistema**
  - ✓ Procesador® Intel® Pentium D con
  - ✓ tecnología de doble núcleo
  - ✓ Hasta 960 (3.6 GHz, 2X2 MB, 800 MHzFSB)
  - ✓ Excelente rendimiento en entornos de multitarea.
- **Memoria**
  - ✓ Memoria, estándar: DDR2 DIMM
  - ✓ Ancho de banda de memoria:
    800 MHz - 12.8 GB/s con dos canales
    667 MHz - 10.7 GB/s con dos canales
  - ✓ Ranuras de memoria: 4 ranuras DIMM
  - ✓ Capacidad: 2GB
- **Almacenamiento**
  - ✓ Disco duro incluido
    SATA 3.0 brinda el doble de ancho de banda que SATA, con una velocidad de transferencia de 3 GBps.
  - ✓ Los beneficios de las unidades SATA II de la OptiPlex 745 son:
    Función de protección con contraseña en la unidad de disco duro. Se debe introducir una contraseña para poder acceder al disco duro y para iniciar el sistema. Esto proporciona un nivel adicional de seguridad de la información. Mayor rapidez, integridad de datos mejorada y escalabilidad optimizada
  - ✓ Sin conexión en caliente, según el modelo
- **Tarjetas controladoras**
  - ✓ Interfaz de red - Solución LAN Broadcom ® 5754 Gigabit Ethernet
    10/100/1000 4 Ethernet con soporte completo de ASF 2.0 y PXE
- **Dimensiones y peso**
  - ✓ Número de bahías
    1 interna de 3.5", 1 externa de 3.5", 1 externa de 5.25"
  - ✓ Dimensiones
    Alto: 15.59" Ancho: 4.5" Profundidad: 13.69"
    Alto: 35.59 cm Ancho: 11.40 cm Profundidad: 43.4 cm
  - ✓ Ranuras
    2 PCI de bajo perfil (Alto: 2.5" X Largo: 6.6")
    1 PCIe x16 de bajo perfil para tarjetas de gráficos (Alto: 2.5" X Largo: 6.6")
    Opcional El riser convierte la ranura PCIe y la PCI a 1 PCIe y 1 PCI o 2 PCI, de altura variable (Alto: 4.2" X Largo: 6.6")
  - ✓ Fuente de energía: 280W

ANEXO 03: INSTALACIÓN Y CONFIGURACIÓN

MANUAL DE INSTALACIÓN CLEAROS

A continuación, demostraremos los pasos de la instalación y configuración de la herramienta tecnológica como solución ClearOS-community-7.1.0-i386. Se simulará en máquina virtual la instalación del software. Utilizando Oracle VM Virtual Box



BOOT CD-ROM

Para instalaciones basadas en CD, grabar la imagen ISO en un CD. Podrá entonces iniciar este CD-ROM para iniciar los ClearOS instalar. Puede que tenga que entrar en la BIOS o presionar una tecla especial para arrancar desde el CD. Preste atención a la pantalla durante el arranque ya que las opciones de las teclas de arranque se exhiben a menudo por un corto período de tiempo.

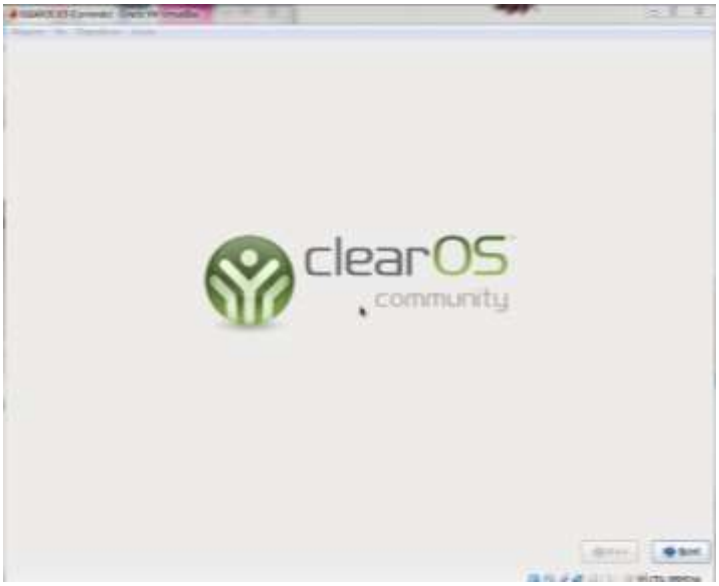
MAQUINAS VIRTUALES

1. Luego que ser ha descargado ClearOS en imagen ISO podemos comenzar la instalación. La mayoría de los entornos de máquinas virtuales pueden arrancar directamente desde una imagen ISO:
2. Una vez que su sistema ha pasado todos los controles de hardware habituales, debería ver la pantalla del instalador se muestra a continuación. Seleccionaremos el modo de la pantalla chica / 800x600 barra de desplazamiento para evitar molestos en el sistema de instalación.

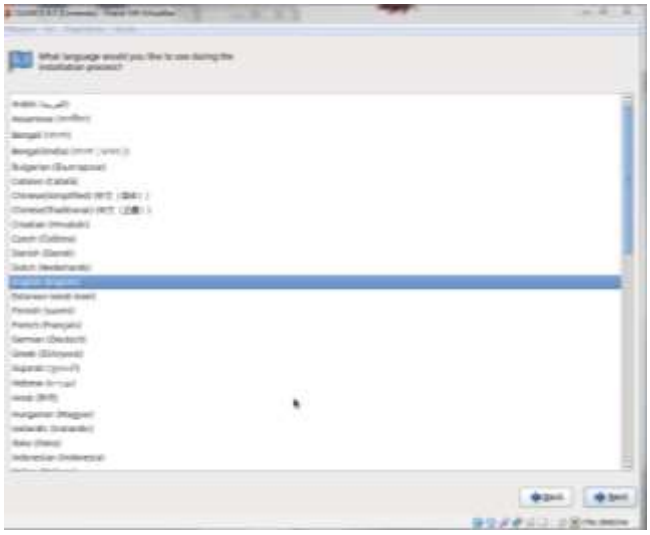
3. Instalar ClearOS ya está en curso y el siguiente paso va a través del asistente de instalación .

ASISTENTE PARA LA INSTALACION
INFORMACION GENERAL
Después de iniciada la instalación , se presentará un asistente de instalación sencilla y breve. El asistente le lleva a través de las opciones de configuración que se requieren para instalar ClearOS en un disco duro o unidad de disco virtual. Una vez completado el asistente, la instalación finalizará en sólo unos pocos minutos.
COMO DESPLAZARSE
Para navegar por el asistente de instalación ClearOS, puede utilizar las siguientes teclas:

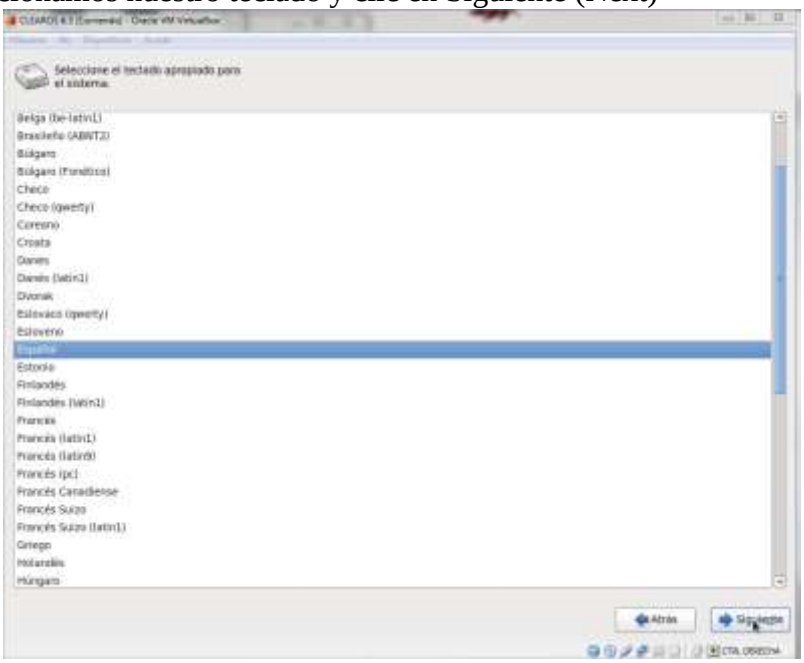
- Tab - navega entre campos
- Teclas de dirección - se utilizan para navegar dentro de los elementos de un campo
- Introduzca - selecciona el elemento resaltado actual
- Seguimos el asistente de instalación, clic en Siguiente (Next)



4. Seleccionamos nuestro idioma y clic en Siguiente (Next).

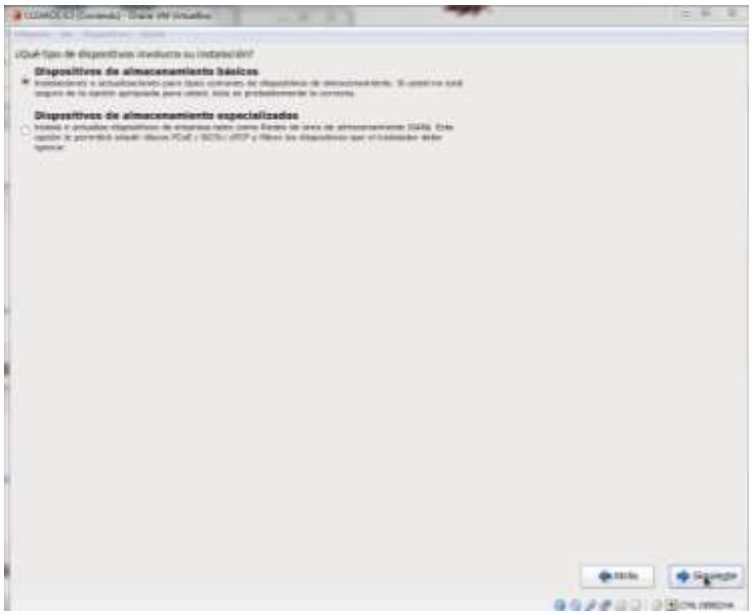


5. Seleccionamos nuestro teclado y clic en Siguiente (Next)



6. **DISPOSITIVOS DE ALMACENAMIENTO**

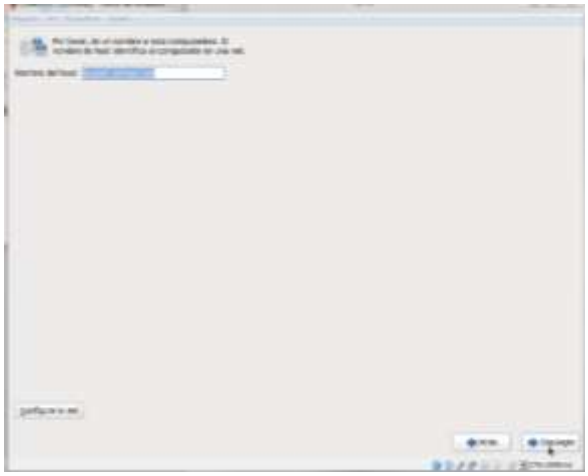
ClearOS soporta muchas opciones avanzadas de almacenamiento: iSCSI, canal de fibra sobre Ethernet (FCoE) y más. En la mayoría de los casos, la selección de la opción de dispositivo de almacenamiento de base es apropiada.



Ventana para detectar particiones y si el dispositivo de almacenamiento puede contener datos, en nuestro caso la máquina virtual se asignó un espacio del disco duro libre de datos. Seleccionamos “Si, descarte todos los datos”

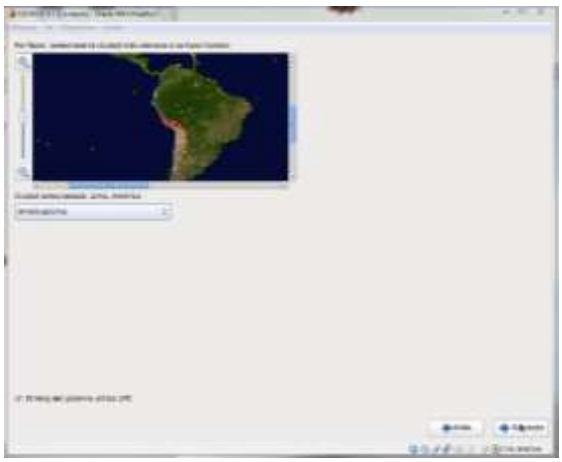
7. NOMBRE DE HOST Y DE RED

Ahora es el momento de seleccionar un nombre de host. Si usted planea desplegar ClearOS con una conexión directa a Internet, le recomendamos que utilice el nombre de host de Internet de bienes, por ejemplo server.example.com. Si usted planea desplegar ClearOS en una red local, puede utilizar un nombre de host interno en lugar, por ejemplo server.example.local.



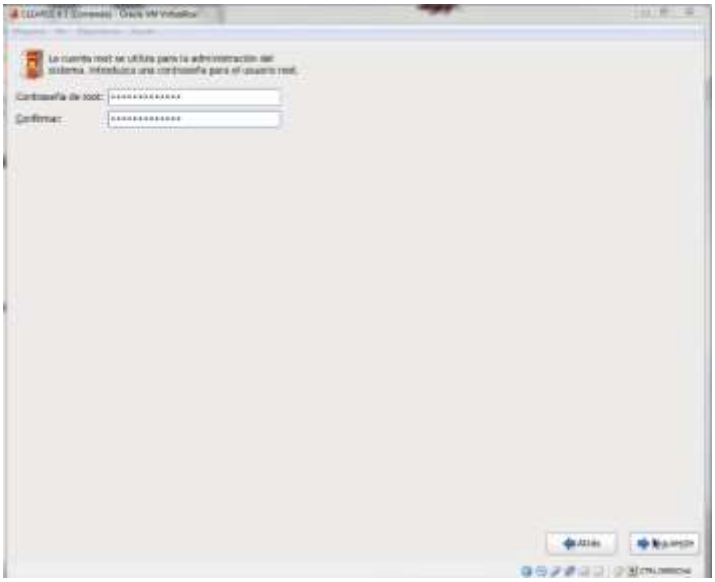
8. ZONA HORARIA

Selección de la zona horaria correcta es importante. Una zona horaria no válida puede romper los sistemas de autenticación y causar un comportamiento extraño con VoIP y otros bits de la tecnología. Puede hacer clic en el mapa o utilice la lista desplegable para seleccionar la zona horaria.



9. CONTRASEÑA DE ROOT

Proporcionar una buena contraseña a utilizar para la cuenta root. Si el instalador detecta una contraseña débil, por favor, siga la recomendación de seleccionar una contraseña mejor.



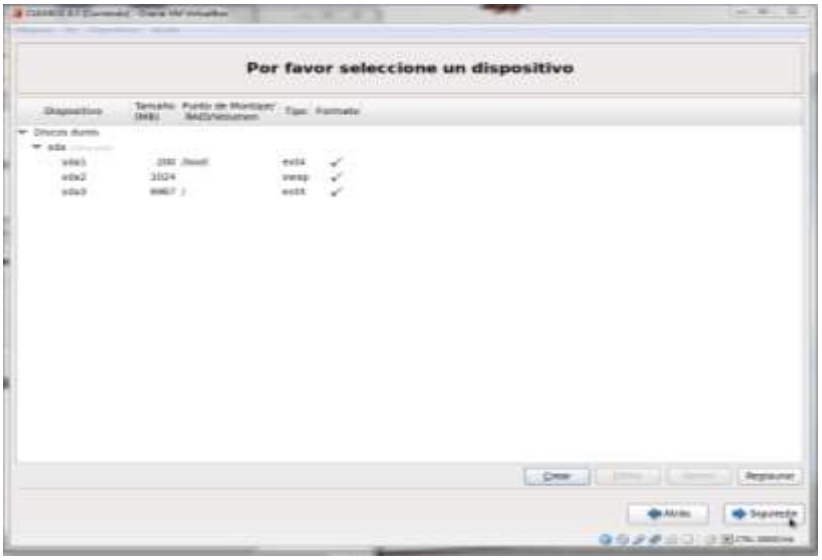
10. PARTICIONAMIENTO DEL DISCO DURO

Las particiones pueden ser la parte más complicada del proceso de instalación. De hecho, hay toda una sección de la Guía del usuario dedicado a este tema y RAID. Aquí están algunas sugerencias para ayudar a guiar el camino.

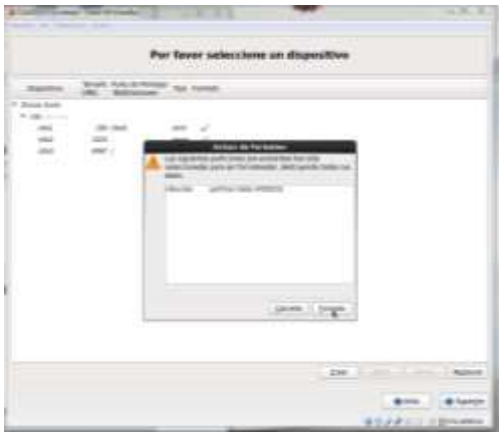
- Utilizar todo el espacio - Seleccione esta opción si no requiere software RAID ni tener una necesidad de una partición de datos de gran tamaño. Esta opción también asume que ClearOS no está compartiendo el disco duro con otros sistemas operativos.
- Vuelva a colocar sistemas de Linux existentes - Similar a utilizar todo el espacio, pero esta opción mantiene las particiones no-Linux.
- Reducir el sistema actual y usar el espacio libre - Desde ClearOS suele ser el único sistema operativo en el sistema de destino, rara vez se utilizan estas dos opciones.

- Crear un diseño personal - Si utiliza el software RAID, tiene una necesidad de una cuota de datos dedicado, han instalado varios discos, a continuación, por favor, lea Configuración de Particiones y RAID para obtener más información.
- En nuestro caso Crearemos un diseño personalizado, en base a la asignación al disco.

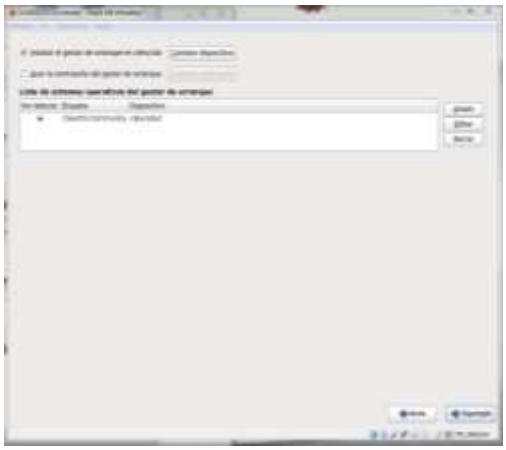
11. En nuestro caso asignaremos la partición /boot (unidad de arranque 200 Mb), swap (se le asigna el doble de la memoria RAM, para que no ralentice el proceso de virtualización asignaremos 1024 MB) y por último la partición raíz / (para esta partición completaremos hasta el tamaño máximo); Clic en siguiente.

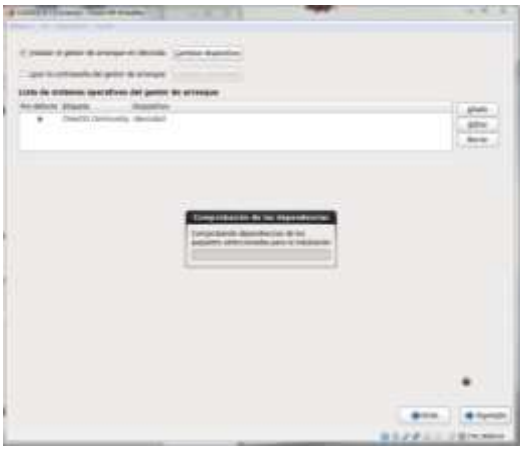


12. Una vez asignadas las particiones, procederemos a formatear la partición raíz donde se instalarán los paquetes.



13. Seleccionamos el gestor de arranque del sistema operativo, y clic en siguiente.





14. Luego, se iniciará la instalación esperamos a que termine el proceso de instalación,

15. Luego que la instalación de ClaerOS está completa, seleccionamos REINICIAR para usar el sistema.

16. Una vez iniciado el sistema ClearOS Community 6.5.0, nos mostrará 2 opciones para poder configurar Network, 1 opción configurar desde el mismo servidor (PC), y la 2 opción es conectarse mediante un interfaz web.

INSTALL WIZARD

Un asistente de software o asistente de configuración, es una interfaz de tipo usuario que presenta una secuencia de cuadros de diálogo; que llevan al usuario a través de una serie de pasos bien definidos.

17. Abrimos nuestro navegador e ingresamos nuestra dirección IP (192.168.1.41) asignada al servidor firewall, el puerto 81 para comunicarnos con el servidor. Ingresamos nuestros datos de Inicio de sesión (username y password).

18. Nos presenta una introducción, y unas breves instrucciones. Clic en Siguiente.

19. Seleccionamos el tipo de conexión entre nuestros dispositivos y el servidor. Para nuestro caso seria “Modo Gateway”

20. Seleccionamos y configuramos las interfaces de red.

21. Información de la configuración DNS de acuerdo al proveedor del servicio de internet.

22. Comprobación y respuesta de conexión con los DNS

23. Bienvenida e información, Gracias por elegir ClearOS. Seleccionamos el tipo de instalación, Opción 1, instalación sin costo (free), desarrollada por la Comunidad ClearOS. Opción 2, instalación bajo costo de adquisición y compra de los servicios de ClearOS Center

24. Configuración, instalación y actualizaciones de repositorios, para acceder a los paquetes a emplear o necesarios para el proyecto.

25. Actualización de los paquetes conectándose a los repositorios.

26. Registro del sistema. Creamos una cuenta e ingresamos los datos.

27. Registramos el sistema, asociando el registro del sistema a nuestra cuenta creada anteriormente.

28. Aceptación del registro. Información detallada de registro del sistema.

29. Ingresar el dominio del sistema.

30. Ingresar el Hostname (nombre de equipo) del sistema.

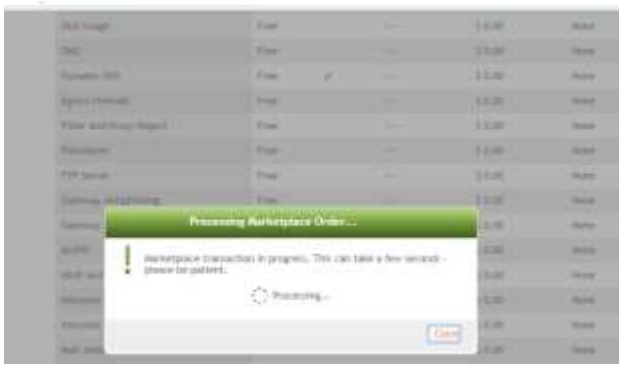
31. Información de la zona horaria, fecha y hora del sistema.

32. Seleccionamos modo de instalación de las aplicaciones (apps) necesarios para el sistema.

33. Seleccionamos las aplicaciones (apps) a utilizar, los cuales se encuentran agrupados y separados por categorías.

34. Lista de las aplicaciones (apps) seleccionadas anteriormente.

35. Descarga e instalación de las aplicaciones (apps).



36. Proceso de descarga e instalación de las aplicaciones (apps).

37. Una vez finalizado la instalación, se reiniciará el sistema. Al reiniciar, seremos recibidos por la pantalla de inicio de sesión del usuario administrador.

ANEXO 04: GUÍAS DE ENCUESTAS

GUÍA DE ENCUESTA N° 01

SEDE	SANTO TOMAS DE CUTERVO
NOMBRE	
ÁREA O UNIDAD	NEGOCIOS
CARGO	

1. ¿Conoce el papel que desempeña el área de TI?
   a) Si
   b) No
   c) No se
2. ¿Utiliza usted equipos de informática en su trabajo?
   a) Siempre
   b) Frecuentemente
   c) A veces
   d) Nunca
3. ¿La información que se genera en el otorgamiento de los créditos, es considerada muy importante en tal virtud considera que se debe contar con equipos más sofisticados?
   a) Si
   b) No
   c) No se
4. ¿Conoce usted de lo que significa el "software libre", lo ha utilizado?
   a) Siempre
   b) Frecuentemente
   c) A veces
   d) Desconozco
5. ¿Es necesario para usted contar con el sistema principal del negocio para su desempeño?
   a) Si
   b) No
   c) No se
6. ¿Estaría de acuerdo que se realice la implementación de los sistemas de información para el desarrollo de sus funciones?
   a) Si
   b) No
   c) No se
7. ¿Considera que con está implementación va a apoyar en su trabajo y en el logro de los objetivos institucionales?
   a) Si
   b) No
   c) No se

GUIA DE ENCUESTA N° 01

SEDE	SANTO TOMAS DE CUTERVO
NOMBRE	
ÁREA O UNIDAD	NEGOCIOS
CARGO	ANALISTA DE CREDITOS

1. ¿Conoce el papel que desempeña el área de TI?
   a) Si
   b) No
   c) No se
2. ¿Utiliza usted equipos de informática en su trabajo?
   a) Siempre
   b) Frecuentemente
   c) A veces
   d) Nunca
3. ¿La información que se genera en el otorgamiento de los créditos, es considerada muy importante en tal virtud considera que se debe contar con equipos más sofisticados?
   a) Si
   b) No
   c) No se
4. ¿Conoce usted de lo que significa el "software libre", lo ha utilizado?
   a) Siempre
   b) Frecuentemente
   c) A veces
   d) Desconozco
5. ¿Es necesario para usted contar con el sistema principal del negocio para su desempeño?
   a) Si
   b) No
   c) No se
6. ¿Estaría de acuerdo que se realice la implementación de los sistemas de información para el desarrollo de sus funciones?
   a) Si
   b) No
   c) No se
7. ¿Considera que con está implementación va a apoyar en su trabajo y en el logro de los objetivos institucionales?
   a) Si
   b) No
   c) No se

EDPYME ALTERNATIVA
Junior Esahim López Huamán
ANALISTA DE CREDITOS

GUIA DE ENCUESTA N° 01

SEDE	**SANTO TOMAS DE CUTERVO**
NOMBRE	
ÁREA O UNIDAD	NEGOCIOS
CARGO	ANALISTA DE CREDITOS

1. ¿Conoce el papel que desempeña el área de TI?
   a) Si
   b) No
   c) No se
2. ¿Utiliza usted equipos de informática en su trabajo?
   a) Siempre
   b) Frecuentemente
   c) A veces
   d) Nunca
3. ¿La información que se genera en el otorgamiento de los créditos, es considerada muy importante en tal virtud considera que se debe contar con equipos más sofisticados?
   a) Si
   b) No
   c) No se
4. ¿Conoce usted de lo que significa el "software libre", lo ha utilizado?
   a) Siempre
   b) Frecuentemente
   c) A veces
   d) Desconozco
5. ¿Es necesario para usted contar con el sistema principal del negocio para su desempeño?
   a) Si
   b) No
   c) No se
6. ¿Estaría de acuerdo que se realice la implementación de los sistemas de información para el desarrollo de sus funciones?
   a) Si
   b) No
   c) No se
7. ¿Considera que con está implementación va a apoyar en su trabajo y en el logro de los objetivos institucionales?
   a) Si
   b) No
   c) No se

GUIA DE ENCUESTA N° 01

SEDE	SANTO TOMAS DE CUTERVO
NOMBRE	
ÁREA O UNIDAD	NEGOCIOS
CARGO	ANALISTA DE CREDITOS

1. ¿Conoce el papel que desempeña el área de TI?
   a) Si
   b) No
   c) No se
2. ¿Utiliza usted equipos de informática en su trabajo?
   a) Siempre
   b) Frecuentemente
   c) A veces
   d) Nunca
3. ¿La información que se genera en el otorgamiento de los créditos, es considerada muy importante en tal virtud considera que se debe contar con equipos más sofisticados?
   a) Si
   b) No
   c) No se
4. ¿Conoce usted de lo que significa el "software libre", lo ha utilizado?
   a) Siempre
   b) Frecuentemente
   c) A veces
   d) Desconozco
5. ¿Es necesario para usted contar con el sistema principal del negocio para su desempeño?
   a) Si
   b) No
   c) No se
6. ¿Estaría de acuerdo que se realice la implementación de los sistemas de información para el desarrollo de sus funciones?
   a) Si
   b) No
   c) No se
7. ¿Considera que con está implementación va a apoyar en su trabajo y en el logro de los objetivos institucionales?
   a) Si
   b) No
   c) No se

EDPYME ALTERNATIVA
Macalopu Serrano José Stalin
ANALISTA DE CREDITOS

ANEXO 04: GUIAS DE ENCUESTAS

GUIA DE ENCUESTA N° 01

SEDE	**SANTO TOMAS DE CUTERVO**
NOMBRE	
AREA O UNIDAD	NEGOCIOS
CARGO	ANALISTA DE CREDITOS

1. ¿Conoce el papel que desempeña el área de TI?
   a) Si
   b) No
   c) No se
2. ¿Utiliza usted equipos de informática en su trabajo?
   a) Siempre
   b) Frecuentemente
   c) A veces
   d) Nunca
3. ¿La información que se genera en el otorgamiento de los créditos, es considerada muy importante en tal virtud considera que se debe contar con equipos más sofisticados?
   a) Si
   b) No
   c) No se
4. ¿Conoce usted de lo que significa el "software libre", lo ha utilizado?
   a) Siempre
   b) Frecuentemente
   c) A veces
   d) Desconozco
5. ¿Es necesario para usted contar con el sistema principal del negocio para su desempeño?
   a) Si
   b) No
   c) No se
6. ¿Estaría de acuerdo que se realice la implementación de los sistemas de información para el desarrollo de sus funciones?
   a) Si
   b) No
   c) No se
7. ¿Considera que con está implementación va a apoyar en su trabajo y en el logro de los objetivos institucionales?
   a) Si
   b) No
   c) No se

COOPYME ALTERNATIVA
Luis Eduardo Farfán Salcedo
ANALISTA DE CREDITOS

GUÍA DE ENCUESTA N° 02 - CONFIDENCIAL

INSTITUCIÓN	**EDPYME ALTERNATIVA**
NOMBRE	
ÁREA O UNIDAD	TI
CARGO	Jefe de TI

CONTROLES PARA LA SEGURIDAD

1. Existen políticas de seguridad para la información sensible.

a) Si
b) No

2. Conoce si existen dispositivos de seguridad y monitoreo de la red en la institución, si su respuesta es afirmativa indique los elementos que identifica.

a) Si
b) No

---

3. Existen políticas de respaldo en los equipos que administra, si la respuesta es afirmativa indique la frecuencia de respaldo.

a) Si
b) No

---

4. En los dispositivos que administra, aplica algún esquema de políticas de seguridad, si la respuesta es afirmativa indique que puntos cubre.

a) Si
b) No

Se reserva derechos de información escrita

---

5. Cuenta la EA con un documento oficial de políticas y procedimientos de seguridad de la información.

a) Si
b) No

6. En caso de existir un documento de políticas de seguridad, el mismo ha sido publicado y comunicado a todos los colaboradores de EA.

a) Si
b) No

Seguridad del Recurso Humano

7. Se han revisado todos los cargos en función de las responsabilidades en materia de seguridad de la información.

a) Si
b) No

8. Existen procedimientos para la contratación, transferencia y terminación de contratos de funcionarios.

a) Si
b) No

9. Se han firmado acuerdos o contratos de confidencialidad con todos los colaboradores y proveedores que maneja información sensible.

a) Si
b) No

SEGURIDAD FÍSICA Y DEL ENTORNO

10. Las claves de acceso de los equipos de comunicación son cambiadas con una periodicidad determinada de acuerdo a su normativa interna, si la respuesta es afirmativa indique la frecuencia de cambio.

a) Si. *Cada 6 meses*
b) No

11. Cuenta la institución con un sistema de suministro no interrumpido de energía o UPS que respalde la totalidad de equipos de cómputo, servidores y equipos de comunicación de la institución.

a) Si
b) No
c) No se

12. Los monitores de los equipos de cómputo están localizados para evitar el acceso y visualización de personas no autorizadas.

a) Si
b) No

13. Los sistemas de cableado estructurado están protegidos contra interceptaciones y daños.

a) Si
b) No

GUÍA DE ENCUESTA N°03

INSTITUCIÓN	**EDPYME ALTERNATIVA**
NOMBRE	Daniel Pérez Tesén
ÁREA O UNIDAD	TI
CARGO	RESPONSABLE DE SERVIDORES REDES Y COMUNICACIONES

GESTION EN LAS COMUNICACIONES

1. Se tiene implementado un sistema de protección contra código malicioso que cubra la totalidad de activos de información en las zonas rurales.

a) Si
b) No
c) No se

2. Para controlar la seguridad de la red en las zonas rurales, se tiene implementado sistemas de autenticación.

a) Si
b) No

3. Para controlar la privacidad de la información de la red, se tienen implementados sistemas de cifrado.

c) Si
d) No

4. Existe en su institución firewall perimetral. Por favor indique la cantidad existente

a) Si
b) No
Cantidad: **02 equipos de protección**

5. Existen sistemas de control capaces de detectar intentos de acceso no autorizados cuando se navega por internet.

a) Si
b) No
c) No se

6. Marque con un aspa "x" en caso de existir. A nivel de seguridad de la información, existe en su institución documentación de:

DOCUMENTACION	**MARQUE**
Políticas, normas y procedimientos de seguridad de la información.	**X**
Documento de evaluación y análisis de riesgo.	**X**
Diagramas de topologías de seguridad perimetral.	**X**
Reglas de seguridad.	**X**

ANEXO 05: GUÍAS DE ENTREVISTAS

GUÍA DE ENTREVISTA N°01: ANÁLISIS DE RIESGO

INSTITUCIÓN	**EDPYME ALTERNATIVA**
NOMBRE	Daniel Pérez Tesén
ÁREA O UNIDAD	TI
CARGO	RESPONSABLE DE SERVIDORES REDES Y COMUNICACIONES

Identificación y evaluación de activos

1. Describa las principales actividades que realiza

   Responsable de monitorear redes, evaluar nuevas infraestructuras físicas y lógicas de servidores, y velar por la seguridad perimetral de los equipos de comunicación

2. Definir los principales activos con los que se cuenta; entendiendo como un activo aquello que tiene valor para la unidad o área y que requiere protección.

ACTIVO	**REQUIERE PROTECCIÓN**
Hardware (equipo de cómputo físico)	**Si**
Software (aplicaciones para realizar su trabajo)	**Si**
Sistemas (aplicaciones adicionales)	**Si**
Datos e Información	**Si**
Personal	**Si**

3. Con base, en los activos mencionados anteriormente indicar el grado de importancia (valor) mediante un aspa (x).

ACTIVO	**MUY IMPORTANTE**	**IMPORTANTE**	**MEDIANAMENTE IMPORTANTE**	**SIN IMPORTANCIA**
Hardware	**X**			
Software	**X**			
Sistemas	**X**			
Datos e información	**X**			
Personal	**X**			

4. Cuál es la forma de almacenamiento para la información manipulada por su área o unidad. Enumérela con base en el orden de uso. (En caso de emplear otras formas mencioné y escriba brevemente)

FORMA DE ALMACENAMIENTO	**ORDEN DE USO**
Disco duro	**X**
Folder (Archivero)	
CD, DVD o Blue Ray	
USB	**X**
Otros	**X**

5. Considera que los medios de almacenamiento para la información, implementados en el Área o Unidad son seguros.

a) Si

b) No

c) No se

6. El personal con quien labora, tiene conocimientos acerca de los temas relacionados con la seguridad de la información.

a) Si

b) No

c) No se

7. Indique con qué frecuencia se presentan las siguientes situaciones marcando con un aspa (x), la situación que más se acerque a la realidad de la institución.

SUCESO	Muy probable	Probable	Poco probable	Probabilidad nula
Robo de información			X	
Ex empleados que hayan tenido acceso a la información sin autorización.		X		
Extravió de información por descuido del personal que la manipula.	X			
Alteración de información por personal no autorizado.				X
Lentitud en la respuesta cuando se trabaja con la red y el internet.	X			
Denegación de los servicios brindados por la red implementada en la institución.			X	
Desastres naturales que dañen equipo de la institución.				X
Personal ajeno a la institución que haya intentado recabar información por medio del servicio de internet		X		
Infección de los equipos de cómputo (virus, gusanos, spyware, malware en general)	X			
Modificación en la configuración de red de sus equipos, por terceros.				X
Fallas en los equipos de cómputo.	X			
Fallas eléctricas.	X			
Robo de equipos de cómputo, que contenga información de la institución.		X		
Acceso no autorizado a la información.			X	
Revelación de información confidencial por el personal que lo manipula.	X			
Copias no autorizadas de la información.			X	
Desconfiguración del sistema o de los dispositivos con los cuales se manipula la información.			X	
Accidentes por desconocer las políticas de seguridad o inexistencia de políticas.		X		
Falta de conocimiento técnico para realizar alguna tarea.		X		
Otros.				X

8. Si se presentarán cualquiera de las situaciones anteriormente mencionadas, que sucedería en la institución.

El riesgo de perder continuidad operativa y como somos una entidad supervisada por la SBS y sobre todo nuestro negocio es de brindar servicios financieros a los clientes, el riesgo de daño económico y de reputación sería muy alto, afectando los objetivos principales de la institución y de los colaboradores.