UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE INGENIERÍA

INGENIERÍA EN SISTEMAS COMPUTACIONALES

TEMA:

Diseño e implementación de una política de seguridad para una PYME. Caso de estudio: Empresa de servicios de Call Center

AUTOR (ES):

MEDIAVILLA SAVINOVICH, VANESSA ISABEL

Trabajo de titulación previo a la obtención del título de

INGENIERO EN SISTEMAS COMPUTACIONALES

TUTOR:

SALAZAR TOVAR, CESAR ADRIANO

Guayaquil, Ecuador

04 de marzo del 2020

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE INGENIERÍA

INGENIERÍA EN SISTEMAS COMPUTACIONALES

CERTIFICACIÓN

Certificamos que el presente trabajo de titulación fue realizado en su totalidad por **MEDIAVILLA SAVINOVICH, VANESSA ISABEL** como requerimiento para la obtención del título de **INGENIERO EN SISTEMAS COMPUTACIONALES**.

TUTOR (A)

f. _____
Salazar Tovar, Cesar Adriano

DIRECTOR DE LA CARRERA

f. _____
Camacho Coronel, Ana Isabel

Guayaquil, a los 04 días del mes de marzo del año 2020

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE INGENIERÍA

INGENIERÍA EN SISTEMAS COMPUTACIONALES

DECLARACIÓN DE RESPONSABILIDAD

Yo, **MEDIAVILLA SAVINOVICH, VANESSA ISABEL**

DECLARO QUE:

El Trabajo de Titulación, **Diseño e implementación de una política de seguridad para una PYME. Caso de estudio: Empresa de servicios de Call Center** previo a la obtención del título de **INGENIERO EN SISTEMAS COMPUTACIONALES**, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance del Trabajo de Titulación referido.

Guayaquil, a los 04 días del mes de marzo del año 2020

EL AUTOR (A)

f. _____
Mediavilla Savinovich, Vanessa Isabel

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE INGENIERÍA

INGENIERÍA EN SISTEMAS COMPUTACIONALES

AUTORIZACIÓN

Yo, **MEDIAVILLA SAVINOVICH, VANESSA ISABEL**

Autorizo a la Universidad Católica de Santiago de Guayaquil a la **publicación** en la biblioteca de la institución del Trabajo de Titulación, **Diseño e implementación de una política de seguridad para una PYME. Caso de estudio: Empresa de servicios de Call Center**, cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y total autoría.

Guayaquil, a los 04 días del mes de marzo del año 2020

EL (LA) AUTOR(A):

f. _____
Mediavilla Savinovich, Vanessa Isabel

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE INGENIERIA

CARRERA DE INGENIERIA EN SISTEMAS COMPUTACIONALES

REPORTE URKUND

URKUND

Urkund Analysis Result

Analysed Document:	Trabajo Titulación VIMS - final 9feb2020.docx (D63713749)
Submitted:	2/10/2020 8:38:00 PM
Submitted By:	${Xml.Encode(Model.Document.Submitter.Email)}
Significance:	1 %

TUTOR

f. _____

Salazar Tovar, Cesar Adriano

AGRADECIMIENTO

Doy gracias a Dios por permitirme llegar hasta este último escalón en conjunto con mi Familia y con todas las personas que de alguna u otra manera estuvieron presente.

DEDICATORIA

Este trabajo de titulación va dedicado a toda mi Familia; pero en especial a dos personas una aquí en tierra que me brindo todo su apoyo desde el inicio hasta el final mi Mami Yoli y a mi segunda persona especial mi Papi César que le prometí que sería una Ingeniera y aquí estoy cumpliendo cada una de mis palabras.

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE INGENIERÍA
INGENIERÍA EN SISTEMAS COMPUTACIONALES

TRIBUNAL DE SUSTENTACIÓN

f. _____

Ing. Ana Isabel Camacho Coronel
DIRECTOR DE CARRERA

f. _____

Ing. Cesar Adriano Salazar Tovar
DOCENTE DE LA CARRERA

f. _____

Ing. Marcos Xavier Miranda Rodriguez
OPONENTE

ÍNDICE

Índice de tablas

Índice de figuras

Índice de Anexos

RESUMEN

El presente trabajo **Diseño e implementación de una política de seguridad para una PYME. Caso de estudio: Empresa de servicios de Call Center** tiene como objetivo la implementación de una política de seguridad en donde se definió realizar el control sobre los accesos hacia internet que tiene el personal de la pyme; para el levantamiento de información se realizó una entrevista al Gerente de la empresa Spiritcom S.A en donde se definió que parámetros se deben cumplir para lograr el objetivo propuesto. Para ello se procedió con la investigación de herramientas acordes a los requerimientos mencionados en el análisis del proyecto mediante la instalación de una máquina virtual montada en un servidor con el software seleccionado. La implementación realizada cumplió con las necesidades del cliente y se logró mejorar el rendimiento en su equipo de trabajo y cumplió el objetivo propuesto desde el inicio del proyecto con la empresa Spiritcom S.A.

Palabras Claves: Pyme, política de seguridad, máquina virtual, servidor,software

ABSTRACT

The present work Design and implementation of a security policy for an SME. Case study: Call Center services company aims to implement a security policy where it was defined to carry out control over access to the Internet that has the staff of the SME; For the gathering of information, an interview was made with the Manager of the company Spiritcom S.A, in which it was defined what parameters must be met to achieve the proposed objective. For this, we proceeded with the investigation of tools according to the requirements mentioned in the project analysis by installing a virtual machine mounted on a server with the selected software. The implementation carried out met the needs of the client and it was possible to improve the performance of their work team and met the objective proposed since the beginning of the project with the company Spiritcom S.A.

Keywords: Pyme, Security Policy, Virtual Machine, Server, Software.

INTRODUCCIÓN

Actualmente la empresa Spirit Communications Spiritcom S.A ofrece el servicio como distribuidora oficial de Claro dirigido a ventas de portabilidad por medio del centro de atención telefónica a corto plazo tiene dimensionado dar servicios de cobranzas y servicios a clientes para diferentes tipos de empresas, motivo por el cual ellos tienen la necesidad de cumplir con certificaciones ISO y protocolos de seguridad que se encuentran definidos en los procesos operativos de la empresa.

Como centro de atención telefónica tienen la función de ofrecer servicios a través de llamadas telefónicas de las cuales pueden ser atención al cliente, soporte técnico o empresariales; los usuarios que forman parte de este grupo tienen varios accesos hacia repositorios de información, accesos a internet, sistema que es su herramienta de trabajo en donde brindan el soporte diario. Para ello es necesario pensar un poco en la seguridad que podríamos brindar para este tipo de negocio; configurar controles de seguridad en donde controle la navegación de los usuarios que se encargan de dar el soporte debido a que manejan información sensible y pueden abrir algún acceso en donde contenga algo malicioso y pueda afectar la operatividad general del centro de atención telefónica.

CAPÍTULO I
EL PROBLEMA

1.1 Planteamiento del problema

En la actualidad los usuarios de Spiritcom S.A tienen libre apertura para navegar hacia cualquier página de internet dentro de su jornada laboral permitiendo acceso a páginas restringidas o con posible spam. Cabe recalcar que la empresa se dedica a recopilar información por lo que trabaja con base de datos internas; las mismas que pueden ser afectadas si no se tienen los controles necesarios a los sitios que ingresan para cualquier tipo de consultas sean laborales o personales. Dado que no se cuenta con una política de seguridad que controle la navegación a internet en las estaciones de los usuarios finales que trabajan en la empresa esto podría llegar a provocar una fuga de información debido a que no existe alguna política de seguridad que prevenga lo antes mencionado por lo que se llegó a la conclusión de que debe diseñar y configurar un control en la navegación de las estaciones que hacen uso los usuarios de la empresa y así no exista fuga de información y poder cumplir con accesos a sitios que no sean corruptos.

1.2 Ubicación del Problema en un Contexto

En la actualidad los usuarios de Spiritcom S.A tienen libre apertura para navegar hacia cualquier página de internet dentro de su jornada laboral permitiendo acceso a páginas restringidas o con posible spam. Cabe recalcar que la empresa se dedica a recopilar información por lo que trabaja con base de datos internas; las mismas que pueden ser afectadas si no se tienen los controles necesarios a los sitios que ingresan para cualquier tipo de consultas sean laborales o personales

1.3 Causas y Consecuencias del Problema

El no poder contar con una política de seguridad que controle la navegación hacia internet en las estaciones de los usuarios finales que trabajan en la empresa podría llegar a provocar una fuga de información y corromper las actividades confidenciales que maneja a la interna la empresa.

1.4 Delimitación del Problema

El proyecto va orientado a una empresa que brinda el servicio de Centro De Atención Telefónica la misma cuenta con personal capacitado para brindar el soporte que brinda la empresa por lo que revisando un poco como trabaja la empresa Spiritcom S.A se validó que es necesario aplicar controles de seguridad en ciertos aspectos del negocio.

1.5 Formulación del Problema

La implementación de la política de seguridad tecnológica en los procesos de navegación de internet en la empresa Spiritcom S.A aumentará los niveles de seguridad y confiabilidad en las operaciones diarias de los usuarios.

1.6 Objetivos

Objetivo General

Diseñar e Implementar una política de Seguridad utilizando una plataforma open source para controlar los accesos internos y externos de los usuarios de la Empresa Spiritcom S.A

Objetivos Específicos

- Identificar la infraestructura de la empresa Spiritcom S.A que permita controlar los accesos internos y externos de los usuarios de la Empresa Spiritcom S.A.

- Diseñar la política de seguridad de acuerdo con el análisis previo en conjunto con la empresa Spiritcom S.A.
- Seleccionar una plataforma de tipo open source para realizar la implementación de la política de seguridad.

1.7 Alcances del problema

En este proyecto se desea diseñar, configurar e implementar lo siguiente:

- Monitorear los sitios de navegación en los endpoints de la empresa.
- Permitir sitios que puedan aumentar la productividad del personal que trabaja dentro de la empresa.
- Denegar los accesos que no son permitidos por la operatividad diaria de los usuarios a través de la plataforma seleccionada.
- Habilitar el acceso a un compartido para el ingreso de los usuarios y guardar información necesaria como parte de la operatividad.

1.8 Justificación e importancia

De acuerdo con lo revisado con la empresa se puede evidenciar las necesidades que desean cubrir para poder tener el mejor funcionamiento y operación de las actividades que desempeñan diariamente por lo que se vio la factibilidad de poder implementar la política de seguridad para mejorar y optimizar el tiempo de cada usuario en la ejecución de sus tareas y complementos diarios; esta implementación será realizada de acuerdo con los escenarios previos identificados.

1.9 Hipótesis o pregunta de investigación.

¿De acuerdo con el modelo de la empresa es factible poder realizar la implementación de una política de seguridad para el control de la navegación de la empresa en mención?

CAPÍTULO II
MARCO TEÓRICO

2.1 Definición de una Pyme

Una pyme es el acrónimo de pequeña y mediana empresa este término aplica para las personas que cuentan con el apoyo o asesoramiento de grandes empresas las mismas que producen altos valores en libros. Las pymes no solo funcionan en un solo ámbito comercial, sino que también se explaya hacia la tecnología. De acuerdo con lo que indica en un artículo comercial Francisco García presidente de la Cámara de la pequeña industria del Guayas: “Las micro, pequeñas y medianas empresas tienen que evolucionar, meterse en la tecnología, actualizarse de manera permanente. Hay algunas que se quedan en el tiempo”.

En cuanto a unos estudios realizados en la Cepal en el año 2013 la mayoría de las pymes de América Latina se encuentra en nuestro país Ecuador con un 44% y de ese porcentaje el 24% están generando o produciendo empleo. Para el Servicio de Rentas Internas las pymes se las conoce como: “conjunto de pequeñas y medianas empresas” esto va de acuerdo con su volumen de ventas, capital social, cantidad de trabajadores y su nivel de producción o activos presentan características propias de este tipo de entidades económicas (SRI, 2017).

En la actualidad, las pymes que se encuentran en el mercado se presentan en todas formas y dimensiones, ya sean sociedades o de un solo propietario, tienen libertad de desarrollar cualquier tipo de actividad, bien sea de producción, comercialización o prestación de servicios, donde se busca una utilidad. Según información del Estudio de Gestión Competitiva de las pequeñas y medianas empresas en la República del Ecuador, en el país las pymes representan el 95% de las unidades productivas (Jácome & King, 2013)

Tabla 1 América latina (8 países): Proporción de empresas, por tamaño

País	Microempresas	Pequeñas empresas	Medianas empresas	Grandes empresas
Argentina	81,6	16,1	1,9	0,4
Brazil	85,4	12,1	1,4	1
Chile	90,4	7,8	1,2	0,6
Colombia	93,2	5,5	1	0,3
Ecuador	95,4	3,8	0,6	0,2
México	95,5	3,6	0,8	0,2
Perú	98,1	1,54	0,34	0,02
Uruguay	83,8	13,4	3,1	0,6

Fuente: Cálculos elaborados por Federico Stezano sobre información de la OCDE y la CEPAL (2013)

2.2 Características de una Pyme

De acuerdo con los datos que indica el INEC en el año del 2017 en el Ecuador existen cerca de 884.236 Empresas distribuidas de la siguiente manera:

Figura N° 1 Variables de clasificación: Tamaño de la empresa.

Tomado de, ecuador en cifras. 2017

En la siguiente gráfica podemos observar que el 0.46% corresponde a las grandes empresas y que la mayoría corresponden a las micro, pequeñas y medianas empresas.

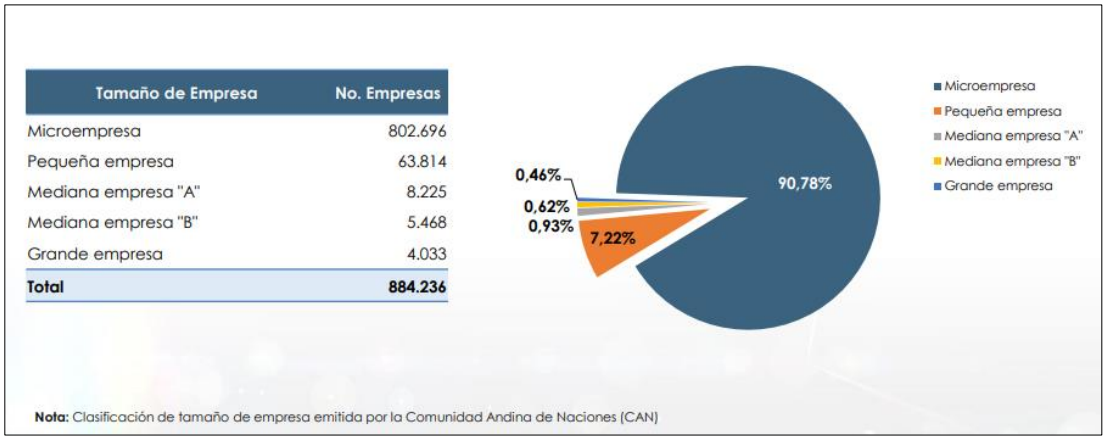

Figura N° 2 Clasificación de tamaño de la empresa.

Tomado de, ecuador en cifras. 2018

En la siguiente imagen que es proporcionada por el Directorio de Empresas y Establecimientos (DIEE) podemos validar que la estructura empresarial de Ecuador a partir de los registros administrativos proporciona información sobre el total de unidades económicas durante el periodo del 2018.

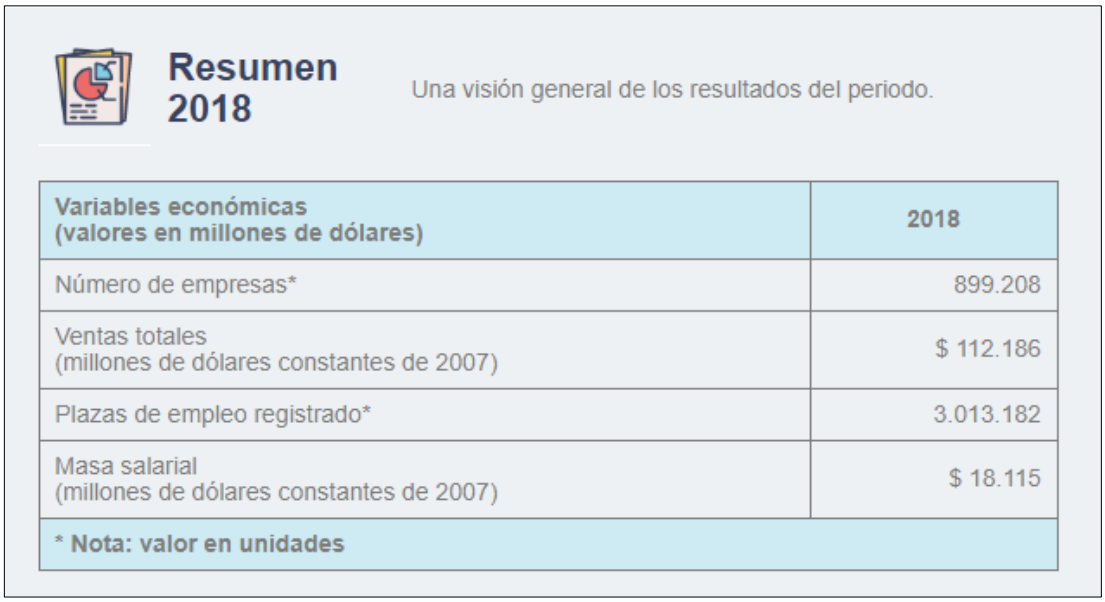

Figura N° 3 Resultados de variables económicas. Visión general de los resultados del período.

Tomado de, ecuador en cifras. 2018

2.3 Ciberseguridad en una Pyme

Es muy importante contar con seguridad tanto a nivel perimetral y dentro de una empresa debido a las diferentes adversidades que se puedan presentar en la pyme esto fue mencionado por Gilberto Vicente RSM Ciberseguridad de Cisco dentro de una sesión webinar en donde se demostró la siguiente imagen:

Figura N° 4 Ciberseguridad en las Pymes.

Tomado de, Conferencia Ciberseguridad en las Pymes. 2020

61% Pymes atacadas en los últimos 12 meses.
67% Personal no capacitado en ciberseguridad.
52% Proliferación de malware y amenazas.
54% Complejidad de soluciones de ciberseguridad.

Uno de los errores comunes en una pyme es que se asume que el problema no afecta cuando en realidad 3 empresas de 4 son atacadas por algún tipo de programa maligno. Eso nos lleva a caer en estrés y/o parálisis es decir que no se sabe o tiene pleno conocimiento a cómo reaccionar ante ello.

El hecho de tener equipos en nuestro rango perimetral o inclusive interno no es tan efectivo en su totalidad recordemos que existen múltiples equipos para proteger el ingreso de intrusos a nuestras redes. Es muy importante conocer e implementar una estrategia para respaldos o inclusive ante desastres naturales; conocer nuestros tiempos de respuestas y planes de acción. Esto nos llevará a mejorar en tres ámbitos: prevenir más, detectar mejor y responder más rápido de esa manera simplificamos todo.

Las consideraciones que debemos tener en cuenta para cuidar de la Seguridad en una Pyme:

- Identificar nuestros activos y en qué ambiente operan.
- Incrementar la visibilidad.
- Detectar y contener la situación.
- Reforzar las contraseñas y seguridad de accesos cada cierto tiempo
- Educar o capacitar al usuario.

2.4 Definición de una política de seguridad

Una política de seguridad es un conjunto de reglas que se deben aplicar de acuerdo con las actividades o tareas que se desempeñan en la empresa esto debe ir orientado a las tareas que realizan los usuarios abarcando controles para la red, seguridad lógica, seguridad física, seguridad de la información y seguridad administrativa para ello se debe tener una revisión previa para poder tener en claro los controles que se deben realizar. (ISO, 2017)

2.5 Definición de controles para la red

Según Massachusetts Institute of Technology indica que “existen tres tipos de controles que se pueden aplicar en la red que son: control físico, control técnico y control administrativo”. (MIT, 2004)

El control físico son las medidas que seguridad dentro de una parte o estructura es decir cerraduras en racks, cámaras dentro de un perímetro establecido, guardias

para controlar el acceso de entrada y salida de algún lugar que requiera de custodia, biométricos, etc.

El control técnico son aquellos que dependen de la tecnología para poder manipular o controlar los accesos hacia datos o información que no deben accederse tan fácilmente por ejemplo encriptar información sensible, hacer uso de tarjetas inteligentes, accesos a plataformas internas que sean integradas con doble autenticación, registro de accesos tal como logs de auditoria para poder tener control de los cambios que son realizados en las plataformas de tal manera que si sucede algún problema se tenga conocimiento desde donde se puede partir con la revisión.

Los controles administrativos son definidos bajo los recursos humanos que administran la seguridad, riesgos y otro tipos de controles dentro de la empresa debido a que la organización es quien determina los accesos que deben o no tener los usuarios hacia las aplicaciones internas que administran es bueno tener en consideración que todas las empresas se debe tener listo un plan de recuperación ante desastres naturales es decir tener un centro alterno listo para operar, saber elegir al personal que estará listo para responder ante este tipo de incidentes o cualquiera que se presente.

2.6 Definición de seguridad de la información

Dentro de la Seguridad de la información según manifiesta Britix (2017) “Seguridad Informática son técnicas desarrolladas para proteger los equipos informáticos individuales y conectados en una red frente a daños accidentales o intencionados”.

Mientras que de acuerdo con lo expresado por Baluja (2000), la Seguridad Informática maneja tres conceptos básicos importantes para la seguridad de la información, en particular, en lo relativo a la seguridad en Internet, o en redes de datos. Estos son: confidencialidad, integridad y disponibilidad. Con respecto a los

usuarios pudieran mencionarse otros como autenticación, autorización, contabilidad y no repudio. Explicando un poco con lo antes mencionado por los autores se llega a las siguientes definiciones de las importancias de la seguridad de la información:

Confidencialidad: Garantizar que el acceso a la información de una empresa es única e intransferible a personas que no sean internas a la misma.
Integridad: Mantener la exactitud y la completa discreción de la información que podemos observar y proteger nuestros conocimientos sin difundir algún detalle.
Disponibilidad: Validar que los usuarios tengan acceso a la información para cada ocasión que lo requieran.

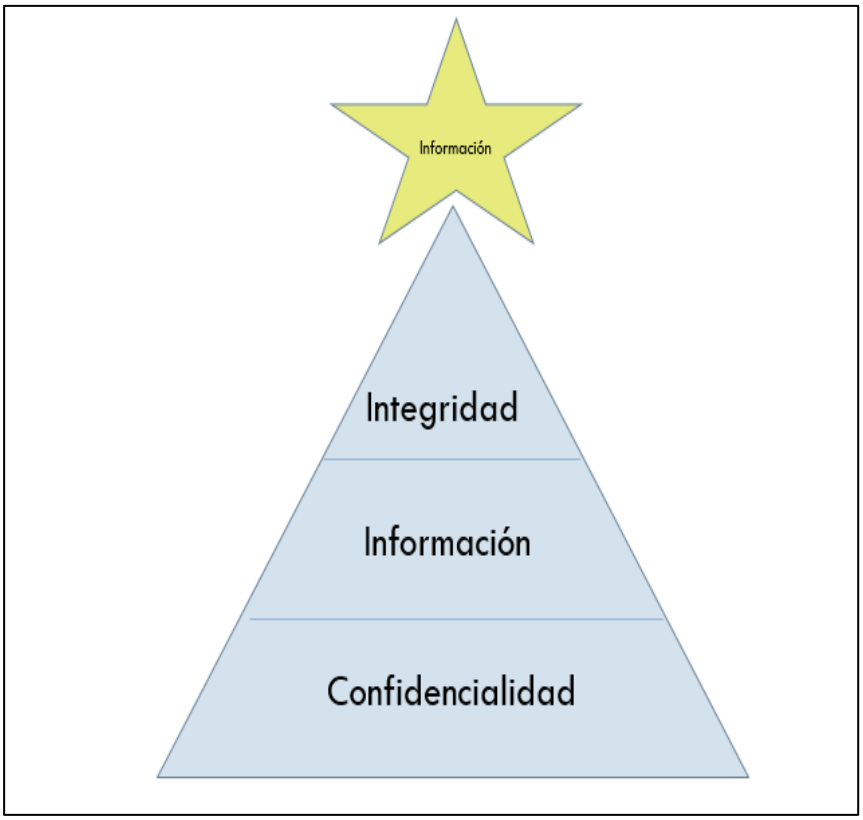

Figura N° 5 Jerarquía de la seguridad de información.

2.7 Definición de ISO 27001

Es un formato que es implementado en las empresas para poder acoplarse a los estándares que implica la seguridad de la información y se deben de ejecutar en lo posible para el cuidado de esta esto va orientado en las pequeñas, medianas o grandes empresas. Se debe tener en claro varios puntos como por ejemplo definir

la política, el alcance de la Seguridad de la Información, el análisis de riesgo, gestión de riesgo, controles, aplicabilidad y la revisión del sistema para que pueda ser auditado y poder cumplir con los lineamientos internos.

La ISO 27001 fue publicada el 15 de octubre de 2005, revisada el 25 de septiembre de 2013 esta ISO es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información; la ISO 27001 es la norma con arreglo a la cual se certifican por auditores externos los SGSIs de las organizaciones.

2.8 Definición de open source

Es una herramienta de uso libre en donde nos permite poder descargarlo de cualquier fuente o acceso que esté compartido de manera gratuita en donde no se requiere del uso de licencias para hacer uso de este; una definición más clara de Open Source es que es un software que permite la libertad de los usuarios. De acuerdo con lo que menciona Arteaga (2001) “los usuarios tienen la libertad de ejecutar, copiar, distribuir, estudiar, modificar y mejorar el software”; es decir, el software libre es una cuestión de libertad mas no de precio.

El documento encontramos información sobre la motivación de los desarrolladores de software libre dice que una fracción considerable está motivada por la idea que el software debería ser libre. El movimiento Open Source también hace cosas positivas, como convencer a más gente para que pruebe el software libre. Pero en sí mismo esto no es suficiente. Según Stallman (2004) comenta que “tenemos que ir más lejos y enseñar a los nuevos usuarios que aprecian el software libre a valorar también la libertad; por eso necesitamos el movimiento del software libre”.

El software de código abierto se desarrolla de forma descentralizada y colaborativa, basándose en la revisión por pares y la producción comunitaria. El software de código abierto es a menudo más barato, más flexible y tiene más longevidad que sus pares propietarios porque está desarrollado por comunidades en lugar de un solo autor o empresa

2.9 Definición de filtrado de navegación

Un filtrado de navegación es un programa diseñado para permitir o denegar los accesos hacia las páginas que se navegan en la web esto nos permite para poder controlar a qué lugares se ingresa desde dispositivos finales como una estación de trabajo. Es necesario que toda empresa o institución se tenga este tipo de controles para poder medir la productividad de su personal, saber qué cantidad de ancho de banda es necesario para ellos incluso hasta para conocer a qué sitios navegan para desempeñar su operatividad nacional o su tiempo libre. De acuerdo con un análisis realizado por (Estándar Magerit para análisis de riesgos informáticos, 2016) lo que menciona es que “se debe configurar adecuadamente el sistema, los servicios y entender las herramientas de detección”.

En la página oficial de Kaspersky (2020) se encontró lo siguiente: Un filtro web, comúnmente conocido como "software de control del contenido", es un software diseñado para restringir los sitios web que un usuario puede visitar en su equipo. Los filtros que normalmente se implementan dentro de un filtrado de navegación son los Whitelist o blacklist: las Whitelist solo permiten el acceso a sitios elegidos específicamente por quien configura el filtro; las blacklist restringen el acceso a sitios no deseados según lo determinado por las normas de la pyme.

2.10 Definición de Cisco ASA

Es un firewall de última generación que nos brinda mayores capacidades para detección de diferentes tipos de intrusiones y cuidados dentro del tráfico de la red este equipo puede funcionar como firewall o muchas veces como un contralor de proxy de última generación.

Es un equipo inteligente en comportamientos en red específicos, pero también nos ayuda para restringir el uso de internet y aplicaciones web que tengan mala reputación dentro de las categorías de acceso de la empresa. De acuerdo con lo que comenta Cisco sobre sus productos es que este equipo ayuda a las organizaciones a aumentar la capacidad y mejorar el rendimiento a través de clústeres de alto rendimiento, múltiples sitios y múltiples nodos también ofrece alta

disponibilidad para aplicaciones de alta resistencia y proporciona colaboración entre dispositivos físicos y virtuales.

2.11 Definición de Pfsense

Dentro de la página de Pfsense (2020) tiene una interfaz muy amigable y de sencilla administración puede ser usado como firewall el mismo es expandible y realizar diferentes funcionalidades de manera open source y evitar los altos costos de los cortafuegos que existen en el mercado adicional tal como menciona Pfsense (2018) es una aplicación que se instala como un sistema operativo ya que tiene varias funcionalidades entre estos servicios de redes LAN y WAN.

Es una herramienta gratuita que puede ser instalada en máquinas virtuales o en servidores dedicados con sistema operativo Linux la funcionalidad de este aplicativo gratuito es que sirve como un proxy en donde se puede dar accesos hacia páginas o bloquear comunicaciones que no deban ser permitidas hacia los usuarios. Como lo indica Torres (2016) una de las ventajas que puedes encontrar con Pfsense es la capacidad de implementar extensiones de terceros y también otra ventaja es la capacidad de redundancia, la traducción de direcciones de red y muchas posibilidades de configuración del DHCP

2.12 Definición de CoovaChilli

Es un controlador de acceso GNU (GLP), está basado en el programa ChilliSpot. Emplea Radius o un protocolo HTTP para ofrecer acceso, se puede configurar una tercera interfaz de modo Gateway para dar conexión a Switch y poder funcionar como si fuera un servidor DHCP. Tal como menciona Puetate (2016) “los usuarios que solicitan una conexión a esta interfaz deben cumplir el requerido proceso de autenticación antes de que el controlador le dé acceso a la red; para un mayor control al acceso se pueden configurar reglas de firewall”.

CAPÍTULO III
METODOLOGÍA DE LA INVESTIGACIÓN

El este capítulo se muestra la metodología utilizada y los resultados obtenidos a través de las herramientas elegidas para el levantamiento de información.

3.1 Tipo de Investigación

El tipo de investigación que se utiliza es de tipo exploratorio y descriptivo debido a que se hace uso de fuentes como libros, revistas, podcast, paginas oficiales de fabricantes, artículos y lecturas tecnológicas.

El método para aplicar es inductivo porque al inicio de la investigación está conformada las necesidades que requiere el cliente dueño de la empresa por lo que se determina los criterios de selección para analizar características fundamentales en el sistema corriendo.

3.2 Diseño de la Investigación

El diseño de la investigación es no experimental transeccional descriptiva debido a que desde el principio del proceso se evalúa que la empresa carecía de ciertos controles internos de seguridad por lo que se indica que se debe empezar con un control de navegación dentro de la red interna de la empresa.

3.3 POBLACIÓN Y MUESTRA

3.3.1 Población

La Empresa Spiritcom S.A es una pyme por lo que es un estudio con población completa; es decir el personal que opera con la atención de usuarios vía telefónica, el supervisor que está disponible para atender requerimientos críticos y el dueño de la empresa que está para establecer acuerdos formales con el personal que lo requiera.

3.4 Instrumentos de recolección de datos

Entre las técnicas de recolección de datos se utilizó una entrevista al dueño de la empresa (Véase **anexo 1**) para poder identificar los inconvenientes o malestares que presenta la pyme y poder buscar la manera de mejorar los controles internos dentro de la pyme. Una gran ventaja de realizar una entrevista es la técnica eficaz para obtener datos relevantes y significados desde el punto de vista de la persona que está siendo entrevistada. (Avendaño , Arciles, Rengifo, & Silva, 2016).

Complementando un poco con lo que menciona Burriel (2011) “la entrevista es una de las herramientas que tenemos disponibles cuando hablamos de análisis etnográfico como medio de indagación de usuarios”. Adicional por medio de la entrevista se pueden captar los gestos, los tonos de voz en cada pregunta que se realiza y también ayuda mucho con la información que se obtiene dentro de la entrevista.

3.5 Análisis de Resultados

3.5.1 Definición de análisis de resultados

Para llevar a cabo la definición del análisis de resultados se tuvo como referencia la entrevista realizada a Ricardo de la Paz Gerente General de Spiritcom S.A en donde expresa cuales son las necesidades que tiene su empresa actualmente como uno de los distribuidores más grandes de Claro requiere tener controles y conocer el rendimiento del personal que tiene a cargo y que la implementación ayude a sus usuarios a incrementar la eficiencia en la operativa diaria.

En la imagen que podemos observar representa la infraestructura de la empresa Spiritcom S.A en donde los usuarios se conectan mediante cable de red LAN y dos usuarios que son los VIP (Gerente General y Supervisor) tienen una tarjeta inalámbrica en donde la red es del mismo segmento de la LAN estos usuarios se conectan a las redes respectivas de tal manera que puedan ejecutar las tareas de su operatividad diaria teniendo en consideración que el acceso a la navegación es directo.

Los usuarios por políticas de la empresa no deben acceder a lugares que no sean permitidos por ejemplo Facebook, YouTube o redes sociales. Razón por la cual se implementó una política de seguridad en donde la función será controlar los accesos a la navegación de los usuarios permitiendo o denegándolos.

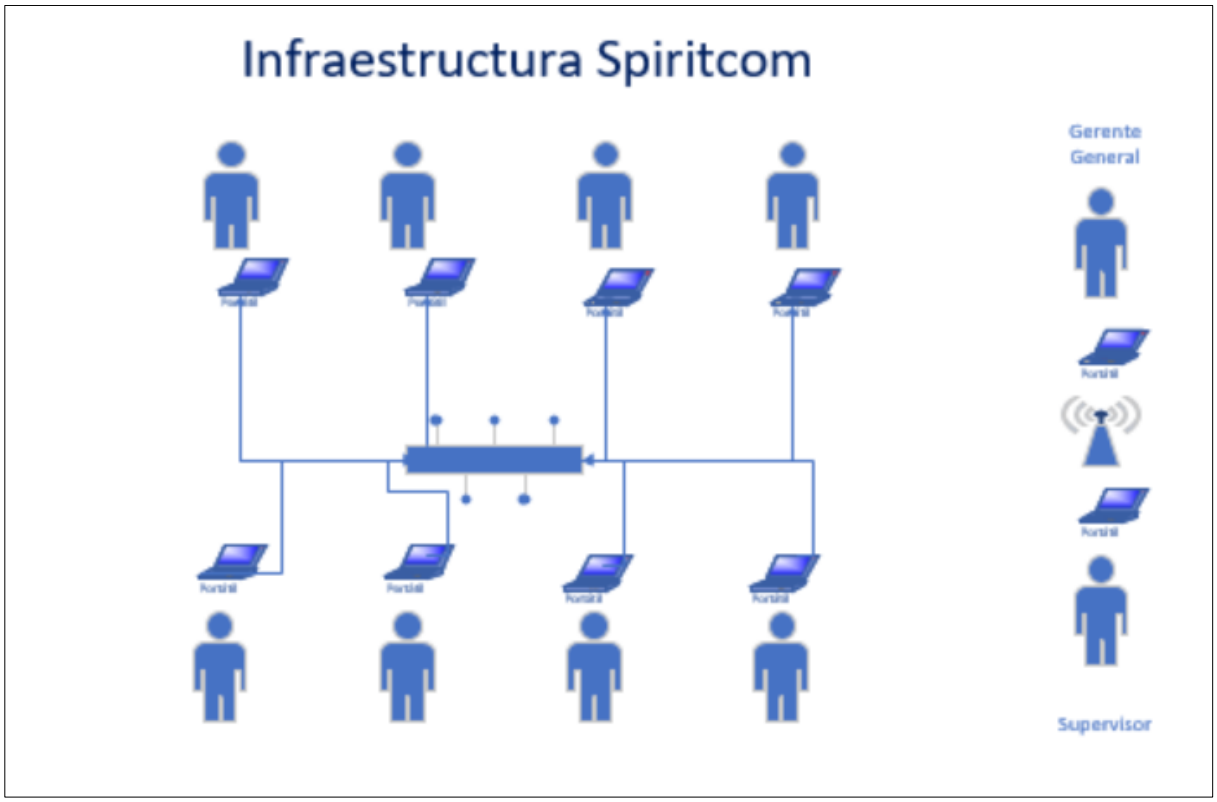

Figura N° 6 Diagrama de infraestructura Spiritcom.

Una de las limitaciones en la infraestructura de Spiritcom S.A es la cantidad de usuarios que trabajan dentro de la empresa es poca a comparación de las soluciones que se pueden invertir para la protección de la infraestructura; por lo que se sugirió en realizar un control a la navegación de dichos usuarios llevando como objetivo poder incrementar la eficiencia en usuarios y disminuir la falta de concentración en la operatividad diaria del centro de atención telefónica. Sin descartar que pueden existir más implementaciones para asegurar y fortalecer todos los componentes que incluyan a la infraestructura de la pyme.

Adicional el Gerente de Spiritcom nos indicó que existen muchas maneras de implementar tecnología dentro de una pyme tanto en costos, mantenimientos e implementación; por lo que se llevó a la conclusión de poder implementar un filtrado de navegación teniendo en cuenta que las políticas de seguridad son necesarias no solo para empresas que custodien información sensible sino más bien para llevar un control dentro de la pyme y poder proteger los puntos de fallo dentro de la infraestructura.

3.5.2 Definición de comparativa de análisis del software

Para la definición de las comparativas del análisis de software a implementar dentro del proyecto se realizó la siguiente tabla comparativa basándonos en los detalles especificados por el usuario adquiriente:

Tabla 2 Tabla Comparativa de las características principales entre Pfsense Vs Cisco ASA Vs CoovaChilli.

Tabla Comparativa	PFSENSE	CISCO ASA	CoovaChilli
Ventajas	Robusto y admite muchas funciones y paquetes.	La marca Cisco es fuerte en la industria de la red.	Permite instalar paquetes para ampliar funcionalidades
	Software gratuito y puede descargar la imagen del software desde cualquier navegador de internet.	Se ejecuta en hardware dedicado.	Software de codigo abierto
	pfSense es un software que se puede instalar en cualquier hardware hace que cumpla de acuerdo a las funciones a cumplir.	Personal Capacitado para poder responder ante los problemas que presentemos en el equipo.	Nos redirecciona a un portal cautivo donde se le piden los datos de acceso
Desventajas	La mayoria de las organizaciones usan una desktop como servidor dedicado para que cumpla las funciones de un control en la navegacion.	Cisco es muy costoso	Servidor dedicado
	Errores se presentan mientras se ejecuta pero no se puede descartar que tipo de error puede ser porque no es un equipo fisico.	Cisco ASA es principalmente un firewall pero se puede habilitar tambien como IDS / IPS no es tan fácil como instalar un paquete como el que tenemos con pfSense.	Se debe tener instalado un Radius para que pueda ser compatible.
	La configuración de pfSense se realiza a través de una interfaz gráfica de usuario (GUI).	Si necesita alguna configuracion especial se solicita a fabrica los cambios.	Implementacion y mantenimiento es a base de sentencias en linux.

La tabla comparativa antes mencionada fue revisada en conjunto con el dueño de la empresa para poder definir la herramienta a utilizar para el proyecto de implementación de una política de seguridad dentro de la pyme; en donde se validó que Pfsense cumplía con los requisitos que se nos proporcionaron al inicio y en la entrevista.

Se detalló que la herramienta escogida es una solución de tipo open source en donde contiene una interfaz gráfica web sencilla para el uso de los administradores de la herramienta también es de fácil instalación solo se debe tener una maquina con recursos abastecidos y funciona correctamente y no se requiere de algún tipo de licencia adicional para funcionar por completo.

CAPÍTULO IV
PROPUESTA TECNOLOGICA

En este capítulo se explica la implementación de una política de seguridad en la empresa Spiritcom S.A en donde se controla los accesos a la navegación que tienen los usuarios que trabajan dentro de la pyme. Esta implementación se la realiza mediante la configuración de la herramienta Pfsense que es una solución open source.

4.1 Política de Seguridad implementada en la Pyme.

La política de seguridad que fue propuesta cumple con la implementación de un filtrado de navegación para controlar las peticiones hacia internet que realizan los usuarios de la empresa dentro de su jornada laboral. El motivo por el cual nació la necesidad es que dentro de la entrevista realizada hacia el Gerente de Spiritcom S.A nos indicó que la mayoría de sus usuarios tienden a realizar varias actividades mientras atienden al usuario (actividades que no son las ideales al momento de realizar una atención al cliente) una de estas es el navegar hacia páginas de entretenimiento como lo son las redes sociales. El motivo por el cual se llevó a la conclusión de que es necesario realizar este tipo de controles que van a mejorar la productividad de los usuarios dando una mejor atención al cliente vía telefónica y evitando ingresar a páginas que no incrementan la productividad dentro de su operatividad diaria.

La política de Seguridad implementada se encarga de restringir los accesos a páginas que no son contempladas por las normas de la empresa para evitar posibles fugas de información, accesos a paginas restringidas o con mala reputación. Para mejorar la robustez de la infraestructura es importante tener un proxy como controlador de navegación por lo que se sugiere la siguiente infraestructura al dueño de la empresa Spiritcom S.A en donde se indicó dos soluciones posibles una de tipo open source.

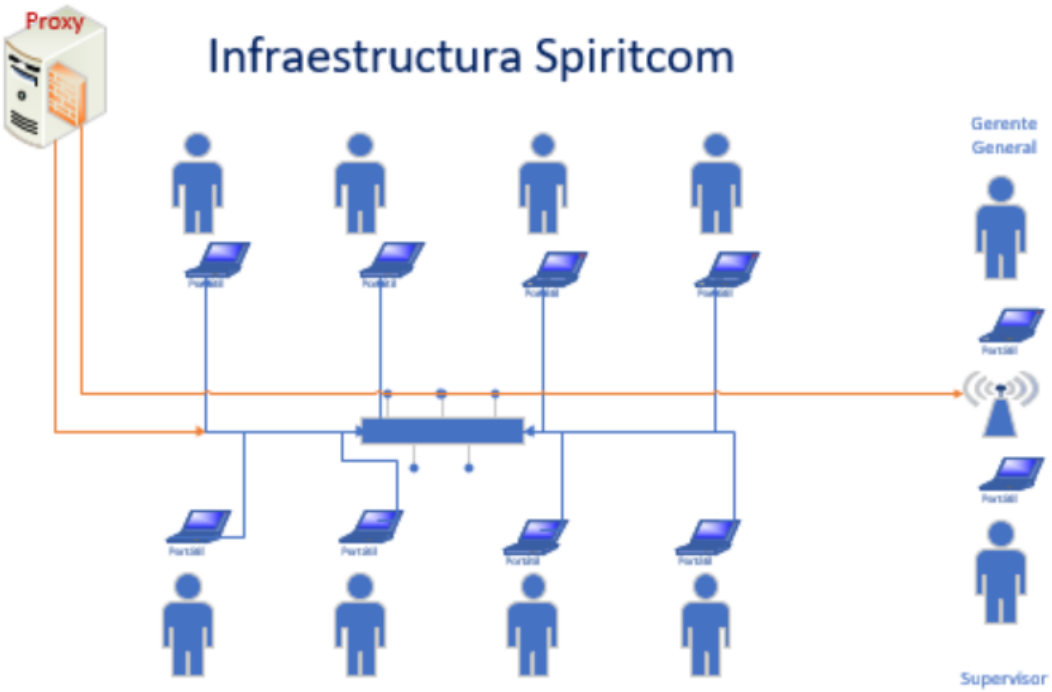

Figura N° 7 Diagrama de infraestructura Spiritcom con proxy pfsense.

4.2 Instalación de las herramientas a aplicar

Para poder iniciar la implementación y configuración de la herramienta Pfsense es necesario cumplir con los siguientes prerrequisitos a nivel de hardware (Véase **anexo 2**).

Con respecto a los prerrequisitos a nivel de software es necesario instalar una máquina virtual para poder hacer sincronización con el Pfsense (Véase **anexo 4**). Una vez instalada la VMware es necesario comenzar con la instalación de la ISO en donde corre el Pfsense (Véase **anexo 5**).

4.3 Configuración de las políticas en Pfsense.

Una vez culminada la instalación de la ISO correspondiente se comienza la configuración de la política de seguridad que es realizar el control de la navegación en la empresa Spiritcom S.A. Las políticas se las realiza desde la consola de administración del Pfsense tales como: ingreso de DNS, inspección de posibles actualizaciones, creación de políticas de acceso con acción allow/block respetando las necesidades de la empresa Spiritcom S.A

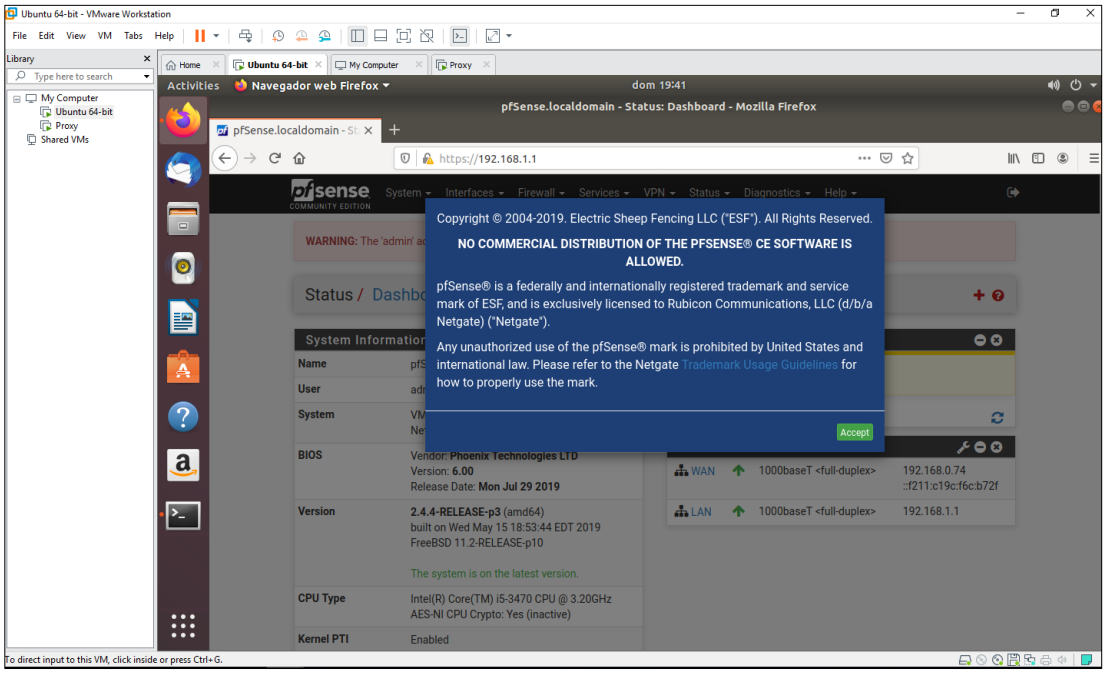

Figura N° 8 Dashboard de la consola de administración del Pfsense.

En el Dashboard se visualiza la sección de System configuration en donde se muestra información principal del equipo como, por ejemplo:

- Nombre del equipo.
- Usuario de inicio de sesión.
- Sistema Operativo/BIOS.
- Versión de la consola y posibles actualizaciones.
- Tipo de CPU.
- Interfaces configuradas.

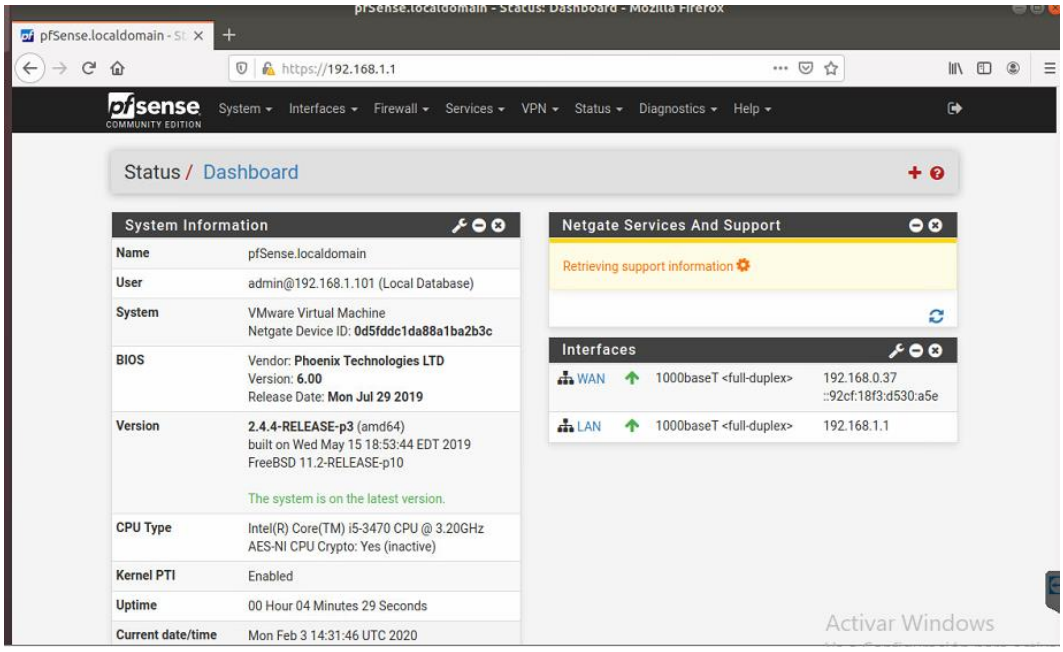

Figura N° 9 Dashboard de la consola de administración del Pfsense.

Es importante tener en cuenta que se debe realizar configuraciones especiales como:

En esta opción solo se debe validar que el admin access se encuentre completo el campo de SSL Certificate.

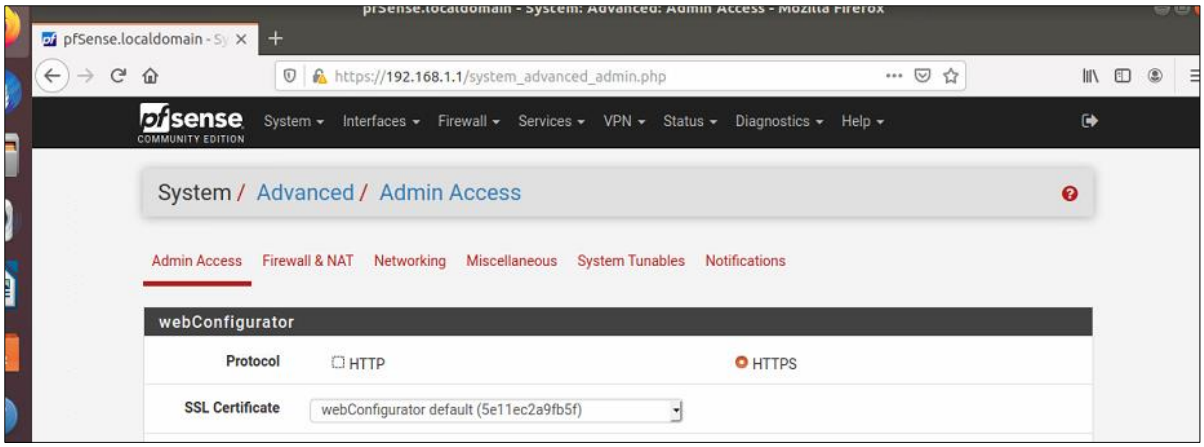

Figura N° 10 Configuracion de SSL Certificate.

La configuración del TFTP Proxy se debe agregar WAN y LAN debido a que son los tipos de redes que va a inspeccionar el Pfsense.

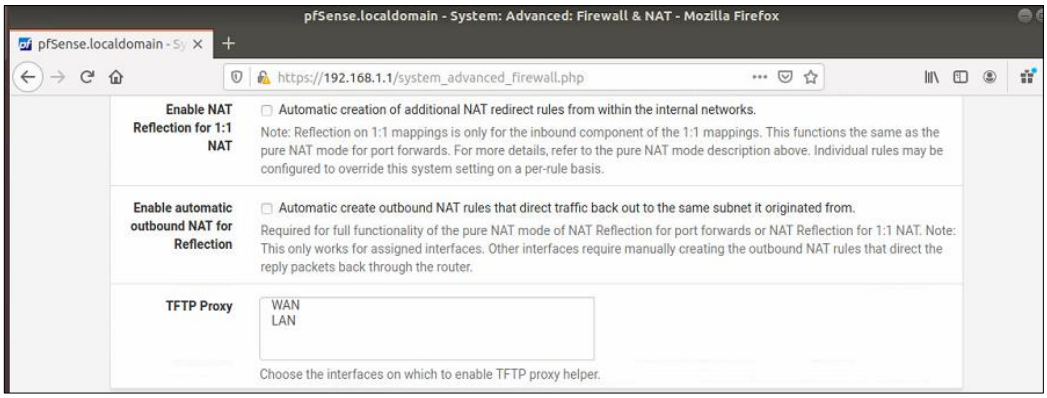

Figura N° 11 Configuración TFTP Proxy.

Para la configuracion de los dns solo se debe habilitar la opción y elegir el puerto de comunicación que es el 53

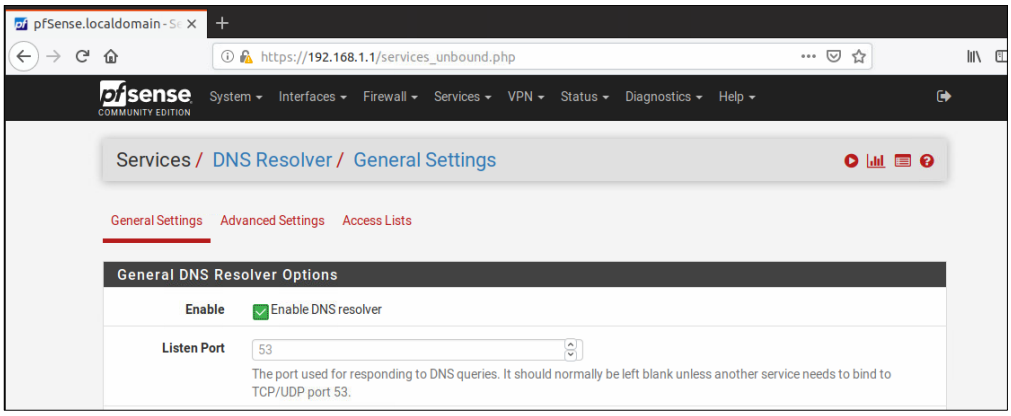

Figura N° 12 Habilitación de dns.

Las interfaces son aprendidas de manera automática en cuanto se empieza con las configuraciones previas de la VMWare con la ISO del Pfsense una vez encendida empieza a hacer un barrido de la data que tiene dentro del equipo.

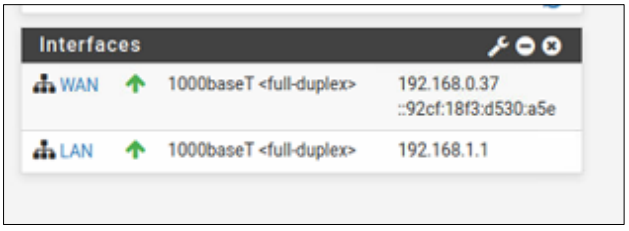

Figura N° 13 Interfaces configuradas.

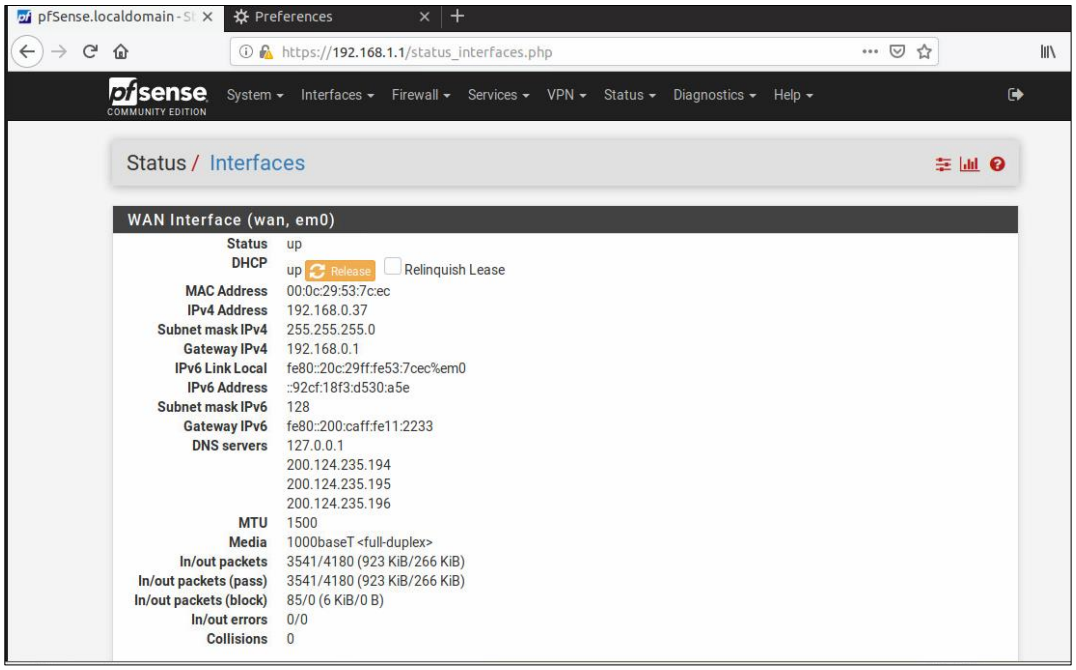

Figura N° 14 Interfaces configuradas WAN.

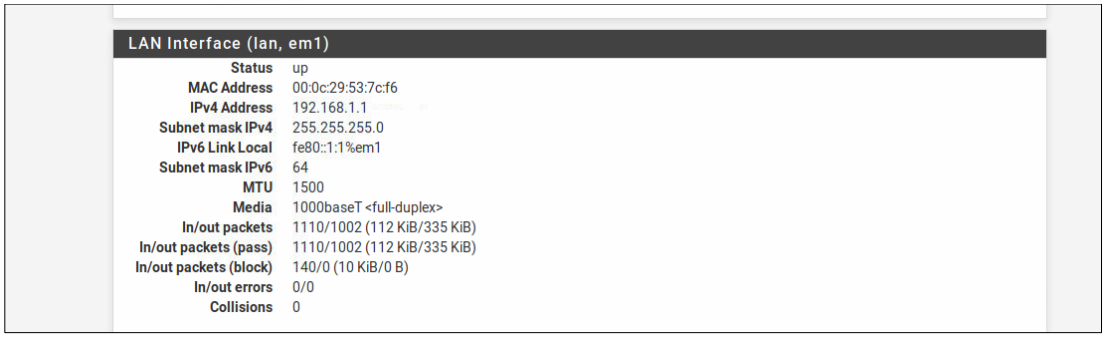

Figura N° 15 Interfaces configuradas LAN.

Blacklist o políticas de bloqueo: Las principales políticas que se tienen configuradas en modo bloqueo por requerimiento de la empresa debido a que no es parte de la operatividad de los usuarios son las siguientes:

Figura N° 16 Configuración de políticas en modo Block.

Pfsense tiene una de las ventajas más importantes en comparación a los otros proxys de que la configuración es fácil y sencilla ya que desde que se realizan los prerrequisitos el equipo empieza a adaptarse a las configuraciones del servidor o maquina dedicada para cumplir con las funciones requeridas. Cabe recalcar que el Pfsense trae por default un pool de reglas de accesos con acción en Block y Permit; este paquete de rule base pueden ser modificados de acuerdo con las necesidades que se requieren tener dentro de configuración de políticas.

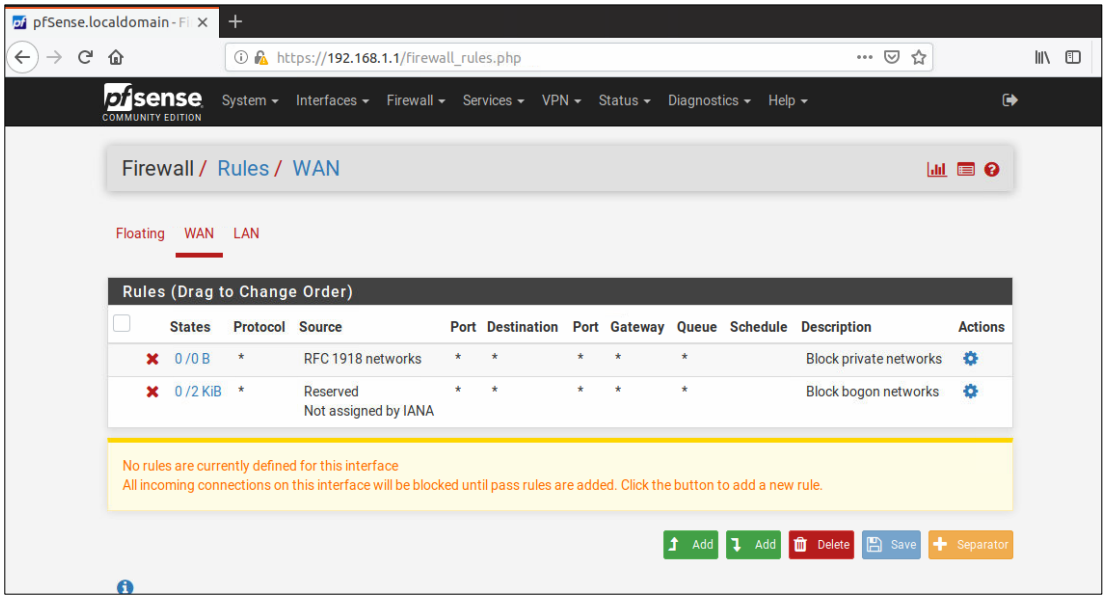

Figura N° 17 Configuración de políticas en modo Block de la red WAN.

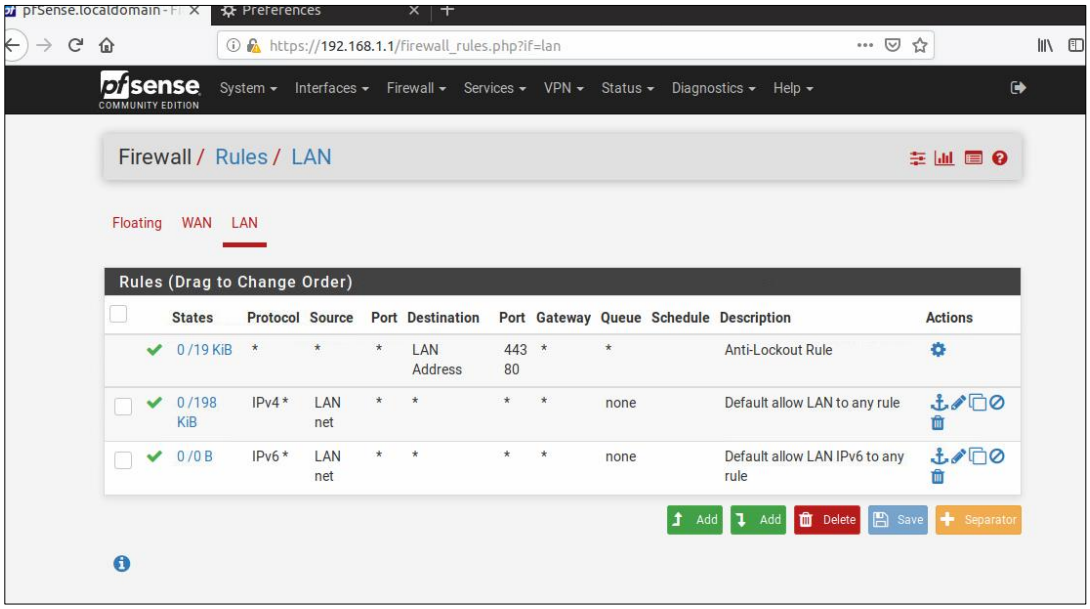

Figura N° 18 Configuración de políticas en modo Block de la red LAN.

Como detalle adicional a las herramientas activas en la pyme se valida las dimensiones del servidor y se configura un recurso a acceso compartido debido a la gran cantidad de información sensible que maneja la empresa Spiritcom S.A y no es centralizada en ningún lugar seguro. (Véase **anexo 3**).

4.3 Estrategias de seguridad aplicadas

Las estrategias aplicadas como parte de seguridad a la política configurada en la empresa Spiritcom S.A se enfocó en la protección avanzada contra las amenazas de spam es decir se tiene activado el paquete de políticas que viene por defecto para que de esa manera no se permita el acceso a páginas que sean de categoría maliciosa esto va de la mano con un control de auditorías y monitoreo a la navegación; por esta razón es necesario revisar periódicamente la bitácora de acceso de los usuarios para validar a que sitios son los que acceden normalmente y de esa manera poder afinar las políticas de acceso en caso de ser necesario o simplemente fortalecer las configuraciones realizadas.

CONCLUSIONES

A continuación, se detallarán las conclusiones del proyecto de implementación de una política de seguridad dentro de una pyme canalizando el acceso a internet a través de una red inalámbrica o cableada:

- Se identificó el diseño y topología de la infraestructura de la empresa y se pudo determinar las falencias en el control a la navegación que realizan los usuarios.
- De acuerdo con los requerimientos obtenidos durante el proceso de levantamiento de información en la pyme se estableció utilizar una plataforma open source para la implementación de la política de seguridad propuesta para la empresa.
- Al implementar un elemento de red como lo es el proxy se va a brindar más seguridad para la infraestructura de la pyme. Ya que puede controlar el tráfico y así serán menos las posibilidades de ataques a hacia la red o posibles spams.

RECOMENDACIONES

A continuación, se detallarán las recomendaciones a seguir para mantener el correcto funcionamiento de la implementación realizada:

- Se recomienda realizar respaldos de la información periódicamente para estar prevenidos ante algún tipo de error que presente el servidor para ello se indicará que se debe realizar capturas de las configuraciones debido a que no permite generar un archivo de backup del equipo administrado.
- Es importante previo a una actualización revisar la hoja de detalles de las mejoras que contiene la nueva versión a instalar debido a que las actualizaciones pueden crear grandes impactos al performance del servidor dedicado al filtro de navegación.
- Se recomienda que la Universidad Católica Santiago de Guayaquil a través de las practicas preprofesionales brinde el soporte a la empresa Spiritcom S.A para cambios específicos que se requieran realizar dentro de las configuraciones globales de la solución.
- Como futuros trabajos a implementar se recomienda que se tenga un equipo adicional con replicación de las configuraciones para hacer uso de este en caso de crearse un incidente o desastre natural y de tal manera poder continuar con la operatividad sin interrupciones.

REFERENCIAS BIBLIOGRAFICAS

Alvarez Torres, Z. E. (2016). *Diseño e implementacion de un sistema integrador de borde con funcionalidad de routing, firewall y central telefonica para PYMES.*

Arteaga, L. (2001). *¿Que es el software libre?*

Avendaño , F., Arciles, J. C., Rengifo, L., & Silva, O. (2016). *Tecnicas de estudio e investigacion .* Caracas.

Baluja. (2000). *Aspectos generales de la seguridad informática.*

BELT IBÉRICA. . (s.f.). *Seguridad informática. ¿Objetivos de la seguridad informática, que tenemos que tener en cuenta?* Obtenido de http://www.belt.es/noticiasmdb/HOME2_noticias.asp?id=13451

BRITIX. (2017). *Seguridad informática* .

CISCO. (s.f.). *Firewalls de próximo generación*. Obtenido de Cisco ASA de la serie 5500-X: https://www.cisco.com/c/es_mx/products/security/asa-5500-series-next-generation-firewalls/index.html

GNU. (2017). *El sistema operativo GNU*. Obtenido de ¿Qué es el software libre?: https://www.gnu.org/philosophy/free-sw.es.html

Gómez, C. (2009). *Open source software in scientific computation, International Workshop on Open-source Software for Scientific Computation(OSSC).* Guiyang. Recuperado el 2019, de : http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5416842&isnumber=5416736

Instituto nacional de estadísticas y censos. (2018). *Sistema de Indicadores de la producción*. Obtenido de https://www.ecuadorencifras.gob.ec/directoriodeempresas/

ISO. (2017). ISO 27000. Obtenido de http://www.iso27000.es/iso27000.html

Jácome, H., & King, K. (2013). *Estudios Industriales de la micro, pequeña y mediana empresa. .* Quito: Flacso.

Kaspersky. (2020). *Kaspersky*. Obtenido de Filtrado web.¿Qué es un filtro web?: https://latam.kaspersky.com/resource-center/definitions/web-filter

Lawrence, R. (2005). *Open Source Licensing: Software Freedom and Intellectual Property Law.* Prentice Hall.

Liu, J. G., Dang, Y. Z., & Wang, Z. G. (2006.). Relationship between the in-degree and out-degree of WWW. En J. G. Liu, Y. Z. Dang, & Z. G. Wang, *Relationship between the in-degree and out-degree of WWW* (págs. 861-869).

Lu, J., & Yang, Y. (2008). WebGIS server based on open source software to build. En *SPATIAL INFORMATION TECHNOLOGY* (págs. 145-147).

MIT. (01 de 01 de 2004). *Controles de seguridad*. Obtenido de Red Hat Enterprise Linux: http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-sg-es-4/s1-sgs-ov-controls.html

NetSolutions. (2020). Obtenido de Flash Start Cloud: https://www.netsolutions.com.uy/index.php?option=com_content&view=article&id=159&Itemid=610

OCDE. (2013). *Perspectivas económicas de América Latina 2013: Políticas de PYMES para el cambio estructural.* Publicaciones de la OCDE., Paris.

Pfense. (2018). *Tele Info IT Security Access*. Obtenido de https://www.teleinfo.mx/que-es-pfsense/

Pfsense. (2020). *Security, Design, Implementation*. Obtenido de https://www.pfsense.org/

Políticas de Seguridad. (2016). Obtenido de http://redyseguridad.fip.unam.mx/proyectos/seguridad/DefinicionPolitica.php

Poveda, J. M. (s.f.). *Los activos de seguridad de la información.* Obtenido de http://www.worldvisioncapacitacion.cl/wp-content/uploads/cursos_adjuntos/f52e0bd4c6c2c203413952826f916237.pdf

Proactive Solutions to the Five Most Critical Networking Problems. (1999). Obtenido de http://www.eisa.com/resources/pdf/Proactive%20Solutions%20to%20the%20Five%20Most%20Critical%20Networking%20Problems%20.pdf

PYMES obligatoriedad a partir del 2019. (2019).

REDHAT. (2020). *La libertad de elegir un proveedor sin depender*. Obtenido de https://www.redhat.com/es/open-source/red-hat-way

Reyes Puetate, R. R. (2016). *SISTEMA DE CONTROL DE ACCESO PARA PEQUEÑAS.* Guayaquil.

Seditel. (2015). *Seguridad de la red: Servicios de firewall de última generación Cisco ASA*. Obtenido de https://www.seditel.eu/asa-seguridad-de-la-red

Sistema de gestión de la seguridad de la información. (2016). Obtenido de http://www.iso27000.es/ download/doc_sgsi_all.pdf

SRI. (31 de 05 de 2017). *¿Qué son las PYMES?* Obtenido de Http://www.sri.gob.ec/de/32

Stallman, R. M. (2004). *Software libre para una socidad libre.* Obtenido de https://www.gnu.org/philosophy/fsfs/free_software.es.pdf

Torres Burriel, D. (25 de 06 de 2011). *La entrevista como herramienta de análisis de usuarios*. Obtenido de https://www.torresburriel.com/weblog/2011/06/25/la-entrevista-como-herramienta-de-analisis-de-usuarios/

Yi, L., Bai, G., & Xiao, G. (2000). Proxy Multi-signature: A New Type of Proxy Signature Schemes.

Zheng, X., Zeng, D., & Li, H. (2007.). Analyzing and modeling open source software as comp lex networks. En X. Zheng, D. Zeng, & H. Li, *Complex Systems and Complexity Science* (Vol. 4, págs. 1-8).

ANEXOS

Anexo 1

TVMS-ENTREVISTA01

Entrevista al dueño de la Empresa SPIRITCOM S.A

- ¿Quién es el cliente?

Spirit Communications SPIRITCOM S.A.

- ¿A qué se dedica?

Distribuidor autorizado de claro, dedicado a la venta como Contact Center de servicios de telefonía

- ¿Cómo están estructurados en Spiritcom S.A?

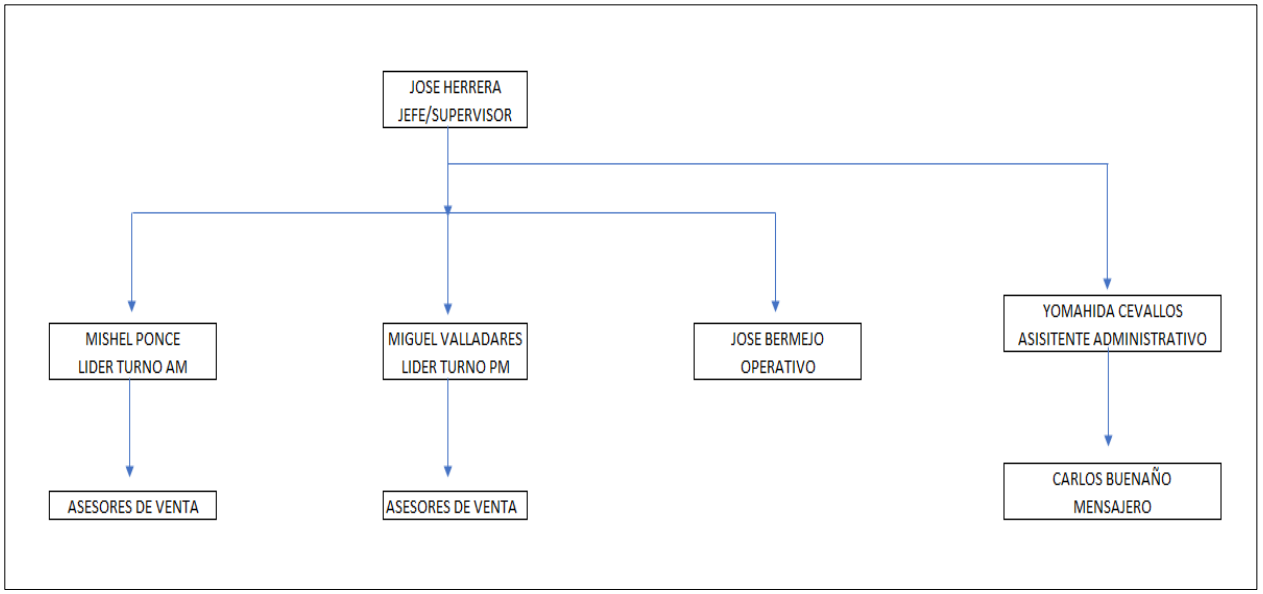

Figura N° 19 Estructura de la Empresa Spiritcom S.A.

- ¿Cuál es el proyecto que se está implementando en la empresa Spiritcom S.A?

Implementar una política de seguridad para el control en la navegación en las máquinas de los usuarios finales.

- ¿Qué objetivos tiene la implementación de este proyecto dentro de su Empresa?

Optimizar el tiempo de ocupación de los vendedores, evitando la distracción de estos en aplicativos y páginas que no van acorde a su gestión, al mismo tiempo evitar la fuga de información confidencial de nuestros clientes.

- ¿Cómo se van a medir los resultados en el personal que lleva a su cargo?

Se debe de mejorar el tiempo de Ocupación de los asesores en un 40%. Se debe de generar un incremento en ventas del 10%

- ¿Quién está implicado en el proyecto?

Está implicado:

- Personal de atención a usuarios vía telefónica
- Supervisor
- Dueño de la empresa

- ¿A qué se dedica el personal de atención al cliente?

Se dedican a las Ventas vía telefónica.

- ¿Cómo se llama y a qué se dedica el Supervisor/líder del personal de atención al cliente?

De acuerdo con la estructura mencionada en la pregunta anterior tengo dos personas que son: Mishel Ponce y Miguel Valladares ellos son mis líderes de Ventas encargados de realizar las tareas de:

- Controlar la producción de los asesores.
- Retroalimentar a los ejecutivos de venta.
- Controlar la asistencia, atrasos y gestión de los asesores.

- ¿Cómo se llama y a qué se dedica el Jefe Administrativo?

Mi jefe administrativo es José Herrera y se dedica a las siguientes actividades:

- Controlar el correcto funcionamiento de la gestión operativa.
- Realizar la proyección de ventas y crecimiento de personal de forma mensual.
- Asegurar el cumplimiento de la proyección en ventas realizada.

- ¿Cuál es su papel en el proyecto implementado?

Bueno la verdad, mi papel en este proyecto es poder tener la tranquilidad de que mi personal desempeña sus tareas de manera eficiente, cabe recalcar que es cierto que confío en mi personal a cargo, pero no está de más poder cumplir con estrategias de seguridad.

Anexo 2

Requisitos de hardware

- Procesador 600Mhz de 64bits
- 8GB DE MEMORIA RAM
- 1TB de Disco Duro
- 2 tarjetas de Red (mínimo WAN y LAN)
- Puerto USB o DVD para instalación del ISO
- Conectividad a Internet
- Referencia: Intel Core i5

En el transcurso de las configuraciones se procedió con la actualización del Sistema Operativo Windows quedando de la siguiente manera:

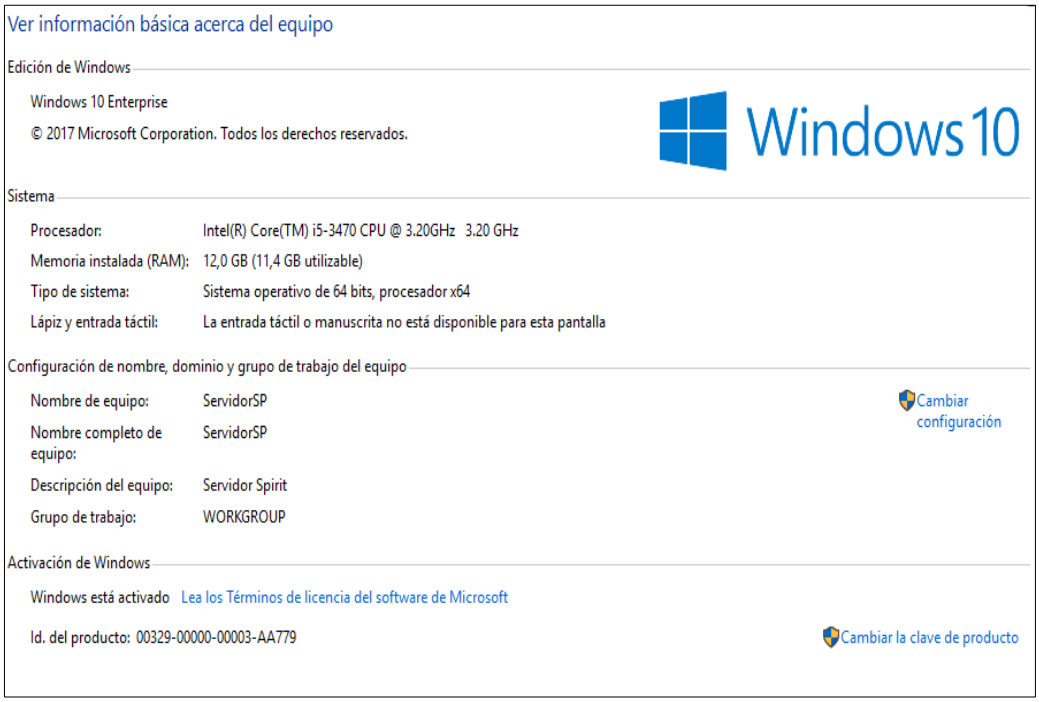

Figura N° 20 Información sobre el equipo.

Anexo 3

Configuración de un recurso compartido

Como parte de la implementación del proyecto en la Pyme se observó la necesidad de realizar la configuración de un recurso compartido en donde servirá como repositorio de información de la empresa Spiritcom S.A

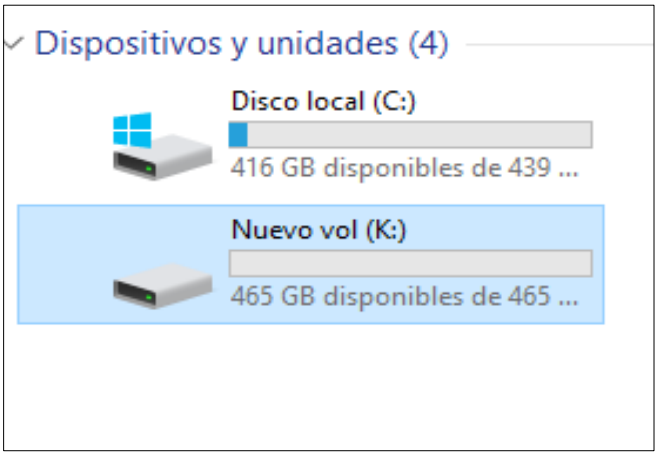

Figura N° 21 Creación de acceso compartido.

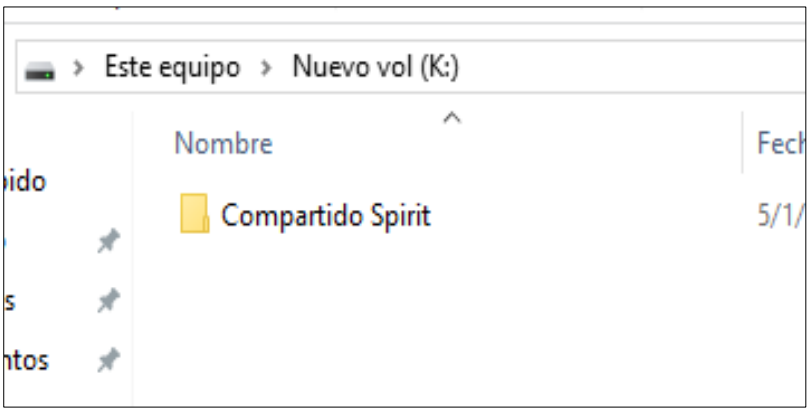

Figura N° 22 Visualización de compartido Spirit.

Anexo 4

Configuración de la máquina virtual

Una de las validaciones previas para la configuración de la máquina virtual es comprobar el tipo de infraestructura de red que esta implementada en la empresa Spiritcom S.A. Se procede con una inspección y se lleva a la conclusión que sus accesos son vía DHCP de acuerdo al rango que tienen reservados en la pyme.

```
Sufijo DNS específico para la conexión. . :
Descripción . . . . . . . . . . . . . . : Broadcom NetXtreme Gigabit Ethernet
Dirección física. . . . . . . . . . . . : 00-10-18-8A-7B-B0
DHCP habilitado . . . . . . . . . . . . : sí
Configuración automática habilitada . . . : sí
Vínculo: dirección IPv6 local. . . : fe80::58d9:6448:7425:9a22%3(Preferido)
Dirección IPv4. . . . . . . . . . . . . : 192.168.0.67(Preferido)
Máscara de subred . . . . . . . . . . . : 255.255.255.0
Concesión obtenida. . . . . . . . . . . : domingo, 5 de enero de 2020 10:08:38
La concesión expira . . . . . . . . . . : domingo, 5 de enero de 2020 11:08:38
Puerta de enlace predeterminada . . . . . : 192.168.0.1
Servidor DHCP . . . . . . . . . . . . . : 192.168.0.1
IAID DHCPv6 . . . . . . . . . . . . . . : 50335768
DUID de cliente DHCPv6. . . . . . . . . : 00-01-00-01-25-A4-02-94-24-BE-05-0E-F4-06
Servidores DNS. . . . . . . . . . . . . : 200.124.235.194
                                         200.124.235.195
                                         200.124.235.196
NetBIOS sobre TCP/IP. . . . . . . . . . : habilitado
```

Figura N° 23 Direccionamiento de red vía DHCP.

Dando inicios a la configuración del PFSENSE se vio la necesidad de instalar una máquina virtual con sistema operativo Linux; en ese ambiente se ejecutarán las configuraciones y pruebas. A continuación, las configuraciones paso a paso de la máquina virtual:

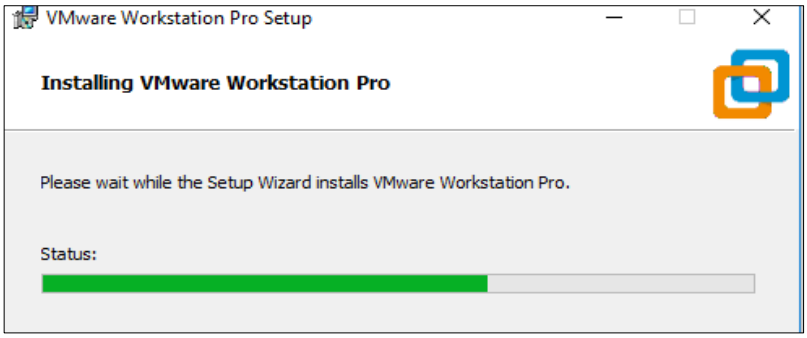

Figura N° 24 Instalación de la máquina virtual.

Una vez ya instalada se comienza con las configuraciones de los parámetros de los recursos necesarios para la máquina virtual

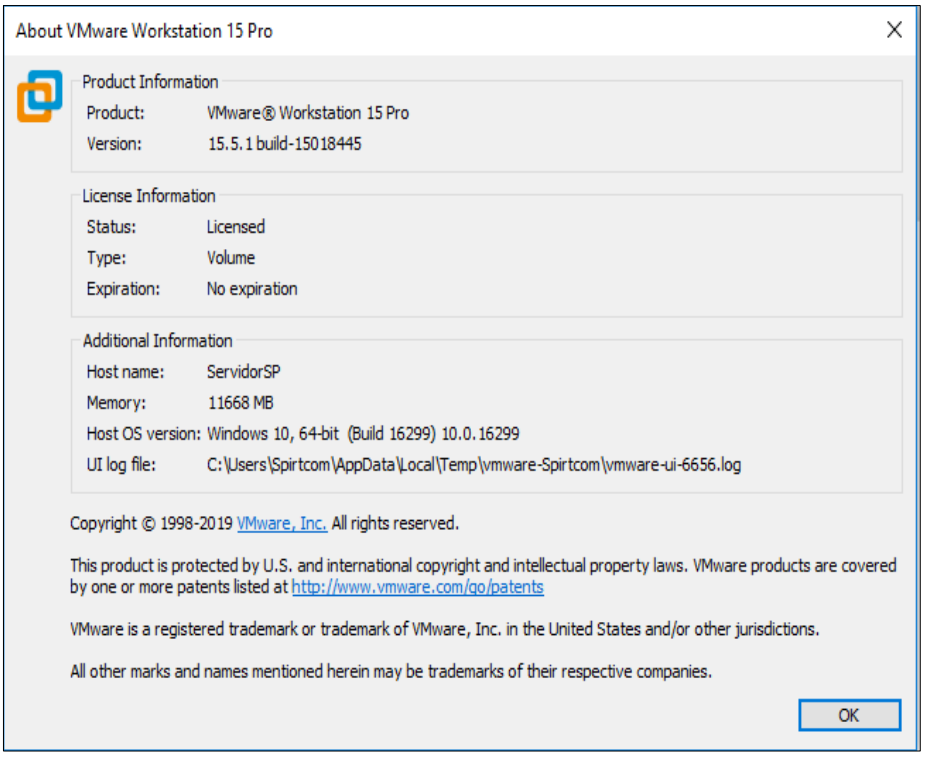

Figura N° 25 Configuración de la máquina virtual.

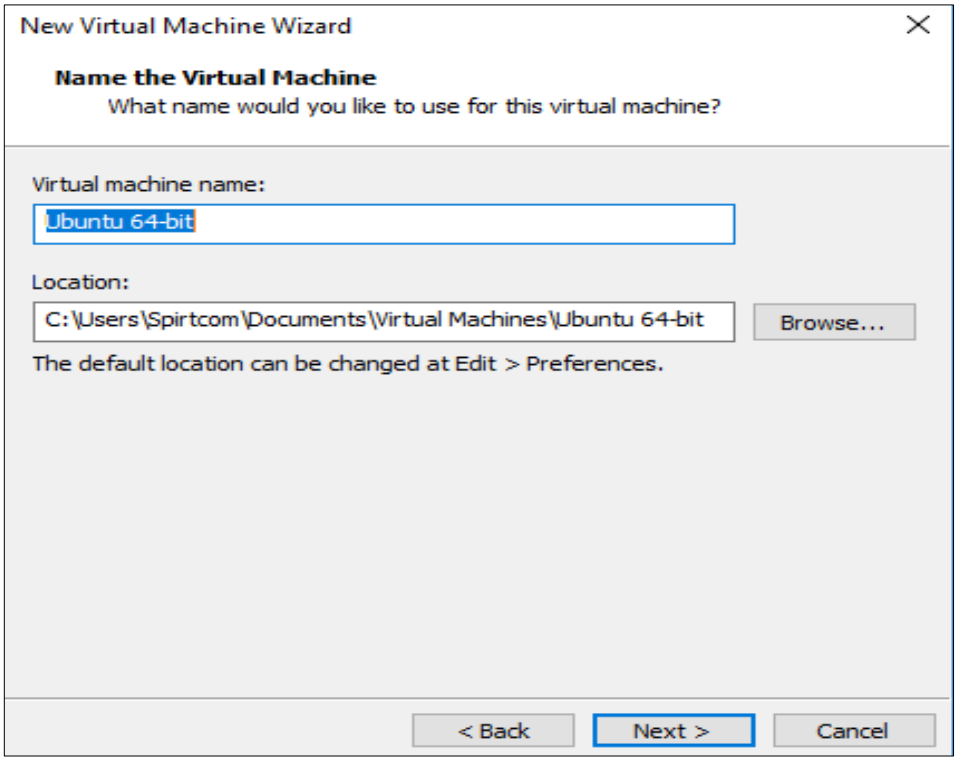

Figura N° 26 Configuración de la máquina virtual.

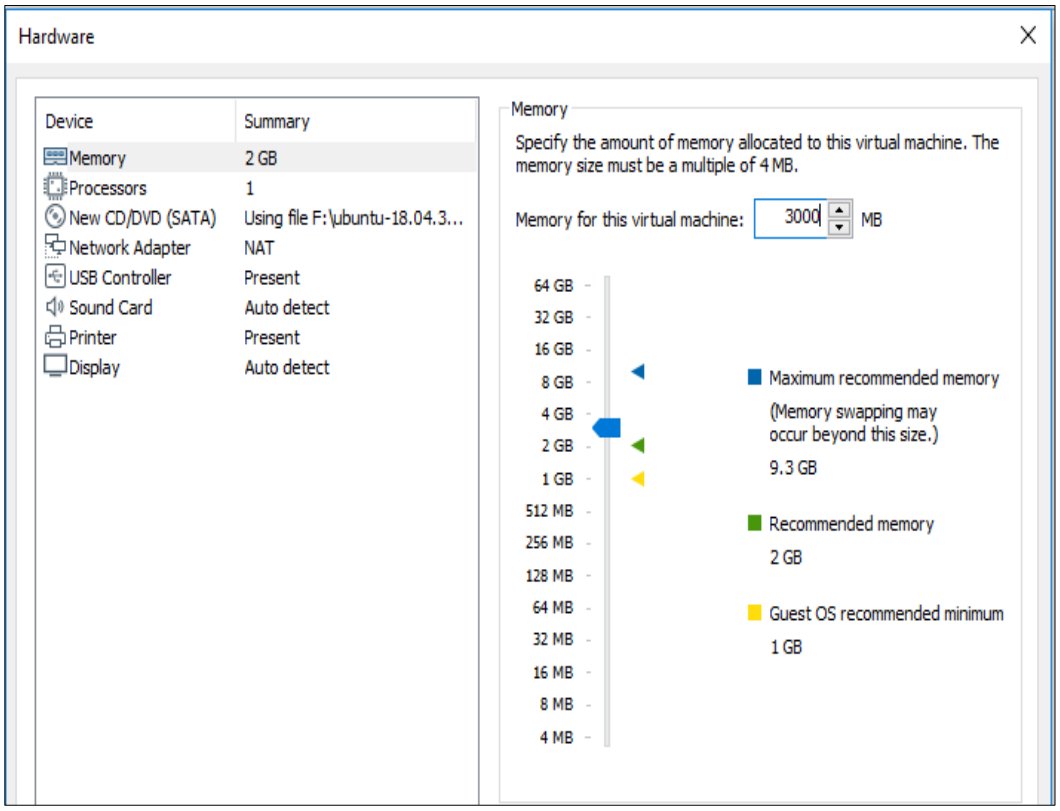

Figura N° 27 Configuración de la máquina virtual.

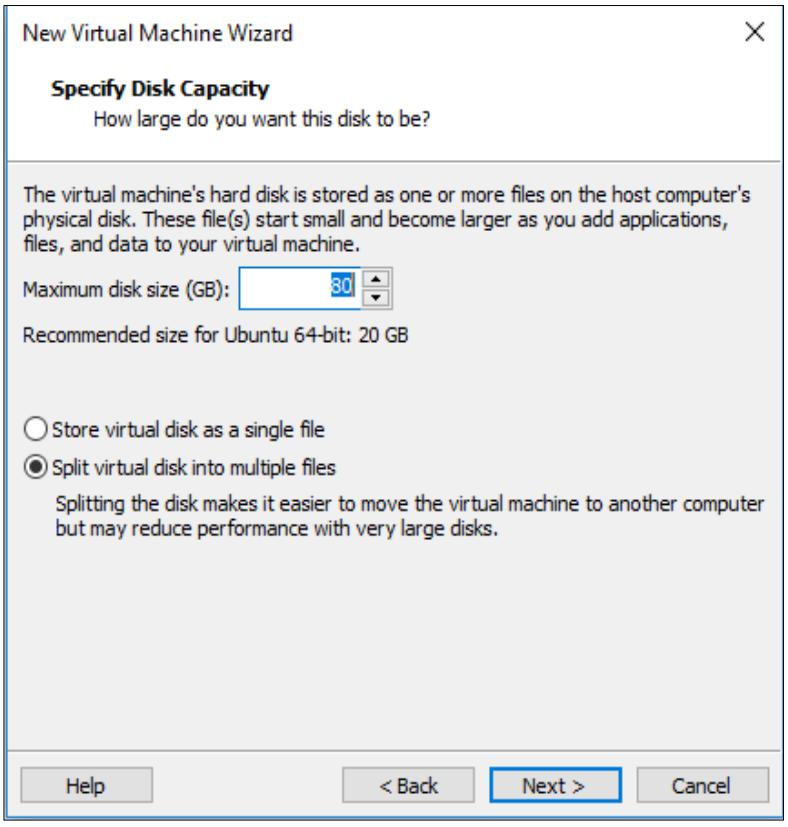

Figura N° 28 Configuración de la máquina virtual.

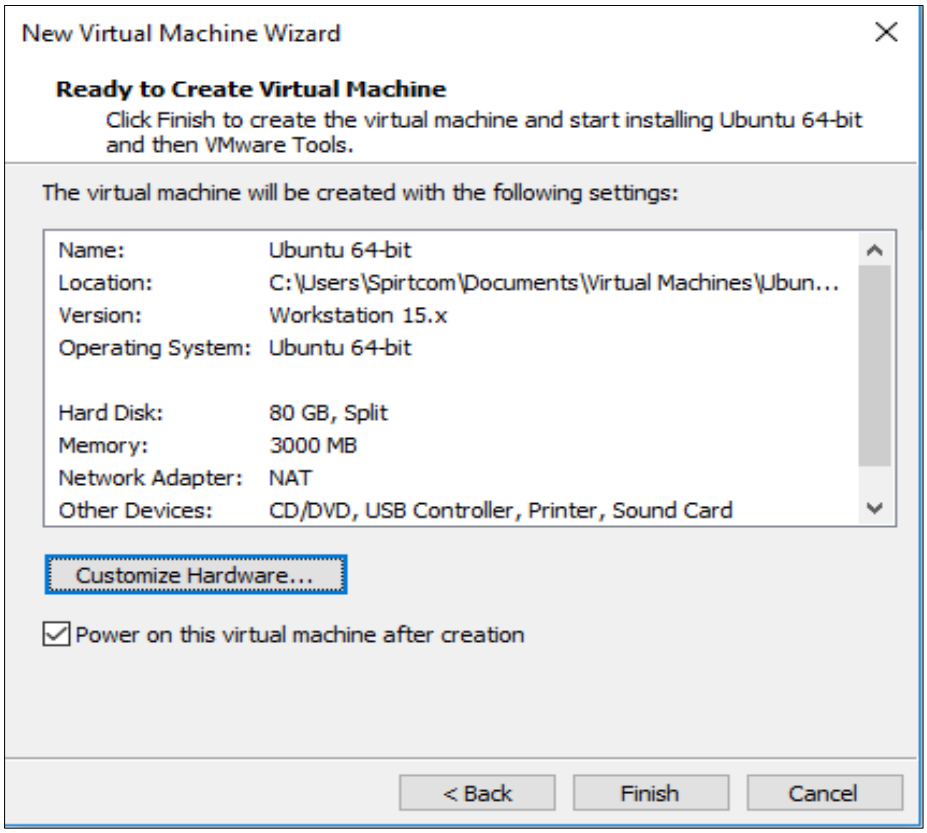

Figura N° 29 Configuración de la máquina virtual.

Una vez ya finalizada la configuración personalizada, la máquina virtual arranca de manera inmediata como se puede observar en la siguiente imagen:

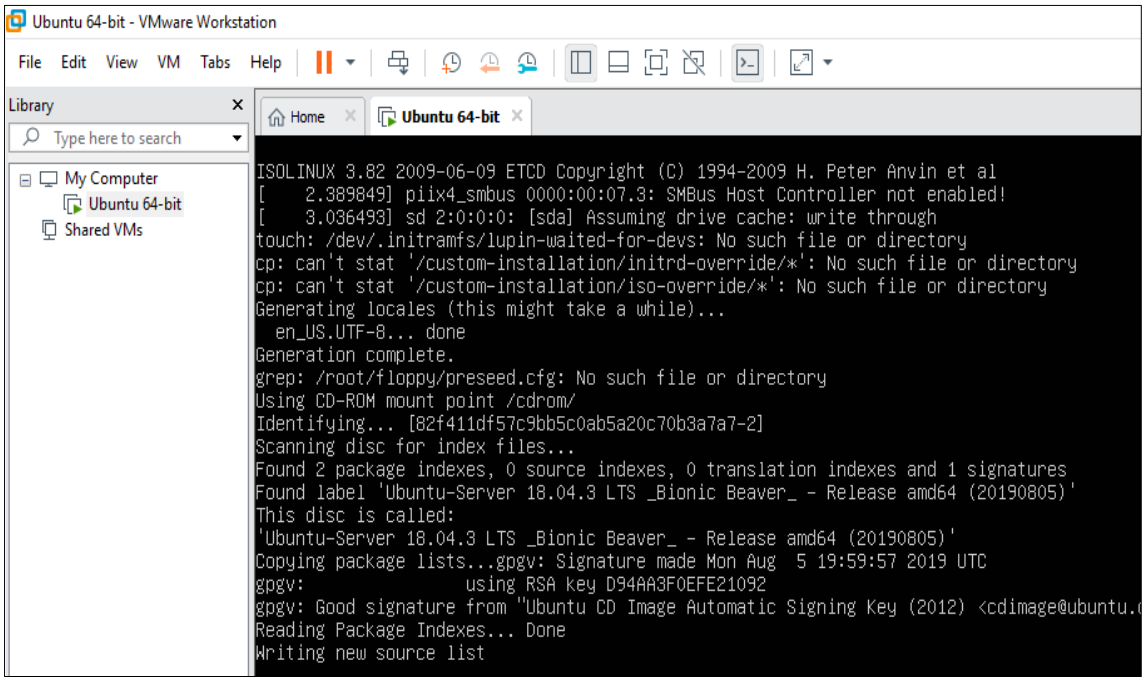

Figura N° 30 Arranque de la máquina virtual.

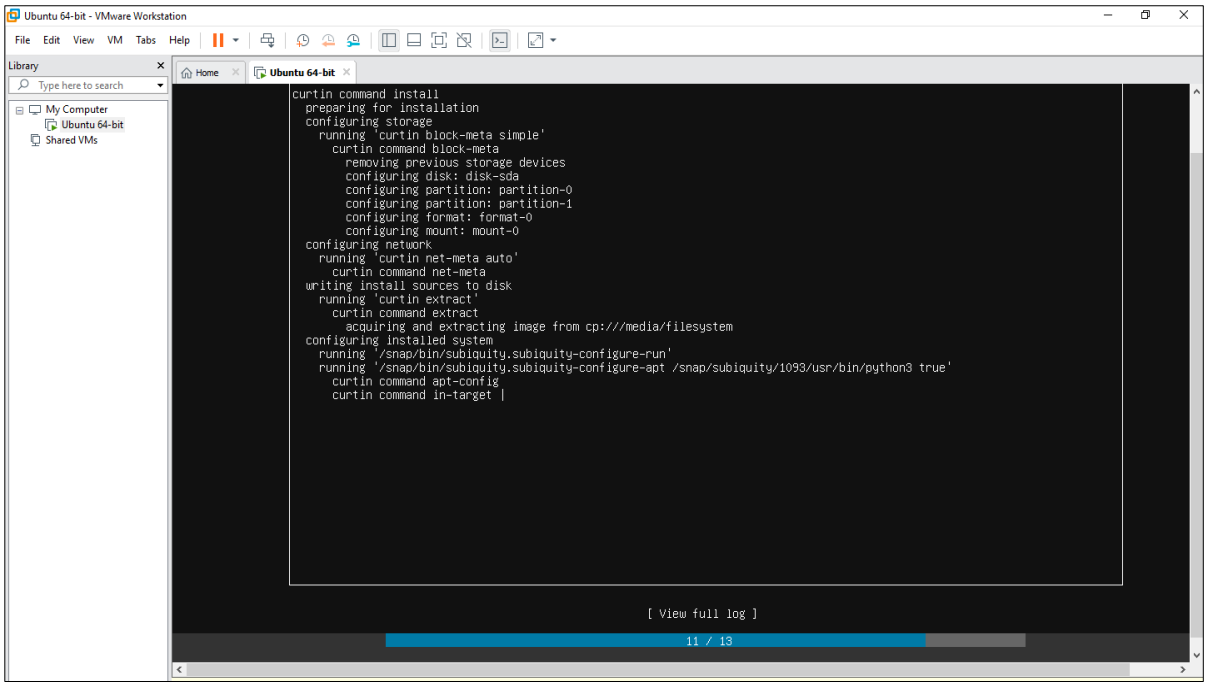

Figura N° 31 Arranque de la máquina virtual.

Anexo 5

Habilitación de ambiente en el Pfsense.

Una vez ya instalada la VMware se realiza la instalación de la ISO correspondiente al PFSENSE a continuación, se mostrará el paso a paso de la instalación:

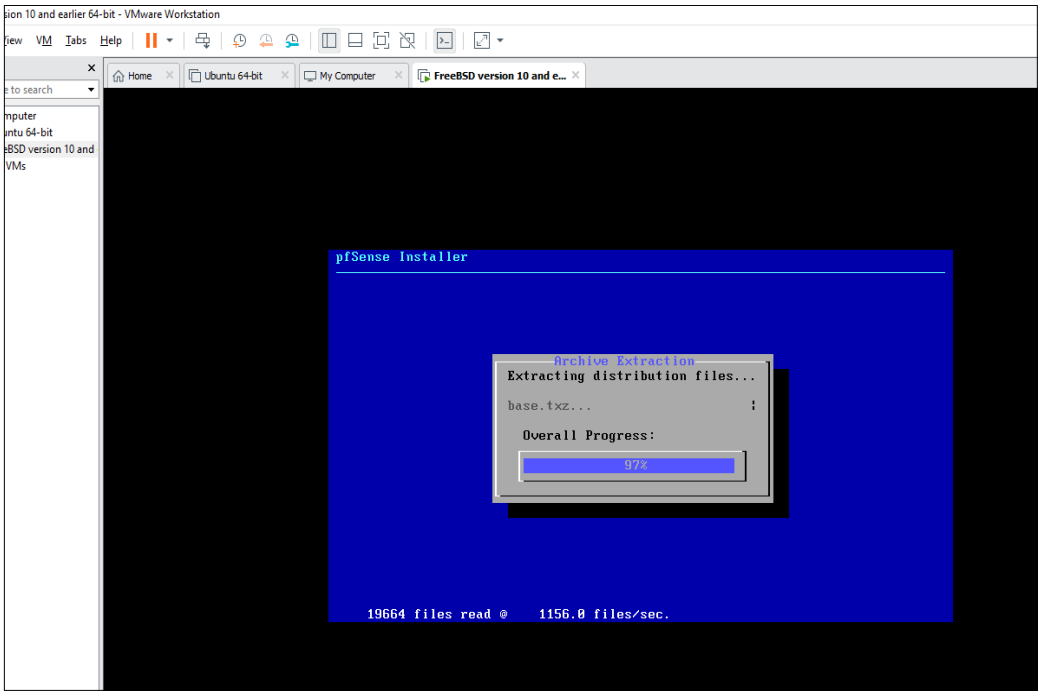

Figura N° 32 Inicialización del Pfsense.

Figura N° 33 Configuración de la ISO correspondiente a Pfsense.

Se puede observar en la siguiente imagen que la ISO del Pfsense quedó habilitada y se encuentra listo para ser ejecutado en la máquina virtual instalada en donde se llevara la administración de las políticas a configurar.

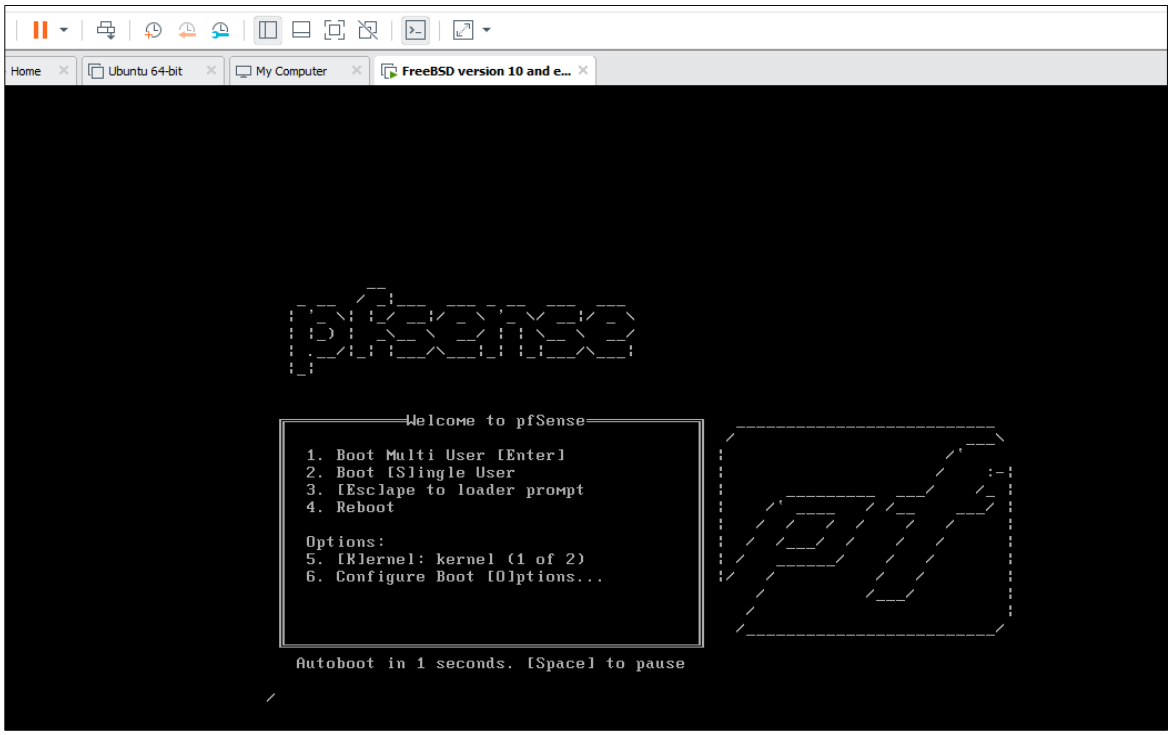

Figura N° 34 Pfsense preparándose para tener el ambiente activo.

En la siguiente imagen podemos observar que el Pfsense se encuentra activo mostrando el siguiente menú de opciones:

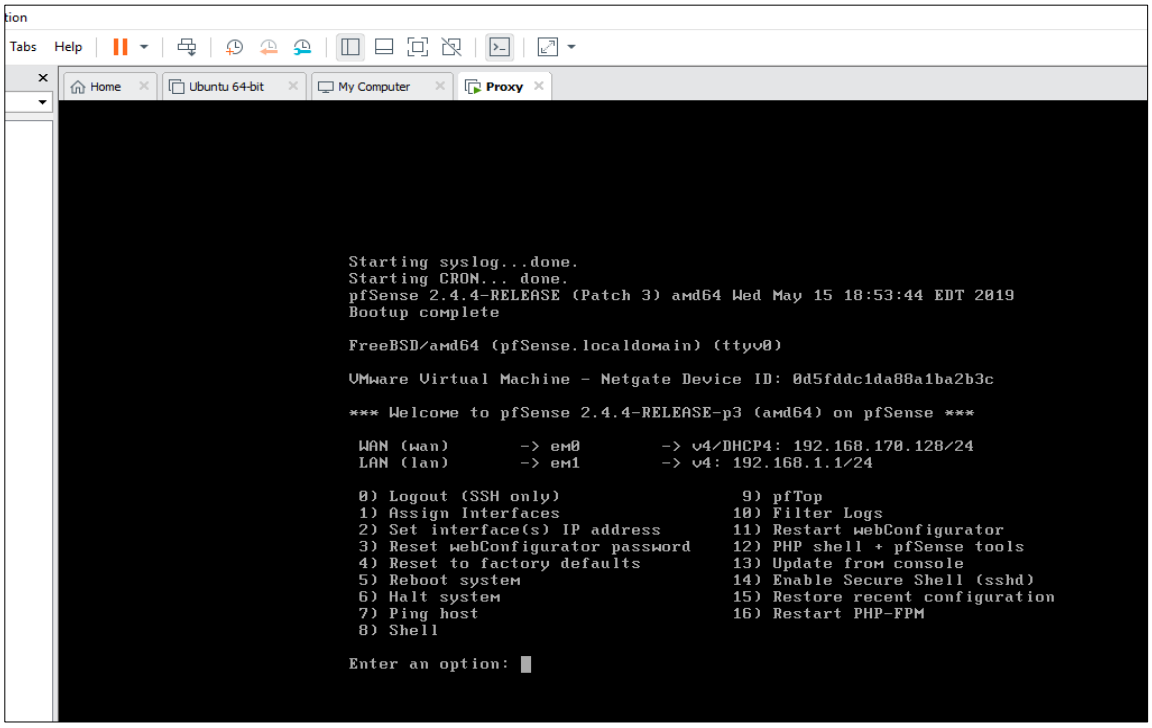

Figura N° 35 Menú de opciones del Pfsense.

1. Logout (SSH only)
2. Assign Interfaces
3. Set interfaces IP address
4. Reset webConfigurator password
5. Reset to factory defaults
6. Reboot System
7. Halt System
8. Ping host
9. Shell
10. PfTop
11. Filter logs
12. Restart webConfigurator
13. PHP shell + pfsense tools
14. Update from console
15. Enable secure shell
16. Restore recent configuration
17. Restart PHP- FPM.

De las cuales solo se harán uso de la opcion 5 y opcion 6 debido a que las configuraciones como tal son aplicadas desde la consola de administracion.

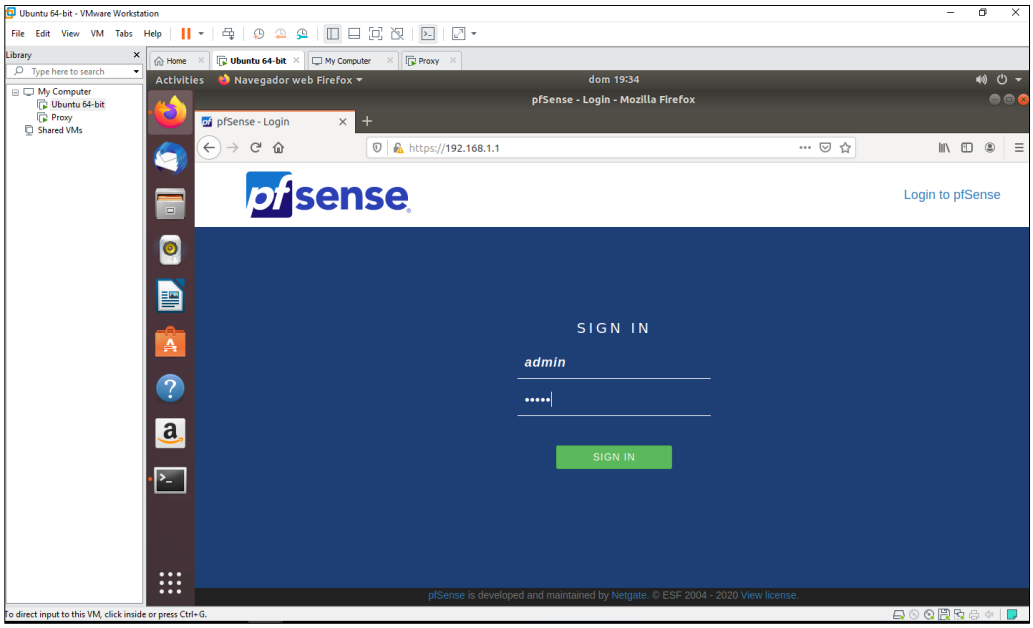

Figura N° 36 Consola de administración del Pfsense.

DECLARACIÓN Y AUTORIZACIÓN

Yo, **MEDIAVILLA SAVINOVICH, VANESSA ISABEL**, con C.C: # **0919390054** autor/a del trabajo de titulación: **Diseño e implementación de una política de seguridad para una PYME. Caso de estudio: Empresa de servicios de Call Center** previo a la obtención del título de **INGENIERO EN SISTEMAS COMPUTACIONALES** en la Universidad Católica de Santiago de Guayaquil.

1.- Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

2.- Autorizo a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de propiedad intelectual vigentes.

Guayaquil, **04** de **marzo** de **2020**

f. _____
Nombre: **Mediavilla Savinovich, Vanessa Isabel**
C.C: **0919390054**

REPOSITORIO NACIONAL EN CIENCIA Y TECNOLOGÍA

FICHA DE REGISTRO DE TESIS/TRABAJO DE TITULACIÓN

TEMA Y SUBTEMA:	**Diseño e implementación de una política de seguridad para una PYME. Caso de estudio: Empresa de servicios de Call Center**		
AUTOR(ES)	**Mediavilla Savinovich, Vanessa Isabel**		
REVISOR(ES)/TUTOR(ES)	**Salazar Tovar, Cesar Adriano**		
INSTITUCIÓN:	Universidad Católica de Santiago de Guayaquil		
FACULTAD:	ingeniería		
CARRERA:	Sistemas Computacionales		
TITULO OBTENIDO:	Ingeniero en sistemas computacionales		
FECHA DE PUBLICACIÓN:	04 de marzo de 2020	**No. DE PÁGINAS:**	62
ÁREAS TEMÁTICAS:	Ciberseguridad, delitos informático, CRP.		
PALABRAS CLAVES/ KEYWORDS:	**Pyme, política de seguridad, máquina virtual, servidor,software**		

RESUMEN/ABSTRACT (150-250 palabras):
El presente trabajo Diseño e implementación de una política de seguridad para una PYME. Caso de estudio: Empresa de servicios de Call Center tiene como objetivo la implementación de una política de seguridad en donde se definió realizar el control sobre los accesos hacia internet que tiene el personal de la pyme; para el levantamiento de información se realizó una entrevista al Gerente de la empresa Spiritcom S.A en donde se definió que parámetros se deben cumplir para lograr el objetivo propuesto. Para ello se procedió con la investigación de herramientas acordes a los requerimientos mencionados en el análisis del proyecto mediante la instalación de una máquina virtual montada en un servidor con el software seleccionado. La implementación realizada cumplió con las necesidades del cliente y se logró mejorar el rendimiento en su equipo de trabajo y cumplió el objetivo propuesto desde el inicio del proyecto con la empresa Spiritcom S.A

ADJUNTO PDF:	☒ SI	☐ NO
CONTACTO CON AUTOR/ES:	**Teléfono:** +5939876535620	E-mail: vanessa.mediavilla@cu.ucsg.edu.ec
CONTACTO CON LA INSTITUCIÓN (C00RDINADOR DEL PROCESO UTE)::	**Nombre: Ing. Edison José Toala Quimí, Mgs.**	
	Teléfono: +593-4-2202763 ext 1025	
	E-mail: edison.toala@cu.ucsg.edu.ec	

SECCIÓN PARA USO DE BIBLIOTECA	
Nº. DE REGISTRO (en base a datos):	
Nº. DE CLASIFICACIÓN:	
DIRECCIÓN URL (tesis en la web):	