

UNIVERSIDAD DE SONORA

División de Ingeniería

Departamento de Ingeniería Industrial

Implementación de plan PCI-DSS

Reporte de Prácticas Profesionales

Presenta

Gustavo Alberto Rodríguez López

INGENIERO EN SISTEMAS DE INFORMACIÓN

Asesor: Dr. Alonso Pérez Soltero

Hermosillo, Sonora.

Enero 2020

ÍNDICE GENERAL

ÍNDICE DE FIGURAS.....	3
1. INTRODUCCIÓN	4
1.1 EXPLICACIÓN DEL PROYECTO.....	5
1.2 OBJETIVOS	6
1.3 METODOLOGÍA.....	6
2. DESCRIPCIÓN DEL CONTEXTO	7
2.1 ENTORNO DONDE SE UBICA LA UNIDAD RECEPTORA	8
2.2 ESTRUCTURA ORGANIZACIONAL DE LA UNIDAD RECEPTORA.....	9
2.3 NORMATIVIDAD DE LA UNIDAD RECEPTORA	10
2.4 EQUIPAMIENTO E INSTALACIONES	11
3. FUNDAMENTO TEÓRICO DE LAS HERRAMIENTAS Y CONOCIMIENTOS APLICADOS.....	13
3.1 PFSENSE	13
3.2 ADMINISTRACIÓN DE SERVIDORES.....	16
3.3 OTRAS HERRAMIENTAS.....	18
4. DESCRIPCIÓN DETALLADA DE LAS ACTIVIDADES REALIZADAS	19
4.1 PRIMERA ETAPA	20
4.2 SEGUNDA ETAPA.....	22
4.3 TERCER ETAPA	26
5. ANÁLISIS DE LA EXPERIENCIA ADQUIRIDA.....	33
5.1 ANÁLISIS GENERAL DEL PROYECTO	33
5.2 ANÁLISIS DE LOS OBJETIVOS DE LAS PRÁCTICAS	34
5.3 ANÁLISIS DE LAS ACTIVIDADES REALIZADAS.....	34
5.4 ANÁLISIS DE LA METODOLOGÍA UTILIZADA.....	35
6. CONCLUSIONES Y RECOMENDACIONES	37
7. REFERENCIAS BIBLIOGRÁFICAS.....	39

ÍNDICE DE FIGURAS

2.1 EDIFICIO DE SZERTEGIA.....	8
2.2 ORGANIGRAMA DE DIRECCIÓN GENERAL.....	9
2.3 HARDWARE DEL SITE DE SZERTEGIA.....	12
2.4 MAPA DEL SITE DE SZERTEGIA.....	13
4.1 PANEL PRINCIPAL DE SERVER MANAGER.....	20
4.2 PANEL DE POLITICAS (GPO).....	21
4.3 PANEL PRINCIPAL DE WSUS.....	22
4.4 START, ENABLE Y STATUS DE SERVIDOR NTP.....	25
4.5 ZKTECO K40.....	26
4.6 VISTA PRINCIPAL DE ATTENDANCE MANAGEMENT PROGRAM.....	27
4.7 INTERFAZ DE EMPLEADOS.....	28
4.8 ADMINISTRACION DE HORARIOS.....	29
4.9 CALCULADORA DE ASISTENCIAS.....	30
5 AREA DE LOCKERS.....	32

1. INTRODUCCIÓN

Con el fin de cumplir con el reglamento de la universidad de sonora y de adquirir los últimos 20 créditos restantes de la carrera de ingeniería en sistemas de información se dio a la tarea de buscar un lugar o institución en el cual se pudiera desempeñar parte de lo aprendido durante la licenciatura y así adquirir nuevos conocimientos en el área laboral. Teniendo una idea de cuál era el área que más se apegaba a las diferentes ramas posibles en la licenciatura cursada, el trabajo de administrador de sistemas que se ofrecía marzo de 2019 se presentó como la mejor opción para realizar las practicas, después de diferentes solicitudes enviadas a diferentes empresas relacionadas con las labores que me llamaban la atención, se eligió desempeñar las prácticas profesionales en la empresa Szertegia.

Szertegia es un callcenter localizado en el boulevard Morelos de Hermosillo, dicha empresa se dedica a lo que es el soporte al cliente de usuarios americanos residentes en dicho país, la empresa tiene diferentes campañas que se dedican a la orientación de personas para obtener casa propia, muchas veces estos clientes no están totalmente enterados de como pueden obtener un crédito inmobiliario y los agentes de Szertegia, son preparados para orientar al cliente y que estos puedan obtener su propio hogar.

Se llevó a cabo durante los meses de mayo, junio y julio, la implementación del plan PCI-DSS, el cual es una normativa que se usan en todos los negocios que quieran hacer uso y manejo de la información de tarjetas de crédito de los clientes, si un negocio no cumple con las normativas de PCI-DSS este negocio no puede llevar acabo transacciones, pagos, depósitos o cualquier movimiento que involucre información de tarjetas de crédito y débito.

El trabajo que se presenta a continuación es una memoria de prácticas en la cual se muestra todo el trabajo realizado durante el periodo de prácticas que fue aproximadamente desde el 20 de mayo al 22 de julio en dicha unidad receptora. Descripción del proyecto, de las activadas realizadas, de la empresa y de como se maneja, así como sistemas y herramientas que se usaron, serán

desglosadas en los siguientes apartados de este documento con el fin de proporcionar una imagen clara de lo que se llevó a cabo durante el periodo de prácticas.

1.1 EXPLICACIÓN DEL PROYECTO

PCI-DSS por sus siglas en inglés (Payment Card Industry Data Security Standard) es un estándar de seguridad que consta de diferentes requerimientos necesarios para poder proteger la información sensible de tarjetas de crédito y débito, es obligatorio para toda aquella empresa que acepten, procesen o tramiten datos de tarjetas de crédito o débito. Las normativas PCI-DSS fueron lanzadas por primera vez en el año 2006 con el fin de gestionar y mejorar la seguridad de los pagos en línea, las grandes marcas de tarjetas de pago (Visa, Mastercard, American Express, Discovery y JCB) establecieron un consejo como órgano autónomo a ellas para crear estas normativas, sin embargo, cabe recalcar que cada empresa que esté dispuesta a manejar la información de titulares de tarjeta de crédito es responsable de la implementación de PCI-DSS en sus propias organizaciones.

Se seleccionó esta unidad receptora principalmente por que el objetivo de esta empresa era la implementación de PCI-DSS, la implementación de dicha normativa conlleva diferentes actividades para poder cumplir con todos los requisitos y esta oportunidad pareció que sería muy buena para aprender nuevas habilidades, dichas actividades incluyen lo que es, configuración de VPN, firewalls, antivirus, limitación de accesos, usuarios únicos, monitoreo de equipos y de sistemas, y la más importante, la protección de datos almacenados de titulares de tarjetas de crédito.

1.2 OBJETIVOS

El objetivo general de este plan fue implementar las normativas de PCI-DSS para poder manejar información confidencial de titulares de tarjetas de crédito, sin embargo, dentro de este mismo plan se tuvieron diferentes objetivos específicos, que también se debieron de cumplir para poder llevar a cabo la implementación exitosa, los principales objetivos específicos se muestran a continuación:

- Ayudar a los clientes actuales con pagos en línea, y procesar su información sensible de tarjetas de crédito o débito en un ambiente seguro.
- Usar la certificación de PCI-DSS como referencia para obtener futuros clientes dentro del callcenter.
- Actualización de la infraestructura de la empresa por medio de los estándares de PCI-DSS

1.3 METODOLOGÍA

La metodología utilizada en este proyecto que se implementó en la empresa constó de tres diferentes fases las cuales fueron divididas en un periodo de diez semanas, a continuación, se explica a detalle de que constaron dichas fases:

La primera fase se trató de la planeación del programa, básicamente fue analizar la empresa en su actual estado con respecto a la normativa PCI para ver que era lo que ya se tenía implementado y que era lo que faltaba por hacer, se crearon documentos iniciales requeridos y políticas de GPO dentro del Server Manager de Windows Server para actualizar normativas

que ya estaban siendo cumplidas y que era necesario implementar alguna configuración adicional para mantenerlas vigentes.

La segunda fase se enfocó a la instalación de software y su configuración, para ello se realizó la configuración de WSUS, Windows Server Update Services, así como la instalación de un servidor NTP dentro del site de Szertegia.

La tercera fase fue enfocada a la instalación y configuración de hardware estructural dentro de Szertegia, se instaló un checador en la entrada para registrar los tiempos de entrada y salida de los agentes, además se hicieron diferentes adiciones de hardware, como tarjeta RAM y discos duros para los actuales servidores que se tienen configurados, así como instalación de lockers en las áreas libres de dispositivos

2. DESCRIPCIÓN DEL CONTEXTO

Localizada a tan solo tres horas de la frontera con Estados Unidos, Szertegia es un callcenter que se dedica a proveer servicios de telemarketing para diferentes negocios por medio de campañas con agentes telefónicos, la empresa cuenta con un sistema de atención a clientes altamente adaptable a cualquier tipo de empresa que cumple con cualquier característica que el cliente necesite ya que los agentes están altamente capacitados para resolver todo tipo de problemas o inconvenientes. La empresa está completamente comprometida a asegurar el éxito en cada detalle, desde la incorporación de las configuraciones necesarias en el sistema para cada campaña hasta la calidad brindada por el personal capacitado.

En Hermosillo Sonora, Szertegia cuenta con dos ubicaciones, la primera ubicada en boulevard Morelos 307, dentro de Plaza Morelos edificio H 201, 202 y en calle de la reforma, colonia Balderrama, las dos ubicaciones en Hermosillo, Sonora.

2.1 ENTORNO DONDE SE UBICA LA UNIDAD RECEPTORA

La unidad receptora está ubicada en Plaza Morelos 307, una plaza relativamente nueva en el boulevard Morelos, a un lado de la zona militar en Hermosillo, la plaza consta de tres torres de oficinas corporativas, seis restaurantes, varios servicios financieros y laboratorios médicos entre otros.

Szertegia Morelos se encuentra ubicada en el edificio H en el segundo piso (figura 2.1). Es la segunda locación de Szertegia, la otra se encuentra en la colonia Balderrama y se encarga de campañas exclusivas en español.



Figura 2.1 Plaza Morelos 307

Para llevar a cabo las actividades que se realizaron día a día en Szertegia, la empresa cuenta con el segundo piso de la torre H en el complejo de negocios de plaza Morelos 307 con un espacio de 146.15 m², cuenta con 5 estacionamientos. El edificio cuenta con aire acondicionado y servicio de fibra óptica para garantizar la mejor conexión a internet. Dentro de las oficinas de Szertegia se cuenta con apartados especiales para los diferentes puestos administrativos que la empresa tiene, área de recursos humanos, área de sistemas, recepción, sala de juntas, cuarto de entrevistas y oficina del director, además se cuenta con baños de hombres y mujeres, lockers para los agentes, una pequeña cocina, y el área donde están los cubículos de los agentes, se tiene un área especial refrigerada las veinticuatro horas del día en donde se encuentra toda la infraestructura de sistemas (servidores, switches, etc.) para su mejor funcionamiento y la seguridad de estos equipos. Se cuenta con un total de sesenta y cinco equipos de cómputo contando los del área administrativa y de agentes para cumplir con las especificaciones, metas y buena calidad de soporte que los clientes esperan de Szertegia.

2.2 ESTRUCTURA ORGANIZACIONAL DE LA UNIDAD RECEPTORA

La empresa Szertegia está organizada en cuatro grandes áreas: Área de IT (Sistemas), Operaciones (Agentes), Ejecutivo de Cuentas y Recursos humanos. A continuación, podemos observar en la figura 2.2, las jerarquías de las diferentes áreas en la empresa:



Figura 2.2 Organigrama de Dirección General.

El encargado de la dirección general de Szertegia Morelos es el licenciado Edgar Dávila Liceaga, se encarga de la coordinación de todos los departamentos para aseguración del buen funcionamiento y comunicación entre ellos, de él dependen las cuatro áreas principales, en las que se encuentra el coordinador de IT, Francisco Nogales que a su vez se encarga de asegurar que todo sistema dentro de la empresa funcione correctamente así como implementar nuevos sistemas para incrementar la productividad de las demás operaciones, cuenta con apoyo de encargados de soporte y programadores. Cristian Jiménez es el gerente de operaciones en piso, se encarga de preparar toda campaña y trabajar día a día con sus supervisores y agentes para cumplir los objetivos y necesidades que el cliente necesita. Por otro lado Mayra Tovar, la ejecutiva de cuentas, se encarga de estar en constante contacto con los clientes, ella es el puente de comunicación con los diferentes representantes y futuros clientes de Szertegia y finalmente esta Liliana Gutiérrez la cual se encarga del área de reclutamiento y contratación de nuevos agentes así como orientarlos con respecto a materia legal y prestaciones, servicios, apoyo moral etc. Apoyada a su vez por el equipo de recursos humanos.

2.3 NORMATIVIDAD DE LA UNIDAD RECEPTORA

En Szertegia se cuentan con diferentes reglas específicas para las diferentes áreas, así como lineamientos y políticas, sobre cómo se llevan acabo los diferentes procesos en la empresa, dichas reglas y lineamientos son definidas por Szertegia y son aplicadas para las dos locaciones.

Los reglamentos que son usados en Szertegia describen, como ya fue mencionado anteriormente, la descripción de los puestos disponibles en la empresa, desde agentes hasta personal administrativo, así como sus principales deberes y roles como parte de la empresa y el propósito del puesto, los requerimientos que el empleado debe de tener para cubrir el puesto y desempeñar el mejor trabajo posible. Dentro de estos reglamentos, en el apartado de descripción de puesto también se especifica el puesto al que se le

reporta, las relaciones que debe de haber con las diferentes áreas de la empresa y los principales retos y obstáculos que deben ser superados.

2.4 EQUIPAMIENTO E INSTALACIONES

La infraestructura de sistemas es la siguientes: se cuenta con 65 computadoras en total de las cuales 15 son Dell vostro, 11 computadoras Inspiron, 37 Dell Optiplex 3060 y 2 Dell Optiplex 2050, 2 impresoras Hp y un cañón Epson para la sala de conferencias.

El site de Szertegia se encuentra en un área especial refrigerada durante las veinticuatro horas, los siete días de la semana para garantizar su buen funcionamiento y prolongar la vida de los componentes. El espacio es pequeño, sin embargo, es lo suficientemente amplio para que tres personas puedan trabajar sin ningún problema, ya sea configurando el funcionamiento de los servidores o instalando nuevos dispositivos en el site.

El site está compuesto de un Servidor Dell PowerEdge r640 cuenta con dos tarjetas RAM de diez y seis gigas, sumando un total de treinta y dos, se cuenta también con dos discos duros de un terabyte, dentro de este servidor Dell se encuentra las maquinas virtuales administradas por el Hyper-V manager de Windows server, también se cuenta con dos patch panels para la administración de los cables ethernet que salen hacia las estaciones y dos switch capa 2 en stack y junto a tres capa tres, debajo de los switches se tiene el sistema de grabación en el cual se conectan las 15 cámaras que graban y transmiten en vivo, este equipo cuenta con un terabyte de almacenamiento.

El site y su conexión a la corriente está protegida por 4 fuentes de poder con batería, en caso de que se vaya la luz, el site puede ser apagado correctamente dentro de los próximos 5 minutos para que las máquinas no sufran algún daño. En la figura 2.3 podemos observar los equipos con los que cuenta el site.

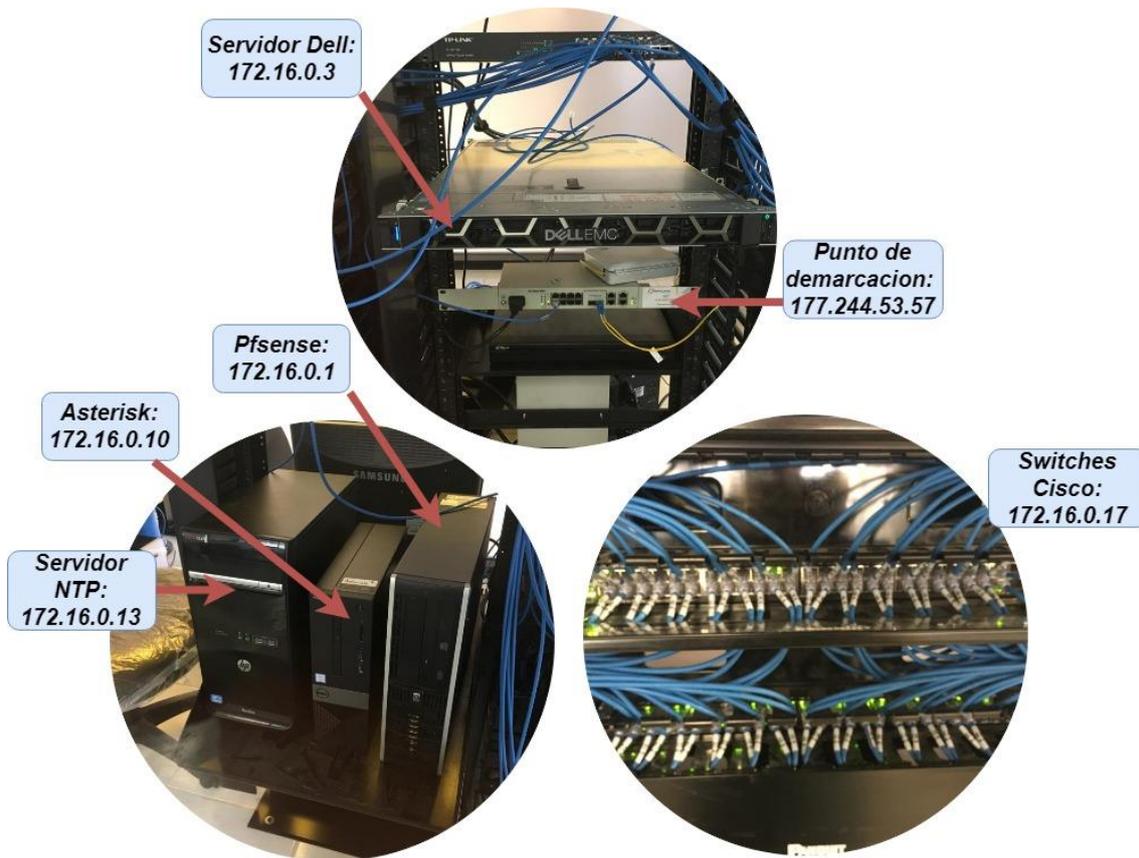


Figura 2.3 Hardware del site de Szertegia.

En cuanto al software que la empresa dispone y utiliza en sus instalaciones, se tiene Microsoft Office Pro, Windows 10 Pro, Zoiper, Google Chrome, Mozilla Firefox, Microsoft Teams y VNC viewer, además de tener instalado PfSense, Vichost y por supuesto Windows Server 2016 en el servidor principal, los servidores web que usan los agentes y supervisores de AFTHA (una de las campañas en inglés), así como QA's son completamente externos, el mantenimiento de estos webserver es proporcionado por el equipo de IT del cliente. Nosotros nos encargamos de la configuración de firewall y configuración de IP externas que tratan de ingresar a nuestra red.

En cuanto a la conectividad, la empresa Szertegia en general cuenta con una Red, cuyo esquema se puede apreciar en la siguiente figura 2.4.

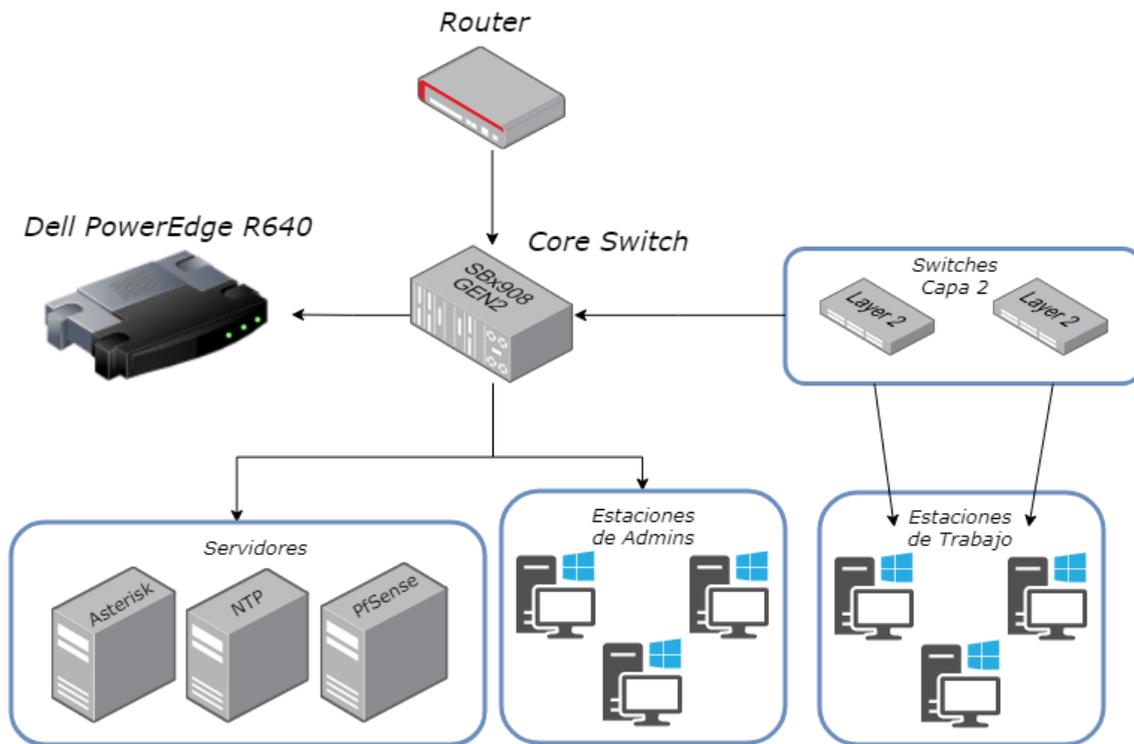


Figura 2.4 Mapa del site de Szertegia.

3. FUNDAMENTO TEÓRICO DE LAS HERRAMIENTAS Y CONOCIMIENTOS APLICADOS

3.1 PfSense

Un firewall es un dispositivo de seguridad de la red que monitorea el tráfico de red -entrante y saliente- y decide si permite o bloquea tráfico específico en función de un conjunto definido de reglas de seguridad.

Los firewalls han constituido una primera línea de defensa en seguridad de la red durante más de 25 años. Establecen una barrera entre las redes internas protegidas y controladas en las que se puede confiar y redes externas que no son de confianza, como Internet. PfSense es una variación de dispositivo UTM suele combinar en forma flexible las funciones de un firewall de inspección activa con prevención de intrusiones y antivirus. Además, puede incluir

servicios adicionales y, a menudo, administración de la nube. Los UTM se centran en la simplicidad y la facilidad de uso¹.

PfSense es un sistema operativo basado en FreeBSD y está diseñado especialmente para montar un firewall que puede ser fácilmente configurable a través de una interface de web y este puede ser instalado en cualquier ordenador además este, contiene una gran lista de addons (paquetes agregables) que permiten su expansión, agregando nuevas funcionalidades sin comprometer la seguridad del sistema, así mismo convirtiéndose en un firewall bastante adaptable a cualquier tipo de red y ecosistema, PfSense es de libre distribución.

El objetivo central de un sistema firewall es proteger a los equipos conectados en una red, servidores, equipos y computadoras personales, contra accesos no deseados o intrusos que pudieran robar datos confidenciales de la empresa o clientes, también con un firewall se puede denegar servicios externos en nuestra red y así disminuir la posibilidad de perder información valiosa a terceros.

Dentro de Szertegia, el firewall que se instaló permite varias tareas y características a destacar las más importantes y que fueron usadas:

- Bloqueo de IP entrantes desconocidas, con esta herramienta se bloqueó automáticamente cualquier dirección IP desconocida antes de que se le diera entrada a la red local, PfSense cuenta con listas de IP seguras las cuales deja entrar automáticamente, las desconocidas tienen que ser verificadas por el personal de IT antes de darles acceso.
- Permitir entrada remota por medio de VPN, con PfSense se puede configurar accesos remotos por medio de la herramienta VPN que trae integrada, de esta forma el equipo de IT puede de una forma segura, conectarse a la red fuera de las oficinas y administrarla en caso de que sea necesario.
- Limitación de ancho de banda, con esta herramienta, se puede limitar la velocidad de carga y de descarga por medio de Aliases a equipos individuales o grupos de computadoras, para evitar degradación en el

¹https://www.cisco.com/c/es_mx/products/security/firewalls/what-is-a-firewall.html. Fecha de consulta: 3 de septiembre de 2019

audio y en la red dentro de las diferentes campañas que Szertegia cuenta actualmente.

- Visualizaciones gráficas de ancho de banda, se puede de una sencilla forma visualizar la entrada y salida de datos de las IP de cualquier computador para identificar picos de alto consumo y la dirección a la cual se están enviando altas cantidades de paquetes o descargando.
- Crecimiento Modular, gracias a la fácil instalación de módulos externos y adicionales, se pudieron instalar diferentes módulos que cubren las necesidades de la empresa conforme se vayan presentando.
- Software Libre, debido a esta característica, se ha podido agregar, instalar y modificar PfSense sin ninguna restricción detrás de algún tipo de pago por parte de la empresa.
- Monitoreo en tiempo real, se ha podido monitorear el ancho de banda, accesos externos y consultas web de nuestros agentes por medio de la interfaz de PfSense.

PfSense es un firewall altamente adaptable a las necesidades de la empresa por lo cual su uso e instalación ha facilitado el manejo de la seguridad en Szertegia, además como es de software libre ha resultado ser una opción bastante económica y gracias a su estabilidad y fama, bastante útil con respecto a funcionamiento y soporte en línea².

La instalación de PfSense es relativamente sencilla para alguien con conocimiento de FreeBSD y no ocupa hardware pesado o costoso. Primero que nada, se necesita tener un ordenador físico, Virtual Box en caso de necesario y el ISO de PfSense que puede ser descargado gratuitamente de la página oficial, en Szertegia, se llevó a cabo la instalación de PfSense en Linux de una forma más sencilla que en Windows ya que solo se necesitó un USB booteable y una conexión a internet por medio de un cable ethernet.

Una vez ya prendido el ordenador con la USB se puede seleccionar las diferentes opciones de PFSense que pueden ser instaladas, se seleccionó la opción USB y con configuraciones por defecto, PfSense tomó su tiempo pero este se instaló en segundo plano, después se seleccionó el kernel que viene

² <https://www.teleinfo.mx/beneficios-de-pfsense/>. Fecha de consulta: 3 de septiembre de 2019

por default y se reinició el ordenador, después se tuvieron que configurar las interfaces de red, donde se le asignó una IP estática por la cual el firewall se identificara, después en un navegador web se accede a la IP que se le asignó y mostrara el portal de acceso de PfSense, donde se deberá introducir el usuario y password por default (admin, PfSense). La instalación es un proceso fácil si se seleccionan las opciones por default, pero cabe resaltar que diferentes empresas pueden tener diferentes necesidades en este caso la forma de instalación puede variar³.

3.2 ADMINISTRACIÓN DE SERVIDORES

En Szertegia el principal servidor que se utilizó es un Dell R640 este potente servidor cuenta con un procesador Intel Xeon de 28 núcleos de procesador dos memorias RAM de 16gb y dos discos duros para almacenamiento de 1TB, el servidor tiene instalado Windows Server 2016, y se le dan varios usos a este servidor:

Contenedores, Windows Server 2016 cuenta con Hyper-V, un hipervisor que permite crear máquinas virtuales dentro de Windows Server, en el manager de Hyper-V se pueden, crear, montar, eliminar máquinas virtuales es un manejador muy completo y en el se tiene montado el sistema de tickets al cual llegan todas las solicitudes de los diferentes departamentos de administración con respecto a problemas técnicos de IT o de software, así como el área de operaciones, también se cuenta con una máquina virtual en la que está montado un ERP, el cual es manejado por el área de recursos humanos para la captura de nóminas y documentos de los empleados en Szertegia, también se tiene una maquina virtual montada para el servicio de LibreNMS el cual es un escáner de vulnerabilidades para sistemas operativos y red locales.

Microsoft Server también cuenta con Group Policy Management, el cual es bastante útil para nosotros, ya que en él se puede asignar reglas a computadoras o usuarios individuales, GPM cuenta diferentes políticas aplicadas por campaña basándose en las necesidades de cada uno, por

³<https://aula128.wordpress.com/2014/09/19/instalacion-y-configuracion-de-pfsense/>. Fecha de consulta: 4 de septiembre de 2019

ejemplo; se puede bloquear el acceso de los agentes a páginas no deseadas o que no son primordiales para su desempeño en operaciones como lo son redes sociales, también se tiene una política de instalación de software por medio del servidor en el cual dependiendo de la campaña se instala el software necesario para esa campaña como por ejemplo Google Chrome, Zoiper o Mozilla Firefox, también hay políticas que pueden ser aplicadas a usuarios en específico, por ejemplo supervisores y agentes de calidad se les tiene activada una política en la cual se abre automáticamente las páginas que necesitan al abrir algún navegador, etc. GPO Manager es una herramienta muy útil para regular accesos a los agentes de operaciones y bastante útil ya que nos ahorra el tiempo de configuración manual de políticas.

Dentro del Manejador de Servidor de Windows se cuenta con WSUS (Windows Server Update Services) el cual se encarga de proporcionar actualizaciones a las computadoras que están conectadas a la red, por medio de WSUS se puede administrar solamente las actualizaciones deseadas y o que realmente sean necesarias dentro del área de operaciones, así se ahorra ancho de banda y tiempo descargando solamente las actualizaciones que se necesitan por campaña, también es muy útil ya que si existe alguna actualización con demasiados bugs o problemas que puedan poner en peligro el funcionamiento de algún ordenador o incluso datos de la empresa, esta puede ser bloqueada, ya que las actualizaciones se descargan solo en el servidor pero no son instaladas hasta que manualmente se le da la opción de hacerlo.

Finalmente, una de las funciones más básicas que se usó en Windows Server es la creación de directorios y usuarios, cada agente se le asigna un log in de Windows, así como a cada computadora se le asignan un nombre único que la identifica en la red, todo esto para mantener los datos ordenados y las computadoras bien localizadas, todo conforme a las reglas de seguridad de PCI.

3.3 OTRAS HERRAMIENTAS

Dentro de las diferentes herramientas que en Szertegia se usan además de las ya mencionadas, se tiene una muy importante, sin costo adicional ya que se usa la versión gratis, esta herramienta es Zoiper. Este software multiplataforma llamado softphone permite al usuario conectarse a internet a través del protocolo SIP (*Session Initiation Protocol*), y permite hacer llamadas por medio de internet desde un equipo de cómputo a cualquier parte, posee una interfaz gráfica fácil de usar y familiarizarse, aunque los agentes solamente manejan la ventana principal de este software, contiene varias opciones de configuración ⁴. En Szertegia, también se usa el paquete de Office, este software ya es bastante conocido y ha sido usado por incontables empresas a lo largo de los años, su instalación benefició a los supervisores y agentes de calidad en la creación de hojas de cálculo de Excel, Documentos de Word y PowerPoint para presentaciones y para crear el material de entrenamiento que los agentes usaran para aprender las distintas tareas que llevaran a cabo⁵. Dentro de Szertegia también se implementó el software VNC Viewer, con este software se puede controlar las tres diferentes pantallas de televisión que se tienen instaladas en el área de operaciones, una pantalla por supervisor, y una pantalla para cada campaña, este software, se conecta al VNC Server que viene instalado por defecto en los Raspberry Pi conectados a las pantallas y por medio de estos dispositivos es posible mostrar información en las pantallas, desde presentaciones de entrenamiento, hojas de Excel, tablas de rankings o incluso videos que los supervisores usan para alentar o informar a los agentes⁶.

⁴ <https://www.telefacil.com/wiki/index.php/Zoiper> Fecha de consulta: 3 de septiembre de 2019

⁵ <https://products.office.com/es-mx/home> Fecha de consulta: 4 de septiembre de 2019

⁶ <https://www.realvnc.com/es/> Fecha de consulta 4 de septiembre del 2019

4. DESCRIPCIÓN DETALLADA DE LAS ACTIVIDADES REALIZADAS

Las actividades se realizaron en el periodo comprendido entre junio y agosto de 2019, de lunes a sábado en un horario de 9 a 17 horas. En general la dinámica de trabajo fue la siguiente:

A partir de las instrucciones emitidas por el coordinador del área de sistema, parte de las actividades se desarrollaron en la oficina, equipada con computadora y acceso a internet, que se disponía para ello; también otra parte del tiempo se atendían requerimientos de todos los agentes de Szertegia así como tareas dentro del área restringida del site, e incluso de los agentes y administradores de la sucursal Balderrama de Szertegia, a los que se atendía vía telefónica y en algunos de los casos directamente en sus áreas de trabajo.

Las actividades se desarrollaron de manera individual o en conjunto con el coordinador de sistemas o con otro practicante. Cuando se presentaba algún problema con el sistema que no se podía resolver internamente se solicitaba ayuda vía telefónica de soporte técnico a los diferentes clientes de las campañas alojadas en Szertegia también incluso con Metro Carrier y con la comisión Federal de electricidad en caso de bajones de electricidad. En todos los casos se realizaban las actividades bajo las instrucciones o supervisión del coordinador de sistemas y se creaban reportes de incidencia los cuales eran mandados a los supervisores, gerentes y COO de Szertegia, en ciertas ocasiones también a los clientes de las campañas.

Las actividades concretas que se desarrollaron se enlistan a continuación para cada una de las tres etapas del periodo de realización de las prácticas profesionales.

4.1 PRIMERA ETAPA

Creación de Políticas

Windows server cuenta con una interfaz llamada Server Manager, en esta interfaz se puede hacer un manejo total del servidor y además se puede acceder a las herramientas principales de una forma práctica, fácil y rápida, como se puede observar en la figura 4.1 se tienen todas las opciones disponibles, desde los roles que cubre cada sección que se tiene instalado al momento.

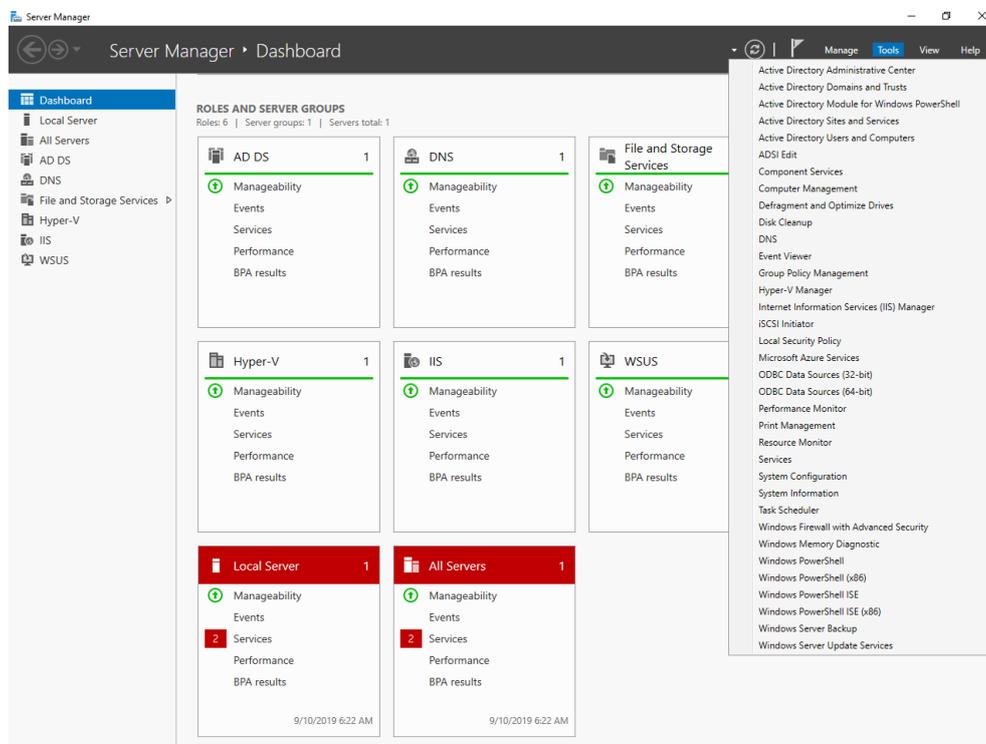


Figura 4.1 Panel principal de Server Manager

En la pestaña de Herramientas (Tools) se puede apreciar los diferentes módulos instalados que se utilizaron para administrar el servidor, para la creación de políticas se debe seleccionar Group Policy Management, en este apartado se muestra todo el directorio activo con las diferentes carpetas y subcarpetas y es aquí donde individualmente se crean las políticas para ser aplicadas, como se puede observar en la figura 4.2 existen políticas aplicadas hasta arriba. Estas políticas se aplican en forma de cascada, por ejemplo la política “GR_wsus_computers” se aplica a todo el servidor “Szertegia.dc” sin

embargo la política “GR_lynx3” se aplica solamente a los usuarios y computadoras que estén dentro de la carpeta “MLS 3” y así sucesivamente, estas políticas se aplican en orden jerárquico, para la creación de políticas se debe seleccionar la carpeta o subcarpeta a la cual se quiere que se agregue dicha política, clic derecho y se selecciona en “crear política en este dominio” así la política será creada y asociada a la carpeta seleccionada, sin embargo, cabe destacar que todas las políticas se crean en la carpeta “Group Policy Objects” por default y estas son solamente asociadas a las carpetas y sub carpetas de elección, de tal modo que si estas son por ejemplo, la política “GR_lynx3” es eliminada de la carpeta “MLS 3” es solamente desasociada y no eliminada por completo del servidor por motivos de seguridad, en la figura 4.2 se puede ver a detalle el panel de políticas.

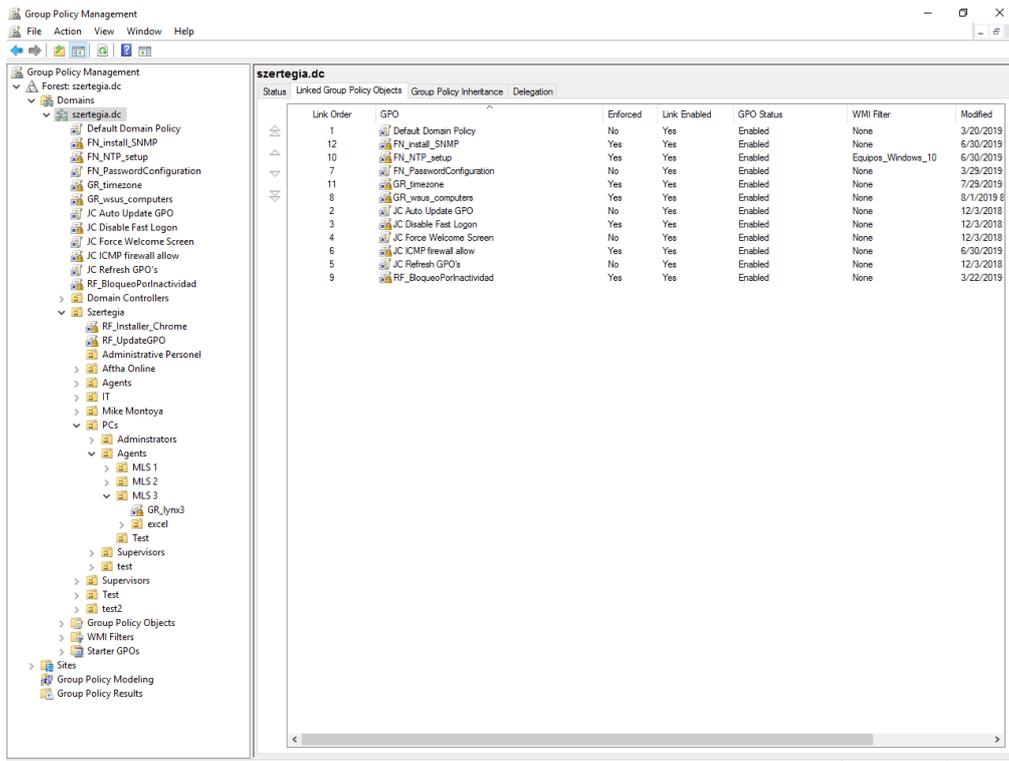


Figura 4.2 Panel de Políticas (GPM)

4.2 SEGUNDA ETAPA

Instalación de WSUS

Como se explicó en el segmento anterior, se llevó a cabo la instalación de las actualizaciones nuevas mediante el uso de WSUS, (Windows Server Update Services), esta herramienta la cual no viene instalada por default en Windows Server 2016 puede ser agregada directamente desde la opción agregar características de Windows en el panel de control. Una vez seleccionada la casilla de WSUS, el servidor debió ser reiniciado y al encender la computadora WSUS quedó instalado. Después de esto se tuvo que configurar, para ello WSUS cuenta con un intuitivo *wizard* set-up para su configuración, en esta configuración rápida se establecieron las horas de actualización y que tipo de actualizaciones se descargarían, es recomendable solo descargar las actualizaciones necesarias para la versión de computadoras que se encuentran en el área de operación, así se ocupa menos espacio en el disco duro y menor tiempo de sincronización para búsqueda de nuevas actualizaciones, una vez terminada la configuración de Windows Update, se presentó una pantalla como la que se muestra en la figura 4.3:

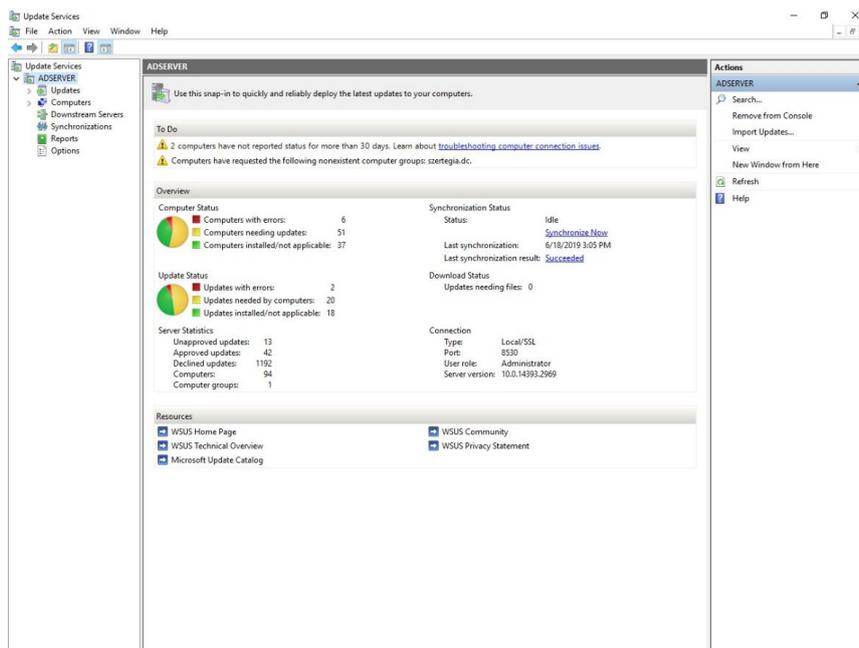


Figura 4.3 Panel principal de WSUS

En el menú de la izquierda se pueden observar las diferentes opciones con las que cuenta la interfaz de WSUS. Actualizaciones es donde se muestra en estatus actual de las actualizaciones, tiene tres apartados, actualizaciones con errores, actualizaciones necesarias, actualizaciones instaladas y sin estatus. En la siguiente opción Computadoras, se observar el grupo de computadoras agregadas a la red y se puede consultar el estado de cada una de las computadoras, es aquí en esta opción donde se fueron agregando las computadoras a WSUS, se agregaron automáticamente si estas están dentro del dominio. La opción siguiente "Servidores de Descarga", tiene como función visualizar en qué lugar se descargan las actualizaciones de Windows, sin embargo, la opción por default es Windows Update Server, después se tiene sincronizaciones, en el cual muestra un estado de las diferentes consultas de búsqueda de nuevas actualizaciones, Reportes es la siguiente opción, aquí se generan reportes detallados de instalaciones y errores de las actualizaciones y finalmente la última sección, Opciones, aquí se muestran diferentes herramientas como actualización de la ruta de descarga y servidores proxy, productos y clasificaciones, donde se selecciona las versiones de actualizaciones que se descargaran, lenguajes, horas de sincronización con el servidor de Windows update, computadoras de la red, y un limpiador inteligente de archivos temporales o archivos basura, para mantener limpio el software. Una vez configurado WSUS lo único que se necesitó hacer es que las computadoras que requieran una actualización hicieran una solicitud de actualización por medio de Windows update y estas se actualizaron dependiendo de la versión de las actualizaciones disponible.

Instalación de Servidor NTP

NTP (protocolo de tiempo de red por sus siglas en inglés, es uno de los protocolos más antiguos y que aún siguen siendo utilizados en internet, fue creado en 1985 y está diseñado para sincronizar los relojes de los ordenadores y redes a través de una red de área local (LAN), su versión más actual (versión 4) consiste de un programa de software que se ejecuta en segundo plano ya sea en Windows o UNIX, un protocolo que intercambia valores de tiempo entre servidores y clientes, y finalmente un conjunto de algoritmos que procesan los valores de tiempo de avance o retroceso del reloj del sistema. NTP funciona dentro del conjunto de protocolos TCP/IP y UDP, la sincronización con NTP es relativamente simple, se usa una fuente de reloj fiable como un GPS o una red de transmisión de radio especialista para recibir la hora UTC de estos relojes.

Existen diferentes formas de uso del servidor NTP así como su instalación, para la instalación que se hizo en el site de Szertegia se requirió un equipo de no muy alto poder de procesamiento, se usó un HP compact 8000 series con Intel core dúo con CentOS 7 instalado, y haciendo boot directamente desde una imagen en una usb, una vez en la consola de comandos de CentOS se usaron los comandos `systemctl stop chronyd.service` seguido de `system disable chronyd.service` el primero para detenerlo ya que lo corre por default y el segundo para deshabilitarlo por completo y evitar que se corra la instancia en algún reinicio, este servicio `chronyd.service` viene por default en CentOS y nos ayuda a configurar automáticamente NTP, ya que se hizo manualmente, se detuvo el servicio en su totalidad, después con los comandos `rafex# yum install ntp` se solicitó a Linux que descargue e instale los paquetes necesarios para correr ntp, ahora, una de las páginas más actualizadas con respecto a servidores NTP es <http://www.pool.ntp.org/zone/mx> la cual contiene una lista de servidores horarios fáciles de usar y configurar. Al archivo ubicado en `/etc/ntp.conf` se le agregaron las siguientes líneas de código `server 0.north-america.pool.ntp.org`, `server 0.north-america.pool.ntp.org`, `server 1.north-america.pool.ntp.org`, `server 2.north-america.pool.ntp.org`, `server 3.north-america.pool.ntp.org` además de `restrict AQUÍ_LA_IP mask 255.255.255.0 nomodify notrap` esta última para configurar el pool como servidor. Finalmente se modificó el firewall de CentOS para permitir peticiones `rafex# firewall-cmd –`

add-service=ntp –permanent” seguido de “rafex# firewall-cmd –reload”, después el servicio fue iniciado y se habilitó con los últimos comandos “systemctl start ntpd”, “systemctl enable ntpd”, “systemctl status ntpd”, el primero activa el servicio, el segundo lo habilita y el tercero regresó la información sobre el status.

```
root@localhost ~# systemctl start ntpd
root@localhost ~# systemctl enable ntpd
ln -s '/usr/lib/systemd/system/ntp.service' '/etc/systemd/system/multi-user.target.wants/ntp.service'
root@localhost ~# systemctl status ntpd
ntp.service - Network Time Service
   Loaded: loaded (/usr/lib/systemd/system/ntp.service; enabled)
   Active: active (running) since Sun 2014-09-14 16:28:41 EEST; 12s ago
     Main PID: 19471 (ntpd)
    CGroup: /system.slice/ntp.service
            └─19471 /usr/sbin/ntpd -u ntp:ntp -g

Sep 14 16:28:41 pxe-server.centos.lan ntpd[19471]: proto: precision = 0.045 usec
Sep 14 16:28:41 pxe-server.centos.lan ntpd[19471]: 0.0.0.0 c01d 0d kern kernel time sync enabled
Sep 14 16:28:41 pxe-server.centos.lan ntpd[19471]: ntp_io: estimated max descriptors: 1024, initial socket boundary: 16
Sep 14 16:28:41 pxe-server.centos.lan ntpd[19471]: Listen and drop on 0 *wildcard 0.0.0.0 UDP 123
Sep 14 16:28:41 pxe-server.centos.lan ntpd[19471]: Listen and drop on 1 *wildcard :: UDP 123
Sep 14 16:28:41 pxe-server.centos.lan ntpd[19471]: Listen normally on 2 lo 127.0.0.1 UDP 123
Sep 14 16:28:41 pxe-server.centos.lan ntpd[19471]: Listen normally on 3 eno16777736 192.168.1.25 UDP 123
Sep 14 16:28:41 pxe-server.centos.lan ntpd[19471]: Listen normally on 4 lo ::1 UDP 123
Sep 14 16:28:41 pxe-server.centos.lan ntpd[19471]: Listening on routing socket on fd #21 for interface updates
Sep 14 16:28:41 pxe-server.centos.lan systemd[1]: Started Network Time Service.
Sep 14 16:28:41 pxe-server.centos.lan ntpd[19471]: 0.0.0.0 c016 06 restart
Sep 14 16:28:41 pxe-server.centos.lan ntpd[19471]: 0.0.0.0 c012 02 freq_set kernel 0.000 PPM
Sep 14 16:28:41 pxe-server.centos.lan ntpd[19471]: 0.0.0.0 c011 01 freq_not_set
Sep 14 16:28:42 pxe-server.centos.lan ntpd[19471]: 0.0.0.0 c014 04 freq_mode
root@localhost ~#
```

Figura 4.4 Start, Enable y Status de servidor NTP

Finalmente, centOS arrojar una imagen parecida a la figura 4.4, en la que se observa cómo se ejecutan los últimos comandos ya mencionados en el párrafo anterior y sus efectos y resultados en la consola.

4.3 TERCERA ETAPA

Instalación de Checador

En cumplimiento con los estándares de PCI se dio a la tarea de la instalación de un checador en la entrada del establecimiento, ya que Szertegia, no contaba con uno, el checador utilizado es de la marca ZKTeco y es el modelo K40 este modelo tiene varias características que cubre las necesidades en el callcenter, tiene un puerto TCP y usb, una batería de respaldo en caso de que se vaya la luz o que sea desconectada la corriente, una pequeña pantalla LCD de 2.8 y puede generar reportes en Excel con ayuda del software que lo acompaña, también cuenta con control de acceso al edificio por medio de huella digital en la figura 4.5 se muestra el checador instalado.



Figura 4.5 ZKTeco K40

Para la configuración del checador fue necesario usar el programa de acompañamiento llamado Attendance Management Program, en este programa se puede manejar por completo las configuraciones del checador y es aquí en este programa donde se da de alta a nuevos usuarios y nuevos horarios de trabajo. Primero que nada, se configuró el checador con el programa, para ello, se tuvo que seleccionar el icono “dispositivo” y luego en el apartado de

“agregar nuevos dispositivo”, la configuración es bastante simple, solo se le asigno la dirección IP estática que usa y listo, una vez agregado el dispositivo se seleccionó y al darle clic al botón verde “Conectar”. en la parte inferior derecha está el estatus desconexiones, una vez que se muestre el mensaje de “conexión exitosa” se puede manejar el dispositivo en su totalidad, en la parte de la izquierda se muestran diferentes menús y opciones-, debido a que la computadora de recepción (que es la que se encarga de administrar el dispositivo) no siempre esta preñida, todo registro de entrada y de salida de los usuarios se guarda directamente en el checador, una vez nuevamente cuando la computadora es encendida y se conecta de nuevo al checador, se debe seleccionar la opción “Descargar logs de asistencia” para que la información sea guardada en la computadora, también se puede usar la opción “Descargar información e usuarios” en caso de que se hayan agregado usuarios manualmente desde el dispositivo. En la siguiente figura 4.6 se observa la vista principal de dicho software:

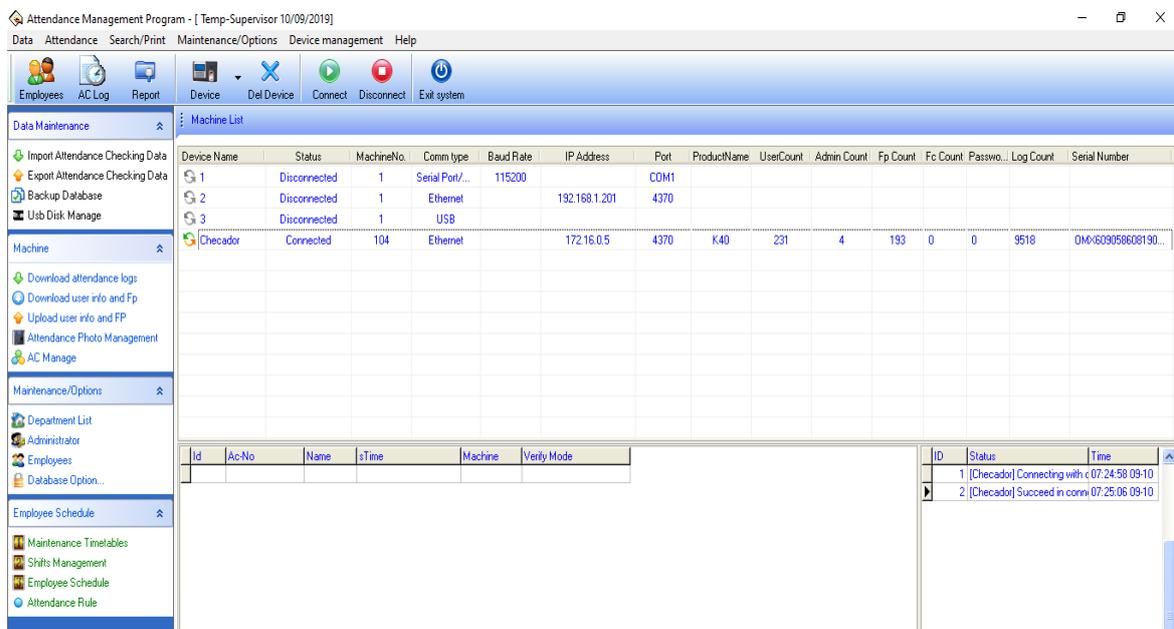


Figura 4.6 Vista Principal de Attendance Management Program

En la parte de la izquierda en la figura 4.6 se puede observar el botón “empleados” al seleccionar esta opción se abre la pantalla de administración de usuarios, como se puede observar en la figura 4.7, es aquí en este apartado donde se realizaron todo tipo de operaciones con respecto a los usuarios que se registraron.

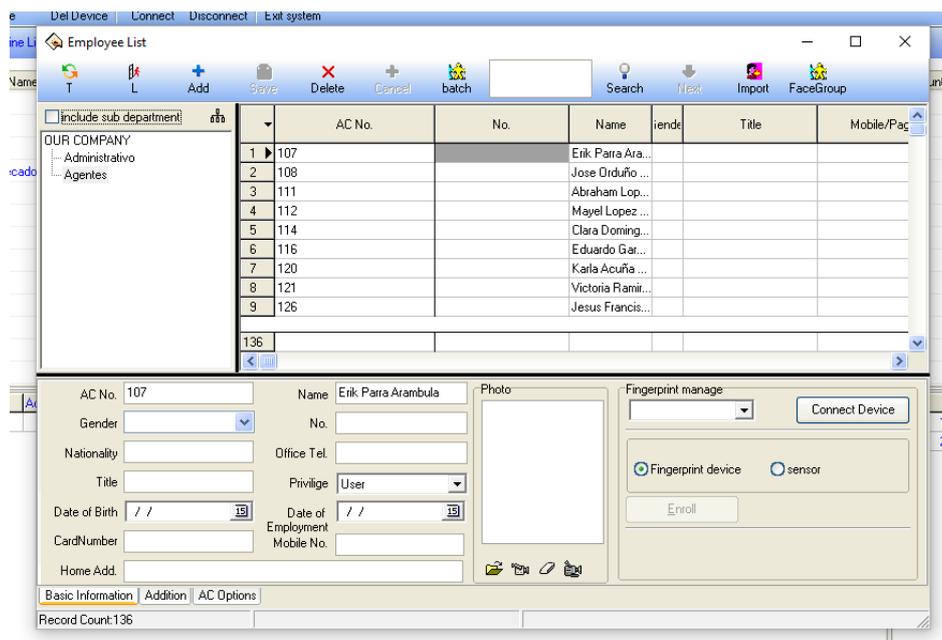


Figura 4.7 Interfaz de empleados

En esta vista el procedimiento que se siguió para la creación usuarios fue sencillo, se selecciono la opción agregar que la distingue una cruz azul, después se agregaron los valores necesarios que se requerían para que el dispositivo los almacenara, en este caso el usuario “Erik Parra Arambula” tiene el AC No. (account number) 107, y tiene la denominación en la parte “privilegios” de usuario ya que es un agente de la campaña AFTHA que se aloja actualmente en el site, debido a que es un agente y solo se requirió sus entradas y salidas asociadas a su nombre, es la única información que se ingresó de el en el dispositivo, además de su huella digital, en el área “manejo de huella digital” se eligió el checador y se selecciono la opción “conectar dispositivo” una vez conectado se pudo registrar la huella digital del dedo índice derecho, al terminar de capturar los datos se seleccionó la opción “guardar” y el agente quedo registrado en el programa.

En Szertegia se tienen dos turnos, de la mañana y de la tarde, estos turnos van de las 6:00 a 2:00 y el turno de la tarde que es 12:00 a 7:00, estos turnos se asignaron a cada agente individualmente en el apartado de “horario de empleados” como se muestra en la figura 4.6, para ello se seleccionó al usuario que se le tenía que modificar o asignar nuevo horario y al presionar la opción “modificar horarios” en la parte superior derecha, se abrió una ventana donde se selecciono el horario adecuado para el agente y el rango de fecha por el que será empleado y listo, el nuevo horario quedo asociado a dicho agente, una vez que todos los agentes fueron agregados, se aseguró que el dispositivo estuviera conectado y se eligió la opción en el panel de la izquierda (que se muestra en la figura 4.8) que dice “subir información de usuarios” y se sincronizo con el checador, una vez que terminó la operación los nuevos cambios se aplicaron en el dispositivo.

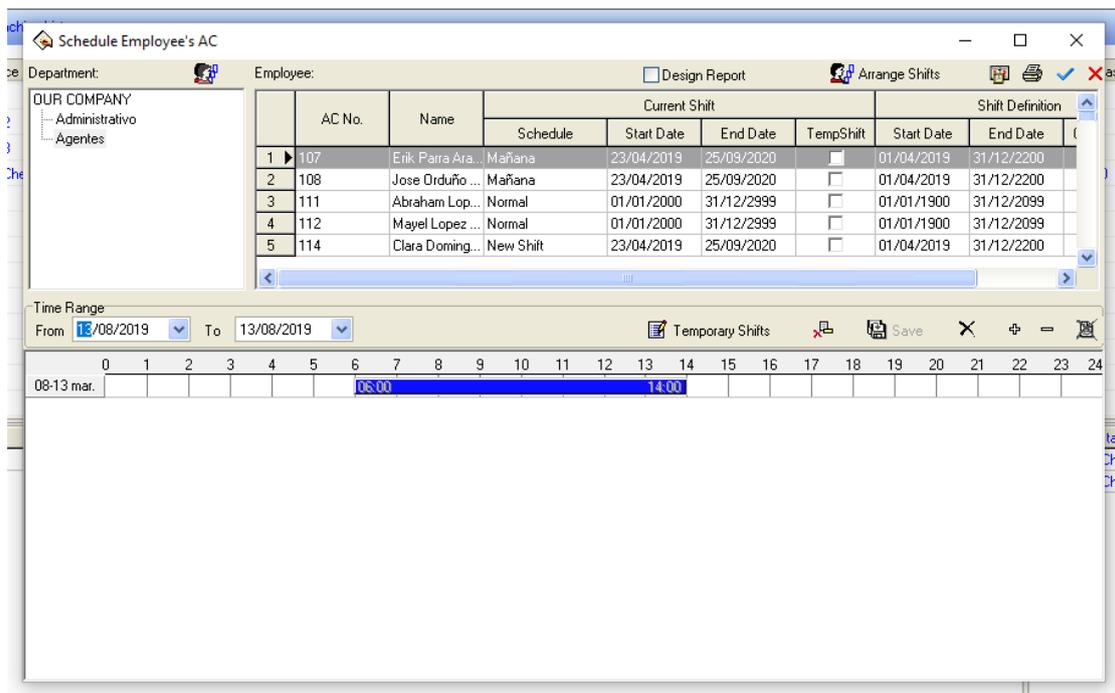


Figura 4.8 Administración de horarios

Una vez que los usuarios fueron registrados y los horarios agregados se esperó una semana para hacer la prueba del checador, durante una semana los agentes fueron registrando sus entradas y salidas con el lector de huellas digitales en el dispositivo, el día viernes cuando se hizo la recopilación de datos primero se seleccionó la opción reporte como podemos ver en la figura 4.9, se abrió la ventana de cálculo de asistencias, es aquí donde se pudo generar reportes automáticos con la información descargada desde el dispositivo, simplemente lo que se hizo fue seleccionar el checador, seleccionar el grupo de usuarios de los que se quieren obtener los datos, en este caso el apartado “agentes” y en la sub selección “todos”, también se eligió el rango de los días de los cuales se deseaba obtener información, de la semana “5/08/2019” a la semana “10/08/2019” y se seleccionó la opción calcular.

Name	Auto-Assign	Date	Timetable	On duty	Off duty	Clock In	Clock Out	Normal	Real time
Erik Parra Arz		05/08/2019	Mañana	06:00	14:00	06:02		1	1
Erik Parra Arz		06/08/2019	Mañana	06:00	14:00	06:01	16:33	1	1
Erik Parra Arz		07/08/2019	Mañana	06:00	14:00	05:58		1	1
Erik Parra Arz		08/08/2019	Mañana	06:00	14:00	05:59		1	1
Erik Parra Arz		09/08/2019	Mañana	06:00	14:00	06:03	13:59	1	1
Erik Parra Arz		10/08/2019	Mañana	06:00	14:00	06:01		1	1
Jose Orduño		05/08/2019	Mañana	06:00	14:00	06:04		1	1
Jose Orduño		06/08/2019	Mañana	06:00	14:00	06:19		1	1
Jose Orduño		07/08/2019	Mañana	06:00	14:00	06:08		1	1
Jose Orduño		08/08/2019	Mañana	06:00	14:00	06:06		1	1
Jose Orduño		09/08/2019	Mañana	06:00	14:00	06:03		1	1
Jose Orduño		10/08/2019	Mañana	06:00	14:00	06:08		1	1
Clara Doming		05/08/2019	gateway	07:00	16:00	06:10		1	1
Clara Doming		06/08/2019	gateway	07:00	16:00	06:04		1	1
Clara Doming		07/08/2019	gateway	07:00	16:00	06:19		1	1
Clara Doming		08/08/2019	gateway	07:00	16:00	06:10		1	1
Clara Doming		09/08/2019	gateway	07:00	16:00	07:10	15:49	1	1
Eduardo Garc		05/08/2019	Mañana	06:00	14:00			1	
Eduardo Garc		06/08/2019	Mañana	06:00	14:00			1	

Figura 4.9 Calculadora de Asistencias

El programa arrojó información de todos los agentes organizada por diferentes secciones dependiendo de la información que se requería consultar, en este ejemplo se muestra la pestaña “excepciones de jornada” y nos muestra el nombre del usuario, sus entradas y salidas de los cinco días laborales, en la opción “reporte” se generó un Excel con toda la información de los agentes.

Instalación de Hardware

Además de las tareas ya descritas anteriormente que fueron más orientadas al software, también se hicieron diferentes modificaciones de hardware entre otro tipo de adiciones al site para cumplir con los estándares de PCI que se necesitan en Szertegia, principalmente como se comentó en el apartado anterior, se adicionó un equipo extra para el servidor NTP, además con respecto al servidor Dell r640 que cuenta Szertegia se agregó un disco duro de alta capacidad especial para ese tipo de servidores de un terabyte punto doscientos megas para los archivos logs que se generan, ya que PCI necesita un registro de un año de logs como mínimo, el terabyte adicional será suficiente para guardar toda esta información. También se le agregó una memoria RAM extra de dieciséis gigabytes para que el servidor contara con un total de treinta y dos gigabytes. Gracias a esta adición de RAM extra se pudo alojar en el hyper-v manager de Windows server los servicios y servidores virtuales que necesitaba la empresa. Se instaló en el ordenador donde se tiene alojado el PfSense una tarjeta de red extra, con dos puertos más, esto para poder redireccionar la señal a un Access Point que está planeado instalarse.

Fuera de las normativas con respecto al software y hardware, pero dentro de las políticas de PCI, existen ciertas reglas que los empleados, en este caso agentes del callcenter y supervisores, deben de seguir, primero que nada todo agente y supervisor en el área de operaciones debe tener su área de trabajo, limpia y libre de cualquier tipo de papel y herramientas de escritura física, esto con el fin de proteger la información de los clientes con los que se trabajan, de la misma manera queda estrictamente prohibido el uso de celulares, cámaras, tabletas, scanner o cualquier dispositivo en el cual se pueda guardar información o que capture imágenes dentro del área de operaciones, no solo los agentes si no también supervisores y agentes de calidad deben de cumplir

con estas reglas, además se estableció el área libre de uso de estos dispositivos en un mapa topográfico del área, solamente los administrativos pueden tener acceso a estos dispositivos o herramientas de escritura física.

Para poder cumplir con los reglamentos de este aparatado de PCI, en Szertegia se instalaron un total de diez estantes de lockers con 4 espacios cada uno (ver figura 4.10). En estos lockers los agentes guardan sus pertenencias, siempre y cuando ellos proporcionen sus candados personales para asegurar sus pertenencias. Parece una tarea bastante simple sin embargo es muy importante y facilitó con el cumplimiento de PCI.



Figura 4.10 Área de Lockers

5. ANÁLISIS DE LA EXPERIENCIA ADQUIRIDA

En este apartado se presenta la valoración de los aprendizajes y lecciones aprendidas durante la estancia profesional en la empresa Szertegia, tanto en términos del proyecto en general, los objetivos que se plantearon para su realización, las actividades desarrolladas y la metodología que se utilizó.

5.1 ANÁLISIS GENERAL DEL PROYECTO

Como análisis general del proyecto, cabe destacar que la tarea de implementación de PCI es una ardua tarea que lleva bastante tiempo y no solamente depende del área de sistemas. Al momento de iniciar el proyecto, el departamento de sistemas esperaba una total cooperación de los demás departamentos para poder llevar a cabo la implementación de las diferentes normativas en la empresa y aunque así lo fue, se debe contar que influyen muchos factores tanto internos como externos para terminar de implementar las normativas de PCI, tanto económicas como directivas y por estas razones, el proyecto avanzó lento y no pudo ser terminado dentro de las horas especificadas en el plan de trabajo del proyecto, incluso dentro del plan de trabajo de la empresa.

A pesar de que no se pudieron cumplir con las normativas en su totalidad, la experiencia adquirida por medio de estos diferentes procesos en el área de sistemas en los cuales se desempeñó fueron sumamente importantes, ya que no solo ayudaron a concretar conocimientos como soporte de sistemas, sino que también fueron de grande ayuda al comprender sobre los diferentes requisitos que se necesitan para la implementación de normativas de PCI en una empresa.

5.2 ANÁLISIS DE LOS OBJETIVOS DE LAS PRÁCTICAS

El objetivo principal de realizar las prácticas profesionales en Szertegia fue implementar las normativas de PCI para tener acceso a campañas en las que se pueda manejar información de tarjetas de crédito, para poder tomar pagos en línea y estar en cumplimiento de los estándares de seguridad que se necesitan para transacciones en línea y de la misma manera aumentar las ganancias en la empresa. La implementación de normativas de PCI es muy amplia y depende de muchos factores externos e internos dentro de las diferentes áreas de la empresa, debido a contratiempos y a estos factores anteriormente mencionados, no pudo ser completada la implementación de las normativas en su totalidad, sin embargo, se avanzó ampliamente en el proceso de implementación y se dejó un plan establecido, más concreto que el que ya se tenía antes para continuar trabajando en la implementación dichas normativas, se identificó también en este plan, las área que deben de ser puestas en alta prioridad y cuales en una prioridad más baja, además se capacitó al personal de la empresa tanto agentes como administradores para llevar buenas prácticas dentro de la empresa que en su futuro facilitarán la implementación de la normativas requeridas

5.3 ANÁLISIS DE LAS ACTIVIDADES REALIZADAS

Debido a que las instalaciones de Szertegia Morelos son relativamente nuevas, cerca de ocho meses de ser instaladas, las principales ventajas de hacer las prácticas profesionales es que pudieron ser realizadas en un periodo de construcción donde hubo facilidad de trabajar en los distintos procesos que se llevaron a cabo en el área de sistemas además de los contemplados dentro del plan de las prácticas profesionales.

Por otra parte, la empresa dispone de una infraestructura y equipamiento que permitió desarrollar adecuadamente las actividades, así como el manejo de sistemas supervisados por el coordinador de IT. En particular, y en cuanto a las tecnologías de la información y comunicación, se dispone de equipo de cómputo, servidores, red de conectividad, los cuales soporta el trabajo que se

lleva acabó dentro de las distintas áreas operativas de la empresa. Debido a que se tiene diferentes áreas dentro de la empresa y con diferentes clientes y campañas, muchas veces los problemas que ocurrían solamente afectaban a un porcentaje de las operaciones, la infraestructura dentro de Szertegia y el modo de operación de las campañas permitía que las operaciones continuaran al presentarse fallos menores, sin embargo, en casos extraordinarios si era necesario tomar acciones inmediatas para restaurar operaciones.

Como se puede observar en el apartado 4 y sus subtemas, se llevaron a cabo distintas actividades en diferentes áreas de la empresa para diferentes empleados, sin embargo, todos con la misma finalidad que fue la implementación de buenas prácticas para la normativa de PCI, de la misma forma se obtuvo diferente experiencia de estas áreas lo cual fue una ventaja ya que se aprendió de diferentes situaciones, tanto críticas como no críticas y que hacer en caso de que se presente una de estas situaciones.

5.4 ANÁLISIS DE LA METODOLOGÍA UTILIZADA

Como preparación de las prácticas profesionales, primero que nada, las primeras dos semanas se tuvo preparación general sobre el trabajo que se desempeñaría, se tomó dos cursos de capacitación sobre soporte basado en COMPTIA A+ y otro basado en PCI-DSS, además que se preparó para llevar a cabo los procesos que la empresa desempeña día a día, esta capacitación fue impartida por el actual coordinador de sistemas y apoyo online de diferentes sitios web

Esa capacitación combinada con la solución de problemas que se presentaban en la operación diaria de los sistemas implementados en Szertegia permitió que se desarrollaran mejor las actividades encomendadas y que el aprendizaje recibido fuera más completo. También fue muy importante la comunicación constante con las áreas diferentes área dentro de Szertegia, ya sea administradores, supervisores, agentes de calidad y gerentes de operación para resolver problemas concretos que se presentaron con la operación de las diferentes campañas.

Por otra parte, la forma de trabajar también permitió obtener un aprendizaje importante. Al principio todas las actividades se desarrollaron por instrucciones y bajo la supervisión del gerente de sistemas, con el paso del tiempo y conforme se fueron adquiriendo nuevas habilidades y conocimientos para a realizar operaciones sin ayuda de un tutor e incluso implementando algunos procesos para mejorar el funcionamiento de las campañas dentro de Szertegia, desde juntas remotas por medio de internet con los clientes en Estados Unidos lo cual ayudó a reforzar el inglés, hasta el movimiento de equipo y hardware para configuraciones específicas tanto en la red local como en las estaciones de los agentes.

6. CONCLUSIONES Y RECOMENDACIONES

Szertegia es una empresa dedicada al soporte al cliente de usuarios americanos residentes en dicho país, la empresa tiene diferentes campañas las cuales son enfocadas al servicio al cliente. La empresa se rige por los estándares más altos de calidad para proporcionar la mejor atención posible a los clientes de las diferentes campañas. Como toda empresa, Szertegia tiene mucho potencial para crecer aún más y expandirse en Hermosillo, debido a que la locación Morelos es relativamente nueva, existen muchas áreas de crecimiento y de oportunidad que se pudieran atender. A continuación, se dará un resumen con las conclusiones de cómo mejorar la empresa y qué oportunidades como ya se mencionó, pueden ser mejoradas.

La empresa dispone de personal encargado de sistemas, el cual está preparado para la atención de problemas de software y hardware en el área de operaciones y área de administración, a su vez el área de administración está en constante contacto con instituciones externas a la empresa. Además, el área de operaciones implementa día a día mejoras y está en constante comunicación externa con el cliente, sin embargo, me parece que una mejor comunicación entre estas tres áreas resolvería muchos mal entendidos u obstáculos que se presentan de vez en cuando y afectan la producción dentro del callcenter.

Con respecto a soporte técnico dentro de la empresa, existen muchas áreas de oportunidad que se pueden aprovechar, además de implementar mejoras al departamento de sistemas y que no solo ayudaría a crear más ventas dentro del área de operaciones si no a llevar un flujo de trabajo más libre y continuo entre las diferentes áreas de la empresa:

- Dentro del site de Szertegia se tiene equipo de alto costo que requiere el mejor mantenimiento posible, no solo para asegurar su máximo desempeño sino también para prolongar su longevidad y que no sea reemplazada a tan corto plazo, esto evitará gastos mayores en caso de que algún equipo dentro del site falle o deje de funcionar y pare operaciones, debido a que la infraestructura eléctrica en la ciudad de

Hermosillo no es la mejor. A lo largo del trabajo desempeñado en Szertegia, hubo varias instancias en las que hubo apagones de luz el site se vio afectado teniendo que reiniciar los equipos, el site cuenta con varias fuentes de poder con batería interna, sin embargo, es necesario la implementación de mejores back ups para prevenir pérdida de equipo.

- La comunicación entre las diferentes áreas es muy importante y actualmente se usa un sistema de correos para la comunicación entre ellas, sin embargo, un sistema unificado en el que se pueda llevar a cabo una comunicación en tiempo real, agilizaría bastante el intercambio de archivos e información primordial para las operaciones día a día y así mejorar la productividad.
- Es de suma importancia que además de la buena comunicación con el área de sistemas en Szertegia, también se tome en cuenta las solicitudes con respecto a gastos económicos dentro del área misma, muchas veces las empresas se centran en el proceso de operación porque es la primordial área de generación de ingresos para la empresa, sin embargo, los gastos relacionados con el área de sistemas para mantenimiento, equipo nuevo y mejoras, son igual de importante para garantizar el funcionamiento de operaciones.

7. REFERENCIAS BIBLIOGRÁFICAS

<https://www.fomentoacademico.gob.ec/wp-content/uploads/downloads/2018/04/Firewall.pdf>

<https://www.teleinfo.mx/beneficios-de-pfsense/>

<https://www.ecured.cu/Pfsense>

https://www.cisco.com/c/es_mx/products/security/firewalls/what-is-a-firewall.html

<https://geekland.eu/que-es-y-para-que-sirve-un-firewall/>

<https://aula128.wordpress.com/2014/09/19/instalacion-y-configuracion-de-pfsense/>

<https://www.telefacil.com/wiki/index.php/Zoiper>

<https://www.zktecolatinoamerica.com/k40>

<https://es.galsys.co.uk/time-reference/ntp-time-servers/how-ntp-works.html>

<https://theworldofrafex.blog/2017/12/14/instalar-y-configurar-ntp-en-centos-7/>

27 de noviembre del 2019

A quien corresponda,

Presente:

Por medio de la presente se hace constar que el C. **Rodríguez López Gustavo Alberto** labora en la empresa Grupo SZLG S. de R.L de C.V como SOPORTE EN SISTEMAS, con un horario de 9 am a 5 pm de lunes a sábados con descansos los domingos.

Tras haber colaborado 360 horas en el periodo comprendido, desempeñando diversas actividades informáticas cubriendo el total de 360 horas acumuladas de sus prácticas profesionales en la fecha antes mencionada, comportándose con buen desempeño, precisión, puntualidad y dedicación que ameritaban las actividades.

Extendemos la presente solicitud del interesado y para los fines que estime conveniente en la ciudad de Hermosillo Sonora al 27 de noviembre del presente año.

ATENTAMENTE,



Irene Domínguez
JEFE DE RECURSOS HUMANOS
GRUPO SZLG S. DE R.L DE C.V

Blvd. Morelos 307, Building H 201 202. C.P. 83145, Hermosillo, Sonora. MX.

Telephone: MX (662)3111286 US +1 8779542409



UNIVERSIDAD DE SONORA

COORDINACIÓN DIVISIONAL DE INGENIERIA

PRÁCTICAS PROFESIONALES

FPP-4

DEPARTAMENTO: Ingeniería Industrial

UNIDAD REGIONAL CENTRO CAMPUS HERMOSILLO

REPORTE FINAL DE ACTIVIDADES

Periodo: Del 20 / 05 / 2019 al 22 / 07 / 2019

Cantidad de 360 Horas de un total de 360 Avance: 100 %

Nombre del practicante: Gustavo Alberto Rodríguez Lopez

Expediente: 214219419 Programa Educativo (Licenciatura): Ingeniería en Sistemas de Información

Nombre del Programa/Proyecto: Aplicación de los requisitos para la certificación de PCI-DSS

Datos de la Unidad Receptora (Razón Social): El objetivo del programa es aplicar todas las medidas de seguridad y cumplir los requisitos para la certificación de PCI-DSS para que la empresa pueda procesar pagos con tarjeta de crédito/débito

Responsable de la Unidad Receptora (Nombre/Puesto): GRUPO SZLG S DE RL DE CV

Contacto: Teléfono/UR: 6624920058 Ext. Celular:

DESCRIPCIÓN GENERAL DE ACTIVIDADES Durante la estancia en Sztergia se realizaron diferentes actividades las cuales fueron apoyadas por el coordinador de sistemas en la empresa durante las dos primeras semanas, se llevaron a cabo varios cursos y asesoramientos por parte del coordinador de sistemas para estar preparado para las tareas más elaboradas, una vez terminado los cursos, se comenzó con pequeñas tareas como lo fue la instalación de un checador a la entrada, hardware y equipo de cómputo adicional en el área de operaciones, de misma forma, se fue configurando los sistemas y equipos necesarios como el puesto lo requiere, se llevaron a cabo diferentes tareas de soporte a los agentes en el área de operaciones, además de las tareas ya mencionadas, se aplicaron diferentes configuraciones a el servidor por medio de GPO's creación de usuarios desde el portal de mantenimiento de supervisor.

RETROALIMENTACIÓN (Comentarios del tutor)

En caso de requerirse, anexar reportes, formatos, diagramas que apoyen las actividades realizadas.

Para las Ingenierías deberá anexar **reporte técnico** en archivo electrónico ≤ 2 MB y carta de terminación de prácticas firmada por el responsable de la empresa.

Observaciones Generales:

 Nombre y firma del alumno	 Dr. Alonso Pérez Soltero Nombre y firma del tutor de prácticas profesionales UniSon.	 Nombre y firma del responsable de la unidad receptora No. 195 COL. BALSERAMA C.P. 83180 Hermosillo, Sonora 6624920058
--------------------------------------	---	--

Original entregar en físico al Coordinador o Responsable de Prácticas Profesionales de la carrera.
Copia para Tutor de Prácticas Profesionales y **Copia** alumno.
Enviar en PDF los documentos al coordinador/responsable de prácticas profesionales de la carrera.

(25/04/2018)