UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA

PROCESO DE TITULACIÓN

OCTUBRE 2018 – MARZO 2019

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA

PRUEBA PRÁCTICA

PREVIO A LA OBTENCIÓN DEL TITULO DE INGENIERO EN SISTEMAS

TEMA:

ANALISIS DE LA INFRAESTRUCTURA DE LA RED INFORMATICA Y SOPORTE DEL DISTRITO DE SALUD 12D05 PALENQUE - VINCES

EGRESADO:

MIGUEL ALFREDO GARCIA GUAMAN

TUTOR:

ING. MALIZA CRUZ WELLINGTON ISAAC

AÑO 2019

1 INTRODUCCIÓN

La infraestructura de Red Informática, con el paso de años se la conoce como Tecnología de la Información (TI), es una rama de la Ingeniería en sistemas esta permite descubrí todo lo esencial en redes y telecomunicaciones, que está combinado por elementos en red los cuales son equipos activos que su funciona principal es disponer del medio para la transmisión y comunicación con el propósito de respaldar el correcto envió de la información.

En el presente estudio de caso se va Análisis de la Infraestructura de la Red Informática y Soporte del Distrito de Salud 12D05 Palenque - Vinces, con ello sabremos anomalías que existen dentro de la institución con el objetivo de dar una mayor calidad y realce al Distrito de Salud 12D05 Palenque – Vinces.

En la actualidad el Distrito de Salud 12D05 Palenque – Vinces, presenta varios problemas con la red y la infraestructura, al no tener implementada una correcta política de Seguridad, existen conflictos con direcciones IP, fallas en los equipos informáticos, Insuficiente Ancho de Banda, Infecciones de Virus y poco mantenimiento preventivo a la infraestructura de Red, Existen criterios que al cumplirse correctamente garantizan un perfecto funcionamiento de la red, los cuales velan por la seguridad y la integridad de la información.

El soporte informático se trata de un servicio el cual puede ser mediante asistencia remota o el servicio técnico personal, métodos y técnicas para resolver algún problema, además brindan asesoramiento a usuarios y empresas que trabajan con Equipos Informáticos. (Cruz, 2014). La metodología que se va a emplear es la descriptiva ya que permite conocer las situaciones predominantes a través de la descripción exacta de las actividades y procesos que realiza la red informática en el Distrito de Salud 12D05 Palenque

– Vinces, los datos se expresaran en términos cualitativos ya que proporcionan una gran cantidad de información valiosa.

El presente estudio, tiene relación a la línea de investigación de desarrollo de sistemas de la información, comunicación y emprendimientos empresariales y tecnológicos basándose el análisis en la sublínea de investigación de procesos de transmisión de datos y telecomunicaciones.

2 DESARROLLO

El análisis de la Infraestructura de Red y Soporte Informático en el Distrito de Salud 12D05 Palenque - Vinces; esta es una institución de derecho público, con altos niveles de atención a la ciudadanía, tratando de garantizar la salud de la población y el acceso mundial a una red de servicios de salud, con la colaboración ordenada de empresas públicas y de la ciudadanía, como lo determine la Constitución de la república del Ecuador y las Leyes (DORDOIGNE, Las redes Administre una red en Windows o Linux: Ejercicios y soluciones (2ª edición), 2018).

El avance de la tecnología con las rede informáticas han diseñado un sistemas para que en una red un ordenador transmita información desde cualquier punto hacia otro punto, o a su vez para diferente instituciones; esta nueva tecnología de comunicación se la conoce como (internet) por lo que no hay cabida de otra forma, porque no nos da a conocer precisamente a la red el importante información que circula en el mundo. (Rodriguez, Telecomunicaciones, Historia y conceptos basicos, 2016)

El Distrito de Salud 12D05 Palenque – Vinces, tiene diseñada en su infraestructura de red una red MAN, esta es la que permite conectarse a la red LAN del distrito, gracias a esta infraestructura el distrito trabajar y transmitir con facilidad su información por medio de una red (Internet). El avance de las nuevas tecnologías ha evolucionado la comunicación a través de los año, debido a que por medio de normas se han incorporado nuevas métodos de comunicación a largas distancia con el objetivo de transmitir datos, sonidos, imágenes y voz con la implementación de equipos informáticos, los cuales son el eje fundamental de la comunicación, esto evoluciono las grandes redes de ordenadores y sistemas de comunicación. (Jimenez, El dasafio de la innovacion de la informatica, 2014)

Para compartir información en El Distrito de Salud 12D05 Palenque - Vinces, en el Data Center tienen implementado un Switch Cisco Poe que puede admitir 48 puertos PoE con una capacidad total de salida de potencia PoE a 370W, que permite a cada usuario tenga acceso a internet en sus equipos de trabajo.

El Firewall es el encargado de brindar seguridad a la infraestructura de red, por este motivo el talento humano de los diferentes departamentos que laboran en el Distrito de Salud 12D05 Palenque – Vinces son los encargados de su usuario y contraseña correspondiente. Un ingeniero de seguridad propone; propone implementar un modelo basado en dos capas con una topología

en estrella extendida, esta garantizara que la red funcione eficazmente, que sea confiable y fácil de manejar para que detecte posibles errores con tiempo de resultados; y el medio de transmisión posea una eficaz disponibilidad.

Los firewalls son dispositivos informáticos que se implementan en hardware y software o a su vez la unión de ambos, se utiliza para prevenir ataques informáticos de personas no autorizadas esto evita que tengan entrada a redes privadas del Distrito de Salud 12D05 que se encuentre conectada a internet. Son configuradas e incorpora a la red y sirve como defensa de cualquier ataque informático. (Carpentier, La Seguridad Informatica en la PYME, 2016)

El ingeniero Olivier Aguilar encargado del Departamento de Sistema del Distrito de Salud 12D05 Palenque – Vinces, en relación a las topologías, la red LAN que está implementada, trabaja utilizando una topología de tipo en estrella en donde el Switch Cisco Poe, es el nodo principal, ya que este permite la conexión de los rack que se halla implementado en el data center en la ubicación principal del distrito, Se está implementando la tecnología estándar Ethernet que sirve para renovar o mejorar los servicios utilizando el protocolo CSMA/CD.

Además manifestó que, el Distrito de Salud 12D05 Palenque - Vinces trabaja con una implementación de cableado estructurado par trenzado UTP de categoría 6A, dispone de 10 colaboradores los cuales se encuentran conectados entre sí a la red LAN que esta en el Distrito de Salud 12D05 Palenque – Vinces. “Los inicios del cableado estructurado, fueron diseñados por compañías telefónicas, para posteriormente las compañías de Sistemas de cómputo; un cableado estructurado correctamente diseñado permite administrar el cableado sin tener la necesidad de conocer la infraestructura de red”. (Tanenbaum, Redes de computadora y Seguridad, 2014)

El Ingeniero Jorge Mora, Jefe de Planificación manifestó que el cableado en el Distrito de Salud, es fácil de administrar debido a las nuevas tecnologías y a su vez permite la flexibilidad para implementar nuevos o futuros servicios adicionales a la red existente, en relación a los servidores suelen que tiene implementado el distrito de salud, se utiliza para almacenar archivos digitales de las diferentes Centros de Salud, es por esto que están conectados a través de la red con un servidor para acceder a la información; cabe destacar que un ordenador puede realizar las funciones de servidor y cliente de modo simultáneo. (Marchionni, Servidores - En administradores de resvidores, 2015)

Entre las distintas clases de servidores los que se encuentran implementados en el Distrito de Salud 12D05 Palenque – Vinces son los siguientes:

• Servidor de archivos.

• Servidor de correo.

• Servidor de Telefonía Ip. (Miguel, 2018).

Los servidores son los encargados de almacenar y distribuir los diferentes tipos de archivos que se encuentran en la red entre los clientes, la localización de los archivos está incorporado dentro de un servidor de archivos o a su vez en la propia máquina. (Carvajal, Manual Seccion, InstalacionConfiguracion y Administraccion de los Servidores, 2017)

Los usuarios que elaboran dentro del Distrito de Salud 12D05 Palenque – Vinces no poseen restricciones al uso de redes sociales, youtube u otra página de entretenimientos esto es un inconveniente ya que no garantiza realizar su labor con eficacia y sin ninguna interrupción para así ofrecer un servicio de calidad a la ciudadanía.

El soporte informático, permite dar solución a cualquier problema que sufran los equipos informáticos, ya sea un ordenador, una impresora o la infraestructura de red tanto el hardware como el software, Estas amenazar para el distrito se las puede tratar en el departamento correspondiente en la institución. Actualmente las empresas necesitan de soporte informático, asistencia informática, Es por esta razón que destinan gran parte de su capital a la implementación y soporte informático para que de esta manera manejar disminuir el grado en cuanto a la perdía de información. (BAUD, 2016). Lo problemas que suelen presentar los equipos informáticos es en el software como en el hardware. Para ello se sugiere implementar medidas de seguridad bajo otorgamiento de una identificación a todos los usuarios internos, externos y temporales. (Alicia García-Holgado, Francisco J. García-Peñalvo, 2015).

Es un punto fundamental dentro del Distrito de Salud 12D05 Palenque - Vinces, implementar políticas de seguridad como por ejemplo, Los usuarios debe ser responsable de cuidar su credenciales. (CARPENTIER, 2016). Trabaja por medios de bloques uno principal y secundario los cuales están divididos en departamentos donde trabajan de manera integral para la Distrito de salud, tiene diseñado con un cableado estructurado par trenzado UTP de categoría 6A, cuenta aproximadamente con 15 usuarios los cuales se conectan a la red LAN además a este número se incluye adicionalmente equipos que tienen asignada una dirección Ip como por ejemplo las

impresoras y teléfonos, otros ordenadores se conectan inalámbricamente por la ausencia de puntos.

En la tabla 1 se puede observar cómo está distribuido los usuarios en los diferentes departamentos que comprenden los 2 bloqueas.

ENTIDAD	FUNCION	NUMERO USUARIOS
Planta Baja	Departamento de asesoría jurídica	2
	Departamento de sistemas	2
	Departamento de secretaria	1
	Departamento de planificación	2
	Departamento de Estadística	1
Primer Piso	Dirección del Distrito de Salud	3
	Departamento de Talento Humano	2
	Departamento de Contabilidad	2
TOTAL		15

Tabla 1: Número de usuarios por departamento
Fuente: Distrito de Salud 12D05 Palenque – Vinces

La Infraestructura física del Distrito de Salud 12D05 Palenque – Vinces

Cantidad	Equipos
14	Computadoras de escritorio
3	Servidores
2	Routers
1	Switch Cisco Poe
1	Pactch Panels
1	Firewall
5	Teléfonos
2	Impresoras

Tabla 2: Infraestructura física Distrito de Salud 12D05 Palenque – Vinces
Fuente: Distrito de Salud 12D05 Palenque – Vinces

Diagrama De Red Del Distrito De Salud 12d05 Palenque – Vinces

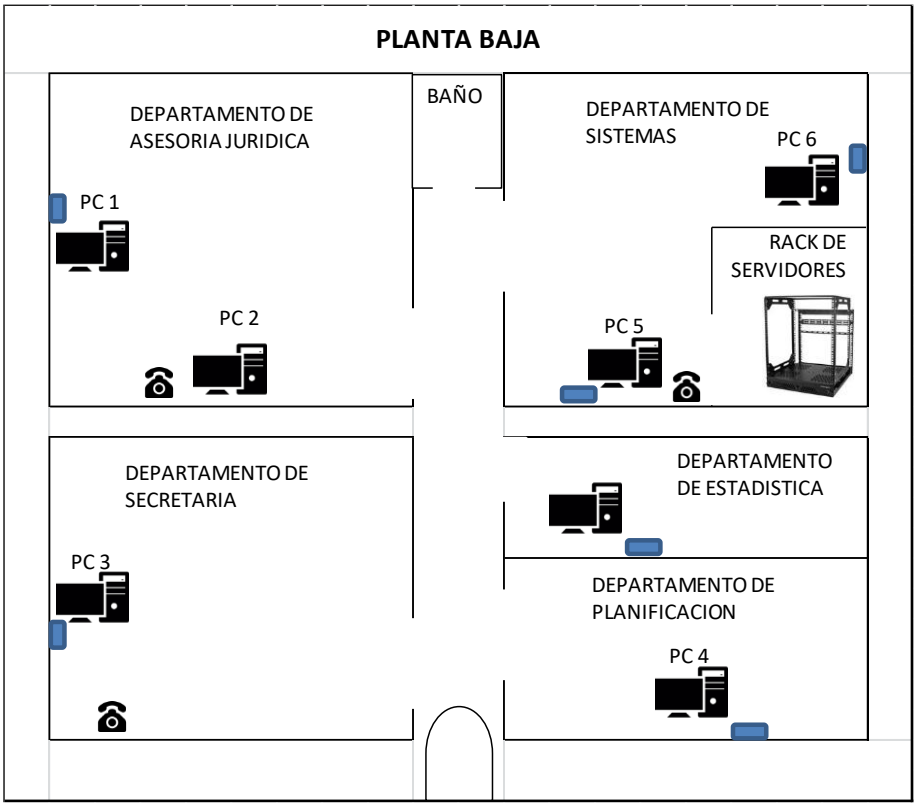

Ilustración 1: Punto de datos y Teléfonos Panta Baja
Fuente: Distrito de Salud 12D05 Palenque Vinces

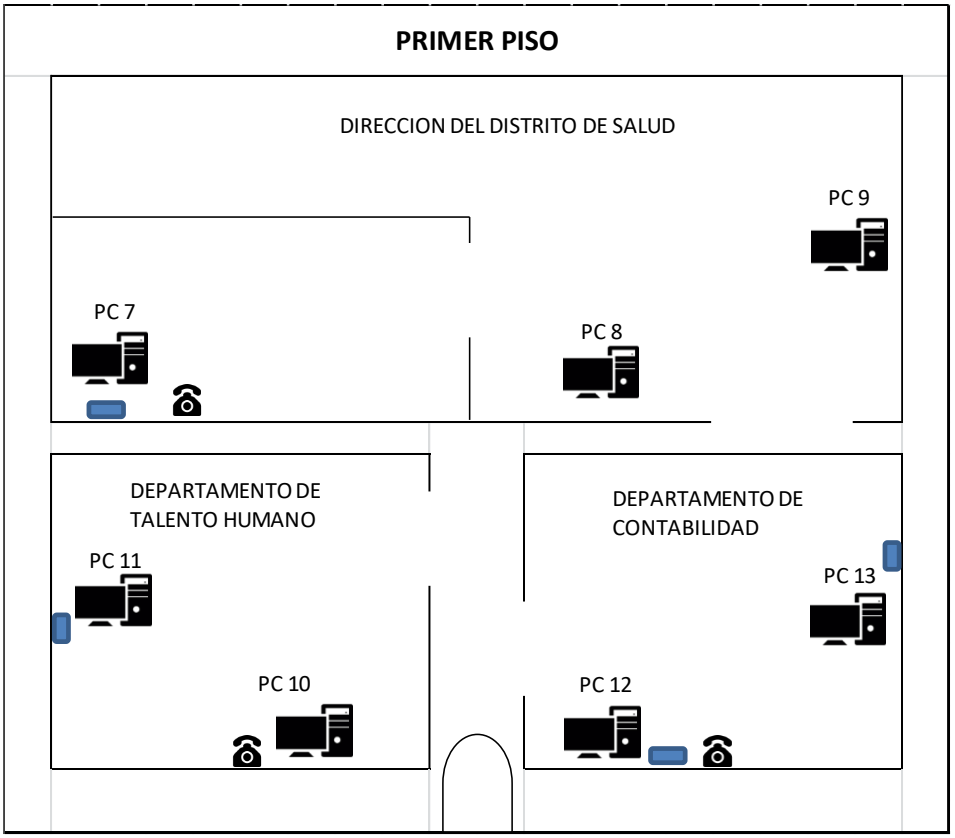

Ilustración 2: Punto de datos y telefonos primer piso
Fuente: Distrito de Salud 12D05 Palenque Vinces

En la actualidad El Distrito de Salud 12D05 cuenta con una red interna precaria, desordenada al no contar con los puntos de conexión de red necesarios el personal que labora se conecta inalámbricamente mediante un Adaptador Usb Wireless, con la cual no cumple con los Estándar de Cableado Estructurado (Ver Anexo 1), esto permite a las oficinas conectarse entre sí y acceder a los servicios en una red congestionada y mal diseñada.

El cableado de la red de datos es en la mayoría de las oficinas improvisado lo cual crea un ambiente inapropiado para la integración, administración y soporte de las aplicaciones administrativas. Lo cual nos da una idea clara y concisa del problema, la infraestructura de red actual no cubre los estándares adecuados para el funcionamiento eficiente de los diferentes departamentos de la institución limitando a los empleados a cumplir con sus funciones y truncando el correcto desempeño del Distrito de Salud Palenque – Vinces, lo que podría llevar a consecuencias mayores debido a que la institución se hace cargo de la información de todas los centros de Salud que están a su cargo.

El cableado estructurado es un método para crear un sistema organizado que pueda ser comprendido por los administradores, instaladores de red y cualquier otro técnico que trabaje en el área de redes. Un eficiente cableado estructurado permite disminuir todas las falencias de conectividad en el Distrito de Salud, es por ello que se sugiere diseñar el cableado estructurado para ser implementada en varias aplicaciones (DORDOIGNE, Redes Informáticas: Dominar los fundamentos (2ª edición), 2018)

Hay tres reglas que ayudan a garantizar la eficiencia y efectividad en los proyectos de diseño del cableado estructurado en una topología de red LAN las cuales enumeramos a continuación:

- **Buscar una solución completa de conectividad.** Una solución óptima para lograr la conectividad de redes abarca todos los sistemas que han sido diseñados para conectar, tender, administrar e identificar los cables en los sistemas de cableado estructurado
- **Planificar teniendo en cuenta el crecimiento futuro.** La cantidad del cableado instalado debe satisfacer necesidades futuras. La instalación de la capa física debe poder funcionar durante diez años o más.
- **Conservar la libertad de elección de proveedores.** Aunque un sistema cerrado y propietario puede resultar más económico en un principio, con el tiempo puede resultar ser mucho más costoso. Con un sistema provisto por un único proveedor y que no cumpla

con los estándares, es probable que más tarde sea más difícil realizar traslados, ampliaciones o modificaciones. (Systems, 2014).

El Distrito de Salud 12D05 Palenque – Vinces tiene implementada una arquitectura Cliente Servidor, esta arquitectura consiste básicamente en un cliente que realiza peticiones a otro programa (el servidor) que le da respuesta. Aunque esta idea se puede aplicar a programas que se ejecutan sobre una sola computadora es más ventajosa en un sistema operativo multiusuario distribuido a través de una red de computadoras. La interacción cliente-servidor en el Distrito es el soporte de la mayor parte de la comunicación por redes por lo que ayuda a entender las bases sobre las que están edificados los algoritmos distribuidos.

La infraestructura El Distrito de Salud 12D05 Palenque – Vinces tiene implementada una topología en estrella donde el Switch Cisco Poe es el nodo principal, La red LAN de área local permite a los usuarios cumplir con sus requisitos laborables y suministra conectividad de usuario a usuario está diseñada de tal manera que pueda aumentar de tamaño sin que se produzca cambios importantes en su diseño. Además es adaptable a cualquier a futuras tecnologías y su administración y monitoreo es fácil de manejar (Jérôme BEZET-TORRES - Nicolas BONNET, 2016).

Evaluación de Madurez de la infraestructura y soporte Informático en el Distrito de Salud 12D05 Palenque – Vinces, respecto a los controles definidos en la ISO/IEC 27001

Se evaluó la madurez respecto a los controles definidos en la ISO 27001 al Distrito de Salud 12D05, los parámetros que se tomaron en cuenta se podrá verificar en el (Anexo 3) de acuerdo a la norma ISO/IEC 27001, como se puede observar en la tabla 3 donde se analizó el Sistema de Gestión de la Seguridad de la Información (SGSI), cumple con una efectividad del 69%, esto quiere decir que existen 14 controles de No Conformidad Mayores que no se cumplen y estos controles afectan a la infraestructura del Distrito de Salud, 41 controles de No Conformidad Menores que no se cumplen pero estos no afectan al Distrito de Salud y existe 1 control que se cumple a cabalidad.

La Gestión de Responsabilidad, cumple con una efectividad del 65%, esto quiere decir que existen 4 controles de No Conformidad Mayores que no se cumplen y estos controles afectan a la infraestructura del Distrito de Salud y 14 controles de No Conformidad Menores que no se

cumplen pero estos no afectan al Distrito de Salud y existen 2 controles que se cumplen a cabalidad.

La Auditoria Interna del SGSI, cumple con una efectividad del 57%, esto quiere decir que existen 2 controles de No Conformidad Mayores que no se cumplen y estos controles afectan a la infraestructura del Distrito de Salud, 4 controles de No Conformidad Menores que no se cumplen pero estos no afectan al Distrito de Salud y no existen controles que se cumplan a cabalidad.

La Revisión por la Dirección del SGSI, cumple con una efectividad del 61%, esto quiere decir que existen 3 controles de No Conformidad Mayores que no se cumplen y estos controles afectan a la infraestructura del Distrito de Salud, 11 controles de No Conformidad Menores que no se cumplen pero estos no afectan al Distrito de Salud y existe 1 control que se cumple no existen controles que se cumplan a cabalidad.
La Mejora del SGSI, cumple con una efectividad del 66 %, esto quiere decir que existen 3 controles de No Conformidad Mayores que no se cumplen y estos controles afectan a la infraestructura del Distrito de Salud, 10 controles de No Conformidad Menores que no se cumplen pero estos no afectan al Distrito de Salud y no existen controles que se cumplan a cabalidad.

Dominio	% de Efectividad	# NC Mayores	# NC Menores	Control OK
4.- SGSI	69%	14	41	1
5.- Gestión de la Responsabilidad	65%	4	14	2
6.- Auditoría Interna Del SGSI	57%	2	4	0
7.- Revisión por la Dirección del SGSI	61%	3	11	1
8.- Mejora del SGSI	66%	3	10	0

Tabla 3: Evaluación de Madurez respecto a los controles definidos en la ISO/IEC 27001
Fuente: Norma ISO/IEC 27001

Se analizó 110 controles que corresponde a la Evaluación de Madurez respecto a los controles definidos en la ISO 27001 del Sistema de Gestión de la Seguridad de la Información (SGSI) como se puede observar en la tabla 4. El Distrito de Salud tiene falencias en su Infraestructura de Red

al no cumplir con ciertos controles del Sistema de Gestión de la Seguridad de la Información (SGSI). entre las falencias que se destacan cabe mencionar la política de Seguridad, no cuenta con los sistemas operativos de los ordenadores actualizados, el cableado es desordenado y los equipos no se encuentran actualizados, por esta razón no cuenta con un servicio de calidad dentro de la infraestructura de red, estos datos fueron mencionados por varios empleados que trabajan en el Distrito de Salud, Al hablar del soporte informático, El talento humano no cuenta con capacitaciones o charlas para poder así resolver algún problema en su equipo informático que utilizan diariamente.

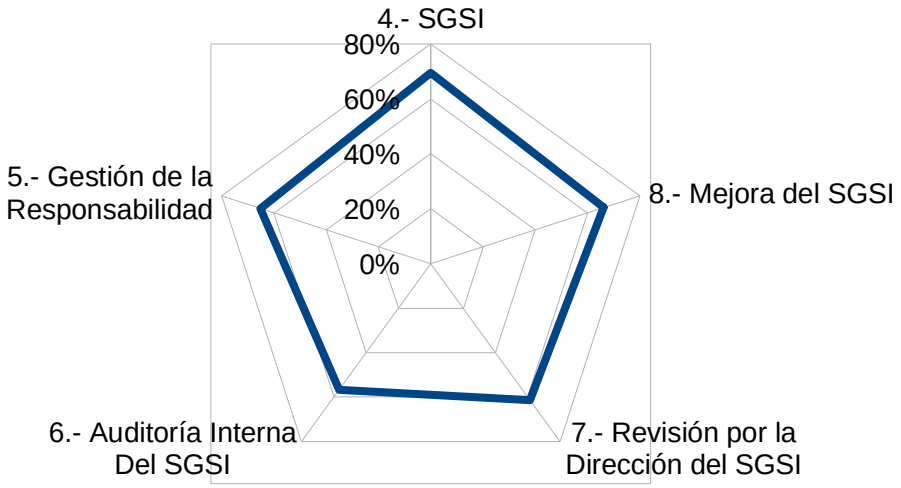

Tabla 4: Evaluación de Madurez respecto a los controles definidos en la ISO/IEC 27001
Fuente: Norma ISO/IEC 27001

3 CONCLUSIONES

Dentro del análisis expuesto, El Distrito de Salud 12D05 Palenque – Vinces, en su infraestructura de Red y soporte informático se llega a las siguientes conclusiones:

- El Distrito de Salud 12D05 Palenque – Vinces, no cumplen con algunos requerimientos en el Sistema de Gestión de la Seguridad de la Información (SGSI), al no definir una política de Seguridad que indiquen las normas, los procedimientos y las actuaciones que se deben cumplir por parte del Distrito, por lo tanto no puede generar una buena gestión estratégica, se sugiere elaborar su propia política de seguridad, que se debe encontrar firmada por las autoridades pertinentes y se establezca la exigencia de su cumplimiento. Esto garantiza el compromiso por parte del Distrito de Salud 12D05 Palenque - Vinces, que es el factor clave para conseguir el éxito.

- Las anomalías identificadas con respecto a la Infraestructura de Red dado que no cumplen con algunos estándares de Cableado estructurado y no cuentan con un ambiente regulado y climatizado en las oficinas de la planta baja, esto puede provocar calentamiento y daños a los equipos, por esta razón se sugiere diseñar la infraestructura basado en algunos de los estándares de cableado estructurado, esto permitirá al Distrito de Salud 12D05 Palenque – Vinces el correcto funcionamiento y rendimiento de la instalación así como también reducir riesgos.

- Se Acota que el Distrito de Salud 12D05 Palenque – Vinces no ha tomado a consideración el Soporte Informático ya que no cuenta con un mantenimiento programado de sus equipos tales como Servidores, UPS, Aplicaciones y capacitaciones al personal, esto reduce el rendimiento y la vida útil de la infraestructura, se sugiere programar cada cierto tiempo mantenimientos preventivo a los equipos y capacitar al personal que labora en la institución esto permitirá al Distrito que los sistemas informáticos se desempeñen en condiciones óptimas, además de poder identificar y solventar las contrariedades que se generen.

ANEXOS

Anexo 1: Estándares de Cableado estructurado

Normas de Cableado Estructurado

ANSI/TIA/EIA-568-B

Cableado de Telecomunicaciones en Edificios Comerciales sobre como cómo instalar el Cableado: TIA/EIA 568-B1 Requerimientos generales;TIA/EIA 568-B2: Componentes de cableado mediante par trenzado balanceado; TIA/EIA 568-B3 Componentes de cableado, Fibra óptica.

ANSI/TIA/EIA-569-A

Normas de Recorridos y Espacios de Telecomunicaciones en Edificios Comerciales sobre cómo enrutar el cableado.

ANSI/TIA/EIA-570-A

Normas de Infraestructura Residencial de Telecomunicaciones.

ANSI/TIA/EIA-606-A

Normas de Administración de Infraestructura de Telecomunicaciones en Edificios Comerciales.

ANSI/TIA/EIA-607

Requerimientos para instalaciones de sistemas de puesta a tierra de Telecomunicaciones en Edificios Comerciales.

ANSI/TIA/EIA-758

Norma Cliente-Propietario de cableado de Planta Externa de Telecomunicaciones.

Anexo 2: Evaluación de Madurez, respecto a los controles definidos en la ISO/IEC 27001

Control de ISO /IEC 27001	Requerimientos obligatorios para el SGSI	Valoración	Observaciones
4	**SGSI**		
4.1	**Requerimientos Generales**		
4.1	La organización debe establecer, implementar, operar, monitorizar, revisar, mantener y mejorar un SGSI documentado	L3	
4.2	**Establecer y Gestionar el SGSI**		
4.2.1	**Establecer el SGSI**		
4.2.1 (a)	Definir el alcance y los límites del SGSI	L3	

4.2.1 (b)	Definir una política de SGSI	L1	No estan definidas politicas de seguridad claves en la infraestructura de red
4.2.1 (c)	Definir el enfoque de la evaluación de Riesgos	L3	
4.2.1 (d)	Identificar los riesgos	L2	
4.2.1 (e)	Analizar y evaluar los riesgos	L3	
4.2.1 (f)	Identificar y evaluar opciones para el tratamiento de riesgos	L1	Se identifican pero no se aplica el tratamiento de riesgos
4.2.1 (g)	Seleccionar objetivos de control y controles para el tratamientos de riesgos	L2	
4.2.1 (h)	Obtener la aprobación por parte de la dirección de los riesgos residuales propuestos	L2	
4.2.1 (i)	Obtener la autorización de la Dirección para implementar y operar el SGSI	L3	
4.2.1 (j)	Preparar una Declaración de aplicabilidad	L3	
4.2.2	**Implementar el SGSI**		
4.2.2 (a)	Elaborar un plan de tratamiento de riesgos	L5	
4.2.2 (b)	Implementar el plan de tratamiento de riesgos para lograr los objetivos de control identificados	L1	Se ha llevado a cabo el análisis de riesgos y se ha establecido un plan al respecto que está dotado de recursos y en ejecución. Aún no se han llevado a cabo mejoras sobre éste
4.2.2 (c)	Implementar los controles seleccionados en 4.2.1g para llegar a los objetivos de control	L1	no cumple a cabalidad con los objetivos de control y controles para el tratamientos de riesgos
4.2.2 (d)	Definir cómo medir la efectividad de los controles o grupos de controles seleccionados y especificar cómo estas mediciones van a ser utilizadas para evaluar la efectividad del control para producir resultados comparables y reproducibles (ver 4.2.3c)	L3	
4.2.2 (e)	Implementar programas de formación y concienciación (ver 5.2.2)	L1	Se ha definido un proyecto para el programa de formación y concienciación que aún no se ha ejecutado
4.2.2 (f)	Gestionar la operación del SGSI	L2	
4.2.2 (g)	Gestionar los recursos para el SGSI (ver 5.2)	L2	
4.2.2 (h)	Implementar procedimientos y otros controles capaces de permitir una rápida detección de eventos de seguridad y respuesta a incidentes de seguridad (ver 4.2.3ª)	L3	

4.2.3	**Monitorizar y Revisar el SGSI**		
4.2.3 (a)	Ejecutar procedimientos de monitorización y revisión y otros controles	L3	
4.2.3 (b)	Llevar a cabo revisiones periódicas de la efectividad del SGSI	L2	
4.2.3 (c)	Medir la efectividad de los controles para verificar que se cumplen los requerimientos de seguridad	L2	
4.2.3 (d)	Revisar las evaluaciones de riesgos en intervalos planificados y revisar los riesgos residuales y los niveles aceptables de riesgos identificados.	L1	Los riesgos se revisan periódicamente o bien cuando hay cambios significativos en el sistema
4.2.3 (e)	Llevar a cabo auditorías internas del SGSI de manera regular (ver 6)	L1	El plan de auditorías está definido y se cumple
4.2.3 (f)	Llevar a cabo una revisión por la dirección del SGSI de manera regular (ver 7.1)	L3	
4.2.3 (g)	Actualizar los planes de seguridad para tener en cuenta los hallazgos de las actividades de monitorización y revisión	L2	
4.2.3 (h)	Registrar acciones y eventos que podrían tener impacto en la efectividad o el rendimiento del SGSI (ver 4.3.3)	L3	
4.2.4	**Mantener y mejorar el SGSI**		
4.2.4 (a)	Implementar las mejoras identificadas en el SGSI	L1	No se implementan mejoras en la infraestructura de red
4.2.4 (b)	Llevar a cabo las acciones correctivas y preventivas de acuerdo con 8.2 y 8.3	L3	
4.2.4 (c)	Comunicar las acciones y mejoras a todas las partes interesadas	L3	
4.2.4 (d)	Asegurar que las mejoras consiguen sus objetivos propuestos	L2	
4.3	**Requerimientos de Documentación**		
4.3.1	**Documentación General del SGSI**		
4.3.1 (a)	Documentar los procedimientos y objetivos de la política del SGSI (ver 4.2.1b)	L3	
4.3.1 (b)	Alcance del SGSI (ver 4.2.1A)	L3	
4.3.1 (c)	Procedimientos y controles de apoyo al SGSI	L1	Existen pero no se llevan a cabo
4.3.1 (d)	Descripción de la metodología de evaluación de Riesgos (ver 4.2.1c)	L2	
4.3.1 (e)	Informe de evaluación de Riesgos (ver desde el 4.2.1c al 4.2.1g)	L3	
4.3.1 (f)	Plan de Tratamiento de Riesgos (ver 4.2.2b)	L2	
4.3.1 (g)	Procedimientos necesitados por la organización para asegurar la planificación efectiva, la operación y el control de sus procesos de seguridad de la información y describir cómo medir la efectividad de los controles (ver 4.2.3c)	L2	
4.3.1 (h)	Registros requeridos por este Estándar Internacional (ver 4.3.3)	L3	
4.3.1 (i)	Declaración de Aplicabilidad	L1	no existe delaracion de aplicabilidad

4.3.2	**Control de Documentos**		
4.3.2	Los Documentos requeridos por el SGSI deberán ser protegidos y controlados. Un procedimiento documentado deberá ser establecido para definir las acciones de la dirección necesitadas para:		
4.3.2 (a)	Aprobar documentos para su adecuación antes de su emisión	L2	
4.3.2 (b)	Revisar y actualizar documentos cuando sea necesario y re-aprobar documentos.	L3	
4.3.2 (c)	Asegurar que los cambios y que los estados de revisión actual de los documentos están identificados	L3	
4.3.2 (d)	Asegurar que las versiones pertinentes de documentos aplicables están disponible y a punto para ser usados	L2	
4.3.2 (e)	Asegurar que los documentos permanecen legibles y fácilmente identificables	L3	
4.3.2 (f)	Asegurar que los documentos están disponibles para aquellos que lo necesiten y son transferidos, almacenados y en última instancia, eliminados de acuerdo a los procedimientos aplicables en base a su clasificación	L1	la informacion no esta disponible
4.3.2 (g)	Asegurar que los documentos de procedencia externa están identificados.	L3	
4.3.2 (h)	Asegurar que la distribución de los documentos está controlada.	L3	
4.3.2 (i)	Prevenir el uso no intencionado de documentos obsoletos.	L1	Los documentos están dentro de carpetas del servidor de ficheros. Las versiones obsoletas comparten carpetas con las versiones vigentes. Esto podría inducir a confusión. Está proyectada la implementación de un software de gestión documental que solucionará este tema.
4.3.2 (j)	Aplicar una identificación adecuada a los documentos si éstos son retenidos para cualquier propósito.	L2	
4.3.3	**Control de los Registros**		
4.3.3 (a)	Los registros deben establecerse y mantenerse para proporcionar evidencias de conformidad a los requerimientos y a la eficacia del SGSI	L3	
4.3.3 (b)	Los registros serán protegidos y controlados	L1	no se cumplen con las politicas de seguridad
4.3.3 (c)	El SGSI debe tener en cuenta los requisitos legales o reglamentarios y las obligaciones contractuales.	L3	
4.3.3 (d)	Los registros deben permanecer legibles, fácilmente identificables y recuperables.	L1	Se centralizan en una carpeta al efecto del servidor de ficheros
4.3.3 (e)	Los controles necesarios para la identificación, almacenamiento, protección, recuperación, tiempo de	L3	

	retención y desechado de los registros serán documentados e implementados.		
4.3.3 (f)	Se mantendrán registros de los resultados del proceso, como se indica en el apartado 4.2 y de todas las ocurrencias de incidentes de seguridad significativos relacionados con el SGSI.	L3	

Control de ISO /IEC 27001	Requerimientos obligatorios para el SGSI	Valoración	Anotaciones
5	**Gestión de la Responsabilidad**		
5.1	**Compromiso de la dirección**		
5.1	La dirección debe proporcionar evidencia de su compromiso con el establecimiento, implementación, operación, monitoreo, revisión, mantenimiento y mejora del SGSI por:	L3	
5.1 (a)	Establecer una política de SGSI	L1	las politicas establecidad no se cumplen
5.1 (b)	Asegurar de que se establecen los objetivos y los planes del ISMS	L3	
5.1 (c)	Establecer roles y responsabilidades para la seguridad de la información	L3	
5.1 (d)	Comunicar a la organización la importancia de satisfacer los objetivos de seguridad de la información y conforme a la política de seguridad de la información, sus responsabilidades en virtud de la ley así como la necesidad de la mejora continua	L2	
5.1 (e)	Proporcionar recursos suficientes para establecer, implementar, operar, monitorizar, revisar, mantener y mejorar el SGSI (ver 5.2.1)	L3	
5.1 (f)	Decidir los criterios de aceptación de riesgos y los niveles de riesgo aceptables	L3	
5.1 (g)	Asegurarse de que las auditorías internas del SGSI se llevan a cabo (ver 6)	L3	
5.1 (h)	La realización de revisiones por la dirección del SGSI (ver 7)	L2	
5.2	**Gestión de los recursos**		
5.2.1	**Provisión de Recursos**		
5.2.1	La organización deberá determinar y proveer los recursos necesarios para:		
5.2.1 (a)	Establecer, implementar, operar, monitorizar, revisar, mantener y mejorar un SGSI	L3	
5.2.1 (b)	Asegurar que los procedimientos de seguridad de la información son compatibles con los requerimientos del negocio	L2	
5.2.1 (c)	Identificar y abordar los requisitos legales y reglamentarios y las obligaciones contractuales de seguridad	L3	
5.2.1 (d)	Mantener la seguridad adecuada mediante la aplicación correcta de todos los controles implementados	L1	no se ejecutan todos los controles implementados
5.2.1 (e)	Llevar a cabo revisiones cuando sea necesario, y dar una respuesta adecuada a los resultados de estas revisiones	L3	
5.2.1 (f)	Cuando sea necesario, mejorar la eficacia del SGSI	L2	

5.2.2	Formación, sensibilización y competencia		
5.2.2	La organización debe asegurarse de que todo el personal al que se le asigna responsabilidades definidas en el SGSI sean competentes para desempeñar las tareas requeridas por:		
5.2.2 (a)	Determinar las competencias necesarias para el personal que realiza trabajo efectivo en el SGSI	L3	
5.2.2 (b)	Proporcionar formación o tomar otras acciones (por ejemplo, el empleo de personal competente) para satisfacer estas necesidades	L1	Se ha definido un proyecto para el programa de formación y concienciación que aún no se ha ejecutado
5.2.2 (c)	Evaluar la efectividad de las acciones llevadas a cabo	L5	
5.2.2 (d)	El mantenimiento de los registros de educación, formación, habilidades, experiencia y calificaciones (véase 4.3.3)	L5	
5.2.2	La organización también debe asegurar que todo el personal pertinente es consciente de la relevancia e importancia de sus actividades de seguridad de la información y de cómo contribuyen al logro de los objetivos del SGSI.	L1	Pendiente del programa de formación y concienciación que aún no se ha ejecutado

Control de ISO /IEC 27001	Requerimientos obligatorios para el SGSI	Valoración	Anotaciones
6	**Auditoría Interna del SGSI**		
6	La organización debe llevar a cabo auditorías internas del SGSI a intervalos planificados para determinar si los objetivos del control, controles, procesos y procedimientos de su SGSI:		
6 (a)	Cumplir con los requisitos de este Estándar Norma y la legislación o los reglamentos pertinentes	L3	
6 (b)	Cumplir con los requisitos de seguridad de la información identificados	L2	
6 (c)	Que está efectivamente implementado y mantenido	L3	
6 (d)	Desempeñe según lo esperado	L1	la infraestructura de red no se desempeña según lo esperado
6 (e)	Que sea planificado un programa de auditoría	L1	Se planfica programas de auditoria pero no se llevan acabo
6 (f)	La dirección responsable del área que esté siendo auditada debe asegurarse de que se toman acciones sin demora injustificada para eliminar las no conformidades detectadas y sus causas. Las actividades de seguimiento deben incluir la verificación de las acciones llevadas a cabo y el informe de resultados de la verificación (ver 8).	L3	

Control de ISO /IEC 27001	Requerimientos obligatorios para el SGSI	Valoración	Anotaciones
7	**Revisión por la dirección del SGSI**		
7.1	**General**		
7.1	La dirección revisará SGSI de la organización a intervalos planificados (por lo menos una vez al año) para asegurar su continua idoneidad, adecuación y eficacia	L2	
7.2 (a)	**Información para la Revisión**		
7.2	La información para una revisión incluirá:		
7.2 (a)	Resultados de Auditorías y revisiones del SGSI	L3	
7.2 (b)	Los comentarios de las partes interesadas	L3	
7.2 (c)	Técnicas, productos o procedimientos, que podrían ser utilizados en la organización para mejorar el rendimiento y la eficacia del SGSI	L2	
7.2 (d)	Estado de las acciones preventivas y correctivas	L1	No se cumplen con acciones preventivas y correctivas
7.2 (e)	Las vulnerabilidades o amenazas no tratadas adecuadamente en la evaluación de riesgos anterior	L1	
7.2 (f)	Los resultados de las mediciones de la eficacia	L3	
7.2 (g)	Las acciones de seguimiento de revisiones previas de la dirección	L3	
7.2 (h)	Todos los cambios que podrían afectar al SGSI	L1	Si al no contar con una red escalable
7.2 (i)	Recomendaciones de mejora	L5	
7,3	**Resultados de la Revisión**		
7,3	El resultado de la revisión por la dirección deben incluir todas las decisiones y acciones relacionadas con lo siguiente:		
7.3 (a)	Mejora de la eficacia del SGSI	L2	
7.3 (b)	Actualización del plan de tratamiento de riesgos y evaluación de riesgos	L3	
7.3 (c)	Modificación de los procedimientos y controles que la seguridad efecto la información, según sea necesario, para responder a eventos internos o externos que pueden influir en el SGSI	L3	
7.3 (d)	Necesidades de Recursos	L2	
7.3 (e)	Mejoras de cómo la efectividad de los controles está siendo medida	L3	

Control de ISO /IEC 27001	Requerimientos obligatorios para el SGSI	Valoración	Anotaciones
8	**Mejora del SGSI**		
8.1	**Mejora continua**		

8.1	La organización debe mejorar continuamente la eficacia del SGSI a través del uso de la política de seguridad de la información, los objetivos de seguridad de la información, resultados de las auditorías, el análisis de los eventos monitorizados, acciones correctivas y preventivas y la revisión por la dirección (véase 7).	L3	
8.2 (a)	**Acción Correctiva**		
8.2	La organización deberá tomar acciones para eliminar la causa de no conformidades con los requisitos del SGSI con el fin de prevenir la recurrencia de éstas. El procedimiento documentado de acciones correctivas debe definir requisitos para:		
8.2 (a)	Identificar las no conformidades	L1	no se identifican las no conformidades que existen en la infraestructura de red
8.2 (b)	Determinar las causas de las no conformidades	L3	
8.2 (c)	Evaluar la necesidad de adoptar medidas para asegurar que las no conformidades no vuelvan a ocurrir	L1	
8.2 (d)	Determinar y aplicar las medidas correctivas necesarias	L3	
8.2 (e)	Registrar los resultados de las acciones tomadas (véase 4.3.3)	L2	
8.2 (f)	Revisar las acciones correctivas tomadas	L3	
8.3 (a)	**Acción Preventiva**		
8.3	La organización determinará acciones para eliminar las causas de no conformidades potenciales con los requisitos del SGSI con el fin de prevenir su ocurrencia. Las acciones preventivas tomadas deben ser apropiadas a los efectos de los problemas potenciales. El procedimiento documentado para las acciones preventivas deben definir requisitos para:		
8.3 (a)	Identificar no conformidades potenciales y sus causas	L1	no se identifican
8.3 (b)	Evaluar la necesidad de actuar para prevenir la ocurrencia de no conformidades	L3	
8.3 (c)	Determinar e implementar las acciones preventivas necesarias	L2	
8.3 (d)	Registrar los resultados de las acciones tomadas (véase 4.3.3)	L3	
8.3 (e)	Revisar las acciones preventivas tomadas	L2	
8,3	La organización debe identificar cambios en los riesgos y determinar las necesidades de acciones preventivas centrando la atención en los riesgos que han cambiado significativamente	L2	

Anexo 3: Tabla de valores

Valor	Efectividad	Significado	Descripción	Número
L0	0%	Inexistente	Carencia completa de cualquier proceso conocido.	0
L1	10%	Inicial / Ad-hoc	Procedimientos inexistentes o localizados en áreas concretas. El éxito de las tareas se debe a esfuerzos personales.	26
L2	50%	Reproducible, pero intuitivo	Existe un método de trabajo basado en la experiencia, aunque sin comunicación formal. Dependencia del conocimiento individual	28
L3	90%	Proceso definido	La organización en su conjunto participa en el proceso. Los procesos están implantados, documentados y comunicados.	52
L4	95%	Gestionado y medible	Se puede seguir la evolución de los procesos mediante indicadores numéricos y estadísticos. Hay herramientas para mejorar la calidad y la eficiencia	0
L5	100%	Optimizado	Los procesos están bajo constante mejora. En base a criterios cuantitativos se determinan las desviaciones más comunes y se optimizan los procesos	4
L6	N/A	No aplica		0

Anexo 4: Preguntas de entrevista

1. Qué herramientas de software utiliza para desempeñar sus funciones. ¿Por qué?
2. Qué estrategias aplica cuando confronta un problema que no logra resolver?
3. En la escala de 1 a 10, como califica su experiencia como administrador de redes, ¿por qué?
4. En su experiencia, ¿cuáles son las actividades obligatorias y opcionales (pero recomendables) que un administrador de redes realiza?
5. Cual es el diseño de red implementado en el Distrito de Salud 12D05 Palenque – Vinces.
6. Que velocidad maneja la red en el Distrito de Salud 12D05 Palenque – Vinces.
7. Que acciones toma al momento que alguna falla en la red.
8. Como asegura la información transmitida a través de la red.
9. Lleva algún control de las actividades de los usuarios y administradores.
10. Cuáles son las normas de seguridad implementadas.

Anexo 5: Certificado de Aprobación para realizar el caso de estudio por parte del Distrito de Salud 12D05 Palenque – Vinces

MINISTERIO DE SALUD PÚBLICA

Vinces, 03 de Enero del 2019

Yo, DRA. ROSA EMILIA SILVA CASTRO Directora del Distrito de Salud 12D05 Palenque - Vinces

CERTIFICO

Al Sr. **Miguel Alfredo García Guamán** con numero de cedula de identidad: **0302663166**, Estudiante de la Universidad Técnica de Babahoyo de la Facultad de Administración, Finanzas e Informática, Carrera de Ingeniería en Sistemas con número de matrícula EST-UTB 6066, le autorizó para que realice el Estudio de Caso con tema, ***Análisis de la Infraestructura de la Red Informática Y Soporte Del Distrito De Salud 12d05 Palenque- Vinces***, En el Departamento de sistemas y además todas las instalaciones que necesite.

Se extiende la presente certificación al interesado, para los fines que crea conveniente

Atentamente:

DISTRITO DE SALUD 12D05 VINCES - PALENQUE DIRECCIÓN

DRA. ROSA EMILIA SILVA CASTRO
Directora Distrito de Salud 12D05 Palenque - Vinces

BIBLIOGRAFÍA

Alicia García-Holgado, Francisco J. García-Peñalvo. (Abril de 2015). *s3.amazonaws.com.* Recuperado el 13 de Enero de 2019, de s3.amazonaws.com: https://s3.amazonaws.com/academia.edu.documents/37313539/GRIAL-TR-2015-001.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1547393611&Signature=GZhuSa22t9BJ%2B6xG6CktPaY9tAU%3D&response-content-disposition=inline%3B%20filename%3DEstudio_sobre_la_evolucion

BAUD, J.-L. (2016). *ITIL® V3 Entender el enfoque y adoptar las buenas prácticas.* España: ENI Ediciones.

Carpentier, J. (2016). *La Seguridad Informatica en la PYME.* España: ENI.

CARPENTIER, J. F. (2016). *La seguridad informática en la PYME: Situación actual y mejores prácticas.* España: ENI Ediciones.

Carvajal, F. (2017). *Manual Seccion, InstalacionConfiguracion y Administraccion de los Servidores.* Madrid: CEP S.L.

Cruz, J. (2014). *Gestión auxiliar de archivo en Soporte Convencional o Informático.* España: IC Editorial. .

DORDOIGNE, J. (2018). *Las redes Administre una red en Windows o Linux: Ejercicios y soluciones (2ª edición).* España: ENI Ediciones.

DORDOIGNE, J. (2018). *Redes Informáticas: Dominar los fundamentos (2ª edición).* España: ENI Ediciones.

Jérôme BEZET-TORRES - Nicolas BONNET. (2016). *Windows Server 2016 Infraestructura de red.* ENI Ediciones.

Jimenez, L. L. (2014). *El dasafio de la innovacion de la informatica.* UOC.

Jose Valderrama, Cristhian Minaya. (23 de Mayo de 2014). *Soporte Informático. Soporte Tecnico Informático Definición, Tipos y Evolución.* Obtenido de Soporte Informático. Soporte Tecnico Informático Definición, Tipos y Evolución.: https://primerojpb.wordpress.com/2014/05/23/soporte-tecnico-informatico-definicion-tipos-y-evolucion/

Marchionni. (2015). Servidores - En administradores de resvidores. *Servidores - En administradores de resvidores* (pág. 352). Argentina: USERS.

Miguel, I. d. (17 de Abril de 2018). *Loogic*. Recuperado el 13 de Enero de 2019, de Loogic: https://loogic.com/telefonia-ip-7-claves-para-elegir-la-empresa-adecuada/

Rodriguez, L. G. (2016). *Telecomunicaiones: Historia y conceptos bàsicos.* Mexico: Colnax.

Systems, C. (2014). *CCNA 1 Suplemento sobre cableado estructurado.* Copyright.

Tanenbaum, W. (2014). *Redes de computadora y Seguridad.* Pearson.