



UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERÍA Y ARQUITECTURA

**ESCUELA PROFESIONAL DE INGENIERÍA DE
SISTEMAS**

**Diseño de una red privada virtual (VPN) basada en software
libre para la mejora de la seguridad de la información de la
jurisdicción de la dirección de redes integradas de salud
Lima Centro**

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE:

Ingeniero de Sistemas

AUTORES:

Lazarte Tirapo, Daniel (ORCID: 0000-0001-8748-4519)

Silva Buitrón, Giancarlos (ORCID: 0000-0001-5196-7404)

ASESOR:

Mg. Quiñones Nieto, Yamil Alexander (ORCID: 0000-0003-4474-0556)

LÍNEA DE INVESTIGACIÓN:

Infraestructura de servicio de redes y comunicaciones

LIMA – PERÚ

2022

DEDICATORIA

DANIEL

Un especial agradecimiento a mi Padre
Florencio por sus enseñanzas,
Mi Madre Zoila quien es mi apoyo y referente principal de vida,
Mi Esposa Carmen por estar conmigo en todo, gracias mi reina
y mis hijas por ser mis fuerzas para seguir adelante.

GIANCARLOS

Dedicatoria

Agradecer a mi familia por el apoyo
durante mi vida, a mi novia por su paciencia y
buenos consejos en el
desarrollo de mi carrera y a Dios por darme salud.

AGRADECIMIENTO

Agradecer a Dios y a nuestras familias por ser el apoyo y soporte en nuestras vidas.

A nuestro asesor por brindarnos sus enseñanzas, consejos y experiencia.

A la DIRIS Lima Centro por brindarnos el apoyo y creer en nuestro proyecto.

Índice de contenidos

Carátula.....	i
Dedicatoria.....	ii
Agradecimiento.....	iii
Índice de contenidos.....	iv
Índice de tablas.....	v
Índice de figuras y gráficos.....	vi
Resumen.....	vii
Abstract.....	viii
I. INTRODUCCIÓN	1
II. MARCO TEÓRICO	6
III. METODOLOGÍA.....	11
3.1. Tipo y Diseño De La Investigación	11
3.2. Variables y Operacionalización.....	11
3.3. Población, Muestra y Muestreo.....	12
3.4. Técnicas e Instrumentos de Recolección de Datos.....	13
3.5. Procedimientos y Resultados	13
3.5.1. Integridad	14
3.5.2. Disponibilidad	16
3.6. Método de Análisis de Datos	19
3.7. Aspectos Éticos	19
3.8. Aspectos Administrativos	20
3.9. Financiamiento	22
3.10. Cronograma.....	22
3.11. Cronograma de Ejecución.....	22
IV. RESULTADOS.....	23
4.1. Fases de la Metodología Top-Down Network Design	23
V. CONCLUSIONES	79
VI. RECOMENDACIONES	80
REFERENCIAS.....	81

Índice de figuras

Figura 1. Histograma 1	15
Figura 2. Histograma 2	15
Figura 3. Histograma 3	17
Figura 4. Histograma 3	18
Figura 5. Proceso de fases de la metodología Top Down	24
Figura 6. Ubicación de la Dirección de Redes Integradas de Salud de Lima Centro	28
Figura 7. Jurisdicción de la Dirección Regional de Lima Centro	29
Figura 8. Ciclo PHVA.....	32
Figura 9. Topología de la red física de la oficina central	33
Figura 10. Topología de la red de sucursales	34
Figura 11. Protocolos LAN	57
Figura 12. Protocolos de enrutamiento.....	58
Figura 13. Redes de seguridad	60
Figura 14. Red local	61
Figura 15. Integradas de salud.....	62
Figura 16. Configuración de servicio VPN.....	67
Figura 17. Generación de certificados y llaves	67
Figura 18. Certificación de la CA	68
Figura 19. Generación de software	70
Figura 20. Configuración de servicio	70
Figura 21. Generación de certificados y llaves	71
Figura 22. Open VPN	71
Figura 23. Conexión VPN.....	72
Figura 24. Instalación del software open vpn	72
Figura 25. Direccionamiento IP	74
Figura 26. Certificados confianza para túnel VPN.....	74

Figura 27. Muestra la conexión de la vpn.....	75
Figura 28. Instalación del software open vpn	76
Figura 29. Trámite documentario antiguo.....	76
Figura 30. Sistema de trámite documentario.....	77
Figura 31. Control de asistencia.....	77
Figura 32. Sistema de trámite documentario.....	78

Índice de tablas

Tabla 1. Variable Independiente: Red Privada Virtual (VPN) Bajo Software Libre	11
Tabla 2. Variable Dependiente: Seguridad de información	12
Tabla 3. Cuadro de participantes del cuestionario	13
Tabla 4. 10 encuestas Pre-Test y 10 encuestas Post-Test para el muestreo en la estadística	14
Tabla 5. N es la cantidad de encuestas tomadas en el PRE y POST TEST	14
Tabla 6. Pruebas de muestras emparejadas	16
Tabla 7. Resumen de procesamiento de datos	16
Tabla 8. Pruebas de normalidad	17
Tabla 9. Estadísticos de prueba	18
Tabla 10. Recursos Humanos sin costo monetario	20
Tabla 11. Recursos Humanos con costo	21
Tabla 12. Recursos Tecnológicos	21
Tabla 13. Otros gastos adicionales en el proceso de la investigación	21
Tabla 14. Total, de gastos incurridos durante el desarrollo del proyecto	22
Tabla 15. Cronograma	22
Tabla 16. Metodología Top Down	25
Tabla 17. Fases de la mejora continua	32
Tabla 18. Lista de dispositivos de la red DIRIS	35
Tabla 19. Red de Comunicaciones Sede Central	38
Tabla 20. Red de Comunicaciones Establecimientos de salud	39
Tabla 21. DIRIS Lima Centro	41
Tabla 22. Mapeo de usuarios	42
Tabla 23. Puntos de red	46
Tabla 24. Distribución de la red DIRIS Lima Centro	49
Tabla 25. Hosts utilizables	52
Tabla 26. Direccionamiento IP	53

Tabla 27. Puestos de salud	54
Tabla 28. Lista de equipos utilizados.....	63
Tabla 29. Características del hardware	66

RESUMEN

La Dirección de Redes Integradas de Salud (DIRIS) Lima Centro es la encargada de administrar los establecimientos de salud, las cuales pertenecen al Ministerio de Salud – MINSA; es la encargada de velar por la salud de la jurisdicción de Lima y San Juan de Lurigancho. Su misión es la de brindar calidad de salud a los pacientes de su jurisdicción.

Los establecimientos de salud brindan servicios de salud a los pacientes de la jurisdicción de la Diris Lima Centro; manejan información de vital importancia la cual sirve para la toma de decisiones; los sistemas que manejan son los siguientes: His, Sistema de Admisión Iqhali, Sien, Arfsis, etc.

Alguno de estos sistemas funcionan mediante un servidor (host), pero actualmente se están emigrando a la plataforma web, sin embargo, el problema que tienen los establecimientos constantemente es la seguridad, pues los usuarios de los equipos de cómputos de las diferentes oficinas y/o servicios no cuentan con estas medidas de seguridad, estos acceden libremente a páginas de ocio, así como instalan aplicativos de uso no laboral y constantemente hay pérdida de información pues los usuarios desinstala el antivirus, el cual protege el equipo de posibles infecciones.

Por tal motivo es necesario la implementación de la VPN la cual se realizará basado en software libre en Linux y utilizará el Programa Open VPN; ésta realizará la conexión del establecimiento de salud a la sede administrativa que refleja la seguridad con la que se trabaja el cual es: Active Directory, Firewall en Linux- Squid.

Palabra's clave: VPN, Host, Linux, Open VPN, Active Directory.

ABSTRACT

The Directorate of Integrated Health Networks (DIRIS) Lima Centro is in charge of managing health establishments, which belong to the Ministry of Health - MINSA; is in charge of ensuring the health of the jurisdiction of Lima and San Juan de Lurigancho. Its mission is to provide quality health care to patients in its jurisdiction.

Health establishments provide health services to patients in the Diris Lima Centro jurisdiction; they handle information of vital importance which is used for decision making; the systems they manage are the following: His, Iqhali Admission System, Sien, Arfsis, etc.

Some of these systems work through a server (host), but they are currently migrating to the web platform, however, the problem that establishments constantly have is security, since the users of the computer equipment of the different offices and/or services do not have these security measures, they freely access leisure pages, as well as install applications for non-work use and there is constant loss of information because users uninstall the antivirus, which protects the computer from possible infections.

For this reason, the implementation of the VPN is necessary, which will be based on free software in Linux and will use the Open VPN Program; this will make the connection of the health establishment to the administrative headquarters that reflects the security with which it works, which is: Active Directory, Firewall in Linux-Squid.

Keywords: VPN, Host, Linux, Open VPN, Active Directory.

I. INTRODUCCIÓN

El Ministerio de salud crea el órgano desconcentrado la Dirección de redes integradas de salud (DIRIS) Lima Centro es la encargada de administrar los establecimientos de salud, las cuales pertenecen al Ministerio de Salud – MINSA; es la encargada de velar por la salud e la jurisdicción de Lima y San Juan de Lurigancho. Su misión es la de brindar calidad de salud a los pacientes de su jurisdicción.

Los establecimientos de salud brindan el servicio de salud a los pacientes de la jurisdicción en mención, se maneja información de vital importancia la cual sirve para la toma de decisiones; los sistemas que manejan son los siguientes: HIS, Sistema de Admisión Eghali, Sien, Arfsis, etc.

La dirección de redes integradas de salud Lima Centro (DIRIS Lima Centro). Existe mucha información interna y externa que se ubicará en cada fase de la metodología que connota la importancia de tomar decisiones basadas en información.

Para poder evaluar el aspecto actual de lo que es la red de seguridad de la DIRIS, es necesario comprender cómo está constituido. En efecto, la actual red de seguridad informática está conformada por una red principal que está ubicada en la DIRIS, y, en segundo lugar, están las Red Integral de Salud (RIS 1,2,3,4,5,6,7) las cuales administran a los 74 establecimientos de salud ubicados en la jurisdicción de Lima y San Juan de Lurigancho. Esta red de datos es utilizada por el personal administrativo y asistencial del centro.

La ubicación de la DIRIS Lima Centro se encuentra en el distrito de Lima Centro de Lima, en la Av. Nicolás de Piérola 617, Cercado de Lima. La DIRIS tiene en su jurisdicción los distritos de Lima, y el distrito de San Juan de Lurigancho.

Alguno de estos sistemas funcionan mediante un servidor, pero actualmente se están emigrando a la plataforma web, sin embargo, el problema que tienen los establecimientos constantemente es la seguridad, pues los usuarios de los equipos de cómputos de las diferentes oficinas y/o servicios no cuentan con

medidas de seguridad, estos acceden libremente a páginas de ocio, así como instalan aplicativos de uso no laboral y constantemente hay pérdida de información pues los usuarios desinstalan el antivirus, el cual protege el equipo de posibles infecciones.

Por tal motivo es necesario el diseño de una red privada virtual - VPN, la cual se realizaría basado en software libre en Linux; Ésta realizaría la conexión del establecimiento de salud a la sede administrativa que refleja la seguridad con la que se trabaja el cual es: Active Directory, Firewall en Linux.

Como parte de la estructura del sector salud en el Perú, se encuentran divididos entes gestoras de la salud, la cual tienen a su cargo la disposición y reglamentación de los procesos administrativos y asistenciales de diversos establecimientos de salud. La carga de información que manejan estas entidades es cuantiosa, teniendo en cuenta la complejidad de salud por la que acuden diversos peruanos a su centro de salud más cercano. Muchos pacientes que necesitan una atención rápida se ven confundidos en una maraña de trámites porque los servicios no cuentan con información confiable y actualizada.

Entonces suelen ocurrir problemas como los siguientes:

- No comprender la importancia de la seguridad de las TI o no ser capaz de cuantificar el valor de la reputación de la organización si tiene lugar una brecha de seguridad
- Confiar en soluciones temporales o a corto plazo, que conducen al resurgimiento de problemas anteriores
- Hacer depender la seguridad perimetral únicamente de los cortafuegos de un proveedor
- No gestionar eficaz y eficientemente los aspectos operativos de la seguridad de las TI
- No comprender las consecuencias de una mala seguridad de la información

- Asignar a funciones específicas a personas incompetentes o que no pueden desempeñar sus tareas eficazmente, así como no formar adecuadamente al personal de seguridad de las TI. (Vemuri, 2006, p. 5)

La realidad de seguridad informática de la Dirección de Redes Integradas de Salud Lima Centro, en el contexto de investigación, no es excepcional. Esta entidad de salud cuenta con 74 establecimientos de salud, cada uno de los cuales cuenta con 12 a 50 equipos de cómputo, en la jurisdicción de Lima y San Juan de Lurigancho, los cuales son utilizadas para realizar funciones administrativas, registrar las atenciones a los pacientes, así como realizar la estadística de la atención diaria y demás registros que estos requieran: En este contexto se producen situaciones críticas que perjudican la seguridad de la información, cuyo origen se encuentra en la concepción de la seguridad perimetral. A falta de una integración de la seguridad de estos establecimientos y al menos de una red de seguridad local, las vulnerabilidades empiezan a aparecer, cuando los técnicos administrativos y en algunos casos asistenciales acceden a los equipos de cómputo instalan todo tipo de software de uso no laboral como Facebook, YouTube, radio por internet, etc.; lo cual se traduce en oportunidades de pérdida de información dado que cada equipo.

Por otro lado, la Dirección de Redes Integradas (DIRIS) Lima Centro actualmente tiene una seguridad de dominio y firewall, la cual permite tener los equipos de cómputo de esta entidad correctamente seguro, lo cual no pasa en sus filiales operativas de su jurisdicción. Las computadoras en la DIRIS trabajan conectadas en una red de área local LAN la cual tiene una topología estrella y tiene acceso a internet mediante un servicio de internet fijo o Híbrido de Fibra Coaxial (HFC), lo cual también deriva en otro problema para la seguridad y en consecuencia termina con la pérdida de información y recursos tecnológicos. Últimamente se han reportado en la DIRIS, problemas de seguridad y de virus, como el ransomware (INCIBE, 2017) que realiza un secuestro de datos y solicita un rescate para recuperar su información (este tipo de virus al ser ejecutado aparenta ser un archivo inofensivo imita a otras aplicaciones, es el más común

y representa el 75% del malware). La disponibilidad de planes de contingencia para contrarrestar estos daños, no están configurados y se ejecutan disposiciones paliativas. Esto disminuye la fiabilidad del sistema que redundando en un círculo vicioso donde la información corporativa adolece. En concreto, la situación problemática de los establecimientos de salud consiste en que cada establecimiento cuenta con su internet mas no están interconectado a la sede administrativa, lo cual es un problema para la seguridad en su red de área local (LAN).

Entre las soluciones sugeridas por los especialistas (Vemuri, 2006) ante esta situación giran en torno al ámbito de la gestión, y las políticas de uso que obedecen a la seguridad lógica y a la creación e implementación de sistemas que controlen la seguridad.

Como parte del proceso de investigación, se propone el diseño de red privada virtual (VPN) para optimizar y brindar un mejor manejo de la información entre los locales de la Dirección de Redes Integradas de Salud (DIRIS) Lima Centro.

¿En qué medida el diseño de un Red Privada Virtual (VPN) basado en software libre influye en la optimización del manejo de información de la jurisdicción de la dirección de redes integradas de Salud Lima Centro?

En función de ello se establece lo siguiente objetivo: Determinar la influencia del Diseño de una Red Privada Virtual (VPN) Bajo Software Libre para la optimización de la seguridad de la información entre los establecimientos de la Dirección de Redes Integradas de Salud Lima Centro.

Entre ellos los objetivos específicos: Determinar la influencia del nivel de seguridad, confiabilidad, escalabilidad del Diseño de una Red Privada Virtual (VPN) Bajo Software Libre en el manejo de Información entre los establecimientos de la Dirección de Redes Integradas de Salud Lima Centro

Este trabajo se justifica porque los establecimientos de salud de la red de salud Lima Centro no cuentan con una adecuada infraestructura diseñada de

seguridad, para evitar la pérdida de información y otros problemas que lo acarrea, con esta Implementación se desea mejorar la seguridad de la información la cual maneja diariamente permitiendo al establecimiento estar conectado de manera adecuada y segura, mediante la VPN a la sede central para así tener todas las medidas de seguridad con la que cuenta (Dominio, Firewall).

Realizando estas implementaciones se permitirá la navegación web de los equipos de cómputo de una manera segura, evitando el ingreso a paginas no institucionales esto permitirá la mejora en la velocidad del internet dado que cuenta con una velocidad básica. Las ventajas son las siguientes: Seguridad en la red de área local (LAN); el firewall nos permitirá mantener los equipos de cómputo navegando en páginas institucionales evitando el mal uso del internet (Speedy); administración de manera óptima, segura y centralizada mediante cuentas de usuario; al estar conectado los equipos de cómputo a un Dominio se evitará la instalación de diversos programas de uso no institucional.

II. MARCO TEÓRICO

Entre los principales antecedentes se cuentan con los siguientes:

Ruiz y Delgado (2018) en su tesis de maestría *Implementación de una solución de seguridad perimetral Open Source en la Red Telemática de la Universidad Nacional Pedro Ruiz Gallo*; en esta investigación se trabaja una solución al tema de la seguridad perimétrica a partir de un software libre. Desde el primer hasta el cuarto capítulo se plantea la solución específica para la realidad de una institución educativa. Este estudio es importante para el trabajo relacionado con los softwares libres, tanto de la planeación hasta el monitoreo de la red.

Asimismo, **Celis (2018)** en su tesis de maestría titulada, *Plan de seguridad de la información aplicado a la Central Hidroeléctrica Carhuaquero*, logran sustentar la importancia del manejo de la seguridad de la información y su impacto para las organizaciones. La seguridad es una inversión importante para poder trabajar dentro de las organizaciones; es un tema estratégico hoy en día, por lo que un ataque a este tema puede perjudicar toda la organización, por ello que se necesita tener políticas claras para poder llevar el proceso.

En conclusión. Vemos cuál es la importancia de tener un tener planificada la seguridad de la información el cual comprende en tener las políticas y herramientas necesarias para dicho monitoreo y control de tal manera de mitigar y brindar resguardo a la información y a la infraestructura de la red de equipos. Para ello están basando la seguridad en los estándares ISO 27001 e ISO 31000.

Por otro lado, **Joaquín (2020)** en su tesis de grado, *Implementación de Firewall Para el Control de Servicio de Internet En la Filial Chanchamayo De la Universidad Peruana los Andes. Huancayo – Perú* indica que las soluciones tecnológicas son las mejores opciones para poder garantizar el control de internet. En el sector educación existe mucha dinámica de parte de los

estudiantes donde se necesitan mayor control y gestión. En ese sentido se desarrolla una estrategia en top down capaz de poder desarrollar un firewall importante para poder soportar la demanda y los accesos a la información a la cual se remonta el uso estudiantil.

En resume se puede apreciar la importancia de tener un firewall correctamente funcional y con las reglas correspondientes en las diferentes capas de acuerdo a las necesidades, alumnos, docentes y personal administrativo, con ello se tiene un mejor uso de la internet y despliegue de políticas de seguridad.

Seguidamente, **Bolaños (2018)** en su tesis de maestría, *Diseño de la arquitectura de seguridad perimetral de la red informática en la industria de licores del Valle* a partir del cual se desarrolla una arquitectura tecnológica capaz de poder mantener la seguridad informática. A través de este trabajo se diseñó un cerco perimetral importante para la empresa donde se desarrolla de manera sistemática la cultura de uso de la tecnología. El trabajo inicia con la recopilación de la demanda de la organización, para lo cual se procedió diseñar el esquema de seguridad, y se logró un trabajo de formación de cultura de uso en los trabajadores.

En conclusión. En esta investigación se dejan las bases claras de los conceptos de seguridad perimetral, se analiza su arquitectura y a su vez se diseña la arquitectura ajustándose a las necesidades requeridas por la institución.

Asimismo, **Díaz (2017)** en su tesis de maestría, *Diseño de prototipo de un Modelo de seguridad perimetral con LDAP*, se propuso realizar la implementación de la seguridad en la red perimetral, esta es necesaria debido a las inseguridad que se presentan constantemente en las entidades, esta es diseñada para poder dar seguridad a los sistemas informáticos y evitar la infiltración y/o robo de información en este trabajo se realiza la solución que está basada en LDAP la cual permite la autenticación de los usuarios para la

conexión en la que se dan restricciones permitiendo así limitar y mantener segura la información.

Se obtuvo mediante esta implementación garantizar la seguridad como tenemos en conocimiento actualmente las tecnologías se han convertido en una necesidad para toda organización, cabe mencionar que el modelo de seguridad hoy en día es fundamental para toda empresa, pues es lo primero que se debe de pensar dado con los ataques de virus que hay actualmente.

En conclusión, con la implementación de LDAP se demostró el uso que nos puede brindar, su ventaja, su capacidad el fácil manejo para la administración y su seguridad nos garantiza una política de seguridad de acorde a lo actual, cabe mencionar que es una herramienta segura para todo tipo de proyecto de seguridad.

Entre los principales conceptos se encuentran el VPN (Virtual Private Network), que se entiende como una tecnología de red que se utiliza para conectar una o más computadoras a una red privada utilizando Internet. Las empresas suelen utilizar estas redes para que sus empleados, desde sus casas, hoteles, etc., puedan acceder a recursos corporativos que, de otro modo, no podrían. Sin embargo, conectar la computadora de un empleado a los recursos corporativos es solo una función de una VPN. (Groujon, 2012, p. 35)

También está la Red Troncal, que es una red que se utiliza para interconectar otras redes, que es una forma de permitir la conexión a múltiples redes o sectores. Por lo general, cuentan con un alto desplazamiento y permiten un mayor rendimiento que las conexiones LAN corporativas. Para conectar múltiples segmentos de red a una sola red troncal, se requieren dispositivos adicionales para acomodar diferentes señales, conectores, cables, protocolos, etc. La red central existe principalmente como un canal que permite que las partes se comuniquen entre sí. La configuración de un edificio de varios pisos requiere una sección horizontal que conecte todas las estaciones de trabajo en

cada piso y una columna vertical desde la parte superior del edificio hasta la planta baja que conecte todos los segmentos. (Lobos, 2012, p. 69)

Atención en Salud

Se hace referencia a la atención de la salud (o asistencia) como el conjunto de procesos mediante los cuales se brinda atención y servicios de atención a la salud a un individuo, familias, comunidad y/o población conjunta.

El objetivo de la atención sanitaria es contribuir a la salud garantizando una gama de servicios de atención que permitan a las personas mantener su salud. Evitar el deterioro de la salud de la población. Restaurar la salud a quienes han caído enfermos para que puedan recuperarse. Detectar lo más rápido posible y evitar un empeoramiento del estado del paciente, especialmente de aquellos para los que no se dispone de tratamiento conocido. Reducir el dolor y reducir el sufrimiento de los pacientes con enfermedades mortales incurables. (Tobar, 2013).

Gestión de la información en salud

La gestión de la información en la salud implica una serie de criterios de calidad para que funcionen como debe ser. Tengamos en cuenta que las decisiones de salud están basadas en información, y estas deben ser usadas con responsabilidad y con eficacia. No obstante, como señala (Restrepo & López, 2015),

Un sistema de información competente no basta por sí solo, debe ir acompañado de una cultura adecuada de generación, procesamiento, análisis y utilización de la información (p. 56)

Cultura de la seguridad de la información

Parte esta cultura es la seguridad de información, que muy pocas veces es visto como una necesidad por la Alta Dirección, pero que desde el ámbito privado se ha desarrollado mucho. Esta problemática está contextualizada en

un problema estructural de gestión que, a ojos de las autoras antes citadas, se da de la siguiente forma:

Las empresas u organizaciones y entre ellas las del sector salud (lentas en la introducción de nuevas tecnologías), ven al área de informática como un mal necesario dentro de la organización, ya que generalmente solo representa gastos y no es palpable el retorno de inversión en informática. Esto sucede generalmente porque en el crecimiento de la organización no se tomó en cuenta al departamento de Tecnología Informática (IT) como parte importante de la planeación estratégica, lo cual indica que no asigna un papel importante en el rol de la empresa, llevando a que los departamentos de informática pasen a un segundo plano en la empresa u organización, lo cual limita su crecimiento y recursos. (p. 56)

Desde los sistemas de gestión en salud, ya se reconocía en 1999, la importancia de la atención a las tecnologías y sistemas para el control de la información. Como señala la (OMS, 1999), la tecnología en el entorno de la salud implica muchos cambios importantes desde la cadena de suministros, la gestión de proyectos, entre otros puntos principales.

III. METODOLOGÍA

3.1. Tipo y Diseño De La Investigación

El tipo de investigación es descriptivo en las cuales se identifican las características de una realidad de la aplicación de un sistema VPN en un contexto de salud, y la forma como se realiza el proceso de implementación. Desde esta perspectiva, el diseño de investigación es cuantitativo (Ñaupas et al., 2018), en la cual se destaca la comprobación de una hipótesis a partir de un marco aplicativo.

3.2. Variables y Operacionalización

Las variables de investigación son las siguientes:

Tabla 1. Variable Independiente: Red Privada Virtual (VPN) Bajo Software Libre

Definición Conceptual	Definición Operacional	Dimensión
VPN es una tecnología de red que permite una extensión segura de la red local (LAN) sobre una red pública o no controlada como Internet, mediante un proceso de encapsulación y de encriptación, de los paquetes de datos a distintos puntos remotos mediante el uso de unas infraestructuras públicas de transporte. Permite que la computadora en la red envíe y reciba datos sobre redes compartidas o públicas como si fuera una red privada. (González, 2014, p. 3)	Variable que expresa una herramienta de conexión entre computadoras a través de una red privada por internet y cuenta con tres dimensiones: seguridad, confiabilidad y escalabilidad.	Seguridad
		Confiabilidad
		Escalabilidad

Tabla 2. Variable Dependiente: Seguridad de información

Definición Conceptual	Definición Operacional	Dimensión	Indicador
Según ADEA es una es las soluciones para evaluar todo tipo de riesgos desde la ISO 27001 según Baldecchi es un SGSI 10, la seguridad de la información queda definida por tres atributos (Figuroa, celiz; 2018; p11)	La variable relacionada a una característica de la información que se transmite a través de las computadoras de una red y sus dimensiones son extensión de conectividad, mejoras en la seguridad, topología de red e infraestructura y medios de uso	Confidencialidad: es la propiedad de prevenir que se divulgue la información a personas o sistemas no autorizados. (Figuroa,celiz; 2018; p11)	confidencialidad de la información
		Integridad: es la propiedad que busca proteger que se modifiquen los datos libres de forma no autorizada. (Figuroa,celiz; 2018; p11)	Integridad de la información
		Disponibilidad: es una característica, cualidad o condición de la información que se encuentra a disposición de quien tiene que acceder a esta, bien sean personas, procesos o aplicaciones. (Figuroa, celiz; 2018; p11)	Disponibilidad de la información

3.3. Población, Muestra y Muestreo

La población total está constituida por 74 establecimientos de salud de las DIRIS Lima Centro, que constituyen cinco distritos de Lima Metropolitana. La muestra elegida para el estudio fue en el centro de salud Materno Infantil El Porvenir para lo cual fue necesario un muestreo de los principales participantes de centro, para la toma de muestra fue necesario 10 personas la cual nos evaluarán mediante un cuestionario que le permite responder en un pre test y posterior a la instalación de la solución tecnológica un post test. Con ello nos permite realizar el reporte estadístico.

Tabla 3. Cuadro de participantes del cuestionario

ITEM	DNI	NOMBRES Y APELLIDOS	CARGO	CONDICIÓN
1	10719918	CHUQUIMAJO MORENO HUMBERTO	TECNICO/A ASISTENCIAL POR ADECUACION R.M.421	NOMBRADO
2	07086374	COSSI CARRASCO WILLIAM BENJAMIN	TECNICO/A ASISTENCIAL POR ADECUACION R.M.421	NOMBRADO
3	09921135	MORCILLO DE ELLIOTT ANA MARIA	TECNICO/A ASISTENCIAL POR ADECUACION R.M.421	NOMBRADO
4	07409340	PADILLA RODAS CARLOS GONZALO	TECNICO/A ASISTENCIAL POR ADECUACION R.M.421	NOMBRADO
5	09451297	RAMOS ROCHA TERESA	2689-TECNICO/A ADMINIST. I	NOMBRADO
6	07475128	ROJAS BEST LAURA MARIA DEL PILAR	AUXILIAR ASISTENCIAL	NOMBRADO
7	08126505	SALAS ARIAS JUAN CARLOS	2689-TECNICO/A ADMINIST. I	NOMBRADO
8	06717981	VERA BELLI ALEJANDRO EDUARDO	TECNICO/A ASISTENCIAL POR ADECUACION R.M.421	NOMBRADO
9	08905917	ZAPATA PALACIOS GERARDO SIMON	TECNICO/A ASISTENCIAL POR ADECUACION R.M.421	NOMBRADO
10	07637138	ARRIETA CUZCANO ANA MARIA	TECNICO ADMINISTRATIVO	CAS

3.4. Técnicas e Instrumentos de Recolección de Datos

La técnica que se utilizó en el trabajo de estudio fue la encuesta, la cual fue construida para la variable dependiente y Red Privada Virtual (VPN) Bajo Software Libre del área en la Dirección de Redes Integradas de Salud de Lima Centro. Para la recolección de datos se empleó el formulario físico de las cuales de tomo a una pequeña población para medir los resultados de nuestra hipótesis. Esta encuesta se basó en una variedad de preguntas el cual tuvo la aprobación de un experto con el fin de recabar información pertinente de las personas, permitiéndonos observar, y aislar los problemas relevantes de nuestro estudio.

3.5. Procedimientos y Resultados

Para obtener los resultados del proyecto este estudio fue desarrollado en base a un puesto de salud el más cercano con el cual se recabo la siguiente información.

Para obtener nuestros resultados nos apoyamos de las dimensiones de la variable dependiente el cuales son, integridad y disponibilidad

3.5.1. Integridad

Este es el primer indicador de nuestra variable independiente “Seguridad de la información” que estamos midiendo y mostrando en las estadísticas, es donde demostramos que tipo de hipótesis obtenido.

Tabla 4. 10 encuestas Pre-Test y 10 encuestas Post-Test para el muestreo en la estadística

	Válido		Casos Perdidos		Total	
	N	Porcentaje	N	Porcentaje	N	Porcentaje
Nota_Pre_Test	10	100,0%	0	0,0%	10	100,0%
Nota_Post_Test	10	100,0%	0	0,0%	10	100,0%

En el resumen podemos el valor N el cual es el número de muestras obtenidas para este indicador que son 10.

Tabla 5. N es la cantidad de encuestas tomadas en el PRE y POST TEST

	Kolmogorov-Smirnov ^a			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
Nota_Pre_Test	,172	10	,200*	,917	10	,330
Nota_Post_Test	,200	10	,200*	,953	10	,703

*. Esto es un límite inferior de la significación verdadera.

a. Corrección de significación de Lilliefors

Para las pruebas de normalidad optamos por utilizar *shapiro-wik* porque nuestra muestra es de 10 encuestas.

Para obtener el resultado el Sig. Tiene que ser mayor al 0.05 para este caso tenemos un resultado mayor en ambos casos tanto para el pre y post test, eso quiere decir que nuestros resultados son paramétricos. Para ello

tenemos que realizar las pruebas de T DE STUDENT, para ello mostramos el siguiente cuadro.

Figura 1. Histograma 1

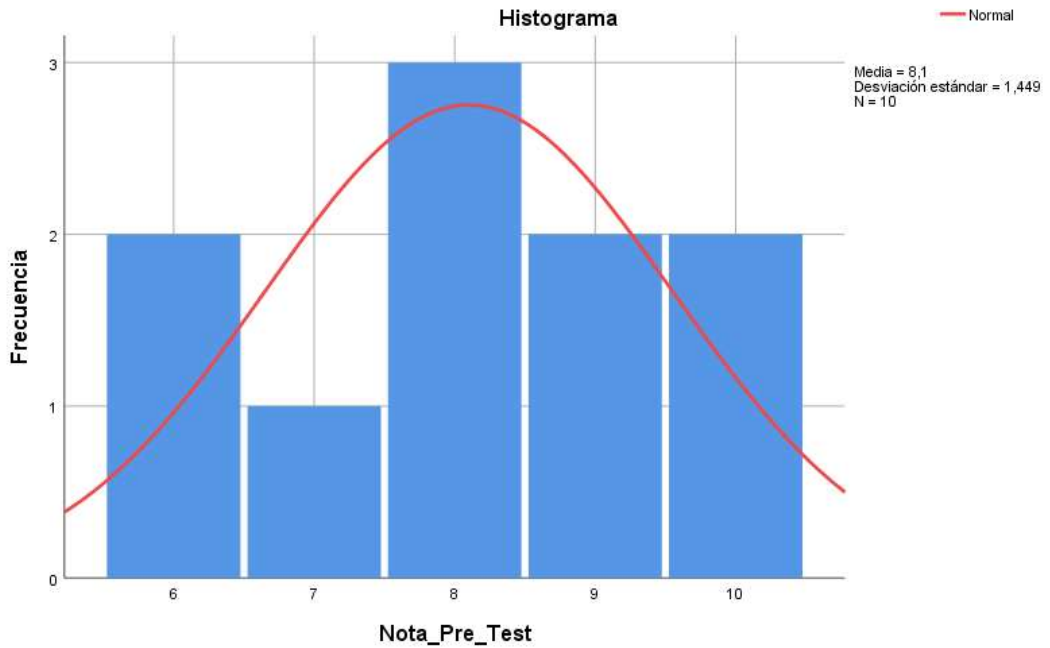


Figura 2. Histograma 2

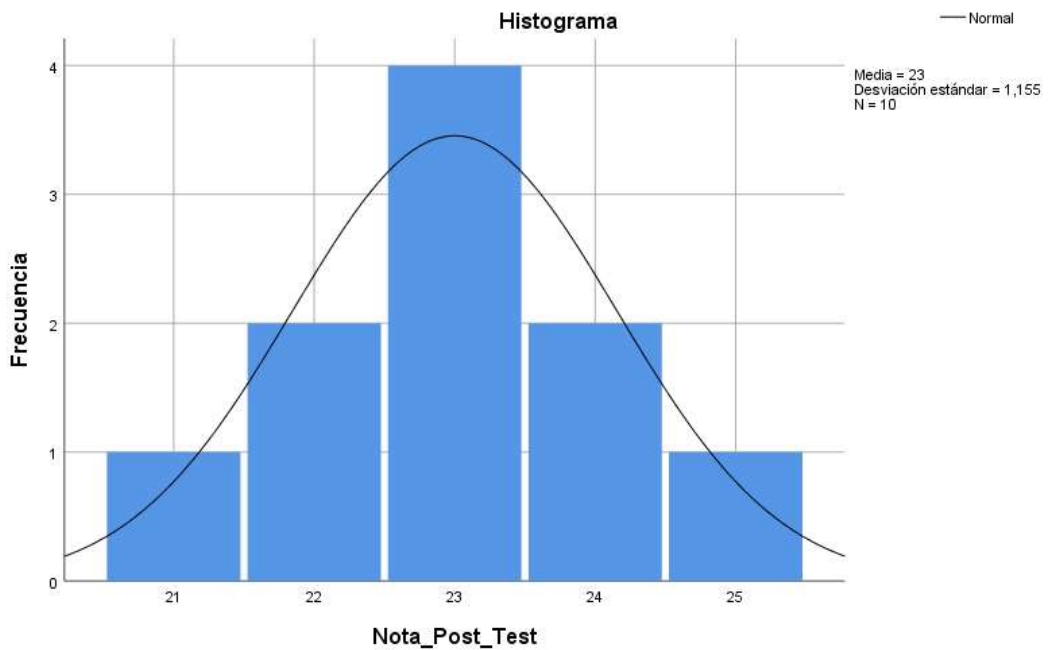


Tabla 6. Pruebas de muestras emparejadas

		Prueba de muestras emparejadas							
		Diferencias emparejadas					t	gl	Sig. (bilateral)
		Media	Desv. Desviación	Desv. Error promedio	95% de intervalo de confianza de la diferencia				
					Inferior	Superior			
Par 1	Nota_Post_Test - Nota_Pre_Test	14,900	1,524	,482	13,810	15,990	30,920	9	,000

Para los resultados con T-Student el valor de Sig. Tiene que ser menor al 0.05 y lo obtenido en nuestros resultados es .000 lo cual nos indica que se acepta la hipótesis de investigación y se rechaza la hipótesis nula considerando un grado de confianza del 95%

3.5.2. Disponibilidad

Este es el segundo indicador de nuestra variable independiente “Seguridad de la información” que estamos midiendo y mostrando en las estadísticas, es donde demostramos que tipo de hipótesis obtenido.

Tabla 7. Resumen de procesamiento de datos

	Resumen de procesamiento de casos					
	Válido		Perdidos		Total	
	N	Porcentaje	N	Porcentaje	N	Porcentaje
Nota_Pre_Test	10	100,0%	0	0,0%	10	100,0%
Nota_Post_Test	10	100,0%	0	0,0%	10	100,0%

En el resumen podemos el valor N el cual es el número de muestras obtenidas para este indicador que son 10.

Tabla 8. Pruebas de normalidad

	Kolmogorov-Smirnov ^a			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
Nota_Pre_Test	,224	10	,168	,942	10	,573
Nota_Post_Test	,274	10	,032	,774	10	,007

a. Corrección de significación de Lilliefors

Para las pruebas de normalidad optamos por utilizar *shapiro-wilk* porque nuestra muestra es de 10 encuestas.

Para obtener el resultado el Sig. Tiene que ser mayor al 0.05 para este caso tenemos un resultado mayor para el pre y menor para post test, eso quiere decir que nuestros resultados son no paramétricos. Para ello tenemos que realizar las pruebas de WILCOXON, para ello mostramos el siguiente cuadro.

Figura 3. Histograma 3

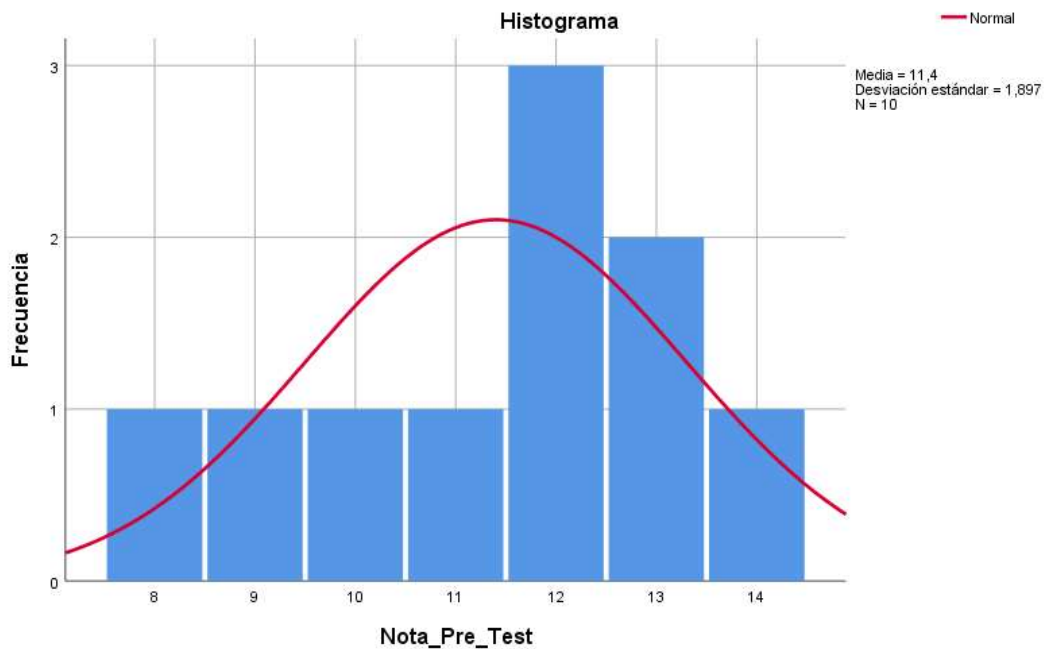


Figura 4. Histograma 3

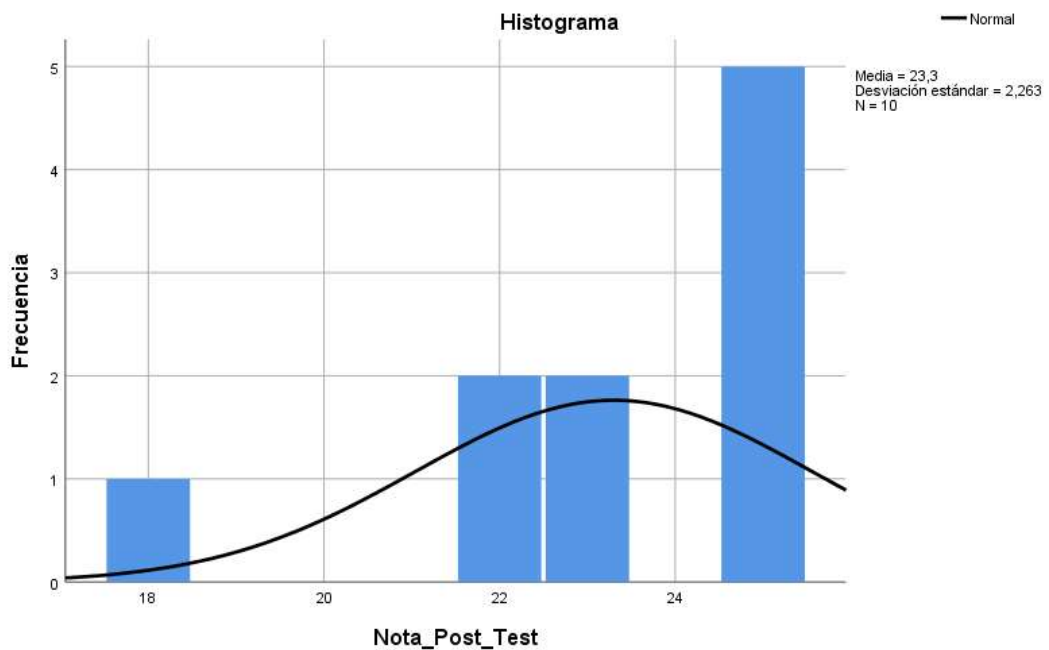


Tabla 9. Estadísticos de prueba

Estadísticos de prueba^a

	Nota_Pre_Te st- Nota_Post_T est
Z	-2,812 ^b
Sig. asintótica(bilateral)	,005

a. Prueba de rangos con signo de Wilcoxon
b. Se basa en rangos positivos.

Para los resultados con Wilcoxon el valor de Sig. Tiene que ser menor al 0.05 y lo obtenido en nuestros resultados es .005 lo cual nos indica que se acepta la hipótesis de investigación y se rechaza la hipótesis nula considerando un grado de confianza del 95%.

3.6. Método de Análisis de Datos

Para poder realizar el análisis de datos se utilizó el software estadístico SPSS, aquí se inserta los valores finales obtenidos por las encuestas realizadas.

uno de los pasos es tener los análisis del Pre_test y Post_Test con esto podemos saber si tipo de estadística obtendremos, para nuestro caso al ser 10 tipos de encuestas por tal motivo utilizaremos a Shapiro-Wilk.

En base a los gráficos estamos tendremos un análisis de situaciones no paramétricas.

Si esta significancia de acuerdo a las pruebas de Xilcoxon de los cuales en este caso al obtener un valor menor a 0.05 se acepta que la hipótesis es de investigación.

3.7. Aspectos Éticos

Desde las distinciones conductuales o éticas, esta investigación cumplirá con las disposiciones de confidencialidad de la información y discreción de identidad por cada uno de los trabajadores de los establecimientos de salud de la Dirección de Redes Integradas de Salud Lima Centro; consentimiento informado (Delgado, 2002), los permisos y el derecho a la pertenencia intelectual de los autores de todo lo escrito y citado en este documento en la cual se tuvo en consideración lo que se señala en APA7.

A nivel cognitivo, este estudio buscó aportar al conocimiento acerca del impacto de la red VPN en el ámbito de la Dirección de Lima Centro en la seguridad de información. En lo procedimental, el trabajo cumplirá con lo dispuesto por la Universidad, para los proyectos de grado de la Maestría en Ingeniería de Sistemas.

A nivel metodológico, este estudio desarrollará un proceso aplicativo desde un enfoque con el fin de aportar a la institución de salud resultados, desde la instalación del VPN.

3.8. Aspectos Administrativos

La elaboración del presente proyecto de investigación se realizará de acuerdo a los reglamentos estipulados por la universidad, además de atender aspectos propios relacionados a recursos humanos, tecnológicos y materiales.

En relación con los Recursos Humanos a utilizarse en la investigación son los siguientes:

- a. Investigadores (02).
- b. Asesor designado por la universidad de posgrado, para guiar al investigador el tiempo que dure la investigación (01).
- c. Revisor especialista asignado por la universidad (01).
- d. Validadores expertos (02) independientes que no pertenezcan a la universidad, y que tengan estudios de Maestría o doctorado en ingeniería de sistemas.
- e. Los trabajadores que componen la muestra (74).
- f. Estadístico especialista en el procesamiento de los datos (01).

Tabla 10. Recursos Humanos sin costo monetario

Cantidad	Descripción	Sin aporte monetario
1	Investigadores: Daniel Lazarte y Giancarlo Silva	Ejecutantes de la investigación.
1	Asesor de la universidad: Ing. Quiñones Nieto, Yamil Alexander	Asesor y quien realiza el seguimiento al investigador desde que inicia hasta que termine la investigación.
1	Revisor de la Universidad	Realiza la revisión constante del proyecto para su aprobación correspondiente.
2	Validadores (expertos)	Para la validez y fiabilidad del instrumento.
74	Trabajadores responsables de la informática en los establecimientos de salud	Personal que forma parte para ser encuestados.

Se cuenta con un especialista estadístico para el proceso de datos hallados. En este caso si se le retribuirá económicamente con aporte dinerario por la labor que realizará en apoyo al investigador con el monto de S/.200.00 soles.

Tabla 11. Recursos Humanos con costo

Unidad	Descripción	Aporte monetario
1	Estadista especializado	S/.200.00 soles

Respecto a los recursos tecnológicos que se utilizó se tiene 02 computadoras Core i5 además de sus equipos celulares, los cuales ya contaban con anterioridad los investigadores; respecto a otros equipos como, una cámara web además de un micrófono se tuvo que renovar para participar en las clases de tutorías que impartió el asesor que ascendió a un monto de S/.145.00 soles.

Tabla 12. Recursos Tecnológicos

Unidad	Descripción	Costo promedio
1	Computadora	S/.800.00
1	Cámara web	S/.150.00
1	Micrófono	S/.80.00
1	Celular	S/4.00.00
Total		S/.1430.00

Elaboración propia

Entre los otros gastos adicionales se tuvo de S/.147.50 soles para, los recursos materiales esta los escritorios, lapiceros, papel bond, archivador, además se requirió recursos económicos para el pago de internet y mejorar los megas.

Tabla 13. Otros gastos adicionales en el proceso de la investigación

Descripción	Cantidad	Costo por unidad s/.	Total, costo s/.
Lapicero	6	S/. 1.50	S/. 9.00
Papel bond (millar)	1	S/.12.50	S/.12.50
Archivador	1	S/. 6.00	S/. 6.00
Internet		S/. 120.00	S/.120.00
Costo Total			S/.147.5

Elaboración propia

Tabla 14. Total, de gastos incurridos durante el desarrollo del proyecto

Descripción	Total
Recurso Humano (estadista)	S/. 200.00
Recursos tecnológicos	S/. 1030.00
Otros adicionales	S/. 147.50
Costo total	S/. 1377.50

Elaboración propia

3.9. Financiamiento

Para la financiación, en su totalidad fue cubierto en este caso el investigador desde el inicio hasta culminar la investigación para su aprobación por la universidad respectiva.

3.10. Cronograma

Es el tiempo de ejecución del proyecto de investigación.

3.11. Cronograma de Ejecución

Tabla 15. Cronograma

		cronograma de actividades											
Fases	Procesos	enero				febrero				marzo			
		SEMANA1	SEMANA 2	SEMANA 3	SEMANA 4	SEMANA1	SEMANA 2	SEMANA 3	SEMANA 4	SEMANA1	SEMANA 2	SEMANA 3	SEMANA 4
1 Analizar Requerimientos	Analizar metas del negocio	■	■										
	Analizar metas técnicas	■	■										
	Analizar red existente	■	■										
	Analizar tráfico existente	■	■										
2 Desarrollar Diseño Lógico	Diseñar topología de red			■	■								
	Diseñar modelos de direccionamiento y hostnames			■	■								
	Seleccionar protocolos para Switching y Routing				■	■							
	Desarrollar estrategias de seguridad					■	■						
	Desarrollar estrategias de administración de red						■	■					
3 Desarrollar Diseño Físico	Seleccionar tecnologías y dispositivos para redes de campus							■	■				
	Seleccionar tecnologías y dispositivos para redes empresariales								■	■			
4 Probar, optimizar y documentar diseño	Probar el diseño de red									■	■		
	Optimizar el diseño de red										■	■	
	Documentar el diseño											■	■

Fuente: Elaboración propia

IV. RESULTADOS

Para el desarrollo de la presente investigación se tomará en cuenta la metodología Top-Down Network Design (que por cierto ha sido aplicado a diversos sectores incluido la salud) para el diseño de redes de la empresa Cisco Systems. Esta metodología tiene criterios importantes para su aplicación. Desde la perspectiva de la (UNID, 2013) existen aspectos importantes al tomar la decisión de aplicar esta metodología

Otro punto importante para comprender esta metodología según la propia metodología Top Down son las mejoras que brinda a las organizaciones que la implementan:

Mejora la comunicación entre diseñadores (actuales y futuros), mejora el control de calidad, ya que detecta defectos en las primeras etapas del diseño, cuando la reparación es más fácil y menos costosa; Mejorar la eficiencia de los diseñadores. Reorganizar tareas de diseño y ejecutar tareas en paralelo en lugar de crear dependencias secuenciales; Reducir la necesidad de una verificación exhaustiva del estado final del diseño. (Top Down Design, 2004 en (UNID, 2013), pp. 11 - 12)

4.1. Fases de la Metodología Top-Down Network Design

La metodología Top Down Design para el diseño del proyecto es de 4 fases

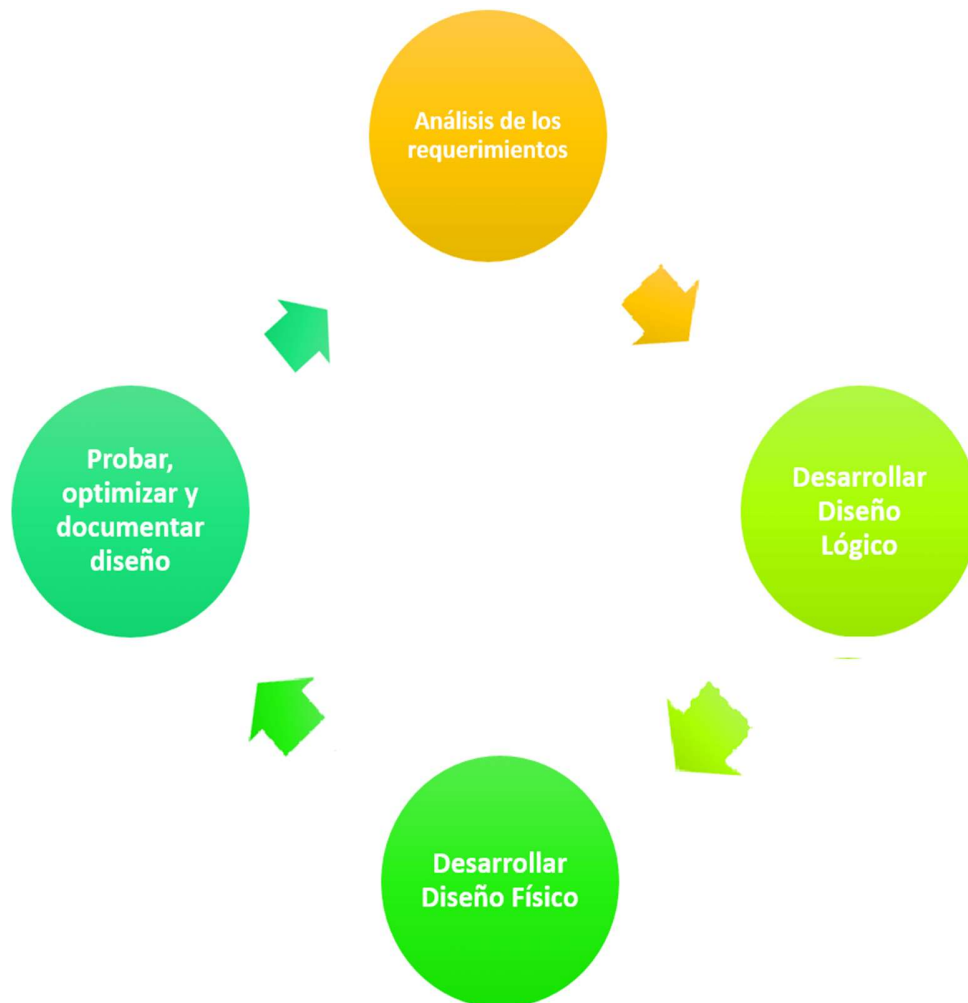
Fase 1: Analizar Requerimientos

Fase 2: Desarrollar Diseño Lógico

Fase 3: Desarrollar Diseño Físico

Fase 4: Probar, optimizar y documentar diseño

Figura 5. Proceso de fases de la metodología Top Down



4.2. Fases y entregables de la Metodología TOP DOWN DESIGN

Tabla 16. Metodología Top Down

Fases	Procesos	Entregables
Fase 1: Analizar Requerimientos	Analizar metas del negocio	<ul style="list-style-type: none"> ▪ Diagnóstico del estado actual de los equipos, personal y servicios de los cuales disponen la DIRIS y su jurisdicción ▪ Perfil de la DIRIS; objetivos enfocados al desarrollo del TI
	Analizar metas técnicas	<ul style="list-style-type: none"> ▪ Diagnóstico de las políticas y acciones de seguridad tecnológica de la DIRIS.
	Analizar red existente	<ul style="list-style-type: none"> ▪ Topología de la red física de la oficina central ▪ Topología de las redes sucursales ▪ Listado de dispositivos de red ▪ Análisis de infraestructura física
	Analizar tráfico existente	<ul style="list-style-type: none"> ▪ Informe de Tráfico de datos: servidor DNS, servidor de base de datos, servidor de aplicaciones web, servicio de internet,

Fase 2: Desarrollar Diseño Lógico	Diseñar topología de red	<ul style="list-style-type: none"> • Diseñar el medio de transmisión • Mapeo de usuarios • Puntos de red • Mapeo de equipos de red • Características de Cableado Estructurado
	Diseñar modelos de direccionamiento y hostnames	<ul style="list-style-type: none"> • Segmentación de direccionamiento lógico • Direccionamiento IP
	Seleccionar protocolos para Switching y Routing	<ul style="list-style-type: none"> • Protocolos LAN • Protocolo de ruteo
	Desarrollar estrategias de seguridad	<ul style="list-style-type: none"> • Esquema de zona desmilitarizada (DMZ)
	Desarrollar estrategias de administración de red	<ul style="list-style-type: none"> • Plan de mantenimiento a los dispositivos de red, servidores e incluso UPS • Acta de constitución del proyecto
Fase 3: Desarrollar Diseño Físico	Seleccionar tecnologías y dispositivos para redes de campus	<ul style="list-style-type: none"> • Estándares para la adquisición de tecnologías y dispositivos
	Seleccionar tecnologías y dispositivos para redes empresariales	<ul style="list-style-type: none"> • Análisis de factibilidad.
Fase 4: Probar, optimizar y documentar diseño	Probar el diseño de red	<ul style="list-style-type: none"> • Implementación de la red
	Optimizar el diseño de red	
	Documentar el diseño	

Fuente: Saavedra (2015)

4.3. Ubicación del Desarrollo Tecnológico

En este apartado se brinda la información preliminar acerca del diseño de la VPN basado en software libre en la Dirección de Redes Integradas de Salud Lima Centro (DIRIS LIMA CENTRO). Existe mucha información interna y externa que se ubicará en cada fase de la metodología que connota la importancia de tomar decisiones basadas en información.

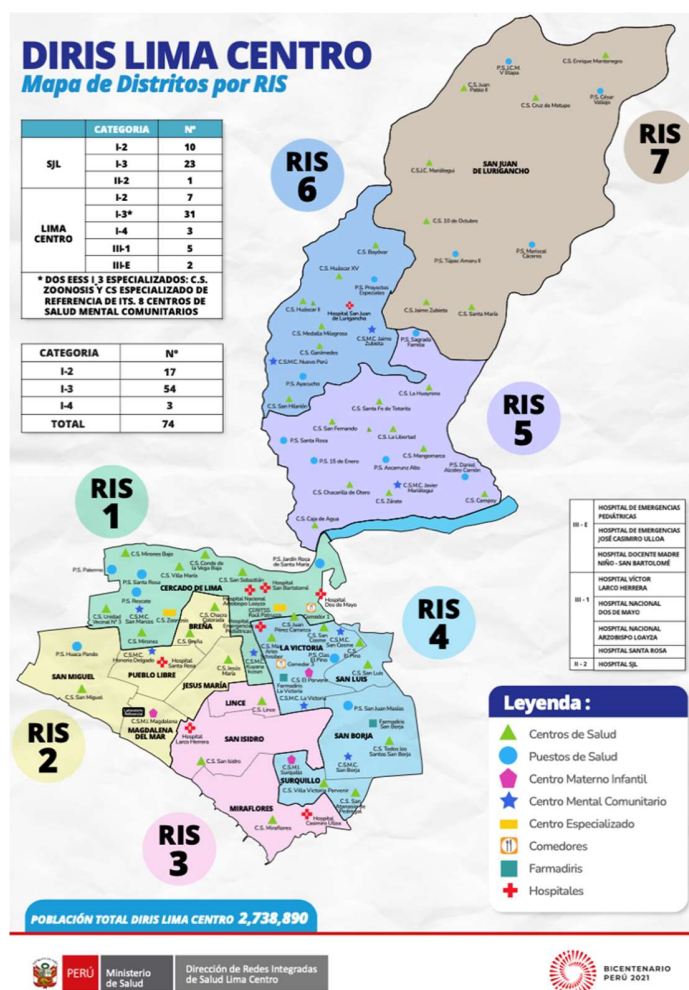
Para poder evaluar el aspecto actual de lo que es la red de seguridad de la DIRIS, es necesario comprender cómo está constituido. En efecto, la actual red de seguridad informática está conformada por una red principal que está ubicada en la DIRIS, y, en segundo lugar, están las RIS N° 1,2,3,4,5,6,7 que velan por los 74 establecimientos de salud ubicados en la jurisdicción de Lima y de San Juan de Lurigancho. Esta red es utilizada por el personal administrativo y asistencial.

La ubicación de la DIRIS Lima Centro está en el distrito de Cercado de Lima, en Av. Nicolás de Piérola 617, Cercado de Lima 15001. La DIRIS tiene en su jurisdicción los distritos de Lima, y el distrito de San Juan de Lurigancho.

Figura 6. Ubicación de la Dirección de Redes Integradas de Salud de Lima Centro



Figura 7. Jurisdicción de la Dirección Regional de Lima Centro



4.4. Fase 01: Análisis de Requerimiento

4.4.1. Actualizar Metas del Negocio

En esta fase identificamos los objetivos y restricciones del negocio, y los objetivos y restricciones técnicos del cliente.

La implementación de servicios de red conlleva a brindar un mejor servicio a los usuarios finales por ello es necesario Implementar una serie de soluciones para la correcta administración de la red.

Lista de metas de negocio:

- Reducir Costos de operación.
- Mejorar las comunicaciones.
- Integrar las redes LAN.
- Movilidad.
- Seguridad de la información.
- Robustez (tolerancia a fallos).
- Las redes deben ofrecer un retardo bajo, requerido para aplicaciones en tiempo real como VoIP.

Lista de restricciones de negocio:

- Presupuesto para la compra de nuevos equipos de comunicaciones (Servidores, Switches, Licencias, etc.).
- Falta de personal técnico disponible.
- Falta de políticas sobre manejo y documentación sobre la administración de la red corporativa.

4.4.2. Diagnóstico del estado actual de los equipos, personal y servicios de los cuales dispones la Diris Lima Centro y su jurisdicción.

Esta presenta acta se realizó previa coordinación de una visita para el levantamiento de algunos puntos (ANEXO 3). Perfil de la DIRIS; objetivos enfocados al desarrollo del TI. Esta presenta acta se realizó previa coordinación de una visita para el levantamiento de algunos puntos (ANEXO 4).

4.4.3. Analizar Metas Técnicas

No se han encontrado hasta el momento documentos oficiales de metas técnicas. Los únicos avances han sido a nivel de políticas generales como los procesos de soporte que están enfocados solamente a desarrollados dos aspectos:

- Gestión de datos
- Gestión de soporte técnico

Se concluye que no hay una mirada ni acciones estratégicas de este tema en la DIRIS, por lo tanto, hay falencias en la gestión y por lo mismo en el funcionamiento de esta red. Esta es una oportunidad para poder implementar una solución importante en medio de estas debilidades y amenazas.

4.4.3.1. Diagnóstico de la políticas y acciones de seguridad tecnológicas de la Diris.

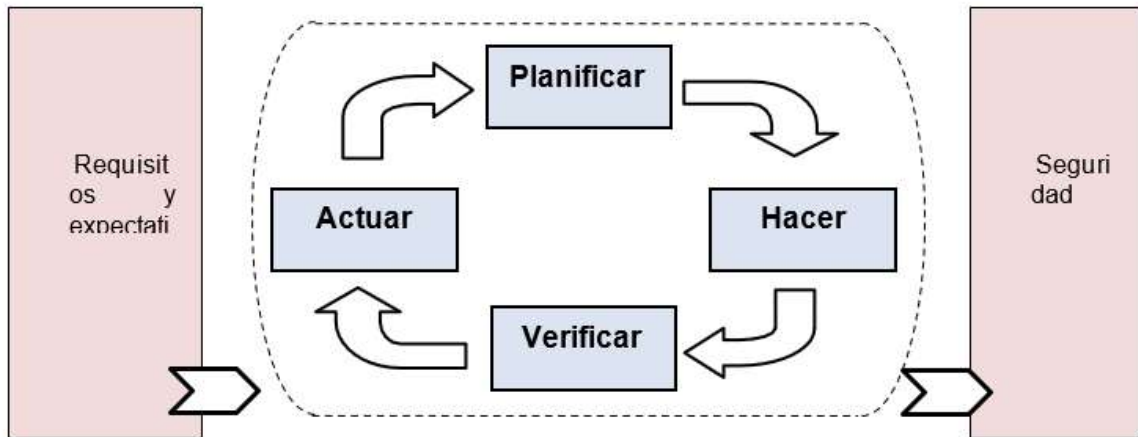
Para conocer el sistema de seguridad es necesario conocer las etapas de acción que la integran y su funcionamiento desde la planificación de este sistema hasta su materialización. Parte del lenguaje que se utiliza para poder conocer sus etapas son usos de las normas estandarizadas de calidad, ya que esas son referencias importantes para el manejo de las herramientas y acciones.

Esta presenta acta se realizó previa coordinación de una visita para el levantamiento de algunos puntos (ANEXO 5).

4.4.3.2. Procesos de un sistema de seguridad

Los procesos que contienen al sistema integral de seguridad son los siguientes:

Figura 8. Ciclo PHVA



La explicación del modelo PHVA tienen las siguientes consideraciones:

Tabla 17. Fases de la mejora continua

Planificar (Establecer el SGSI)	Es el proceso donde se estipulan las políticas y las lógicas de gestión del sistema.
Hacer (Implementar y operar el SGSI)	Se relaciona con la aplicación óptima de los procesos y el control de los mismos.
Verificar (Revisar y dar seguimiento al SGSI)	Verificar y revisar los procesos en función de las políticas estipuladas
Actuar (Mantener y mejorar el SGSI)	Se trata de las acciones correctivas y preventivas luego de identificados los riesgos

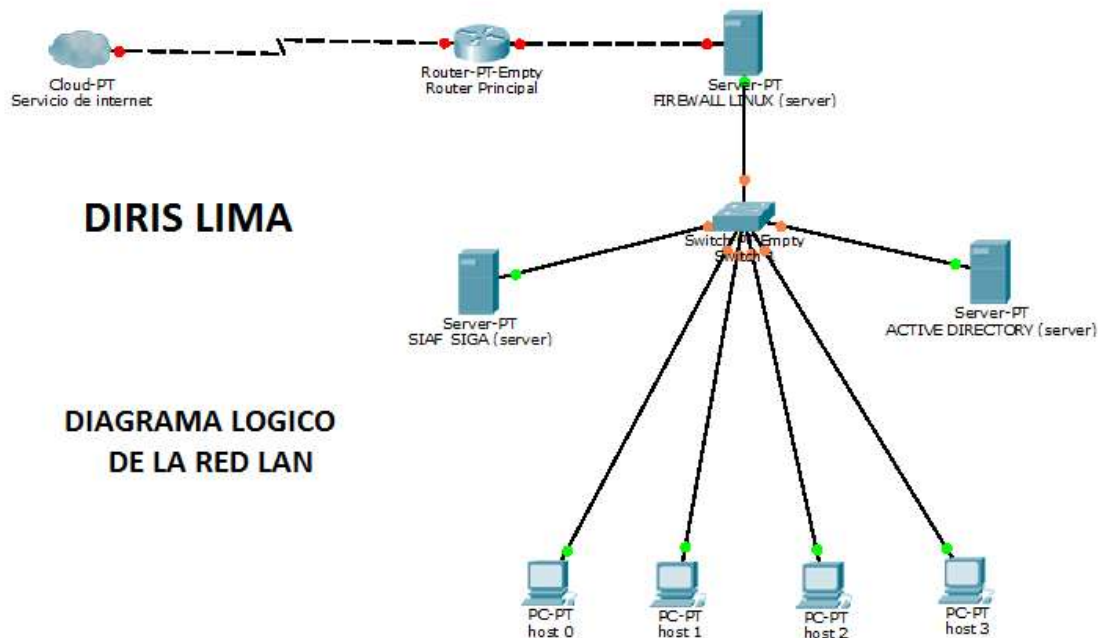
4.4.4. Analizar Red existente

La red existente está en función de los 74 establecimientos de salud. Cada una es una isla; no hay una integración, por lo tanto, los riesgos se hacen mayores.

4.4.4.1. Topología de la Red Física de la Oficina Central

Para la oficina central tenemos un servicio de fibra óptica del servicio de internet, actualmente tiene un servidor firewall y posterior a ello va a uno de los switch core para la distribución a los servidores de servicio y a otro host de la oficina central, como muestra el grafico es una red más organizada

Figura 9. Topología de la red física de la oficina central

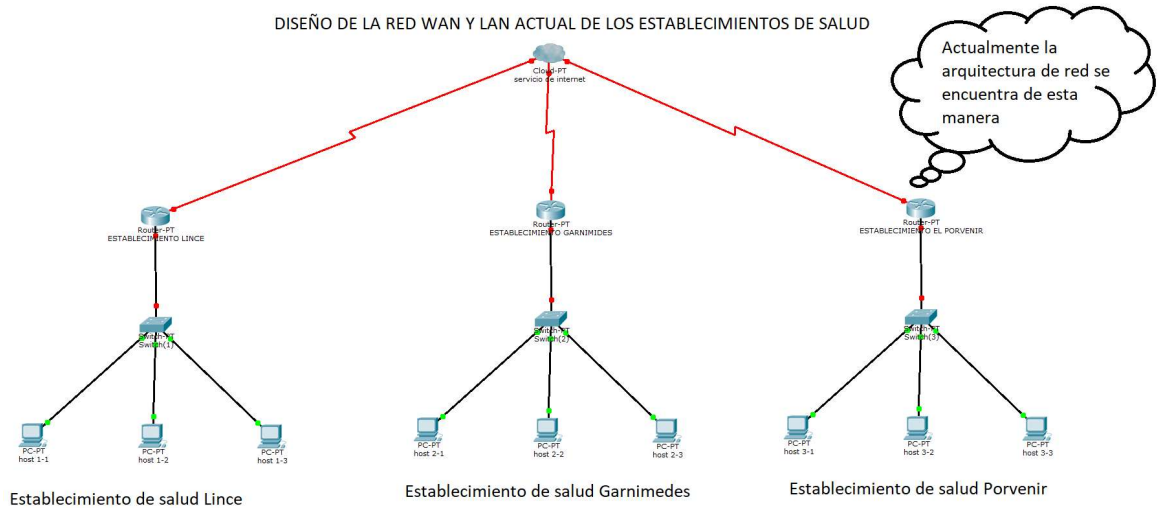


4.4.4.2. Topología de la Redes Sucursales

En los puestos de salud debido a la lejanía y a la falta de organización la parte estructural no fue el mejor planeado en esos casos el servicio suele ser por ADSL o en el mejor de los casos HFC y es un servicio que no tiene restricciones o políticas de uso, actualmente es de libre demanda,

viéndolo por el lado de la seguridad se encuentra expuesto a cualquier tipo de ataque u robo de datos, se presenta el diagrama.

Figura 10. Topología de la red de sucursales



4.4.4.3. Listado de Dispositivos de Red

Un dispositivo de red es un término ampliamente utilizado para cualquier hardware que conecte diferentes recursos de red. Los dispositivos clave que comprenden una red son conmutadores, enrutadores, bridge (puentes), repetidores y puertas de enlace.

Todos los dispositivos tienen características de alcance por separado, según los requisitos y escenarios de la red.

Tabla 18. Lista de dispositivos de la red DIRIS

OFICINA	DIRECCIÓN DE RED	MÁSCARA DE RED	PUERTA DE ENLACE	NOMBRE DE EQUIPO	PISO
UNIDAD FUNCIONAL DE BIENESTAR SOCIAL	10.0.0.30	255.2555.0.0	10.0.0.5	PCBS01P1	PISO 1
UNIDAD FUNCIONAL DE BIENESTAR SOCIAL	10.0.0.31	255.2555.0.0	10.0.0.5	PCBS02P1	PISO 1
UNIDAD FUNCIONAL DE BIENESTAR SOCIAL	10.0.0.32	255.2555.0.0	10.0.0.5	PCBS03P1	PISO 1
UNIDAD FUNCIONAL DE BIENESTAR SOCIAL	10.0.0.33	255.2555.0.0	10.0.0.5	PCBS04P1	PISO 1
OFICINA DE ASESORÍA LEGAL	10.0.0.34	255.2555.0.0	10.0.0.5	PCAL01P1	PISO 1
OFICINA DE ASESORÍA LEGAL	10.0.0.35	255.2555.0.0	10.0.0.5	PCAL02P1	PISO 1
OFICINA DE ASESORÍA LEGAL	10.0.0.36	255.2555.0.0	10.0.0.5	PCAL03P1	PISO 1
OFICINA DE RECURSOS HUMANOS	10.0.0.37	255.2555.0.0	10.0.0.5	PCPRH01P1	PISO 1
OFICINA DE RECURSOS HUMANOS	10.0.0.38	255.2555.0.0	10.0.0.5	PCPRH02P1	PISO 1
OFICINA DE RECURSOS HUMANOS	10.0.0.39	255.2555.0.0	10.0.0.5	PCPRH03P1	PISO 1
OFICINA DE RECURSOS HUMANOS	10.0.0.40	255.2555.0.0	10.0.0.5	PCPRH04P1	PISO 1
OFICINA DE RECURSOS HUMANOS	10.0.0.41	255.2555.0.0	10.0.0.5	PCPRH05P1	PISO 1
OFICINA DE RECURSOS HUMANOS	10.0.0.42	255.2555.0.0	10.0.0.5	PCPRH06P1	PISO 1
OFICINA DE RECURSOS HUMANOS	10.0.0.43	255.2555.0.0	10.0.0.5	PCPRH07P1	PISO 1
OFICINA DE RECURSOS HUMANOS	10.0.0.44	255.2555.0.0	10.0.0.5	PCPRH08P1	PISO 1
OFICINA DE INTERVENCIONES SANITARIAS	10.0.0.45	255.2555.0.0	10.0.0.5	PCIS01P1	PISO 1
OFICINA DE INTERVENCIONES SANITARIAS	10.0.0.46	255.2555.0.0	10.0.0.5	PCIS02P1	PISO 1
OFICINA DE INTERVENCIONES SANITARIAS	10.0.0.47	255.2555.0.0	10.0.0.5	PCIS03P1	PISO 1
OFICINA DE INTERVENCIONES SANITARIAS	10.0.0.48	255.2555.0.0	10.0.0.5	PCIS04P1	PISO 1
OFICINA DE INTERVENCIONES SANITARIAS	10.0.0.49	255.2555.0.0	10.0.0.5	PCIS05P1	PISO 1
OFICINA DE INTERVENCIONES SANITARIAS	10.0.0.50	255.2555.0.0	10.0.0.5	PCIS06P1	PISO 1
OFICINA DE INTERVENCIONES SANITARIAS	10.0.0.51	255.2555.0.0	10.0.0.5	PCIS07P1	PISO 1
OFICINA DE INTERVENCIONES SANITARIAS	10.0.0.52	255.2555.0.0	10.0.0.5	PCIS08P1	PISO 1
OFICINA DE INTERVENCIONES SANITARIAS	10.0.0.53	255.2555.0.0	10.0.0.5	PCIS09P1	PISO 1
OFICINA DE INTERVENCIONES SANITARIAS	10.0.0.54	255.2555.0.0	10.0.0.5	PCIS10P1	PISO 1
OFICINA DE INTERVENCIONES SANITARIAS	10.0.0.55	255.2555.0.0	10.0.0.5	PCIS11P1	PISO 1
OFICINA DE INTERVENCIONES SANITARIAS	10.0.0.56	255.2555.0.0	10.0.0.5	PCIS12P1	PISO 1
OFICINA DE INTERVENCIONES SANITARIAS	10.0.0.57	255.2555.0.0	10.0.0.5	PCIS13P1	PISO 1
OFICINA DE INTERVENCIONES SANITARIAS	10.0.0.58	255.2555.0.0	10.0.0.5	PCIS14P1	PISO 1
OFICINA DE INTERVENCIONES SANITARIAS	10.0.0.59	255.2555.0.0	10.0.0.5	PCIS15P1	PISO 1
OFICINA DE INTERVENCIONES SANITARIAS	10.0.0.60	255.2555.0.0	10.0.0.5	PCIS16P1	PISO 1
OFICINA DE INTERVENCIONES SANITARIAS	10.0.0.61	255.2555.0.0	10.0.0.5	PCIS17P1	PISO 1

OFICINA DE INTERVENCIONES SANITARIAS	10.0.0.62	255.2555.0.0	10.0.0.5	PCIS18P1	PISO 1
OFICINA DE INTERVENCIONES SANITARIAS	10.0.0.63	255.2555.0.0	10.0.0.5	PCIS19P1	PISO 1
OFICINA DE ECONOMÍA	10.0.0.64	255.2555.0.0	10.0.0.5	PCEC01P1	PISO 1
OFICINA DE ECONOMÍA	10.0.0.65	255.2555.0.0	10.0.0.5	PCEC02P1	PISO 1
OFICINA DE ECONOMÍA	10.0.0.66	255.2555.0.0	10.0.0.5	PCEC03P1	PISO 1
OFICINA DE ECONOMÍA	10.0.0.67	255.2555.0.0	10.0.0.5	PCEC04P1	PISO 1
OFICINA DE ECONOMÍA	10.0.0.68	255.2555.0.0	10.0.0.5	PCEC05P1	PISO 1
OFICINA DE ECONOMÍA	10.0.0.69	255.2555.0.0	10.0.0.5	PCEC06P1	PISO 1
OFICINA DE ECONOMÍA	10.0.0.70	255.2555.0.0	10.0.0.5	PCEC07P1	PISO 1
OFICINA DE CONTABILIDAD	10.0.0.71	255.2555.0.0	10.0.0.5	PCCON01P1	PISO 1
OFICINA DE CONTABILIDAD	10.0.0.72	255.2555.0.0	10.0.0.5	PCCON02P1	PISO 1
OFICINA DE CONTABILIDAD	10.0.0.73	255.2555.0.0	10.0.0.5	PCCON03P1	PISO 1
OFICINA DE CONTABILIDAD	10.0.0.74	255.2555.0.0	10.0.0.5	PCCON04P1	PISO 1
OFICINA DE CONTABILIDAD	10.0.0.75	255.2555.0.0	10.0.0.5	PCCON05P1	PISO 1
OFICINA DE TRAMITE DOCUMENTARIO	10.0.0.76	255.2555.0.0	10.0.0.5	PCTD01P1	PISO 1
OFICINA DE TRAMITE DOCUMENTARIO	10.0.0.77	255.2555.0.0	10.0.0.5	PCTD02P1	PISO 1
DIRECCIÓN DE ADMINISTRACIÓN	10.0.0.78	255.2555.0.0	10.0.0.5	PCADM01P1	PISO 1
DIRECCIÓN DE ADMINISTRACIÓN	10.0.0.79	255.2555.0.0	10.0.0.5	PCADM02P1	PISO 1
DIRECCIÓN DE ADMINISTRACIÓN	10.0.0.80	255.2555.0.0	10.0.0.5	PCADM03P1	PISO 1
OFICINA DE ABASTECIMIENTO	10.0.0.81	255.2555.0.0	10.0.0.5	PCABAS01P2	PISO 2
OFICINA DE ABASTECIMIENTO	10.0.0.82	255.2555.0.0	10.0.0.5	PCABAS02P2	PISO 2
OFICINA DE ABASTECIMIENTO	10.0.0.83	255.2555.0.0	10.0.0.5	PCABAS03P2	PISO 2
OFICINA DE ABASTECIMIENTO	10.0.0.84	255.2555.0.0	10.0.0.5	PCABAS04P2	PISO 2
OFICINA DE ABASTECIMIENTO	10.0.0.85	255.2555.0.0	10.0.0.5	PCABAS05P2	PISO 2
OFICINA DE ABASTECIMIENTO	10.0.0.86	255.2555.0.0	10.0.0.5	PCABAS06P2	PISO 2
OFICINA DE ABASTECIMIENTO	10.0.0.87	255.2555.0.0	10.0.0.5	PCABAS07P2	PISO 2
OFICINA DE ABASTECIMIENTO	10.0.0.88	255.2555.0.0	10.0.0.5	PCABAS08P2	PISO 2
OFICINA DE ABASTECIMIENTO	10.0.0.89	255.2555.0.0	10.0.0.5	PCABAS09P2	PISO 2
OFICINA DE ABASTECIMIENTO	10.0.0.90	255.2555.0.0	10.0.0.5	PCABAS10P2	PISO 2
OFICINA DE ABASTECIMIENTO	10.0.0.91	255.2555.0.0	10.0.0.5	PCABAS11P2	PISO 2
OFICINA DE ABASTECIMIENTO	10.0.0.92	255.2555.0.0	10.0.0.5	PCABAS12P2	PISO 2
OFICINA DE ABASTECIMIENTO	10.0.0.93	255.2555.0.0	10.0.0.5	PCABAS13P2	PISO 2
OFICINA DE SEGURO	10.0.0.94	255.2555.0.0	10.0.0.5	PCSE01P2	PISO 2
OFICINA DE SEGURO	10.0.0.95	255.2555.0.0	10.0.0.5	PCSE02P2	PISO 2
OFICINA DE SEGURO	10.0.0.96	255.2555.0.0	10.0.0.5	PCSE03P2	PISO 2
OFICINA DE SEGURO	10.0.0.97	255.2555.0.0	10.0.0.5	PCSE04P2	PISO 2
OFICINA DE SEGURO	10.0.0.98	255.2555.0.0	10.0.0.5	PCSE05P2	PISO 2
OFICINA DE SEGURO	10.0.0.99	255.2555.0.0	10.0.0.5	PCSE06P2	PISO 2
OFICINA DE EPIDEMIOLOGIA	10.0.0.100	255.2555.0.0	10.0.0.5	PCEPI01P2	PISO 2

OFICINA DE EPIDEMIOLOGIA	10.0.0.101	255.2555.0.0	10.0.0.5	PCEPI02P2	PISO 2
OFICINA DE EPIDEMIOLOGIA	10.0.0.102	255.2555.0.0	10.0.0.5	PCEPI03P2	PISO 2
OFICINA DE EPIDEMIOLOGIA	10.0.0.103	255.2555.0.0	10.0.0.5	PCEPI04P2	PISO 2
OFICINA DE EPIDEMIOLOGIA	10.0.0.104	255.2555.0.0	10.0.0.5	PCEPI05P2	PISO 2
OFICINA DE EPIDEMIOLOGIA	10.0.0.105	255.2555.0.0	10.0.0.5	PCEPI06P2	PISO 2
OFICINA DE EPIDEMIOLOGIA	10.0.0.106	255.2555.0.0	10.0.0.5	PCEPI07P2	PISO 2
UNIDAD FUNCIONAL DE ESTADÍSTICA	10.0.0.107	255.2555.0.0	10.0.0.5	PCEST01P2	PISO 2
UNIDAD FUNCIONAL DE ESTADÍSTICA	10.0.0.108	255.2555.0.0	10.0.0.5	PCEST02P2	PISO 2
UNIDAD FUNCIONAL DE ESTADÍSTICA	10.0.0.109	255.2555.0.0	10.0.0.5	PCEST03P2	PISO 2
UNIDAD FUNCIONAL DE ESTADÍSTICA	10.0.0.110	255.2555.0.0	10.0.0.5	PCEST04P2	PISO 2
UNIDAD FUNCIONAL DE ESTADÍSTICA	10.0.0.111	255.2555.0.0	10.0.0.5	PCEST05P2	PISO 2
UNIDAD FUNCIONAL DE ESTADÍSTICA	10.0.0.112	255.2555.0.0	10.0.0.5	PCEST06P2	PISO 2
UNIDAD FUNCIONAL DE ESTADÍSTICA	10.0.0.113	255.2555.0.0	10.0.0.5	PCEST07P2	PISO 2
UNIDAD FUNCIONAL DE ESTADÍSTICA	10.0.0.114	255.2555.0.0	10.0.0.5	PCEST08P2	PISO 2
DIRECCIÓN ADJUNTA	10.0.0.115	255.2555.0.0	10.0.0.5	PCDA01P2	PISO 2
DIRECCIÓN ADJUNTA	10.0.0.116	255.2555.0.0	10.0.0.5	PCDA02P2	PISO 2
DIRECCIÓN GENERAL	10.0.0.117	255.2555.0.0	10.0.0.5	PCDIR01P2	PISO 2
DIRECCIÓN GENERAL	10.0.0.118	255.2555.0.0	10.0.0.5	PCDIR02P2	PISO 2
DIRECCIÓN GENERAL	10.0.0.119	255.2555.0.0	10.0.0.5	PCDIR03P2	PISO 2
UNIDAD FUNCIONAL DE SERVICIOS GENERALES	10.0.0.120	255.2555.0.0	10.0.0.5	PCSRG01P2	PISO 2
UNIDAD FUNCIONAL DE SERVICIOS GENERALES	10.0.0.121	255.2555.0.0	10.0.0.5	PCSRG02P2	PISO 2
UNIDAD FUNCIONAL DE SERVICIOS GENERALES	10.0.0.122	255.2555.0.0	10.0.0.5	PCSRG03P2	PISO 2
OFICINA DE TECNOLOGÍAS DE LA INFORMACION	10.0.0.123	255.2555.0.0	10.0.0.5	PCOTI01P2	PISO 2
OFICINA DE TECNOLOGÍAS DE LA INFORMACION	10.0.0.124	255.2555.0.0	10.0.0.5	PCOTI02P2	PISO 2
OFICINA DE TECNOLOGÍAS DE LA INFORMACION	10.0.0.125	255.2555.0.0	10.0.0.5	PCOTI03P2	PISO 2
OFICINA DE TECNOLOGÍAS DE LA INFORMACION	10.0.0.126	255.2555.0.0	10.0.0.5	PCOTI04P2	PISO 2
OFICINA DE TECNOLOGÍAS DE LA INFORMACION	10.0.0.127	255.2555.0.0	10.0.0.5	PCOTI05P2	PISO 2
OFICINA DE TECNOLOGÍAS DE LA INFORMACION	10.0.0.128	255.2555.0.0	10.0.0.5	PCOTI06P2	PISO 2
OFICINA DE TECNOLOGÍAS DE LA INFORMACION	10.0.0.129	255.2555.0.0	10.0.0.5	PCOTI07P2	PISO 2

Servicios públicos el término se utilizó por primera vez en Francia en 1875 para describir un proyecto ferroviario.

Sin embargo, antes del siglo XVIII, el desarrollo de la infraestructura comenzó con caminos y canales para el transporte y el riego. Desde la década de 1800 hasta principios de la de 1900, se introdujeron telégrafos, ferrocarriles, electricidad, alcantarillado, subterráneos y comunicaciones telefónicas.

Las empresas confían rápidamente en la tecnología a medida que la tecnología evoluciona desde las computadoras básicas hasta Internet y más allá. Con el tiempo, la infraestructura de tecnología de la información (TI) se ha convertido en la columna vertebral de una empresa. Hoy en día, el término se utiliza para incluir las plataformas en evolución, los componentes estructurales y las relaciones de las estructuras empresariales integradas actuales. Los términos tomados del francés tienen los siguientes significados. Esto confirma la necesidad de una base sólida para sustentar un marco organizativo sólido.

SEDE CENTRAL

En la oficina de tecnologías de la información de la DIRIS lima centro tenemos los siguientes equipos como parte de la infraestructura física de la red de comunicaciones la cual es parte principal de las comunicaciones de la sede principal.

Tabla 19. Red de Comunicaciones Sede Central

EQUIPO DE COMUNICACIÓN	MARCA	MODELO	CANTIDADES	DESCRIPCION
ROUTER	MITRASTAR	GPT-2741	1	EQUIPO INSTALADO POR LA OPERADORA DE SERVICIO - MOVISTAR
FIREWALL	HP	PROLIANT 350 G9	1	SEVIDOR GAMA MEDIA CONFIGURADO CON LINUX
SWITCH	D-LINK	DGS-1024D	8	EQUIPO PARA LA CONEXIÓN DE SUBDIVISION DE RED
SERVIDOR	VIRTUALIZADO	XEON 2.20/ 16GB/1TB	1	ACTIVE DIRECTORY
SERVIDOR	FISICO	XEON 2.4/ 24GB/ 600GB	1	SERVIDOR FISICO PARA EL SISTEMA (SIAF)
SERVIDOR	VIRTUALIZADO	XEON 2.20/30GB/1TB	1	SERVIDOR VIRTUAL PARA EL SISTEMA (SIGA)
HOST	INTEL	CORE I5/8GB/500GB	366	TERMINALES PARA LOS DIFERENTES USUARIO

ESTABLECIMIENTOS DE SALUD

En los establecimientos de salud tenemos los siguientes equipos como parte de la infraestructura física de la red de comunicaciones, el cual está compuesta por los mismos equipos y diseño para todos los establecimientos de salud.

Tabla 20. Red de Comunicaciones Establecimientos de salud

EQUIPO DE COMUNICACIÓN	MARCA	MODELO	CANTIDADES	DESCRIPCION
ROUTER	HITRON	CGNV22	1	EQUIPO INSTALADO POR LA OPERADORA DE SERVICIO - MOVISTAR
SWITCH	D-LINK	DGS-1024D	1	EQUIPO PARA LA CONEXIÓN DE SUBDIVISION DE RED
HOST	INTEL	CORE I3/8GB/500GB	30	TERMINALES PARA LOS DIFERENTES USUARIO

4.4.4.4. Analizar Tráfico existente

El análisis del tráfico se realiza mediante software libre los cuales nos darán unas mediciones de nuestra Red de área Local, para controlar el tráfico en la plataforma actual se utiliza el software.

4.4.4.5. Informe de Tráfico de Datos: Servidor DNS, Servidor de bases de datos, Servidor de aplicaciones web, Servicio de internet

Ntop:

Es un analizador de la dinámica de las interconexiones de las redes en internet, se basa en los estándares y se crea las interfaces a través del cual se configura el uso de la organización.

Apreciación: El detalle del Tráfico de Broadcast – Sede Central muestra un porcentaje de tráfico de broadcast del 59.84% y el Detalle del Tráfico de Broadcast – Ris N° 1 expone que el tráfico de red es de 77.89%, muy por encima del permitido que es 20%, lo que demuestra que hay una congestión de solicitudes de uso de

la red de la Diris Lima Centro y de la Ris N°1, todo lo que cual ocasiona demoras.

4.5. FASE 2: Desarrollar Diseño Lógico

Diseñar Topología de Red

Diseño Medio de Transmisión

El diseño lógico está constituido por la información de la organización y se basan en la base de datos a partir del cual se sustentan el desarrollo.

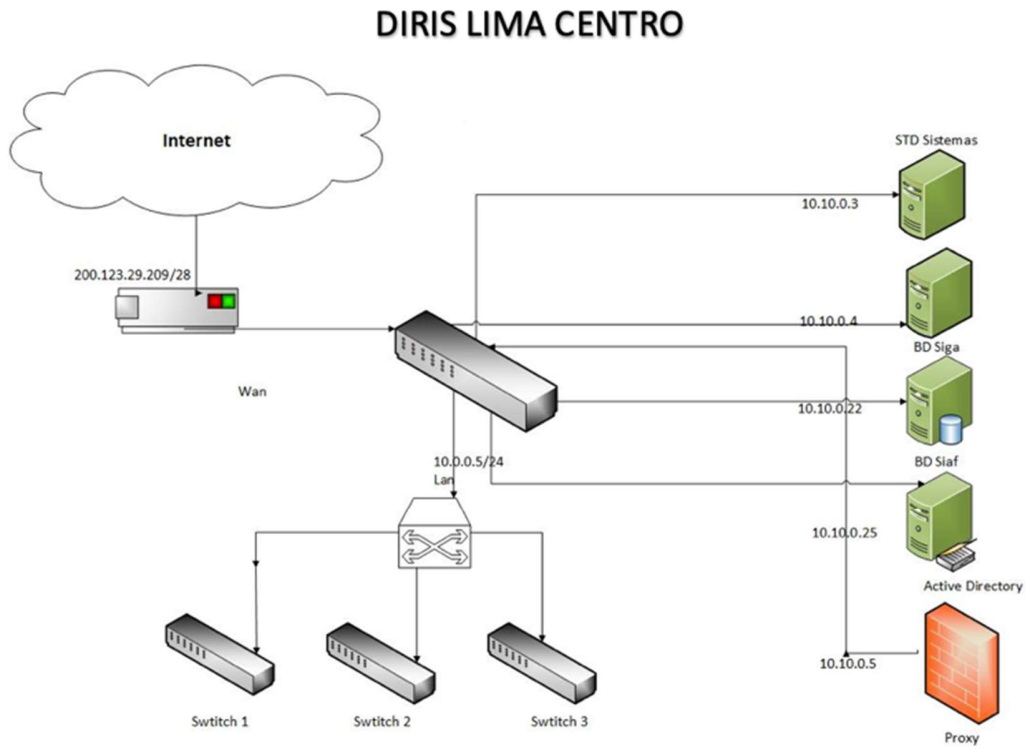
Se pasa del concepto a la lógica de los datos, en el cual se puede ver las relaciones entre los computadores, las jerarquías y los objetivos claros de cada proceso de la empresa.

Entre los principales elementos de un diseño lógico está los siguientes:

- Modem con conexión a internet.
- Router de permisos.
- Swich para ingreso de nuevos usuarios.
- Patch panel para la ubicación de las redes.

Actualmente el diseño de transmisión se encuentra de la siguiente manera:

Tabla 21. DIRIS Lima Centro



4.5.1. Mapeo de Usuarios

Tabla 22. Mapeo de usuarios

OFICINA	DIRECCIÓN DE RED	MASCARA DE RED	PUERTA DE ENLACE	NOMBRE DE EQUIPO	PISO
UNIDAD FUNCIONAL DE BIENESTAR SOCIAL	10.0.0.30	255.2555.0.0	10.0.0.5	PCBS01P1	PISO 1
UNIDAD FUNCIONAL DE BIENESTAR SOCIAL	10.0.0.31	255.2555.0.0	10.0.0.5	PCBS02P1	PISO 1
UNIDAD FUNCIONAL DE BIENESTAR SOCIAL	10.0.0.32	255.2555.0.0	10.0.0.5	PCBS03P1	PISO 1
UNIDAD FUNCIONAL DE BIENESTAR SOCIAL	10.0.0.33	255.2555.0.0	10.0.0.5	PCBS04P1	PISO 1
OFICINA DE ASESORIA LEGAL	10.0.0.34	255.2555.0.0	10.0.0.5	PCAL01P1	PISO 1
OFICINA DE ASESORIA LEGAL	10.0.0.35	255.2555.0.0	10.0.0.5	PCAL02P1	PISO 1
OFICINA DE ASESORIA LEGAL	10.0.0.36	255.2555.0.0	10.0.0.5	PCAL03P1	PISO 1
OFICINA DE RECURSOS HUMANOS	10.0.0.37	255.2555.0.0	10.0.0.5	PCPRH01P1	PISO 1
OFICINA DE RECURSOS HUMANOS	10.0.0.38	255.2555.0.0	10.0.0.5	PCPRH02P1	PISO 1
OFICINA DE RECURSOS HUMANOS	10.0.0.39	255.2555.0.0	10.0.0.5	PCPRH03P1	PISO 1
OFICINA DE RECURSOS HUMANOS	10.0.0.40	255.2555.0.0	10.0.0.5	PCPRH04P1	PISO 1
OFICINA DE RECURSOS HUMANOS	10.0.0.41	255.2555.0.0	10.0.0.5	PCPRH05P1	PISO 1
OFICINA DE RECURSOS HUMANOS	10.0.0.42	255.2555.0.0	10.0.0.5	PCPRH06P1	PISO 1
OFICINA DE RECURSOS HUMANOS	10.0.0.43	255.2555.0.0	10.0.0.5	PCPRH07P1	PISO 1
OFICINA DE RECURSOS HUMANOS	10.0.0.44	255.2555.0.0	10.0.0.5	PCPRH08P1	PISO 1
OFICINA DE INTERVENCIONES SANITARIAS	10.0.0.45	255.2555.0.0	10.0.0.5	PCIS01P1	PISO 1
OFICINA DE INTERVENCIONES SANITARIAS	10.0.0.46	255.2555.0.0	10.0.0.5	PCIS02P1	PISO 1
OFICINA DE INTERVENCIONES SANITARIAS	10.0.0.47	255.2555.0.0	10.0.0.5	PCIS03P1	PISO 1
OFICINA DE INTERVENCIONES SANITARIAS	10.0.0.48	255.2555.0.0	10.0.0.5	PCIS04P1	PISO 1
OFICINA DE INTERVENCIONES SANITARIAS	10.0.0.49	255.2555.0.0	10.0.0.5	PCIS05P1	PISO 1
OFICINA DE INTERVENCIONES SANITARIAS	10.0.0.50	255.2555.0.0	10.0.0.5	PCIS06P1	PISO 1
OFICINA DE INTERVENCIONES SANITARIAS	10.0.0.51	255.2555.0.0	10.0.0.5	PCIS07P1	PISO 1
OFICINA DE INTERVENCIONES SANITARIAS	10.0.0.52	255.2555.0.0	10.0.0.5	PCIS08P1	PISO 1
OFICINA DE INTERVENCIONES SANITARIAS	10.0.0.53	255.2555.0.0	10.0.0.5	PCIS09P1	PISO 1
OFICINA DE INTERVENCIONES SANITARIAS	10.0.0.54	255.2555.0.0	10.0.0.5	PCIS10P1	PISO 1
OFICINA DE INTERVENCIONES SANITARIAS	10.0.0.55	255.2555.0.0	10.0.0.5	PCIS11P1	PISO 1

OFICINA DE INTERVENCIONES SANITARIAS	10.0.0.56	255.2555.0.0	10.0.0.5	PCIS12P1	PISO 1
OFICINA DE INTERVENCIONES SANITARIAS	10.0.0.57	255.2555.0.0	10.0.0.5	PCIS13P1	PISO 1
OFICINA DE INTERVENCIONES SANITARIAS	10.0.0.58	255.2555.0.0	10.0.0.5	PCIS14P1	PISO 1
OFICINA DE INTERVENCIONES SANITARIAS	10.0.0.59	255.2555.0.0	10.0.0.5	PCIS15P1	PISO 1
OFICINA DE INTERVENCIONES SANITARIAS	10.0.0.60	255.2555.0.0	10.0.0.5	PCIS16P1	PISO 1
OFICINA DE INTERVENCIONES SANITARIAS	10.0.0.61	255.2555.0.0	10.0.0.5	PCIS17P1	PISO 1
OFICINA DE INTERVENCIONES SANITARIAS	10.0.0.62	255.2555.0.0	10.0.0.5	PCIS18P1	PISO 1
OFICINA DE INTERVENCIONES SANITARIAS	10.0.0.63	255.2555.0.0	10.0.0.5	PCIS18P1	PISO 1
OFICINA DE ECONOMÍA	10.0.0.64	255.2555.0.0	10.0.0.5	PCEC01P1	PISO 1
OFICINA DE ECONOMÍA	10.0.0.65	255.2555.0.0	10.0.0.5	PCEC02P1	PISO 1
OFICINA DE ECONOMÍA	10.0.0.66	255.2555.0.0	10.0.0.5	PCEC03P1	PISO 1
OFICINA DE ECONOMÍA	10.0.0.67	255.2555.0.0	10.0.0.5	PCEC04P1	PISO 1
OFICINA DE ECONOMÍA	10.0.0.68	255.2555.0.0	10.0.0.5	PCEC05P1	PISO 1
OFICINA DE ECONOMÍA	10.0.0.69	255.2555.0.0	10.0.0.5	PCEC06P1	PISO 1
OFICINA DE ECONOMÍA	10.0.0.70	255.2555.0.0	10.0.0.5	PCEC07P1	PISO 1
OFICINA DE CONTABILIDAD	10.0.0.71	255.2555.0.0	10.0.0.5	PCCON01P1	PISO 1
OFICINA DE CONTABILIDAD	10.0.0.72	255.2555.0.0	10.0.0.5	PCCON02P1	PISO 1
OFICINA DE CONTABILIDAD	10.0.0.73	255.2555.0.0	10.0.0.5	PCCON03P1	PISO 1
OFICINA DE CONTABILIDAD	10.0.0.74	255.2555.0.0	10.0.0.5	PCCON04P1	PISO 1
OFICINA DE CONTABILIDAD	10.0.0.75	255.2555.0.0	10.0.0.5	PCCON05P1	PISO 1
OFICINA DE TRAMITE DOCUMENTARIO	10.0.0.76	255.2555.0.0	10.0.0.5	PCTD01P1	PISO 1
OFICINA DE TRAMITE DOCUMENTARIO	10.0.0.77	255.2555.0.0	10.0.0.5	PCTD02P1	PISO 1
DIRECCION ADMINISTRACION DE	10.0.0.78	255.2555.0.0	10.0.0.5	PCADM01P1	PISO 1
DIRECCION ADMINISTRACION DE	10.0.0.79	255.2555.0.0	10.0.0.5	PCADM02P1	PISO 1
DIRECCION ADMINISTRACION DE	10.0.0.80	255.2555.0.0	10.0.0.5	PCADM03P1	PISO 1
OFICINA DE ABASTECIMIENTO	10.0.0.81	255.2555.0.0	10.0.0.5	PCABAS01P2	PISO 2
OFICINA DE ABASTECIMIENTO	10.0.0.82	255.2555.0.0	10.0.0.5	PCABAS02P2	PISO 2

OFICINA DE ABASTECIMIENTO	10.0.0.83	255.2555.0.0	10.0.0.5	PCABAS03P2	PISO 2
OFICINA DE ABASTECIMIENTO	10.0.0.84	255.2555.0.0	10.0.0.5	PCABAS04P2	PISO 2
OFICINA DE ABASTECIMIENTO	10.0.0.85	255.2555.0.0	10.0.0.5	PCABAS05P2	PISO 2
OFICINA DE ABASTECIMIENTO	10.0.0.86	255.2555.0.0	10.0.0.5	PCABAS06P2	PISO 2
OFICINA DE ABASTECIMIENTO	10.0.0.87	255.2555.0.0	10.0.0.5	PCABAS07P2	PISO 2
OFICINA DE ABASTECIMIENTO	10.0.0.88	255.2555.0.0	10.0.0.5	PCABAS08P2	PISO 2
OFICINA DE ABASTECIMIENTO	10.0.0.89	255.2555.0.0	10.0.0.5	PCABAS09P2	PISO 2
OFICINA DE ABASTECIMIENTO	10.0.0.90	255.2555.0.0	10.0.0.5	PCABAS10P2	PISO 2
OFICINA DE ABASTECIMIENTO	10.0.0.91	255.2555.0.0	10.0.0.5	PCABAS11P2	PISO 2
OFICINA DE ABASTECIMIENTO	10.0.0.92	255.2555.0.0	10.0.0.5	PCABAS12P2	PISO 2
OFICINA DE ABASTECIMIENTO	10.0.0.93	255.2555.0.0	10.0.0.5	PCABAS13P2	PISO 2
OFICINA DE SEGURO	10.0.0.94	255.2555.0.0	10.0.0.5	PCSE01P2	PISO 2
OFICINA DE SEGURO	10.0.0.95	255.2555.0.0	10.0.0.5	PCSE02P2	PISO 2
OFICINA DE SEGURO	10.0.0.96	255.2555.0.0	10.0.0.5	PCSE03P2	PISO 2
OFICINA DE SEGURO	10.0.0.97	255.2555.0.0	10.0.0.5	PCSE04P2	PISO 2
OFICINA DE SEGURO	10.0.0.98	255.2555.0.0	10.0.0.5	PCSE05P2	PISO 2
OFICINA DE SEGURO	10.0.0.99	255.2555.0.0	10.0.0.5	PCSE06P2	PISO 2
OFICINA DE EPIDEMIOLOGIA	10.0.0.100	255.2555.0.0	10.0.0.5	PCEPI01P2	PISO 2
OFICINA DE EPIDEMIOLOGIA	10.0.0.101	255.2555.0.0	10.0.0.5	PCEPI02P2	PISO 2
OFICINA DE EPIDEMIOLOGIA	10.0.0.102	255.2555.0.0	10.0.0.5	PCEPI03P2	PISO 2
OFICINA DE EPIDEMIOLOGIA	10.0.0.103	255.2555.0.0	10.0.0.5	PCEPI04P2	PISO 2
OFICINA DE EPIDEMIOLOGIA	10.0.0.104	255.2555.0.0	10.0.0.5	PCEPI05P2	PISO 2
OFICINA DE EPIDEMIOLOGIA	10.0.0.105	255.2555.0.0	10.0.0.5	PCEPI06P2	PISO 2
OFICINA DE EPIDEMIOLOGIA	10.0.0.106	255.2555.0.0	10.0.0.5	PCEPI07P2	PISO 2
UNIDAD FUNCIONAL DE ESTADISTICA	10.0.0.107	255.2555.0.0	10.0.0.5	PCEST01P2	PISO 2
UNIDAD FUNCIONAL DE ESTADISTICA	10.0.0.108	255.2555.0.0	10.0.0.5	PCEST02P2	PISO 2
UNIDAD FUNCIONAL DE ESTADISTICA	10.0.0.109	255.2555.0.0	10.0.0.5	PCEST03P2	PISO 2

UNIDAD FUNCIONAL ESTADISTICA	DE	10.0.0.110	255.2555.0.0	10.0.0.5	PCEST04P2	PISO 2
UNIDAD FUNCIONAL ESTADISTICA	DE	10.0.0.111	255.2555.0.0	10.0.0.5	PCEST05P2	PISO 2
UNIDAD FUNCIONAL ESTADISTICA	DE	10.0.0.112	255.2555.0.0	10.0.0.5	PCEST06P2	PISO 2
UNIDAD FUNCIONAL ESTADISTICA	DE	10.0.0.113	255.2555.0.0	10.0.0.5	PCEST07P2	PISO 2
UNIDAD FUNCIONAL ESTADISTICA	DE	10.0.0.114	255.2555.0.0	10.0.0.5	PCEST08P2	PISO 2
DIRECCIÓN ADJUNTA		10.0.0.115	255.2555.0.0	10.0.0.5	PCDA01P2	PISO 2
DIRECCIÓN ADJUNTA		10.0.0.116	255.2555.0.0	10.0.0.5	PCDA02P2	PISO 2
DIRECCIÓN GENERAL		10.0.0.117	255.2555.0.0	10.0.0.5	PCDIR01P2	PISO 2
DIRECCIÓN GENERAL		10.0.0.118	255.2555.0.0	10.0.0.5	PCDIR02P2	PISO 2
DIRECCIÓN GENERAL		10.0.0.119	255.2555.0.0	10.0.0.5	PCDIR03P2	PISO 2
UNIDAD FUNCIONAL SERVICIOS GENERALES	DE	10.0.0.120	255.2555.0.0	10.0.0.5	PCSRG01P2	PISO 2
UNIDAD FUNCIONAL SERVICIOS GENERALES	DE	10.0.0.121	255.2555.0.0	10.0.0.5	PCSRG02P2	PISO 2
UNIDAD FUNCIONAL SERVICIOS GENERALES	DE	10.0.0.122	255.2555.0.0	10.0.0.5	PCSRG03P2	PISO 2
OFICINA DE TECNOLOGIAS DE LA INFORMACION	DE	10.0.0.123	255.2555.0.0	10.0.0.5	PCOTI01P2	PISO 2
OFICINA DE TECNOLOGIAS DE LA INFORMACION	DE	10.0.0.124	255.2555.0.0	10.0.0.5	PCOTI02P2	PISO 2
OFICINA DE TECNOLOGIAS DE LA INFORMACION	DE	10.0.0.125	255.2555.0.0	10.0.0.5	PCOTI03P2	PISO 2
OFICINA DE TECNOLOGIAS DE LA INFORMACION	DE	10.0.0.126	255.2555.0.0	10.0.0.5	PCOTI04P2	PISO 2
OFICINA DE TECNOLOGIAS DE LA INFORMACION	DE	10.0.0.127	255.2555.0.0	10.0.0.5	PCOTI05P2	PISO 2
OFICINA DE TECNOLOGIAS DE LA INFORMACION	DE	10.0.0.128	255.2555.0.0	10.0.0.5	PCOTI06P2	PISO 2
OFICINA DE TECNOLOGIAS DE LA INFORMACION	DE	10.0.0.129	255.2555.0.0	10.0.0.5	PCOTI07P2	PISO 2

UNIDAD FUNCIONAL DE ESTADÍSTICA	PISO 2	1
UNIDAD FUNCIONAL DE ESTADÍSTICA	PISO 2	1
DIRECCIÓN ADJUNTA	PISO 2	1
DIRECCIÓN ADJUNTA	PISO 2	1
DIRECCIÓN GENERAL	PISO 2	1
DIRECCIÓN GENERAL	PISO 2	1
DIRECCIÓN GENERAL	PISO 2	1
UNIDAD FUNCIONAL DE SERVICIOS GENERALES	PISO 2	1
UNIDAD FUNCIONAL DE SERVICIOS GENERALES	PISO 2	1
UNIDAD FUNCIONAL DE SERVICIOS GENERALES	PISO 2	1
OFICINA DE TECNOLOGIAS DE LA INFORMACION	PISO 2	1
OFICINA DE TECNOLOGIAS DE LA INFORMACION	PISO 2	1
OFICINA DE TECNOLOGIAS DE LA INFORMACION	PISO 2	1
OFICINA DE TECNOLOGIAS DE LA INFORMACION	PISO 2	1
OFICINA DE TECNOLOGIAS DE LA INFORMACION	PISO 2	1
OFICINA DE TECNOLOGIAS DE LA INFORMACION	PISO 2	1
OFICINA DE TECNOLOGIAS DE LA INFORMACION	PISO 2	1

4.5.3. Mapeo de Equipos de Red

El mapeo de red es un proceso que se utiliza para descubrir nuevos dispositivos, interfaces y visualizar la conectividad de red física y virtual. El mapeo de redes ayuda a descomponer la red para facilitar el mantenimiento y la gestión de la red. Esto se puede hacer con la ayuda de un software o herramienta de mapeo de redes. Los escáneres de red detectan la red junto con todos sus componentes y muestra una lista de todos los dispositivos. Esto se puede usar para crear un mapa de red o una topología de red. Las herramientas de mapeo de redes integran los procesos de escaneo y mapeo y mapean una red automáticamente. OpManager, el software de mapeo de redes automatizado, le permite configurar y generar mapas de red fácilmente.

En la oficina principal del de DIRIS LIMA CENTRO se realizó un mapeado de la red encontrando los siguientes dispositivos conectados, se presenta el cuadro demostrativo

Tabla 24. Distribución de la red DIRIS Lima Centro

NOMBRE DE EQUIPO	TIPO DE INTERFAZ	DESCRIPCION Y OBJETIVO	VLAN	CAPA	IP DE RED	IP DE INTERFASE	MASCARA DE RED
Router Sede Principal	LAN 0	Conexión a SwitchDIRISLC	-	L2	10.0.0.5	10.0.0.0	255.255.0.0
	LAN 1	Sin conexión	-		-	-	-
	LAN 2	Sin conexión	-		-	-	-
	LAN 3	Sin conexión	-		-	-	-
	LAN 4	Sin conexión	-		-	-	-
Router Ris Nº1	LAN 0	Sin conexión	-		-	-	-
	LAN 1	Conexión a SwRIS1	-	L2	192.168.1.1	192.168.1.0	255.255.255.0
	LAN 2	Sin conexión	-		-	-	-
	LAN 3	Sin conexión	-		-	-	-
	LAN 4	Sin conexión	-		-	-	-
Router Ris Nº2	LAN 0	Sin conexión	-		-	-	-
	LAN 1	Sin conexión	-		-	-	-
	LAN 2	Conexión a SwRIS2	-		192.168.1.1	192.168.1.0	255.255.255.0
	LAN 3	Sin conexión	-		-	-	-
	LAN 4	Sin conexión	-		-	-	-
Router Ris Nº3	LAN 0	Sin conexión	-		-	-	-
	LAN 1	Sin conexión	-		-	-	-
	LAN 2	Sin conexión	-		-	-	-
	LAN 3	Conexión a SwRIS3	-		192.168.1.1	192.168.1.0	255.255.255.0
	LAN 4	Sin conexión	-		-	-	-
Router Ris Nº4	LAN 0	Sin conexión	-		-	-	-
	LAN 1	Sin conexión	-		-	-	-
	LAN 2	Sin conexión	-		-	-	-
	LAN 3	Sin conexión	-		-	-	-
	LAN 4	Conexión a SwRIS4	-		192.168.1.1	192.168.1.0	255.255.255.0
Router Ris Nº5	LAN 0	Sin conexión	-		-	-	-
	LAN 1	Conexión a SwRIS5	-		192.168.1.1	192.168.1.0	255.255.255.0
	LAN 2	Sin conexión	-		-	-	-
	LAN 3	Sin conexión	-		-	-	-
	LAN 4	Sin conexión	-		-	-	-
Router Ris Nº6	LAN 0	Sin conexión	-		-	-	-
	LAN 1	Sin conexión	-		-	-	-
	LAN 2	Conexión a SwRIS6	-		192.168.1.1	192.168.1.0	255.255.255.0
	LAN 3	Sin conexión	-		-	-	-
	LAN 4	Sin conexión	-		-	-	-
Router Ris Nº7	LAN 0	Sin conexión	-		-	-	-
	LAN 1	Sin conexión	-		-	-	-
	LAN 2	Sin conexión	-		-	-	-
	LAN 3	Conexión a SwRIS7	-		192.168.1.1	192.168.1.0	255.255.255.0
	LAN 4	Sin conexión	-		-	-	-

4.5.4. Características de Cableado Estructurado

En este punto se detalla las especificaciones técnicas a la cual se estructura el cableado, con ello las normas a la que debe de adecuarse. El cableado se encuentra en las siguientes normas:

Categoría 5e:

La categoría 5e (Cat 5e) es una versión mejorada del cable Cat 5 diseñado por TIA/EIA en 2001. Fue creado con el objetivo de mejorar algunas de las propiedades del cableado necesarias para el funcionamiento de Gigabit Ethernet. Este cable está fabricado para admitir velocidades de hasta 1000 Mbps "Gigabit", lo que da como resultado velocidades más rápidas que los cables Cat 5. Los cables Ethernet Cat 5e se distribuyen en muchos lugares.

Categoría 6:

Los cables Cat 6 son cables de calibre 23 y los cables de conexión Cat 5e son cables de calibre 24, que son un poco más pequeños. Cat 6 también cuenta con un divisor para controlar y reducir la diafonía, aislando cada uno de los cuatro pares trenzados de los demás, aumentando las tasas de datos y proporcionando el doble de ancho de banda. El cable admite efectivamente velocidades de 10 Gigabit Ethernet y opera a frecuencias de hasta 250 MHz. El cable de conexión Cat 6 delgado de diámetro pequeño modelo FS 28AWG se muestra en el siguiente video.

4.5.5. Diseño Modelos de direccionamiento y hostnames

4.5.5.1. Segmentación de Direccionamiento Lógico

La segmentación de la red implica dividirla en subredes para aumentar la cantidad de computadoras conectadas a ella para

mejorar el rendimiento, teniendo en cuenta el entorno de trabajo único donde hay una sola topología, un solo protocolo de comunicación y un solo protocolo de comunicación.

Entre los principales factores para tener en cuenta al construir redes:

- Número de subredes.
- Número de host requeridas.
- Número de host utilizables.

4.5.5.2. Direccionamiento IP

La dirección IP está constituido por dos partes: la identificación de la red y la ubicación de los equipos de cómputo, de esta forma se sabe cuántos bits se utilizan.

Clases de direccionamiento IP

Las direcciones IP tienen clases por las cuales se dividen para poder definir las redes de tamaño grande (clase A), mediano (clase B), pequeño (clase C).

Tabla 26. Direccionamiento IP

Clase A
• Rango de direcciones IP: 1.0.0.0 a 126.0.0.0
• Máscara de red: 255.0.0.0
• Direcciones privadas: 10.0.0.0 a 10.255.255.255
Clase B
• Rango de direcciones IP: 128.0.0.0 a 191.255.0.0
• Máscara de red: 255.255.0.0
• Direcciones privadas: 172.16.0.0 a 172.31.255.255
Clase C
• Rango de direcciones IP: 192.0.0.0 a 223.255.255.0
• Máscara de red: 255.255.255.0
• Direcciones privadas: 192.168.0.0 a 192.168.255.255
Clase D
• Rango de direcciones IP: 224.0.0.0 a 239.255.255.255 uso multicast o multidifusión
Clase E
• Rango de direcciones IP: 240.0.0.0 a 254.255.255.255 uso experimental

Para el caso de la red de la Diris lima centro se tiene la versión de comunicación IPV4 manteniendo la clase A para el direccionamiento de la red, a continuación, la lista de equipos conectados a la red el cual se tiene que tener en cuenta para la respectiva comunicación con los puestos de salud.

Tabla 27. Puestos de salud

RIS Nº 1	DIRECCION DE RED	MASCARA DE RED	PUERTA DE ENLACE	NOMBRE DE EQUIPO	PISO
OFICINA DE RIS Nº 1	172.20.1.20	255.2555.255.0	172.20.1.5	PCRIS1-01P1	PISO 1
OFICINA DE RIS Nº 1	172.20.1.21	255.2555.255.0	172.20.1.5	PCRIS1-02P1	PISO 1
OFICINA DE RIS Nº 1	172.20.1.22	255.2555.255.0	172.20.1.5	PCRIS1-03P1	PISO 1
OFICINA DE RIS Nº 1	172.20.1.23	255.2555.255.0	172.20.1.5	PCRIS1-04P1	PISO 1
OFICINA DE RIS Nº 1	172.20.1.24	255.2555.255.0	172.20.1.5	PCRIS1-05P1	PISO 1
OFICINA DE RIS Nº 1	172.20.1.25	255.2555.255.0	172.20.1.5	PCRIS1-06P1	PISO 1
OFICINA DE RIS Nº 1	172.20.1.26	255.2555.255.0	172.20.1.5	PCRIS1-07P1	PISO 1
OFICINA DE RIS Nº 1	172.20.1.27	255.2555.255.0	172.20.1.5	PCRIS1-08P1	PISO 1
OFICINA DE RIS Nº 1	172.20.1.28	255.2555.255.0	172.20.1.5	PCRIS1-09P1	PISO 1

RIS Nº 2	DIRECCION DE RED	MASCARA DE RED	PUERTA DE ENLACE	NOMBRE DE EQUIPO	PISO
OFICINA DE RIS Nº 2	172.20.2.20	255.2555.255.0	172.20.2.5	PCRIS2-01P1	PISO 1
OFICINA DE RIS Nº 2	172.20.2.21	255.2555.255.0	172.20.2.5	PCRIS2-02P1	PISO 1
OFICINA DE RIS Nº 2	172.20.2.22	255.2555.255.0	172.20.2.5	PCRIS2-03P1	PISO 1
OFICINA DE RIS Nº 2	172.20.2.23	255.2555.255.0	172.20.2.5	PCRIS2-04P1	PISO 1
OFICINA DE RIS Nº 2	172.20.2.24	255.2555.255.0	172.20.2.5	PCRIS2-05P1	PISO 1
OFICINA DE RIS Nº 2	172.20.2.25	255.2555.255.0	172.20.2.5	PCRIS2-06P1	PISO 1
OFICINA DE RIS Nº 2	172.20.2.26	255.2555.255.0	172.20.2.5	PCRIS2-07P1	PISO 1
OFICINA DE RIS Nº 2	172.20.2.27	255.2555.255.0	172.20.2.5	PCRIS2-08P1	PISO 1
OFICINA DE RIS Nº 2	172.20.2.28	255.2555.255.0	172.20.2.5	PCRIS2-09P1	PISO 1

RIS Nº 3	DIRECCION DE RED	MASCARA DE RED	PUERTA DE ENLACE	NOMBRE DE EQUIPO	PISO
OFICINA DE RIS Nº 3	172.20.3.20	255.2555.255.0	172.20.3.5	PCRIS3-01P1	PISO 1
OFICINA DE RIS Nº 3	172.20.3.21	255.2555.255.0	172.20.3.5	PCRIS3-02P1	PISO 1
OFICINA DE RIS Nº 3	172.20.3.22	255.2555.255.0	172.20.3.5	PCRIS3-03P1	PISO 1
OFICINA DE RIS Nº 3	172.20.3.23	255.2555.255.0	172.20.3.5	PCRIS3-04P1	PISO 1
OFICINA DE RIS Nº 3	172.20.3.24	255.2555.255.0	172.20.3.5	PCRIS3-05P1	PISO 1
OFICINA DE RIS Nº 3	172.20.3.25	255.2555.255.0	172.20.3.5	PCRIS3-06P1	PISO 1
OFICINA DE RIS Nº 3	172.20.3.26	255.2555.255.0	172.20.3.5	PCRIS3-07P1	PISO 1
OFICINA DE RIS Nº 3	172.20.3.27	255.2555.255.0	172.20.3.5	PCRIS3-08P1	PISO 1
OFICINA DE RIS Nº 3	172.20.3.28	255.2555.255.0	172.20.3.5	PCRIS3-09P1	PISO 1

RIS Nº 4	DIRECCION DE RED	MASCARA DE RED	PUERTA DE ENLACE	NOMBRE DE EQUIPO	PISO
OFICINA DE RIS Nº4	172.20.4.20	255.2555.255.0	172.20.4.5	PCRIS4-01P1	PISO 1
OFICINA DE RIS Nº4	172.20.4.21	255.2555.255.0	172.20.4.5	PCRIS4-02P1	PISO 1
OFICINA DE RIS Nº4	172.20.4.22	255.2555.255.0	172.20.4.5	PCRIS4-03P1	PISO 1
OFICINA DE RIS Nº4	172.20.4.23	255.2555.255.0	172.20.4.5	PCRIS4-04P1	PISO 1
OFICINA DE RIS Nº4	172.20.4.24	255.2555.255.0	172.20.4.5	PCRIS4-05P1	PISO 1
OFICINA DE RIS Nº4	172.20.4.25	255.2555.255.0	172.20.4.5	PCRIS4-06P1	PISO 1
OFICINA DE RIS Nº4	172.20.4.26	255.2555.255.0	172.20.4.5	PCRIS4-07P1	PISO 1
OFICINA DE RIS Nº4	172.20.4.27	255.2555.255.0	172.20.4.5	PCRIS4-08P1	PISO 1
OFICINA DE RIS Nº4	172.20.4.28	255.2555.255.0	172.20.4.5	PCRIS4-09P1	PISO 1

RIS Nº 5	DIRECCION DE RED	MASCARA DE RED	PUERTA DE ENLACE	NOMBRE DE EQUIPO	PISO
OFICINA DE RIS Nº5	172.20.5.20	255.2555.255.0	172.20.5.5	PCRIS5-01P1	PISO 1
OFICINA DE RIS Nº5	172.20.5.21	255.2555.255.0	172.20.5.5	PCRIS5-02P1	PISO 1
OFICINA DE RIS Nº5	172.20.5.22	255.2555.255.0	172.20.5.5	PCRIS5-03P1	PISO 1
OFICINA DE RIS Nº5	172.20.5.23	255.2555.255.0	172.20.5.5	PCRIS5-04P1	PISO 1
OFICINA DE RIS Nº5	172.20.5.24	255.2555.255.0	172.20.5.5	PCRIS5-05P1	PISO 1
OFICINA DE RIS Nº5	172.20.5.25	255.2555.255.0	172.20.5.5	PCRIS5-06P1	PISO 1
OFICINA DE RIS Nº5	172.20.5.26	255.2555.255.0	172.20.5.5	PCRIS5-07P1	PISO 1
OFICINA DE RIS Nº5	172.20.5.27	255.2555.255.0	172.20.5.5	PCRIS5-08P1	PISO 1
OFICINA DE RIS Nº5	172.20.5.28	255.2555.255.0	172.20.5.5	PCRIS5-09P1	PISO 1

RIS Nº 6	DIRECCION DE RED	MASCARA DE RED	PUERTA DE ENLACE	NOMBRE DE EQUIPO	PISO
OFICINA DE RIS Nº6	172.20.6.20	255.2555.255.0	172.20.6.5	PCRIS6-01P1	PISO 1
OFICINA DE RIS Nº6	172.20.6.21	255.2555.255.0	172.20.6.5	PCRIS6-02P1	PISO 1
OFICINA DE RIS Nº6	172.20.6.22	255.2555.255.0	172.20.6.5	PCRIS6-03P1	PISO 1
OFICINA DE RIS Nº6	172.20.6.23	255.2555.255.0	172.20.6.5	PCRIS6-04P1	PISO 1
OFICINA DE RIS Nº6	172.20.6.24	255.2555.255.0	172.20.6.5	PCRIS6-05P1	PISO 1
OFICINA DE RIS Nº6	172.20.6.25	255.2555.255.0	172.20.6.5	PCRIS6-06P1	PISO 1
OFICINA DE RIS Nº6	172.20.6.26	255.2555.255.0	172.20.6.5	PCRIS6-07P1	PISO 1
OFICINA DE RIS Nº6	172.20.6.27	255.2555.255.0	172.20.6.5	PCRIS6-08P1	PISO 1
OFICINA DE RIS Nº6	172.20.6.28	255.2555.255.0	172.20.6.5	PCRIS6-09P1	PISO 1

RIS Nº 7	DIRECCION DE RED	MASCARA DE RED	PUERTA DE ENLACE	NOMBRE DE EQUIPO	PISO
OFICINA DE RIS Nº 7	172.20.7.20	255.2555.255.0	172.20.7.5	PCRIS6-01P1	PISO 1
OFICINA DE RIS Nº 7	172.20.7.21	255.2555.255.0	172.20.7.5	PCRIS6-02P1	PISO 1
OFICINA DE RIS Nº 7	172.20.7.22	255.2555.255.0	172.20.7.5	PCRIS6-03P1	PISO 1
OFICINA DE RIS Nº 7	172.20.7.23	255.2555.255.0	172.20.7.5	PCRIS6-04P1	PISO 1
OFICINA DE RIS Nº 7	172.20.7.27	255.2555.255.0	172.20.7.5	PCRIS6-05P1	PISO 1
OFICINA DE RIS Nº 7	172.20.7.25	255.2555.255.0	172.20.7.5	PCRIS6-06P1	PISO 1
OFICINA DE RIS Nº 7	172.20.7.26	255.2555.255.0	172.20.7.5	PCRIS6-07P1	PISO 1
OFICINA DE RIS Nº 7	172.20.7.27	255.2555.255.0	172.20.7.5	PCRIS6-08P1	PISO 1
OFICINA DE RIS Nº 7	172.20.7.28	255.2555.255.0	172.20.7.5	PCRIS6-09P1	PISO 1

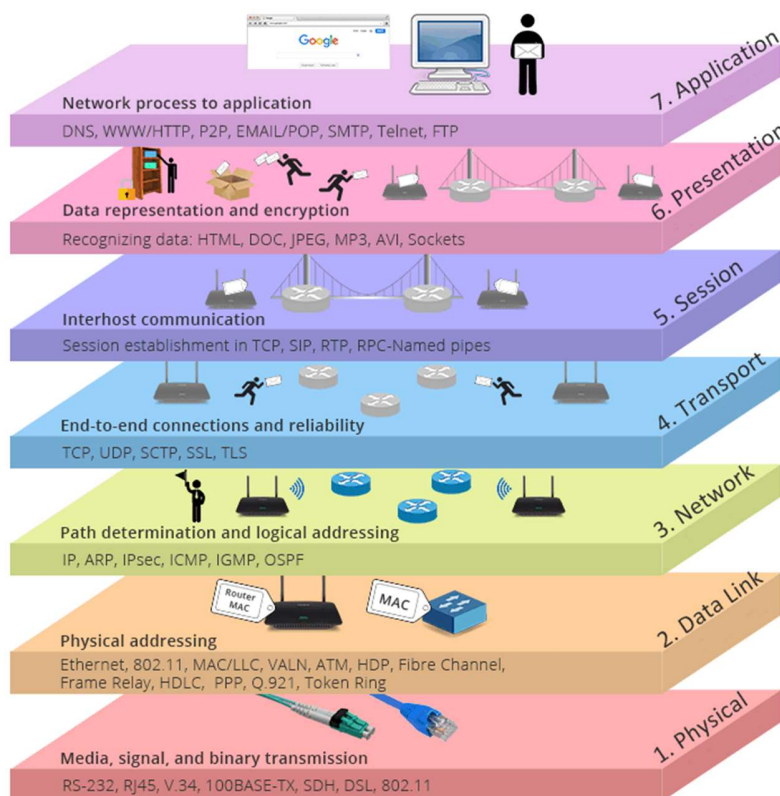
4.5.6. Seleccionar Protocolos para Switching y Routing

Protocolos LAN

Los sistemas informáticos no cuentan con la capacidad propia de poder transaccionar datos sin apoyo, por lo tanto, no puede haber ninguna conexión entre ellas, ni, aunque pareciera que con un cable LAN sea posible pensar que están conectados. La ayuda consiste en los parámetros de la red, y el alcance que tiene, quienes actúan una capa de mediación y establecen cómo será el intercambio de datos, el enrutamiento, el control de riesgos, etc. De alguna forma esto quiere decir que si hay una posibilidad de conectividad entre computadoras esto es gracias a que están conectados en una misma red y cuentan con similares situaciones que las facilita.

En efecto en el mundo de las conexiones LAN o lo que sería su extensión más compleja se utiliza la OSI que están validadas por la ISO, supone un hito importante por comprender el lenguaje particular de las redes informáticas, su complejidad entre otras razones estructurales.

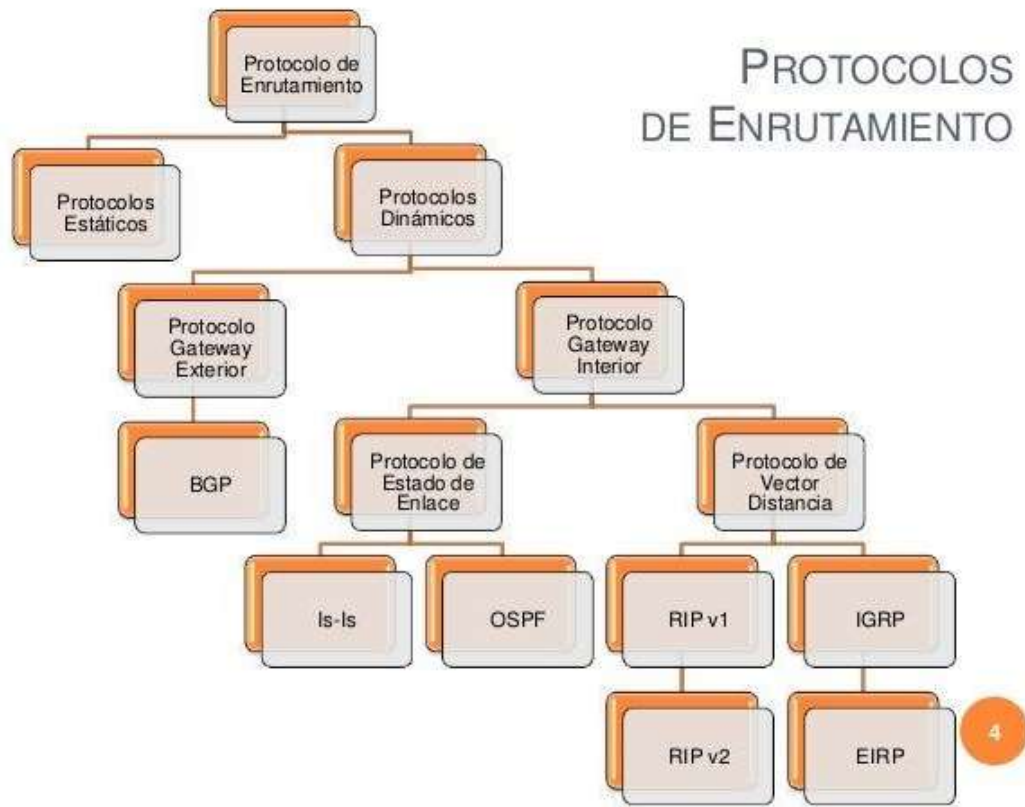
Figura 11. Protocolos LAN



4.5.7. Protocolos de Ruteo

El ruteo es el proceso de mover los datos entre diferentes redes de capa 3, eso en su forma más básica. Los routers son dispositivos que cumplen con esa función también lo pueden hacer otros dispositivos como los switches.

Figura 12. Protocolos de enrutamiento



El uso de un protocolo de enrutamiento para anunciar las rutas descubiertas por otros medios, como otro protocolo de enrutamiento, rutas estáticas o rutas conectadas directamente, se conoce como entrega. otra vez. A pesar del deseo de ejecutar un solo protocolo de enrutamiento en toda una red IP, el enrutamiento multiprotocolo es popular por una variedad de razones, incluida la estandarización comercial, la gestión de múltiples departamentos por parte de múltiples administradores de red y un entorno de múltiples proveedores. La implementación de diferentes protocolos de enrutamiento suele ser parte del diseño de la red. De cualquier manera, tener un entorno multiprotocolo hace necesaria la redistribución. La redistribución puede ocurrir debido a diferencias en las características del protocolo de

enrutamiento, como métricas, distancia administrativa, capacidades clasificadas y no clasificadas. Estas diferencias deben tenerse en cuenta para que la redistribución sea exitosa.

Enrutamiento Estático. Es una de las formas manuales en las cuales se busca incorporar el router a la tipología de red; no siempre resulta positiva, aunque sin embargo si beneficia para lo siguiente

- Cuando hay una sola conexión; y se establece una única ruta estática.
- Un usuario solo desea manejar el mismo la conexión y el enrutamiento sin compartir con otros

Enrutamiento Predeterminado. El router tiene mayor amplitud incluso se va por aquellos routers desconocidos. Es una forma más dinámica y fácil de poder enrutar dominios de salida.

Enrutamiento Dinámico. La forma de enrutar tiene respaldo en tablas de información además puede medirse la consecuencia de las rutas. Es una de las más sugeridas a nivel de redes.

4.5.8. Desarrollar Estrategias de Seguridad

4.5.8.1. Esquema de Zona Desmilitarizada (DMZ)

Para reducir el riesgo de que un servidor con acceso a Internet pueda comprometer la seguridad de la empresa, se recomienda utilizar un firewall y una red local como puente vigilado denominada zona desmilitarizada o DMZ (por su traducción del inglés, Demilitarized Zone).

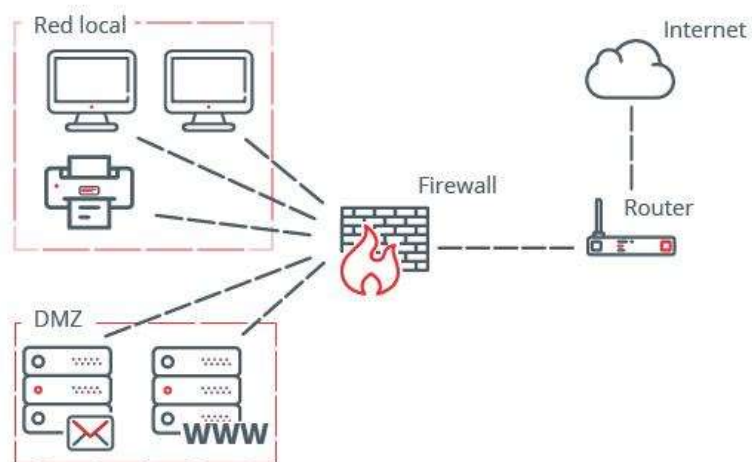
¿Qué es la zona desmilitarizada?

En general, la DMZ permite conexiones tanto desde Internet como desde la red de área local de la empresa donde se encuentran las computadoras del trabajador, pero no permite conexiones desde la DMZ a la red de área local. Esto se debe a que los servidores que tienen acceso a Internet son más vulnerables a ataques que pueden poner en peligro su seguridad. Si

un ciberdelincuente ingresa a un servidor en la DMZ, será muy difícil acceder a la red local de la organización porque las conexiones desde la DMZ están prohibidas.

Los diagramas de red ayudan a las organizaciones y los equipos a visualizar cómo funcionan juntos los dispositivos como las computadoras y la revolución de las comunicaciones. Los diagramas esquemáticos de red le permiten dibujar una imagen de cómo funcionan estas redes, identificar componentes como enrutadores, firewalls y dispositivos, y mostrar visualmente cómo se cruzan. Esta hoja de ruta es un modelo para que los profesionales hagan cosas como comprender y solucionar problemas y errores, ampliar las redes y mantener la seguridad y el cumplimiento. Su organización puede usar un diagrama de red tan detallado o tan grande como sea posible para mostrar solo dispositivos individuales, una sola aplicación o áreas de servicio.

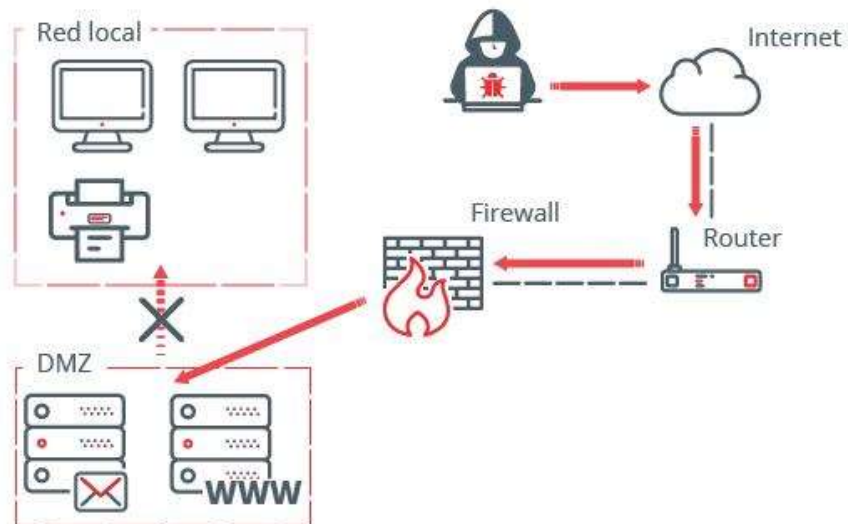
Figura 13. Redes de seguridad



En general, la DMZ permite conexiones tanto desde Internet como desde la red local de la empresa donde se encuentran las computadoras del trabajador, pero no permite conexiones desde la DMZ a la red local. Esto se debe a que los servidores que tienen acceso a Internet son más vulnerables a ataques que pueden poner en peligro su seguridad. Si un

ciberdelincuente ingresa a un servidor en una zona desmilitarizada, el acceso a la red local de la organización será más difícil porque las conexiones desde la zona desmilitarizada están prohibidas.

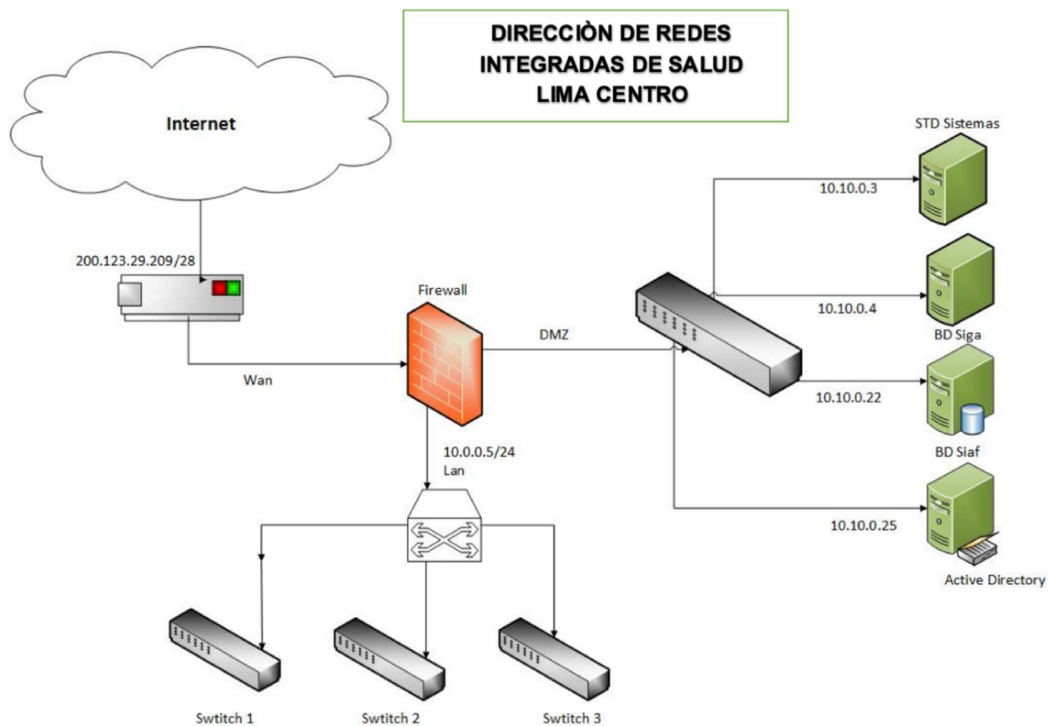
Figura 14. Red local



Los diagramas de red ayudan a las organizaciones y los equipos a visualizar cómo funcionan juntos dispositivos como computadoras y redes como telecomunicaciones. Los diagramas de red le permiten representar cómo funcionan estas redes activas, identificando componentes como enrutadores, firewalls y dispositivos, y mostrando visualmente cómo se cruzan. Esta hoja de ruta sirve como plantilla para los profesionales que hacen cosas como comprender y resolver problemas y errores, escalar redes y mantener la seguridad y el cumplimiento.

Su organización puede usar diagramas de red tan detallados o extensos como sea posible para mostrar dispositivos individuales, aplicaciones individuales o simplemente áreas de servicio.

Figura 15. Integradas de salud



4.5.9. Desarrollar Estrategias de Administración de Red

4.5.9.1. Plan de Mantenimiento a los Dispositivos de Red de Servidores e incluso UPS

El presente documento es el procedimiento con respecto al mantenimiento a los dispositivos de red y servidores. Esta presenta acta se realizó previa coordinación de una visita para el levantamiento de algunos puntos (ANEXO 6).

4.5.9.2. Acta de Constitución de Proyecto

El presente documento del acta de constitución se realizó en conjunto con la oficina encargada de la institución.

Esta presenta acta se realizó previa coordinación de una visita para el levantamiento de algunos puntos (ANEXO 7).

4.6. FASE 3: Desarrollar Diseño Físico

Para el desarrollo del diseño se está montando en una Pc que hace la función de servidor firewall en la sede principal DIRIS Lima Centro, y por el otro lado el centro de salud tenemos un equipo como servidor firewall en ambos casos con el sistema operativo SUSE Linux Enterprise Server.

Tabla 28. Lista de equipos utilizados.

	SEDE PRINCIPAL	CENTRO DE SALUD MATERNO INFANTIL EL PORVENIR
PROCESADOR	20GB	CORE I3- TERCERA GENERACION
MEMORIA RAMM	300 GB HOT SWAP(RAID1)	4GB
ALMACENAMIENTO	INTEL XEON 2.4GHZ	250GB
S.O.	SUSE LINUX	SUSE LINUX O WINDOWS

4.6.1. Seleccionar de Tecnologías y dispositivos para redes de campus

Las tecnologías a utilizar son las siguientes:

SUSE LINUX 11.4

Es un Sistema operativo libre, como particularidades el que permite configuraciones de red, de cortafuegos y de administración de usuario.

OPEN VPN 2.14

Es una herramienta de conectividad basado en software libre que permite realizar la conectividad de la red privada virtual (túnel).

4.6.2. Estándares Para la Adquisición de Tecnología y Dispositivos

Esta presenta acta se realizó previa coordinación de una visita para el levantamiento de algunos puntos (ANEXO 8).

4.6.3. Análisis de Factibilidad

Este estudio de factibilidad técnica que se realizó en la Diris Lima Centro se diseñó en el presente proyecto de investigación el cual para su desarrollo se basa en la metodología Top Down, los puntos a considerar fueron el parque informático y el impacto económico que implica el despliegue del diseño tecnológico.

Actualmente la Diris Lima Centro no tiene la manera de desplegar las políticas de seguridad y sistemas de información a los centros de salud de su jurisdicción es por ello la importancia de brindar una solución tecnológica de esta envergadura.

Las Direcciones, Oficinas de la institución manejan como sistema operativo Windows en sus distintas versiones, nuestro diseño se basa en software libre, la implementación del Servidor firewall en Linux (open SuSE 11.4), al cual se le configura el Open VPN, estos sistemas son bastante manejables y se puede instalar en un hardware mínimo y con miras a poder migrarlo a un mejor servidor de hardware.

Se procede a mencionar los equipos utilizados para demostrar la operatividad del presente proyecto:

4.6.4. Factibilidad Técnica

En coordinación con la Oficina de Tecnologías de la información la cual es encargada de la parte tecnológica de esta institución se pudo verificar que cuenta con servidores los cuales cumplen con el hardware mínimo para la implementación del presente proyecto.

En las visitas realizadas a los establecimientos de salud se pudo constatar que cuentan con equipos de cómputo de última generación como antiguos, los cuales realizando el análisis para la presente e implementación cumple con los requisitos mínimos de conexión, esto se pudo constatar en las pruebas realizadas.

Se cuenta con personal con perfiles como: técnicos administrativos, auxiliares los cuales son los encargados del manejo de los equipos de cómputo, la edad aproximada de la persona fluctúa entre los 25 a 62 años, el personal tiene conocimientos de computación en el buen manejo de los equipos de cómputo.

4.6.5. Sistema Operativo

El sistema operativo a utilizarse en esta implementación es software libre Linux Open SuSE 11.4, en el cual se realizará las configuración y segmentaciones de red la cual permitirá conectarse adecuadamente a la red de área local (LAN), posterior a esto se configura la Open VPN la cual permitirá la conexión (túnel) del establecimiento a la sede principal.

4.6.6. Características del hardware disponible para la Implementación

Las características técnicas de los equipos de cómputo con el que se dispone actualmente para el presente proyecto, se muestran a continuación:

Tabla 29. Características del hardware

EQUIPO	DESCRIPCION	CAPACIDAD
SERVIDOR	MEMORIA RAMM	20GB
	DISCO DURO	300GB HOT SWAP (RAID 1)
	MICROPROCESADOR	INTEL XEON 2.4GHZ
COMPUTADORA1	MEMORIA RAMM	4GB
	DISCO DURO	500GB
	MICROPROCESADOR	CORE I3 CUARTA GENERACION DE 3.5GHZ
COMPUTADORA2	MEMORIA RAMM	8GB
	DISCO DURO	1TB
	MICROPROCESADOR	CORE I7 NOVENA GENERACION DE 2.9GHZ

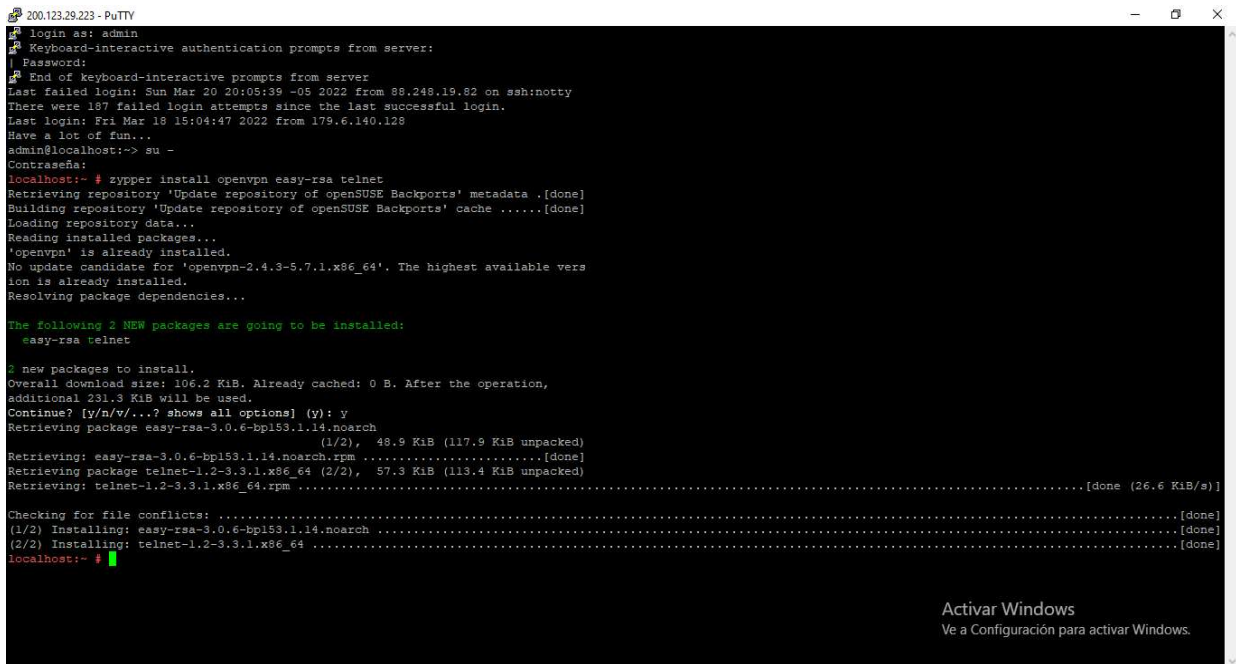
4.6.7. Conclusión de factibilidad Técnica

Como se puede apreciar líneas arriba según la evaluación realizada para el presente proyecto se cuenta con los equipos necesarios tanto en hardware, software y personal capacitado para la implementación de este proyecto el cual será una mejora enorme en las labores diarias de los usuarios de los establecimientos de salud.

4.7.FASE 04: Probar, Optimizar y documentar Diseño

Figura 16. Configuración de servicio VPN

zypper install openvpn easy-rsa telnet



```
200.123.29.223 - PuTTY
login as: admin
Keyboard-interactive authentication prompts from server:
| Password:
| End of keyboard-interactive prompts from server
Last failed login: Sun Mar 20 20:05:39 -05 2022 from 88.248.19.82 on ssh:notty
There were 187 failed login attempts since the last successful login.
Last login: Fri Mar 18 15:04:47 2022 from 179.6.140.128
Have a lot of fun...
admin@localhost:~> su -
Contraseña:
localhost:~ # zypper install openvpn easy-rsa telnet
Retrieving repository 'Update repository of openSUSE Backports' metadata .[done]
Building repository 'Update repository of openSUSE Backports' cache .....[done]
Loading repository data...
Reading installed packages...
'openvpn' is already installed.
No update candidate for 'openvpn-2.4.3-5.7.1.x86_64'. The highest available version is already installed.
Resolving package dependencies...

The following 2 NEW packages are going to be installed:
+easy-rsa telnet

2 new packages to install.
Overall download size: 106.2 KiB. Already cached: 0 B. After the operation,
additional 231.3 KiB will be used.
Continue? [y/n/v/...? shows all options] (y): y
Retrieving package easy-rsa-3.0.6-bp153.1.14.noarch
(1/2), 48.9 KiB (117.9 KiB unpacked)
Retrieving: easy-rsa-3.0.6-bp153.1.14.noarch.rpm .....[done]
Retrieving package telnet-1.2-3.3.1.x86_64 (2/2), 57.3 KiB (113.4 KiB unpacked)
Retrieving: telnet-1.2-3.3.1.x86_64.rpm .....[done (26.6 KiB/s)]

Checking for file conflicts: .....[done]
(1/2) Installing: easy-rsa-3.0.6-bp153.1.14.noarch .....[done]
(2/2) Installing: telnet-1.2-3.3.1.x86_64 .....[done]
localhost:~ #
```

Generación de Certificados y Llaves

En cuanto a la certificación es necesario previamente hacer ajustes al VPN. De esta forma se obtiene la llave y la certificación. En ese sentido, se necesita entrar al directorio /etc/openvpn, y se origina el archivo varsy luego vars.example y se inicia la edición:

Figura 17. Generación de certificados y llaves



```
200.123.29.223 - PuTTY
localhost:~ # cp /etc/easy-rsa/vars.example /etc/easy-rsa/vars
localhost:~ # vi /etc/easy-rsa/vars
```

```

set_var EASYRSA_PKI          "/etc/pki"

# Define X509 DN mode.
# This is used to adjust what elements are included in the Subject field as the DN
# (this is the "Distinguished Name.")
# Note that in 'cn_only' mode the Organizational fields further below aren't used.
#
# Choices are:
#   'cn_only' - use just a CN value
#   'org'     - use the "traditional" Country/Province/City/Org/OU/email/CN format

set_var EASYRSA_DN          "cn_only"

# Organizational fields (used with 'org' mode and ignored in 'cn_only' mode.)
# These are the default values for fields which will be placed in the
# certificate. Don't leave any of these fields blank, although interactively
# you may omit any specific field by typing the "." symbol (not valid for
# email.)

set_var EASYRSA_REQ_COUNTRY  "PE"
set_var EASYRSA_REQ_PROVINCE "LIMA"
set_var EASYRSA_REQ_CITY    "LIMA"
set_var EASYRSA_REQ_ORG     "DIRIS-LIMA-CENTRO"
set_var EASYRSA_REQ_EMAIL   "admin@dirislimacentro.gob.pe"
set_var EASYRSA_REQ_OU      "AREA DE SISTEMAS"

# Choose a size in bits for your keypairs. The recommended value is 2048. Using
# 2048-bit keys is considered more than sufficient for many years into the
# future. Larger key sizes will slow down TLS negotiation and make key/DN
# generation take much longer. Values up to 4096 should be accepted by most
# software. Only used when the crypto alg is rsa (see below.)

set_var EASYRSA_KEY_SIZE    2048

# The default crypto mode is 'rsa'; so can enable elliptic curve support.
# Note that not all software supports ECC. So use care when enabling it.

```

Desde el directorio `/etc/openvpn` se inicia a trabajar el comando `pktool` para originar los permisos de **CA**:

```

200.123.29.223 - PuTTY
localhost:/etc/openvpn # cd /etc/openvpn
localhost:/etc/openvpn # easyrsa init-pki

Note: using Easy-RSA configuration from: /etc/easy-rsa/vars

init-pki complete; you may now create a CA or requests.
Your newly created PKI dir is: /etc/openvpn/pki

localhost:/etc/openvpn #

```

Se origina la certificación de la **CA**:

Figura 18. Certificación de la CA

```

200.123.29.223 - PuTTY
localhost:/etc/openvpn # cd /etc/openvpn
localhost:/etc/openvpn # easyrsa init-pki

Note: using Easy-RSA configuration from: /etc/easy-rsa/vars

init-pki complete; you may now create a CA or requests.
Your newly created PKI dir is: /etc/openvpn/pki

localhost:/etc/openvpn # easyrsa build-ca nopass

Note: using Easy-RSA configuration from: /etc/easy-rsa/vars

Using SSL: openssl OpenSSL 1.1.1d 10 Sep 2019
Generating RSA private key, 2048 bit long modulus (2 primes)
.....+++++
e is 65537 (0x010001)
Can't load /etc/openvpn/pki/.rnd into RNG
139878881601344:error:2406F079:random number generator:RAND_load_file:Cannot open file:crypto/rand/randfile.c:98:Filename=/etc/openvpn/pki/.rnd
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Common Name (eg: your user, host, or server name) [Easy-RSA CA]:ares

CA creation complete and you may now import and sign cert requests.
Your new CA certificate file for publishing is at:
/etc/openvpn/pki/ca.crt

```


Figura 19. Generación de software

```
localhost:/etc/openvpn # easyrsa sign-req server servidor
Note: using Easy-RSA configuration from: /etc/easy-rsa/vars
Using SSL: openssl OpenSSL 1.1.1d 10 Sep 2019

You are about to sign the following certificate.
Please check over the details shown below for accuracy. Note that this request
has not been cryptographically verified. Please be sure it came from a trusted
source or that you have verified the request checksum with the sender.

Request subject, to be signed as a server certificate for 1080 days:
subject=
  commonName          = ares

Type the word 'yes' to continue, or any other input to abort.
Confirm request details: yes
Using configuration from /etc/easy-rsa/easyrsa.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
commonName            :ASN.1 12:'ares'
Certificate is to be certified until Mar  5 01:33:22 2025 GMT (1080 days)

Write out database with 1 new entries
Data Base Updated

Certificate created at: /etc/openvpn/pki/issued/servidor.crt
localhost:/etc/openvpn #
```

Configuración de Servicio

El archivo **server.conf** permitirá abrir **OpenVPN** que viene a ser el mismo archivo ubicado en `/usr/share/doc/packages/openvpn/sample-config-files` como se aprecia a continuación:

Figura 20. Configuración de servicio

```
localhost:/etc/openvpn # cp /usr/share/doc/packages/openvpn/sample-config-files/server.conf /etc/openvpn
localhost:/etc/openvpn # vi /etc/openvpn/server.conf
```

Edición y Configuración del Archivo server.conf

Figura 21. Generación de certificados y llaves

```
# from the Network Connections panel if you
# have more than one. On XP SP2 or higher,
# you may need to selectively disable the
# Windows firewall for the TAP adapter.
# Non-Windows systems usually don't need this.
;dev-node MyTap

# SSL/TLS root certificate (ca), certificate
# (cert), and private key (key). Each client
# and the server must have their own cert and
# key file. The server and all clients will
# use the same ca file.
#
# See the "easy-rsa" directory for a series
# of scripts for generating RSA certificates
# and private keys. Remember to use
# a unique Common Name for the server
# and each of the client certificates.
#
# Any X509 key management system can be used.
# OpenVPN can also use a PKCS #12 formatted key file
# (see "pkcs12" directive in man page).
ca /etc/openvpn/ca.crt
cert /etc/openvpn/server.crt
key /etc/openvpn/server.key # This file should be kept secret
tls-auth /etc/openvpn/ta.key 0
cipher AES-256-GCM

comp-lzo

# SE ENCUENTRAN LOS CERTIFICADOS REVOCADOS.
crl-verify /etc/openvpn/pki/crl.pem

# -- CONFIGURACION DEL MTU DE LA INTERFAZ TUN:
tun-mtu 1500

;activate log with each connected user
```

Contenido del archivo de configuración del servicio open vpn.

Figura 22. Open VPN

```
port 1194
proto tcp

;dev tun
dev tun

;dev-node MyTap

ca /etc/openvpn/easy-rsa/keys/ca.crt
cert /etc/openvpn/easy-rsa/keys/server.crt
key /etc/openvpn/easy-rsa/keys/server.key
dh /etc/openvpn/easy-rsa/keys/dh1024.pem

server 11.6.0.0 255.255.255.0

;remote 192.168.1.1 1194
;remote 192.168.1.2 1194
;remote 192.168.1.3 1194
;remote 192.168.1.4 1194
;remote 192.168.1.5 1194
;remote 192.168.1.6 1194
;remote 192.168.1.7 1194
;remote 192.168.1.8 1194
;remote 192.168.1.9 1194
;remote 192.168.1.10 1194
;remote 192.168.1.11 1194
;remote 192.168.1.12 1194
;remote 192.168.1.13 1194
;remote 192.168.1.14 1194
;remote 192.168.1.15 1194
;remote 192.168.1.16 1194
;remote 192.168.1.17 1194
;remote 192.168.1.18 1194
;remote 192.168.1.19 1194
;remote 192.168.1.20 1194
;remote 192.168.1.21 1194
;remote 192.168.1.22 1194
;remote 192.168.1.23 1194
;remote 192.168.1.24 1194
;remote 192.168.1.25 1194
;remote 192.168.1.26 1194
;remote 192.168.1.27 1194
;remote 192.168.1.28 1194
;remote 192.168.1.29 1194
;remote 192.168.1.30 1194

client-config-dir ccd
ccd-exclusive

;remote 192.168.1.1 1194
;remote 192.168.1.2 1194
;remote 192.168.1.3 1194
;remote 192.168.1.4 1194
;remote 192.168.1.5 1194
;remote 192.168.1.6 1194
;remote 192.168.1.7 1194
;remote 192.168.1.8 1194
;remote 192.168.1.9 1194
;remote 192.168.1.10 1194
;remote 192.168.1.11 1194
;remote 192.168.1.12 1194
;remote 192.168.1.13 1194
;remote 192.168.1.14 1194
;remote 192.168.1.15 1194
;remote 192.168.1.16 1194
;remote 192.168.1.17 1194
;remote 192.168.1.18 1194
;remote 192.168.1.19 1194
;remote 192.168.1.20 1194
;remote 192.168.1.21 1194
;remote 192.168.1.22 1194
;remote 192.168.1.23 1194
;remote 192.168.1.24 1194
;remote 192.168.1.25 1194
;remote 192.168.1.26 1194
;remote 192.168.1.27 1194
;remote 192.168.1.28 1194
;remote 192.168.1.29 1194
;remote 192.168.1.30 1194

;learn-address ./script

;push "dhcp-option DNS 192.168.1.1"
;push "dhcp-option DNS 192.168.1.2"

;client-to-client

;duplicate-cn

keepalive 10 120

;tls-auth ta.key 0 # Make this 0 to disable

;cipher BF-CBC # Blowfish (default)
;cipher AES-128-CBC # AES
;cipher AES-256-CBC # 256-bit AES

comp-lzo

"server.conf" 69L, 1192C
```

Contenido que muestra las llaves creadas para los clientes que se conectarán mediante la vpn.

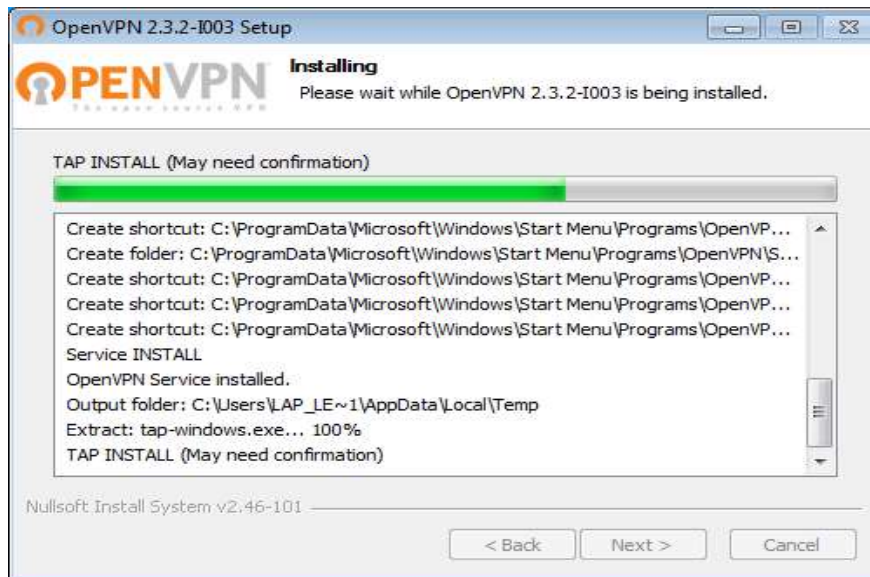
Figura 23. Conexión VPN

```
167 ll
168 history
linux-jsoj:/etc/openvpn/easy-rsa/keys # ls -l
total 84
-rw-r--r-- 1 root root 3572 Mar 23 08:35 01.pem
-rw-r--r-- 1 root root 3670 Mar 23 08:37 02.pem
-rw-r--r-- 1 root root 3572 Mar 23 08:41 03.pem
-rw-r--r-- 1 root root 1249 Mar 23 08:34 ca.crt
-rw-r--r-- 1 root root 916 Mar 23 08:34 ca.key
-rw-r--r-- 1 root root 3572 Mar 23 08:35 cliente1.crt
-rw-r--r-- 1 root root 688 Mar 23 08:35 cliente1.csr
-rw-r--r-- 1 root root 912 Mar 23 08:35 cliente1.key
-rw-r--r-- 1 root root 3572 Mar 23 08:41 cliente2.crt
-rw-r--r-- 1 root root 688 Mar 23 08:40 cliente2.csr
-rw-r--r-- 1 root root 912 Mar 23 08:40 cliente2.key
-rw-r--r-- 1 root root 245 Mar 23 08:34 dh1024.pem
-rw-r--r-- 1 root root 334 Mar 23 08:41 index.txt
-rw-r--r-- 1 root root 21 Mar 23 08:41 index.txt.attr
-rw-r--r-- 1 root root 21 Mar 23 08:37 index.txt.attr.old
-rw-r--r-- 1 root root 222 Mar 23 08:37 index.txt.old
-rw-r--r-- 1 root root 3 Mar 23 08:41 serial
-rw-r--r-- 1 root root 3 Mar 23 08:37 serial.old
-rw-r--r-- 1 root root 3670 Mar 23 08:37 server.crt
-rw-r--r-- 1 root root 688 Mar 23 08:37 server.csr
-rw-r--r-- 1 root root 916 Mar 23 08:37 server.key
linux-jsoj:/etc/openvpn/easy-rsa/keys # cd ..
linux-jsoj:/etc/openvpn/easy-rsa # ll
total 92
drwxr-xr-x 2 root root 4096 Mar 23 16:39 2.0
-rw-r--r-- 1 root root 6075 Mar 23 08:26 README
drwxr-xr-x 2 root root 4096 Mar 23 16:39 Windows
-rw-r--r-- 1 root root 242 Mar 23 08:26 build-ca
-rw-r--r-- 1 root root 228 Mar 23 08:26 build-dh
-rw-r--r-- 1 root root 529 Mar 23 08:26 build-inter
-rw-r--r-- 1 root root 516 Mar 23 08:26 build-key
-rw-r--r-- 1 root root 424 Mar 23 08:26 build-key-pass
-rw-r--r-- 1 root root 695 Mar 23 08:26 build-key-pkcs12
-rw-r--r-- 1 root root 662 Mar 23 08:26 build-key-server
-rw-r--r-- 1 root root 466 Mar 23 08:26 build-req
-rw-r--r-- 1 root root 402 Mar 23 08:26 build-req-pass
-rw-r--r-- 1 root root 280 Mar 23 08:26 clean-all
drwxr-xr-x 2 root root 4096 Mar 23 16:39 keys
-rw-r--r-- 1 root root 264 Mar 23 08:26 list-ctrl
-rw-r--r-- 1 root root 268 Mar 23 08:26 make-ctrl
-rw-r--r-- 1 root root 7487 Mar 23 08:26 openssl.cnf
-rw-r--r-- 1 root root 268 Mar 23 08:26 revoke-crt
-rw-r--r-- 1 root root 593 Mar 23 08:26 revoke-full
-rw-r--r-- 1 root root 411 Mar 23 08:26 sign-req
-rw-r--r-- 1 root root 1276 Mar 23 08:29 vars
linux-jsoj:/etc/openvpn/easy-rsa #
```

CONFIGURACIÓN EN EL HOST DEL CENTRO DE SALUD

Figura 24. Instalación del software open vpn





Después de realizar la instalación el software “OPEN VPN “se realiza la configuración de la llave de conexión, esta llave es la que integra la conexión de seguridad con el túnel virtual. Muestra el contenido de la llave direccionando a la ip publica asignada.

Figura 25. Direccionamiento IP

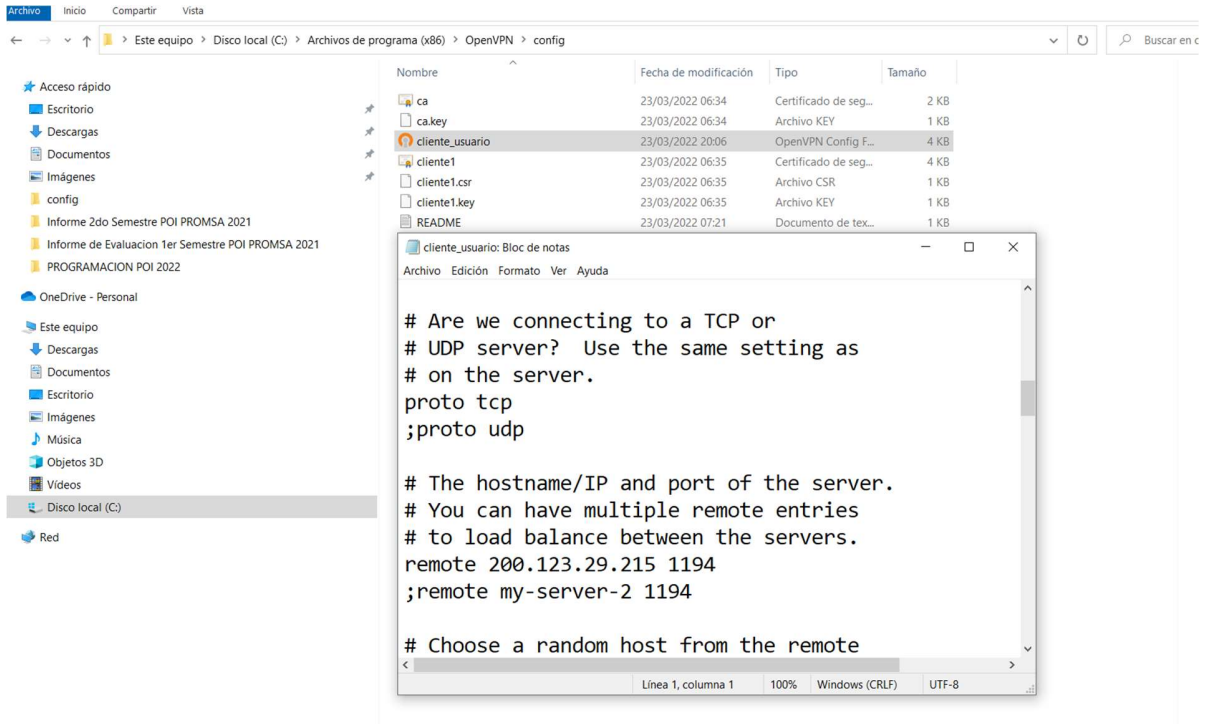
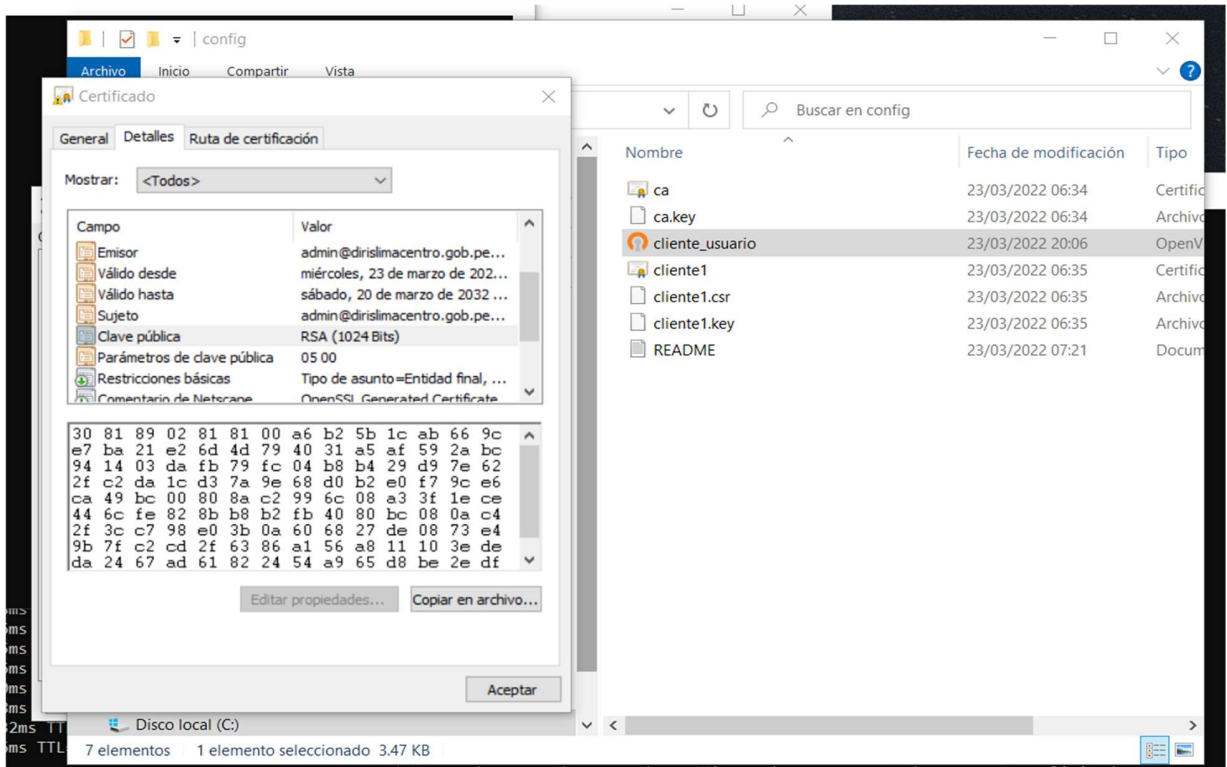
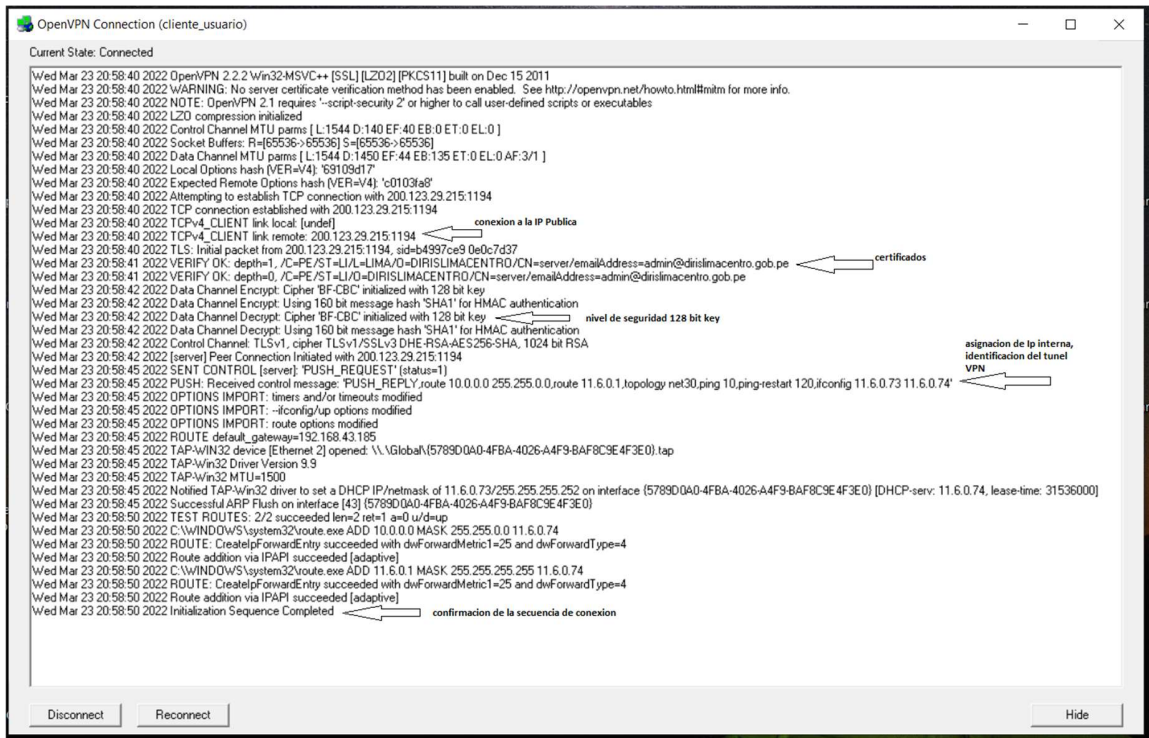


Figura 26. Certificados confianza para túnel VPN.





En este grafico se observa que desde que inicializa la conexión del VPN se realiza con éxito validando los certificados de seguridad (llave).

Figura 27. Muestra la conexión de la vpn

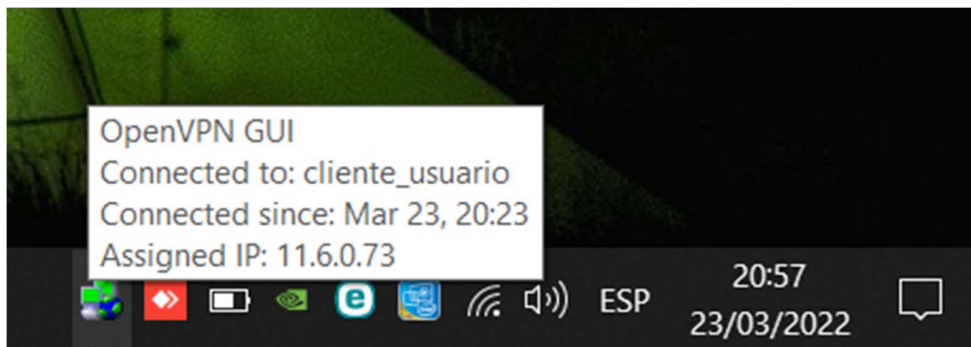
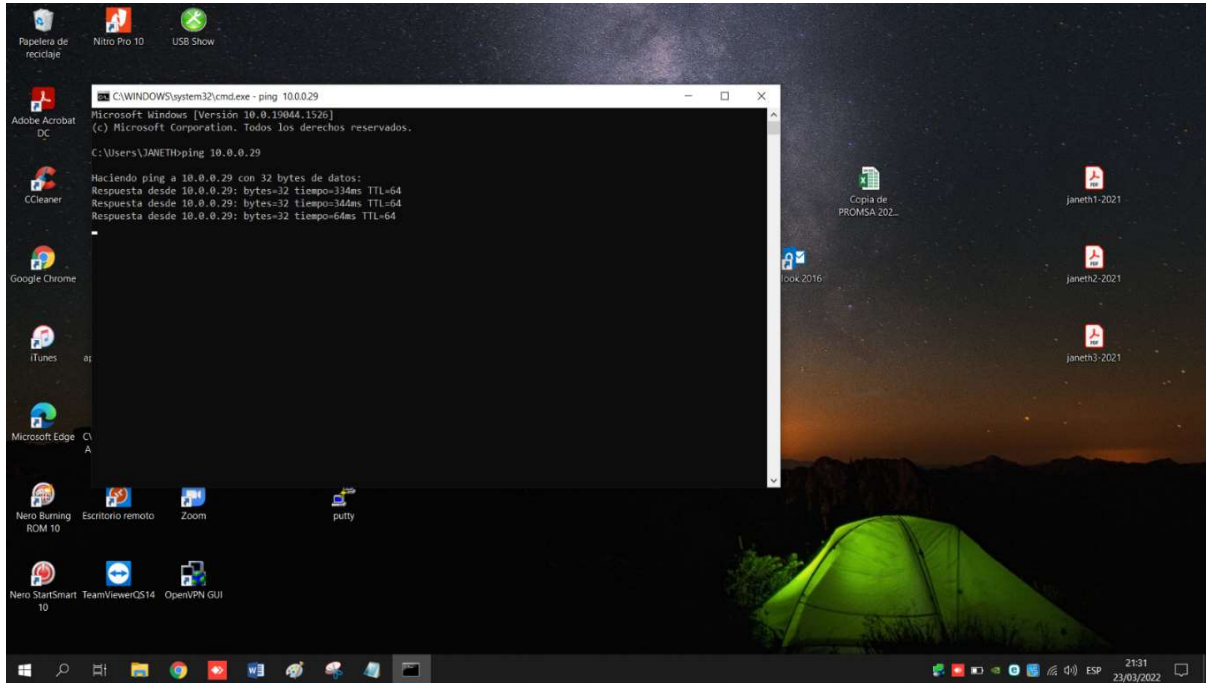


Figura 28. Instalación del software open vpn



Se realiza ping de conexión al servidor de tramite documentario antiguo(consultas).

Figura 29. Trámite documentario antiguo

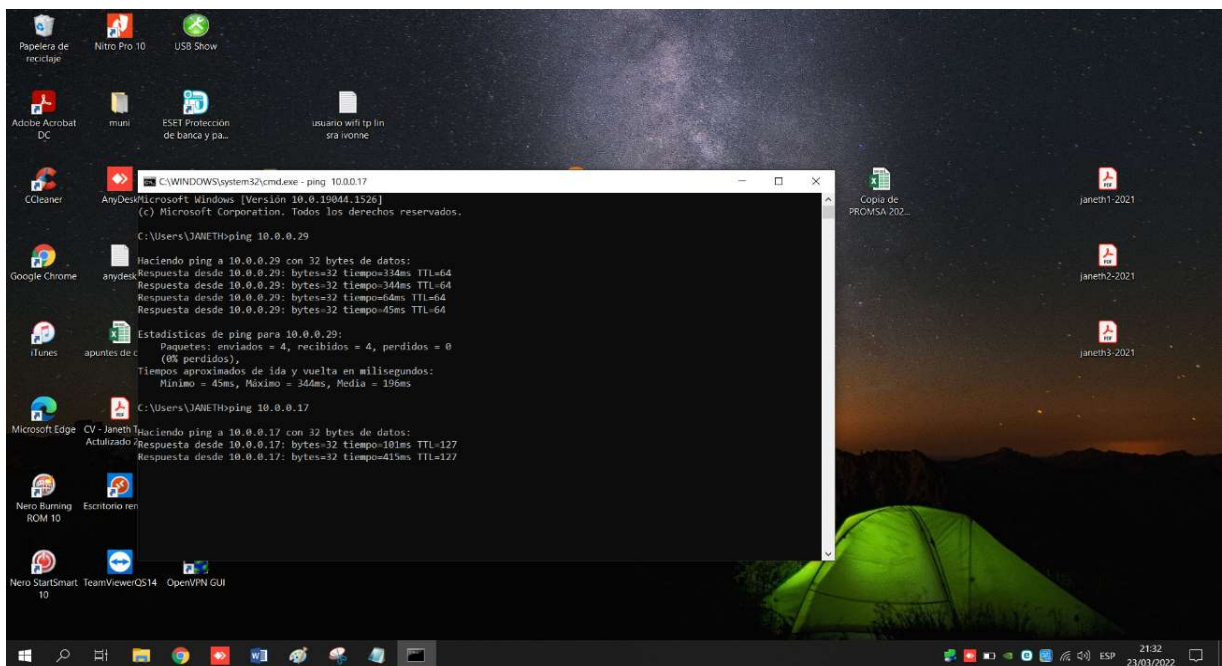
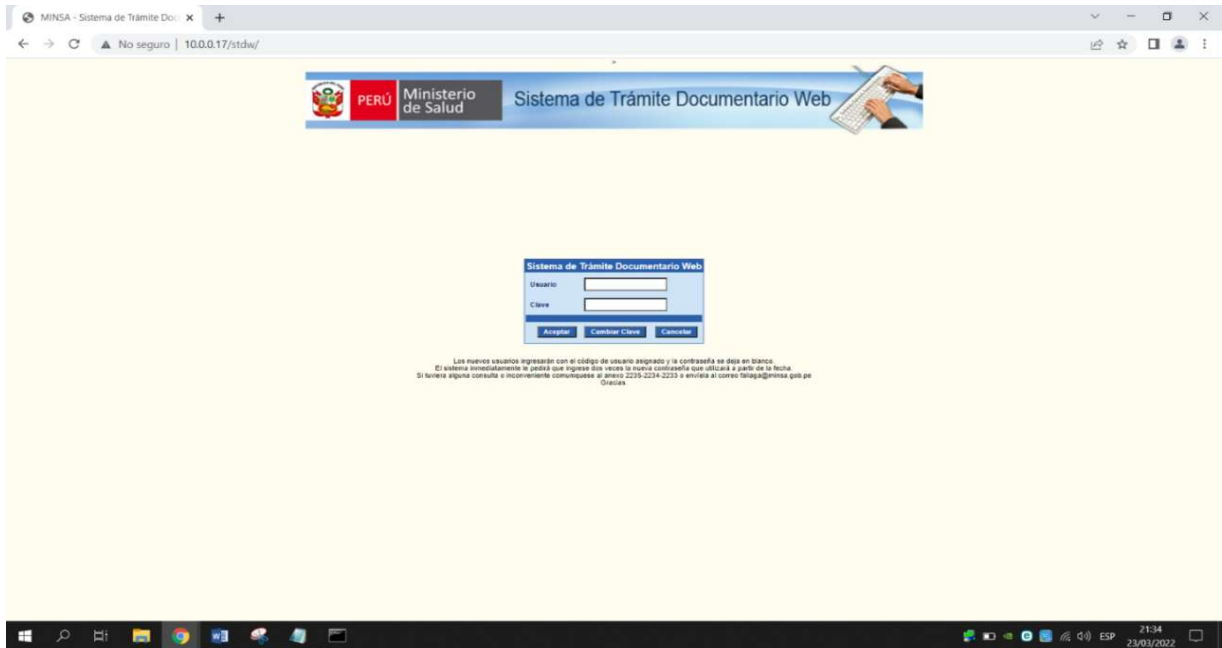


Figura 30. Sistema de trámite documentario



Se realiza ping de conexión al servidor de tramite documentario de producción y sistema de control de asistencia.

Figura 31. Control de asistencia

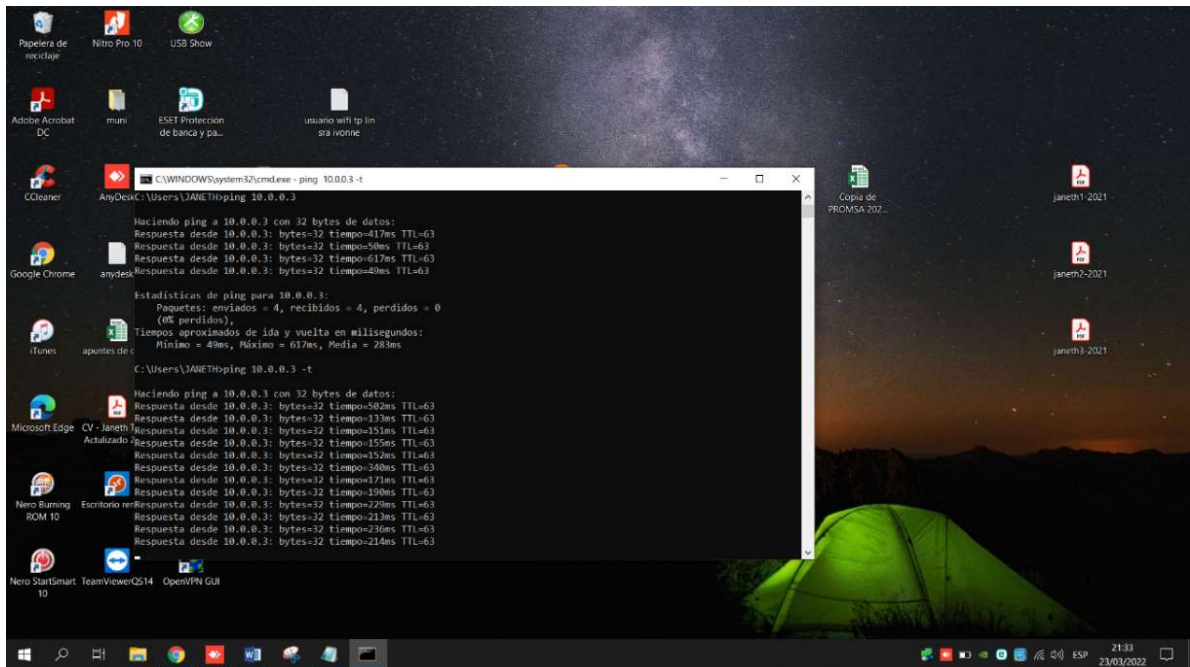
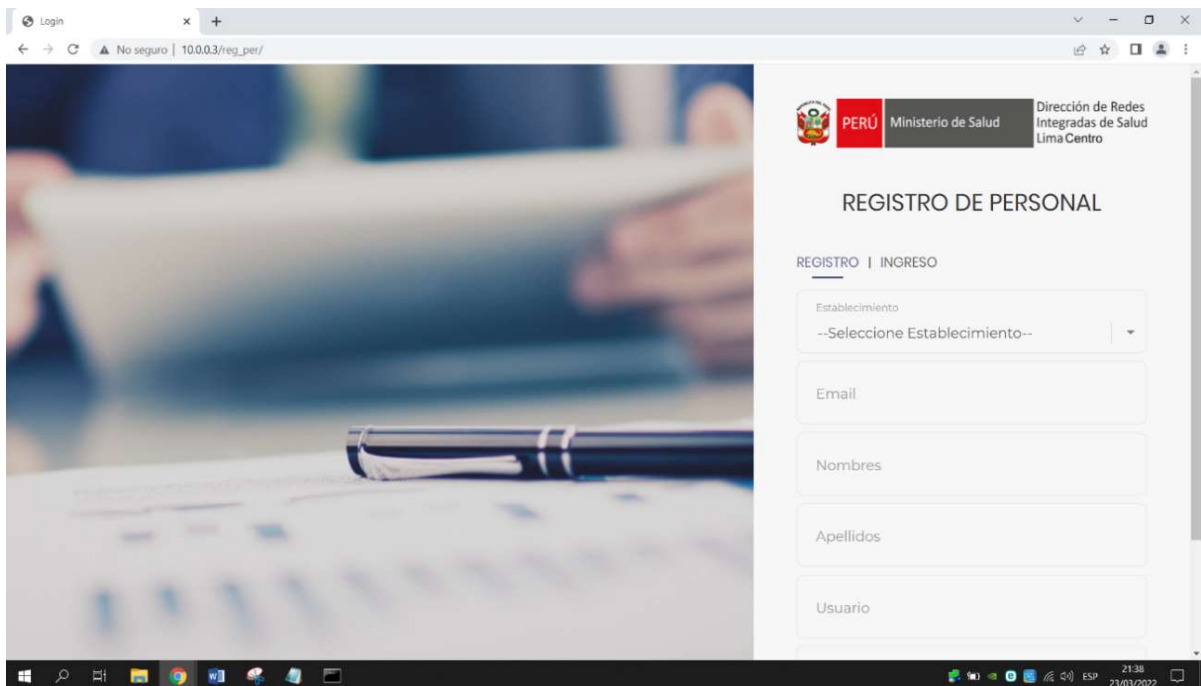


Figura 32. Sistema de trámite documentario



V. CONCLUSIONES

Se demuestra que el uso de la VPN brinda seguridad, confiabilidad y escalabilidad al realizar las conexiones de los hosts (clientes), dado que con este tipo de solución nos permite conectar las sedes remotas a las cuales se brindaran las herramientas con las que cuenta la sede principal dado que en el presente estudio de este proyecto se pudo constatar la vulnerabilidades y necesidades que cuentan los establecimientos de salud.

Esta solución como se aprecia líneas arriba realiza la conexión mediante llaves las cuales cuentan con certificados de seguridad, estos certificados son creados con el dominio de la institución los cuales nos permitirá una administración adecuada de las conexiones que se puedan realizar en su debido momento.

Verificando los certificados y llaves podemos apreciar que estos brindan una confiabilidad en temas de conexión y seguridad dado que estos certificados en RSA de 1024 bits basados en algoritmos, son bastantes seguros impidiendo así algún tipo de vulnerabilidades que se pueda dar.

Esta solución nos permitirá adaptarnos según las necesidades que se vayan presentando en cuanto a las conexiones futuras que se puedan presentar en los establecimientos de salud dado que es bastante adaptable para la migración y/o mejora del hardware. Teniendo en cuenta que a cuantas más conexiones mayor consumo de recursos tendrá el servidor.

VI. RECOMENDACIONES

Es recomendable las capacitaciones continuas respecto a uso de las TIC a los usuarios de los establecimientos de salud, dado que en la presente investigación se pudo constatar de desconocimiento y resistencia a cambios tecnológicos, esto influye en el uso no adecuado de las soluciones o implementaciones tecnológicas que se brinden en los centros de salud.

Es recomendable que los usuarios finales tengan el compromiso de usar adecuadamente esta solución tecnológica, la cual les ayudara y facilitara el trabajo diario que estos realizan debido a los múltiples beneficios de los sistemas y seguridad que estos podrán tener en los equipos de cómputo y en la red local.

El impacto con esta solución tecnológica ha sido bueno por los comentarios positivos que tuvimos en las visitas y toma de encuestas de la presente solución

VII. REFERENCIAS

Bermúdez, KG y Bailón, ER. (2018). Análisis en seguridad informática y seguridad de la información basado en la NORMA ISO/IEC 27001 - Sistemas de gestión de seguridad de la información dirigido a una empresa de servicios financieros. [Tesis de maestría, Universidad Politécnica Salesiana Sede Guayaquil] <https://dspace.ups.edu.ec/bitstream/123456789/10372/1/UPS-GT001514.pdf>

González, A. (2014). Redes Privadas Virtuales. Universidad Técnica Federico Santa María.
[http://profesores.elo.utfsm.cl/~agv/elo322/1s14/projects/reports/G20/Redes%20Privadas%20Virtuales%20\(VPN\).pdf](http://profesores.elo.utfsm.cl/~agv/elo322/1s14/projects/reports/G20/Redes%20Privadas%20Virtuales%20(VPN).pdf)

Alegsa, L. (2015). Definición de Red de Computadoras. Obtenido de http://www.alegsa.com.ar/Dic/red_de_computadoras.php

- Amendolia, D., & Cendagorta, J. (2004). Políticas de seguridad informáticas. Argentina: Seguridad informática. Obtenido de http://www.criptored.upm.es/guiateoria/gt_m148q.htm
- Bernal, O., & Forero, J. (2011). Sistemas de información en el sector salud en Colombia. Bogotá: Universidad de Los Andes. Obtenido de <http://www.scielo.org.co/pdf/rgps/v10n21/v10n21a06.pdf>
- Castro, D., & Rojas, Á. (2013). Riesgos, amenazas y vulnerabilidades de los sistemas de información geográfica. Bogotá: Universidad Católica de Colombia. Obtenido de <https://repository.ucatolica.edu.co/bitstream/10983/1305/1/RIESGOS%20AMENAZAS%20Y%20VULNERABILIDADES%20DE%20LOS%20SISTEMAS%20DE%20INFORMACION%20GEOGRAFICA%20GPS.pdf>
- Chicaiza, D. (2014). Estudio de las tecnologías de seguridad perimetral informáticas y propuesta de un plan de implementación para la agencia nacional de tránsito. Quito: Pontificia Universidad Católica de Ecuador. Obtenido de <http://repositorio.puce.edu.ec/bitstream/handle/22000/7896/9.56.000616.pdf?sequence=4&isAllowed=y>
- Cordova, N. (2003). Plan de seguridad informática para una entidad financiera. Lima: UNMSM. Obtenido de http://sisbib.unmsm.edu.pe/bibvirtualdata/Tesis/Basic/Cordova_RN/T_completo.pdf
- Da Silva, R., & Silva, J. (2016). Efecto de la implementación del sistema PfSense en la seguridad perimetral lógica en los servicios de la red troncal de la Universidad Nacional de la Amazonía Peruana - Iquitos 2016. Iquitos: Universidad de la Amazonía Peruana. Obtenido de <http://repositorio.ups.edu.pe/bitstream/handle/UPS/10/Tesis%20Jhony%20Rene.pdf?sequence=3&isAllowed=y>
- Díaz, C. M. (2013). http://oa.upm.es/22228/1/PFC_CARLOS_MANUEL_FABUEL_DIAZ.pdf. Obtenido de

http://oa.upm.es/22228/1/PFC_CARLOS_MANUEL_FABUEL_DIAZ.pdf:
http://oa.upm.es/22228/1/PFC_CARLOS_MANUEL_FABUEL_DIAZ.pdf

Free Software, F. (2019). ¿Qué es el software libre? USA: GNU. Obtenido de <https://www.gnu.org/philosophy/free-sw.es.html>

Gestion de redes telemáticas (2016) DigitalBooks. Recuperado de: <http://reader.digitalbooks.pro/content/preview/books/37922/book/OEBPS/Text/chapter1.html>

Goujon, A. (10 de 09 de 2012). Obtenido de <https://www.welivesecurity.com/la-es/2012/09/10/vpn-funcionamiento-privacidad-informacion/>

Guerra, E. (4 de Julio de 2012). Un servidor de seguridad perimetral. Obtenido de <http://sisena-evidenciasi.blogspot.com/2012/07/un-servidor-de-seguridad-perimetral.html>

Hernández, J., & Florez, J. (junio de 2011). Universidad de Rioja. Obtenido de <https://dialnet.unirioja.es/descarga/articulo/4166933.pdf>

INCIBE. (2017). Ransomware: una guía de aproximación para el empresario. Obtenido de https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ransomware_metad.pdf

ISO 27000, P. (2005). ¿Qué es una SGSI? Obtenido de <http://www.iso27000.es/sgsi.html>

Jiménez, J. (2013). NAT y PAT. Obtenido de <https://es.scribd.com/document/170204481/DEBER-5-NAT-Y-PAT>

Lobos, L. (03 de 2012). loslobosdel2012.blogspot.com. Obtenido de [loslobosdel2012.blogspot.com](http://loslobosdel2012.blogspot.com/2012/03/redes-troncales.html):
<http://loslobosdel2012.blogspot.com/2012/03/redes-troncales.html>

López, H (2005). Diseño de una zona Wi-Fi como herramienta de apoyo al modelo educativo de la Universidad Autónoma Indígena de México. Ra Ximhai, 1(2), [fecha de Consulta 19 de noviembre de 2019]. ISSN: 1665-0441. Disponible en: <https://www.redalyc.org/articulo.oa?id=461/46110209>

- Más Adelante. (s.f.). ¿Qué significa HTTP? Obtenido de <https://www.masadelante.com/faqs/que-significa-http>
- Microsoft. (29 de agosto de 2006). Supervisión de la seguridad y detección de ataques. Obtenido de <https://docs.microsoft.com/es-es/security-updates/security/supervisindelaseguridadydeteccindeataques>
- Noboa, J. V. (2017). Diseño e implementación de seguridad perimetral para la infraestructura de la inmobiliaria Fasko S.A.
- OMS. (1999). El establecimiento de sistemas de información en servicios de atención de salud. Guía para el análisis de requisitos, especificación de las aplicaciones y adquisición. Washington D.C: PAHO. Obtenido de <https://apps.who.int/medicinedocs/documents/s16596s/s16596s.pdf>
- Perozo, B. (2003). Factores de riesgo que influyen en la inoperatividad de las redes privadas virtuales con tecnologías Frame Relay y X.25. *Télématique*, 2(2). [fecha de Consulta 19 de noviembre de 2019]. ISSN: 1856-4194. Disponible en: <https://www.redalyc.org/articulo.oa?id=784/78420204>
- Redes, E. b. (s.f.). Qué es una red (computadores). Obtenido de <http://elblogdelasredes.blogspot.com/p/video-sobre-que-son-redes-y-tipos.html>
- Restrepo, L., & López, M. (2015). Sistema de información para la calidad en salud: una realidad por explorar, para conocer y decidir responsablemente. Medellín: Revista CES Salud Pública Volumen 6 No.1 enero - Junio / 2015. Obtenido de http://revistas.ces.edu.co/index.php/ces_salud_publica/article/view/2979
- Rick, J. A. (2008). Router, Enrutador o Encaminador. Obtenido de <https://github.com/tectijuana/redes7a-Archived/wiki/Router,-Enrutador-o-Encaminador>
- Sahuquillo, M. R. (27 de 06 de 2017). <https://elpais.com>. Obtenido de https://elpais.com/internacional/2017/06/27/actualidad/1498568187_011218.html

- Santillán, J. (2010). Firewalls, controlando el acceso a la red. México: Revista Seguridad. Obtenido de <https://revista.seguridad.unam.mx/print/2105>
- Srivedi S. & Manjaiah D. (2012) Technical Overview of Virtual Private Networks(VPNs). Research Paper vol 2 (7). Recuperado de: https://www.researchgate.net/publication/274929918_Technical_Overview_of_Virtual_Private_NetworksVPNs
- Torres, R. (2015). Redes de comunicación, seguridad perimetral. Ibarra Ecuador: Universidad Técnica del Norte. Obtenido de <http://repositorio.utn.edu.ec/bitstream/123456789/3768/3/04%20RED%20041%20Informe%20T%C3%A9cnico-%20Espa%C3%B1ol.pdf>
- Vemuri, L. R. (10 de abril de 2006). ISO 2700.es. Obtenido de http://www.iso27000.es/download/Preparing_for_the_Security_Audit.pdf

Anexo 1. Matriz de consistencia

Diseño de una red privada virtual (VPN) basada en software libre para la mejora de la seguridad de la información de la jurisdicción de la dirección de redes integradas de salud Lima Centro					
PROBLEMAS	OBJETIVOS	HIPÓTESIS	VARIABLES Y DIMENSIONES	METODOLOGÍA	PROCESAMIENTO DE LA INFORMACIÓN
<p>Problema General: ¿En qué medida el diseño de una Red Privada Virtual basado en software libre influye en la optimización de la seguridad de información de la jurisdicción de la Dirección de Redes Integradas de Salud Lima Centro?</p> <p>Problema Específicos: a) ¿En qué medida el nivel de seguridad del Diseño de una Red Privada Virtual (VPN) basado en software libre influye en la optimización de la seguridad de información de la jurisdicción de la Dirección de Redes Integradas de Salud Lima Centro? b) ¿En qué medida el nivel de confiabilidad del Diseño de una Red Privada Virtual (VPN) basado en software libre influye en la optimización de la seguridad de información de la jurisdicción de la Dirección de Redes Integradas de Salud Lima Centro?</p>	<p>Objetivo General: Determinar la influencia del Diseño de una Red Privada Virtual (VPN) Bajo Software Libre Para Optimizar la seguridad de la Información entre los Locales de la Dirección de Redes Integradas de Salud Lima Centro</p> <p>Objetivos Específicos: a) Determinar la influencia del nivel de seguridad del Diseño de una Red Privada Virtual (VPN) basado en Software Libre para optimizar la seguridad de Información entre los Locales de la Dirección de Redes Integradas de Salud Lima Centro b) Determinar la influencia del nivel de confiabilidad del Diseño de una Red Privada Virtual (VPN) basado en Software Libre Para Optimizar la seguridad de la Información entre los Locales de la Dirección de Redes Integradas de Salud Lima Centro</p>	<p>Hipótesis General: El diseño de una Red Privada Virtual (VPN) Bajo Software Libre influye significativamente en la optimización de la seguridad de la información en la jurisdicción de la Dirección de Redes Integradas de Salud Lima Centro</p> <p>Hipótesis General: a) El nivel de seguridad del Diseño de una Red Privada Virtual (VPN) basado en Software Libre para optimizar influye significativamente en la optimización de la seguridad de la información de la jurisdicción de la Dirección de Redes Integradas de Salud Lima Centro b) El nivel de confiabilidad del Diseño de una Red Privada Virtual (VPN) basado en Software Libre para optimizar influye significativamente en la optimización de la seguridad de información de la jurisdicción de la Dirección de Redes Integradas de Salud Lima Centro</p>	<p><i>Variable independiente</i> Red Privada Virtual (VPN) Bajo Software Libre</p> <p><i>Variable dependiente</i> Seguridad de información</p>	<p>Tipo: Cuantitativo - Descriptivo</p> <p>Diseño: El diseño será preexperimental (piloto)</p> <p>Población: 74 establecimientos de salud Lima Centro</p> <p>Muestra: Dirección de Salud Lima Centro</p> <p>Muestreo: Se utilizará el muestreo no probabilístico</p> <p>Procedimientos: Se utilizará el sistema SPSS v.23 se logrará la representación escrita, tabular y gráfica mediante el uso correcto del programa Excel</p>	<p>El procesamiento de la información seguirá los requerimientos del análisis de los datos cuantitativos. En primera instancia realizar las encuestas y guías de observación.</p> <p>a. Seleccionar el programa estadístico b. Ejecutar el programa SPSS v.23 c. Analizar y visualizarlos datos por variable d. Realizar análisis adicionales e. Analizar hipótesis f. Evaluar confiabilidad</p>

<p>c) ¿En qué medida el nivel de escalabilidad en el Diseño de una Red Privada Virtual (VPN) basado en software libre influye en la optimización de la seguridad de la información de la jurisdicción de la Dirección de Redes Integradas de Salud Lima Centro?</p>	<p>c) Determinar la influencia del nivel de escalabilidad en el Diseño de una Red Privada Virtual (VPN) basado en Software Libre Para Optimizar influye en la seguridad de la Información entre los Locales de la Dirección de Redes Integradas de Salud Lima Centro</p>	<p>c) El nivel de escalabilidad del Diseño de una Red Privada Virtual (VPN) basado en Software Libre para optimizar influye significativamente en la optimización de la seguridad de la información de la jurisdicción de la Dirección de Redes Integradas de Salud Lima Centro</p>			
---	--	---	--	--	--

Anexo 2. Cuadro de operacionalización de variables

Variable Dependiente: Seguridad de la Información

Definición Conceptual	Definición Operacional	Dimensión	Indicador	Nivel de Medición
Según ADEA es una es las soluciones para evaluar todo tipo de riesgos desde la ISO 27001 según Baldecchi es un SGSI 10, la seguridad de la información queda definida por tres atributos (Figueroa, celiz; 2018; p11)	La variable relacionada a una característica de la información que se transmite a través de las computadoras de una red y sus dimensiones son extensión de conectividad, mejoras en la seguridad, topología de red e infraestructura y medios de uso	Confidencialidad: es la propiedad de prevenir que se divulgue la información a personas o sistemas no autorizados. (Figueroa,celiz; 2018; p11)	confidencialidad de la información	Ordinal
		Integridad: es la propiedad que busca proteger que se modifiquen los datos libres de forma no autorizada. (Figueroa,celiz; 2018; p11)	Integridad de la información	
		Disponibilidad: es una característica, cualidad o condición de la información que se encuentra a disposición de quien tiene que acceder a esta, bien sean personas, procesos o aplicaciones. (Figueroa, celiz; 2018; p11)	Disponibilidad de la información	

Anexo 3. Diagnóstico estado actual de equipos de cómputo

DIAGNÓSTICO ESTADO ACTUAL DE EQUIPOS DE COMPUTO DE LA DIRECCIÓN DE REDES INTEGRADAS DE SALUD LIMA CENTRO

Durante el diagnóstico del estado actual de los equipos de cómputo de la Dirección de Redes de Salud Lima Centro, se han ido adquiriendo equipos para ir solucionando los problemas que actualmente se cuentan, para solucionar las deficiencias se han ido programando adquisiciones semestrales.

En los primeros años de creación (02 de junio 2017) de la Diris Lima Centro se ha ido mejorando paulatinamente la renovación de equipos los cuales, a nivel de la sede administrativa y establecimientos de salud, en algunos casos obsoletas debido a su antigüedad de estas algunas oficinas y/o servicios se han quedado sin equipos debido a estos problemas mencionados. Actualmente se está dotando de equipamiento nuevo para evitar que sucedan estos inconvenientes en el futuro.

1. Tenemos un total 1767 computadoras distribuidas de la siguiente forma, 100 computadoras operativas al servicio de la sede administrativa, 1667 computadoras en los establecimientos de salud, 40 computadora malograda por placa, fuente de poder, microprocesador, 10 computadoras están de relevó por si algunas se malogran.

INVENTARIO DE LA SEDE ADMINISTRATIVA 2022

LUGAR	PROCESADOR	CANTIDADES	DIAGNOSTICO
SEDE ADMINISTRATIVA	CORE 2 DUO	6	EQUIPOS PRESENTAN PROBLEMAS ALEATORIOS DEBIDO A SU ANTIGUEDAD COMO SON EL CASO LOS EQUIPOS CORE 2 DUO, CORE 13, CORE5, CORE 17 DE PRIMERA, TERCERA, CUARTA GENERACION.
SEDE ADMINISTRATIVA	CORE 13 - CUARTA GENERACION	8	
SEDE ADMINISTRATIVA	CORE 15 - CUARTA GENERACION	5	
SEDE ADMINISTRATIVA	CORE 17 NOVENA GENERACION	5	
SEDE ADMINISTRATIVA	CORE 13 OCTAVA GENERACION	1	
SEDE ADMINISTRATIVA	CORE 15 DECIMA GENERACION	2	
SEDE ADMINISTRATIVA	CORE 15 OCTAVA GENERACION	10	
SEDE ADMINITRATIVA	CORE 15 PRIMERA GENERACION	6	
SEDE ADMINISTRATIVA	CORE 15 TERCERA GENERACION	13	
SEDE ADMINISTRATIVA	CORE 17 CUARTA GENERACION	16	
SEDE ADMINISTRATIVA	CORE 17 OCTAVA GENERACION	6	
SEDE ADMINISTRATIVA	CORE 17 SEPTIMA GENERACION	13	
SEDE ADMINISTRATIVA	CORE 17DECIMA GENERACION	9	
TOTAL		100	

C.S. Breña	CORE 15- CUARTA GENERACION	1
C.S. Chacra Colorada	CORE 2 DUO	5
C.S. Chacra Colorada	CORE 13- TERCERA GENERACION	3
C.S. Chacra Colorada	CORE 15- TERCERA GENERACION	2
C.S. Chacra Colorada	CORE 17- SEGUNDA GENERACION	1
C.S. Chacra Colorada	CORE 17-CUARTA GENERACION	3
C.S. Chacra Colorada	CORE 17-SEPTIMA GENERACION	
C.S. Chacra Colorada	CORE 15- SEGUNDA GENERACION	1
C.S. Chacra Colorada	CORE 17- NOVENA GENERACION	9
C.S. Chacra Colorada	CORE 15- CUARTA GENERACION	2
C.S. Chacra Colorada	CORE 13-SEGUNDA GENERACION	1
C.S. Conde de la Vega	CORE 2 DUO	7
C.S. Conde de la Vega	CORE 2 DUO	
C.S. Conde de la Vega	CORE 15- SEGUNDA GENERACION	2
C.S. Conde de la Vega	DUAL CORE	2
C.S. Conde de la Vega	CORE 13-SEGUNDA GENERACION	2
C.S. Conde de la Vega	CORE 17- SEGUNDA GENERACION	1
C.S. Conde de la Vega	CORE 15- TERCERA GENERACION	1
C.S. Conde de la Vega	CORE 17- NOVENA GENERACION	9
C.S. Conde de la Vega	CORE 15- CUARTA GENERACION	1
C.S. Conde de la Vega	CORE 13- TERCERA GENERACION	2
C.S. V.M.P. Socorro	CORE 13- TERCERA GENERACION	3
C.S. V.M.P. Socorro	CORE 2 DUO	6
C.S. V.M.P. Socorro	CORE 15- TERCERA GENERACION	2
C.S. V.M.P. Socorro	DUAL CORE	1
C.S. V.M.P. Socorro	CORE 15- CUARTA GENERACION	1
C.S. V.M.P. Socorro	CORE 13-SEGUNDA GENERACION	2
C.S. V.M.P. Socorro	CORE 15- SEGUNDA GENERACION	1
C.S. V.M.P. Socorro	CORE 17-CUARTA GENERACION	1
C.S. Mirones Bajo	CORE 2 DUO	4
C.S. Mirones Bajo	CORE 13-SEGUNDA GENERACION	4
C.S. Mirones Bajo	CORE 15- CUARTA GENERACION	2
C.S. Mirones Bajo	CORE 15- SEGUNDA GENERACION	1
C.S. Mirones Bajo	CORE 13- TERCERA GENERACION	1
C.S. Mirones Bajo	CORE 15- TERCERA GENERACION	2
C.S. Mirones Bajo	PENTIUM D	2
C.S. Mirones Bajo	CORE 15- SEGUNDA GENERACION	
C.S. Mirones Bajo	CORE 17-SEPTIMA GENERACION	1
P.S. Santa Rosa	CORE 2 DUO	3
P.S. Santa Rosa	CORE 13- TERCERA GENERACION	4
P.S. Santa Rosa	CORE 15- TERCERA GENERACION	3
P.S. Rescate	DUAL CORE	2
P.S. Rescate	CORE 13-SEGUNDA GENERACION	2
P.S. Rescate	CORE 13- TERCERA GENERACION	3
P.S. Rescate	CORE 2 DUO	3
P.S. Rescate	CORE 17- NOVENA GENERACION	7

P.S. Rescate	CORE I5- SEGUNDA GENERACION	1
P.S. Palermo	DUAL CORE	
P.S. Palermo	CORE I3- TECERA GENERACION	5
P.S. Palermo	CORE I7- SEGUNDA GENERACION	1
P.S. Palermo	CORE 2 DUO	3
P.S. Palermo	CORE I7- NOVENA GENERACION	7
P.S. Palermo	CORE I5- TERCERA GENERACION	2
C.S. San Sebastián	CORE I3- TECERA GENERACION	3
C.S. San Sebastián	DUAL CORE	2
C.S. San Sebastián	CORE I3-SEGUNDA GENERACION	4
C.S. San Sebastián	CORE I5- CUARTA GENERACION	2
C.S. San Sebastián	CORE 2 DUO	2
C.S. San Sebastián	CORE I7-CUARTA GENERACION	1
C.S. San Sebastián	CORE I5- SEGUNDA GENERACION	1
C.S. San Sebastián	CORE I5- TERCERA GENERACION	1
C.S. Unidad Vecinal Nro 3	CORE I3- TECERA GENERACION	3
C.S. Unidad Vecinal Nro 3	CORE 2 DUO	5
C.S. Unidad Vecinal Nro 3	CORE I5- SEGUNDA GENERACION	2
C.S. Unidad Vecinal Nro 3	DUAL CORE	1
C.S. Unidad Vecinal Nro 3	AMD SEMPRON	1
C.S. Unidad Vecinal Nro 3	CORE I5- TERCERA GENERACION	1
C.S. Unidad Vecinal Nro 3	CORE I5- CUARTA GENERACION	1
C.S. Unidad Vecinal Nro 3	CORE I3-SEGUNDA GENERACION	2
C.S. Unidad Vecinal Nro 3	CORE I7-SEPTIMA GENERACION	1
C.S. Magdalena	DUAL CORE	2
C.S. Magdalena	CORE I5- SEGUNDA GENERACION	2
C.S. Magdalena	CORE I3- TECERA GENERACION	4
C.S. Magdalena	CORE 2 DUO	8
C.S. Magdalena	CORE I5- TERCERA GENERACION	2
C.S. Magdalena	CORE I7- SEGUNDA GENERACION	1
C.S. Magdalena	CORE I7-CUARTA GENERACION	1
C.S. Magdalena	CORE I5- CUARTA GENERACION	2
C.S. Magdalena	CORE I3-SEGUNDA GENERACION	2
C.S. Jesús María	CORE I3-SEGUNDA GENERACION	3
C.S. Jesús María	CORE I5- SEGUNDA GENERACION	2
C.S. Jesús María	CORE 2 DUO	5
C.S. Jesús María	CORE I7-SEPTIMA GENERACION	1
C.S. Jesús María	DUAL CORE	2
C.S. Jesús María	PENTIUM D	1
C.S. Jesús María	CORE I5- TERCERA GENERACION	1
C.S. Jesús María	CORE I5- CUARTA GENERACION	1
C.S. Jesús María	CORE I7- NOVENA GENERACION	9
C.S. San Miguel	CORE I3- TECERA GENERACION	3
C.S. San Miguel	CORE 2 DUO	5
C.S. San Miguel	DUAL CORE	4
C.S. San Miguel	CORE I5- TERCERA GENERACION	5

C.S. San Miguel	CORE I3-SEGUNDA GENERACION	3
C.S. San Miguel	CORE I7- SEGUNDA GENERACION	1
C.S. San Miguel	CORE I5- CUARTA GENERACION	2
C.S. San Miguel	CORE I5- SEGUNDA GENERACION	2
C.S. San Miguel	CORE I7-CUARTA GENERACION	1
P.S. Huaca Pando	CORE 2 DUO	2
P.S. Huaca Pando	CORE I3- TERCERA GENERACION	4
P.S. Huaca Pando	CORE I7-SEPTIMA GENERACION	1
P.S. Huaca Pando	DUAL CORE	1
P.S. Huaca Pando	CORE I5- TERCERA GENERACION	1
C.S. El Porvenir	CORE I5- CUARTA GENERACION	2
C.S. El Porvenir	CORE 2 DUO	7
C.S. El Porvenir	DUAL CORE	2
C.S. El Porvenir	CORE I5- SEGUNDA GENERACION	2
C.S. El Porvenir	CORE I7- NOVENA GENERACION	12
C.S. El Porvenir	CORE I3-SEGUNDA GENERACION	4
C.S. El Porvenir	CORE I7- SEGUNDA GENERACION	1
C.S. El Porvenir	CORE I5- TERCERA GENERACION	2
C.S. El Porvenir	CORE I3- TERCERA GENERACION	5
C.S. Max Arias Schreiber	CORE 2 DUO	4
C.S. Max Arias Schreiber	CORE I3-SEGUNDA GENERACION	4
C.S. Max Arias Schreiber	CORE I7-CUARTA GENERACION	2
C.S. Max Arias Schreiber	CORE I5- CUARTA GENERACION	2
C.S. Max Arias Schreiber	DUAL CORE	1
C.S. Max Arias Schreiber	CORE I7- NOVENA GENERACION	2
C.S. Max Arias Schreiber	CORE I3- TERCERA GENERACION	3
C.S. Max Arias Schreiber	CORE I5- SEGUNDA GENERACION	2
C.S. Max Arias Schreiber	CORE I5- TERCERA GENERACION	1
C.S. Max Arias Schreiber	CORE I7- SEGUNDA GENERACION	2
C.S. Max Arias Schreiber	CORE I7-SEPTIMA GENERACION	2
C.S. Lince	CORE I5- CUARTA GENERACION	2
C.S. Lince	CORE I5- SEGUNDA GENERACION	2
C.S. Lince	CORE 2 DUO	5
C.S. Lince	CORE I3-SEGUNDA GENERACION	3
C.S. Lince	CORE I7-CUARTA GENERACION	1
C.S. Lince	CORE I5- TERCERA GENERACION	1
C.S. Lince	CORE I7-SEPTIMA GENERACION	1
C.S. Lince	DUAL CORE	1
C.S. San Luis	CORE I3-SEGUNDA GENERACION	3
C.S. San Luis	CORE 2 DUO	5
C.S. San Luis	CORE I5- TERCERA GENERACION	2
C.S. San Luis	CORE I5- CUARTA GENERACION	2
C.S. San Luis	CORE I7- NOVENA GENERACION	9
C.S. San Luis	DUAL CORE	3
C.S. San Luis	CORE I5- SEGUNDA GENERACION	2
C.S. San Luis	CORE I3- TERCERA GENERACION	2

C.S. San Luis	CORE 17- SEGUNDA GENERACION	1
C.S. El Pino	CORE 2 DUO	2
C.S. El Pino	CORE 13- TERCERA GENERACION	3
C.S. El Pino	DUAL CORE	5
C.S. El Pino	CORE 17-CUARTA GENERACION	9
C.S. El Pino	CORE 13-SEGUNDA GENERACION	3
C.S. El Pino	CORE 15- TERCERA GENERACION	2
C.S. El Pino	CORE 15- CUARTA GENERACION	2
C.S. El Pino	CORE 15- SEGUNDA GENERACION	1
P.S. Clas El Pino	CORE 13-SEGUNDA GENERACION	4
P.S. Clas El Pino	CORE 17-SEPTIMA GENERACION	1
P.S. Clas El Pino	CORE 13- TERCERA GENERACION	3
P.S. Clas El Pino	CORE 17- NOVENA GENERACION	7
P.S. Clas El Pino	CORE 2 DUO	2
P.S. Clas El Pino	CORE 15- SEGUNDA GENERACION	1
C.S. San Cosme	DUAL CORE	2
C.S. San Cosme	CORE 15- TERCERA GENERACION	2
C.S. San Cosme	CORE 2 DUO	4
C.S. San Cosme	CORE 17- SEGUNDA GENERACION	1
C.S. San Cosme	PENTIUM CELERON	
C.S. San Cosme	CORE 17-CUARTA GENERACION	1
C.S. San Cosme	CORE 13- TERCERA GENERACION	3
C.S. San Cosme	CORE 15- CUARTA GENERACION	2
C.S. San Cosme	CORE 15- SEGUNDA GENERACION	2
C.S. San Cosme	CORE 13-SEGUNDA GENERACION	1
C.S. Surquillo	DUAL CORE	5
C.S. Surquillo	CORE 2 DUO	6
C.S. Surquillo	CORE 13-SEGUNDA GENERACION	3
C.S. Surquillo	CORE 15- TERCERA GENERACION	2
C.S. Surquillo	CORE 17-SEPTIMA GENERACION	1
C.S. Surquillo	AMD SEMPRON	1
C.S. Surquillo	CORE 17- NOVENA GENERACION	9
C.S. Surquillo	CORE 13- TERCERA GENERACION	6
C.S. Surquillo	CORE 15- CUARTA GENERACION	2
C.S. Surquillo	AMD ATHLON II	1
C.S. Surquillo	CORE 15- SEGUNDA GENERACION	1
C.S. V. Victoria Porvenir	CORE 2 DUO	3
C.S. V. Victoria Porvenir	CORE 13- TERCERA GENERACION	3
C.S. V. Victoria Porvenir	CORE 15- SEGUNDA GENERACION	2
C.S. V. Victoria Porvenir	CORE 17- SEGUNDA GENERACION	1
C.S. V. Victoria Porvenir	DUAL CORE	2
C.S. V. Victoria Porvenir	CORE 17-CUARTA GENERACION	1
C.S. V. Victoria Porvenir	CORE 15- TERCERA GENERACION	1
C.S. V. Victoria Porvenir	AMD SEMPRON	1
C.S. V. Victoria Porvenir	CORE 15- CUARTA GENERACION	1
P.S. Pedregal	CORE 13-SEGUNDA GENERACION	3

P.S. Pedregal	DUAL CORE	4
P.S. Pedregal	CORE 2 DUO	2
P.S. Pedregal	CORE I7- NOVENA GENERACION	7
P.S. Pedregal	CORE I5- TERCERA GENERACION	1
P.S. Pedregal	CORE I7- SEGUNDA GENERACION	1
C.S. San Borja	CORE I3-SEGUNDA GENERACION	3
C.S. San Borja	CORE 2 DUO	2
C.S. San Borja	CORE I7-CUARTA GENERACION	1
C.S. San Borja	PENTIUM D	2
C.S. San Borja	CORE I3- TERCERA GENERACION	3
C.S. San Borja	CORE I5- CUARTA GENERACION	1
C.S. San Borja	CORE I5- SEGUNDA GENERACION	1
C.S. San Borja	CORE I5- TERCERA GENERACION	1
C.S. San Borja	CORE I7-SEPTIMA GENERACION	1
P.S. San Juan Masías	CORE I3- TERCERA GENERACION	4
P.S. San Juan Masías	CORE 2 DUO	2
P.S. San Juan Masías	CORE I7- NOVENA GENERACION	7
P.S. San Juan Masías	CORE I5- CUARTA GENERACION	1
P.S. San Juan Masías	CORE I7- SEGUNDA GENERACION	1
C.S. Miraflores	CORE 2 DUO	3
C.S. Miraflores	CORE I3-SEGUNDA GENERACION	3
C.S. Miraflores	DUAL CORE	6
C.S. Miraflores	CORE I7-CUARTA GENERACION	1
C.S. Miraflores	CORE I7-SEPTIMA GENERACION	1
C.S. Miraflores	CORE I5- SEGUNDA GENERACION	1
C.S. Miraflores	PENTIUM D	2
C.S. Miraflores	CORE I5- TERCERA GENERACION	1
C.S. Miraflores	CORE I5- CUARTA GENERACION	1
C.S. San Isidro	CORE I3-SEGUNDA GENERACION	3
C.S. San Isidro	CORE I5- SEGUNDA GENERACION	2
C.S. San Isidro	CORE 2 DUO	5
C.S. San Isidro	CORE I7- NOVENA GENERACION	9
C.S. San Isidro	CORE I5- TERCERA GENERACION	1
C.S. San Isidro	CORE I7- SEGUNDA GENERACION	1
C.S. San Isidro	DUAL CORE	1
C.S. San Isidro	CORE I5- CUARTA GENERACION	1
C.S. San Isidro	AMD SEMPRON	1
C.S. ZARATE	AMD ATHLON II	2
C.S. ZARATE	CORE 2 DUO	2
C.S. ZARATE	CORE I5- TERCERA GENERACION	1
C.S. ZARATE	CORE I5- CUARTA GENERACION	1
C.S. ZARATE	CORE I5- SEGUNDA GENERACION	1
C.S. ZARATE	Pentium D	2
C.S. MANGOMARCA	CORE I5- TERCERA GENERACION	1
C.S. MANGOMARCA	CORE I5- CUARTA GENERACION	1
C.S. MANGOMARCA	AMD ATHLON II	1

C.S. MANGOMARCA	CORE 2 DUO	2
C.S. MANGOMARCA	CORE 17-CUARTA GENERACION	3
C.S. MANGOMARCA	CORE 13- TERCERA GENERACION	1
C.S. MANGOMARCA	CORE 15- SEGUNDA GENERACION	1
C.S. CHACARILLA DE OTERO	CORE 15- TERCERA GENERACION	4
C.S. CHACARILLA DE OTERO	CORE 2 DUO	5
C.S. CHACARILLA DE OTERO	CORE 15- CUARTA GENERACION	2
C.S. CHACARILLA DE OTERO	CORE 17- CUARTA GENERACION	18
C.S. CHACARILLA DE OTERO	CORE 15- SEGUNDA GENERACION	1
C.S. CHACARILLA DE OTERO	CORE 17-SEPTIMA GENERACION	3
C.S. CAMPOY	AMD ATHLON II	2
C.S. CAMPOY	CORE 15- TERCERA GENERACION	4
C.S. CAMPOY	CORE 15- CUARTA GENERACION	4
C.S. CAMPOY	CORE 2 DUO	3
P.S. AZCARRUNZ ALTO	AMD ATHLON II	1
P.S. AZCARRUNZ ALTO	CORE 15- CUARTA GENERACION	1
C.S. CAJA DE AGUA	CORE 15- TERCERA GENERACION	1
C.S. CAJA DE AGUA	CORE 2 DUO	5
C.S. CAJA DE AGUA	CORE 15- CUARTA GENERACION	1
C.S. CAJA DE AGUA	CORE 13-SEGUNDA GENERACION	1
C.S. CAJA DE AGUA	CORE 17-CUARTA GENERACION	3
C.S. CAJA DE AGUA	CORE 15- SEGUNDA GENERACION	1
P.S. DANIEL ALCIDES CARRION	CORE 15- TERCERA GENERACION	1
P.S. DANIEL ALCIDES CARRION	CORE 13-SEGUNDA GENERACION	1
P.S. DANIEL ALCIDES CARRION	CORE 15- CUARTA GENERACION	1
P.S. DANIEL ALCIDES CARRION	CORE 15- SEGUNDA GENERACION	1
P.S. DANIEL ALCIDES CARRION	AMD ATHLON II	1
P.S. DANIEL ALCIDES CARRION	CORE 2 DUO	1
P.S. AYACUCHO	AMD ATHLON II	1
P.S. AYACUCHO	CORE 15- TERCERA GENERACION	1
P.S. AYACUCHO	CORE 15- CUARTA GENERACION	1
P.S. AYACUCHO	CORE 17-SEPTIMA GENERACION	1
P.S. AYACUCHO	Pentium D	1
C.S. SAN HILARION	Pentium D	2
C.S. SAN HILARION	CORE 2 DUO	4
C.S. SAN HILARION	CORE 17- NOVENA GENERACION	9
C.S. SAN HILARION	CORE 15- SEGUNDA GENERACION	2
C.S. SAN HILARION	CORE 15- TERCERA GENERACION	1
C.S. SAN HILARION	CORE 15- CUARTA GENERACION	1
C.S. SAN HILARION	CORE 13-SEGUNDA GENERACION	1
C.S. JAIME ZUBIETA	CORE 15- TERCERA GENERACION	3
C.S. JAIME ZUBIETA	CORE 15- CUARTA GENERACION	3
C.S. JAIME ZUBIETA	CORE 2 DUO	6
C.S. JAIME ZUBIETA	CORE 17- SEGUNDA GENERACION	3
C.S. JAIME ZUBIETA	CORE 15- SEGUNDA GENERACION	3
C.S. JAIME ZUBIETA	Pentium D	2

C.S. JAIME ZUBIETA	AMD ATHLON II	1
C.S. JAIME ZUBIETA	CORE I3-SEGUNDA GENERACION	1
P.S. TUPAC AMARU II	CORE I5- TERCERA GENERACION	2
P.S. TUPAC AMARU II	CORE I7-CUARTA GENERACION	2
P.S. TUPAC AMARU II	CORE I5- CUARTA GENERACION	1
P.S. TUPAC AMARU II	CORE I5- SEGUNDA GENERACION	1
C.S. LA LIBERTAD	CORE I5- CUARTA GENERACION	2
C.S. LA LIBERTAD	CORE I5- SEGUNDA GENERACION	2
C.S. LA LIBERTAD	CORE 2 DUO	6
C.S. LA LIBERTAD	CORE I3-SEGUNDA GENERACION	3
C.S. LA LIBERTAD	CORE I5- TERCERA GENERACION	1
C.S. LA LIBERTAD	Pentium D	2
C.S. CRUZ DE MOTUPE	CORE I5- TERCERA GENERACION	2
C.S. CRUZ DE MOTUPE	CORE I5- CUARTA GENERACION	2
C.S. CRUZ DE MOTUPE	CORE 2 DUO	3
C.S. CRUZ DE MOTUPE	DUAL CORE	1
C.S. CRUZ DE MOTUPE	CORE I5- SEGUNDA GENERACION	1
C.S. CRUZ DE MOTUPE	CORE I7-SEPTIMA GENERACION	1
C.S. CRUZ DE MOTUPE	CORE I3- TERCERA GENERACION	1
C.S. GANIMEDES	CORE 2 DUO	7
C.S. GANIMEDES	Pentium D	2
C.S. GANIMEDES	CORE I5- SEGUNDA GENERACION	4
C.S. GANIMEDES	AMD ATHLON II	4
C.S. GANIMEDES	CORE I5- TERCERA GENERACION	3
C.S. GANIMEDES	CORE I5- CUARTA GENERACION	3
C.S. MEDALLA MILAGROSA	DUAL CORE	1
C.S. MEDALLA MILAGROSA	CORE I5- TERCERA GENERACION	2
C.S. MEDALLA MILAGROSA	AMD ATHLON II	2
C.S. MEDALLA MILAGROSA	CORE I5- CUARTA GENERACION	1
C.S. MEDALLA MILAGROSA	CORE I5- SEGUNDA GENERACION	1
C.S. MEDALLA MILAGROSA	CORE 2 DUO	1
C.S. MEDALLA MILAGROSA	CORE I7- SEGUNDA GENERACION	1
C.S. JOSE CARLOS MARIATEGUI	CORE I5- CUARTA GENERACION	4
C.S. JOSE CARLOS MARIATEGUI	CORE I5- SEGUNDA GENERACION	3
C.S. JOSE CARLOS MARIATEGUI	CORE I5- TERCERA GENERACION	3
C.S. JOSE CARLOS MARIATEGUI	CORE I7-CUARTA GENERACION	1
C.S. JOSE CARLOS MARIATEGUI	PENTIUM CELERON	2
C.S. BAYOVAR	AMD PHENOM	2
C.S. BAYOVAR	CORE 2 DUO	3
C.S. BAYOVAR	CORE I3- TERCERA GENERACION	
C.S. BAYOVAR	CORE I5- SEGUNDA GENERACION	3
C.S. HUASCAR II	AMD ATHLON II	2
C.S. HUASCAR II	CORE I7-SEPTIMA GENERACION	1
C.S. HUASCAR II	CORE I3- TERCERA GENERACION	1
C.S. HUASCAR II	CORE I5- TERCERA GENERACION	1
C.S. HUASCAR II	CORE 2 DUO	2

C.S. HUASCAR II	CORE I5- CUARTA GENERACION	1
C.S. HUASCAR XV	AMD ATHLON II	2
C.S. HUASCAR XV	CORE I5- SEGUNDA GENERACION	2
C.S. HUASCAR XV	CORE I5- TERCERA GENERACION	2
C.S. HUASCAR XV	CORE I7- NOVENA GENERACION	9
C.S. HUASCAR XV	CORE I3- TERCERA GENERACION	1
C.S. HUASCAR XV	CORE I5- CUARTA GENERACION	1
C.S. HUASCAR XV	CORE 2 DUO	2
C.S. LA HUAYRONA	CORE 2 DUO	5
C.S. LA HUAYRONA	CORE I5- CUARTA GENERACION	1
C.S. LA HUAYRONA	CORE I5- SEGUNDA GENERACION	1
C.S. LA HUAYRONA	CORE I7- SEGUNDA GENERACION	2
C.S. LA HUAYRONA	Pentium D	1
C.S. LA HUAYRONA	CORE I5- TERCERA GENERACION	2
C.S. LA HUAYRONA	CORE I3- TERCERA GENERACION	1
C.S. LA HUAYRONA	CORE I3-SEGUNDA GENERACION	1
C.S. JUAN PABLO II	CORE I5- CUARTA GENERACION	2
C.S. JUAN PABLO II	CORE I5- SEGUNDA GENERACION	2
C.S. JUAN PABLO II	CORE I5- TERCERA GENERACION	1
C.S. JUAN PABLO II	CORE 2 DUO	2
C.S. JUAN PABLO II	CORE I3-SEGUNDA GENERACION	1
P.S. PROYECTOS ESPECIALES	Pentium D	2
P.S. PROYECTOS ESPECIALES	CORE I5- TERCERA GENERACION	1
P.S. PROYECTOS ESPECIALES	AMD PHENOM	2
P.S. PROYECTOS ESPECIALES	CORE I3- TERCERA GENERACION	1
P.S. PROYECTOS ESPECIALES	CORE I7-CUARTA GENERACION	2
P.S. SAGRADA FAMILIA	Pentium D	1
P.S. SAGRADA FAMILIA	AMD PHENOM	1
P.S. SAGRADA FAMILIA	CORE 2 DUO	2
P.S. SAGRADA FAMILIA	CORE I5- CUARTA GENERACION	1
P.S. SAGRADA FAMILIA	CORE I5- SEGUNDA GENERACION	1
P.S. SAGRADA FAMILIA	CORE I5- TERCERA GENERACION	1
C.S. SAN FERNANDO	CORE 2 DUO	7
C.S. SAN FERNANDO	CORE I5- CUARTA GENERACION	4
C.S. SAN FERNANDO	CORE I5- SEGUNDA GENERACION	4
C.S. SAN FERNANDO	CORE I7-SEPTIMA GENERACION	1
C.S. SAN FERNANDO	Pentium D	2
C.S. SAN FERNANDO	CORE I3- TERCERA GENERACION	3
C.S. SAN FERNANDO	CORE I5- TERCERA GENERACION	4
C.S. SAN FERNANDO	CORE I3-SEGUNDA GENERACION	2
C.S. SANTA MARIA	CORE 2 DUO	4
C.S. SANTA MARIA	CORE I5- CUARTA GENERACION	1
C.S. SANTA MARIA	CORE I7- NOVENA GENERACION	9
C.S. SANTA MARIA	CORE I3-SEGUNDA GENERACION	1
C.S. SANTA MARIA	CORE I7- SEGUNDA GENERACION	2
C.S. SANTA MARIA	AMD PHENOM	1

C.S. SANTA MARIA	AMD ATHLON II	2
C.S. SANTA MARIA	CORE I5- SEGUNDA GENERACION	1
C.S. SANTA MARIA	CORE I5- TERCERA GENERACION	1
C.S. STA FE DE TOTORITA	CORE I3-SEGUNDA GENERACION	3
C.S. STA FE DE TOTORITA	CORE I7-CUARTA GENERACION	2
C.S. STA FE DE TOTORITA	CORE I5- CUARTA GENERACION	4
C.S. STA FE DE TOTORITA	CORE I5- SEGUNDA GENERACION	4
P.S. CESAR VALLEJO	CORE I7-SEPTIMA GENERACION	2
P.S. CESAR VALLEJO	CORE I5- TERCERA GENERACION	1
P.S. CESAR VALLEJO	CORE I7- NOVENA GENERACION	7
P.S. CESAR VALLEJO	CORE I5- CUARTA GENERACION	1
P.S. CESAR VALLEJO	CORE I5- SEGUNDA GENERACION	1
P.S. JOSE CARLOS MARIATEGUI V ETAPA	CORE 2 DUO	4
P.S. JOSE CARLOS MARIATEGUI V ETAPA	CORE I5- TERCERA GENERACION	1
P.S. JOSE CARLOS MARIATEGUI V ETAPA	CORE I7- SEGUNDA GENERACION	1
P.S. JOSE CARLOS MARIATEGUI V ETAPA	CORE I5- CUARTA GENERACION	1
P.S. JOSE CARLOS MARIATEGUI V ETAPA	CORE I5- SEGUNDA GENERACION	4
P.S. 15 DE ENERO	CORE I7-CUARTA GENERACION	1
P.S. 15 DE ENERO	CORE I5- TERCERA GENERACION	1
P.S. 15 DE ENERO	CORE I3-SEGUNDA GENERACION	1
P.S. 15 DE ENERO	CORE I5- SEGUNDA GENERACION	1
P.S. 15 DE ENERO	CORE I5- CUARTA GENERACION	1
C.S. CAJA DE AGUA	CORE I7-SEPTIMA GENERACION	3
P.S. AZCARRUNZ ALTO	CORE I7- SEGUNDA GENERACION	1
C.S. ZARATE	CORE I7-CUARTA GENERACION	3
C.S. MANGOMARCA	CORE I7-SEPTIMA GENERACION	2
C.S. CAMPOY	CORE I7- NOVENA GENERACION	9
P.S. DANIEL ALCIDES CARRION	CORE I7- SEGUNDA GENERACION	1
C.S. SAN FERNANDO	CORE I7-CUARTA GENERACION	2
C.S. SAN HILARION	CORE I7-SEPTIMA GENERACION	2
C.S. SANTA ROSA	CORE I7- NOVENA GENERACION	9
C.S. LA LIBERTAD	CORE I7- SEGUNDA GENERACION	2
C.S. LA HUAYRONA	CORE I7-CUARTA GENERACION	2
C.S. SANTA FE DE TOTORITA	CORE I7-SEPTIMA GENERACION	2
P.S. 15 DE ENERO	CORE I7- NOVENA GENERACION	7
C.S. GANIMEDES	CORE I7- SEGUNDA GENERACION	2
C.S. HUSCAR II	CORE I7-CUARTA GENERACION	2
C.S. HUASCAR XV	CORE I7-SEPTIMA GENERACION	2
C.S. MEDALLA MILAGROSA	CORE I7- NOVENA GENERACION	9
P.S. AYACUCHO	CORE I7- SEGUNDA GENERACION	1
C.S. JAIME ZUBIETA	CORE I7-CUARTA GENERACION	3
C.S. BAYOVAR	CORE I7-SEPTIMA GENERACION	2
P.S. PROYECTOS ESPECIALES	CORE I7- SEGUNDA GENERACION	2
P.S. SAGRADA FAMILIA	CORE I7-CUARTA GENERACION	2
C.S. JOSE CARLOS MARIATEGUI	CORE I7-SEPTIMA GENERACION	2
C.S. CRUZ DE MOTUPE	CORE I7- NOVENA GENERACION	9

C.S. ENRIQUE MONTENEGRO	CORE 17- SEGUNDA GENERACION	4
C.S. 10 DE OCTUBRE	CORE 17-CUARTA GENERACION	2
C.S. JUAN PABLO II	CORE 17-SEPTIMA GENERACION	2
P.S. JOSE CARLOS MARIATEGUI V ETAPA	CORE 17- NOVENA GENERACION	7
P.S. MARISCAL CACERES	CORE 15- SEGUNDA GENERACION	4
P.S. CESAR VALLEJO	CORE 17-CUARTA GENERACION	2
P.S. AZCARRUNZ ALTO	CORE 15- SEGUNDA GENERACION	4
C.S. HUSCAR II	CORE 15- TERCERA GENERACION	4
C.S. BAYOVAR	CORE 17-NOVENA GENERACION	6
P.S. TUPAC AMARU II	CORE 17- SEGUNDA GENERACION	1
P.S. SAGRADA FAMILIA	CORE 17-SEPTIMA GENERACION	1
C.S. JOSE CARLOS MARIATEGUI	CORE 17- NOVENA GENERACION	9
C.S. CRUZ DE MOTUPE	CORE 17- SEGUNDA GENERACION	1
C.S. ENRIQUE MONTENEGRO	CORE 17-CUARTA GENERACION	5
C.S. 10 DE OCTUBRE	CORE 17-SEPTIMA GENERACION	1
C.S. JUAN PABLO II	CORE 17- NOVENA GENERACION	9
P.S. MARISCAL CACERES	CORE 17-CUARTA GENERACION	1
C.S. CAJA DE AGUA	CORE 17- NOVENA GENERACION	9
C.S. CAJA DE AGUA	CORE 17- SEGUNDA GENERACION	2
P.S. AZCARRUNZ ALTO	CORE 17-CUARTA GENERACION	1
C.S. ZARATE	CORE 17- SEGUNDA GENERACION	2
C.S. ZARATE	CORE 17-SEPTIMA GENERACION	1
C.S. MANGOMARCA	CORE 17- NOVENA GENERACION	9
C.S. MANGOMARCA	CORE 17- SEGUNDA GENERACION	3
C.S. CAMPOY	CORE 17- SEGUNDA GENERACION	3
P.S. DANIEL ALCIDES CARRION	CORE 17-CUARTA GENERACION	1
P.S. DANIEL ALCIDES CARRION	CORE 17-SEPTIMA GENERACION	1
P.S. DANIEL ALCIDES CARRION	CORE 17- NOVENA GENERACION	7
C.S. JAIME ZUBIETA	CORE 17-SEPTIMA GENERACION	1
P.S. SAGRADA FAMILIA	CORE 17- NOVENA GENERACION	7
P.S. SAGRADA FAMILIA	CORE 17- SEGUNDA GENERACION	2
P.S. AZCARRUNZ ALTO	CORE 17- NOVENA GENERACION	7
C.S. CAMPOY	CORE 17-SEPTIMA GENERACION	2
C.S. SAN FERNANDO	CORE 17- SEGUNDA GENERACION	1
C.S. SAN HILARION	CORE 17-CUARTA GENERACION	1
C.S. SANTA ROSA	CORE 17-SEPTIMA GENERACION	2
C.S. LA LIBERTAD	CORE 17- NOVENA GENERACION	9
C.S. SANTA FE DE TOTORITA	CORE 15-TERCERA GENERACION	4
P.S. 15 DE ENERO	CORE 17-SEPTIMA GENERACION	1
C.S. GANIMEDES	CORE 17- NOVENA GENERACION	12
C.S. HUSCAR II	CORE 17- SEGUNDA GENERACION	2
C.S. HUASCAR XV	CORE 17-CUARTA GENERACION	1
C.S. MEDALLA MILAGROSA	CORE 17-SEPTIMA GENERACION	1
P.S. AYACUCHO	CORE 17- NOVENA GENERACION	7
C.S. BAYOVAR	CORE 17-CUARTA GENERACION	1

C.S. SANTA MARIA	CORE I7-SEPTIMA GENERACION	1
P.S. TUPAC AMARU II	CORE I7- NOVENA GENERACION	7
C.S. ENRIQUE MONTENEGRO	CORE I7- TERCERA GENERACION	2
P.S. MARISCAL CACERES	CORE I7- SEGUNDA GENERACION	3
C.S. 10 DE OCTUBRE	CORE I7-NOVENA GENERACION	4
C.S. 10 DE OCTUBRE	CORE I3- TERCERA GENERACION	3
C.S. 10 DE OCTUBRE	CORE I5- TERCERA GENERACION	3
C.S. CHACARILLA DE OTERO	CORE I7-NOVENA GENERACION	12
C.S. ENRIQUE MONTENEGRO	CORE I7- NOVENA GENERACION	12
C.S. ENRIQUE MONTENEGRO	CORE 2 DUO	4
C.S. HUASCAR II	CORE I7-NOVENA GENERACION	9
C.S. HUSCAR II	CORE I7- NOVENA GENERACION	9
C.S. HUSCAR II	CORE 2 DUO	4
C.S. JAIME ZUBIETA	CORE I7-NOVENA GENERACION	9
C.S. JOSE CARLOS MARIATEGUI	CORE I 5- TERCERA GENERACION	4
C.S. JOSE CARLOS MARIATEGUI	CORE 2 DUO	7
C.S. Juan Perez Carranza	CORE I7- NOVENA GENERACION	9
C.S. LA HUAYRONA	CORE I7-NOVENA GENERACION	9
C.S. Lince	CORE I7-NOVENA GENERACION	9
C.S. Magdalena	CORE I7-NOVENA GENERACION	12
C.S. Max Arias Schreiber	CORE I7-SEPTIMA GENERACION	12
C.S. Miraflores	CORE I7-NOVENA GENERACION	9
C.S. Mirones	CORE I7- NOVENA GENERACION	9
C.S. Mirones Bajo	CORE I7-NOVENA GENERACION	9
C.S. Raul Patrucco	CORE I7-NOVENA GENERACION	12
C.S. San Borja	CORE I7-NOVENA GENERACION	9
C.S. San Cosme	CORE I7-NOVENA GENERACION	9
C.S. SAN FERNANDO	CORE I7- NOVENA GENERACION	9
C.S. San Miguel	CORE I7-NOVENA GENERACION	9
C.S. San Sebastian	CORE I7-NOVENA GENERACION	9
C.S. SANTA FE DE TOTORITA	CORE I5-SEGUNDA GENERACION	4
C.S. SANTA FE DE TOTORITA	CORE I7-NOVENA GENERACION	9
C.S. SANTA FE DE TOTORITA	CORE 2 DUO	4
C.S. SANTA ROSA	CORE I 5- TERCERA GENERACION	4
C.S. SANTA ROSA	CORE I5-SEGUNDA GENERACION	4
C.S. SANTA ROSA	CORE 2 DUO	6
C.S. STA FE DE TOTORITA	CORE I7-NOVENA GENERACION	9
C.S. STA FE DE TOTORITA	CORE 2 DUO	5
C.S. STA FE DE TOTORITA	CORE I 5- TERCERA GENERACION	3
C.S. Unidad Vecinal Nro 3	CORE I7-NOVENA GENERACION	9
C.S. V. Victoria Porvenir	CORE I7-NOVENA GENERACION	9
C.S. V.M.P. Socorro	CORE I7-NOVENA GENERACION	9
C.S. ZARATE	CORE I7-NOVENA GENERACION	9
P.S. 15 DE ENERO	CORE 2 DUO	4
P.S. AZCARRUNZ ALTO	CORE 2 DUO	4
P.S. AYACUCHO	CORE 2 DUO	3

P.S. CESAR VALLEJO	CORE 2 DUO	3
P.S. Huaca Pando	CORE I7-NOVENA GENERACION	7
P.S. MARISCAL CACERES	CORE 2 DUO	5
P.S. MARISCAL CACERES	CORE I7- NOVENA GENERACION	7
P.S. PROYECTOS ESPECIALES	CORE I7- NOVENA GENERACION	7
P.S. PROYECTOS ESPECIALES	CORE 2 DUO	3
P.S. Rosa de Sta. María	CORE I7-NOVENA GENERACION	7
P.S. Santa Rosa	CORE I7- NOVENA GENERACION	7
P.S. TUPAC AMARU II	CORE 2 DUO	4
TOTAL		1667

2. servicio de internet es inadecuado dado es ADSL y/o hfc, el sistema de cableado de red, los puertos o puntos de los RJ-45 necesitan mantenimiento urgente y se necesitan más puertos operativos para conectar PC a internet, todo el sistema de cableado necesita una atención adecuada y prudente (cambio de cableado por encontrarse en algunos casos dañados).
3. En algunos establecimientos de salud hubo inconvenientes con la velocidad del internet, por este motivo se fue aumentando la velocidad para evitar inconvenientes de lentitud, sin embargo, por el momento el problema persiste.
4. En el turno de la mañana hay alta demanda en la atención a los pacientes de los eess, el internet suele ponerse bastante lento, esto se debe a varios factores como: uso sin restricciones del internet, saturación, cantidad de máquinas que sobrepasa el ancho de banda de internet, etc.

DIAGNOSTICO DE PERSONAL

Actualmente el personal administrativo y asistencial tanto de la sede administrativa como establecimientos de salud tiene inconvenientes en esta emergencia sanitaria de Covid 19, dado que el personal se está contagiando y por ende algunas oficinas y/o servicios se quedan desabastecidos, faltando recursos humanos para brindar una buena atención, como son el caso de:

1. Personal administrativo y asistencial disminuido por contagios de Covid 19.
2. Falta de personal en algunos servicios y/o oficinas para satisfacer la alta demanda.
3. Personal Administrativo mal remunerado y altamente expuesto a pacientes Covid, debido a que estos atienden para los tramites administrativa diarios antes y después de la atención médica.
4. Personal con dificultades para el uso de equipos informáticos.
5. Falta de actualización en software como: ofimática, sistema operativo, etc.
6. Falta de familiaridad de ingreso a sistemas de la información.

DIAGNOSTICO DE SERVICIOS DE SALUD

La Dirección de Redes Integradas de Salud Lima Centro brinda servicios de atención de la salud a la comunidad de los 13 distritos de Lima y San Juan de Lurigancho

1. Personal administrativo y asistencial disminuido por contagios de Covid 19.
2. Falta de personal en algunos servicios y/o oficinas para satisfacer la alta demanda.
3. Personal Administrativo mal remunerado y altamente expuesto a pacientes Covid, debido a que estos atienden para los tramites administrativa diarios antes y después de la atención médica.
4. Personal con dificultades para el uso de equipos informáticos.
5. Falta de actualización en software como: ofimática, sistema operativo, etc.
6. Falta de familiaridad de ingreso a sistemas de la información.



INTEGRANTE DEL PROYECTO
SILVA BUITRÓN GIANCARLOS



INTEGRANTE DEL PROYECTO
LAZARTE TIRAPO DANIEL



PERU | Ministerio de Salud | Dirección de Redes Integradas de Salud Lima Centro

.....
Inga PAOLA JESUS LLAVE ESCOBEDO
Jefa de la Oficina de Gestión de la Información
DIRIS Lima Centro

Anexo 4. Objetivos de Desarrollo tecnológico

OBJETIVOS AL DESARROLLO DE TECNOLOGÍAS DE LA INFORMACION

1. Objetivos de TI

La Oficina de Tecnologías de Información es la encargada de brindar el apoyo, soporte y Velar por un adecuado uso y aprovechamiento de los recursos informáticos para la optimización de los procesos, actividades y atención oportuna, integral, confiable de la información para la toma de decisiones de las demás unidades orgánicas mediante el desarrollo, implementación y supervisión del correcto funcionamiento de los sistemas de la información y comunicaciones, así como la adquisición y control del parque informático, garantizando a su vez la integridad y calidad de los disponibles, permitiendo a la Dirección de Redes Integradas de Salud Lima Centro ciudad lograr sus objetivos.

Los Objetivos de la Oficina de Tecnologías de la información son los siguientes:

- Diseñar sistemas, supervisando el desarrollo de sus aplicaciones en la institución. Programar y supervisar la implementación de sistemas.
- Efectuar diagnósticos referido a la utilización potencial de las computadoras, formulando planes de contingencia para su mejor operatividad.
- Implementar controles con el propósito de salvaguardar los datos, con la finalidad de preservar la integridad de la información procesada por la institución.
- La Oficina de Tecnologías de la Información da la asistencia técnica - TIC (Tecnologías de la Información y Comunicación) a las Direcciones Y/o Oficinas de la sede administrativa para la toma de decisiones en favor de la comunidad de la jurisdicción de la Dirección de Redes Integradas de Salud Lima Centro.
- La Oficina de Tecnologías de la Información en coordinación con la Oficina de Comunicaciones y Reclamaciones realiza el mantenimiento y mejoramiento de la página web de la Dirección de Redes Integradas de Salud Lima Centro.
- Identificar y proponer nueva aplicación de tecnologías de información.

2. Situación General de la Oficina de Tecnologías de la información

La Oficina de Tecnologías de la Información actualmente cuenta con diversos problemas de adquisiciones estos con por falta de presupuesto, los cuales impiden que se puedan cumplir las metas trazadas para el mejoramiento de la Tecnologías de la Información y comunicaciones para los establecimientos de salud y sede administrativa, estas son las siguientes:

- Falta de presupuesto para la Adquisición de Equipos Informáticos para los establecimientos de salud y sede administrativa.
- Falta de presupuesto para Adquisiciones de Materiales para instalación de cableado estructurados (Red e internet) para los establecimientos de salud y sede administrativa.
- Falta de presupuesto para adquisición de Repuestos para reparación de equipos de cómputo e impresoras de los establecimientos de salud y sede administrativa.
- La Oficina de Tecnologías de la Información no cuenta con un presupuesto asignado lo cual retrasa la adquisición de diversos equipos lo cual se requiere para el trabajo diario, asimismo sería recomendable que esta Oficina sea una Dirección al Igual que nuestro ente superior la Oficina General de Tecnologías de la información del Ministerio de Salud.

3. Estructura Interna y Funciones

Oficina de Tecnologías de la Información

La Oficina de Tecnologías de la Información, depende de la Dirección Administrativa de la Dirección de Redes Integradas de Salud Lima Centro.

La Oficina de Tecnologías de la Información es responsable de conducir el uso de recursos informáticos a su cargo en la DIRIS LC, y de proponer las políticas, planes, documentos normativos y estándares pertinentes.

Conduce, planea, organiza, supervisa y coordina el desarrollo de las actividades administrativas y técnicas de la Programación y Desarrollo Informático; Soporte Técnico; y telecomunicaciones y Redes, de la Dirección de Redes Integradas de Salud Lima Centro.

Son funciones de la Oficina de Tecnologías de la Información, las siguientes:

- a) Formular, proponer, evaluar e implementar los planes de gestión y plan estratégico en materia de tecnologías de la información de la DIRIS LC, en concordancia con las políticas nacionales y los principios de buen gobierno sobre la materia y la normatividad vigente.
- b) Conducir, Coordinar, ejecutar y controlar el funcionamiento, instalación, operación y mantenimiento de la infraestructura física, software y programas informáticos de los órganos y áreas funcionales de la DIRIS LC; así como implementar soluciones de protección de redes, equipos y sistemas de información, en concordancia con las políticas de seguridad establecidas.
- c) Diseñar, desarrollar, implantar, capacitar y mantener los sistemas de información que sirvan de apoyo a las actividades operativas y de gestión de la DIRIS LC.
- d) Administrar los medios informáticos, sistemas de información a través del desarrollo de software personalizados, así como también las redes locales y remotas de los órganos y áreas funcionales de la DIRIS LC, garantizando su operatividad, disponibilidad y seguridad.
- e) Proponer, desarrollar e implementar los documentos normativos y estándares relacionados con el desarrollo de los sistemas de información, nuevas oportunidades de aplicación de tecnología de la información y comunicación, adquisición y administración de equipamiento de cómputo, redes y comunicaciones, y el uso de los recursos informáticos de la DIRIS LC, en el marco de la normativa vigente.
- f) Elaborar, desarrollar, ejecutar, evaluar y actualizar el Plan Estratégico de Tecnologías de Información (PETI) de la DIRIS LC, en armonía con el Plan Estratégico Institucional.
- g) Asesorar y brindar asistencia técnica en los temas relacionados con las Tecnologías de la Información y Redes de Comunicación en la DIRIS LC, en coordinación con los órganos competentes.
- h) Formular las políticas, planes y proyectos referidos a la modernización de la gestión y estandarización de procesos para el desarrollo de sistemas de información y de comunicaciones.
- i) Establecer los planes de contingencia necesarios para la seguridad de los procesos informáticos y la información de la DIRIS LC.
- j) Administrar y supervisar la ejecución del portafolio de proyectos de Tecnologías de la Información y Comunicaciones de la DIRIS LC.
- k) Implementar y ejecutar el diseño de arquitectura y desarrollo de sistemas, investigación y proyectos de tecnología de información, mantenimiento preventivo y correctivo de equipos informáticos y la implementación de sistemas de mejora continua.
- l) Participar de la presentación referidos a servicios informáticos, así como en la propuesta para la elaboración de proyectos de inversión en el sistema informático del ámbito geográfico de la Dirección de Redes Integradas de Salud Lima Centro.

- m) Brindar y apoyar en las especificaciones o características técnicas para la adquisición de equipos informáticos de la Dirección de Redes Integradas de Salud Lima Centro, en concordancia con las normas y estándares establecidos.
- n) Brindar soporte técnico a los usuarios de equipos y sistemas informáticos y capacitarlos en el marco de su competencia.
- o) Supervisar el cumplimiento de los contratos de los servicios públicos de telecomunicaciones; así como de los trabajos encargados a terceros relacionados a las infraestructuras tecnológicas y aplicativos de la DIRIS LC.
- p) Cumplir y hacer cumplir el código de ética de la función pública, los reglamentos, directivas, manuales e instrumentos de gestión institucional, de acuerdo a la Oficina a su cargo.
- q) Implementar las recomendaciones emitidas por el órgano de control interno y externo.

La Oficina de Tecnologías de la Información, desarrolla su función a través de las siguientes Unidades Funcionales:

- Unidad Funcional de Telecomunicaciones y Redes
- Unidad Funcional de Soporte Técnico

Unidad Funcional de Telecomunicaciones y Redes

Aplica la tecnología de las telecomunicaciones y redes como herramienta de apoyo a las funciones y toma de decisiones de la Dirección de Redes Integradas de Salud Lima Centro.

Son funciones de la Unidad Funcional de Telecomunicaciones y Redes, las siguientes:

- a) Participar en la implementación de los objetivos y metas específicos asignados a la Dirección de Redes Integradas de Salud Lima Centro, en el Plan Estratégico de Sistemas de Información del Ministerio de Salud y la elaboración del Plan Operativo Anual de la Oficina.
- b) Formular, proponer e implementar directivas y procedimientos de gestión para la mejora continua y optimización de los procesos inherentes a sus funciones, según normatividad vigente.
- c) Monitorear y evaluar el cumplimiento de los contratos de los servicios públicos de telecomunicaciones de la Dirección de Redes Integradas de Salud Lima Centro.
- d) Identificar, priorizar y proponer nuevas oportunidades de aplicación de las necesidades de diseño y mejoramiento de los sistemas de Telecomunicaciones.
- e) Diseñar, administrar, mantener actualizada, controlar y supervisar la red de comunicaciones para permitir una rápida y eficiente comunicación de voz, imágenes y datos a través de cualquier punto de la red en las comunicaciones internas (intranet), externas con clientes (extranet) y las comunicaciones por internet.
- f) Definir la arquitectura de comunicaciones y su integración con los servicios informáticos que la red posee.
- g) Analizar, evaluar y recomendar la adquisición de nuevo equipamiento con el objetivo de mejorar la infraestructura de comunicaciones LAN, WAN, cableada estructurada y medios de transmisión u otros que la nueva tecnología ofrezca.
- h) Implementar y ejecutar proyectos de desarrollo de telecomunicaciones que se programen.
- i) Evaluar, planificar y coordinar las mejoras en la red de comunicaciones, en cuanto a recursos de hardware, software, interconexión de equipos, redes con otras redes de otras instituciones con posibles convenios suscritos, ancho de banda y de la infraestructura de comunicaciones en la Sede Administrativa, red de Oficinas y demás.
- j) Intervenir en las evaluaciones técnicas de los procesos y adquisición de equipos, componentes, insumos, reparaciones de equipos, servicios de cableado estructurado, instalaciones y otros relacionados a la arquitectura de comunicaciones de la Dirección de Redes Integradas de Salud Lima Centro, así como la participación en la supervisión de los trabajos y servicios indicados.

- k) Diseñar, supervisar y mantener actualizado la página institucional de la Dirección de Redes Integradas de Salud Lima Centro.
- l) Brindar a los usuarios internos y externos asesoría y asistencia técnica cuando se requiera en el uso de aplicaciones de telefonía y redes de comunicación y nuevas tecnologías de información, acorde a las normas y estándares de informática y de telecomunicaciones establecidas por el Ministerio de Salud.
- m) Cumplir y hacer cumplir el código de ética de la función pública, controlar y supervisar el cumplimiento de todas las normas existentes, correspondientes a la Unidad Funcional de Telecomunicaciones y Redes.
- n) Otras funciones que la jefatura le asigne explícitamente.

Unidad Funcional de Telecomunicaciones

I. Logros

- Se atendieron oportunamente las dificultades de caídas y/o ampliaciones de puntos de red e internet en los establecimientos de salud y sede administrativa.
- Se realizó implementaciones de cableado estructurado en los centros comunitarios mentales los cuales fueron inaugurados en el año 2019, actualmente todos cuenta con puntos de internet.
- Se ha incrementado la línea de internet en los Establecimiento de Salud.
- Se ha migrado las líneas de internet de ADSL (Tecnologías Antiguas) a HFC (Tecnología Actual) a 15 Establecimiento de Salud a 60Mb al 20% de velocidad.
- Se está coordinado para el aumento de velocidad a los establecimientos de salud que no tengas factibilidades técnicas para realizar el cambio de tecnología.
- Se ha brindado la asistencia técnica para la implementación de nuevos puntos de red e internet en los establecimientos de salud, los cuales han adquiridos sus materiales mediante caja chica.
- Se dio solución a los problemas suscitados en el Sistema de Video Vigilancia de los establecimientos de salud.
- Se ha brindado asistencia técnica para la solución de los problemas encontrados con los relojes marcadores los cuales presentan problemas de conectividad y/o reubicación debido a trabajos de infraestructuras.
- Coordinaciones con las empresas que nos brinda Servicio de telefonía fija, para la reubicación y traslados de líneas en los establecimientos de salud.

II. Debilidades

- Carencia de Recursos informático, materiales para cableado estructurado y Recursos Humanos.
- Falta con capacitaciones en cursos de telecomunicaciones.
- Demora en los procesos de adquisiciones de esta oficina.
- Falta de presupuesto en los servicios y/o requerimientos solicitados para mejora de los establecimientos de salud.

III. Oportunidades

- Avance tecnológico en las telecomunicaciones que permita el acceso a nuevas tecnologías para acceso a internet, telefonía voz Ip, etc.

- Recibir practicantes de institutos relacionados a ingeniería de sistemas, electrónica, soporte técnico, redes y otros fines.
- Ejecutar proyectos de telecomunicaciones en apoyo a las áreas.
- Acceso a tecnología de punta con reducción de costos en comunicación.

IV. Amenazas

- Falta de cultura de las telecomunicaciones de parte del personal de la Dirección de Redes Integradas de Salud Lima Centro.
- Falta de Presupuesto asignado para capacitación de personal de la Oficina de Tecnología de Información y para la implantación de una nueva infraestructura tecnológica.
- Desfase tecnológico de los equipos de telecomunicaciones.
- Falta de priorización en el presupuesto para la compra de equipos de telecomunicaciones de última tecnología y contratación de personal calificado.

Unidad Funcional de Soporte Técnico

Son funciones de la Unidad Funcional de Soporte Técnico, las siguientes:

- Contribuir en la formulación del Plan Operativo Anual de la Oficina de Tecnologías de la Información.
- Formular, implementar y/o proponer directivas y procedimientos de gestión para la mejora continua y optimización de los procesos inherentes a sus funciones, según normatividad vigente.
- Identificar y priorizar las necesidades de diseño y mejoramiento de los sistemas de información administrativa, gestión, asistencial y estadística.
- Optimizar que los usuarios internos y externos, tengan la disponibilidad de asesoría y asistencia técnica en el uso de aplicaciones informáticas, telecomunicaciones y nuevas tecnologías de la información, establecidas por el Ministerio de Salud.
- Brindar asistencia técnica a las unidades funcionales de la Dirección de Redes integradas de Salud lima Centro en asuntos de proyectos de tecnología de información, diseño y desarrollo de sistemas.
- Programar y ejecutar el mantenimiento preventivo de los equipos de cómputo.
- Formular, proponer e implementar los manuales de procedimientos para el buen uso de equipos o hardware informático, copias de seguridad, contingencias, envío, recepción de información, acceso a la red, internet.
- Definir y aplicar controles de acceso general (Seguridad física y lógica de los equipos centrales de servicio general).
- Supervisar y Monitorear el inventario del parque informático, controlar el buen uso de los Equipos, repuestos y programas fuentes y proponer acciones de mantenimiento y reformas de todos los sistemas de la Dirección de Redes Integradas de Salud Lima Centro.
- Cumplir y hacer cumplir el código de ética de la función pública, controlar y supervisar el cumplimiento de todas las normas existentes, correspondientes a la Unidad Funcional de Soporte Técnico.
- Otras funciones que el Jefe/a de la Oficina de Tecnologías de la Información, le asigne explícitamente.

I. Logros

- Se realizó el Inventario, Mantenimiento de Equipos de Cómputo e Impresoras de la sede administrativa.
- Diariamente se procede a brindar soporte técnico a los usuarios de los diferentes establecimientos de salud, así como las oficinas de la Sede Administrativa, en cuanto a configuración, reinstalación y apoyo informático.
- Diariamente se brinda el apoyo en la sede administrativa con configuración de impresoras, problemas con el pc, reinstalación de sistema operativo, etc., se da Soporte Help Desk a los usuarios finales aproximadamente de 15 a 20 minutos por día.
- Esta Oficina Realizo correctamente el mantenimiento y actualización del Siga y Siaf de la Diris Lima Centro, coordinando con la Sectorista del Ministerio de Economía y Finanzas.
- Se solucionó problemas técnicos en los Sistemas de Administración financiera-Siaf y sistema integrado de Gestión Administrativa –Siga, en coordinación con el Ministerio de Economía y Finanzas.
- Se ha realizado la adquisición de un storage de 32Tb para el almacenamiento de la información y Backup de los Sistemas que se cuentan actualmente como: Siga, Siaf, Sistema Tramite Documentario, Módulo de defunciones-SIS, Módulo de planeamiento, Módulo de vacuna, Módulo de tablero de mando, Módulo de papeletas de salida, Módulo de banco de sangre, etc.
- Se ha implementado en el servidor sistemas virtuales para así poder solucionar problemas con algún servidor en caso de caída (backup).
- Se realizó el mapeado de los equipos de cómputo que se conectan al firewall y al internet de la sede administrativa, esta configuración se ha realizado mediante la Mac y/o Ip de las tarjetas de red, así logra administrar las Pc y proporcionar accesos a ciertas páginas de acuerdo a la solicitud del Director y/o Jefe.

II. Debilidades

- Carencia de Recursos informáticos, repuestos y Recursos Humanos.
- Falta de capacitaciones al personal, falta de capacitación especializada en tecnologías de Información y Comunicación(TIC) al personal de la Oficina de Tecnologías de Información.

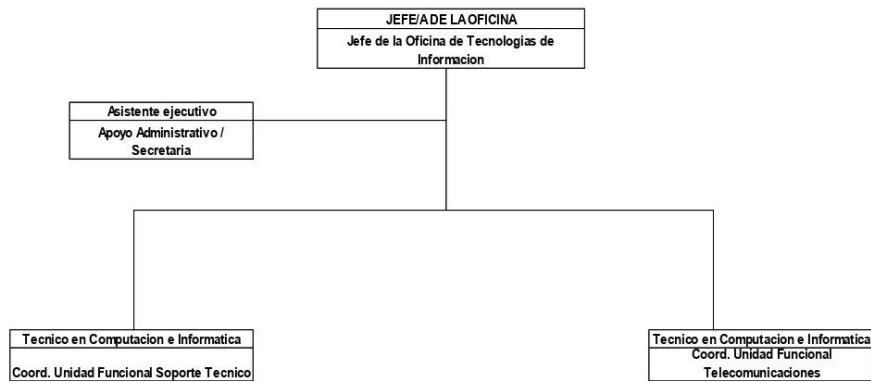
III. Oportunidades

- Avance tecnológico que permita el acceso a nuevas tecnológicas de información.
- Recibir practicantes de institutos relacionados a ingeniería de sistemas, electrónica, soporte técnico, redes y otros fines.
- Ejecutar proyectos informáticos en apoyo a las áreas.
- Buena imagen de la Dirección de Redes Integradas de Salud Lima Centro ante la comunidad.

IV. Amenazas

- Falta de cultura informática de parte del personal de la Dirección de Redes Integradas de Salud Lima Centro.
- Personal de la Dirección de Redes Integradas de Salud Lima Centro poco capacitado en el uso de software de ofimática, sistema operativo, otros.
- Falta de Presupuesto asignado para capacitación de personal de la Oficina de Tecnología de Información y para la implantación de una nueva infraestructura de la oficina.
- Desfase tecnológico de los equipos informáticos y telecomunicaciones.
- Falta de priorización en el presupuesto para la compra de equipos informático de última tecnología y contratación de personal calificado.
- Presencia Virus, gusanos y otros cada vez más sofisticados que deterioran el sistema informático.

ORGANIGRAMA FUNCIONAL DE LA OFICINA DE TECNOLOGÍAS DE INFORMACION




INTEGRANTE DEL PROYECTO
SILVA BUITRON GIANCARLOS


INTEGRANTE DEL PROYECTO
LAZARTE TIRAFO DANIEL


INTEGRANTE DEL PROYECTO
INO. PAOLAVICUS LLAVE ESCOBEDO
JEFE DE LA OFICINA DE TECNOLOGÍAS DE INFORMACION

Anexo 5. Diagnóstico de las políticas

DIAGNÓSTICO DE LAS POLÍTICAS Y ACCIONES DE SEGURIDAD TECNOLÓGICA DE LA DIRIS

La Oficina de Tecnologías de la Información es la encargada de velar por los recursos de la Tecnologías de la Información de la Dirección de Redes Integradas de Salud Lima Centro.

Situación de la Oficina de Tecnologías de la Información

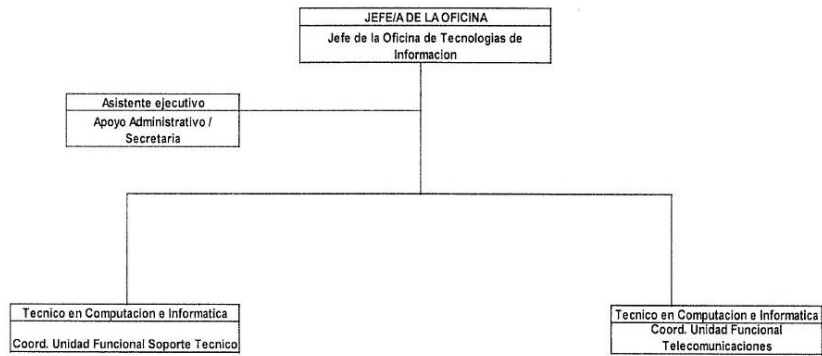
La Oficina de Tecnologías de la Información está bajo la responsabilidad de la Dirección Administrativa de la Dirección de Redes Integradas de Salud Lima Centro, esta oficina se encarga de toda la parte de Tecnologías de la Información y Comunicación – TIC las cuales son fundamentales para el avance de las metas institucionales.

La Oficina de Tecnologías de Información tiene las siguientes funciones:

1. Proponer, desarrollar e implementar sistemas informáticos tendentes a una Administración integrada con base de datos, redes y sistemas de soporte informático.
2. Implementar y coordinar el mantenimiento de los sistemas automatizados de información de la institución (SIAF-SIGA).
3. Administrar los sistemas y equipos informáticos, proponiendo acciones orientadas a su modernización y actualización.
4. Proponer y desarrollar planes de contingencia y de seguridad de la información (BACKUP).
5. Programar, ejecutar, supervisar y evaluar las actividades relacionadas con el soporte tecnológico y el mantenimiento de los programas y equipos informáticos, así como de las redes y comunicaciones de datos.
6. Promover la capacitación del personal de la institución en los conocimientos de TIC, para un buen manejo sistemático y de atención a los usuarios.
7. Mantener un inventario actualizado de los equipos de cómputo, de sistemas y programas informáticos y de licencias de Software.
8. Planear, organizar, dirigir, ejecutar, controlar y evaluar los programas y proyectos de Tecnologías de la Información.
9. Mantenimiento a la Página Web y el Portal Electrónico de la Dirección de Redes Integradas de Salud Lima Centro.
10. Custodiar la información producida por los sistemas de información de la institucional.

11. Identificar y evaluar nuevas oportunidades de aplicación de las tecnologías de información y comunicación.
12. Mantener actualizado el Portal de Transparencia con la información que remitan las diferentes oficinas y/ o Direcciones de la Dirección de Redes Integradas de Salud Lima Centro.
13. Realizar otras funciones de su competencia que son asignadas a la Oficina de Tecnologías de Información.

ORGANIGRAMA FUNCIONAL DE LA OFICINA DE TECNOLOGIAS DE INFORMACION



Fortalezas, Oportunidades Debilidades, Amenazas de la Oficina de Tecnologías de la Información.

Fortalezas	Oportunidades
<p>-Desarrollo de plan de acciones inmediatas para la solución de distintas incidencias.</p> <p>- Personal con experiencia y capacidad técnica para la ejecución de sus labores en las Oficinas y/o Direcciones que conforman la Dirección de Redes Integradas de Salud Lima Centro (Desarrollo de Software, Desarrollo Web, Redes y Telecomunicaciones).</p> <p>-Personal proactivo e identificado con la institución.</p> <p>-Contamos con Políticas y procedimientos de Backup y de Contingencia, que aseguran la continuidad de los servicios y reacción inmediata frente a posibles desastres.</p>	<p>-Avance tecnológico que permita el acceso a nuevas tecnológicas de información.</p> <p>-Recibir practicantes de institutos relacionados a ingeniería de sistemas, electrónica, soporte técnico, redes y otros fines.</p> <p>- Ejecutar proyectos informáticos en apoyo a las direcciones y /o oficinas.</p> <p>- Buena imagen de la Dirección de Redes Integradas de Salud Lima Centro ante la comunidad.</p> <p>-Acceso a tecnología de punta con reducción de costos en comunicación y soporte técnico.</p>
Debilidades	Amenazas
<p>-Carencia de Recursos informáticos, telecomunicaciones y Recursos Humanos.</p> <p>-Falta de capacitaciones al personal, falta de capacitación especializada en tecnologías de Información y Comunicación (TIC) al personal de la Oficina de Tecnologías de Información.</p> <p>- Falta de Personal calificado para la realizacion de Directivas, documento de tic, etc.</p>	<p>- Falta de cultura informática de parte del personal de la Dirección de Redes Integradas de Salud Lima Centro.</p> <p>- Personal de la Dirección de Redes Integradas de Salud Lima Centro poco capacitado en el uso de software de ofimática, sistema operativo, otros.</p> <p>- Falta de Presupuesto asignado para capacitación de personal de la Oficina de Tecnología de Información y para la implantación de una nueva infraestructura de la oficina.</p> <p>-Desfase tecnológico de los equipos informáticos y telecomunicaciones.</p> <p>-Falta de priorización en el presupuesto para la compra de equipos informático de última tecnología y contratación de personal calificado.</p> <p>-Presencia Virus, gusanos y otros cada vez más sofisticados que deterioran el sistema informático.</p>



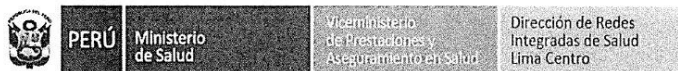
INTEGRANTE DEL PROYECTO
SILVA BUITRÓN GIANCARLOS



INTEGRANTE DEL PROYECTO
LAZARTE TIRAPO DANIEL



JEFE DE LA OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN
DIRIS Lima Centro



PLAN DE MANTENIMIENTO PREVENTIVO - CORRECTIVO

**DIRECCIÓN DE REDES INTEGRADAS DE SALUD LIMA
CENTRO**

OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN

Dirección: Av. Nicolás de Piérola N.º 617-623, Cercado de Lima –Perú
Telf. (511) 207-5700 Anexo:1507



PERÚ

Ministerio
de Salud

Viceministerio
de Prestaciones y
Aseguramiento en Salud

Dirección de Redes
Integradas de Salud
Lima Centro

Tabla de Contenido

1. INTRODUCCIÓN
2. OBJETIVO
 - 2.1. Objetivo General
 - 2.2. Objetivo Específicos
3. DEFINICIONES
4. ALCANCE DL DOCUMENTO
5. POLITICAS DE CUMPLIMIENTO PARA LOS RESPONSABLES
6. RESPONSABILIDAD
7. PLAN DE MANTENIMIENTOS
 - 7.1. Cronograma de Mantenimientos
 - 7.2. Seguimiento y Monitoreo
 - 7.3. Riesgos

Dirección: Av. Nicolás de Piérola N.º 617-623, Cercado de Lima –Perú
Telf. (511) 207-5700 Anexo:1507



1. INTRODUCCIÓN

La Oficina de Tecnologías de la Información en la Dirección de Redes Integradas de Salud Lima Centro, realiza el Plan de Mantenimiento de Equipos Informáticos como un proceso continuo de planeación para así evitar el deterioro de los equipos informáticos. Estas acciones buscan asegurar la reanudación eficiente y efectiva de los servicios y operaciones de Tecnologías de la Información y Comunicaciones en el menor tiempo e impacto posible.

El presente plan permite a la oficina de tecnologías de la información contar con un registro detallado de necesidad, falencias e intervalos de tiempo; variables con las cuales esta oficina procederá a suministrar a los diferentes grupos y optimizar los recursos para el buen funcionamiento.

Este Plan de Mantenimiento permite actualizar los servicios habilitados, normalizar los procedimientos y realizar el seguimiento y control para dar mejores servicios tecnológicos a los usuarios finales.

2. OBJETIVO

EL objetivo del mantenimiento es evitar los fallos constantes, logrando evitarlas consecuencias de las fallas de los equipos, previniendo esto antes de que ocurra.

Los mantenimientos preventivos se incluyen cambios de piezas desgastadas o que estes fallando como coolers, fuentes de poder, discos duros, etc., esto debe evitar los fallos en los equipos antes de que ocurran.

2.1. Objetivo General

Se determina las condiciones de operación de los equipos de cómputo, impresora para disminuir los daños ocasionados por factores de falta de mantenimiento y presencias de fallas debido al sobrecalentamiento y/o antigüedad de los equipos.

2.2. Objetivo Especifico

El presente mantenimiento servirá para evitar el deterioro o el daño total de los equipos, esto se realizará en un tiempo prudencial previo análisis de los tiempos evitando así que los procesos diarios se vean afectados.

3. DEFINICIONES

Estas son las siguientes definiciones que se utilizan en las Tecnologías de la Información y Comunicación:

Hardware: Hace referencia a cualquier componente físico tecnológico, que trabaja con la computadora.

Microsoft Windows 2016 R2: Es un sistema operativo de la familia de Windows de la compañía Microsoft para servidores.



PERÚ

Ministerio
de Salud

Viceministerio
de Prestaciones y
Aseguramiento en Salud

Dirección de Redes
Integradas de Salud
Lima Centro

Servidor: Computadora que es compartida, en una red informática por múltiples usuarios en el almaceno sistema para el uso de los usuarios.

Sistema Web: Aquellas aplicaciones en que los usuarios puede utilizar accediendo a un servidor web a través de internet o de una intranet mediante un navegador.

Switch: Es un Dispositivo que permite la interconexión de redes solo cuando esta conexión es necesaria y correctamente instalada.

Software: Conjunto de los componentes lógicos necesarios para hacer posible la realización de una tarea específica.

TIC: Tecnologías de Información y Comunicación.

Ups: Sistema de alimentación Ininterrumpida, fuente de suministro eléctrico que posee una batería con el fin de seguir dando energía a un dispositivo en el caso de interrupción eléctrica.

Windows 10: Sistema operativo de la familia Windows de la compañía Microsoft para estaciones de trabajo.

Office: Microsoft Office es un paquete de programas informáticos para oficina desarrollado por Microsoft, contiene Microsoft Word, Excel, Power Point, etc.

Cableado Estructurado: El cableado estructurado consiste en cable de par trenzados protegidos, esta solución ayuda a la implementación de una red de área local LAN.

Mantenimiento: Es un proceso que se realiza para mantener la operatividad de un bien (equipos), esto con la finalidad de seguir funcionando sin problema alguno, esto se divide en los siguientes:

Mantenimiento Preventivo: esto se realiza con un determinado tiempo evitando así los desperfectos, esto consiste en dar limpieza general al equipo de cómputo y verificar su óptimo funcionamiento, estos se dividen en dos fases:

- Mantenimiento físico
- Mantenimiento de software

Mantenimiento Correctivo: esto se realiza de manera forzosa e imprevista cuando comienza a fallar los equipos esto con la necesidad de repararlos para así evitar que deje de funcionar completamente.

Storage: es nombre correspondiente a una tecnología de almacenamiento dedicado a compartir información a través de una carpeta al equipo de cómputo, estos accesos se dan a través de un usuario y clave independiente para cada usuario y mediante ftp.



PERÚ

Ministerio
de Salud

Viceministerio
de Prestaciones y
Aseguramiento en Salud

Dirección de Redes
Integradas de Salud
Lima Centro

Ups: es un dispositivo el cual tiene batería esto permite que ante un apagado total de la energía eléctrica el equipo de cómputo pueda seguir prendido por un determinado tiempo dando la oportunidad de guardar la información.

4. ALCANCE DEL DOCUMENTO

De acuerdo a las actividades a realizar dentro del presente plan de mantenimiento de la Diris Lima Centro, el alcance de este documento corresponde a:

- a. La definición del cronograma del mantenimiento preventivo para los servicios tecnológicos de la entidad.
- b. Asignación de responsabilidades de cumplimiento al equipo a la Oficina de Tecnologías de la Información – Unidad Funcional de Soporte Técnico.

5. POLITICAS DE CUMPLIMIENTO PARA LOS RESPONSABLES

Teniendo en cuenta los servicios que presta la Oficina de Tecnologías de tecnologías de la Información, se indica las responsabilidades que cumplen por parte del equipo de la Unidad de Soporte Técnico - Tecnologías de tecnologías de la Información:

- 5.1.1 El Administrador y el responsable del data center; deberá de realizar un programa anual de mantenimiento preventivo de los equipos y presentarlos al jefe de la oficina para su valoración y aprobación.
- 5.1.2 Todo programa de mantenimiento preventivo debe considerar dentro de sus actividades entre otras las siguientes:
 - La verificación diaria al funcionamiento del sistema de aire acondicionado través e la lectura a los medidores de temperatura y humedad.
 - La verificación mensual al sistema de aire acondicionado para corroborar que no tenga fugas, así como la limpieza de los filtros.
 - Verificar mensualmente que los sistemas de UPS mantengan un nivel de carga adecuado. Los sistemas de extinción deben ser verificados mensualmente, que se encuentren funcionales, así como la verificación de la fecha caducidad.
- 5.2 Las actividades de mantenimiento a los servidores o equipos dentro del Centro de Procesamiento de Datos deben de realizarse previa programación y se debe informar a los usuarios al menos con un día de anticipación en el caso que el servicio se suspenda.
- 5.3 El operador o responsable de la Unidad del Centro de Procesamiento de Datos tiene la obligación de supervisar el trabajo realizado de mantenimiento preventivo y correctivo, vigilar los procedimientos de diagnóstico que el personal técnico lleva a cabo.
- 5.4 El operador del Centro de Procesamiento de Datos debe de verificar que el personal técnico de mantenimiento debe de registrar las actividades en el aplicativo de mesa de ayuda.



PERÚ

Ministerio
de Salud

Viceministerio
de Prestaciones y
Aseguramiento en Salud

Dirección de Redes
Integradas de Salud
Lima Centro

- 5.5 Al terminar el mantenimiento el operador del centro de Procesamiento de Datos debe informar al encargado del proyecto que se cumplieron las actividades del mantenimiento.
- 5.6 Es responsabilidad del operador del centro de procesamiento de datos reportar la hora y fecha en la que concluyen los servicios de mantenimiento.
- 5.7 Es responsabilidad del líder de programa supervisa los trabajos que se realizan de adecuación y/o actualización de infraestructura tecnológica en horarios no laborales en el centro de procesamiento de datos.
- 5.8 Los recursos de tecnologías de la información deben ser utilizados en el desarrollo de las funciones y actividades laborales del servidor público y vinculado al cumplimiento de los objetivos de la función pública de la Diris lima centro.
- 5.9 El servidor Público en su carácter de usuario del equipo de cómputo, independientemente de su nivel y cargo debe de apegarse a los lineamientos establecidos y demás disposiciones aplicables.
- 5.10 El usuario a cargo de un bien con componente TIC, entendiéndose por este entre otros; las computadoras, periféricos (impresoras, escáner, etc.) y demás bienes similares tienen la obligación de firmar el resguardo respectivo en los formatos que para tales efectos utiliza la Oficina de Tecnologías de la Información.
- 5.11 Cada equipo debe de contar con su licencia correspondiente de uso instalación del mismo de acuerdo con la plataforma de software autorizada, todos los usuarios de bienes de TIC deben de enterarse de la forma de uso y operación de los equipos y licencias descritas del propietario antes de usar el bien respectivo.
- 5.12 Son obligaciones de los usuarios de un bien de TIC:
- Apagar el equipo completamente al concluir su jornada de trabajo o durante los recesos o descanso prologando (horas de comida, reuniones comisiones, etc.)
 - Mantener limpias las aéreas cercanas al equipo de cómputo.
 - Proporcionar limpieza exterior frecuentemente.
 - No colocar cerca de los equipos de cómputo líquidos, comida, cigarrillos encendido o materiales que puedan causar daños en su normal funcionamiento.
 - Mantener despejadas las hendiduras de ventilación que tienen los equipos de cómputo y no colocar objetos encima del equipo.
 - Todo usuario tiene la obligación de hacer copia de respaldo de la información institucional.
 - Dar aviso inmediato a la mesa de ayuda de la Oficina de Tecnologías de la Información a través de las líneas telefónicas y/o mandar correo a la mesa de ayuda, cuando su equipo presente alguna falla de tipo de cableado o cableado eléctrico,



de hardware o software en el entendido que el usuario nunca debe tratar de corregir cualquier situación fuera de su alcance.

- h) Mantener en secreto cuando por mantenimiento programado preventivo, acuda personal asignado o aprobado para estos fines.
- i) Todos los equipos TIC adquiridos para la Diris Lima Centro son administrados por la Oficina de Tecnologías de la Información, el cual dispone de su usuario o ubicación de acuerdo con el criterio de necesidades existentes.
- j) Queda estrictamente prohibido a los usuarios de equipos de cómputo y responsables de dependencias lo siguiente:
 - a. Instalar cualquier tipo de programas, protectores de pantalla, tapices, sonidos y configuraciones externas sin autorización de la Oficina de Tecnologías de la Información.
 - b. Realizar movimiento del equipo a un distinto al asignado sin notificar a la Oficina de Tecnologías de la Información de la Diris Lima Centro.
 - c. Dejar sobre los teclados objetos extraños (grapas, clips, residuos de alimentos, etc.) así como derramar líquidos sobre ellos, pues aparte de impedir su correcto funcionamiento puede causar fallas físicas en el componente y aun en la computadora.
 - d. Participar en cualquier tipo de juegos a través de internet, así como utilizar la red para tratar o promover negocios personales.
 - e. Ejecutar herramientas y utilerías para infringir los esquemas de seguridad de los equipos y/o escaneo de contraseñas residentes en el mismo.

5.13 La Oficina de Tecnologías de la Información debe considerar en su programa anual de mantenimiento preventivo de existir el presupuesto por lo menos dos veces al año.

5.14 Los usuarios finales deberán de asegurarse de respaldar la información que consideren importante para así evitar pérdida de la misma cuando este equipo sea trasladado para mantenimiento y/o reparación.

5.15 Todos los equipos de cómputo deberán estar conectado a un estabilizador y/o ups el cual regulará el voltaje, cuidando al hardware de picos de energía eléctrica esto evitara el malogro o deterioro de los mismos.

5.16 El equipo de cómputo o cualquier recurso informático que sufra de algún daño por maltrato, descuido o negligencia por parte del usuario que resguarda el equipo, se informará mediante un reporte el incumplimiento de las políticas de seguridad.

6 RESPONSABILIDAD

La Oficina de Tecnologías de la Información, será el responsable de asegurar la capacitación del personal para el cumplimiento del plan de mantenimiento y realizar el seguimiento estratégico de implementación de este plan.

7 PLAN DE MANTENIMIENTO

Para la realización de plan de mantenimiento de los equipos tecnológicos de la Oficina de Tecnologías de la Información, se darán de los siguientes:

Dirección: Av. Nicolás de Piérola N.º 617-623, Cercado de Lima –Perú
Telf. (511) 207-5700 Anexo:1507



PERÚ

Ministerio de Salud

Viceministerio de Prestaciones y Aseguramiento en Salud

Dirección de Redes Integradas de Salud Lima Centro

Los tipos de mantenimiento que se brinda desde la Oficina de Tecnologías de la Información son:

Correctivo: se realiza de manera forzosa e imprevista cuando ocurre un fallo y que impone la necesidad de reparar el equipo antes de poder continuar haciendo uso de él. El mantenimiento correctivo implica que la reparación se lleve a cabo con la mayor rapidez para evitar pérdida de tiempo en el trabajo diario que realiza el usuario de la institución.

Preventivo: Se realiza con anticipación y de manera programada con el fin de evitar desperfectos, el mantenimiento preventivo consiste en dar limpieza general al equipo de computo y verificar el correcto funcionamiento, en el caso de las computadoras el mantenimiento se puede dividir en equipo físico (hardware) y el software (lógico).

7.1 Cronogramas de Mantenimiento

Se presenta el cronograma de mantenimiento preventivo para los equipos informativos de la Oficina de Tecnologías de la Información.

ACTIVIDAD	PERIODICIDAD
MANTENIMIENTO PREVENTIVO Y CORRECTIVO DE EQUIPOS DE COMPUTO	SEMESTRE
MANTENIMIENTO PREVENTIVO, CORRECTIVO DE DATA CENTER-SERVIDORES	SEMESTRE
MANTENIMIENTO PREVENTIVO, CORRECTIVO DE SERVIDORES VIRTUALES	TRIMESTRE
MANTENIMIENTO PREVENTIVO, CORRECTIVO DEL AIRE ACONDICIONADO	ANUAL

7.2 Seguimiento y Monitoreo

El cronograma de mantenimiento se ejecutará en el lugar de trabajo y se acordará con el usuario la realización del mismo para no afectar las actividades diarias de los usuarios.

El técnico reportara al Coord. de la Unidad funcional de soporte Técnico de la Oficina de Tecnologías de la Información el respectivo informe correspondiente al mantenimiento para después realizar acciones que permitan mejorar el plan de acción.

7.3 Riesgos

Los riesgos que se pueden presentar en la ejecución del plan de mantenimiento son:


- Falta de repuestos para el cambio durante el mantenimiento.
- Disponibilidad de recursos humanos para la realización del mantenimiento.
- Incumplimiento en los tiempos de repuestas.
- Sucesos imprevistos ajenos a la entidad, ejemplo: fuerza mayor o caso fortuito.
- Reporte a destiempo de las fallas por parte de los usuarios.

Dirección: Av. Nicolás de Piérola N.º 617-623, Cercado de Lima
Telf. (511) 207-5700 Anexo:1507



PERÚ Ministerio de Salud Dirección de Redes Integradas de Salud Lima Centro
Ing. PAOLA JESÚS LLAVE ESCOBEDO
Jefa de la Oficina de Tecnología de la Información
DIRIS Lima Centro

Anexo 7. Acta de Constitución de Proyecto


	FORMATO	Versión: 1
	Acta de Constitución del Proyecto	DIRIS-220310
		FECHA EDICIÓN 10-03-2022

MINISTERIO DE SALUD

Dirección de Redes Integradas de Salud Lima Centro

ACTA DE CONSTITUCION DE PROYECTO

**DISEÑO DE UNA RED PRIVADA VIRTUAL VPN BASADO EN
SOFTWARE LIBRE PARA LA DIRECION DE REDES INTEGRADAS DE
SALUD LIMA CENTRO**

	FORMATO	Versión: 1
	Acta de Constitución del Proyecto	DIRIS-220310
		FECHA EDICIÓN 10-03-2022

1. INFORMACION GENERAL DEL PROYECTO

Nombre del proyecto:	Diseño de una red privada virtual (VPN) basada en software libre para la mejora de la seguridad de la información de la jurisdicción de la dirección de redes integradas de salud Lima Centro
Patrocinadores:	Lazarte Tirapo Daniel – Silva Buitron Giancarlos
Gerente:	Ing. Paola Llave Escobedo

2. DESCRIPCION DEL PROYECTO


Con este proyecto de diseño de una red privada virtual (VPN) se busca el brindar una mayor seguridad e integración a la red interna de la DIRIS Lima Centro ya que la conexión que se tienen con los centros de salud de su jurisdicción en los distintos distritos actualmente no es eficiente ya que son islas las cuales se encuentran desprotegidas y expuestas a cualquier tipo de ataque provocando fallos y problemas en la atención principal que es la salud.

3. OBJETIVOS

- **OBJETIVO GENERAL:** Determinar la influencia de una red privada virtual bajo software libre en la seguridad de la información entre sus locales de su jurisdicción.
- **OBJETIVOS ESPECIFICOS:** los objetivos específicos van al medir el nivel de seguridad, confiabilidad y escalabilidad que nos brinda el diseño de la red privada virtual basado bajo software libre.

4. JUSTIFICACION

La justificación de este proyecto son realizar un diseño de una VPN con software libre las cuales nos permite ser versátil para la instalación como para el despliegue en los diferentes centros de salud, para ello no hay un impacto mayor con respecto a hardware para el desarrollo de la implementación.

 <p>PERÚ Ministerio de Salud Dirección de Redes Integradas de Salud Lima</p>	FORMATO	Versión: 1
	Acta de Constitución del Proyecto	DIRIS-220310
		FECHA EDICIÓN 10-03-2022

5. ALCANCES


Los alcances de este proyecto es la del diseño de una red (VPN) se realizaron todos los estudios de acuerdo a la información brindada y ajustando el diseño en base al software libre, en este punto es muy importante el costo considerado para la implementación ya que puede proseguir en una implementación.

6. ENTREGABLES

Entregables del alcance del producto		
No.	Fase	Entregable
1.	Análisis de Requerimiento	•
2.	Desarrollar diseño lógico	•
3.	Desarrollar diseño físico	•
4.	Probar, optimizar y documentar diseño	•

7. CRONOGRAMA

		cronograma de actividades											
Fases	Procesos	enero				febrero				marzo			
		SEMANA 1	SEMANA 2	SEMANA 3	SEMANA 4	SEMANA 1	SEMANA 2	SEMANA 3	SEMANA 4	SEMANA 1	SEMANA 2	SEMANA 3	SEMANA 4
1 Analizar Requerimientos	Análisis de metas del negocio												
	Análisis de metas técnicas												
	Análisis de red existente												
	Análisis de tráfico existente												
2 Desarrollar Diseño Lógico	Diseñar topología de red												
	Diseñar modelos de direccionamiento + hostnames												
	Seleccionar protocolos para Switching y Routing												
	Desarrollar estrategias de seguridad												
3 Desarrollar Diseño Físico	Desarrollar estrategias de administración de red												
	Seleccionar tecnologías y dispositivos para redes de campus												
	Seleccionar tecnologías y dispositivos para redes empresariales												
	Probar el diseño de red												
4 Probar, optimizar y documentar diseño	Optimizar el diseño de red												
	Documentar el diseño												

	FORMATO	Versión: 1
	Acta de Constitución del Proyecto	DIRIS-220310
		FECHA EDICIÓN 10-03-2022

8. PRESUPUESTO

Unidad	Descripción	Costo promedio
1	Computadora	S/.900.00
1	Tarjeta de Red	S/.80.00
	Total	S/.980.00

El presupuesto para la presente implementación es por establecimiento de salud.

9. RESTRICCIONES


Los permisos a las locaciones son importantes para la implementación y configuración del hardware y software.

10. RIESGOS DEL PROYECTO


Una restricción podría ser el presupuesto, ya que al considerar el presupuesto para el sector salud este se hace de manera anual y de no contar con ello afectaría el desarrollo del mismo.

11. ACEPTACION Y FIRMAS

<p>Patrocinador del proyecto</p>    <p> Ing. PAOLA LLAVE ESCOBEDO <small>Jefa de la Oficina de Tecnologías de la Información</small> DIRIS Lima Centro </p> <p>Nombre completo: Llave Escobedo Paola</p> <p>Cargo – Dependencia: Jefa de la Oficina de Tecnologías de la Información</p>
--

 <p>PERÚ Ministerio de Salud Dirección de Redes Integradas de Salud Lima</p>	FORMATO	Versión: 1
	Acta de Constitución del Proyecto	DIRIS-220310
		FECHA EDICIÓN 10-03-2022

<p>Correo : pllave@dirislimacentro.gob.pe Teléfono: 205-5700 anexo 1503</p>	
Patrocinador del proyecto	
 <hr/> <p>Nombre completo: Lazarte Tirapo Daniel Cargo – Dependencia Correo : daniel.lt1@hotmail.com Teléfono: 991473742</p>	
Patrocinador del proyecto	
 <hr/> <p>Nombre completo: Silva Buitron Giancarlos Cargo – Dependencia Correo : gian33@hotmail.com Teléfono: 962634024</p>	
Gerente del proyecto	
<hr/>	

 PERÚ Ministerio de Salud Dirección de Redes Integradas de Salud Lima	FORMATO	Versión: 1
	Acta de Constitución del Proyecto	DIRIS-220310
		FECHA EDICIÓN 10-03-2022

MINISTERIO DE SALUD
 DIRECCIÓN DE REDES INTEGRADAS DE SALUD - LIMA CENTRO
 OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN
 REGION DE TRABAJO: REDES Y TELECOMUNICACIONES

Téc. Juan Alberto Vega Guaniño
 Nombre completo: Juan Vega Guaniño

Cargo – Dependencia: Coord. Unidad Funcional de Telecomunicaciones

Correo : jvega@dirislimacentro.gob.pe

Teléfono: 207-5700 anexo 1513

Anexo 7. Estándares para la adquisición de tecnología y dispositivos



PERÚ

Ministerio
de Salud

Vicerrectoría
de Promoción y
Asesoramiento en Salud

Dirección de Redes
Integradas de Salud
Lima Centro

ESTANDARES PARA LA ADQUISICION DE TECNOLOGIA Y DISPOSITIVOS

**DIRECCIÓN DE REDES INTEGRADAS DE SALUD LIMA
CENTRO**

OFICINA DE TECNOLOGIAS DE LA INFORMACIÓN

Dirección: Av. Nicolás de Piérola N.º 617-623, Cercado de Lima –Perú.
Telf. (511) 207-5200 Anexo 1507



PERÚ

Ministerio
de Salud

Viceministerio
de Prestaciones y
Aseguramiento en Salud

Dirección de Redes
Integradas de Salud
Lima Centro

Tabla de Contenido

1. INTRODUCCIÓN
2. DESCRIPCIÓN
3. OBJETIVO
 - 3.1. Objetivo General
 - 3.2. Objetivo Específicos
4. ALCANCE
5. RESPONSABILIDADES
6. DIRECTRICES
7. POLÍTICAS Y NORMAS DE INFORMATICA
8. DISPOSICIONES GENERALES
9. ORGANIZACIÓN
10. ESTANDARES INFORMATICOS
 - 10.1. ESTANDARES PARA LA ADQUISICION DE EQUIPOS DE COMPUTO Y SERVICIOS
 - 10.1.1. DIMENSIONAMIENTO DE LAS CARACTERISTICAS TECNICAS DE LOS EQUIPOS
 - 10.1.2. ESTANDARES PARA LA ADQUISICION DE PARA EQUIPOS DE COMPUTO
 - 10.1.3. CONSIDERACIONES PARA LA ADQUISICION DE EQUIPOS DE COMPUTO O SERVICIOS
 - 10.2. ESTANDARES PARA REDES
 - 10.2.1. ESTANDARES PARA ARQUITECTURA DE REDES Y COMUNICACIONES
 - 10.3. ESTANDARES PARA GESTION DE CALIDAD
 - 10.3.1. FUDAMENTO
 - 10.3.2. PATRON
 - 10.4. ESTANDARES PARA GESTION DE ADQUISICION TECNOLOGICA





PERÚ

Ministerio
de Salud

Viceministerio
de Prestaciones y
Aseguramiento en Salud

Dirección de Redes
Integradas de Salud
Lima Centro

1. INTRODUCCIÓN

El presente manual es brindar una metodología de procesos unificado, esto ayudara para la coordinación de las futuras adquisiciones de equipos tecnologicos.

Este instrumento regula la presente metodología aplicada a los procesos de adquisición de tecnología informática para la institución, esto representa un marco de referencia técnico el cual permitirá la integración homogeneidad de los procesos operativos soportados por las tecnologías de la información, de esta forma permitiría orientar a las unidades de trabajo en la planificación en el desarrollo de los procesos.

2. DESCRIPCIÓN

Los estándares informáticos presentados en el presente manual, es generar un conjunto de especificaciones técnicas, los cuales logren unificar la adquisición tecnológica, se entenderá por estandarización informática es aquel, un parametro o patron permite uniformidad en características de equipos el cual garantizara la integridad y compatibilidad en los procesos tecnologicos de la institución.

3. OBJETIVO

3.1. Objetivo General

Proporcionar a las diferentes entidades y dependencias, políticas y lineamientos en torno al desarrollo, control de los procesos informáticos; esto mejorara los niveles de uniformidad, calidad, comunicaciones y coordinación con los procedimientos de la institución.

3.2. Objetivo Especifico

- Definir estándares en relación a los procesos, herramientas, equipos, software, comunicaciones involucradas en procesos informáticos, esto con el fin de lograr la homogeneidad en el desarrollo tecnológico de la institución.
- Impulsar un desarrollo informático el cual será sustentado en los lineamientos establecidos, esto para impulsar un avance continuo para un crecimiento ordenado y estratégico.



4. ALCANCE

El presente manual define estándares basados en el aprovisionamiento de recursos tecnológicos, administración de infraestructura de la tecnología y presentación de servicios informáticos.

5. RESPONSABILIDADES

La Oficina de Tecnologías de la Información es la responsable de dar a conocer los estándares, políticas del presente manual.



PERÚ

Ministerio
de Salud

Viceministerio
de Prestaciones y
Aseguramiento en Salud

Dirección de Redes
Integradas de Salud
Lima Centro

6. DIRECTRICES

Los funcionarios de la Dirección de Redes Integradas de Salud Lima Centro, en su totalidad, la responsabilidad de acatar las disposiciones en el presente manual.

7. POLITICAS Y NORMAS DE INFORMATICA

El presente manual contiene lineamientos los cuales deben ser considerados por las dependencias de la institución y sus trabajadores, con el fin de cumplir políticas informáticas las cuales fortalecerán el desarrollo de los procesos institucionales.

La aplicación del manual de políticas es necesaria y obligatoria en las direcciones, oficinas y establecimientos de salud, dado que su aplicación será atinente a todas las labores cotidianas, utilización y adquisición de equipos de computo hardware entre otros aspectos relacionados con las tecnologías de la información.

8. DISPOSICIONES GENERALES

La Oficina de Tecnologías de la Información con el apoyo de las direcciones y/o oficinas en el presente proceso son encargados de:

- Definir las políticas, estrategias en materias de informática.
- Establecer el modelo general en el uso de las tecnologías de información, llamado arquitectura tecnológica y de sistemas de información, esto promoverá la implementación y consolidación en forma planificada, esto logrará la modernización y el mejoramiento de la calidad en los servicios y procesos informáticos.
- El fortalecimiento de las direcciones y/o oficinas mediante la dotación de equipos, el diseño e implementación de sistemas de información y la comunicación adecuada para agilizar el servicio a los usuarios y el flujo de información.
- Para la adquisición de tecnologías de la información existen procedimiento de contrataciones, los cuales nos ayudan a seguir los pasos para una adecuada adjudicación, teniendo en cuenta el manual de estándares para el desarrollo de un proyecto.



9. ORGANIZACIÓN

La Dirección de Redes Integradas de Salud Lima Centro realiza el uso de las tecnologías de la información como medidas de apoyo para desarrollar sus objetivos institucionales, es por esto que las TIC son realmente eficientes y necesarias para poder realizar adecuadamente los procesos y/o necesidad en tiempos razonables y adecuados.

La Oficina de Tecnologías de la Información se presenta de la siguiente manera:

Dirección: Av. Nicolás de Piérola N.º 617-623, Cercado de Lima - Perú
Telf. (511) 207-5700 Anexo:1507



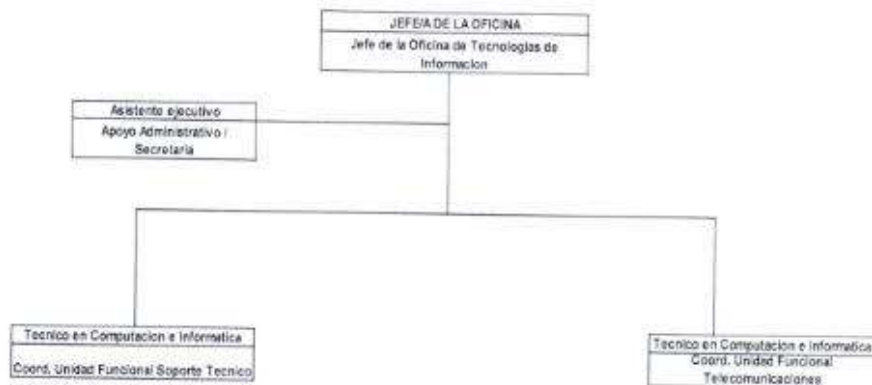
PERÚ

Ministerio de Salud

Viceministerio de Prestaciones y Aseguramiento en Salud

Dirección de Redes Integradas de Salud Lima Centro

ORGANIGRAMA FUNCIONAL DE LA OFICINA DE TECNOLOGÍAS DE INFORMACION



10. ESTANDARES INFORMATICOS

10.1. ESTANDARES PARA LA ADQUISICION DE EQUIPOS DE COMPUTO Y SERVICIOS
EL objeto de los estándares para la adquisición de cómputo, sea por modalidad de adquisición y/o alquiler, tienen como objetivos que estas propuestas sean diseñadas para el mejoramiento de los servicios informáticos.

10.2. DIMENSIONAMIENTO DE LAS CARACTERISTICAS TECNICAS DE LOS EQUIPOS
Al requerir equipos de cómputo estos pueden ser alquilados y/o comprados, necesitamos saber las necesidades que tenemos para así requerir técnicamente el equipo adecuado, se presenta una lista de consideraciones según la necesidad:

10.2.1. Generalidades: son aspectos básicos para cualquier tipo de equipo:

10.2.1.1. Propósito del equipo: antes de iniciar con el la necesidad del equipo teniendo en cuenta el hardware (según la necesidad de trabajo), se deberá establecer claramente el propósito de la adquisición, deberá de sustentarse la necesidad para la adquisición de este equipo para así presupuestarlo.





- 10.2.1.2.** Entorno de Operación: se deberá verificar el lugar de ubicación e instalación del equipo por adquirir, deberán evaluarse aspectos como temperatura, espacio físico, seguridad, etc., todo esto con el propósito de realizar un análisis del entorno y determinar las mejores opciones para la instalación del equipo.
- 10.2.1.3.** Capacitación: Cuando se adquiera equipo con características tecnológicas de última generación, deberá capacitarse al personal y/o responsable de la gestión de estos equipos, esto con el fin de realizar una administración adecuada.
- 10.2.1.4.** Garantías: Para cualquier tipo de adquisición, estos equipos deberán tener una garantía prudente según evaluado por el área técnica, la cual deberá contemplar el hardware del CPU ante cualquier inconveniente.
- 10.2.1.5. Ata disponibilidad:** Los equipos de cómputo destinado a soportar procesos críticos, que administren o resguarden información de alta importancia, estos deberán contar con las condiciones que garanticen alta disponibilidad y tolerancia a fallos, contemplando desde su entorno de operación, estos deberán tener redundancia propias atinentes a la arquitectura del equipo (redundancia en fuente de poder, discos duros, controladoras, etc.), deberán establecer mecanismos los cuales agilicen la resolución de incidencias.
- 10.2.1.6. Estación de Trabajo:** al adquirir las estaciones de trabajo deberán considerarse los siguientes aspectos:
- 10.2.1.6.1.** Orientación técnica: deberá de definirse claramente para que sector profesional será adquirido el equipo lo cual permitirá realizarlas las características técnicas adecuadas.
- 10.2.1.6.2.** Licenciamiento: estos tipos de software (sistema operativo) y software producción (aplicaciones específicas), estos serán analizando los hardware adecuados para su desempeño.
- 10.2.1.6.3.** Especificaciones técnicas: se determinará la orientación técnica del equipo, para lo cual las características técnicas serán de acuerdo al uso de oficina considerando lo siguiente:
- Procesador
 - Memoria
 - Almacenamiento
 - Red
 - Estructura del equipo (case)
 - Periféricos





PERÚ

Ministerio
de Salud

Viceministerio
de Prestaciones y
Aseguramiento en Salud

Dirección de Redes
Integradas de Salud
Lima Centro

10.2.1.7. Computadoras Portátiles: si requieren equipos portátiles deberá ser de las siguientes características:

- 10.2.1.7.1.** Orientación Técnica: debe definirse el tipo de usuario que utilizara este portátil para tener en cuenta sus características técnicas.
- 10.2.1.7.2.** Licenciamiento: serán adquiridos en la portátil.
- 10.2.1.7.3.** Especificaciones técnicas mínimas: una vez verificado la necesidad del usuario final.

10.2.1.8. Impresoras: al adquirirse impresoras deben de consideras lo siguiente:

- a) Orientación técnica: definir claramente para que el sector profesional que esta adquiriendo los equipos.
- b) Funcionalidades: con características mínimas, funcionales las cuales seran definidas por el usuario final.
- c) Licenciamiento: Análisis de los requerimientos de licenciamiento para la utilizacion de las funcionalidades requeridas.
- d) Especificaciones: Una vez tenida la orientacion tecnica del equipo, deberan de indicar sus funciones que tengan para las ncesidades del usuario final.
 - a) Tipo
 - b) Modalidades de impresión
 - c) Cartuchos
 - d) Resolución
 - e) Bandejas
 - f) Tipo de papel
 - g) Memoria
 - h) Red
 - i) Almacenamiento

10.2.1.9. Servidores: las siguiente características tienen que ser contempladas para la adquisición de un servidor.

- a) Proceso a soportar: deben definirse los requerimientos del servicio a soportar estimado de transacciones, estimado de conexiones, entorno de operación, para tener esta información deberán estar involucrados el área técnica.
- b) Licenciamiento: tipo de software y/o producción, previo análisis de los requerimiento de hardware.
- c) Redundancia: verificar las características de alta disponibilidad del equipo, analizando sus componentes de hardware para así tener una mejor tolerancia a fallas.
- d) Escalabilidad: contemplar la capacidad de escalabilidad del equipo, para realizar actualizaciones de su hardware.





PERÚ

Ministerio
de Salud

Ministerio
de Prestaciones y
Aseguramiento en Salud

Dirección de Redes
Integradas de Salud
Lima Centro

- e) Especificaciones técnicas mínimas a considerar: una vez determinadas las especificaciones técnicas del equipo, deberán considerar los siguientes aspectos:
- a) Procesador
 - b) Memoria
 - c) Almacenamiento
 - d) Unidades de Respaldo
 - e) Red
 - f) Estructura del equipo
 - g) Periféricos
 - h) Características

10.2.2. Equipo de Telecomunicaciones: estos aspectos deberán ser considerador para la adquisición de equipos para red:

10.2.2.1. Servicios de red a soportar: deben definirse los requerimientos de los servicios a soportar, en función del ancho de banda, tráfico, seguridad, eficiencia en administración y confiabilidad.

10.2.2.2. Determinación del tipo de equipo: considerar los requerimientos, características, compatibilidad para selección de dispositivos de recomo: enrutadores, switch, firewall, access point entre otros.

10.2.2.3. Integridad de la plataforma: se mantendrá la integridad en los componentes o equipos a adquirir, en relación con la plataforma existente, esto facilitará la interacción con un mismo sistema operativo.

10.2.2.4. Redundancia: determinar características de alta disponibilidad de equipo, analizar características técnicas lo cual permitira una tolerancia ante fallas.

10.2.2.5. Escalabilidad: verificar la capacidad de escalabilidad del equipo.

10.2.2.6. Especificaciones Técnicas mínimas: realiza la orientación técnica del equipo, deberán considerarse los componentes primarios.

- a) Capacidad de procesamiento de paquetes
- b) Memoria, tipo y velocidad
- c) Componentes
- d) Estructura del equipo
- e) Características del equipo
- f) Software

10.2.3. Infraestructura para telecomunicaciones: esto deberá de verificarse por medios físicos de transmisión de datos, así como otros componentes y accesorios de red necesarios para correcta operación de la red de datos, estas son:

10.2.3.1. Topología de red: determinación y diseño de la topología de red que presenta la solución según los requerimiento y servicios de red necesarios.

10.2.3.2. Cable TUP y fibra óptica: tipo de cable y su categoría siguiendo las normas de cableado estructurado establecidas por la IEE.

10.2.3.3. Gabinetes de pared o rack: tamaño y tipo de gabinete, con sus respectivos accesorios de red como organizadores, regletas, ups, etc:





PERÚ

Ministerio
de Salud

Viceministerio
de Prestaciones y
Aseguramiento en Salud


Dirección de Redes
Integradas de Salud
Lima Centro

- 10.2.3.4. Instalación eléctrica:** indicar el estado de la instalación eléctrica, la cual tiene que cumplir con las normas respectivas.
- 10.2.3.5. Conectores de Red:** tipo de conectores y elementos de red para la determinación de la mejor configuración de red.



Dirección: Av. Nicolás de Piérola N.º 617-623, Cercado de Lima (Perú)
Telf: (511) 207-9700 Anexo:1507

Anexo 8. Matriz de validación del instrumento

MATRIZ DE VALIDACIÓN DEL INSTRUMENTO								
Título de la tesis: Diseño de una red privada virtual (VPN) basada en software libre para la mejora de la seguridad de la información de la jurisdicción de la dirección de redes integradas de salud Lima Centro								
Apellidos y Nombres de los Investigadores: LAZARTE TIRAPO DANIEL , SILVA BUITRON GIANCARLOS								
Apellidos y Nombres del Experto:								
ASPECTO POR EVALUAR								
VARIABLES	DIMENSIONES	INDICADORES	PREGUNTA	ESCALA	De acuerdo	Desacuerdo	OBSERVACIONES	
Seguridad de la información	Confiabilidad	Tiempo Promedio de Fallas (TPDF)	El tiempo promedio de falla es menor al horario laboral de la institucion	Variable cualitativa ordinal Escala e intervalaos tipo dicotomías, De Acuerdo y En Desacuerdo	<input checked="" type="checkbox"/>			
			el tiempo promedio de respuesta ante fallas es menor a 15minutos					
		Tiempo Promedio para Reparar (TPDR)	El tiempo promedio para reparar es menor a 1 hora		<input checked="" type="checkbox"/>			
	Integridad	confiabilidad de la informacion			Lo problemas de mayor complejidad son reparados rapidamente	<input checked="" type="checkbox"/>		
					la informacion que se enviara por la VPN es confiable			
					la interconexion de la VPN mostrara la informacion en tiempo real			
	Disponibilidad	completitud de la informacion			las porliticas de seguridad a travez de la VPN brindan confiabilidad	<input checked="" type="checkbox"/>		
					la informacion que se transmite por la VPN es integra			
					la conectividad por VPN nos garantiza la confiabilidad de la informacon	<input checked="" type="checkbox"/>		
		horas totales de disponibilidad			el diseño de seguridad a travez de la VPN se encuentra disponible en el horario laboral	<input checked="" type="checkbox"/>		
					existe alta disponibilidad en la conexión VPN	<input checked="" type="checkbox"/>		
					las políticas de seguridad se replican mediante la VPN los 365 días del año	<input checked="" type="checkbox"/>		
			los mantenimientos se encuentra progarmados en fechas y horas no laborales					
	horas paradas por mantenimiento		los mantenimientos no superan las 2 horas de corte de la VPN					
			los trabajos de mantenimiento son informados adecuadamente					
								
FIRMA DEL EXPERTO				FECHA: <input type="text" value="."/>				