UNIVERSIDAD NACIONAL "HERMILIO VALDIZÁN"

FACULTAD DE INGENIERÍA INDUSTRIAL Y DE SISTEMAS

ESCUELA ACADÉMICO PROFESIONAL DE INGENIERÍA DE SISTEMAS

PROGRAMA DE CAPACITACIÓN Y TITULACIÓN PROFESIONAL

IMPLEMENTACIÓN DE UN SOPORTE INFORMÁTICO REMOTO PARA PERSONAL DEL MINISTERIO PÚBLICO – DISTRITO FISCAL DE HUÁNUCO - 2017

TESIS PARA OPTAR EL TÍTULO DE INGENIERO DE SISTEMAS

TESISTA: **Bach. Jhordy Andoni MELGAREJO CHAUPIS.**

ASESOR: **Mg. Luis Andres MEZA ORDOÑES.**

HUÁNUCO – PERÚ

2017

DEDICATORIA

Este trabajo está dedicado a las personas que a lo largo de mi vida me han dado la formación de ser una persona cada día mejor. Se la dedico a mis padres y a mi hermana, que son las personas que me motivaron, me aconsejaron y me apoyaron siempre, en cada momento, y que cada día me alientan a seguir adelante.

El autor.

AGRADECIMIENTO

Los agradecimientos están dirigidos a todas las personas y a la entidad que hicieron posible la realización exitosa de esta investigación, principalmente agradecemos a nuestros padres y hermanas por el apoyo y motivación entregada.

El autor.

RESUMEN

La Tesis denominada “IMPLEMENTACIÓN DE UN SOPORTE INFORMÁTICO REMOTO PARA EL PERSONAL DEL MINISTERIO PÚBLICO – DISTRITO FISCAL DE HUÁNUCO - 2017”, tuvo como objetivo implementar un software libre que permite ver el escritorio de una maquina remota y controlarlo con ratón y teclado, mejorando la efectividad de la oficina de tecnologías de información en la solución de incidencias de soporte informático, con las ventajas de ahorro de tiempo y costo.

La investigación que se realizó fue de tipo aplicada o tecnológica, y el diseño que se ajustó a la investigación fue el diseño experimental, y tipo de diseño experimental utilizado fue experimental pura con diseño de dos grupos aleatorizados con preprueba y postprueba.

La aceptación del soporte informático por parte del personal del Ministerio Público – Distrito Fiscal Huánuco fue al 98% y el tiempo de solución de incidencias de soporte informático se disminuyó a un 95%.

Palabras clave: remoto, efectividad, soporte informático.

SUMMARY

The thesis entitled "IMPLEMENTATION OF A REMOTE COMPUTER SUPPORT FOR PUBLIC MINISTRY STAFF - HUÁNUCO FISCAL DISTRICT - 2017", aimed to implement a free software that allows to view the desktop of a remote machine and control it with mouse and keyboard, improving the effectiveness of the office of information technologies in the solution of incidences of computer support, with the advantages of saving time and cost.

The research carried out was applied or technological, y the design that fit the research was experimental design, and experimental design type was pure experimental design with two groups randomized with pre-test and post-test.

The acceptance of the computer support by the staff of the Public Ministry - Fiscal District Huánuco was 98% and the time of solution of incidences of computer support was reduced to 95%.

Key words: remote, effectiveness, computer support.

INTRODUCCIÓN

El presente trabajo tiene como objetivo proponer la implementación de soporte informático remoto, para para mejorar la efectividad de atención al personal del Ministerio Público - Distrito Fiscal Huánuco. Este proyecto permitirá a los ingenieros de la Oficina de Tecnologías de Información pueda ayudar de manera remota a los usuarios que están dentro de su MAN, VLAN y LAN disminuyendo los tiempos de respuesta a los incidentes, así mismo permitirá solucionar problemáticas que no sean tan complejas de una manera más rápida y simple.

La comunicación entre la aplicación cliente y la aplicación servidor se puede realizar sobre cualquier plataforma de redes de comunicaciones TCP/IP y la calidad del video en la aplicación cliente puede mejorar a medida que mejore la tecnología utilizada en las redes de datos. La solución tecnológica propuesta cubrirá con los siguientes ítems:

- Soporte informático remoto para el personal.
- La herramienta permitirá administrar las conexiones en grupos, departamento, piso, obteniendo un organigrama de las conexiones de manera central y facilitando la búsqueda de conexiones.
- Esta implementación por ser multiplataforma permitirá realizar conexiones a sistemas operativos Windows y Linux.
- Capacitar a los ingenieros de soporte técnico acerca de la instalación y uso de la herramienta planteada.

- Solucionar incidencias que genera los sistemas que hacen uso el Ministerio Público Fiscalía – Distrito Fiscal de Huánuco.

El trabajo de investigación está desarrollado en los siguientes capítulos, a continuación, el resumen de cada uno:

CAPITULO I: PROBLEMA DE INVESTIGACIÓN, se presenta todo el aspecto concerniente, como descripción del problema (ubicación, conflictos, etc.), formulación del problema, objetivos, hipótesis, variables, justificación, viabilidad y limitaciones.

CAPITULO II: MARCO TEÓRICO, aquí se describen los antecedentes de investigación, bases teóricas y definiciones conceptuales. También en este capítulo se realiza la descripción de la institución donde se ha realizado el desarrollo de la implementación, datos generales, estructura organizacional, entre otros.

CAPITULO III: METODOLOÍA DE INVESTIGACIÓN, se determina el tipo de investigación, población y muestra, técnicas e instrumentos de la recolección de datos, como las técnicas para el procesamiento de datos.

CAPITULO IV: IMPLEMENTACIÓN, este capítulo incluye toda la etapa de implementación del software de acceso remoto. Se dividen en fases: Manual técnico, manual de usuario y políticas de seguridad.

ÍNDICE.

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

I. PROBLEMA DE INVESTIGACIÓN

1.1. DESCRIPCIÓN DEL PROBLEMA.

1.1.1. Ubicación del problema en un contexto.

El Ministerio Público – Distrito Fiscal de Huánuco (MP-DFHCO), está conformado por las provincias de Huánuco, Leoncio Prado, Dos de Mayo, Huamalíes, Pachitea, Lauricocha, Yarowilca y Ambo; MP-DFHCO organismo constitucionalmente autónomo, defensor de la legalidad y los Derechos Humanos, a nivel del Distrito Fiscal de Huánuco se enmarca dentro de los preceptos y lineamientos generales de nuestra mística institución, ofrece servicios a disposición de la ciudadanía en ocho provincias del departamento (Fiscalías Penales, Fiscalías de Civil y Familia, Fiscalías Especializadas, División Médico Legal, Unidad Distrital de Atención a Víctimas y Testigos y Servicio de Administración).

La Oficina de Tecnologías de Información (OTI) está encargada de realizar diferentes actividades para mantener el funcionamiento de todos los sistemas que hace uso el MP-DFHCO en las 8 provincias mencionadas. En la actualidad la OTI no tiene un sistema de soporte remoto, debido a la falta de esta herramienta afecta de cierta manera las actividades de los ingenieros (especialistas administrativos) de la Oficina de Tecnologías de Información.

Los principales inconvenientes se dan al momento de brindar un el servicio de soporte informático al personal (jurídico y administrativo), ya que los

ingenieros deben desplazarse hacia el lugar de incidencia, esto ocasiona que se genere gastos por motivo de movilización y a su vez generando insatisfacción con el personal que reporta la incidencia, debido a la demora en resolver la incidencia.

1.1.2. Situación conflictos nudos críticos.

El Ministerio Publico consta de 8 provincias interconectadas por enlaces de datos e internet, en cada provincia hay una cantidad de personal jurídico y administrativo, a los cuales se les brinda soporte técnico.

El problema se da cuando sucede algún incidente en los equipos de cómputo del personal, por tanto, se requiere brindar servicio de soporte informático, que en varios de los casos se pierde mucho tiempo en trasladarse desde la Oficina de Tecnologías de Información hasta el personal que está reportando la incidencia y esto ocasiona pérdida de tiempo y de recursos humanos.

La implementación de una herramienta de soporte remoto, permitirá ofrecer a la Oficina de Tecnologías de Información, la comodidad de solucionar incidencias, inconvenientes y problemas que no tienen mayor dificultad que se puedan resolver vía conexión remota, así ahorramos tiempo y recursos que se puedan distribuir en otras actividades.

1.1.3. Síntomas, Causas, Pronóstico y Control de Pronostico.

Síntomas:

- Demora de atención de Soporte informático al personal jurídico y administrativo del Ministerio Público – Distrito Fiscal de Huánuco.
- Insatisfacción del personal jurídico y administrativo por el servicio de soporte informático de la Oficina de Tecnologías de Información.
- Estrés laboral en el personal de la Oficina de Tecnologías de Información.
- Fallos en los sistemas que hacen uso el Ministerio Público – Distrito Fiscal de Huánuco

Causas:

- La realización del Soporte informático al personal jurídico y administrativo se realiza de forma presencial.
- La Oficina de tecnologías de la Información no cuenta con el número de personal adecuado para el Distrito Fiscal de Huánuco.
- No existe una herramienta que ayude a solucionar incidencias de menor dificultad.

Pronostico:

- Si la Oficina de Tecnologías de Información sigue con el método tradicional de Soporte al personal jurídico y administrativo, generara insatisfacción en todo el personal del Ministerio Publico – Distrito Fiscal Huánuco.

Control del pronóstico:

- Con la implementación de un soporte informático remoto se mejora a efectividad de la Oficina de Tecnologías de Información en brindar el servicio de soporte técnico.

1.2. DELIMITACIÓN DEL PROBLEMA.

La herramienta de soporte remoto estará destinada para fortalecer de manera eficaz y rápida la ayuda al personal jurídico y administrativo, lo cual estará dirigida específicamente a los ingenieros de la Oficina de Tecnologías de Información. Esta propuesta dará asistencia al personal a través de escritorio remoto, un software libre basado en una arquitectura Cliente-Servidor, el cual consiste en tomar el control del ordenador servidor remotamente a través de un ordenador cliente.

Tabla 1. Delimitación de la investigación

Campo:	Legalidad del derecho
Aspecto:	Software libre que permite a los administradores de sistema dar soporte de manera remoto a los usuarios.
Tema:	IMPLEMENTACIÓN DE UN SOPORTE INFORMÁTICO REMOTO PARA PERSONAL DEL MINISTERIO PÚBLICO – DISTRITO FISCAL DE HUÁNUCO – 2017
Geográfica:	El Ministerio Publico - Distrito Fiscal Huánuco
Espacio:	2017 – 2018

Fuente: Elaboración propia.

1.3. FORMULACIÓN DEL PROBLEMA.

1.3.1. Formulación de problema general

¿De qué manera mejorará el servicio de atención de soporte informático al personal jurídico y administrativo del Ministerio Publico - Distrito Fiscal de Huánuco por parte de la Oficina de Tecnologías de Información?

1.3.2. Formulación de problemas específicos.

- ¿Cuál será la óptima herramienta de conexión remota para la implementación en la Oficina de Tecnologías de Información del Ministerio Público - Distrito Fiscal de Huánuco?
- ¿Cuál de los procesos de soporte informático al personal jurídico y administrativo se debe optimizar, por parte de la Oficina de Tecnologías de Información del Ministerio Público - Distrito Fiscal de Huánuco?
- ¿Existirá políticas de seguridad y normas necesarias para la implementación en el Ministerio Publico – Distrito Fiscal de Huánuco?

1.4. OBJETIVOS.

1.4.1. Objetivo general.

Implementar un soporte informático remoto en la Oficina de Tecnologías de Información para mejorar la efectividad de la atención de soporte al personal jurídico y administrativo del Ministerio Publico - Distrito Fiscal de Huánuco - 2017.

1.4.2. Objetivos específicos.

- Identificar el software de conexión remota óptima para la implementación en la Oficina de Tecnologías de Información del Ministerio Público - Distrito Fiscal de Huánuco.
- Identificar los procesos a optimizar de soporte informático al personal jurídico y administrativo por parte de la Oficina de Tecnologías de Información del Ministerio Público - Distrito Fiscal de Huánuco.
- Identificar las políticas de seguridad y normas necesarias para la implementación en el Ministerio Publico – Distrito Fiscal de Huánuco.

1.5. HIPÓTESIS.

1.5.1. Hipótesis general.

La implementación de un soporte informático remoto en la Oficina de Tecnologías de Información mejorara la efectividad de la atención de soporte al personal jurídico y administrativo del Ministerio Publico - Distrito Fiscal de Huánuco.

1.5.2. Hipótesis especificas

- TightVNC es el software de conexión remota óptima para la implementación en la Oficina de Tecnologías de Información del Ministerio Público - Distrito Fiscal de Huánuco.
- El causante de cuello de botella es el procedimiento de traslado para solucionar la incidencia del proceso de soporte informático al personal jurídico y administrativo, por parte de la Oficina de Tecnologías de Información del Ministerio Público - Distrito Fiscal de Huánuco.
- Existe políticas de seguridad y normas necesarias para la implementación de un software en el Ministerio Público - Distrito Fiscal de Huánuco.

1.6. VARIABLES.

1.6.1. Variable independiente.

- Soporte Informático Remoto.

1.6.2. Variable dependiente.

- Atención al personal.

1.7. OPERACIONALIZACIÓN DE VARIABLES.

Tabla 2. Operacionalización de variables

VARIABLES	DIMENSIONES	INDICADORES
	Seguridad.	Cumplimiento a las políticas de seguridad propuestas.
	Confidencialidad.	Cumplimiento con estándar propuesto.
	Productividad.	Total, de atenciones por día.
	Reducción de costos.	Ahorro de nuevos soles.

Fuente: elaboración propia.

1.8. JUSTIFICACIÓN E IMPORTANCIA.

Actualmente la Oficina de Tecnologías de Información del Ministerio Público – Distrito Fiscal de Huánuco realiza sus actividades sin tener una definición clara de sus procesos, procurando un agrupamiento por tareas. Los procesos se desarrollan rápidamente para afrontar las necesidades inmediatas de una mejor planificación de la oficina. Los sistemas de información y las tecnologías de información han cambiado la forma en que operan las organizaciones actuales. A través de su uso se logran importantes mejoras, ya que automatizan los procesos operativos, suministran una plataforma de información necesaria y lo más resaltante que logra ventajas competitivas.

El acceso remoto es una herramienta que se basa en la calidad de servicio y el desarrollo eficaz y eficiente de los procesos que cubren las actividades más importantes del soporte informático.

Razón por el cual es importante realizar un estudio para la implementación de la conexión remota mediante un software que ayude a la Oficina de Tecnologías de información basado en Acceso Remoto, optimizando el soporte informático al personal jurídico y administrativo del Ministerio Publico – Distrito Fiscal de Huánuco.

1.9. VIABILIDAD.

Recursos humanos. El presente trabajo será viable porque el personal encargado intervendrá directamente en el diseño de los procesos para la implementación de la herramienta de soporte remoto.

Recursos económicos. Se dispondrá de recursos económicos para cubrir las expectativas propuestas y obtener el resultado.

Recursos tecnológicos (materiales). Se dispone de recursos materiales (escritorio y tecnología), para el procesamiento y obtención de la información requerido para el desarrollo del presente estudio.

1.10. LIMITACIONES.

A continuación, se listan de las limitaciones en el desarrollo y concretización del presente trabajo:

- Se desarrollará en el Ministerio Público - Distrito Fiscal Huánuco.
- La investigación para el proyecto se basa a la percepción del sistema y especificaciones del coordinador de las tecnologías de Información del Ministerio Público.
- El sistema desarrollado solo funcionara dentro de instalaciones del Ministerio Público del Distrito Fiscal de Huánuco por ser una zona desmilitarizada.
- Se debe utilizar un software open source.

II. MARCO TEÓRICO.

2.1. ANTECEDENTES DE LA INVESTIGACIÓN.

- (Arboleda Orejuela, 2015), realizo una investigación: “IMPLEMENTACIÓN DE UNA HERRAMIENTA TECNOLÓGICA PARA ATENCIÓN A USUARIOS EN LA PONTIFICIA UNIVERSIDAD CATÓLICA DE ECUADOR SEDE EN ESMERALDA”

  Objetivo general: Mejorar el servicio de atención a usuarios en el departamento de TIC de la PUCESE, mediante la implementación de una herramienta tecnológica.

  Conclusiones:

  - EL impacto general de nuestro proyecto es positivo, lo que demuestra que es rentable económicamente desde el punto de vista financiero, y en mismos términos ambientales y tecnológicos.
  - Se mejora el servicio de soporte técnico en la PUCESE involucrando la modernidad y servicios acordes a los avances tecnológicos.
  - Se brinda servicios de alta calidad que va acorde a los avances tecnológicos, demostrando que el departamento de TIC de la PUCESE se preocupa por las necesidades de sus usuarios y brinda soluciones a problemáticas de su entorno.

- (León Robayo, 2015), realizo una investigación: “IMPLEMENTACIÓN DE UNA MESA DE AYUDA EN EL DEPARTAMENTO DE TECNOLOGÍA DE LA INFORMACIÓN DE UNIFINSA PARA SOPORTE AL USUARIO BASADO EN LAS MEJORAR PRÁCTICAS DE LA LIBRERÍA DE INFRAESTRUCTURA DE TECNOLOGÍAS DE INFORMACIÓN(ITIL)”.

  Objetivo general: Realizar el análisis e implementación de una mesa de ayuda en el departamento de tecnología de la información para soporte de UNIFINSA basado en ITIL.

  Conclusiones:

  - Para apoyar la implementación de la mesa de ayuda en el departamento de tecnología de la información de UNIFINSA Sociedad Financiera basado en ITIL, mediante los resultados de las encuestas de satisfacción luego de la implantación de la mesa de ayuda.
  - Se procedió con la parametrización y personalización del software SYSAID para su adaptación a los requerimientos del área de TI de UNIFINSA Sociedad financiera.
  - La implementación de una mesa de ayuda permitió mejorar el soporte a los usuarios en el departamento de Tecnologías de Información de UNIFINSA Sociedad Financiera.

- (López García, 2013), realizo una investigación: “SISTEMA DE SOPORTE TÉCNICO VÍA REMOTA PARA USUARIOS DE EQUIPOS DE CÓMPUTO EN RED”.

  Objetivo general: Implementar un sistema de soporte técnico vía remota para usuarios de equipo de cómputo en red.

  Conclusiones:

  - Al concluir este proyecto de tesis, se cumplieron los objetivos iniciales, con que podemos definir que se ha llevado a cabo de manera exitosa. Con la cual se obtuvo un sistema de soporte técnico vía remota, el cual nos proporciona una manera más fácil y rápida de solucionar vía remota, el cual nos proporciona una manera más fácil y rápida de solucionar los problemas que se prestan en los equipos de cómputo, esto con la ayuda de herramientas de vanguardia, que en su conjunto dormán el sistema completo.
  - Este proyecto se llevó a cabo pesando en cubrir necesidades de la Unidad de Servicios de Cómputo de la Facultad de Ingeniería UNAM, pero se puede implementar en cualquier red de datos que cumpla con los requerimientos generales.

2.2. BASES TEÓRICAS.

2.2.1. Soporte técnico.

(Gary, 2001), refiere que el soporte técnico, es un rango de servicios que proporcionan asistencia con el hardware o software de una computadora, o algún otro dispositivo electrónico o mecánico. En general los servicios de soporte técnico tratan de ayudar al usuario a resolver determinados problemas con algún producto en vez de entrenar o personalizar. La mayoría de las compañías que venden hardware o software ofrecen soporte técnico de manera telefónica o en línea. Las instituciones y compañías por lo general tienen sus propios empleados de soporte técnico. Existen a su vez múltiples lugares libres en la web respecto a soporte técnico, en los cuales los usuarios más experimentados ayudan a los novatos.

Áreas de Desempeño:

- Empresas.
- Instituciones.
- Hogares
- En cualquier parte donde haya un equipo que reparar.

a. Niveles de soporte técnico.

El soporte técnico generalmente está dividido en capas o niveles, para así contar con una manera más eficaz de dar solución a los problemas de los usuarios. El número de niveles es establecido por cada organización, y es

fundamentalmente definido de acuerdo de sus características y sus necesidades.

Los niveles de soporte técnico están definidos según el tipo de atención requerida, la severidad del problema y el tiempo que llevará la solución de dicho problema.

A continuación, se listan los diferentes niveles de soporte técnico, que por lo general suelen ser 4 niveles:

- **Nivel 1.** Este es el nivel básico de soporte técnico, responsable de las incidencias básicas del cliente. La principal función en este nivel es reunir toda la información del cliente, para determinar mediante un análisis la fuente del problema. Los administradores en este nivel están directamente en contacto con los clientes y generalmente manejan problemas básicos a los cuales se les soluciona de manera sencilla y generalmente hacen uso de aplicaciones de Software para una solución más rápida.

  Algunos de los conocimientos con los que cuenta el técnico en este nivel son: formateo de computadoras, instalación de paquetería y cambio de componentes de equipo de cómputo.

- **Nivel 2.** Este es un nivel más especializado, ya que, en este, sus integrantes cuentan con conocimientos más sólidos en el área computacional. Por lo que las personas que realizan este tipo de

soporte están especializadas en redes de datos, sistemas operativos, bases de datos, etc.

Los técnicos que brindan soporte técnico en este nivel cuentan con por lo menos 1 año en el área de soporte y cuenta con los conocimientos de nivel 1 y con conocimientos de recuperación de información nivel Software, manejo de paquetería de oficina a nivel básico y configuración de redes inalámbricas y cableados en grupos de trabajo.

- **Nivel 3**. Este nivel es el de mayor capacidad para resolver problemas, cuando un problema llega a este nivel se considera de alto impacto o de resolución avanzada

  El personal asignado a este nivel, son expertos en sus campos, y son responsable de brindar ayuda al personal de los niveles 1 y 2, además de que una de sus actividades fundamentales es la de investigar y desarrollar soluciones a problemas nuevos o desconocidos. Este nivel tiene por lo menos 2 años en el área de soporte cuenta con los conocimientos del nivel 1 y 2, además tiene conocimientos en la reparación de equipo de cómputo y periféricos a nivel componente. Cuenta con conocimientos de electrónica y es capaz de diagnosticar cualquier falla, a nivel circuito. Puede reparar

equipo de cómputo portátil (Laptops), conoce a nivel avanzado paquetería de oficina y da soluciones rápidas a nivel de redes.

- **Nivel 4.** El personal de este nivel cuenta con los conocimientos de los niveles anteriores, además de manejar operación de Servidores Microsoft y Linux, la instalación, configuración, interconexión, administración y operación de los servidores. Es responsable normalmente del área de Sistemas de una corporación y tiene por lo menos dos certificaciones en el área.

b. Tipos de soporte técnico.

(Kajko-Mattsson, 2004), menciona que el soporte técnico se puede dar por distintos tipos de medio, incluyendo el correo electrónico, chat, software de aplicación, faxes, y técnicos, aunque el más común es el teléfono.

En los últimos años hay una tendencia a la prestación de soporte técnico en remoto, donde un técnico se conecta al ordenador mediante una aplicación de conexión remota. Existen 2 tipos de soporte técnico:

- **Soporte técnico presencial.** En el cual el usuario del equipo que presenta la falla informa al técnico de lo sucedido y para poder solucionar el problema el técnico se desplaza hasta el lugar donde se encuentra el equipo físicamente para poder averiguar la causa y dar la solución al problema.

Algunas de las ventajas que podemos tener al realizar este tipo de soporte, es que el técnico tiene un control total del equipo, lo que le ayuda a solucionar rápido el problema. Ya que con esto evita un mal diagnóstico por parte del usuario acerca de la falla que presenta el equipo o una mala comunicación con los usuarios respecto a los problemas de sus equipos.

La gran desventaja que presenta este tipo de soporte es que en ocasiones se pierde demasiado tiempo en trasladarse el técnico hasta el lugar donde se encuentra el equipo con la falla o incluso puede llevar más tiempo el traslado que la misma solución. Además de que, en ocasiones, al estar el técnico fuera de su área de trabajo o en constante movimiento pudiera complicar la manera de contactarlo en caso de que se presente algún otro problema en los equipos.

- **Soporte técnico a distancia o remoto.** Este tipo de soporte en los últimos años ha tenido una gran tendencia gracias a las características que presenta que son de gran utilidad. En este tipo de soporte el usuario avisa el técnico de que se ha presentado un problema en su equipo, y entonces el técnico con ayuda de una aplicación de conexión remota puede conectarse al equipo que presenta la falla y tomar el control total del equipo, proporcionando así la solución remotamente.

Con este tipo de soporte técnico tenemos muchas ventajas, entre las cuales tenemos que se da una solución rápida, ya que el técnico no tiene que desplazarse hasta donde se encuentra el equipo con la falla. Además de que el técnico tiene el control total del equipo y con ello puede saber exactamente cuál es el problema y solucionarlo de la manera más rápida posible.

El soporte técnico vía remota es el que en los últimos años ha tenido una gran aceptación por las ventajas que nos proporciona. En la actualidad podemos encontrar varias aplicaciones de conexión remota, cada una con diferentes características, podemos encontrar aplicaciones para diferentes plataformas de sistemas operativos o en algunos casos multiplataforma. Además de que actualmente hay aplicaciones de conexión remota de código libre o en su defecto de licencia gratuita y cada una la podemos encontrar de modo administrador o usuario.

En general en estos días tenemos una gran cantidad de este tipo de aplicaciones, la elección de cuál de ellas es mejor depende de las características de la organización y de nuestros equipos de cómputo. Además de considerar el alcance y el costo que se tiene definido para poder proporcionar el soporte técnico.

El tipo de soporte técnico con el que se cuenta siempre debe ser acorde a las características de nuestra red y debe ser considerado

desde un principio, cuando se diseña e implementa la red, ya que en ocasiones se deja un poco de lado este servicio, pero no debe ser así, ya que este servicio es muy importante para el desarrollo de las actividades de los usuarios, que su vez se ven reflejados en el desempeño de la organización.

c. Soporte informático.

(Appser Data Engineering S.L. (APSER), 2015). Se trata de un servicio mediante el cual los especialistas en apoyo informático o expertos en digital te ofrecen asistencia técnica, soporte remoto ante algún problema y asesoramiento a individuos y organizaciones que trabajan cada día con las nuevas tecnologías. El soporte informático puede estar proporcionado por un departamento de la empresa o por un proveedor externo que es contratado por ti y que trabajará con tu negocio cuando lo necesites.

Una de las clasificaciones más claras de este servicio es la que distingue las dos formas de prestación de la ayuda, por ello, nos podemos encontrar:

- Soporte técnico físico: Es aquel que atiende y ejecuta automáticamente los programas de diagnóstico para resolver problema in situ, es decir, en la sede de la empresa. De todas formas, su labor no es solo la de diagnosticar un problema y solucionarlo, sino que también pueden formar al equipo en el uso del software o el hardware o las redes de la empresa.

- Servicio informático remoto: Se realiza a través de la red o por teléfono y se suele dar por parte de proveedores que ofrecen un servicio y también la solución a posibles problemas que puedan surgir con él. El servicio técnico remoto cada vez está avanzando más, de forma que es una manera muy útil de detectar un problema, hacer un diagnóstico y buscar una solución. Por ejemplo, a partir de opciones como el escritorio remoto, el técnico puede acceder directamente al equipo del cliente para poder llevar a cabo su trabajo de una forma totalmente libre y ofrecer los mejores resultados.

2.2.2. Acceso remoto

(Dordoinge & Philippe, 2006) El acceso remoto se refiere a la capacidad de acceder a una computadora, como un ordenador personal o una computadora de red de oficina, desde una ubicación remota. Esto permite a los empleados trabajar fuera del sitio, como en casa o en otro lugar, mientras aún tiene acceso a una computadora o red distante, como la red de la oficina. El acceso remoto se puede configurar utilizando una red de área local (LAN), una red de área extensa (WAN) o incluso una red privada virtual (VPN) para que los recursos y sistemas se puedan acceder de forma

remota. El acceso remoto también se conoce como inicio de sesión remoto.[1]

La tecnología de las redes informáticas constituye el conjunto de las herramientas que permiten a los ordenadores compartir información y recursos.

Beneficios del acceso remoto:

- Aumento de la productividad.
- Ahorro de costes.
- Flexibilidad laboral.
- Ahorro de tiempo.
- Aumento de motivación.
- Retención de personal.
- Conciliación profesional.

Para que un servicio tenga éxito en el día a día es necesario identificar, analizar y gestionar los riegos y valorarlos frente a los beneficios:

- Seguridad. Los recursos corporativos se publican en el exterior con información sensible.
- Viabilidad técnica de la solución.
- Administración. Controlar / Auditar accesos.
- Facilidad de uso. Rechazo de los usuarios

[1] Definición tomada y traducida de: https://www.techopedia.com/definition/5553/remote-access

a. Características del acceso remoto.

- Distintos perfiles de usuarios. Se realiza un “PERFILADO” centrado en el usuario: Se categoriza a los usuarios de la empresa, se especifican sus necesidades y entonces se construye un conjunto de soluciones para cada categoría.
    - Empresas externas e aplicaciones.
    - Personal de sistemas.
    - Directivos.
    - Desarrolladores.
    - Usuarios.
    - Etc.
- Distinto tipo de información.
    - Aplicaciones Web:
        - Correo Web.
        - Intranet.
        - Listín Corporativo.
        - HelpDesk.
        - Aplicaciones de Proveedores.
        - Etc.
    - Aplicaciones de “Escritorio”
        - Contabilidad.
        - Facturación.

        - Terminal Financiero.
        - Acceso a BBDD.
        - Aplicaciones departamentales.
        - Etc.
- Necesidad del acceso.
    - Disponibilidad 24x7
    - Desde distintos dispositivos (móviles, navegadores, web, servidores, etc.)
    - Facilidad de uso.
    - Encriptación de las comunicaciones.
    - Ancho de Banda eficiente.
    - Movilidad
    - Etc.
- Métodos de autentificación.
    - Usuario /Contraseña, Passphrase
    - Token, Token móvil, SoftToken, etc.
    - Certificados usuarios
    - Tarjeta de claves
    - Biometría.
    - Autenticación multifactorial.
    - Factores a tener en cuenta.

        - Ha de ser fiable con una probabilidad muy elevada (Tasa de fallos baja).
        - Económicamente factible para la organización (si su precio es superior al valor de lo que se intenta proteger, tenemos un sistema incorrecto).
        - Soportar con éxito cierto tipo de ataques.
        - Ser aceptable para los usuarios, que serán al fin y al cabo quienes lo utilicen.
- Sistema de auditoria.
    - Almacenamiento de Logeos.
    - Trazabilidad.
    - Posibilidad de Análisis Forense.
    - Alertas en tiempo real.
    - Consolidación y correlación de eventos.
- Administración.
    - ¿Quién lo administra?
    - ¿Cómo se dan de alta, baja?
- Seguridad.
    - Establecer controles fuertes en los canales de acceso (control IP)
    - Antivirus usuario / Servidor.
    - Comprobar procesos en ejecución.

- Parches de Seguridad
- Securizar el puesto de trabajo remoto.
- Securizar las comunicaciones.

2.2.3. Principios fundamentes de la seguridad de la información aplicada en red.

Concepto.

"Seguridad en redes es mantener bajo protección los recursos y la información que se cuenta en la red. A través de procedimientos basados en una política de seguridad tales que permitan el control de lo actuado”[2]

Los mecanismos necesarios para salvaguardar la información frente a todo tipo de ataques y amenazas se fundamentan en los siguientes principios: confidencialidad, integridad y disponibilidad.

a. Confidencialidad

Tiene por objetivo el garantizar que los datos, objetos y recursos solamente pueden ser leídos por sus destinatarios legítimos.

---

[2] Ing. Leonardo Hoet, Rodolfo Cozzi, Rodolo Baader y Rodigo Seguel, Manueal de Seguridad de redes.

b. Integridad

Proceso mediante el cual se garantiza que los datos, objetos y recursos no han sido alterados. Permanecen completos y son fiables.

c. Disponibilidad

Es la garantía de que los recursos e información permanecen accesibles para los usuarios autorizados cuando los necesiten.

d. Controles para asegurar la Confidencialidad e Integridad

Los más utilizados para salvaguardar la confidencialidad antes de las amenazas son:

- **Cifrado de datos**. Garantiza que la información no es legible para individuos, entidades o procesos no autorizados. La técnica que utiliza es transformar un texto claro mediante un algoritmo en un texto cifrado, gracias a una información secreta o clave de cifrado. Existen dos técnicas:
- **Cifrado Simétrico o de clave secreta.** Es cuando se emplea la misma clave en operaciones de cifrado y descifrado en el origen y en el destino. Estos sistemas son muy rápidos y resultan apropiados para cifrar grandes volúmenes de información de datos o de información en tiempo real, como transmisiones de video o voz.

- **Cifrado Asimétrico o de clave pública.** Cuando se utiliza una pareja de claves (una privada y una pública) para separar los procesos de cifrado y descifrado. Una clave, la privada, se mantiene secreta, mientras que la segunda clave, la pública debe ser conocida por todos. Tiene la propiedad de que a partir de la clave pública no es posible determinar la clave privada. Estos resultan más lentos que los simétricos y son adecuados para las funciones de autenticación, distribución de claves y firmas digitales. El algoritmo de clave pública más usada es el RSA. [3]
- **Autenticación de Usuarios.** Es el proceso que asegura la identidad de los sujetos participantes en una comunicación o sesión de trabajo, mediante: contraseñas, biometría (huellas dactilares, identificación de retina), tarjetas inteligentes o de banda magnética, o procedimientos similares.
- **Autorización de Usuarios**. Una vez que la identidad del sujeto a ha sido correctamente validada, a este usuario legítimo, debe dotársele de privilegios para poder efectuar ciertas operaciones con los datos, objetos y recurso protegidos como leerlos, modificarlos, crearlos, borrarlos e imprimirlos.

---

[3] Este algoritmo fue descrito por Ron Rivest, Adi Shamir y Len Adleman las letras RGa son las iniciales de sus apellidos.

- **Clasificación de datos[4].** No todos los datos poseen el mismo grado de privacidad, sensibilidad o confidencialidad. La clasificación de datos típicamente tiene cuatro niveles, ordenados de mayor a menor seguridad requerida:
- **Confidencial**. Aplicado a información cuyo uso por personas no autorizadas puede suponer un importante daño en la Organización
- **Sensible o Restringido.** Aplicado a información cuya utilización por personas no autorizadas iría contra los intereses de la Organización y lo sus clientes.
- **Privado o Uso Interno**. Para datos que no necesitan ningún grado de protección para su difusión dentro de la Organización.
- **Público**. Datos que no necesitan ningún grado de protección para su difusión.

2.2.4. Amenazas, ataques y vulnerabilidades en Red

a. Amenazas

Una amenaza es una acción o evento que sin importar su naturaleza puede violar la seguridad en un entorno de sistemas de información, se las puede clasificar en intencionadas, no intencionadas y naturales. Los componentes de la amenaza son: objetivo, agentes y eventos.

---

[4] Gonzalo Álvarez Marañon, Pedro Pablo Peréz García, Seguridad para empresa y particulares.

Objetivo. Es el principio de seguridad que puede ser atacado (confidencialidad, integridad y disponibilidad). Estos objetivos corresponden a la motivación o razones reales que se encuentran detrás de la amenaza.

Agentes. Las personas u organizaciones que originan la amenaza, pretendiendo dañar a una Organización. Un agente debe tener tres características: acceso, conocimiento y motivación.

- **Acceso.** Es la capacidad que tiene un agente para llegar a un objetivo, este acceso puede ser directo (un usuario que tenga una cuenta en el sistema) o indirecto (Personal no autorizado tenga acceso a las instalaciones por algún otro medio). El acceso que tiene un puede explotar una vulnerabilidad y convertirse en amenaza.
- **Conocimiento**. Se refiere al nivel y tipo de información que el agente debe tener con respecto al objetivo, es de utilidad para un agente conocer: identificadores de usuarios, contraseñas, ubicaciones de archivos, direcciones de red, procedimientos de seguridad.
- **Motivación**. Son las razones que puede tener un agente para representar una amenaza hacia el objetivo, la motivación es una característica clave que permite identificar el objetivo principal.

Eventos. El tipo de acción que representa la amenaza, son las maneras en las que un agente de amenaza puede o podría causar daño a la Organización:

Entre los eventos más conocidos están los siguientes: abuso del acceso no autorizado, alteración malintencionada de la información, alteración accidental de la información, acceso no autorizado a la información, destrucción mal intencionada de la información, interrupción de las comunicaciones internas o externas, robo de hardware o software.

Tipos de Amenaza.

- **Recopilación de información (Harvesting**). Un agente o intruso busca obtener información acerca de topologías de red, tipos de dispositivos presentes y su configuración. Con esta información puede descubrir vulnerabilidades y puntos de entrada.
- **Interceptación de tráfico (Sniffing).** Son programas que interceptan el tráfico sin modificarlo, en busca de contraseñas e información sensible que circula por la red.
- **Falsificación (Spoofing).** El agente oculta su identidad real, haciéndose pasar por otro usuario o equipo. Utiliza para enmascarar la dirección real de procedencia de un ataque o para burlar un sistema de control de acceso en función de la dirección IP de origen. Es considerado un ataque por spoofing la modificación y creación

de paquetes con el objetivo de falsear la identidad de algún componente de la transmisión de un mensaje.

- **Secuestro de Sesión (Hijacking).** El intruso usa una aplicación para simular el comportamiento de un cliente o de un servidor, o bien intercepta los paquetes de red pudiendo visionarios y modificarlos a su antojo. Cómo consecuencia el servidor o el Cliente creen estar comunicándose con el equipo legítimo, cuando en realidad se trata del equipo atacante. Es utilizado para obtener información de autenticación y datos sensibles.
- **Denegación de Servicio (Denial of Services).** El intruso busca denegar a usuarios legítimos el acceso a los servidores o servicios de red, inundándola con tráfico espurio que consuma ancho de banda y recursos.

b. Ataques

Los ataques a una red pueden ocurrir a través de medios técnicos como herramientas diseñadas para ataques a vulnerabilidades detectadas en algún elemento de red o sistema de computación, también suelen presentarse por medio de la ingeniería social.

Enumeración. Es una técnica que se usa para poder detectar los sistemas existentes en una red, para ello se pueden usar varias herramientas como: ping, tracert, snmp.

- **Escaneo de puertos.** Es una técnica cuyo objetivo es determinar que puertos están abiertos y consiste en enviar un paquete TCP con el flan SYN activo, al que el sistema destino deberá contestar con SYN+ACK en caso de estar abierto o RST en caso de estar cerrado. Para un rastreo UDP se envía un paquete sobre un puerto y con la respuesta se determina como cerrado al recibir un ICMP port unreachable o se supone abierto si no se recibe este paquete.
- **FingerPrinting de aplicaciones.** Permite detectar el sistema operativo y la versión de un equipo remoto, así como también la posibilidad de descubrir aplicaciones remotas que se están ejecutando, esto normalmente se lo consigue usando la detección por coincidencia de un puerto característico asociado a un servicio o con visualizar la información presentada, hasta detectar en función de peticiones no estándar el protocolo, aplicación y versión existente.
- **Escaneo de vulnerabilidades.** Este tipo de ataque lo que busca es encontrar fallos de seguridad conocidos, ya sea por descuidos de configuración o por errores de seguridad publicados. Para asegurarse, es recomendable realizar auditorías periódicas con herramientas para conocer el estado de exposición de los sistemas, aplicaciones, servicios y bases de datos.

- **Ruptura de contraseñas (Cracking).** El objetivo de este ataque es lograr irrumpir a un sistema obteniendo la contraseña del sistema, existe dos mecanismos; el primero se lo denomina ataque de fuerza bruta y consiste en automatizar un intento de acceso en el cual se prueben todas las combinaciones de usuario/ contraseña. Este es un método que no es muy deseable para un atacante debido a que el tiempo que consume es elevado.

  El segundo mecanismo se lo conoce como ataque de diccionario, porque existe la posibilidad de automatizar un intento de acceso probando todas las posibles combinaciones de usuario / contraseña. Existen dos técnicas de intento de ataque:

- **Ruptura de contraseña de hash no conocido.** Ante una autenticación se prueba un usuario con una contraseña, luego otra y otra, hasta que se termina acertando con la correcta. Esta tarea se lo realizada con programas que lo automatizan, por ejemplo, para plataformas Unix destaca Hydra y para Windows Brutus ataque por diccionario o fuerza bruta sobre servicios remotos como HTTP, telnet, POP3, FTP, SMB, IMAP o NNTP.

- **Ruptura de contraseñas de hash conocido.** Se fundamenta en ir probando posibles palabras, calculando su hash y comprobando si coinciden con el hash conocido. Este sistema es el más difundido dado que en los computadores se guardan en lugares estándares

los archivos de contraseñas y siempre emplean métodos de hash con algoritmos públicos.

- **Adware.** El adware es software que durante su funcionamiento despliega publicidad de distintos productos o servicios. Estas aplicaciones incluyen código adicional que muestra la publicidad en ventanas emergentes o a través de una barra que aparece en la pantalla. La forma de distribución se basa en ofrecer software gratis en internet, así el usuario no paga por usar el programa, pero debe soportar la presencia de banners.

  Los autores de estas aplicaciones incluyen código adicional para servir los anuncios, que pueden ser mostrados a través de pop-ups, en una barra especial del navegador, o en una zona dedicada de la interfaz del programa en cuestión.

- **Spyware.** Es aquel programa que se instala y se ejecuta en un ordenador y que transmite información a terceros sin el consentimiento (ni el conocimiento) del usuario. El spyware procede de sitios de pornografía gratuitos, sitios de descarga de crack y programas piratas. Además, no se instala solo, siempre el usuario es el responsable ya que normalmente no lee los términos y se los acepta durante la instalación de software descargado desde el Internet, la forma en la cual estos se propagan es al descargar

software de sitios Web. Los síntomas de este tipo de ataque generalmente son:

- El rendimiento del ordenador se vea afectado, es más lento en el procesamiento ya que los recursos de memoria y procesador son usados generalmente para abrir ventanas con contenido pornográfico.
- En el historial de favoritos del explorador se registran sitios sin que el usuario los haya registrado.
- Aparecen ventanas de Pop-up en el navegador, incluso cuando no se está conectado al Internet.

Existen varias herramientas en combatir el spyware, tanto preventivamente como reactivamente cuando el spyware ya está instalado en el disco duro. Una herramienta es el Ad-Aware versión 6.0 de Lavasoft, otros también son: spychecker, spyRemover entre los más conocidos.

Entre los programas con enfoque preventivo están: Panda Platinum Internet Security, SpywareBlaster, Spyware Guard.

La mejor forma de evitar este tipo de ataque es lograr que el usuario se mantenga alejado de los sitios mencionados y no usar los programas de intercambio de archivos (P2P).

c. Vulnerabilidades

Es una vía de ataque potencial o susceptible de convertirse en amenaza. Las vulnerabilidades pueden existir en redes y sistemas de computación, en procedimientos administrativos y en las seguridades físicas de la Organización. Una vulnerabilidad está caracterizada por la dificultad y el nivel de capacidad técnica que se requiera para explotarla.

Las vulnerabilidades son paliadas mediante contramedidas estos controles pueden ser de cinco tipos:

- Preventivo: Intenta evitar ocurrencia de sucesos indeseados.
- Detectivo: Intenta identificar sucesos indeseados después de que hayan ocurrido.
- Disuasorio: Intenta disuadir a los individuos que violaran intencionadamente las políticas o procedimientos de seguridad.
- Correctivo: Intenta remediar las circunstancias que permitieron la actividad ilegítima o devolver el sistema al estado anterior a la violación.
- Recuperativo: Intenta restaurar los recursos perdidos y ayudar a la organización a recuperarse de las pérdidas económicas causadas por la violación.

2.2.5. Gestión de seguridad de la información.

La Gestión de la seguridad es el conjunto de directrices, procedimientos y criterios que se implementan con el fin de alcanzar los niveles de seguridad exigibles en una Organización.

La Gestión de la seguridad de información comienza con definir las expectativas formales de seguridad que una Organización tiene y el contexto de seguridad en el cual se va a aplicar.

a. Gestión de riesgo.

En seguridad, se considera que la primera premisa es que “Los riesgos no pueden eliminarse por completo, lo que se debe buscar es disminuir el impacto a niveles aceptables de manera que no causen daño.[5]

b. Gestión de seguridad en el espacio.

La Prevención evita tener que recurrir a la recuperación, mientras que la detección facilita la recuperación y realimenta la prevención. Para que un sistema sea razonablemente seguro, deben implantarse los tres tipos de medidas coordinadamente.

---

[5] Eric Nauwald (2003), Fundamentos de Seguridad en Redes

Figura 1. Controles de seguridad

Fuente: Tesis “Implementación de políticas de seguridad en Red LAN Corporativa”

Tabla 3. Controles de seguridad

Función	Descripción	Mecanismo
Prevenir	Aumentar el nivel de seguridad evitando que los ataques tengan éxito.	Cortafuegos
Detectar	Se encargan de velar por que todo esté en orden y de alertar cuando se produce una anomalía, normalmente debida a un intruso.	Sistema de Detección de Intrusos IDS
Recuperar	Garantizan que ante un incidente de segundad, Política de Copias de Recuperar causado o fortuito, se pueda recuperar toda la seguridad información y retomar a la normalidad en el menor tiempo posible	Política de copias de seguridad.

Fuente: Tesis “Implementación de políticas de seguridad en Red LAN Corporativa”

c. Gestión de la seguridad en el tiempo

Desde una óptica relacionada con el tiempo, se plantea otra estrategia de carácter cíclico que puede dividirse en tres tareas principales: alcanzar la seguridad, mantener la seguridad y evaluar la seguridad.

Figura 2. Estrategia de seguridad en el tiempo[6]

Fuente: Tesis "Implementación de políticas de seguridad en Red LAN Corporativa"

2.2.6. Seguridad perimetral.

La infraestructura de red de las organizaciones ha ido creciendo de acuerdo a los requerimientos de la administración y crecimiento del

[6] Gonzalo Álvarez M.; Pedro Pérez G. (2004), seguridad informática para empresas y particulares.

negocio. La necesidad mantener y mejorar las relaciones comerciales con proveedores y clientes ha determinado que se establezcan puntos de contacto o puertas de enlace de la red corporativa con otras redes.

Para implementar estos requerimientos es necesario establecer puntos de contacto o puertas de enlace como por ejemplo puede ser el acceso a Internet o la interconexión de Redes por medio de la configuración de una Red Virtual Privada (VPN). Estos dispositivos que permiten establecer estas puertas de enlace constituyen dispositivos perimetrales.

a. Dispositivo perinatal

Es básicamente un dispositivo que, rutea paquetes entre dos redes como puede ser un firewall o ruteador y un conmutador.

Conoce acceso a la red corporativa y esto permite ampliar al perímetro a más clientes, estos pueden ser Controladores de USB, los clientes y servidores.

Estos perímetros, constituye la frontera con el resto del mundo la seguridad de los sistemas depende en gran medida de las conexiones que tienen con el exterior.

b. Caracterización e Identificación de un dispositivo perimetral

Una tarea importante antes de identificar los dispositivos perimetrales es hacer un inventario de los elementos de red existentes en la misma, una

vez realizado esta operación, se hace una descripción de aquello que se ha encontrado, esto es identificar hosts estáticos y hosts dinámicos de red y documentar sus características de red y la configuración general.

- **Un host estático** es aquel que se conecta de forma permanente en la red. sus características de red y la configuración general del sistema rara vez se modifica, ejemplos pueden ser: servidores, estaciones de trabajo, servidores de seguridad.
- **Un host dinámico** es un dispositivo conectado temporalmente, el cual se conecta y desconecta según las solicitudes de los usuarios o servicios, algunos ejemplos podrían ser los clientes VPN remotos, las sincronizaciones de base de datos de oficinas remotas y los equipos portátiles inalámbricos.

c. Criterios para identificar dispositivos perimetrales

Este inventario se lo puede hacer de forma manual, verificando localmente o mediante de servicios de terminales o automatizada con el uso de herramientas por software.

Una vez identificados todos los hosts existentes en el perímetro físico, se puede documentar y analizar todas las características.

- **Dispositivos de hardware de red.** Según la ubicación que ocupen en la infraestructura de red. entre éstos incluimos: servidores como ISA Server sobre plataforma de sistema operativo Windows,

ruteadores como CISCO, módems utilizados para acceso remoto usando líneas telefónicas, conmutadoras y concentradoras inalámbricas.

- **Servidores y clientes.** Tras identificar a los servidores y clientes como posibles dispositivos perimetrales, se deberá tener en cuenta: el sistema operativo, los servicios y las aplicaciones que se encuentran instalados en los equipos, así como los parámetros de configuración. Estas características determinan si el sistema se puede exponer o no a la red interna desde redes externas, ya que pueden dejar abiertas entradas en la red con determinadas configuraciones avanzadas.

d. Definición del perímetro de la red

Luego de completar el análisis de los hosts de la red según lo descrito en las secciones anteriores, puede trazar un diagrama lógico de la red perimetral. El perímetro de la red se constituye a partir de la asignación lógica de los dispositivos de Host. Como se muestra en la siguiente ilustración:

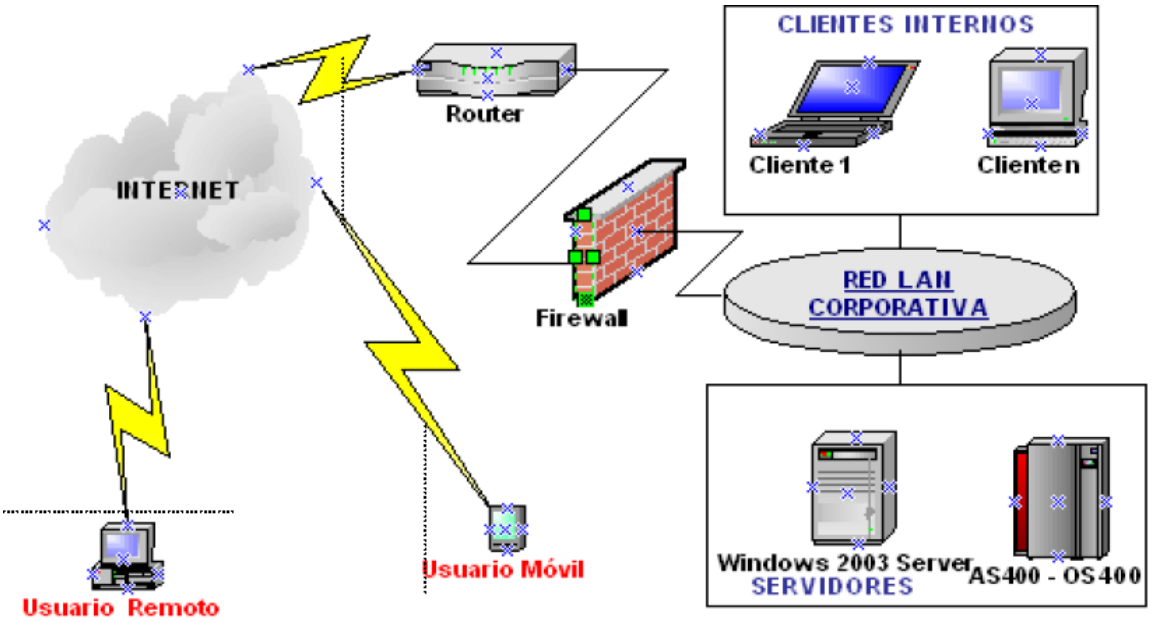


Figura 3. Diagrama Lógico o Perímetro de la Red

Fuente: Tesis "Implementación de políticas de seguridad en Red LAN Corporativa"

2.2.7. Redes y Comunicaciones

a. Dominio de colisión

Ethernet. Es un segundo segmento donde pueden ocurrir colisiones, en medio compartido de la LAN en forma de concentrador, un HUB o un cable. Cuando más tráfico hay sobre un dominio de colisión, más probable es que ocurran colisiones. Por el contrario, el incremento de colisiones implica que los equipos gasten más tiempo en intentar retransmitir.

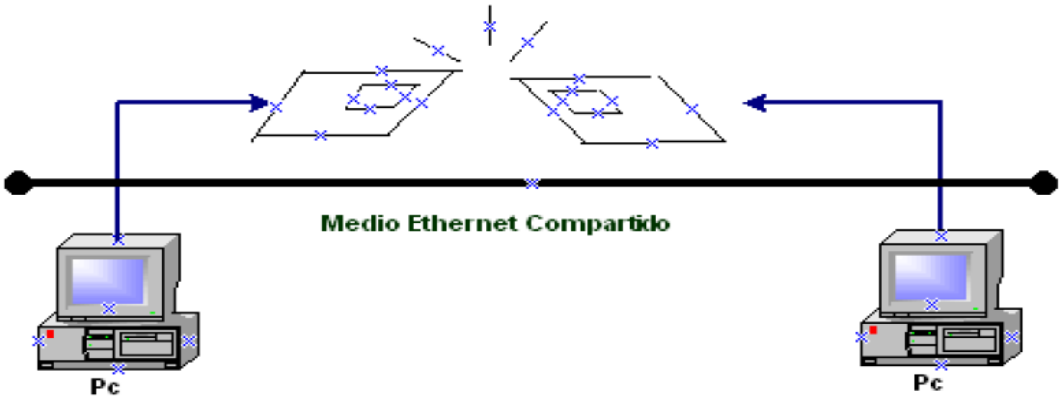


Figura 4. Dominios en colisión

Fuente: Tesis “Implementación de políticas de seguridad en Red LAN Corporativa”

Preservar la información y la integridad de un sistema informático es algo muy importante para una empresa u organización, por lo que en pérdidas económicas y de tiempo podría suponer, sin olvidarnos del peligro que podría acarrear el acceso al sistema de un usuario no autorizado.

Ethernet, usa el algoritmo de Acceso múltiple con detección de portadora (CSMA/ CD), para escuchar el tráfico, detectar colisiones y abortar las transmisiones. Este algoritmo controla y restringe el acceso al cable para asegurar la integridad de las transmisiones

b. Arquitectura TCP/IP y el modelo OSI

La Arquitectura de comunicaciones más extendido en el mundo es TCP/IP, debido a su flexibilidad y amplia disponibilidad para todo sistema operativo

es utilizado en Internet, Intranets y Extrañéis. Internet es una red de redes con cobertura mundial. Una Intranet, es una red interna de una Organización que usa protocolos de Internet y finalmente una Extranet es una red de interconexión privada con el exterior para prestar servicios a clientes o empresas con algún vínculo de comercial.

La principal ventaja de TCP/IP, es la confianza ante fallos, si un enlace se pierde la información puede fluir por otro camino incluso sin que el origen y el destino se den cuenta.

TCP/IP, se compone de una pila de protocolos que se fundamenta en el modelo OSI.

Tabla 4. TCP/IP y Modelo OSI

MODELO OSI	DESCRIPCIÓN	TCP-IP	Protocolo
APLICACIÓN	Proporciona al usuario la interfaz con el sistema de comunicaciones.	APLICACION	FTP, SMTP TELNET
PRESENTACION	Proporciona un mecanismo para transmitir la presentación de datos deseada entre las aplicaciones.	APLICACION	HTTP
SESIÓN	Gestiona la logística de las conexiones. Permite que dos aplicaciones sincronicen sus comunicaciones e intercambien datos.	APLICACION	RPC
TRANSPORTE	Proporciona mecanismos de Control de flujo en él envió, recepción y la retransmisión de paquetes que se perdieron.	TRANSPORTE	TCP,UDP
RED	El mensaje aumenta su tamaño en unos bits y se convierte en datagrama o paquete, cada cabecera de paquete tiene na dirección de red lógica.	INTER	IP
		RED	ARP
		Interfaz de RED	802.3 802.5
FISICA	Codifica o decodifica los pulsos en ceros o unos binarios y los ordena en unidades de bits)	Interfaz de RED	Bits

Fuente: Tesis “Implementación de políticas de seguridad en Red Lan Corporativa”

Interfaz de Red. Presenta una primera capa de acceso físico en contacto directo con los elementos de red, codifica y decodifica los pulsos eléctricos en unos y ceros binarios, los ordena en forma de unidades de bits. La segunda capa, de acceso al medio o de enlace se encarga de la negociación con el modelo físico.

Internetwork. Está relacionada con el acceso y encaminamiento de los datos a través de la red. El protocolo de Internet IP se utiliza en esta capa para ofrecer el encaminamiento de paquetes o datagramas[7] entre el emisor y receptora a través de varias redes. Actualmente IP se encuentra en dos versiones en versiones IPv4 e IPv6.

---

[7] Paquetes orientados a conexión con TCP y transporte datagramas no orientado a conexión con UDP

Tabla 5. IPv4 - IPv6

IPv4	Ipv6
La versión IPv4. Presenta una serie de ventajas desde el punto de vista de la disponibilidad y confianza ante fallos, pero muchas lagunas en lo que se refiere a seguridad.	Las direcciones pasan de los 32 a 128 bits, o sea a 2128 direcciones (3.402823669 e38. o sea sobre 1.000 sixtillones).
Pueden direccionar máximo 232 bits (4.294.667.296) para guardar la dirección IP.	La representación de las direcciones IP cambian y pasan de estar representadas por 4 octetos separados por puntos a estar divididas en grupos de 16 bits (representadas como 4 dígitos hexadecimal) separados por el carácter dos puntos. Por ejemplo: Dirección en IPv4 es 193.110.128.200 En IPv6 la misma IP sería: 2002.450.9.10.71. siendo su representación completa: 2002:0450:0009:0010:0000:0000:0000:0071
Desde la calidad de servicio, los paquetes pueden marcarse con prioridades para poder realizar distinciones de entre tráficos más o menos importantes.	Auto configuración (RFC2462) IPv8 incluye esta funcionalidad en el protocolo base. La propia pila intenta auto configurarse y descubrir el camino de conexión a Internet (router Discovery). Movilidad (RFC2462) de IPv6 es la posibilidad de conexión y desconexión de nuestro ordenador de redes IPv8 y. por tanto, la facilidad de poder viajar con él sin necesitar otra aplicación que nos permita que ese enchufe/desenchufe se pueda hacer directamente.
	EL núcleo de IPv6 incluye IPsec. un protocolo que permite autenticación y encriptación del de forma que todas las aplicaciones se pueden beneficiar de ello. Para conseguir esto, la siguiente cabecera puede tener valores AH (Authentication Header) y ESP ('Encapsulation Security Payload"). que permiten, emplear las mismas extensiones del protocolo empleadas en IPv4.

Fuente: Tesis “Implementación de políticas de seguridad en Red LAN Corporativa”

Transporte. Aquí, la información se une con cada servicio y es responsable del flujo de datos entre los equipos que forman la comunicación. Los protocolos que dan este servicio son:

- TCP Protocolo orientado a conexión.
- UDP Protocolo no orientado a conexión.
- ICMP Protocolo de paquetes de control de Internet.

Aplicación. Proporciona al usuario la interfaz con el sistema de comunicaciones y también un mecanismo para transmitir la presentación de datos deseada entre las aplicaciones.

Gestiona la logística de las conexiones y permite que dos aplicaciones sincronicen sus comunicaciones e intercambien datos. Coexisten protocolos orientados a ofrecer diferentes servicios: smtp. Http. rpc. Ftp. snmp. X-windows. Telnet. nfs. ssh

c. Redes Virtuales Privadas

Es una configuración de red que permite mediante una técnica de encriptación y de la definición de un túnel mediante protocolos de comunicación y seguridad, el seguro transporte de datos en tránsito entre distintos puntos remotos usando las infraestructuras de red pública públicas con un costo razonablemente bajo porque solo realizan llamadas

locales. Los protocolos como que más comúnmente se usan son IP. Ipsec. Frame Relay y Atm:

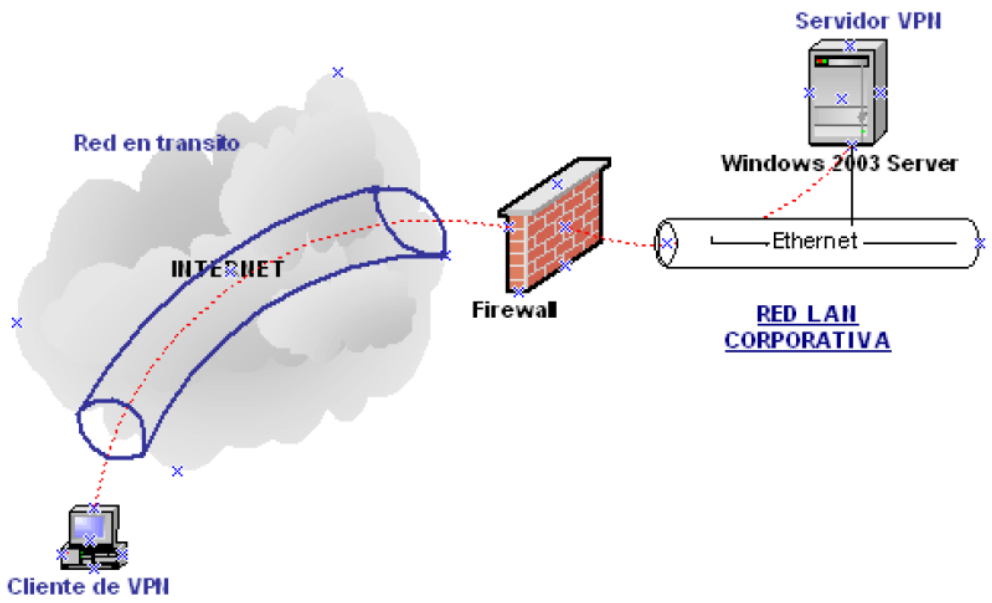


Figura 5. Red Virtual privada

Fuente: Tesis "Implementación de políticas de seguridad en Red LAN Corporativa"

Existen varias formas de configurar una VPN. Entre las conocidas, tenemos:

- **VPN de usuario** que son redes virtuales privadas entre la máquina de un usuario individual y la red o servidor de la VPN, el usuario se conecta a Internet mediante a un ISP por teléfono o con un módem de cable. Este tipo de configuración se recomienda cuando

empleados o usuario s internos móviles o que viajan tengan necesidad de conectarse al mail o a determinados archivos.

- **VPN de Sitio** que son redes que establecen una conexión privada virtual entre dos redes LAN para iniciar la conexión un sitio intenta enviar tráfico hacia el otro, los dos extremos negociaron parámetros de la conexión dependiendo de las políticas de los sitios, las dos redes también autenticaran entre sí, utilizando una clave compartida que haya sido configurado previamente o bien mediante un certificado de clave pública. Normalmente se utilizan las VPN como respaldo para líneas arrendadas.

2.2.8. Elementos De Red Y Seguridad.

HUB o Concentrador.

A pesar de ser elemento más simple de una red, actualmente ya están es fuera de uso porque la tendencia tecnológica ha hecho que sean reemplazados por SWITCH con importantes mejoras desde el punto de vista funcional.

Dentro del modelo OSI el concentrador opera en la capa 1 simplemente une conexiones y no altera las tramas que le llegan. Es un dispositivo que permite centralizar el cableado de una red, también conocido con el nombre de HUB, estos dispositivos pueden funcionar en modo pasivo, no necesita energía eléctrica y en modo activo necesita alimentación.

También llamados Smart hubs, son hubs activos que incluyen microprocesador.

Switch o Conmutador.

Este dispositivo de red opera en la capa 2 del modelo OSI, aunque los conmutadores o switches son los elementos que fundamentalmente se encargan de transportar las tramas de nivel 2 entre los diferentes puertos. Existen lo denominados conmutadores de nivel 3 o superior, que permiten crear en un mismo dispositivo múltiple redes de nivel 2 y encaminar los paquetes a nivel 3 entre las redes, realizando por tanto las funciones de transporte y encaminamiento.

Router o Ruteador

Son dispositivos de red que permiten interconectar dos redes al nivel de IP capa 3 del modelo OSI; y separa en distintos dominios de multidifusión, la configuración se base en disponer una serie de rutas estáticas o con protocolos de aprendizaje de rutas dinámicas sus principales funciones son:

- Aprender rutas dinámicamente solo de orígenes confiables, direcciones IP[8].
- Conviene usar las versiones RIP v2 u OSPF, evitando el uso de versiones anteriores como Rip v1 por ser susceptible a fallos de seguridad.
- Evitar propagar peticiones de broadcast en los ruteadores periféricos hacia el interior de la red corporativa.
- Los ruteadores ofrecen la posibilidad de añadir reglas que permiten o deniegan el tráfico en función de las direcciones IP y puertos, esto se lo realiza: configurando Listas de Control de Acceso (Access Lists) más conocidas en las arquitecturas de CISCO.
- Otra funcionalidad clave, es la traducción de direcciones de red (NAT). esto impide que un atacante pueda descubrir los rangos de direcciones internas y así poder iniciar un ataque por el direccionamiento a las máquinas internas. Es una técnica que se utiliza en Ipv4.
- Inhabilitar usuarios por defecto y cambio de contraseñas iniciales.

---

[8] GONZALO ÁLVAREZ M.: PEDRO PÉREZ G. (2004). Seguridad Informática para empresas y particulares.

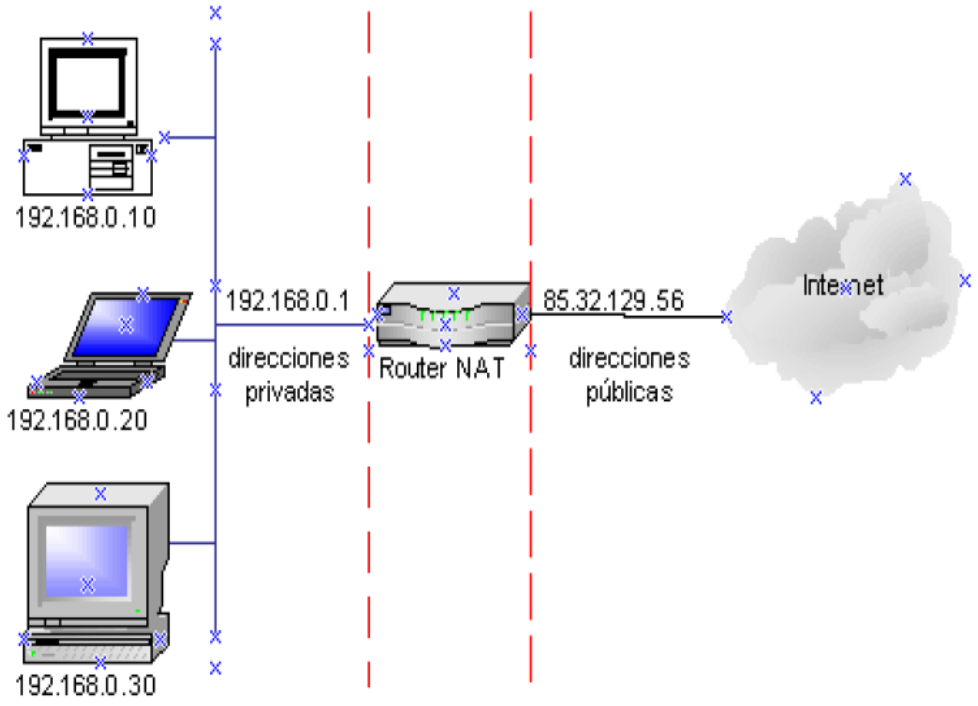


Figura 6. Ilustración del concepto de NAT

Fuente: Tesis “Implementación de políticas de seguridad en Red LAN Corporativa”

Dispositivos de Acceso Remoto

Son dispositivos de red que permiten a usuarios remotos acceder mediante el uso de algún medio de comunicación a servicios y recursos de red de la Organización. Los dispositivos usados por el cliente son MODEM telefónicos convencionales o celulares, mientras que el servidor puede ser por software como el componente de Windows RAS o por hardware como productos IBM.

Módem

Es un dispositivo que codifica y decodifica (transforma) las señales digitales a analógicas y viceversa para ser utilizadas por los ordenadores en señales apropiadas para viajar a través de redes de telefonía.

Gateway o Pasarela

Son dispositivos usados para interconectar dos redes de diferente protocolo, este dispositivo se encarga de interpretar la información dentro de un protocolo para todas sus capas y prepararla para emitirla en otra red con un protocolo totalmente distinto. Un ejemplo podría ser interconectar una red A con TCP-IP a una B con SNA.

Servidores Proxy y Firewall

Un Firewall en Internet es un sistema o grupo de sistemas que impone una política de seguridad entre la organización de red privada y el Internet. El firewall determina cuál de los servicios de red pueden ser accesados dentro de esta por los que están fuera, es decir quién puede entrar para utilizar los recursos de red pertenecientes a la organización. Para que un firewall sea efectivo todo tráfico de información a través del Internet deberá pasar a través del mismo donde podrá ser inspeccionada la información. El firewall podrá únicamente autorizar el paso del tráfico, y el mismo podrá ser inmune a la penetración. “Desafortunadamente, este sistema no puede

ofrecer protección alguna una vez que el agresor lo traspasa o permanece en torno a este[9].

2.2.9. Metodología evaluación de la seguridad de una red[10].

La metodología con la cual se aplicará el desarrollo práctico de esta investigación se basa en los siguientes procesos:

- **Identificar el perímetro de la red.** Tiene por objetivo determinar los elementos de la red sobre los cuales se va a realizar el estudio.
- **Rastreo de dispositivos perimetrales.** Para identificar los equipos accesibles y de sus servicios de red (ejemplo: smtp, http).
- **Identificación de los servicios de red**. Para lo cual se debe utilizar herramientas que permitan identificar las aplicaciones, así como la plataforma y versión de los servicios accesibles.
- Investigación de vulnerabilidades conocidas.
- Realización de pruebas de bajo nivel con el fin de identificar direcciones IP internas analizando todas las respuestas ICMP y direcciones de amplia difusión para sub redes.
- Pruebas en busca de vulnerabilidades.

---

[9] Chuck Semeria - 3Com Corp, www.3com.com/nsc/500619

[10] Chris McNab (2004), Network Security Assessment

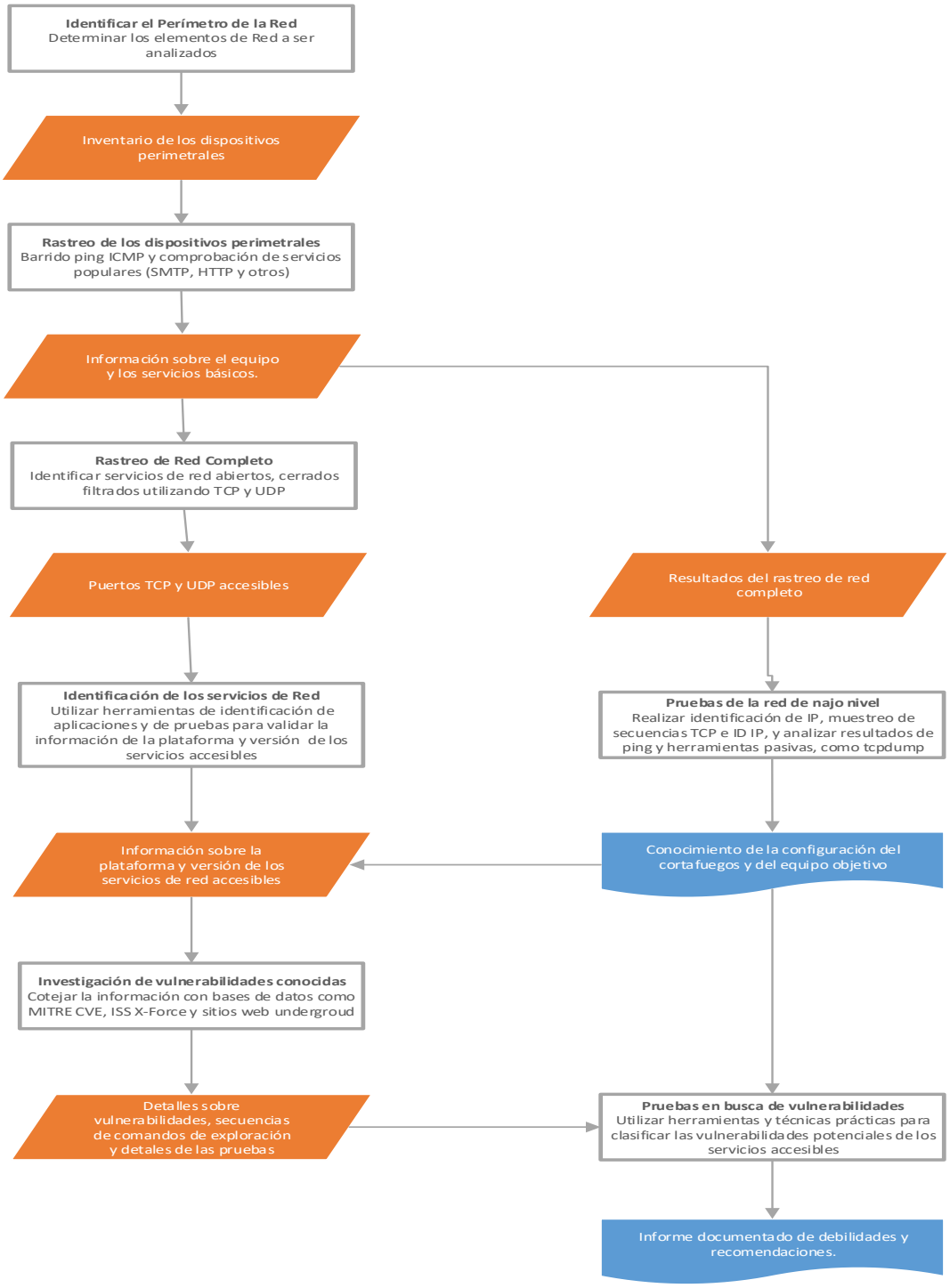


Figura 7. Metodología de evaluación de Red

Fuente: Tesis “Implementación de políticas de seguridad en Red LAN Corporativa”

2.2.10. Escritorios remotos.

Se trata de la interfaz gráfica desde la cual podemos manejar de forma remota un equipo, desde otra terminal ubicada en otro lugar, es decir, conectarnos a un equipo de cómputo que se encuentra en otra ubicación y tomar el control del mismo para poder trabajar, como si estuviéramos enfrente de dicho equipo.

Algunas veces los escritorios remotos son de gran utilidad ya que nos pueden servir desde poder conectarse a equipos de una misma red local poder y prescindir de más de un monitor y periféricos conectados o simplemente la comodidad de administrarlo desde uno solo, hasta iniciar sesión en equipos a los que no se tiene acceso físico a través de la red, y trabajar con ellos como uno local.

Y otra de las funciones que tienen en la actualidad es la de brindar soporte técnico a usuarios de equipos de cómputo, ya que facilita esta labor a los administradores de las redes de datos.

2.2.11. Software de acceso remoto.

Actualmente podemos encontrar varios tipos de software de conexión remota los cuales nos permiten configurar el escritorio remoto de algún equipo de cómputo para poder conectarnos a él, y tomar el control del mismo para poder trabajar.

Entre el software más común de acceso remoto en estos días tenemos los siguientes:

a. Team Viewer.

Team Viewer es una aplicación intuitiva, rápida y segura para controlar un equipo de cómputo de forma remota e incluso llevar a cabo reuniones en línea. Como solución todo en uno, Team Viewer puede utilizarse:

- Para ofrecer soporte remoto a compañeros, amigos o clientes.
- Para mostrar su escritorio en reuniones, presentaciones o colaboraciones.
- Para establecer una conexión entre ordenadores con distintos sistemas operativos.
- Team Viewer se ejecuta bajo Windows, Mac OS o Linux.

Tabla 6. Requerimientos de Team Viewer

Requerimientos				
Team Viewer	Windows	Linux	Código Libre, Licencia Gratuita	Pago de Licencia
Sistema operativo	Win98/98SE/Me/NT/ XP/2003/Vista/7/8/10	Cualquier distribución	Licencia Gratuita sin fines de lucro	Opcional, permite contar con características adicionales
Conexión a internet	Opcional, permite contar con características adicionales y permite conectarse a uno de nuestros equipos desde una red externa.			

Fuente: Elaboración propia.

b. LogMeIn.

LogMeIn sirve para tener acceso remoto a tu equipo de cómputo, o al de algún conocido o cliente que necesite asistencia, de forma muy fácil y práctica.

Una vez conectado con el equipo remoto, podrás controlar su ratón y teclado, pero además cuentas con algunas prácticas herramientas.

Su completo menú de control se maneja completamente desde el navegador (comprobado en Firefox e Internet Explorer).

Tabla 7. Requerimientos de LogMeIn

Requerimientos				
LogMeIn	Windows	Linux	Código Libre, Licencia Gratuita	Pago de Licencia
Sistema operativo	Win98/98SE/Me/NT/ XP/2003/Vista/7/8/10	No hay versión para Linux	Licencia gratuita previo registro. Versión Free con algunas limitaciones.	Pago de licencia para obtener la versión completa.
Conexión a internet	Necesaria, para poder conectarse a un equipo de cómputo ya sea en la red local de una red externa.			

Fuente: Elaboración propia.

c. VNC.

VNC es un protocolo para el acceso remoto a las interfaces gráficas de usuario. Su significado es Virtual Network Computing, se basa en concepto de framebuffer remoto o RFB. Este simplemente permite ver e interactuar con un ordenador (servidor VNC), usando un programa simple en otra

computadora (Visor VNC) en cualquier lugar desde el internet, debido a que funciona a nivel de framebuffer es potencialmente aplicable a todos los sistemas operativos.

d. TightVNC

Es un Paquete gratuito de software de control remoto. Con TightVNC, se puede ver el escritorio de una máquina remota y controlarlo con el mouse, como los teclados locales, al igual que lo haría sentado en el frente de ese equipo. Este servidor puede ser muy útil no solo a los administradores de sistemas si no a los servicios de apoyo, pero para todos los usuarios que quieren beneficiarse de este servicio al igual que otros sistemas de VNC.

Además, es un proyecto defendido por Constantin Kaplinsky. Muchas otras personas como empresas participan en el desarrollo, prueba y soporte. Está conformada por dos partes: El servidor el cual comparte la pantalla de la máquina que se está ejecutando, el visor que muestra la pantalla remota recibida por el servidor.

- Libre (publicado bajo Licencia Pública General de GNU), tanto para uso personal y comercial, con el código fuente completo
- Útil en la administración, soporte técnico, educación, y para muchos otros propósitos.
- Multiplataforma, disponible para Windows y Unix, con el cliente Java incluido.

- Compatible con el software VNC estándar, conforme a las especificaciones del protocolo RFB.

Beneficios de Herramienta TightVNC.

- Reducir sus gastos y ahorrar su tiempo en viajes.
- Ayudar a sus amigos y familiares para resolver problemas con sus equipos de forma remota.
- Asegurarse de que nada malo está sucediendo en sus equipos cuando usted está ausente.
- Ser útil para el aprendizaje a distancia y soporte al cliente remoto.

Compatibilidad e Interoperabilidad.

TightVNC es totalmente compatible con el protocolo RFB estándar utilizado, así que usted puede utilizar el visor de la herramienta con el servidor VNC estándar y viceversa. Pero tenga en cuenta que las mejoras de protocolos implementados funcionarán sólo si estas son apoyadas a ambos lados de la conexión.

Características de TightVNC

- Las transferencias de archivos en versiones para Windows. Puede subir archivos desde el equipo local para el TightVNC Server, y descargar archivos desde el servidor a su computadora.
- Soporte para el conductor espejo de vídeo (Windows 2000 y superiores). TightVNC Server puede utilizar el controlador espejo DFMirage para detectar las actualizaciones de pantalla y los datos

de los píxeles de agarre de una manera muy eficiente, ahorro de ciclos de procesador para otras aplicaciones.

- Escalado del escritorio remoto (visor para Windows y Java espectador). Puede ver el escritorio remoto en su totalidad en una pantalla de tamaño más pequeño, o se puede acercar la imagen para ver la pantalla remota en más detalles.
- Eficiente codificación "Tight" con opción de compresión JPEG. Nueva codificación Tight está optimizado para conexiones lentas como de velocidad media, por lo tanto, genera mucho menos tráfico en comparación con codificaciones VNC tradicionales. A diferencia de otras codificaciones, la codificación apretada es configurable a través de los niveles de compresión y ajuste de calidad de imagen JPEG.
- Acceso del navegador web actualizado. TightVNC incluye un visor de Java muy mejorado con soporte completo para la codificación apretada, el modo de color de 24 bits, y más. El visor de applets Java se puede acceder a través de una función de servidor HTTP como en el estándar VNC.
- Soporte para dos contraseñas, control total, como de lectura. El servidor permite o no, el teclado remoto y eventos de mouse en función de los cuales se utilizó la contraseña para la autenticación.

- Tunelización automática SSH en Unix. La versión Unix de TightVNC Viewer puede conexiones de túnel a través de SSH automáticamente utilizando SSH local de instalación de cliente / OpenSSH.
- Visualización y manejo de escritorios remotos, esta es la funcionalidad principal de la aplicación. TightVNC permite visualizar el escritorio de otra máquina de forma remota desde nuestro propio equipo, además de tomar el control del mismo si así lo deseamos. De esta forma, esta funcionalidad facilita la asistencia técnica a distancia, entre otros aspectos.

Velocidad de ejecución

La velocidad de ejecución y de uso es, en general fluido. En la mayoría de los casos, la fluidez dependerá de las características y el estado de la red, al acceder a un equipo remoto a través de la red misma.

Usabilidad.

El diseño de la interfaz es sencillo, todo lo que puede pedirse para una aplicación de estas características. Puesto que el principal objetivo de TightVNC es la visualización y el manejo de un escritorio remoto, la mayor parte del tiempo que manipulemos en el uso del programa se efectuará operando las interfaces del equipo remoto.

La herramienta dispone de una ventana para la configuración de las preferencias de la conexión. Esta ventana es de diseño sencillo y está

estructuradas de manera que la configuración resulte lo más intuitiva posible para el usuario. Los parámetros a especificar son de fácil comprensión y evita que el usuario tenga complicaciones.

Durante la conexión, se despliega una barra con botones en la parte superior que permite acceder a las acciones disponibles durante la monitorización, tales como zoom, envío de Ctrl+Alt+Del o la funcionalidad de grabación de vídeo. De esta forma, el acceso a las opciones del programa es rápido y sencillo.

Facilidad de uso.

Puesto que es posible realizar una conexión con un equipo remoto, tan sólo especificando la dirección IP del equipo, la facilidad de uso del programa es máxima. Además, el resto de opciones que aparecen en las ventanas de configuración, permiten que se establezcan de forma rápida las preferencias para la conexión a realizar.

e. UltraVNC

Software de acceso remoto de computadoras, que pueden mostrar la pantalla de otra computadora/ a través de Internet o de la red) en su pantalla. El programa permite utilizar el mouse y el teclado para controlar la otra computadora, como si estuviera sentado en frente de ella, desde su ubicación actual. Para este evento se debe de ejecutar un servidor VNC en

el equipo que comparte el escritorio de su pc y ejecutar un cliente VNC en el equipo que tenga acceso al escritorio compartido.

Tabla 8. Requisitos de UltraVNC

Requerimientos				
UltraVNC	Windows	Linux	Código Libre, Licencia Gratuita	Pago de Licencia
Sistema operativo	Win98/98SE/Me/NT/XP/ 2003/Vista/7/8/10	Cualquier distribución	Licencia Gratuita sin fines de lucro	Opcional, permite contar con características adicionales
Conexión a internet	Opcional, permite contar con características adicionales y permite conectarse a uno de nuestros equipos desde una red externa.			

Fuente: Elaboración propia.

f. Vinagre

Es un visor de escritorio remoto para GNOME, licenciado bajo GPL (licencia pública general de GNU), trabaja bajo sistema operativo Unix. Vinagre tiene varias características, como la posibilidad de conectarse a varios servidores simultáneamente y cambiar entre ellos usando pestaña. GNOME ha abarcado Vinagre en su instalación por defecto como su cliente oficial de VNC, y es el programa establecido que se utiliza para la opción de escritorio compartido que ofrece la empatía cliente de mensajería instantánea.

2.2.12. Comparativa de funcionalidades entre servidores VNC

Según la investigación que realizo, se ha centrado en esta temática y ha seleccionado, de entre las diversas soluciones existentes en el mercado, las herramientas de control remoto Vinagre, TightVNC y UltraVNC.

Además, estas tres herramientas han superado positivamente el informe establecido por la Metodología de Análisis de Confianza para proyectos de Software Libre, la cual fue desarrollada por el CESLCAM, para evaluar si el proyecto tiene la calidad necesaria para ser recomendada desde el Centro.

Uno de los aspectos a tener más en cuenta será la fluidez con que se realiza la conexión entre ambos equipos, cliente y servidor. Aquí cabe destacar UltraVNC sobre el resto, puesto que el retardo entre las acciones realizadas en el equipo cliente y el despliegue de las mismas en el equipo servidor es mínimo. A pesar de esto, Vinagre y TightVNC no experimentan un retardo excesivo, aunque aquí Vinagre presenta un retardo sensiblemente superior al resto.

Para finalizar, destacamos los puntos fuertes de cada una de las herramientas:

- Vinagre: versatilidad y completitud, por ser la más variada y completa en cuanto a funcionalidad.
- TightVNC: compatibilidad y portabilidad, por ser la más compatible en relación al número de plataformas en las que puede correr al

estar su visor implementado en Java. Además, este visor es completamente portable, no habiendo necesidad de instalarlo para ser utilizado.

- UltraVNC: ligereza, por ser la que funciona con más fluidez[11].

Tabla 9. Comparativa de Herramientas.

Características del servidor	TightVNC	Vinagr	UltraVN
Compartir sólo una ventana determinada	NO	NO	SI
Compartir sólo ventana activa	NO	NO	SI
Compartir sólo terminales de consola	NO	NO	SI
Compartir sólo ventana bajo evento	NO	NO	SI
Habilitar/Deshabilitar transferencia de archivos	SI	NO	SI
Modo espectador obligado	SI	SI	SI
Ocultar fondo de escritorio	SI	NO	SI
Configurar lista de acceso	SI	NO	NO
Establecer contraseña	SI	SI	SI
Establecer TimeOut	SI	NO	SI
Funcionalidad del visor	TightVNC	Vinagr	UltraVN
Visualización de escritorios remotos	SI	SI	SI
Control de escritorios remotos	SI	SI	SI
Ajustar ventana	SI	SI	NO
Modo de pantalla completa	NO	SI	SI
Conexiones inversas	NO	SI	NO
Conexión con varios equipos en una misma sesión	NO	SI	NO
Añadir conexiones a marcadores	NO	SI	NO
Rastreo de equipos en la red	NO	SI	NO
Capturas de pantalla remota	NO	SI	NO
Grabación en video	SI	NO	NO
Actualizar pantalla	SI	NO	SI
Modo Zoom	SI	NO	NO

[11] http://www.bilib.es/fileadmin/user_upload/estudio-bilib-comparativa-control- remoto.pdf

Información de estado de la conexión	NO	NO	SI
Envió de tecla de inicio	SI	NO	SI
Envió de Ctrl+Alt+Supr	SI	SI	SI
Envió de combinación de teclas personalizadas	NO	NO	SI

Fuente: Elaboración propia.

2.2.13. Comparativa de software de acceso remoto.

Herramienta	RAM	Procesador	Espacio	Sistema Operativo	Tipo de Licencia	Conexión
Team Viewer	128MB	400MHz	15MB	Windows 2000 o superior	Libre y Pagada	Vía Internet
LogMeIn				Solo necesita navegadores	Libre y Pagada	Vía Red o Internet
VNC	512MB	2.4GHz	1GB	Windows XP o superior y Linux	Libre y Pagada	Vía Internet

Fuente: Elaboración propia.

Mediante un análisis y estudio se determinó realizar la propuesta con el software TightVNC que es una variante de VNC.

2.2.14. Ética Informática.

Concepto de ética.

La ética es la teoría o la ciencia del comportamiento moral de los hombres en sociedad, es decir, es la ciencia de una forma específica de conducta humana.

La palabra moral procede del latín mos o mores, costumbre o costumbres, en el sentido de conjunto de normas o reglas adquiridas por hábito. La moral tiene que ver así con el comportamiento adquirido.

La palabra ética proviene del griego ethos, que significa análogamente modo de ser o carácter en cuanto a forma de vida también adquirida.

2.2.15. Ética Profesional.

Los seres humanos no solo deben tener presentes todos los conceptos y principios que involucran los términos ética y moral, pues es muy importante que al hablar de profesionistas se tenga presente el elemento ético, ya que es un componente inseparable de la actuación profesional, pues no se debe olvidar que toda profesión no solo es una manera de ganarse la vida y de realizarse personalmente, sino que también tiene un fin social, que consiste en servir adecuadamente a cada una de las necesidades que la sociedad debe satisfacer para obtener el bien común.

Por lo anterior es muy importante contar con un código de ética en cada profesión, que permita poner en manifiesto una serie de cualidades

morales (honestidad intelectual, desinterés personal, decisión en la defensa de la verdad, etc.) cuya posesión asegure una mejor realización del objetivo fundamental (la búsqueda de la verdad) que preside la actividad de cada actividad.

Por ello los códigos de ética deben inculcar en lo estudiantes o profesionistas un patrimonio de valores, es decir, una formación ética, que oriente al profesionista a ejercer una profesión de forma adecuada.

Aspectos que considerar de la ética profesional:

- El profesionista siempre debe de tener presente el elemento ético.
- La ética es un componente inseparable de la actividad profesional.
- Toda profesión tiene un fin social, por lo que debe de tomarse en cuenta la ética profesional.
- Con la actividad profesional siempre se debe de obtener un bien común.
- Contar con un código de ética para cada profesión.
- Poner en manifiesto las cualidades de los profesionistas.
- Los códigos de ética deben inculcar los valores.
- Una formación ética orientara al profesionista a ejercer su profesión de manera adecuada.

2.3. DEFINICIONES CONCEPTUALES.

- Cliente / Servidor: Es un modelo de aplicación distribuida en la que el trabajo se reparten entre los proveedores de recursos o servicios, llamados servidores, y los solicitantes, llamados clientes. En esta arquitectura la capacidad de proceso está distribuida entre los clientes como los servidores, aunque son más importante las ventajas de tipo organizativo debido a la centralización de la gestión de la información y separación de responsabilidades, lo que facilita la clarificación del diseño del sistema.

- VNC: Significativo de las siglas Virtual Network Computing (Computación Virtual en Red), es un programa de software libre basado en una arquitectura cliente / Servidor, lo cual permite tomar el control del ordenador servidor remotamente a través de un ordenador cliente.

- Software: Se considera que el software es la parte lógico e intangible de un ordenador, en otro concepto de software son todas las aplicaciones informáticas que viene o se instala en un computador, como los procesadores de textos, los procesadores de cálculo y los editores de imágenes.

- Tecnología de la información: El término se lo utiliza comúnmente como sinónimo de ordenadores y redes informáticas para almacenar, manipular y recuperar datos, también abarca otras informaciones tecnológicas.

- Protocolo: Conjunto de reglas y ceremoniales que deben de seguirse en ciertos actos, normas de cortesía que deben de seguirse.

- TCP / IP: Significativo de las siglas (Transmission Control Protocol / Internet Protocol), es un lenguaje básico de comunicación o protocolo de internet, también se puede utilizar como un protocolo de comunicaciones en una red privada.

- RDP: Significativo de las siglas (Remote Desktop Protocol), es el protocolo de escritorio remoto de Microsoft, ofrece visualización grafica e introducción capacidades remotas a otros ordenadores través de una conexión de red.

- WinSCP: Significativo de las siglas (Windows Secure CoPy), es un software de código abierto utiliza los siguientes protocolos SFTP, SCP, FTP cliente para Windows, su función principal es la

transferencia segura de archivos entre una red local o redes remotas.

- SSH: Significativo de las siglas (Secure Shell), es un protocolo que facilita las comunicaciones seguras entre dos sistemas usando una arquitectura cliente/servidor, permite a los usuarios conectarse a un host remotamente.

2.4. MINISTERIO PÚBLICO – DISTRITO FISCAL E HUÁNUCO

2.4.1. DESCRIPCIÓN.

Es el organismo constitucional autónomo creado por la Constitución Política del Perú en 1979, con la misión fundamental de defender la legalidad y los Derechos Humanos. Sus actividades al servicio de la ciudadanía las inició formalmente el 12 de mayo de 1981.

2.4.2. RESEÑA HISTÓRICA.

Como el antecesor más remoto del Ministerio Público se considera al funcionario que defendía la jurisdicción y los intereses de la hacienda real en los Tribunales del Consejo de Indias, cuya función fue establecida en 1542 al instalarse la Real Audiencia de Lima y después la del Cuzco.

La asimilación de los miembros del Ministerio Público al aparato judicial se mantuvo durante la época republicana. Desde la instalación de la Alta

Cámara de Justicia y la creación de la Corte Suprema (1825) el Ministerio Público siempre estuvo al lado de los jueces. Los Reglamentos de Organización de los Tribunales no lo mencionaban como un organismo.

En la evolución legislativa del Estado Peruano, constitucionalmente no fue regulada la actividad del Ministerio Público en forma clara y nítida hasta la Constitución de 1979, según un estudio del doctor Alejandro Espino Méndez, Fiscal Provincial Penal de Lima.

2.4.3. DATOS GENERALES.

- Razón Social: Ministerio Público
- Sector: Público
- Actividad Específica: Legalidad del Derecho
- Dirección: Jr. Dos de Mayo N.º 1155

2.4.4. VISIÓN Y MISIÓN.

VISIÓN

Ser reconocido nacional e internacionalmente como una institución moderna y confiable, consolidada por la excelencia de sus servicios y el adecuado soporte médico, legal y forense; que contribuye a una recta y real administración de justicia y de esta manera a la convivencia pacífica y al desarrollo de la sociedad.

MISIÓN

Defender la legalidad y los intereses públicos tutelados por la ley; prevenir y perseguir el delito; defender a la sociedad, al menor y a la familia en juicio; velar por la independencia de los órganos jurisdiccionales y por la recta administración de justicia.

2.4.5. VALORES.

El Ministerio Público, persigue y fomenta la vigencia de un sistema de valores, que rija el accionar de los servidores que conforman la institución, la práctica de estos valores contribuirá a la consolidación y fortalecimiento de una institución eficaz, eficiente autónoma e independiente. Entre estos valores de práctica cotidiana se pueden mencionar:

- Lealtad de la constitución Política del Estado y la Institución
- Justicia
- Vocación de Servicio
- Respeto y Dedicación
- Honradez
- Honestidad
- Imparcialidad
- Integridad y Objetividad
- Transparencia
- Puntualidad

- Responsabilidad
- Igualdad de Género

2.4.6. ESTRUCTURA ORGANIZACIONAL.

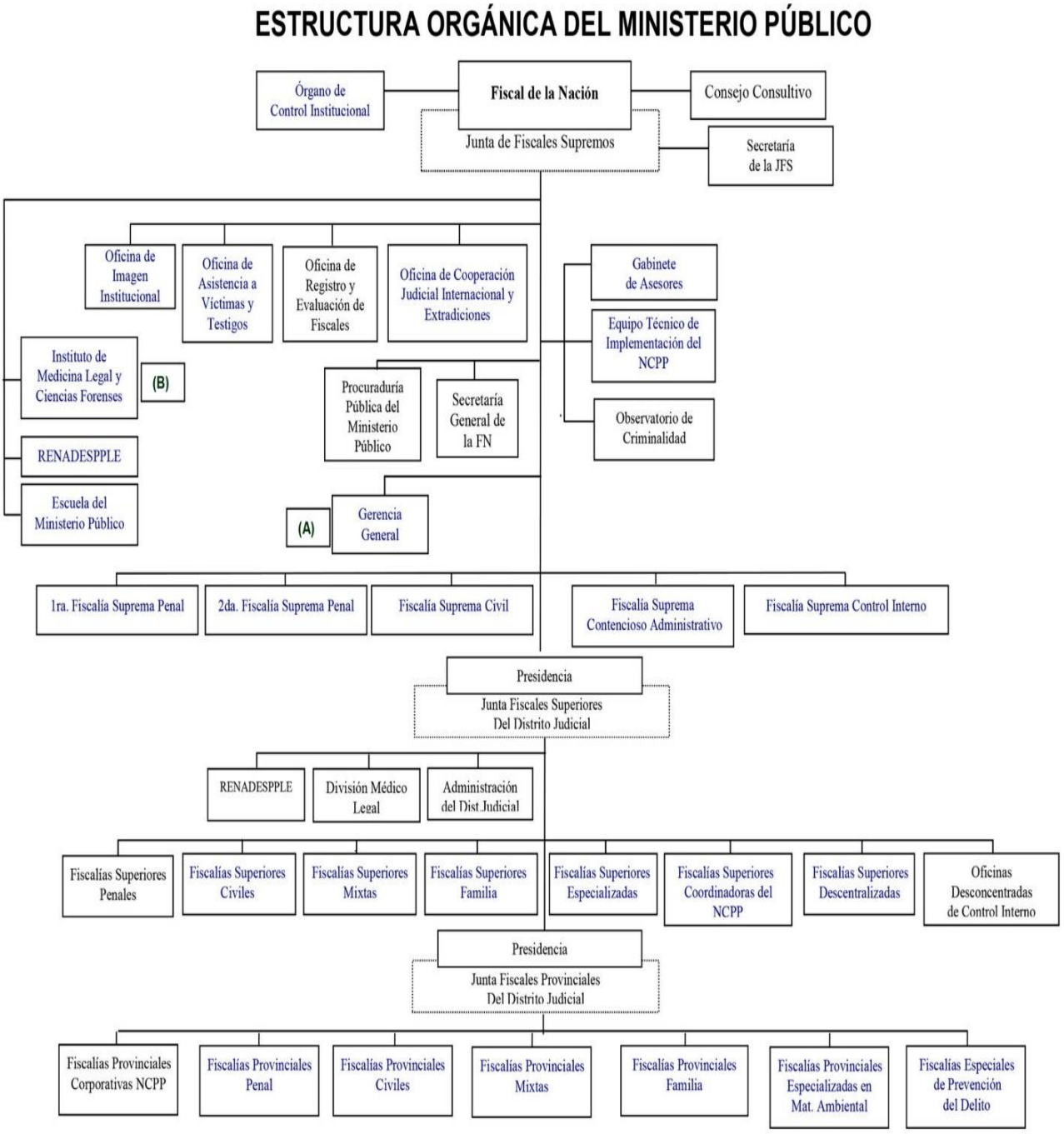


Figura 8. Organigrama del Ministerio Público

Fuente: Pagina del Ministerio Público: http://www.mpfn.gob.pe/?K=363

2.4.7. OFICINA DE TECNOLOGÍAS DE INFORMACIÓN

a. Funciones[12]

- Llevar y tener en custodia los archivos de respaldo de los sistemas instalados.
- Deshabilitar todas las disqueteras de forma lógica.
- Actualizar periódicamente los programas de servido al usuario (antivirus).
- Programar, en coordinación con el Administrador del Distrito Judicial, el Plan de Mantenimiento de los equipos y sistemas informáticos.
- Custodiar las llaves de los equipos de cómputo debiendo entregar una copia de las mismas al Administrador del Distrito Judicial y verificar que los sellos de garantía se encuentren intactas o que estos hayan sido puestos una vez concluidas los trabajos de reparación o mantenimiento realizado por servidos externos, así como la colocación de los candadas de seguridad.
- Coordinar con el Administrador del Distrito Judicial el reporte de los equipos de cómputo malogrados el cual será remitido a la Gerencia de Redes, Soporte Técnico y Comunicaciones de la Gerencia Central de Tecnologías de la información.

---

[12] MOF del Misterio Público.

- Velar que los usuarios respeten las normas de uso de los equipos y sistemas de cómputo, así como de su limpieza y mantenimiento.
- Recepcionar, en coordinación con el Administrador del Distrito Judicial, los nuevos equipos de cómputo, debiendo verificar que las cantidades y los numeras de serie coincidan con los registrados en la guía de remisión.
- Encargarse de la distribución de los equipos de cómputo en coordinación con el Administrador del Distrito Judicial, previa autorización del Fiscal Superior Decano.
- Garantizar la seguridad de la información en la red, aplicando las políticas de seguridad dadas para la Gerencia Central de Tecnología de la Información.
- Organizar y aplicar los procedimientos de back up de la información que se maneje en el Distrito Judicial.
- Mantener operativos los servicios de Red LAN en coordinación con la Gerencia de Redes, Sistema Técnico y Comunicaciones.
- Mantener actualizado el inventario de hardware, software y equipos de comunicación del Distrito Judicial, debiendo remitir una copia del mismo a la Gerencia de Redes, Soporte Técnico y Comunicaciones de la Gerencia Central de Tecnologías de la Información.
- Administrar el correcto funcionamiento de los equipos informáticos, determinando los orígenes de las posibles fallas de estos y/o de los

sistemas de cómputo, dirección ando el reporte a la Gerencia correspondiente de la Gerencia Central de Tecnologías de la Información.

- Coordinar con el Administrador del Distrito Judicial el requerimiento de equipos informáticos nuevos y accesorios informáticos, formulando la propuesta Plan de Adquisiciones del Distrito Judicial.
- Coordinar con las Gerencias de la Gerencia Central de Tecnologías de la Información para diferenciar y/o solucionar los problemas ocasionados por errores en el funcionamiento de los programas de cómputo, sistemas autorizados y confeccionados a la medida para la Institución.
- Realizar las gestiones necesarias, en coordinación con el Administrador del Distrito Judicial, en caso de problemas técnicos y/o administrativos ante la Gerencia de Redes, Sistema Técnico y Comunicaciones.
- Informar periódicamente a la Gerencia de Redes, Soporte Técnico y Comunicaciones las actividades y/o sucesos presentados en el servicio de red.
- Comunicar todos los viernes la conformidad de la operatividad del servicio y recepción de los correos, vía correo electrónico, al personal designado por la Gerencia de Redes, Sistema Técnico y Comunicaciones.

- Realizar copia de seguridad diaria de la información y comprobar el estado de la copia en forma mensual, estableciendo un cronograma de trabajo.
- Reportar al Administrador del Distrito Judicial, la situación actual de las cintas y prever el cambio de aquellas que se encuentren no operativas.
- Guardar las cintas físicas de la copia del. mes, informando sobre su contenido e indicando las pautas necesarias para el cuidado de las mismas al Administrador del Distrito Judicial.
- Coordinar con el Administrador del Distrito Judicial la autorización del ingreso de bienes o equipos de cómputo, que no sean de propiedad del Ministerio Público.
- Realizar los servicios de asistencia técnica sólo a los equipos de la institución.
- Mantener informado de sus actividades al Administrador del Distrito Judicial,
- Las demás funciones que le asigne el Administrador del Distrito Judicial.

b. Línea de autoridad.[13]

- El coordinador de tecnologías de información depende directamente de Administrador del Distrito Judicial.

c. Nivel de responsabilidad.[14]

- Cumplir y hacer cumplir las políticas, reglamentos, directivas y procedimientos relacionados con la Administración del Distrito Judicial, así como demás normas internas.
- Responsable de la información almacenada en el servidor de información a su cargo.
- Responsable de garantizar que todos los servicios ofrecidos por la red sean únicamente para uso del personal de la institución (Fiscales, funcionarios, Profesionales de la Salud y Personal Administrativo).
- Garantizar que el personal autorizado para abrir los equipos de cómputo sean técnicos acreditados por los proveedores.

---

[13] MOF de Ministerio Publico.

[14] MOF de Ministerio Publico.

d. Nivel de coordinación.[15]

- Realizar coordinaciones con cada una de las diferentes unidades orgánicas de la Institución relacionadas con el hacer del Distrito Judicial, así como las Gerencias de la Gerencia central de tecnología de la información.

e. Personal.

Tabla 10. Personal de la Oficina de Tecnologías de Información

APELLIDOS Y NOMBRES	**Cargo**
RODRIGUEZ GONZALEZ, Denisse Jessica	Especialista administrativo
GIRON TOVAR, Hernando Rosmel	Especialista administrativo (Coordinador)

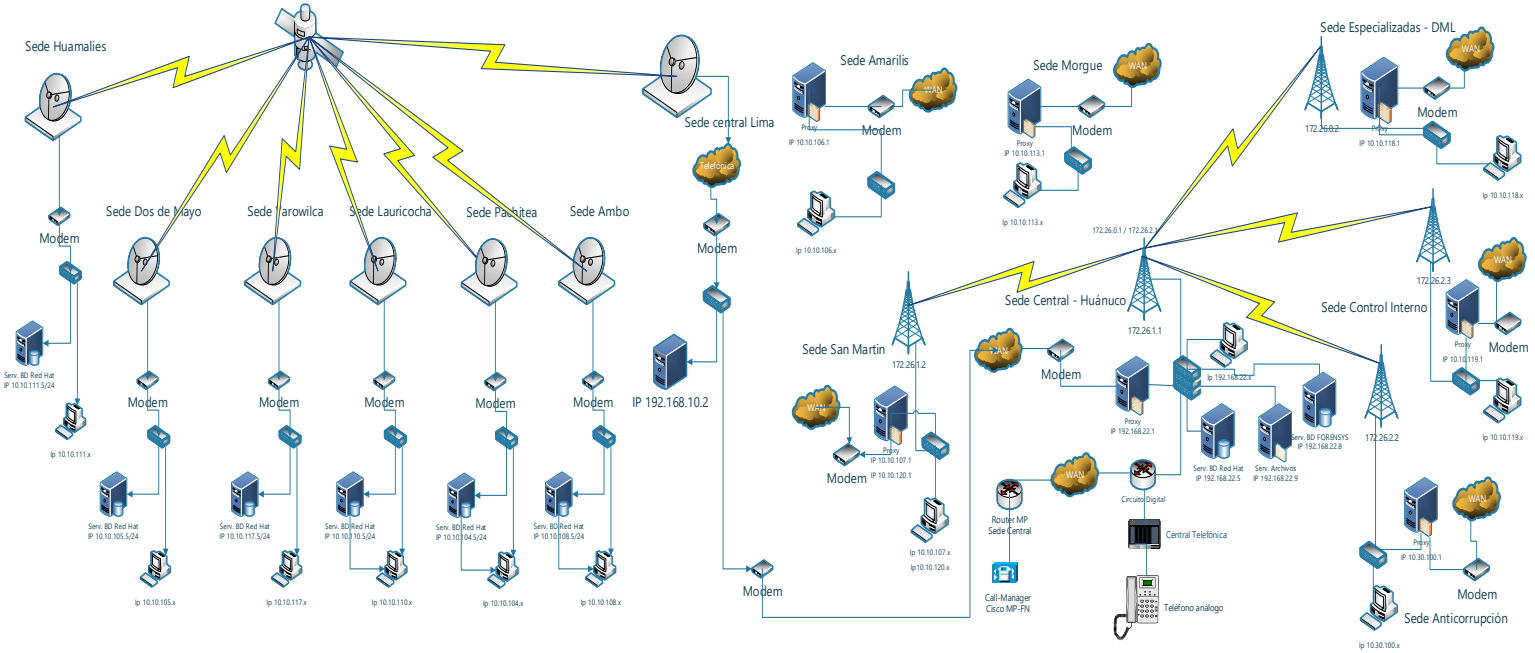
Fuente: Elaboración propia.

[15] MOF de Ministerio Publico.

f. Infraestructura tecnológica.

- Topología de Red del Ministerio Público - Huánuco

Figura 9. Topología de Red del Ministerio Público – Huánuco



Fuente: Elaboración propia.

- Inventario de software.

Tabla 11. Software

NOMBRE DE SOFTWARE	TIPO DE LICENCIA	PLATAFORMA	TIPO DE SOFTWARE	STATUS	N° MAQUINAS
Windows	Comercial	Windows 7	Sistema Operativo	Bueno	837
Open Office	GPL	Windows 7	Aplicación	Bueno	815
Mcafee	Comercial	Windows 7	Aplicación	Bueno	837
Cliente ACE (Sybase)	Comercial	Windows 7	Aplicación	Bueno	854
7-Zip	GPL	Windows 7	Aplicación	Bueno	854
SPIJ	Red	Windows 7	Aplicación	Bueno	22
SPIJ	Mono Usuario	Windows 7	Aplicación	Bueno	20
Debian	GPL	Linux	Sistema Operativo	Bueno	20
Windows	Comercial	Windows Server 2008	Sistema Operativo	Bueno	8
Red Hat	Comercial	Red Hat	Sistema Operativo	Bueno	2
Novell	Comercial	Novell	Sistema Operativo	malo	1
Windows	Comercial	Windows XP	Sistema Operativo	Regular	17
Microsoft Office 2010	Comercial	Windows 7	Aplicación	Bueno	22

Fuente: Elaboración propia

- Inventario de hardware.

Tabla 12. Unidad Central de Proceso

CPU								PROCESADORES						
FUNCION DE SERVIDOR														
BASE DE DATOS	ARCHIVOS	PROXY	SASPRO	VPN										
						1	952	2	19	74	79	129	27	634
0	0	0	0	0	0	1	952	2	19	74	79	129	27	634
TOTAL, CPU														953

Fuente: Elaboración propia.

Tabla 13. Servidores

SERVIDOR									PROCESADORES	
	BASE DE DATOS							ACTULIZACIONES		
	FORENSYS	DICEMEL	SIGA	SIATF	SGF	SIAF	PRINCIPAL TODAS LAS BD PRINCIPAL	WASUS		
2	1	1		1	1		9		31	1
2	1	1	0	1	1	0	9	0	31	1
TOTAL, DE SERVIDORES										15

Fuente: Elaboración propia.

Tabla 14. Laptops

TOTAL, LAPTOP	PROCESADORES				
83	2	44	1	25	11
83	2	44	1	25	11
TOTAL, DE LAPTOPS					83

Fuente: Elaboración propia.

III. METODOLOGÍA DE INVESTIGACIÓN

3.1. TIPO DE INVESTIGACIÓN.

La investigación aplicada o tecnológica, aquella que se realiza sobre concretos específicos, de carácter netamente utilitarios, para lo cual se realiza sobre hechos específicos, de carácter netamente utilitarios, para lo cual se vale de conocimiento teórico que hagan posible explicar estos fenómenos, los resultados de este tipo de investigación permite al hombre conocer y dominar los fenómenos que lo circundad.

(Ñaupas Paitán, Mejía Meja, Novoa Ramírez, & Villagómez Paucar, 2011).

Es aquella que está orientada a resolver objetivamente los problemas de los procesos, de producción, distribución circulación y consumos de bienes y servicios, de cualquier actividad humana, principalmente de tipo industrial, comercial comunicacional, etc.

La investigación tecnológica o aplicada fue desarrollada en la presente tesis, ya que gracias a ella se puede determinar si es eficiente, ineficiente, eficaz o ineficaz la implementación del software para el soporte informático remoto.

3.1.1. Enfoque.

(Hernández Sampieri, Fernández Collado, & Baptista Lucio, 2006) Enfoque cuantitativo usa la recolección de datos para probar hipótesis, con base en la medición numérica y análisis estadístico, para establecer patrones de comportamiento y probar teorías.

En este trabajo se empleó una modalidad de investigación orientada al aspecto cuantitativo, por cuanto se asume una realidad estable, no obstante, también se requiere una caracterización de los elementos que integran la solución propuesta.

3.1.2. Alcance o nivel.

(PICOYA HERMOSA, 1987) La investigación en tecnologías formales comprende los campos de la programación de computadoras, análisis de sistemas, investigación operativa y cibernética. En este campo que se han desarrollado la tecnología algorítmica, debido a que se fundamentan en teorías matemáticas. Las disciplinas que sustentan estas investigaciones son el cálculo de probabilidades, la teoría de grafos, la teoría de juegos, el álgebra de Boole, etc.

3.1.3. Diseño

(Kerlinger, 1991)El experimento es una investigación científica en el cual el investigador manipula o controla una o más variables independientes y observa a la variable o variables dependientes, en busca de una variación concomitante con la manipulación de variables independientes.

(Ñaupas Paitán, Mejía Meja, Novoa Ramírez, & Villagómez Paucar, 2011) Tipo de diseños experimentos puros. Son características de control aleatorizado, manipulación, observación y medición, aunque la última característica a veces sea incompleta.

Diseño de dos grupos aleatorizados, con preprueba-postprueba.

Tabla 15.Diseño de dos grupos aleatorizados, con preprueba - postprueba

	Grupo	Preprueba	Variable Independiente	Postprueba
R	E	O_1	X	O_2
R	C	O_1		O_3

Fuente: Elaboración propia.

- E: grupo experimental aleatorio.
- C: grupo de control aleatorio.
- O_i : Observación i.
- La comparación de las Postprueba de ambos grupos (O_2 y O_3) no indica si hubo o no efecto de la manipulación.

- La adición de la Preprueba ofrece dos ventajas: primera, las puntuaciones de las Preprueba sirven para fines de control en el experimento, pues al compararse las Preprueba de los grupos se evalúa qué tan adecuada fue la asignación aleatoria, lo cual es conveniente con grupos pequeños. En grupos grandes la técnica de distribución aleatoria funciona, pero cuando tenemos grupos de 15 personas o menos no está de más evaluar qué tanto funcionó la asignación al azar. La segunda ventaja reside en que es posible analizar el puntaje-ganancia de cada grupo (la diferencia entre las puntuaciones de la Preprueba y la Postprueba).

3.2. POBLACIÓN Y MUESTRA.

3.2.1. Determinación de la población.

El Ministerio Público – Distrito Fiscal de Huánuco cuenta con un personal de 787 personal administrativo y jurídico.

En total se tiene 124 fiscales y 35 administrativos en la ciudad de Huánuco, que en total hacen 159 personas, la cual estratégicamente será mi población.

3.2.2. Selección de muestra.

MARGEN DE ERROR MÁXIMO ADMITIDO	5.0%
TAMAÑO DE LA POBLACIÓN	159

Tamaño para un nivel de confianza del 95% 113

Figura 10. Calculo de tamaño óptimo de una muestra

Fuente: elaboración propia.

El tamaño óptimo de la muestra es 113 personas.

3.3. TÉCNICAS E INSTRUMENTOS DE RECOLECCIÓN.

3.3.1. Técnicas.

- Observación.
- Entrevista.
- La encuesta.

3.3.2. Instrumentos.

- Políticas de seguridad.
- Formato de confidencialidad.
- Fichas de atención por día.
- Ficha de reducción de tiempo
- Ficha de reducción de costos.

3.3.3. Técnicas para el procesamiento de la información.

- Revisión crítica de la información recogida, es decir, limpieza de la información defectuosa, contradictoria incompleta, no pertinente, etcétera.
- Repetición de la recolección en ciertos casos individuales, para corregir fallas de contestación.
- Estudio estadístico de datos para la presentación.

3.3.4. Análisis e interpretación.

El procedimiento para el procesamiento y análisis de los datos será el siguiente:

Calificación y tabulación de datos.

- Tabulación de la información mediante las tablas de resumen de resultados, donde se determinan los casos que encajan en las distintas preguntas.

Análisis e integración de los datos.

- Se relacionará y se comparará los contenidos documentales obtenidos.
- Los procedimientos utilizados para realizar la tabulación, análisis y la interpretación de los datos recopilados serán realizados a través d encuestas y/o entrevistas. Este método permitirá clasificar la información obtenida y analizarla.
- La recolección de información se realizará mediante una investigación de campo que se realizará en el distrito fiscal de Huánuco.

IV. IMPLEMENTACIÓN.

4.1. MANUAL TÉCNICO.

4.1.1. Introducción

El manual técnico es un soporte para los usuarios que requieran saber de los requerimientos que necesita la herramienta para implementar y llevar la administración de los accesos al soporte remoto al personal del Ministerio Público – Distrito Fiscal de Huánuco.

4.1.2. Objetivo

El objetivo principal de este manual es poder ayudar a entender la arquitectura, estructura y funcionamiento de la aplicación de tal manera que los especialistas administrativos adquieran una concepción técnica de la herramienta TightVNC.

4.1.3. Aplicación

Para la implementación del sistema de soporte remoto, utilizamos la siguiente aplicación: TightVNC. Estas aplicaciones son Open Source, libre de modificar, usar y adaptar de acuerdo con las necesidades de la empresa.

Utilizamos como servidores a TightVNC, que a su vez va instalado en cada computadora del personal del Ministerio Público - Distrito Fiscal de Huánuco.

4.1.4. TightVNC Server

Figura 11. TightVNC

Fuente: http://www.tightvnc.com/

a. Requerimientos

Actualmente en el paquete de instalación .MSI, viene incluido el servidor y el Viewer de TightVNC, para esta implementación solo se va a utilizar el servidor. La herramienta permite realizar dos tipos de instalaciones la cuales son:

- Uso del asistente de instalación.
- Instalación silenciosa.

Hardware: TightVNC se ejecuta básicamente en cualquier versión de Windows:

- Windows XP/ Vista/ 7/ 8,8.1,10
- Windows Server 2003/2008/2008 R2/2012

Es compatible con ambos sistemas, ya sea de 64 bits (x64) o 32 bits (x86). TightVNC no tiene requisitos mínimos de espacio en disco o memoria RAM, utiliza tan poco espacio y memoria que se puede ejecutar fácilmente en

cualquier sistema operativo Windows. TightVNC no instala nada en el directorio del sistema.

4.1.5. Uso de asistente de instalación

1. Descargar la aplicación de http://www.tightvnc.com/download.php
2. Copia el archivo de instalación tightvnc.msi al ordenador del usuario y ejecutarlo para iniciar la instalación.

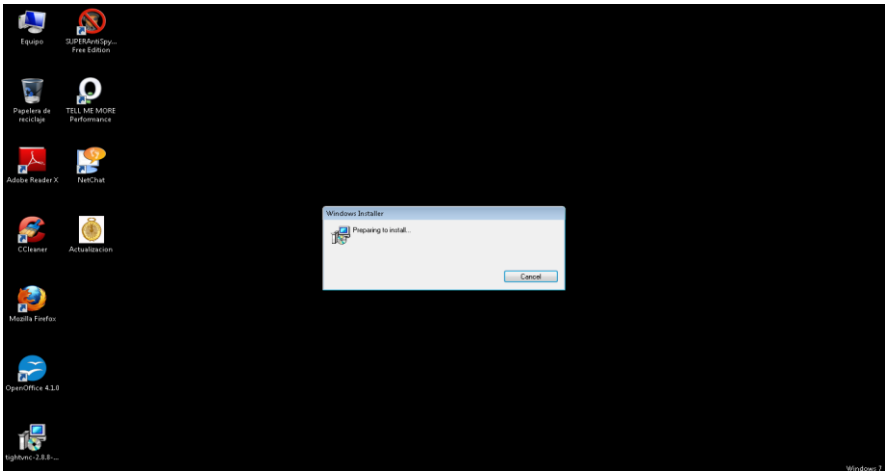


Figura 12. Preparando la instalación.

Fuente: Elaboración propia.

3. Nos muestra la pantalla de Bienvenido de TightVNC. Clic en el botón **Next** (Siguiente).

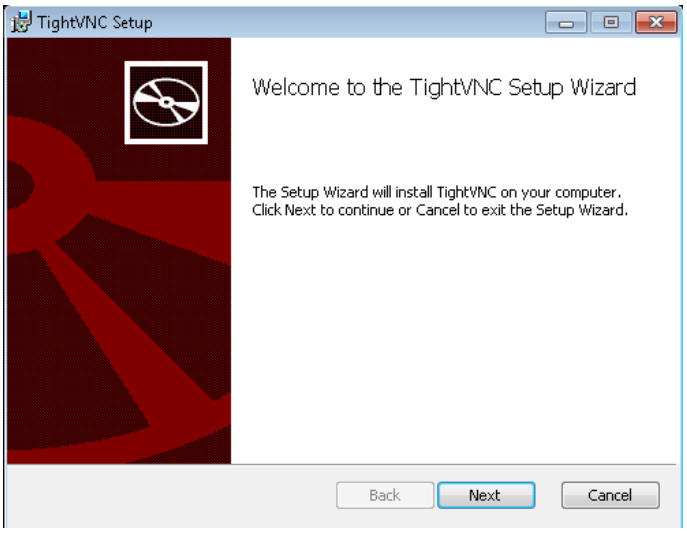


Figura 13. Instalación de TightVNC

Fuente: Elaboración propia.

4. End-User License Agreement. Aceptación de la licencia de usuario final, seleccionar el checkbox de I accept… Yo acepto… y dar clic en el botón Next.

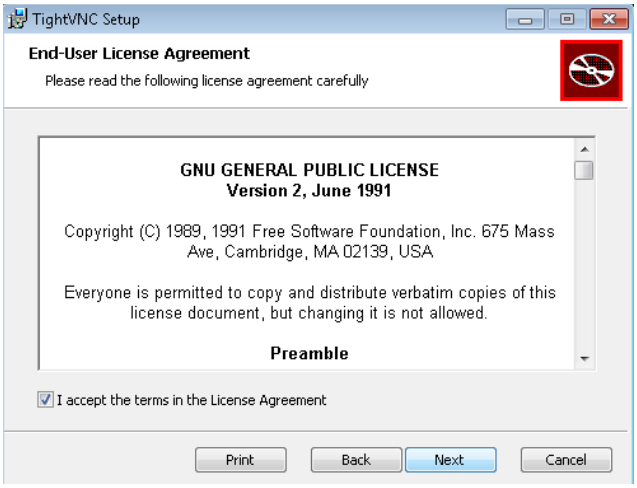


Figura 14. Aceptación de licencia de usuario

Fuente: Elaboración propia.

5. **Choose Setup Type**. Elige tipo de instalación, en este caso vamos a instalar solo el servidor (**Server**) y no instalamos el Visor (**Viewer**). De esta forma mantendremos el control y la seguridad de que los usuarios no disponga en sus máquinas el visor y traten de acceder a otras máquinas.

   Para esto seleccionamos el botón **Custom** (Personalizada) que nos permite realizar una instalación personalizada.

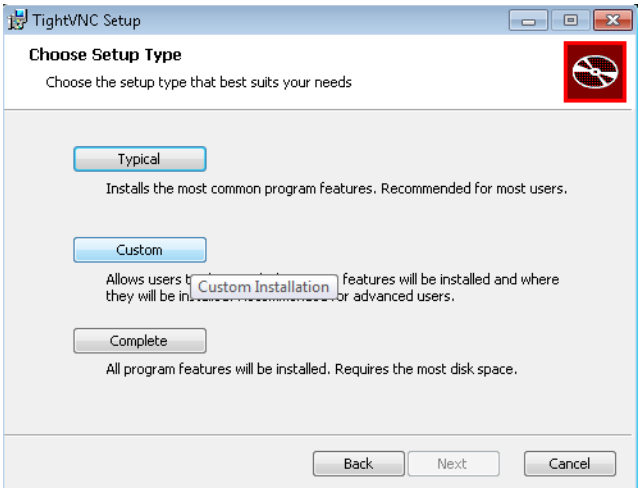


Figura 15. Tipo de instalación

Fuente: Elaboración propia.

6. **Custom Setup**. Instalación personalizada, desplegamos el combo **TightVNC Viewer** y seleccionamos la opción **X** (X = Esta característica no estará disponible) esto lo hacemos para no instalar el visor VNC. Clic en el botón **Next.**

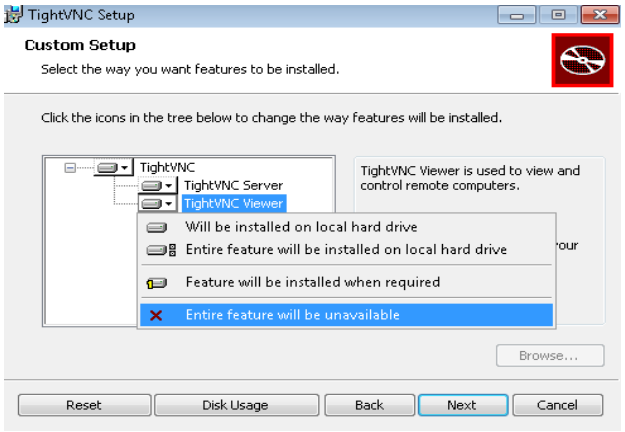


Figura 16Instalación personalizada - 1

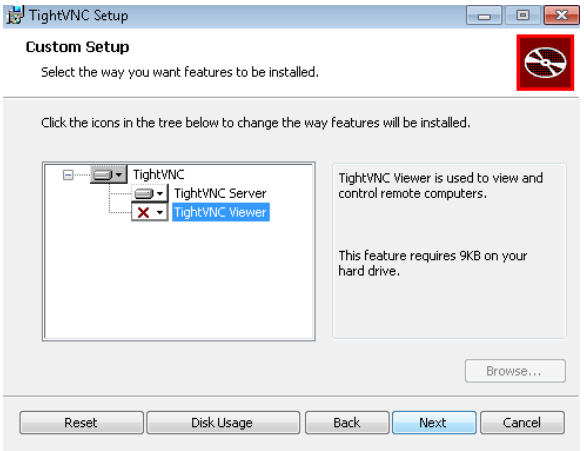


Figura 17. Instalación personalizada - 2

Fuente: Elaboración propia.

7. **Select Additional Tasks.** Seleccionar tareas adicionales. En este caso deja marcadas las 3 opciones que se ofrecen por defecto y pulsa en el botón **Next** (Siguiente):
   - **Register TightVNC Server as a system service.** Registrar el servidor de TightVNC como un servicio de sistema. De esta

forma el servidor se iniciará de forma automática cuando arranque el ordenador.

- **Configure system to allow services simulate Ctrl+Alt+Del.** Configurar sistema para permitir servicios que simulen Ctrl+Alt+Del.
- Windows Firewall configuration:
  - **Add exception for TightVNC to Windows Firewall.** Configuración del Firewall de Windows: Añadir una excepción para TightVNC al firewall de Windows

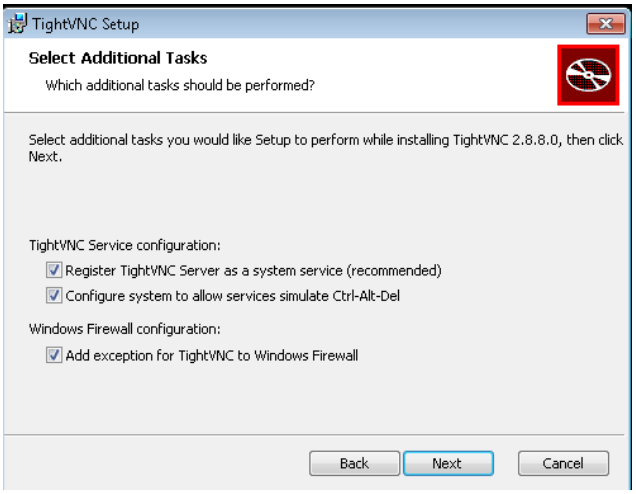


Figura 18. Tareas adicionales en la instalación

Fuente: Elaboración propia.

8. **Ready to install TightVNC.** Listo para instalar TightVNC. Clic en el botón **Install** (Instalar).

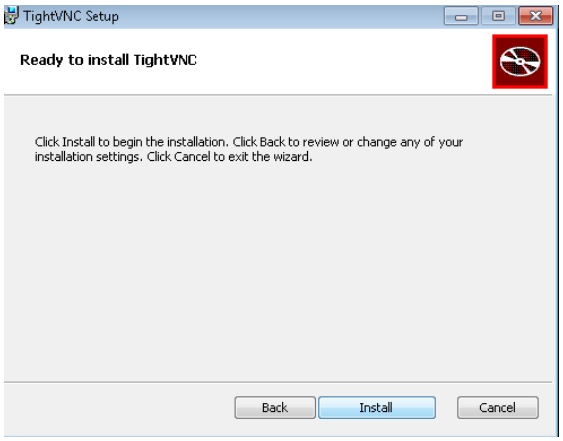


Figura 19. Listo para instalar - 1.

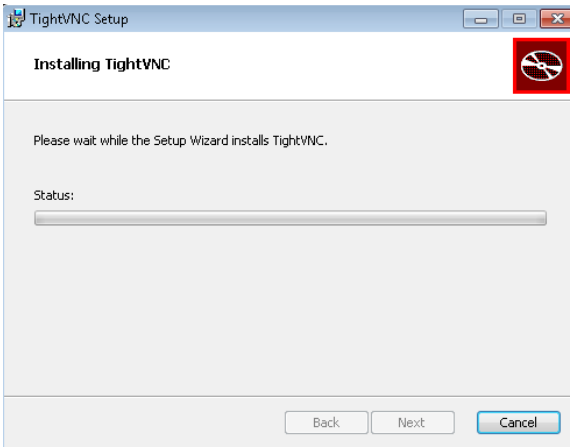


Figura 20. Listo para instalar – 2.

Fuente: Elaboración propia.

9. **TightVNC Server: Set Passwords.** Servidor TightVNC: configurar contraseñas. En este paso conviene definir las dos contraseñas que se indican:

   - Password for Remote Access. Contraseña para Acceso Remoto. Es la contraseña que el Ing. de soporte técnico

tendrá que introducir desde su equipo para acceder de forma remota al equipo del usuario. Es recomendable definirla por motivo de seguridad y para evitar que un intruso ingrese a la máquina. Marca la opción. Require password-based authentication (Requiere autentificación basada en contraseña) y teclea la contraseña (máximo 8 caracteres).

- **Administrative Password.** Contraseña de Administración. Es la contraseña que el Ing. de soporte técnico tendrá que introducir en el equipo del usuario para acceder al panel de administración del server del programa instalado en ese ordenador. Marca la opción **Protect control interface with an administrative password** (Proteger el interfaz de control con una contraseña administrativa) y teclea la contraseña (máximo 8 caracteres).

Figura 21. Configuración de contraseña

Fuente: Elaboración propia.

10. Clic en el botón Ok para guardar las contraseñas definidas. A continuación, se muestra el panel **Completed the TightVNC Setup Wizard** (Asistente de instalación de TightVNC completado). Clic en el botón **Finish** (Terminar).

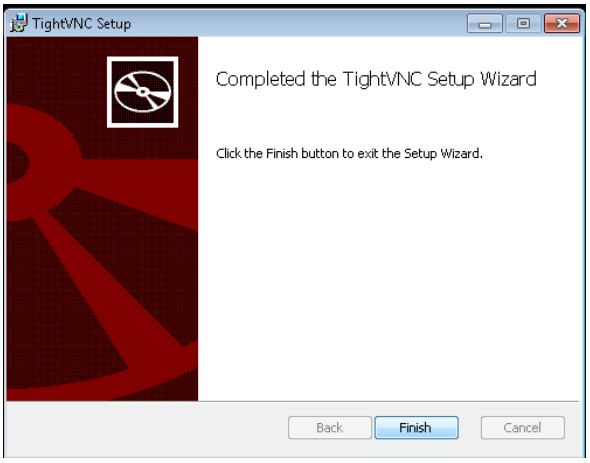


Figura 22. Instalación completada

Fuente: Elaboración propia.

11. Una vez finalizado el proceso de instalación, nos dirigimos a la **bandeja de sistema de Windows** en la esquina inferior derecha de la barra de tareas se mostrará un icono que proporcionará acceso al panel de **administración** del programa.

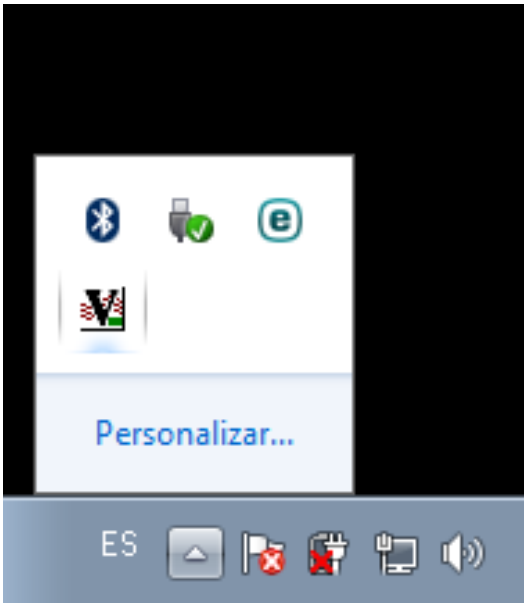


Figura 23. Icono de la herramienta.

Fuente: Elaboración propia.

4.2. MANUAL DE USUARIO.

4.2.1. Introducción.

El manual de usuario es un soporte para saber el funcionamiento de cada opción que engloba la herramienta TightVNC. Cuyo objetivo es permitir que la aplicación de soporte remoto pueda brindarle una interacción amigable, fácil para el manejo entre usuario y el departamento de sistema.

4.2.2. Funcionamiento.

1. Abrimos la aplicación TightVNC Viewer.

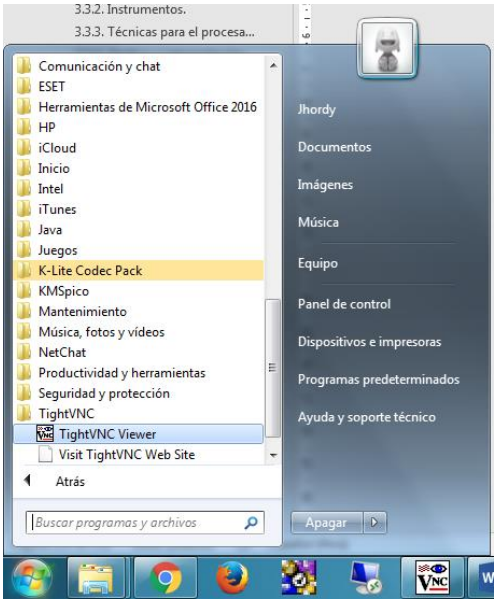


Figura 24. Abrimos la TightVNC Viewer.

Fuente: Elaboración propia.

2. Ingresamos el IP del equipo de cómputo que queremos solucionar la incidencia.

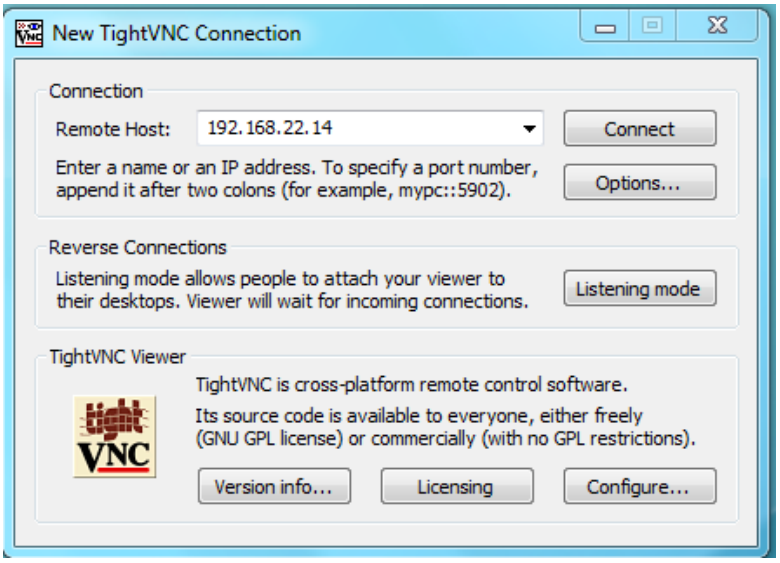


Figura 25. conexión a un escritorio del personal mediante IP

Fuente: Elaboración propia.

3. ingresar la clave de autentificación

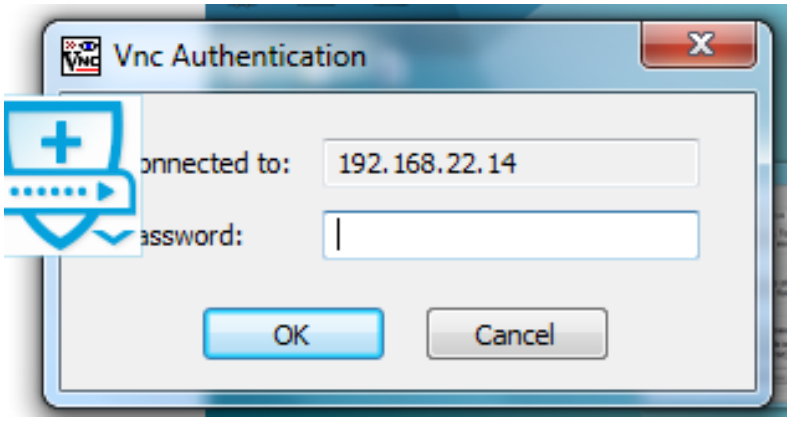


Figura 26. Ingresar clave de autentificación

Fuente: Elaboración propia.

4. conexión activa.

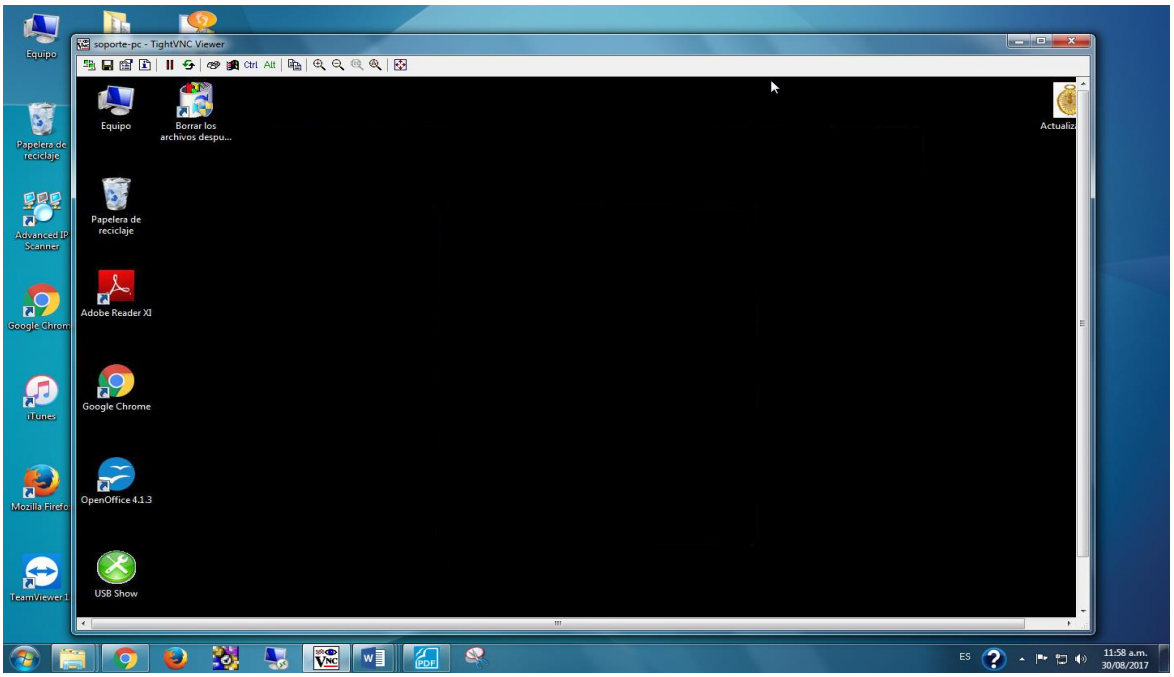


Figura 27. Conexión Activa

Fuente: Elaboración propia.

4.2.3. Opciones de TightVNC

a. Panel Principal de TightVNC

ICONO DE TIGHTVNC SERVER

Figura 28. Icono de TightVNC

Fuente: http://www.tightvnc.com/

Se muestra información de las configuraciones de los servicios de TightVNC.

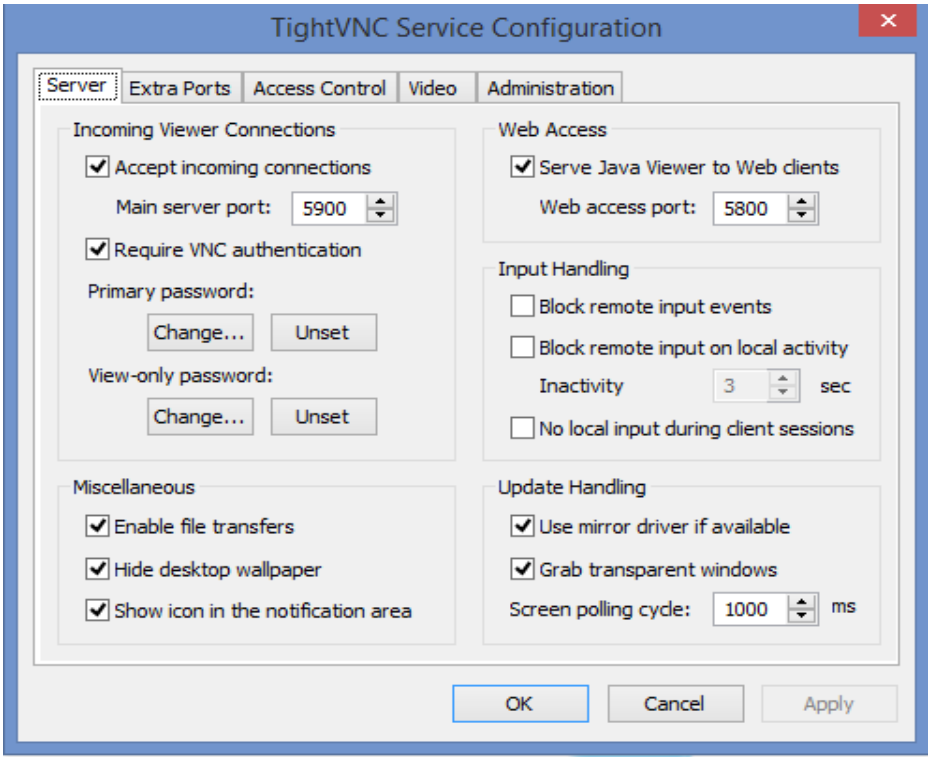


Figura 29. Opciones panel principal de TightVNC.

Fuente: Elaboración propia.

De manera visual se puede configurar la contraseña global el cual me va a permitir tener el acceso total de la conexión remota, también puedo incluir otra contraseña con solo permiso de lectura. Es muy importante definir una contraseña para la interface del administrador y así podemos evitar que el usuario tenga acceso a realizar algún cambio.

También tenemos la opción de realizar el soporte remoto por acceso web utilizando el port 5800, actualmente esta opción no la utilizamos debido a que el soporte se lo realiza todo dentro de la LAN corporativa.

4.3. Políticas de seguridad

4.3.1. Políticas para el personal de soporte técnico.

- El personal de soporte técnico tiene la obligación de responder oportunamente a los requerimientos de los usuarios.
- Cada personal de soporte técnico debe ofrecer un óptimo servicio con un amplio conocimiento de solución de problemas.
- El personal de soporte técnico deberá dar mantenimiento preventivo 2 veces al año a cada computador.
- Todo personal de soporte técnico debe ser responsable de la entrega y asignación de las computadoras y piezas dependiendo de la situación.
- El personal de soporte técnico tiene la responsabilidad de gestionar y administrar las licencias de software y realizar su distribución entre las unidades administrativas que las requieran.

- Deben proveer soporte técnico a los usuarios de las aplicaciones, así como a la información y la infraestructura del organismo.
- Cualquier tarea que implique una degradación o interrupción del servicio debe realizarse en las horas de inactividad o de menor demanda de este, siempre que sea posible.
- Debe dar prioridad a los requerimientos de acuerdo a la severidad del problema.
- El personal de soporte técnicos tiene la tarea de llevar un control exacto de las licencias y de los equipos en las que están en uso.

Que no se debe hacer:

- Instalar software sin licencia en las computadoras a menos que sean gratuitos. Introducir software malicioso en la red o computadoras.
- Dejar inconclusos tickets atendidos.
- Realizar actividades personales en jomadas laborales que afecten a los usuarios.
- Negar servicios a los usuarios en horarios de trabajo.

4.3.2. Políticas para el personal jurídico y administrativo.

- Todo usuario debe tener un nombre de usuario y contraseña, proporcionado por la Oficina de Tecnologías de Información. para acceder a su computadora personal.
- Cada personal es responsable del uso correcto del computador asignado para el desarrollo de sus labores, y si presentan problemas, generar de manera inmediata el ticket para el área de soporte técnico.
- El personal administrativo debe usar la computadora exclusivamente para realizar tareas relacionadas con sus funciones.
- Cada personal debe usar únicamente el software autorizado y que corresponde a su puesto de trabajo.
- Cada personal tiene la responsabilidad de apagar correctamente su computador luego de la jomada de trabajo.
- En caso de pérdida de algún componente o computador reportar de manera inmediata al responsable de la Oficina de Tecnologías de Información.

- Si el personal se da cuenta que está siendo atacado por algún virus, parar todo lo que esté haciendo, y llamar al departamento de soporte técnico.

- Cumplir con todas las normas, políticas y regulaciones autorizadas por el Departamento de Tics.

Lo que el usuario no debe de hacer:

- Ningún personal debe intentar acceder con otra identificación, o dar la suya.
- Usar cualquier computadora para acceder a páginas sociales. chats, juegos, radios en línea o cualquier página de internet porque pueden presentar riesgos para la segundad informática de la universidad.
- Uso de cualquier hardware para acceder, descargar, imprimir, transmitir cualquier material ajeno a la institución.
- Utilizar computadoras para fines ilegales o no autorizados.
- Usar algún sistema o servicio informático para acosar o amenazar a los personales de la institución o externos.
- Ver archivos, imágenes, videos, información de otros usuarios sin su permiso. Usar algún sistema informático para dañar el hardware o des configurar el software de la computadora.
- Enviar intencionalmente cualquier tipo de virus, gusano cuya intensión sea destructiva.
- Descargar material ilegal o ajeno a la institución.
- Comer o beber cerca del computador, cualquier partícula o líquido puede causar daño severo.

- Ingresar cualquier tipo de medio de almacenamiento si previamente no ha sido revisada y analizada por el personal de soporte técnico.

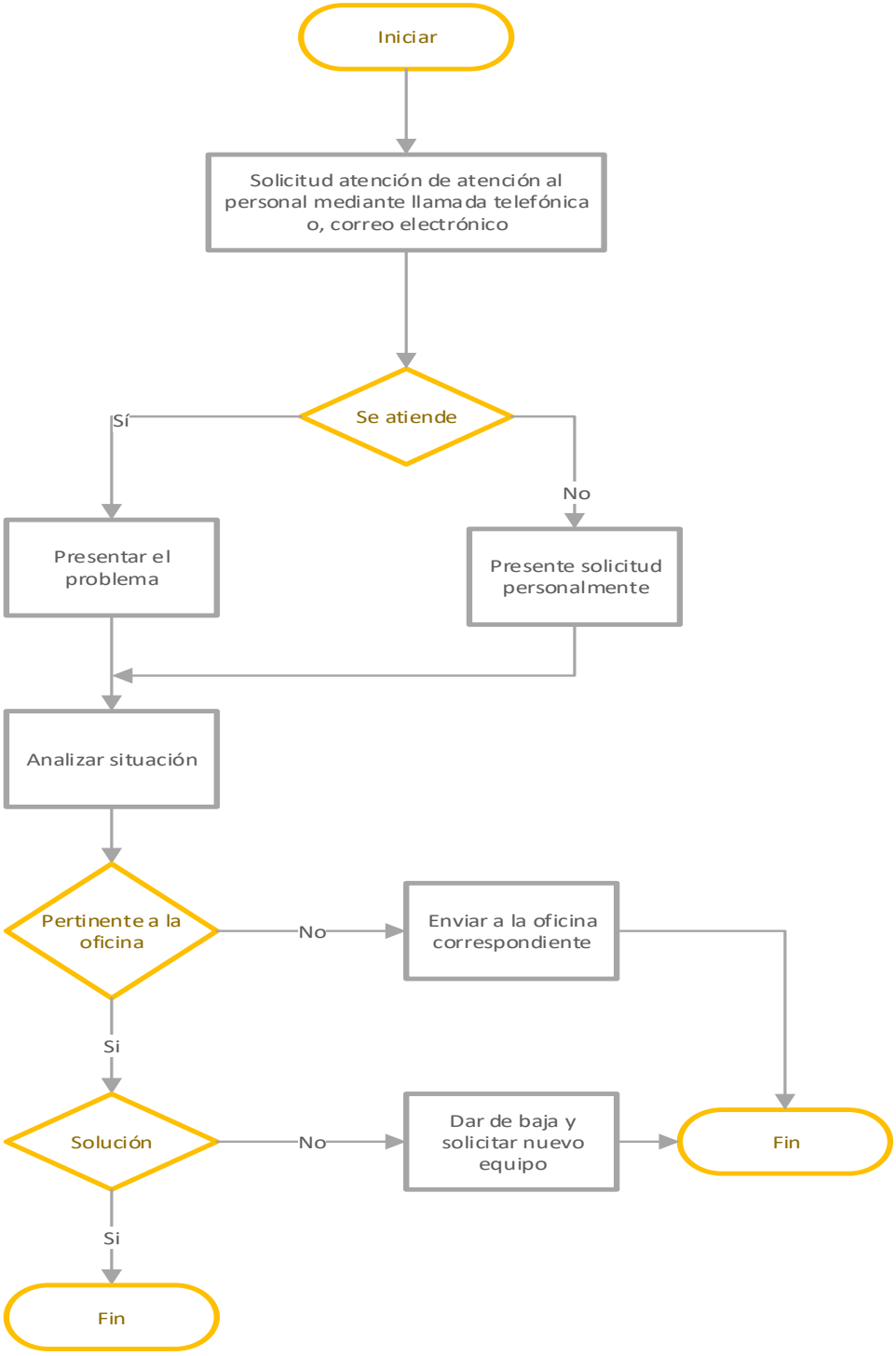
4.3.3. Políticas para la configuración de los equipos de cómputo.

- Los equipos de cómputo deben tener dos usuarios: FN (Usuario Estándar) y Soporte (Usuario Administrador).
- Se debe instalar todos los softwares establecidos por la oficina de tecnologías de información.

4.3.4. Políticas para el acceso remoto.

- Para poder obtener la salida o soluciones de la herramienta se necesita un terminal que tenga internet o que esté conectado a la red del Ministerio Publico Distrito Fiscal de Huánuco.
- El personal que solicita el soporte debe autorizar el soporte remoto.
- El personal de soporte técnico solo debe enfocarse en la petición del personal solicitante.

Tabla 16. Diagrama de Flujo de soporte técnico



Fuente: Elaboración propia.

V. RESULTADOS.

5.1. Resultados de la encuesta a personal - 01.

5.1.1. Pregunta 1

¿De qué manera usted reporta mayormente las incidencias que tiene en su equipo de cómputo al coordinador de la Oficina de Tecnologías de Información? (Marque con un aspa un solo inciso).

a. Resultados.

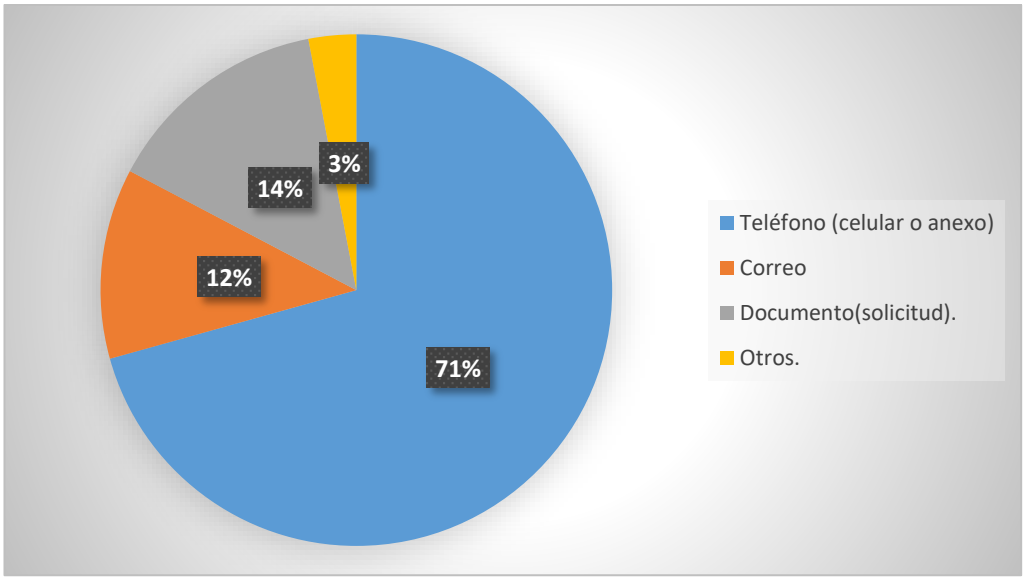


Figura 30. Resultados de pregunta 1.

Fuente: Elaboración propia.

En el grafico se observó que el personal del ministerio público el 71% utiliza el medio telefónico para reportar su incidencia en su equipo de cómputo.

5.1.2. Pregunta 2.

Marca con un aspa (X) los servicios de soporte informático que siempre solicita a la Oficina de Tecnologías de Información.

a. Resultados.

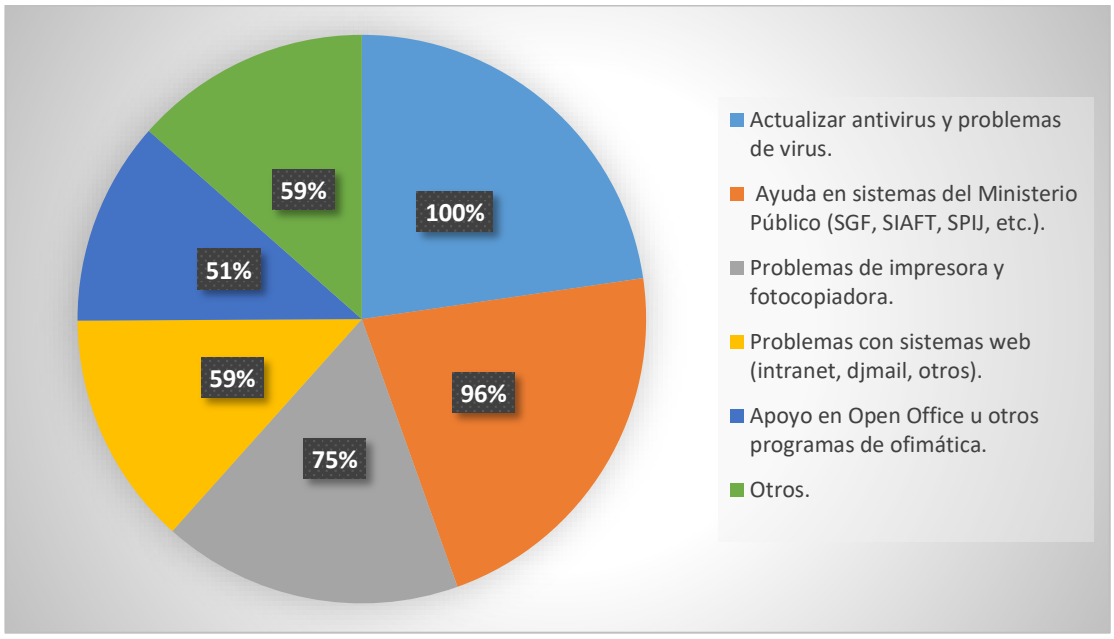


Figura 31. Resultado de la pregunta 2.

Fuente: Elaboración propia

En el grafico se observó que el personal del ministerio público se dedica a reportar incidencias que requieren el soporte informático remoto siendo en un 76.2 % a respuesta de los 5 primeros incisos.

5.1.3. Pregunta 3.

Cuento tiempo se demora la Oficina de Tecnologías de Información en solucionar su incidencia en su equipo de cómputo (Marque con un aspa un solo inciso).

a. Resultados.

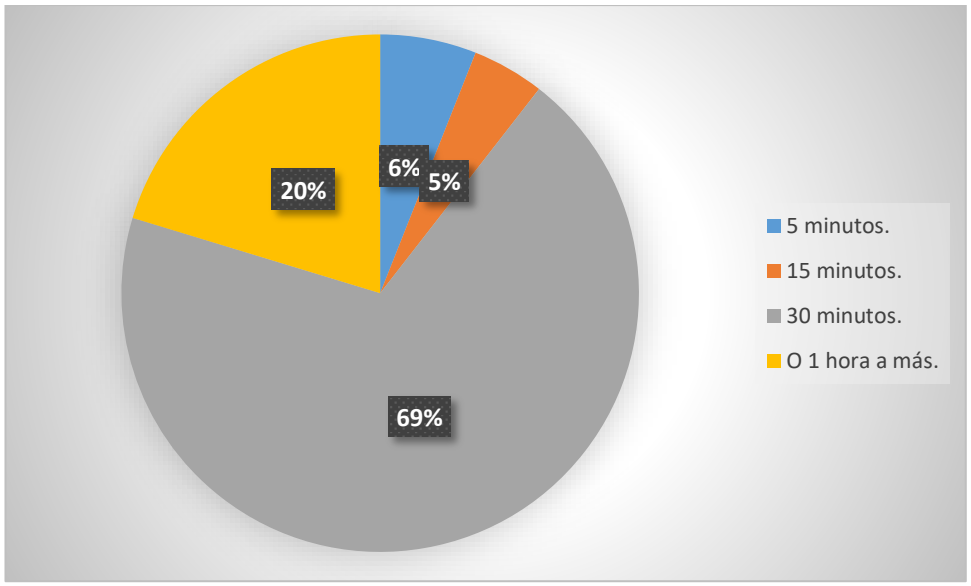


Figura 32. Resultado de la pregunta 3.

Fuente: elaboración propia.

En el grafico se observó que la Oficina de Tecnologías de Información se demora un de 30 minutos a mas en resolver una incidencia.

5.2. Resultados de la encuesta al personal - 02.

5.2.1. Pregunta 1.

Cuento tiempo se demora la Oficina de Tecnologías de Información en solucionar su incidencia en su equipo de cómputo (Marque con un aspa un solo inciso).

a. Resultados.

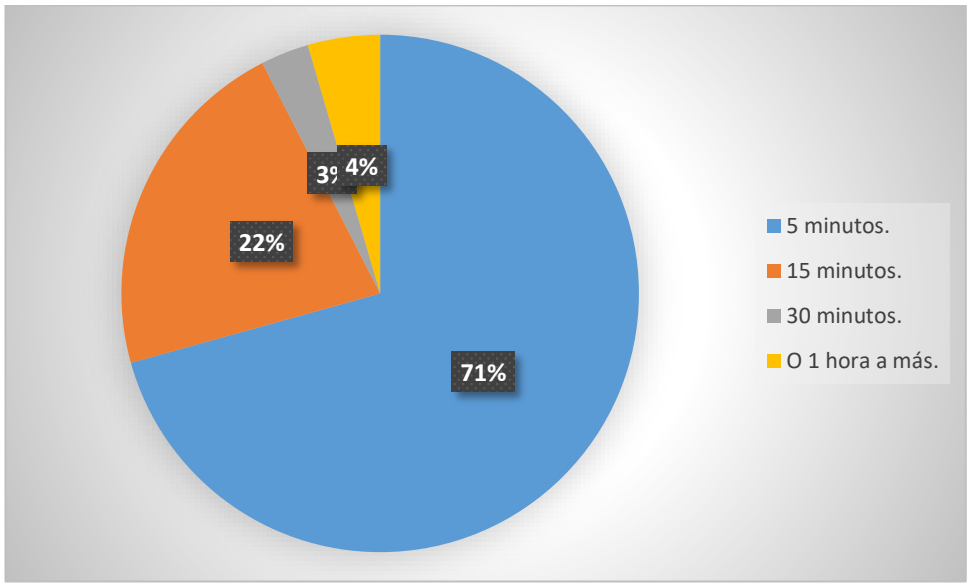


Figura 33. Resultado de la pregunta 1.

Fuente. Elaboración propia.

En el grafico se observó que la Oficina de Tecnologías de Información se demora de 5 a 15 minutos en resolver una incidencia.

5.2.2. Pregunta 2.

Está contento con la nueva forma de atención de soporte informático por parte de la Oficina de Tecnologías de Información. (Marque con un aspa un solo inciso).

O Muy contento.

O Contento.

O Descontento.

O Muy descontento.

a. Resultados.

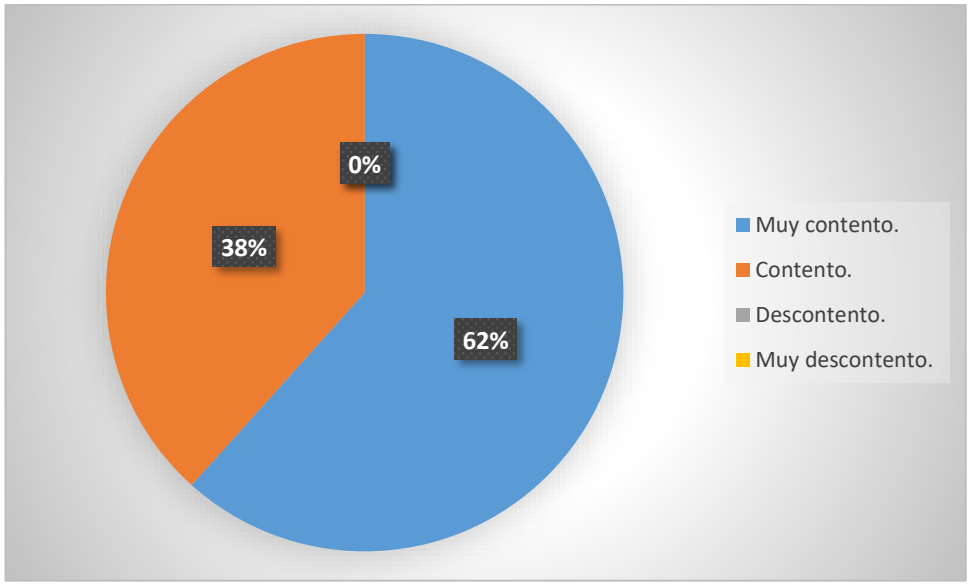


Figura 34. Resultado de la pregunta 2.

Fuente: Elaboración propia.

En el grafico se observó que el personal del ministerio público está contento con el soporte informático remoto brindado por la Oficina de tecnologías de la Información.

5.3. Comprobación de diseño.

	Grupo	Preprueba	Variable Independiente	Postprueba
R	E	O_1	X	O_2
R	C	O_1		O_3

- E: grupo experimental aleatorio.
- C: grupo de control aleatorio.
- O_1 : De la encuesta número 01 de la pregunta 3, el dato importante a tomar es el 89% del personal encuestado responde que la solución a sus incidencias de soporte informático se demora de 30 minutos a más.
- O_2 : De la encuesta número 02 de la pregunta 1. El dato importante a tomar en el 93% del personal encuestado responde que la solución a sus incidencias aplicando el soporte informático remoto se demora de 5 minutos a 15 minutos.
- O_3 : El autor supone que es igual a la O_1. No se realizó otra encuesta por motivos

El resultado es el siguiente O_2 la demora de tiempo es de 30 minutos a mas, mientras en la O_3 la demora de tiempo es de 5 minutos a 15 minutos.

Por lo tanto, el autor dedujo que mediante la implantación de soporte informático se disminuye el tiempo de 15 minutos.

CONCLUSIONES.

- La implementación del software TightVNC se realizó sin ningún inconveniente en las diferentes sedes del Ministerio Público – Distrito Fiscal Huánuco
- Con la implementación de software de acceso remoto se mejoró la efectividad de atención de la Oficina de Tecnologías de información, reduciendo el tiempo de atención de incidencias del soporte informático en un 95%.
- Se hizo entrega de políticas de seguridad para la realización del soporte informático remoto, así mismo se hizo entrega del manual técnico y manual de usuario del software TightVNC.
- Al realizar una encuesta posterior a la implementación al personal, se llegó a deducir que el 98% del personal está contenta con la nueva forma de realizarse el soporte informático por parte de la Oficina de Tecnologías de Información.
- En la investigación realizada se dedujo que el personal del Ministerio Público no conoce los avances tecnológicos que ayudan a mejorar sus actividades laborales.
- El personal del Ministerio Público generalmente dispone de 5 a 15 min para ayudar a solucionar sus incidencias, al sobrepasarse ese tiempo, se genera molestia e incomodidad en sus actividades laborales.

RECOMENDACIONES.

Por lo anteriormente expuesto y para mejorar la realización de este tipo de trabajos de investigaciones, se recomienda algunos puntos que mejorarían la realización de los mismos.

- Se recomienda la total implementación en las diferentes sedes del Distrito fiscal de Huánuco
- Se recomienda cumplir las políticas de seguridad entregadas, juntamente con el manual de usuario para poder evitar algunas incidencias mayores.
- Se recomienda seguir implementado nuevas tendencias tecnologías que ayuden a mejorar el servicio de soporte técnico informático al personal, como por ejemplo una mesa de ayuda.
- Se recomienda tener un inventario de hardware y software para un mayor control de sus actividades.
- Se recomienda tener un listado de IP con el respectivo personal que esté haciendo uso de ello, para realizar una auditoría
- El análisis en el campo de la legislación es muy complejo, ya que se involucran Fiscales, los cuales son muy cortos de tiempo y te brinda muy poca información.

BIBLIOGRAFÍA

ALLPORT. (2011). *LAS SADASDADASD.* ESPAÑA: LIMAS FD.

Appser Data Engineering S.L. (APSER). (2015). *APSER CLOUD SERVICES*. Obtenido de http://www.apser.es/blog/2017/01/13/soporte-informatico-definicion-tipos/

Arboleda Orejuela, J. A. (2015). IMPLEMENTACIÓN DE UNA HERRAMIENTA TECNOLOGICA PARA ATENCIÓN A USUSARIOS EN LA PONTIFICIA UNIVERSIDAD CATOLICA DE ECUADOR SEDE EN ESMERALDA. *IMPLEMENTACIÓN DE UNA HERRAMIENTA TECNOLOGICA PARA ATENCIÓN A USUSARIOS EN LA PONTIFICIA UNIVERSIDAD CATOLICA DE ECUADOR SEDE EN ESMERALDA*. Ecuador.

Ayala Marín, G. A., & Taipe Nuñez, N. G. (2006). Implementación de políticas de seguridad en Red Lan Corporativa. Quito, Ecuador.

Ayala Marín, G. A., & Taipe Nuñez, N. (s.f.). Implementación de políticas de seguridad en Red Lan Corporativa. *POLÍTICA DE SEGURIDAD;RED LAN CORPORATIVA;INFRAESTRUCTURA TECNOLÓGICA;SEGURIDAD EN RED.* Universidad De Las Américas, Quito.

Dordoinge, J., & Philippe, A. (2006). *Redes Informáticas-Conceptos Fundamentales.* Ediciones ENI.

Garcia, A., Cervigon , H., & Alegre Ramos, M. (2011). *Seguridad del informática.* Paraninfo.

Gary, W. (2001). *IT Production Services (Harris Kern's Enterprise Computing Institute).*

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, P. (2006). *Metodología de la ivestigacion.* Iztapalapa. Mexico Distrito Federal: McGraw-Hill Interamericana.

Kajko-Mattsson, M. (2004). *Problems within front-end support. Journal oí Software Maintenance and Evolution.*

Kerlinger, F. N. (1991). *Investigación del Comportamiento.* Mexico: Mc-Graw-Hill.

León Robayo, J. D. (2015). IMPLEMENTACIÓN DE UNA MESA DE AYUDA EN EL DEPARTAMENTO DE TECNOLOGÍA DE LA INFORMACIÓN DE UNIFINSA PARA SOPORTE AL USUARIO BASADO EN LAS MEJORAR PRÁCTICAS DE LA LIBRERÍA DE INFRAESTRUCTURA DE TECNOLOGÍAS DE INFORMACIÓN(ITIL)". Sangolquí, Ecuador.

López García, J. L. (2013). SISTEMA DE SOPORTE TÉCNICO VÍA REMOTA PARA USUARIOS DE EQUIPOS DE COMPUTOS. MÉXICO.

Mondéjar, J. P. (25 de Abril de 2008). *Escuala Técnica Superior de Ingeniería de Telecomunicaciones.* Obtenido de http://www.teleco.upct.es/documentos/empresas/AccesoRemoto.pdf

Nación, M. P. (s.f.). *Ministerio Público Fiscalia de la Nación*. Obtenido de Ministerio Público Fiscalia de la Nación: http://portal.mpfn.gob.pe/descargas/transparencia/normas_adm/mof_admdjb.pdf

Ñaupas Paitán, H., Mejía Meja, E., Novoa Ramírez, E., & Villagómez Paucar, A. (2011). *METODOLOGÍA DE LA INVESTIGACIÓN CIENTÍFICA Y ASESORAMIENTO DE TESIS.* Lima : Centro de Producción Editorial e Imprenta de la Universidad Nacional Mayor de San Marcos.

PICOYA HERMOSA, L. (1987). *Investigación Cientifica y educacacional.* Lima: Amaru Editores.

Sánchez Carlessi, H., & Reyes Meza, C. (2006). *Medología y Diseños en la investigación científica.* Lima: Visión Universitaria .

Talaván, G. E. (2006). *Cómo usar la PC en forma segura.* octubre: Mundo Grafico S.R.L.

ANEXOS

Anexo N° 01: Matriz de consistencia

Planteamiento del problema	Objetivos	Variables	Conceptualización	Dimensiones	Indicadores	Instrumento	Metodología
FORMULACIÓN DEL PROBLEMA PRINCIPAL ¿De qué manera mejorará el servicio de atención de soporte informático al personal jurídico y administrativo del Ministerio Publico – Distrito Fiscal de Huánuco por parte de la Oficina de Tecnologías de Información? FORMULACIÓN DE PROBLEMAS ESPECÍFICOS ¿Cuál será la óptima herramienta de conexión remota para la implementación en la Oficina de Tecnologías de Información del Ministerio Público – Distrito Fiscal de Huánuco? ¿Cuál de los procesos de soporte informático al personal jurídico y administrativo se debe optimizar, por parte de la Oficina de Tecnologías de Información del Ministerio Público – Distrito Fiscal de Huánuco? ¿Existirá políticas de seguridad y normas necesarias para la implementación en el Ministerio Publico – Distrito Fiscal de Huánuco?	GENERAL: Implementar un soporte informático remoto en la Oficina de Tecnologías de Información para mejorar la efectividad de la atención de soporte al personal jurídico y administrativo del Ministerio Publico - Distrito Fiscal de Huánuco. ESPECÍFICOS: Identificar el software de conexión remota óptima para la implementación en la Oficina de Tecnologías de Información del Ministerio Público - Distrito Fiscal de Huánuco. Identificar los procesos a optimizar de soporte informático al personal jurídico y administrativo por parte de la Oficina de Tecnologías de Información del Ministerio Público - Distrito Fiscal de Huánuco. Identificar las políticas de seguridad y normas necesarias para la propuesta de implementación en el Ministerio Publico – Distrito Fiscal de Huánuco.	VARIABLE INDEPENDIENTE: (X) Soporte Informático Remoto	Procesos que ayudan al mejoramiento del soporte a usuarios de una empresa.	VARIABLE INDEPENDIENTE Seguridad. Confidencialidad.	VARIABLE INDEPENDIENTE Cumplimiento con estándar propuesto. Cumplimiento con estándar propuesto.	VARIABLE INDEPENDIENTE Cumplimiento a las políticas de seguridad. Cumplimiento a las políticas de seguridad.	Tipo de investigación: Investigación aplicada o tecnológica. Enfoque de investigación: Enfoque cuantitativo.
		VARIABLE DEPENDIENTE: (Y) Atención al Personal	Efectividad para dar soluciones a los problemas e incidencias.	VARIABLE DEPENDIENTE Productividad. Reducción de costos	VARIABLE DEPENDIENTE Total, de atenciones por día Ahorro de nuevos soles	VARIABLE DEPENDIENTE Fichas de atención por día. Ficha de reducción de costos	Nivel o alcance de investigación: Investigación en tecnologías formales. Diseño de investigación: Experimentación pura de dos grupos con preprueba y postprueba

Anexo N° 02: Formato de cuestionario al personal - 01.

1. ¿De qué manera usted reporta mayormente las incidencias que tiene en su equipo de cómputo al coordinador de la Oficina de Tecnologías de Información? (Marque con un aspa un solo inciso).

   O Teléfono (celular o anexo)

   O Correo

   O Documento(solicitud).

   O otros.

2. Marca con un aspa (X) los servicios de soporte informático que siempre solicita a la Oficina de Tecnologías de Información.

   O Actualizar antivirus y problemas de virus.

   O Ayuda en sistemas del Ministerio Público (SGF, SIAFT, SPIJ, etc.).

   O Problemas de impresora y fotocopiadora.

   O Problemas con sistemas web (intranet, djmail, otros).

   O Apoyo en Open Office u otros programas de ofimática.

3. Cuento tiempo se demora la Oficina de Tecnologías de Información en solucionar su incidencia en su equipo de cómputo (Marque con un aspa un solo inciso).

   O 5 minutos.

   O 15 minutos.

   O 30 minutos.

   O 1 hora a más.

Anexo N° 03: Formato de cuestionario al personal - 02.

1. Cuento tiempo se demora la Oficina de Tecnologías de Información en solucionar su incidencia en su equipo de cómputo (Marque con un aspa un solo inciso).

O 5 minutos.

O 15 minutos.

O 30 minutos.

O 1 hora a más.

2. Está contento con la nueva forma de atención de soporte informático por parte de la Oficina de Tecnologías de Información. (Marque con un aspa un solo inciso).

O Muy contento.

O Contento.

O Descontento.

O Muy descontento.

Anexo N° 04: Lista de población encuestada.

DEPENDENCIA		Nombres y Apellidos	CARGO
		CORNEJO FALCON, MANUEL AUGUSTO	F.S. (T)
		BORJAS ROA, JUAN MANUEL	F.A.S. (T)
		IBAÑEZ ZAVALA, NORA RAQUEL	F.A.S. (T)
		VEGA BILLAN, RODOLFO	F.S. (T)
		PAIRAZAMAN SILVA, VICTORIA CONSUELO	F.A.S. (T)
		MAYTA DELZO, ROCIO PILAR	F.A.S. (T)
		CHAVEZ MATOS, ANA MARIA	F.S. (T)
		VARGAS ROMERO, SANTIAGO ELEAZAR	F.A.S. (T)
		MAMANI DAVILA, BRIAN FRANK	F.A.S. (T)
		AGUIRRE VISAG, VICTOR ALBERTO	F.S.(P)
		HERNANDEZ AGUILAR, CHRISTIAN	F.A.S. (T)
		PAUCAR GONZALES, MANUELA NORA	F.A.S. (T)
		CERRON UCEDA, AMADEO	F.S. (F)
		MORALES BESADA, GIOVANNA ORFELINDA	F.A.S. (T)
		OLLAGUE ROJAS, HERBERTH JEAN	F.P. (T)
		HIDALGO PASQUEL, KELER LUBE	F.A.P. (P)
		ALVAREZ CORTIJO, RONALD PERCY	F.A.P. (T)
		GUTIERREZ GAMBOA, REYNA GISSELLA	F.P. (T)
		PRADO ESTRADA, ARON DENIS	F.A.P. (P)
		APAZA HUISA, LALI MARIBEL	F.A.P. (T)
		TOMAS VILCAHUAMAN, GINA CLAUDIA	F.P. (P)
		MALPARTIDA ACUÑA, EVELYN ALANA	F.A.P. (T)
		OSCO MAMANI, BROSELY	F.A.P. (T)
		PALLI CALLA, CESAR FERNANDO	F.P. (T)
		HUAYHUA ALMONACID, ERIKA MARIELA	F.A.P. (T)
		COLQUEHUANCA RODRIGUEZ NELIDA	F.A.P. (P)
		MAYTA BALDEON, NATHALIE KAROL	F.P. (T)

2° Fiscalía Provincial Penal Corporativa Huánuco - Jr. San Martin Nº 765	1er Despacho	HUAROC CHANCASANAMPA, ANGEL EDGAR	F.A.P. (T)
		MAMANI AYCACHI OSCAR FERNANDO	F.A.P. (T)
		MONZON MONTESINOS, MAO YASSER	F.P. (P)
		ARANGUREN MARTINEZ JESUS ALBERTO	F.A.P. (T)
		SOLIS BARRUETA, ALEACIB	F.A.P. (T)
		RAMIREZ VERA, KELLY ROXANA	F.P. (T)
		CARUHAPOMA ORTEGA, JUDITH GISELLA	F.A.P. (T)
		GALARZA BRAVO, ROSA ELVIRA	F.A.P. (T)
		LECARO ALVARADO, ROBERTO GERARDO	F.P. (T)
		PEREZ TERRAZAS, GRACE	F.A.P. (T)
		RICAPA CASTILLO, PEDRO MIGUEL	F.A.P. (T)
		ZUMARAN RAMIREZ, HENRY WILLIAM	F.P. (T)
		TERROBA GUTIERREZ, BLANCA SUSANA	F.A.P. (T)
		VILCA ALVAREZ RIVERTT LENIN	F.A.P. (T)
		SERNA ROMAN, RODOLFO RAPHAEL	F.P. (T)
		SUAREZ FERRER, ALAN WILMER	F.A.P. (T)
		VARGAS SANDOVAL, LETICIA MABEL	F.A.P. (T)
		JIMENEZ FUENTES, RUDY	F.P. (T)
		MARTINEZ MUCHA, WILLIAM WILFREDO	F.A.P. (T)
		RIVERA PEREZ, JOSE LUIS	F.A.P. (T)
		BUSTAMANTE ZEVALLOS, CARLOS ALBERTO	F.P. (T)
		QUISPE PALMA, ELIZABETH	F.A.P. (T)
		ALARCON MORALES, GABRIELA MIRIAM	F.A.P. (T)
		ASTETE MALDONADO, FERNANDO EFRAIN	F.P. (T)
		GARCIA LAURA, JUAN ANTONIO	F.A.P. (T)
		CAMACHO LEON, GANDHY	F.A.P. (T)
		RETAMOZO BORDA, ALEXANDER VLADIMIR	F.P. (T)
		VALENCIA OVIEDO, CARLOS ENRIQUE	F.A.P. (T)
		VIZCARRA CUEVAS, LUIS MIGUEL	F.A.P. (T)
		COAQUERA PACCI, EDWIN LEONARDO	F.P. (P)
		MEZA CORRALES, JOSE CARLOS	F.A.P. (T)
		PORTILLO MAMANI, MIGUEL ANGEL	F.A.P. (T)

	4to Despacho	LOPEZ LOARTE, LUIS LEONARDO	F.P. (T)
		RAMOS ROMERO JULISSA ISABEL	F.A.P. (T)
		VILLARREAL HERRERA, EVELYN DENISSE	F.A.P. (T)
		CHIRINOS ÑASCO, JOSE LUIS	F.P. (T)
		DELGADO DIAZ, JUAN JESUS	F.A.P. (T)
		FALCON FRETEL, YSABELA MELANIA	F.A.P. (S)
		MALMA CORDERO, CLAUDIA ADRIANA	F.P. (T)
		PASQUEL PAREDES, LUIS	F.A.P. (T)
		VARGAS PAYA, GUILIANA ARACELI ANGELICA	F.A.P. (T)
		MELLADO SALAZAR, JULIA	F.P. (T)
		GONZALES RADO STEFEEN ERICK	F.A.P. (T)
		LARA ESPINOZA, CARITO MARIA	F.A.P. (P)
		CHAVEZ GARCIA, MARILUZ	F.P. (T)
		TASAYCO YATACO JESUS ORLANDO	F.A.P. (T)
		CHANGARAY HUAMAN, TONY WAGNER	F.A.P. (T)
		MALPARTIDA MENDOZA, MIGUEL ANGEL	F.P. (T)
		GOMEZ HERRERA, ELIZABETH GLADYS	F.A.P. (T)
		ECHEVARRIA CUADROS OBDUL GONZALO	F.A.P. (T)
		FERNANDEZ TINCO, YOHANA	F.P. (T)
		MORALES CERNA, JOSUE ALVARO	F.A.P. (T)
		ANCO FERNANDEZ MELISSA JACKELINE	F.A.P. (T)
		PEÑA VELA WERNER HANS	F.P. (T)
		AGUIRRE BUSTAMANTE, JUAN LUIS	F.A.P. (T)
		MELGAR YAURICASA NOE SAUL	F.A.P. (T)
		QUISPE RODRIGUEZ ELISEO AGUEDO	F.P. (T)
		PINEDO SANCHEZ, LUZ ANGELICA	F.A.P. (T)
		LURITA MORENO JAMES JUNIOR	F.A.P. (T)
		ESCALANTE ALAY, LUIS ROMAN	F.P. (P)
		CASTILLO UCULMANA, NELLY CECILIA	F.A.P. (T)
		MELGAREJO VIDAL, EMERSON TONINO	F.A.P. (P)
		SERRANO COZ, ZOCIMO REMO	F.P. (T)
		LASTRA CLAUDIO, ELSA TEOFILA	F.A.P. (T)

		NORIA LOZANO, ROCIO YOANNA	F.A.P. (P)
		CASTRO MARTINEZ, ROCIO JANETH	F.P. (T)
		ESPINOZA MATIAS, JIMY PERCY	F.A.P. (P)
		CARNERO TOLMOS, DIANA OFELIA	F.A.P. (T)
		ALDANA TELLO, ELVIRA ROSA	F.P. (T)
		ANGULO RIVERA, DAVID EDWIN	F.A.P. (P)
		ALVAREZ HUAMAN, VERTILA	F.A.P. (P)
		ROJAS GUTIERREZ, LUIS ANGELLO	F.A.P. (P)
		AGUILAR SOLORZANO, ENEIDA	F.P. (T)
		ORDAYA LOPEZ, CARLOS	F.A.P. (T)
		PONCE FACUNDO, CARLOS JUAN	F.A.P. (P)
		CHAGUA TIMOTEO, LUZ OLGA	F.P. (P)
		AGUI ESTEBAN, LAURA	F.A.P (T)
		GARCIA VERA, NOE HUMBERTO	F.A.P (T)
		CASTILLO VELARDE, ROBERTO	F.S. (T)
		BAÑEZ LEYVA, HILDA HAYDEE	F.P. (P)
		APARI VITOR, SONIA LUZ	F.P. (P)
		HERRERA BERNEDO, MARCO ANTONIO	F.P. (T)
		CASTRO PEREYRA, ELIZABETH	F.A.P (T)
		ALVAREZ MORAN, ERICK JESUS	F.A.P (T)
		ALEJOS VILCHEZ RENATO FERNANDO	FISC.SUPERIOR (T)
		BASTIDAS ALIAGA, JOHANA	FISC.ADJ.SUPER. (T)
		ROJAS VELASQUEZ, JEREMIAS	FISC.ADJ.SUPER. (T)
		SANCHEZ FIGUEROA, LUZ MERCEDES	FISC.PROVINCIAL (T)
		ROJAS MAYTA MIGUEL JHONY	FISC.ADJ. PROV. (T)
		FERNANDEZ LAZO, PERCY FERNANDO	FISC.ADJ. PROV. (P)
		JARA SILVA, RUBEN WILIAM	FISC.PROVINCIAL
		LIYANAGE PALACIOS, CARLA LEONOR	FISC.ADJ. PROV. (T)

		NUÑEZ ARQUINIO, LAURA LETICIA	FISC.ADJ. PROV. (T)
		ESPIRITU MATOS, MARCO ANTONIO	FISC.PROVINCIAL (T)
		FERNANDEZ AQUINO, ISABEL	FISC.ADJ. PROV. (T)
		CARRION CABRERA, VIRGILIO IVAN	FISC.PROVINCIAL
		MORE CHUMACERO, REYNA ELIANA	FISC.ADJ. PROV.

	Apellidos y Nombres	Cargo.
Personal administrativo	BECERRA MORI, CAROLA MILAGROS	ANA.
	SERRANO RUIZ, OSCAR MANUEL	ANA.
	VILLAIZAN CAJAS, CESAR ROBERTO	ANA.
	TADEO CHAVEZ, KOENING EVERARDO	ANA
	CARLOS GARCIA, OSCAR	ANA.
	ESPINOZA GONZALES, GIANINA ROCIO	ANA.
	SANTA CRUZ AMBROSIO, ROMER	E.A.
	PICON MARCOS, LILIANA	E.A.
	GONZALES PARIONA, LIDA ADELINA	E.A.
	CAMPOS SALAZAR, JOHNNY POMPEYO	E.A.
	ADAMA ESPINOZA, FELIX	E.A.
	BALDEON ROMERO, ALEX HERACLIDES	A.A.(S.A)
	MARZANO HURTADO, DANTTI GIOVANNI	A.A.(S.A)
	MORY TREJO, EMILIA	A.A.(S.A)
	CAJA CULQUI, EUSEBIA ASUNTA	A.A.(S.A)
	PALACIOS BORJA, JANEEL	A.A.(S.A)
	VIA RAMIREZ, LAURA ROCIO	A.A.(S.A)
	PABLO SANTOS, DANIEL EDWIN	A.A.(S.A)

	CARRASCO DIAZ, JORGE ALEXANDER	A.A.(S.A)
	CORNEJO MALDONADO, JOSE ANTONIO	A.A.(S.A)
	ESPINOZA AGUIRRE, EDY LUZ	A.A.(S.A)
	PEÑA EUGENIO, JESUS MANUEL	A.A.
	LUCAS TRUJILLO, JOSE CARLOS	A.A. (COND.)
	ARGANDOÑA CALDAS, MELCHOR	A.A. (COND.)
	CAMARA JAPA, JOSE LUIS	A.A. (COND.)
	SOLANO RAMIREZ, RODDY YUL	A.A. (COND.)
	JAIMES CIPRIANO, VICTOR ABRAHAM	A.A. (COND.)
	SOLANO ALDECOA, JESUS FRANCISCO	A.A. (COND.)
	ALVARADO FASABI, PABLO	A.A. (COND.)
	PAJARES DIAZ, LUIS ROBERTO	A.A. (COND.)
	GARCIA APOLINARIO, CARLOS ALBERTO	A.A. (COND.)
	VILLANUEVA ZEVALLOS, OSCAR ENRIQUE	A.A. (COND.)
	RENGIFO HIDALGO, MABEL	A.A.(NOT.)
	ILDIFONSO VENTURO, SARA ESTER	A.A.(NOT.)
	DIAZ HUAMAN, TESSY IVETH	A.A.(NOT.)

Anexo N° 05:

Reducción de tiempo.

Tiempo de realización del soporte informático de manera presencial. (Marque con un aspa un solo inciso).

O 5 minutos.

O 15 minutos.

O 30 minutos.

O 1 hora a más.

Tiempo de realización de soporte informático con acceso remoto. (Marque con un aspa un solo inciso).

O 5 minutos.

O 15 minutos.

O 30 minutos.

O 1 hora a más.

Nota: Se realizará la resta del tiempo de soporte informático presencial menos el tiempo que se realiza con el soporte informático remoto, obteniendo como resultado la reducción de tiempo de atención.

Anexo N° 06:

Ficha de Productividad.

Cuantas incidencias de soporte informático resuelve al día la Oficina de Tecnologías de información utilizando la herramienta de acceso remoto (escriba el total).

O …….

Nota: La suma total de todas las incidencias diarias será la productividad mensual y se compara con los meses anteriores sin la utilización de la herramienta de acceso remoto.

Anexo N° 07: Implementación

Sede	Inicio	Termino
San Martin	17/07/17	21/07/17
Sede Central	03/07/17	07/07/17
FEMA y DML	10/07/17	12/07/17
Anticorrupción	13/07/17	14/07/17
Control Interno	31/07/17	01/08/17
Morgue	02/08/17	03/08/17
Amarilis	04/08/17	04/08/17

Anexo N° 08: Lista de IP – Sede San Martin

CARGO	MESA PARTES		1FPPCHCO		2FPPCHCO		3FPPCHCO		4FPPCHCO		5FPPCHCO		6FPPCHCO		OFICINAS	
COORDINADOR	10.10.107.21		10.10.107.51	Angélica Aquino Suarez	10.10.107.91	Karol Mayta	10.10.107.131	Rodolfo Serna Román	10.10.107.171	VIVIANO FRETEL, LILIANA JEA	10.10.107.211	CHAVEZ ALARCÓN, EVER JAVI	10.10.120.11	COLINA ARTURO	10.10.120.51	CRISTOBAL LOAYZA, EDWARD
2DO FISCAL	10.10.107.22	RAMIREZ HUAMAN, OSMAR	10.10.107.52	palli	10.10.107.92	PACHAS CABRERA, ERNESTO	10.10.107.132	Henry Zumarán Ramírez	10.10.107.172	ACHOMA TITO, JOSÉ ANTONI	10.10.107.212		10.10.120.12	MINAYA ZORICICH, NINOSKA CLARA	10.10.120.52	BLANCAS CAJAHUAMAN, AIDA
3ER FISCAL	10.10.107.23	LILIANA PICON	10.10.107.53	María Atarama Palacios	10.10.107.93	PANTOJA ROSAS, GILMER	10.10.107.133	BUSTAMANTE ZEVALLOS, CAR	10.10.107.173	LOPEZ LOARTE, LUIS LEONARD	10.10.107.213	MALMA CORDERO, CLAUDIA	10.10.120.13	TARAZONA TRUJILLO MARLENE	10.10.120.53	CASTILLO ROJAS, SUSANA
4TO FISCAL	10.10.107.24	OSCAR SERRANO	10.10.107.54	Jorge López Rodríguez	10.10.107.94	SOLIS BARRUETA, ALEACIB	10.10.107.134	Raúl Caballero Castillo	10.10.107.174	CAMARGO MORA, CECILIA RO	10.10.107.214	MARTEL TRUJILLO,JOHN	10.10.120.14	LIBERATO FALCON	10.10.120.54	MEDINA OLIVAS, JHONN
1ER F. ADJUNTO	10.10.107.25	EMILIA MORY	10.10.107.55	Enoc Quispe Nestares	10.10.107.95	LECARO ALVARADO, ROBERTO	10.10.107.135	Vertila Alvarez Huamán	10.10.107.175	BALBUENA CARRASCO, GIANC	10.10.107.215	TAUMA BACALLA, FELIPE	10.10.120.15	TICONA CASTRO, JUAN CARLOS	10.10.120.55	
2DO F. ADJUNTO	10.10.107.26	LIDA GONZALES	10.10.107.56	Evelyn Malpartida Acuña	10.10.107.96		10.10.107.136	Carito Lara Espinoza	10.10.107.176	RAMÍREZ VALDEZ, ROCÍO JAQ	10.10.107.216	RODIL NAUPAY, ALEXANDER	10.10.120.16	ROJAS TRUJILLO, ZULMA ROSALINDA	10.10.120.56	SERRANO MALPARTIDA, WILLI
3ER F. ADJUNTO	10.10.107.27	VILLAIZAN CAJAS, CESAR	10.10.107.57	Alicia Chagua Timoteo	10.10.107.97		10.10.107.137	Lesli Mendoza Fuentes	10.10.107.177	FRIAS SOTO, LUIS ALDO	10.10.107.217	CHANGARAY HUAMAN, TONY	10.10.120.17	CIPRIANO FRETEL, LUIS ENRIQUE	10.10.120.57	TIBURCIO FIGUEROA, JUAN CA
4TO F. ADJUNTO	10.10.107.28	CARLOS GARCIA, OSCAR	10.10.107.58	Dashiel Porras Arancial	10.10.107.98	CIENFUEGOS SALVATIERRA, K	10.10.107.138	Hands Coronado Andrade	10.10.107.178	VILLAREAL HERRERA, EVELYN	10.10.107.218	LEIVA CANTARO, TEODARDO	10.10.120.18	LUZ PINEDO	10.10.120.58	MINAYA SANCHEZ DE ARRAMB
5TO F. ADJUNTO	10.10.107.29	CAJA CULQUI, EUSEBIA ASUNT	10.10.107.59	APAZA HUISA, LALI	10.10.107.99	SILVA CARHUARICRA, MYLENE	10.10.107.139	Christian Prado Arteaga	10.10.107.179	HILARIO CALIXTO, GAVI VIOLE	10.10.107.219	GUTIERREZ GAMBOA, GISSELL	10.10.120.19	TARAZONA GONZALES, OLCHESE	10.10.120.59	ISLA HERRERA, YANET
6TO F. ADJUNTO	10.10.107.30	PALACIOS BORJA, JANEEL	10.10.107.60	APOLAYA LEVANO, VICTO	10.10.107.100	GALARZA BRAVO, ROSA	10.10.107.140	Silvia Chávez Montés	10.10.107.180	GARCIA LAURA, JUAN ANTON	10.10.107.220	VARGAS PAYA, GUILIANA	10.10.120.20	VARA BERROSPI, MARIA DEL ROSARIO	10.10.120.60	LLANO QUISPE, LUZMILA
7MO F. ADJUNTO	10.10.107.31		10.10.107.61	Victor Céspedes Guzmán	10.10.107.101	RICAPA CASTILLO, PEDRO	10.10.107.141	Jürghens Isaak Aicardi	10.10.107.181	CAMACHO LEON, GANDHY	10.10.107.221	PASQUEL PAREDES, LUIS	10.10.120.21	GOMEZ HERRERA, ELIZABETH GLADYS	10.10.120.61	MESA DE PARTES
8VO F. ADJUNTO	10.10.107.32	ESPINOZA CACHIS, VANESSA	10.10.107.62		10.10.107.102	PEREZ TERRAZAS, GRACE	10.10.107.142	Alan Suarez Ferrer	10.10.107.182	CÓRDOVA HUAMÁN, ROMEL	10.10.107.222	--	10.10.120.22		10.10.120.62	
AST.FUN.FIS 01	10.10.107.33	RENGIFO HIDALGO, MABEL	10.10.107.63	DIAZ REATEGUI, ELIZABET	10.10.107.103	MATIAS MEZA, ALDO	10.10.107.143	Mirko Flores Gómez	10.10.107.183	AMAYO CARDENAS, CHELY	10.10.107.223	SOLANO ROJAS, JHONATAN	10.10.120.23	ANCAJIMA SAAVEDRA, MARIA MILAG	10.10.120.63	
AST.FUN.FIS 02	10.10.107.34	VIA RAMIREZ, LAURA ROCIO	10.10.107.64		10.10.107.104	YATACO PEREZ, HUGO	10.10.107.144	Katty Inga Alcántara	10.10.107.184	DAVILA ROJAS, RICHARD NOE	10.10.107.224	CARRANZA TOLEDO, VLADIMI	10.10.120.24	ESTEBAN CAMACHO, ELMER ROLY	10.10.120.64	
AST.FUN.FIS 03	10.10.107.35	SANCHEZ DAVILA, ELVIS	10.10.107.65		10.10.107.105	TAPIA SAAVEDRA, SUSY	10.10.107.145	Gerber Quispe Machicado	10.10.107.185	ALBINO ABUNDO, JHON VENI	10.10.107.225	CHUMBIMUNI AGUILAR, SHER	10.10.120.25	SANCHEZ ALARCON, ALFREDO JHON	10.10.120.65	
AST.FUN.FIS 04	10.10.107.36	ADAMA ESPINOZA, FELIX	10.10.107.66	Patricia Figueroa Jaramill	10.10.107.106	HERRERA SALAZAR, IVAN	10.10.107.146	Mary Araujo Huaylinos	10.10.107.186	CHAMORRO MEZA, YULLY ISA	10.10.107.226	DIAZ PEREZ, LUIS FERNANDO	10.10.120.26	SALAZAR FONSECA, VANESSA	10.10.120.66	
AST.FUN.FIS 05	10.10.107.37	CARRASCO DIAZ, JORGE	10.10.107.67		10.10.107.107	ROJAS MANZANO, JUDITH	10.10.107.147	Luis Castillo Tapia	10.10.107.187	TARAZONA MORALES, ORLAN	10.10.107.227	SEDANO ZAPATA, PAMELA	10.10.120.27	TRUJILLO ROBLES, JONATHAN ADRUV	10.10.120.67	
AST.FUN.FIS 06	10.10.107.38	CARRASCO DIAZ, JORGE	10.10.107.68	Jesús valdivia Ramírez	10.10.107.108	DURAND ROBLES, ROY	10.10.107.148	Sorelinda Gallegos Torres	10.10.107.188	MILLA GARGUREVICH, INGRID	10.10.107.228	BASUALDO GRANDEZ, ANA	10.10.120.28	ARBIETO LEIVA, FELIX ZENON	10.10.120.68	
AST.FUN.FIS 07	10.10.107.39		10.10.107.69		10.10.107.109		10.10.107.149	Carolina Medrano Céspedes	10.10.107.189	ROSALES CHAVEZ, JULIO CESA	10.10.107.229	BERROSPI ZEVALLOS, CINDY	10.10.120.29	QUISPE PEREZ, SUSAN CATHERINE	10.10.120.69	
AST.FUN.FIS 08	10.10.107.40		10.10.107.70	Jimmy Santiago Espinoza	10.10.107.110	REATEGUI MESIA, MIGUEL	10.10.107.150	otilia llanos suarez	10.10.107.190	CUEVA FUSTER, DAVID RONAL	10.10.107.230	PARIONA LANDA, LIZET	10.10.120.30	RAMOS HUERTA, NADIA SAMANTHA	10.10.120.70	
AST.ADM. 01	10.10.107.41	CAROLA BECERRA	10.10.107.71	Antonina Espinoza Minaya	10.10.107.111		10.10.107.151	Mesa de partes	10.10.107.191	ALBINO BENITES, YULIANA	10.10.107.231	CASTILLA SOTO, CARLOS MIGU	10.10.120.31	VANESSA HUAMAN	10.10.120.71	Cano
AST.ADM. 02	10.10.107.42	ALEX ASESOR	10.10.107.72	HUETE RODRIGUEZ, ELBA	10.10.107.112		10.10.107.152	Gerson Chaupis Soto	10.10.107.192	AMANCIO MARTINEZ, BEATRI	10.10.107.232	MESA DE PARTES	10.10.120.32	AREVALO BERROSPI, BETTZZY ARLETT	10.10.120.72	
AST.ADM. 03	10.10.107.43		10.10.107.73	Solio Espinoza Tacuche	10.10.107.113		10.10.107.153	Henry Modesto Davila	10.10.107.193	CESPEDES LOPEZ, LEONCIO	10.10.107.233	CORREA COZ, OSCAR LIZARDO	10.10.120.33	LEANDRO MORA, VIVIANA	10.10.120.73	
AST.ADM. 04	10.10.107.44		10.10.107.74	CAMPOS ALFARO, KATERI	10.10.107.114	VIDAL LIZANDRO, JHULIANA	10.10.107.154	Susan Tarazona Herrera	10.10.107.194	GOMEZ OLARTE, DANIA SULEI	10.10.107.234	*MICHELL G.	10.10.120.34		10.10.120.74	
Impresora 01	**10.10.107.45**		**10.10.107.75**		**10.10.107.115**		**10.10.107.155**		**10.10.107.195**		**10.10.107.235**		**10.10.120.35**		**10.10.120.75**	
Impresora 02	**10.10.107.46**		**10.10.107.76**		**10.10.107.116**		**10.10.107.156**		**10.10.107.196**		**10.10.107.236**		**10.10.120.36**		**10.10.120.76**	
Impresora 03	**10.10.107.47**	**IMPRESORA ADMINIS**	**10.10.107.77**		**10.10.107.117**		**10.10.107.157**		**10.10.107.197**		**10.10.107.237**		**10.10.120.37**		**10.10.120.77**	
Impresora 04	**10.10.107.48**	**FOTOCOPIADORA PERSONAL**	**10.10.107.78**	**AGUIRRE FABIAN, CARLA**	**10.10.107.118**		**10.10.107.158**		**10.10.107.198**		**10.10.107.238**		**10.10.120.38**		**10.10.120.78**	
Fotocopiadora 01	**10.10.107.49**		**10.10.107.79**		**10.10.107.119**		**10.10.107.159**		**10.10.107.199**		**10.10.107.239**		**10.10.120.39**		**10.10.120.79**	
Fotocopiadora 02	**10.10.107.50**		**10.10.107.80**		**10.10.107.120**		**10.10.107.160**		**10.10.107.200**		**10.10.107.240**		**10.10.120.40**		**10.10.120.80**	
Reservas			10.10.107.81		10.10.107.121	BURGA BURGOS, JACKELINE	10.10.107.161	Asistonta de serna	10.10.107.201	william garay	10.10.107.241		10.10.120.41		10.10.120.81	
Reservas	10.10.107.16	Ivan Renadesple	10.10.107.82		10.10.107.122		10.10.107.162	cachis	10.10.107.202		10.10.107.242		10.10.120.42		10.10.120.82	
Reservas			10.10.107.83		10.10.107.123		10.10.107.163		10.10.107.203		10.10.107.243		10.10.120.43		10.10.120.83	
Reservas			10.10.107.84	percy lazo	10.10.107.124		10.10.107.164		10.10.107.204		10.10.107.244		10.10.120.44		10.10.120.84	
Reservas			10.10.107.85	Jaqueline Rodríguez Cáce	10.10.107.125		10.10.107.165		10.10.107.205		10.10.107.245		10.10.120.45		10.10.120.85	
Reservas			10.10.107.86		10.10.107.126		10.10.107.166		10.10.107.206		10.10.107.246		10.10.120.46		10.10.120.86	
Reservas			10.10.107.87	Personal Chino Alberth	10.10.107.127		10.10.107.167		10.10.107.207		10.10.107.247		10.10.120.47		10.10.120.87	
Reservas			10.10.107.88		10.10.107.128		10.10.107.168		10.10.107.208		10.10.107.248		10.10.120.48		10.10.120.88	
Reservas			10.10.107.89	renadesple tv	10.10.107.129		10.10.107.169		10.10.107.209		10.10.107.249		10.10.120.49		10.10.120.89	
Reservas			10.10.107.90		10.10.107.130		10.10.107.170		10.10.107.210		10.10.107.250		10.10.120.50		10.10.120.90	

Anexo N° 09: Lista de IP – Sede Central

CARGO	1RA SUPERIOR	2DA SUPERIOR	3RA SUPERIOR	4TA SUPERIOR	1RA SUP. FAMILIA	1RA FAMILIA	2DA FAMILIA	PREVENCION	INFORMATICA
1ER FISCAL	192.168.22.36	192.168.22.51	192.168.22.66	192.168.22.81	192.168.22.96	192.168.22.111	192.168.22.126	192.168.22.141	192.168.22.156
1ER F. ADJUNTO	192.168.22.37	192.168.22.52	192.168.22.67	192.168.22.82	192.168.22.97	192.168.22.112	192.168.22.127	192.168.22.142	192.168.22.157
2DO F. ADJUNTO	192.168.22.38	192.168.22.53	192.168.22.68	192.168.22.83	192.168.22.98	192.168.22.113	192.168.22.128	192.168.22.143	192.168.22.158
AST.FUN.FIS 01	192.168.22.39	192.168.22.54	192.168.22.69	192.168.22.84	192.168.22.99	192.168.22.114	192.168.22.129	192.168.22.144	192.168.22.159
AST.FUN.FIS 02	192.168.22.40	192.168.22.55	192.168.22.70	192.168.22.85	192.168.22.100	192.168.22.115	192.168.22.130	192.168.22.145	192.168.22.160
AST.ADM. 01	192.168.22.41	192.168.22.56	192.168.22.71	192.168.22.86	192.168.22.101	192.168.22.116	192.168.22.131	192.168.22.146	192.168.22.161
Impresora 01	192.168.22.42	192.168.22.57	192.168.22.72	192.168.22.87	192.168.22.102	192.168.22.117	192.168.22.132	192.168.22.147	192.168.22.162
Impresora 02	192.168.22.43	192.168.22.58	192.168.22.73	192.168.22.88	192.168.22.103	192.168.22.118	192.168.22.133	192.168.22.148	192.168.22.163
Fotocopiadora 01	192.168.22.44	192.168.22.59	192.168.22.74	192.168.22.89	192.168.22.104	192.168.22.119	192.168.22.134	192.168.22.149	192.168.22.164
Reservas	192.168.22.45	192.168.22.60	192.168.22.75	192.168.22.90	192.168.22.105	192.168.22.120	192.168.22.135	192.168.22.150	192.168.22.165
Reservas	192.168.22.46	192.168.22.61	192.168.22.76	192.168.22.91	192.168.22.106	192.168.22.121	192.168.22.136	192.168.22.151	192.168.22.166
Reservas	192.168.22.47	192.168.22.62	192.168.22.77	192.168.22.92	192.168.22.107	192.168.22.122	192.168.22.137	192.168.22.152	192.168.22.167
Reservas	192.168.22.48	192.168.22.63	192.168.22.78	1 192.168.22.93	192.168.22.108	192.168.22.123	192.168.22.138	192.168.22.153	192.168.22.168
Reservas	192.168.22.49	192.168.22.64	192.168.22.79	192.168.22.94	192.168.22.109	192.168.22.124	192.168.22.139	192.168.22.154	192.168.22.169
Reservas	192.168.22.50	192.168.22.65	192.168.22.80	192.168.22.95	192.168.22.110	192.168.22.125	192.168.22.140	192.168.22.155	192.168.22.170

CARGO	ADMINISTRACION	CARGO	PRESIDENCIA		CARGO	POLICIA		Terrorismo	
ADMINISTRADOR	192.168.22.21	Presidente	192.168.22.171	cabezon	Jefe Policia	192.168.22.186		1ER FISCAL	192.168.22.201
JEFE PERSONAL	192.168.22.22	Coordinador	192.168.22.172	jimy	Policia 1	192.168.22.187		1ER F. ADJUNTO	192.168.22.202
JEFE LOGISTICA	192.168.22.23	Mesa de Partes	192.168.22.173	leslie	Policia 2	192.168.22.188		2DO F. ADJUNTO	192.168.22.203
ANALISTA ADM.	192.168.22.24	Asistete Funcisc	192.168.22.174	segundo	Policia 3	192.168.22.189		AST.FUN.FIS 01	192.168.22.204
ANALISTA LOG.	192.168.22.25	AST.ADM. 01	192.168.22.175	nina	Policia 4	192.168.22.190		AST.FUN.FIS 02	192.168.22.205
AST.ADM. 01	192.168.22.26	Secretaria	192.168.22.176	fabiola	Policia 5	192.168.22.191		AST.ADM. 01	192.168.22.206
Impresora 01	192.168.22.27	Impresora 01	192.168.22.177		Impresora 01	192.168.22.192		Impresora 01	192.168.22.207
Impresora 02	192.168.22.28	Impresora 02	192.168.22.178		Impresora 02	192.168.22.193		Impresora 02	192.168.22.208
Fotocopiadora 01	192.168.22.29	Fotocopiadora 01	192.168.22.179		Fotocopiadora 01	192.168.22.194		Fotocopiadora 01	192.168.22.209
Reservas	192.168.22.30	Reservas	192.168.22.180		Reservas	192.168.22.195	personal nuevo	Reservas	192.168.22.210
Reservas	192.168.22.31	Reservas	192.168.22.181		Reservas	192.168.22.196		Reservas	192.168.22.211
Reservas	192.168.22.32	Reservas	192.168.22.182	Impresora FS4300DN	Reservas	192.168.22.197		Reservas	192.168.22.212
Reservas	192.168.22.33	Reservas	192.168.22.183	Laptop roja	Reservas	192.168.22.198		Reservas	192.168.22.213
Reservas	192.168.22.34	Reservas	192.168.22.184	nylan	Reservas	192.168.22.199		Reservas	192.168.22.214
Reservas	192.168.22.35	Reservas	192.168.22.185		Reservas	192.168.22.200		Reservas	192.168.22.215

Anexo N° 10: Lista de IP – FEMA y DML

CARGO	DROGAS		AMBIENTAL	
1ER FISCAL	10.10.108.21		10.10.108.36	
1ER F. ADJUNTO	10.10.108.22		10.10.108.37	
2DO F. ADJUNTO	10.10.108.23		10.10.108.38	
AST.FUN.FIS 01	10.10.108.24		10.10.108.39	
AST.FUN.FIS 02	10.10.108.25		10.10.108.40	
AST.ADM. 01	10.10.108.26		10.10.108.41	
Impresora 01	10.10.108.27		10.10.108.42	
Impresora 02	10.10.108.28		10.10.108.43	
Fotocopiadora 01	10.10.108.29		10.10.108.44	
Reservas	10.10.108.30		10.10.108.45	
Reservas	10.10.108.31		10.10.108.46	
Reservas	10.10.108.32		10.10.108.47	
Reservas	10.10.108.33		10.10.108.48	
Reservas	10.10.108.34		10.10.108.49	
Reservas	10.10.108.35		10.10.108.50	

CARGO	ADMINISTRACION				CARGO	PRESIDENCIA		Policia	PRESIDENCIA		
ADMINISTRADOR	192.168.22.21				Presidente	192.168.22.171		Jefe Policia	192.168.22.186		
JEFE PERSONAL	192.168.22.22				Coordinador	192.168.22.172		Policia 1	192.168.22.187		
JEFE LOGISTICA	192.168.22.23				Mesa de Partes	192.168.22.173		Policia 2	192.168.22.188		
ANALISTA ADM.	192.168.22.24				Asistete Funcisc	192.168.22.174		Policia 3	192.168.22.189		
ANALISTA LOG.	192.168.22.25				AST.ADM. 01	192.168.22.175		Policia 4	192.168.22.190		
AST.ADM. 01	192.168.22.26				Secretaria	192.168.22.176		Policia 5	192.168.22.191		
Impresora 01	**192.168.22.27**				Impresora 01	**192.168.22.176**		Impresora 01	**192.168.22.176**		
Impresora 02	192.168.22.28				Impresora 02	192.168.22.178		Impresora 02	192.168.22.193		
Fotocopiadora 01	192.168.22.29				Fotocopiadora 01	192.168.22.179		Fotocopiadora 01	192.168.22.194		
Reservas	192.168.22.30				Reservas	192.168.22.180		Reservas	192.168.22.195		
Reservas	192.168.22.31				Reservas	192.168.22.181		Reservas	192.168.22.196		
Reservas	192.168.22.32				Reservas	192.168.22.182		Reservas	192.168.22.197		
Reservas	192.168.22.33				Reservas	192.168.22.183		Reservas	192.168.22.198		
Reservas	192.168.22.34				Reservas	192.168.22.184		Reservas	192.168.22.199		
Reservas	192.168.22.35				Reservas	192.168.22.185		Reservas	192.168.22.200		

Anexo N° 11: Lista de IP – Sede Control Interno

CARGO	1RA	2DA	3RA	4TA	5TA	6TA	2DA FAMILIA	PREVENCION	INFORMATICA
COORDINADOR	10.10.119.21	10.10.119.39	10.10.119.57	10.10.119.75	192.168.22.96	192.168.22.111	192.168.22.126	192.168.22.141	192.168.22.156
Provincial 1	10.10.119.22	10.10.119.40	10.10.119.58	10.10.119.76	192.168.22.97	192.168.22.112	192.168.22.127	192.168.22.142	192.168.22.157
Provincial 2	10.10.119.23	10.10.119.41	10.10.119.59	10.10.119.77	192.168.22.98	192.168.22.113	192.168.22.128	192.168.22.143	192.168.22.158
AST.FUN.FIS 01	10.10.119.24	10.10.119.42	10.10.119.60	10.10.119.78	192.168.22.99	192.168.22.114	192.168.22.129	192.168.22.144	192.168.22.159
AST.FUN.FIS 02	10.10.119.25	10.10.119.43	10.10.119.61	10.10.119.79	192.168.22.100	192.168.22.115	192.168.22.130	192.168.22.145	192.168.22.160
AST.FUN.FIS 03	10.10.119.26	10.10.119.44	10.10.119.62	10.10.119.80	192.168.22.101	192.168.22.116	192.168.22.131	192.168.22.146	192.168.22.161
AST.FUN.FIS 04	10.10.119.27	10.10.119.45	10.10.119.63	10.10.119.81	**192.168.22.102**	**192.168.22.117**	**192.168.22.132**	**192.168.22.147**	**192.168.22.162**
AST.ADM. 01	10.10.119.28	10.10.119.46	10.10.119.64	10.10.119.82	192.168.22.103	192.168.22.118	192.168.22.133	192.168.22.148	192.168.22.163
AST.ADM. 02	10.10.119.29	10.10.119.47	10.10.119.65	10.10.119.83	192.168.22.104	192.168.22.119	192.168.22.134	192.168.22.149	192.168.22.164
Impresora 01	**10.10.119.30**	**10.10.119.48**	**10.10.119.66**	**10.10.119.84**	192.168.22.105	192.168.22.120	192.168.22.135	192.168.22.150	192.168.22.165
Impresora 02	**10.10.119.31**	**10.10.119.49**	**10.10.119.67**	**10.10.119.85**	192.168.22.106	192.168.22.121	192.168.22.136	192.168.22.151	192.168.22.166
Fotocopiadora 01	**10.10.119.32**	**10.10.119.50**	**10.10.119.68**	**10.10.119.86**	192.168.22.107	192.168.22.122	192.168.22.137	192.168.22.152	192.168.22.167
Reservas	10.10.119.33	10.10.119.51	10.10.119.69	10.10.119.87	192.168.22.108	192.168.22.123	192.168.22.138	192.168.22.153	192.168.22.168
Reservas	10.10.119.34	10.10.119.52	10.10.119.70	10.10.119.88	192.168.22.109	192.168.22.124	192.168.22.139	192.168.22.154	192.168.22.169
Reservas	10.10.119.35	10.10.119.53	10.10.119.71	10.10.119.89	192.168.22.110	192.168.22.125	192.168.22.140	192.168.22.155	192.168.22.170
Reservas	10.10.119.36	10.10.119.54	10.10.119.72	10.10.119.90					
Reservas	10.10.119.37	10.10.119.55	10.10.119.73	10.10.119.91					
Reservas	10.10.119.38	10.10.119.56	10.10.119.74	10.10.119.92					

CARGO	ADMINISTRACION		CARGO	PRESIDENCIA		CARGO	POLICIA		
ADMINISTRADOR	192.168.22.21		**Presidente**	192.168.22.171		**Jefe Policia**	192.168.22.186		
JEFE PERSONAL	192.168.22.22		**Coordinador**	192.168.22.172		**Policia 1**	192.168.22.187		
JEFE LOGISTICA	192.168.22.23		**Mesa de Partes**	192.168.22.173		**Policia 2**	192.168.22.188		
ANALISTA ADM.	192.168.22.24		**Asistete Funcisc**	192.168.22.174		**Policia 3**	192.168.22.189		
ANALISTA LOG.	192.168.22.25		**AST.ADM. 01**	192.168.22.175		**Policia 4**	192.168.22.190		
AST.ADM. 01	192.168.22.26		**Secretaria**	192.168.22.176		**Policia 5**	192.168.22.191		
Impresora 01	**192.168.22.27**		**Impresora 01**	**192.168.22.177**		**Impresora 01**	**192.168.22.176**		
Impresora 02	192.168.22.28		**Impresora 02**	192.168.22.178		**Impresora 02**	192.168.22.193		
Fotocopiadora 01	192.168.22.29		**Fotocopiadora 01**	192.168.22.179		**Fotocopiadora 01**	192.168.22.194		
Reservas	192.168.22.30		**Reservas**	192.168.22.180		**Reservas**	192.168.22.195		
Reservas	192.168.22.31		**Reservas**	192.168.22.181		**Reservas**	192.168.22.196		
Reservas	192.168.22.32		**Reservas**	192.168.22.182		**Reservas**	192.168.22.197		
Reservas	192.168.22.33		**Reservas**	192.168.22.183		**Reservas**	192.168.22.198		
Reservas	192.168.22.34		**Reservas**	192.168.22.184		**Reservas**	192.168.22.199		
Reservas	192.168.22.35		**Reservas**	192.168.22.185		**Reservas**	192.168.22.200		

Anexo N° 12: Lista de IP – Sede Anticorrupción

CARGO	SUPERIOR		1DESPCHCO	2DESPCHCO		3DESPCHCO	4TODESPCHCO	0	CARGO	OFICINAS	
COORDINADOR	10.10.100.21	Superior	10.10.100.36	10.10.100.51		10.10.100.66	10.10.100.81		MESA UNICA	10.10.100.96	
1ER F. ADJUNTO	10.10.100.22	Jeremias	10.10.100.37	10.10.100.52	Laura Nuñez	10.10.100.67	10.10.100.82		AUDIO VIDEO	10.10.100.97	
2DO F. ADJUNTO	10.10.100.23	Johana	10.10.100.38	10.10.100.53		10.10.100.68	10.10.100.83		PERITO CONTA	10.10.100.98	
AST.FUN.FIS 01	10.10.100.24		10.10.100.39	10.10.100.54	sivya	10.10.100.69	10.10.100.84		PERITO CIVIL	10.10.100.99	
AST.FUN.FIS 02	10.10.100.25		10.10.100.40	10.10.100.55		10.10.100.70	10.10.100.85		NOTIFICADORES	10.10.100.100	
AST.ADM. 01	10.10.100.26		10.10.100.41	10.10.100.56	Mayra	10.10.100.71	10.10.100.86		NOTIFICADORES	10.10.100.101	
Impresora 01	**10.10.100.27**		**10.10.100.42**	**10.10.100.57**		**10.10.100.72**	**10.10.100.87**		**Impresora 01**	**10.10.100.102**	
Impresora 02	**10.10.100.28**		**10.10.100.43**	**10.10.100.58**		**10.10.100.73**	**10.10.100.88**		**Impresora 02**	**10.10.100.103**	
Fotocopiadora 01	**10.10.100.29**		**10.10.100.44**	**10.10.100.59**		**10.10.100.74**	**10.10.100.89**		**Fotocopiadora 01**	**10.10.100.104**	
Fotocopiadora 02	**10.10.100.30**		**10.10.100.45**	**10.10.100.60**		**10.10.100.75**	**10.10.100.90**		**Fotocopiadora 02**	**10.10.100.105**	
Reservas	10.10.100.31		10.10.100.46	10.10.100.61		10.10.100.76	10.10.100.91	Sindy Rojas Panduro	**Reservas**	10.10.100.106	
Reservas	10.10.100.32		10.10.100.47	10.10.100.62		10.10.100.77	10.10.100.92		**Reservas**	10.10.100.107	
Reservas	10.10.100.33		10.10.100.48	10.10.100.63		10.10.100.78	10.10.100.93		**Reservas**	10.10.100.108	
Reservas	10.10.100.34		10.10.100.49	10.10.100.64		10.10.100.79	10.10.100.94		**Reservas**	10.10.100.109	
Reservas	10.10.100.35		10.10.100.50	10.10.100.65		10.10.100.80	10.10.100.95		**Reservas**	10.10.100.110	Dr. Virgilio