# UNIVERSIDAD SAN PEDRO

# FACULTAD DE INGENIERÍA

**PROGRAMA DE ESTUDIO DE INGENIERIA INFORMÁTICA Y DE SISTEMAS**


## DISEÑO DE UN SISTEMA DE SEGURIDAD DE LA RED DE DATOS PARA GESTIONAR LOS RECURSOS INFORMATICOS EN LA DIRECCIÓN REGIONAL DE EDUCACIÓN DE LIMA – PROVINCIAS 2013 DRELP

TESIS PARA OPTAR EL TITULO DE INGENIERO EN INFORMATICA Y DE SISTEMAS

**AUTORES**

Mauricio Prado, Ángela Antonella

Romero Urbina, Fernando Javier

**ASESOR**

Arroyo Tirado, Jorge Luis

Código Orcid: 0000-0001-6263-5721

Huacho – Perú

**2021**

## Palabras Clave

| | |
|---|---|
| *Tema* | Redes |
| *Especialidad* | Seguridad de redes |

## Keywords

| | |
|---|---|
| *Topic* | Networks |
| *Speciality* | Network Security |

### Línea de Investigación

| | |
|---|---|
| *Área* | Ingeniería y Tecnología |
| *Sub Área* | Ingeniería Eléctrica, Electrónica e Informática |
| *Disciplina* | Telecomunicaciones |
| *Línea* | Infraestructura de Tecnología de Información |

# “DISEÑO DE UN SISTEMA DE SEGURIDAD DE LA RED DE DATOS PARA GESTIONAR LOS RECURSOS INFORMATICOS EN LA DIRECCIÓN REGIONAL DE EDUCACIÓN DE LIMA – PROVINCIAS 2013 DRELP”

# INDICE

## RESUMEN

A lo largo de la historia las redes han logrado manipular los datos de la información, optimizando el tiempo de trabajo y automatizando tareas y procesos para el ser humano. Pero a la vez han estado apareciendo amenazas que afectan la seguridad de la información. Es por ello que al ver la problemática existente en la Dirección Regional de Educación de Lima Provincias - DRELP hemos optado por dar una propuesta que brinde mayor seguridad de la información cumpliendo con las normas y estándares establecidos.

Nuestra investigación está orientada a identificar controles y sistemas en base a normas y estándares informáticos utilizando la metodología del ISO 27001, el cual nos permiten establecer pautas para las mejoras continuas de los servicios de red, previniendo así que la información y datos de nuestra institución no se vean vulnerados ante cualquier eventualidad.

Este trabajo, der ser implementado mejorará la seguridad física de la institución cumpliendo con las normas establecidas y la seguridad lógica brindando mayor protección a los datos e información de la institución, siendo más difícil la vulnerabilidad de estos.

# ABSTRACT

Throughout history have managed to manipulate network data information, optimizing working time and automating tasks and processes to humans. But both have been appearing threats to the information security. That is why seeing the problems in the Regional Education Directorate Andhra Pradesh - DRELP have chosen to give a proposal to provide greater information security standards and compliance with established standards.

Our research is aimed at identifying controls and systems based on IT standards and rules using the methodology of ISO 27001, which allows us to establish guidelines for continuous improvement of the network services, thus preventing information and data from our institution does not are violated for any eventuality.

This job, to be implemented der improve the security of the institution in compliance with established safety rules and logic providing better protection for data and information about the institution, the vulnerability of being more difficult.

# INTRODUCCION

## Antecedentes y fundamentación científica

Rubén Bustamante Sánchez (2006), Desarrolló un estudio de ciberseguridad, en el que especifica que existen dos tipos de ciberseguridad: seguridad física y seguridad lógica. En el primer caso se debe estar atento a cualquier incidencia que se presente, y tomar medidas preventivas. En el segundo, tener cuidado con aquellos que no deben acceder a la información, como piratas informáticos, piratas informáticos, etc. Quien busca algo que le interesa y luego puede poseerlo, o también puede probar hasta dónde puede llegar, explotando la vulnerabilidad de la víctima, como la ingenuidad del sistema operativo o de los trabajadores al recibir archivos desconocidos y abrirlos, a través de virus u otro tipo de herramienta infecta el sistema. Es por esto que se deben tomar medidas preventivas para combatir estos delitos, ya sea a través de políticas de seguridad organizacional, herramientas de seguridad del sistema operativo o capacitación del personal, que es fundamental para obtener una buena seguridad.

Asimismo, Juan Pablo Orjuela (2010) Muestra que su investigación tiene como objetivo proponer el diseño e implementación de LAN mediante la aplicación de arquitectura de cableado y administración de redes, lo que propone analizar el estado actual para actualizarlo, para luego intercambiar y estandarizar al 100% la red. La tecnología utilizada para la recolección de datos son las encuestas y las herramientas utilizadas son cuestionarios relacionados con la situación de docentes y estudiantes. Los resultados del estudio muestran que los estudiantes que viven lejos del centro local UNA-Amazonas tienen dificultades para recibir asesoramiento por teléfono y desean un método de aprendizaje a distancia personalizado. Por otro lado, la administración determinó que no todas las oficinas pueden compartir sus recursos. Método de análisis de sistema aplicado. Con la implementación de esta infraestructura, proporciona varias condiciones de valor importante porque ayuda a controlar de manera efectiva las actividades.

Por su parte, Nuttsy Aurora Lazo García (2012) En su trabajo sobre el diseño e implementación de la LAN denominado PUCP, consideró que, debido al desarrollo de Internet, hoy nos enfrentamos a una nueva forma de comunicación en un entorno globalizado. Para tal fin, se propuso diseñar e implementar redes LAN y WLAN que puedan evitar el robo de identidad y reducir la brecha entre las redes cableadas tradicionales y las redes inalámbricas en términos de seguridad. Además, utilizan protocolos GLBP y Etherchannel, en calidad de medios para el control y redundancia en el control de transferencia de datos como mecanismos de redundancia y controlar el ancho de banda por medio del balanceo de carga para optimizar los recursos en la red. También implementa un sistema de control de acceso AAA (autenticación, autorización y contabilidad) y lo implementa utilizando los protocolos TACACS y RADIUS, ambos de arquitectura cliente / servidor. En la autenticación de usuarios y administración de archivos y sus atributos.

Finalmente, Milla Cazana (2012) diseñó una red LTE para el distrito de Callao, Long Term Evolution es el nombre detrás de estas siglas y representa una tecnología móvil. En el futuro, en comparación con otras tecnologías, LTE permitirá velocidades de transmisión de datos muy altas y menores retrasos en los paquetes de datos, que es una demanda cada vez mayor en los servicios actuales. Por lo tanto, lo mejor es utilizar esta red porque cuenta con diferentes instalaciones deportivas, sectores industriales, especialmente el Aeropuerto Internacional Jorge Chávez, que generará mucho tráfico. Por lo tanto, a través de este diseño, se espera atender la demanda generada en la región.

## Justificación de la investigación

En el presente proyecto mejoraremos el aspecto del ambiente de la institución dando una mejor imagen en lo que respecta al cableado del área de informática y los demás departamentos, también contaremos con un sistema de validación y manejo de usuarios la cual permitirá controlar de una mejor manera el uso de los equipos de cómputo.

Desarrollaremos íntegramente utilizando LINUX GNU, un sistema operativo cuya naturaleza lo hace estable y nos ofrece seguridad y flexibilidad.
En este sentido, la presente investigación está justificada por:

- ✓ **Justificación Operativa:**
  - Mejorar el control sobre los usuarios evitando el uso de software no autorizado que ocasione daños a la información de la institución.
  - Evitar el uso indebido de internet por parte de los trabajadores, de esta manera se mejora el acceso y servicio.
  - Administrar de modo eficiente las computadoras de todos los departamentos de la DRELP en prevención de incidentes que puedan dañar los equipos informáticos.
  - Mejorar el control físico sobre los equipos ya que se contara con un sistema de vigilancia a través de cámaras.

- ✓ **Justificación Económica:**
  - En la actualidad implementar soluciones a nivel de servidores es costoso sobre todo por las licencias a adquirir, aparte de la compra de software y programas que se deberán instalar en el servidor, pero al trabajar con Linux, las licencias no tiene un costo ya que es un software libre.

## Problema

### Situación Problemática

La Dirección Regional de Educación de Lima Provincias-DRELP, en la actualidad cuenta con cableado estructurado inadecuado que permite comunicar el área de informática con las demás áreas de la DRELP, así también todas las áreas no cuentan con acceso a internet. El cableado actual no cumple con las normas establecidas, ya que este cableado no está debidamente instalado, no cuenta en gran parte con canaletas, esto hace que los cables se encuentren en mal estado y estén colgando por todas las áreas de la DRELP. En síntesis, el servicio que se presta a través de la red es deficiente.

Asimismo, respecto del uso de internet por parte del personal se encuentra normado, ya que sólo pueden acceder a algunas páginas de internet para uso estrictamente de trabajo, pero no siempre se cumple con esta norma establecida. Los servidores se encuentran en una habitación que no tiene la más mínima seguridad, no cumplen con las normas establecidas, los software no son originales ni se encuentran debidamente licenciados, tan sólo el antivirus es original pero con licencia hasta el 31 de diciembre de 2013. En este aspecto, la red también es deficiente.

Ante tal situación, los autores, con finalidad de solucionar esta problemática, nos hemos planteado la siguiente interrogante:

**¿Cómo diseñar un sistema de seguridad de la red de datos para gestionar los recursos informáticos en la Dirección Regional de Educación de Lima Provincias-DRELP?**

## Conceptualización y Operacionalización de la Variable

Como punto de partida de nuestro marco referencial procedemos a describir los siguientes aspectos.

### 5.4.Normas Técnicas de Seguridad utilizadas en la empresa

**A. <u>Normas Técnicas de Seguridad Física</u>**

- Directiva No. 008-95-INEI / SJI "Recomendaciones Técnicas para la Protección Física de Equipos y Medios de Procesamiento de Información en la Administración Pública", aprobada por Resolución Jefatural 090-95-INEI.
- Directiva 500-04 Mantenimiento de equipos de cómputo: La gerencia de cada unidad debe formular una política de mantenimiento de equipos de cómputo para optimizar su rendimiento
- La norma técnica peruana "NTP-ISO / IEC 17799: 2007 EDI. Tecnología de la Información. Código Buenas Prácticas en Gestión

de Seguridad de la Información. Segunda. Versión" aprobó la Resolución Ministerial No. 2007 entre todas las entidades que integran el sistema informático nacional. Aprobación 246-2007-PCM La Resolución Ministerial No. 129-2012PCM que aprueba el uso obligatorio de la norma EDI NTP-ISO / IEC 27001: 2008. tecnologías de la información. tecnología de seguridad. Sistema de gestión de seguridad de la información: "Acerca de la seguridad física y ambiental".

**B. <u>Normas Técnicas de Seguridad Lógica</u>**

- Directiva No. 015-94-INEI / SJI-Normas Técnicas para el Almacenamiento y Respaldo de Información Procesada por Entidades Nacionales-Aprobada por Resolución 340-94-INEI.
- "Normas para la Prevención, Detección y Eliminación de Virus Informáticos en Equipos Informáticos de las Administraciones Públicas", aprobado mediante Resolución 362-94-INEI.
- "Recomendaciones Técnicas sobre Seguridad e Integridad en el Tratamiento de la Información Administrativa Pública", aprobadas mediante Resolución. O76-95-INEI.

**Normas ISO 27001**

**POLITICA DE SEGURIDAD**

- Política De La Seguridad De La Información
- Documento De Política De La Seguridad De Información
- Revisión Y Evaluación

**ASPECTOS ORGANIZATIVOS PARA LA SEGURIDAD**

- Organización Interna
- Comité De Gestión De Seguridad De La información
- Coordinación De La Seguridad De La Información
- Asignación De Responsabilidades Sobre Seguridad De La Información

- Proceso De Autorización De Recursos Para El Tratamiento De La información
- Acuerdos De Confiabilidad
- Contactos Con Autoridades
- Contactos Con Grupos De Interés Social
- Revisión Independiente De La Seguridad De La información
- Seguridad En El Acceso De Terceras Partes
- Identificación De Los Riesgos Por El Acceso De Terceros.

## SEGURIDAD FISICA Y DEL ENTORNO

### AREAS SEGURAS

- Para evitar el acceso no autorizado, daños e interferencias con la sede y la información de la empresa, se recomienda implementar una política de limpieza de escritorios y pantallas para reducir estos riesgos. Además, las instalaciones que procesan información crítica o sensible deben definirse como un cerco dentro el área protegida y un adecuado control de acceso. "La protección debe ser acorde con el riesgo identificado".
- Perímetro De Seguridad
- Controles Físicos De Entradas
- Seguridad De Oficinas, Despachos Y Recursos
- Protección Contra Amenazas Externas Y Ambientales
- Trabajo En Las Áreas Seguras
- Áreas De Cargas, Descarga Y Acceso Seguro

**SEGURIDAD DE LOS EQUIPOS**

- Instalación Y Protección De Equipos
- Suministro Eléctrico
- Seguridad Del Cableado
- Mantenimiento De Equipos
- Seguridad De Equipos Fuera De Los Locales De La Organización
- Seguridad En La Reutilización O Eliminación De Equipos
- Traslado De Activos

**SEGURIDAD INFORMATICA**

La seguridad informática, es el área de la informática se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta (incluyendo la información contenida).

Objetivos:

La seguridad informática está concebida para proteger los activos informáticos, entre los que se encuentran:

- **La información contenida**

  Se ha convertido en uno de los elementos más importantes dentro de una organización. La seguridad informática debe ser administrada según los criterios establecidos por los administradores y supervisores, evitando que usuarios externos y no autorizados puedan acceder a ella sin autorización.

  **• Infraestructura informática**

  La parte básica del almacenamiento y la gestión de la información y el funcionamiento de la organización. La función de la seguridad informática en este sentido es asegurar que el

equipo funcione correctamente y anticipar robos, incendios, boicots, desastres naturales, cortes de energía y cualquier otro plan de falla que amenace la infraestructura informática.

**• Usuario**

Son personas que utilizan estructuras técnicas, campos de comunicación e información de gestión. La seguridad informática debe establecer estándares para minimizar el riesgo de información o infraestructura informática. Estas reglas incluyen horarios laborales, restricciones en determinados lugares, autorizaciones, denegaciones, perfiles de usuario, planes de contingencia, convenios y todo lo necesario para lograr un buen nivel de seguridad informática. (Wikipedia, s.f.).

## SEGURIDAD FISICA

Cuando hablamos de seguridad física, nos estamos refiriendo a todos estos mecanismos -generalmente de prevención y detección- diseñados para proteger físicamente cualquier recurso del sistema; estos recursos van desde un simple teclado hasta una cinta de respaldo que contiene toda la información del sistema, pasando por los de la máquina. propia CPU. A continuación, mencionaremos algunos de los problemas de seguridad física que podemos enfrentar y qué medidas podemos tomar para evitar estos problemas o al menos minimizar su impacto.

**Protección de hardware**

El hardware suele ser el elemento más caro de cualquier sistema informático, por lo que las medidas para garantizar su integridad son una parte importante de la seguridad física de cualquier organización.

Los problemas que enfrentamos: acceso físico, desastres naturales e interferencia ambiental.

**Electricidad**

a) Electricidad: Quizás los problemas más comunes en el entorno de trabajo son los relacionados con el sistema eléctrico que alimenta nuestro equipo; cortocircuitos, picos de voltaje y cortes de corriente. Para corregir el problema de sobretensión, podemos instalar una conexión a tierra o un filtro de regulación de tensión.

b) Ruido eléctrico: El ruido eléctrico es generado por motores eléctricos o maquinaria pesada, así como otras computadoras o equipos diversos, y se transmite a través de espacios o líneas eléctricas cercanas a nuestras instalaciones.

**c)** Temperatura extrema: Las temperaturas muy altas, ya sean sobrecalentadas o extremadamente frías, pueden dañar gravemente todos los equipos. Protección de datos, Además de proteger el hardware, nuestra estrategia de seguridad también debe incluir medidas de protección de datos, porque de hecho el propósito de la mayoría de los ataques es obtener información, no destruir el medio físico que contiene la información.

**d) Eavesdropping**

La interceptación o escuchas clandestinas es el proceso por el cual un agente captura información dirigida a él; esta captura se puede hacer de muchas formas: olfateando en una red Ethernet o inalámbrica (el dispositivo entra en modo promiscuo y analiza todo el tráfico que pasa por la red), capturando electromagnéticos radiación (Muy caro, pero permite la detección de pulsaciones de teclas, contenido de pantalla), etc.

e) Copia de seguridad

Obviamente, se necesita establecer una estrategia de respaldo adecuada en la organización; al igual que los dispositivos y sistemas, los medios en los que se ubican estas copias deben estar protegidos físicamente; de hecho, quizás deberíamos usar medidas más fuertes en el servidor.

f) Medios no electrónicos

Otro factor importante en la protección de la información son los elementos no electrónicos que se utilizan para transmitir información, principalmente papel. (Impresoras, plotters, faxes, teletipos).

**Acciones Hostiles**

Se trata de especificar las medidas de seguridad que se deben tomar para prevenir robos, actos vandálicos o fraudes.

a). robo:

Las computadoras son activos muy valiosos de la empresa y pueden ser fácilmente "robadas", al igual que algunas acciones o incluso dinero. Los operadores suelen utilizar las computadoras de la empresa para realizar trabajos privados para otras organizaciones, robando así tiempo de la máquina. Puede copiar información importante o confidencial.

b) Fraude:

De hecho, las pérdidas causadas por el fraude y los problemas de prevención y detección del fraude están aumentando en los sistemas informáticos.

c) Sabotaje:

El peligro más temido para los centros de procesamiento de datos es el sabotaje. Las empresas que intentan implementar programas de seguridad avanzados han descubierto que prevenir el sabotaje es

uno de los desafíos más abrumadores. Puede ser un empleado o alguien ajeno a la propia empresa.

**d). No colocar vidrios exteriores como pared y ventanas en locales de riesgo**

El centro de procesamiento de datos ubicado entre las paredes de vidrio inferiores o las ventanas de vidrio grandes es fácil de ver desde la acera o lugares altos y vulnerable a los ataques. Estos centros de procesamiento de datos se enfrentan a estrategias destructivas que pueden ser adoptadas por grupos o individuos disidentes.

**GNU/ LINUX**

Según Talens-Oliag, T. (n.d.) GNU / Linux es uno de los términos utilizados para referirse al kernel libre similar a Unix o la combinación del kernel Linux y el sistema GNU. Su desarrollo es uno de los ejemplos más destacados de software libre. Cualquiera puede usar, modificar y redistribuir libremente todo su código fuente bajo los términos de GPL (Licencia Pública General GNU) Como sistema de programación La colección de utilidades de programación GNU es, con mucho, la familia de compiladores más utilizada en este sistema operativo. Tiene la capacidad de compilar C, C ++, Java, Ada, Pascal y otros lenguajes. También admite varias arquitecturas a través de la compilación cruzada, lo que lo convierte en un entorno adecuado para el desarrollo heterogéneo.

Hay una variedad de entornos de desarrollo integrados disponibles para GNU / Linux, incluidos Anjuta, KDevelop, Lazarus, Ultimate ++, Code: Blocks, NetBeans IDE y Eclipse. También hay editores extensibles, como Emacs o Vim. GNU / Linux también tiene una función de lenguaje de scripting Además del clásico lenguaje de programación de shell, o

procesador de texto llamado modo awk y expresión regular, la mayoría de las distribuciones tienen instalado Python, Perl, PHP y Ruby.

**Aplicaciones de usuario**

Las aplicaciones GNU / Linux se distribuyen principalmente en formatos .deb y .rpm, que fueron creados por desarrolladores de Debian y Red Hat, respectivamente. También puede instalar aplicaciones desde el código fuente en todas las distribuciones.

**Software de código cerrado para GNU / Linux**

En las primeras etapas, había pocas aplicaciones de código cerrado para GNU / Linux. Con el tiempo, los programas no libres se han adaptado a sistemas GNU / Linux, incluidos Adobe Reader, Adobe Flash, Opera, etc.

## Hipótesis

No es necesaria una Hipótesis porque está dada de manera explícita.

## Variables

- **Sistema Seguridad:** Sistema de Software que se instala en el ordenador para evitar el acceso no autorizado desde internet.
  **Dimensiones:** Riesgos, confiabilidad y cumplimiento
- **Gestión de Recursos:** administración de recursos de la cual se produce un beneficio.
  **Dimensiones:** Control, Auditabilidad y Capacitación.

## Objetivos

Diseñar un sistema de seguridad de la red de datos para gestionar los recursos informáticos en la Dirección Regional de Educación de Lima Provincias DRELP.

**Objetivos específicos:**

- Determinar un diagnostico institucional referente al análisis físico y lógico de la red de datos actual de la DRELP.
- Identificar el Análisis físico y lógico de la red de datos de la DRELP.
- Aplicar la Metodología ISO 27001 en la DRELP para dar seguridad física y lógica.
- Diseñar un sistema de seguridad de datos basada en estándares para la DRELP.

# METODOLOGIA

Una vez aplicada la encuesta, realizamos los gráficos estadísticos que nos revelaron cual es realmente el estado de la red actual en la DRELP, que permitió observar las dificultades que se presentan periódicamente y que realizan el manejo de la información y el trabajo dentro de la institución.

Estos resultados nos permitieron como base para proponer un diseño que mejore la red y que permita el mejor procesamiento y manejo de la información.

## Tipo y Diseño de Investigación

### A. Tipo de Investigación

De acuerdo a la orientación del presente trabajo de investigación el tipo de investigación es aplicada por lo que no se va a generar ningún nuevo conocimiento o modificación teórica en este presente caso de estudio.

### B. Diseño de Investigación

No experimental de carácter descriptivo porque se va a detallar la propuesta de cómo debe organizarse física y lógicamente la seguridad en la DRELP.

## Población y Muestras

La población estuvo conformada por la totalidad de personas que laboran en la institución que se adecue con el 100% del total de la población.

La población se orientó con el total de trabajadores por tratarse de un número menor (67 personas).

Por tanto, la muestra estuvo representada por la totalidad de trabajadores.

## Aplicación de la Metodología

Del análisis anterior y como aplicación de las normas de seguridad utilizadas por la institución, podemos establecer que:

Respecto de la **Política de Seguridad,** la Dirección regional de educación de lima provincias no tienen en cuenta o no cumple con la **Política de Seguridad** ya que evaluamos los siguientes activos: Hardware, Software, Datos, Personas, Documentación:

Por lo tanto, la DRELP deberá: Establecer una política clara y en línea con los objetivos del negocio y demostrar su apoyo y compromiso con la seguridad de la información mediante la publicación y mantenimiento de una política de seguridad de la información para toda la Institución, todos los recursos de informática (equipos, programas y datos) deberán ser asignados a una persona responsable. La responsabilidad de informática es compartida con la persona responsable del recurso y la planeación, implementación, monitoreo y control de la seguridad, podrá ser delegada tomando en cuenta al responsable. Las políticas de seguridad son controles y procedimientos obligatorios para todos los sistemas de la organización, para asegurar la buena práctica de seguridad. Los controles de seguridad que van más allá de los procedimientos y estándares establecidos, deberán ser justificados por el usuario, de acuerdo a sus necesidades de seguridad y su responsabilidad.

Asimismo, en los **Aspectos Organizativos,** la Institución no cuenta con un comité que se encargue de la seguridad de la información la cual vea las deficiencias que hay en la institución en la parte de la seguridad informática.
El cual el encargado del área de informática deberá cumplir con todo lo establecido por el comité, pero en la institución carecen de las dos cosas fundamentales.

Por lo tanto, la DRELP deberá de contar:

- Existe un comité de seguridad de la información responsable de revisar y aprobar las políticas de seguridad de la información.
- El Comité de Seguridad de la Información debe ser responsable de definir políticas, estándares y procedimientos relacionados con la seguridad de la información, y asegurar su implementación y cumplimiento.
- El coordinador de TI será responsable de asegurar el cumplimiento del plan organizacional requerido para la gestión de la seguridad de la información y asegurar la implementación de las medidas de gestión de la seguridad de la información. También es responsable de formular las tareas necesarias para mantener estas medidas.
- A través de la implementación de programas de comunicación, difusión, capacitación y educación, todos los usuarios del SGSI deben ser conscientes de la cultura de seguridad de la información.

Respecto de la **Seguridad Física y del entorno en las Áreas Seguras,** Actualmente el personal que labora en la institución no sabe cuáles son las áreas seguras o restringidas las cuales solo debe de entrar el personal capacitado el motivo es que no hay señalizaciones, también está permitido la entrada a terceros.

Por lo tanto, la DRELP deberá contar:

- ✓ Se aplicará la Metodología ISO 27001 en la DRELP para dar seguridad física y lógica.
- ✓ Se debe designar y mantener protección físicas y pautas para trabajar en áreas seguras.
- ✓ Los trabajadores solo conocen la existencia de áreas seguras o sus actividades cuando es necesario para el trabajo.

- ✓ Por razones de salud y oportunidades para evitar actividades maliciosas, evite el trabajo sin supervisión en áreas seguras.
- ✓ El área segura debe cerrarse y revisarse regularmente cuando esté vacía.
- ✓ A menos que esté especialmente autorizado, no se permiten fotografías, videos, audio u otras formas de equipo de búsqueda.

Los arreglos para trabajar en un área segura deben incluir el control de los empleados, contratistas y usuarios de terceros que trabajan en el área, así como otras actividades de terceros que ocurren allí.*Fig. N° 1 Diseño de la DRELP*

*Fuente: DRELP*

Sala de Servidores: Área de informática


*Fig. N° 2Diseño del Cableado de la DRELP*

Respecto a la **Seguridad en los Equipos c**omo pudimos apreciar la DRELP no cuentan con un orden o un plan donde se tenga en cuenta el mantenimiento de los equipos y a que área se hará el mantenimiento respectivo, tampoco cuentan con un taller de reparación

Las condiciones ambientales no son las mejores ya que por tener una infraestructura inadecuada pone en riesgo al mantenimiento de los quipos.

***Propuesta para la Implementación física del Área de Informática***

El presente diseño del área de informática y de sistema, está basado en los estándares y nc Fuente: *DRELP* su implementación y adecuación del ambiente es el siguiente:

- El equipo debería situarse y protegerse para reducir el riesgo de materialización de las amenazas del entorno, así como las oportunidades de acceso no autorizado.
- Se colocarán un cinto autoadhesivo que selle la tapa del case.
- El Comité Ejecutivo de Informática determinará las áreas que deban contar con servicio de aire acondicionado.
- Realizar el mantenimiento de los equipos de aire acondicionado mínimo una vez al año. En las salas deservidores y equipos de comunicaciones, según lo planificado.
- Los equipos de aire acondicionado de las salas deservidores y equipos de comunicaciones deben cumplir con las normas de calidad
- Disponer de soporte técnico para el mantenimiento de los equipos d computo

- La data center debe cumplir con el espacio establecido por normativa. Con las instalaciones de red eléctrica y de data.

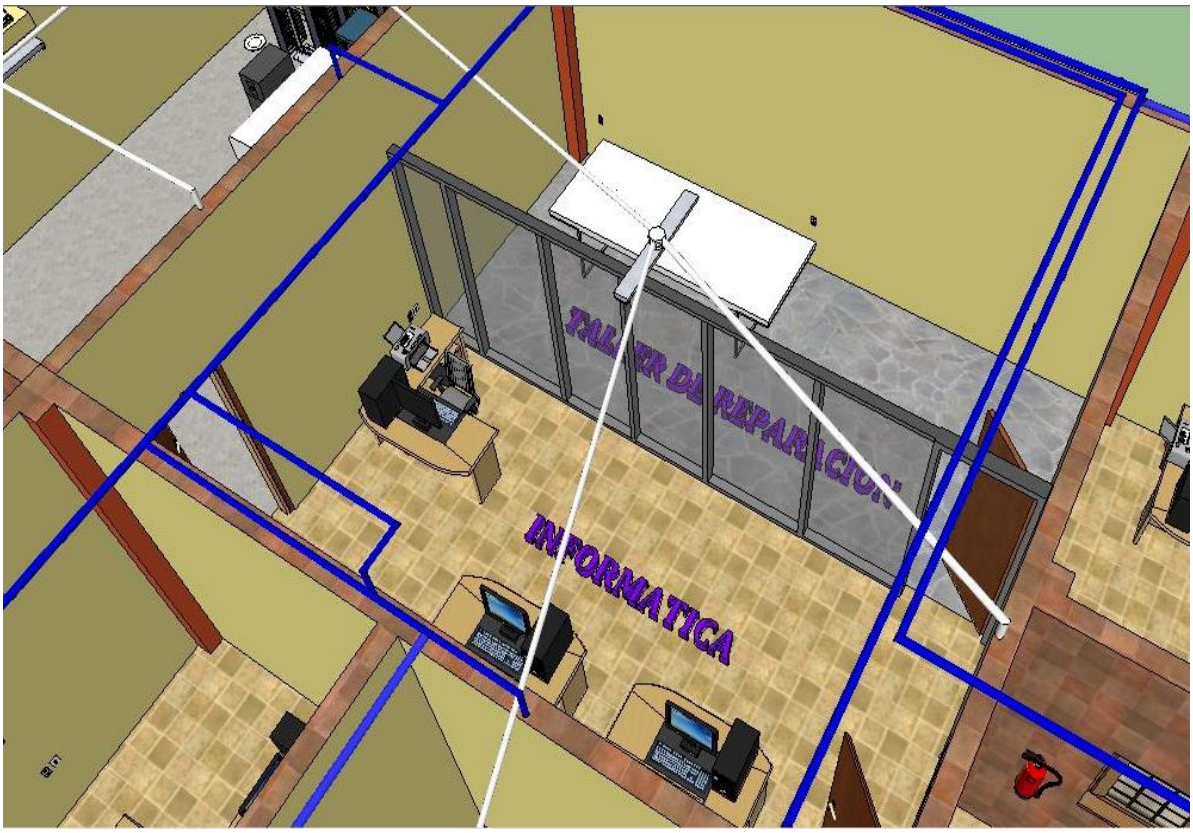



*Fig. N° 3 Área de informática*

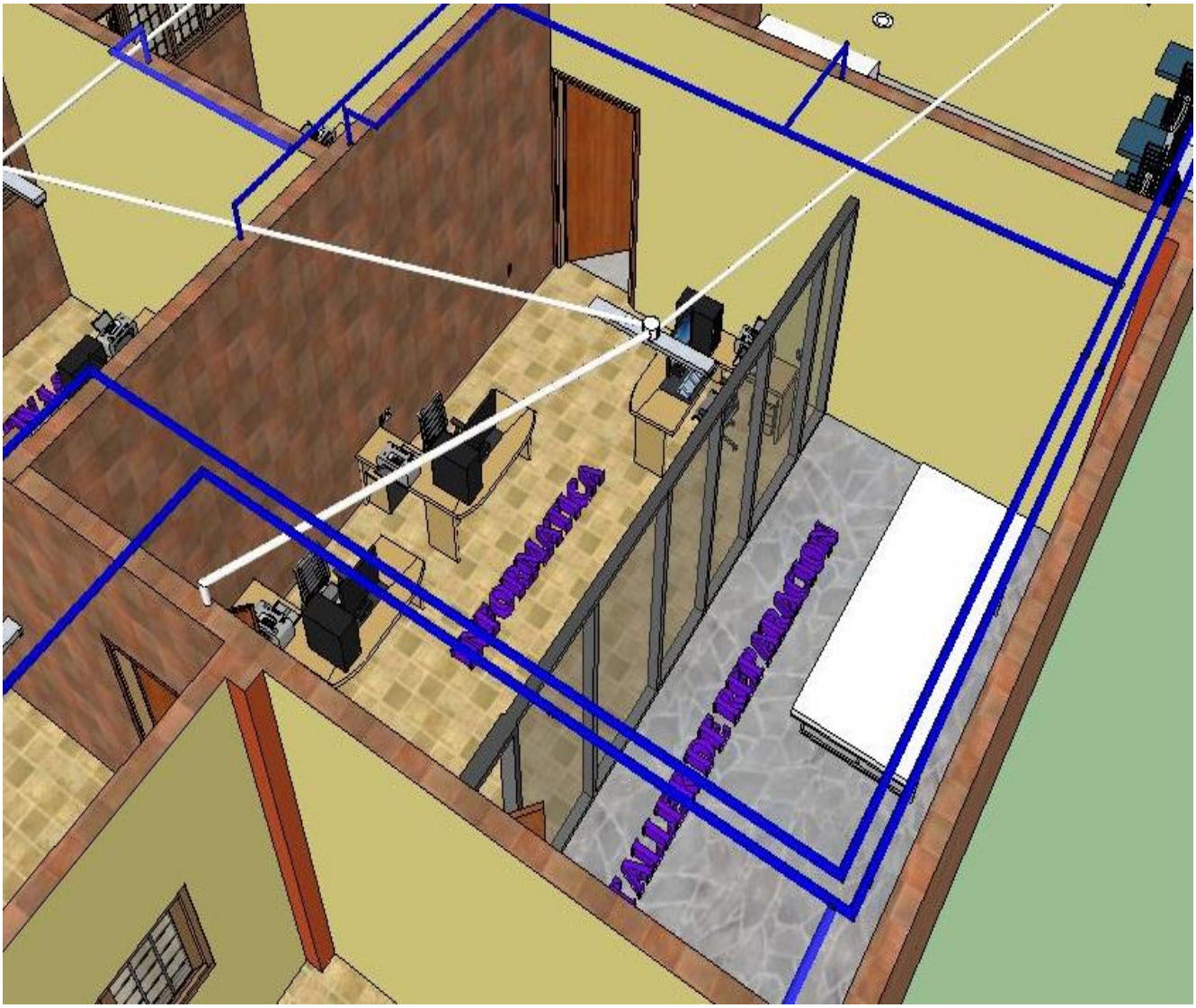



*Fig. N° 4 Área de informática*

Según los estándares establecidos anteriormente un cuarto de equipo debe de contar con lo siguiente:

- ✓ Extintores
- ✓ Aire acondicionado
- ✓ Swicth
- ✓ Cámaras de seguridad

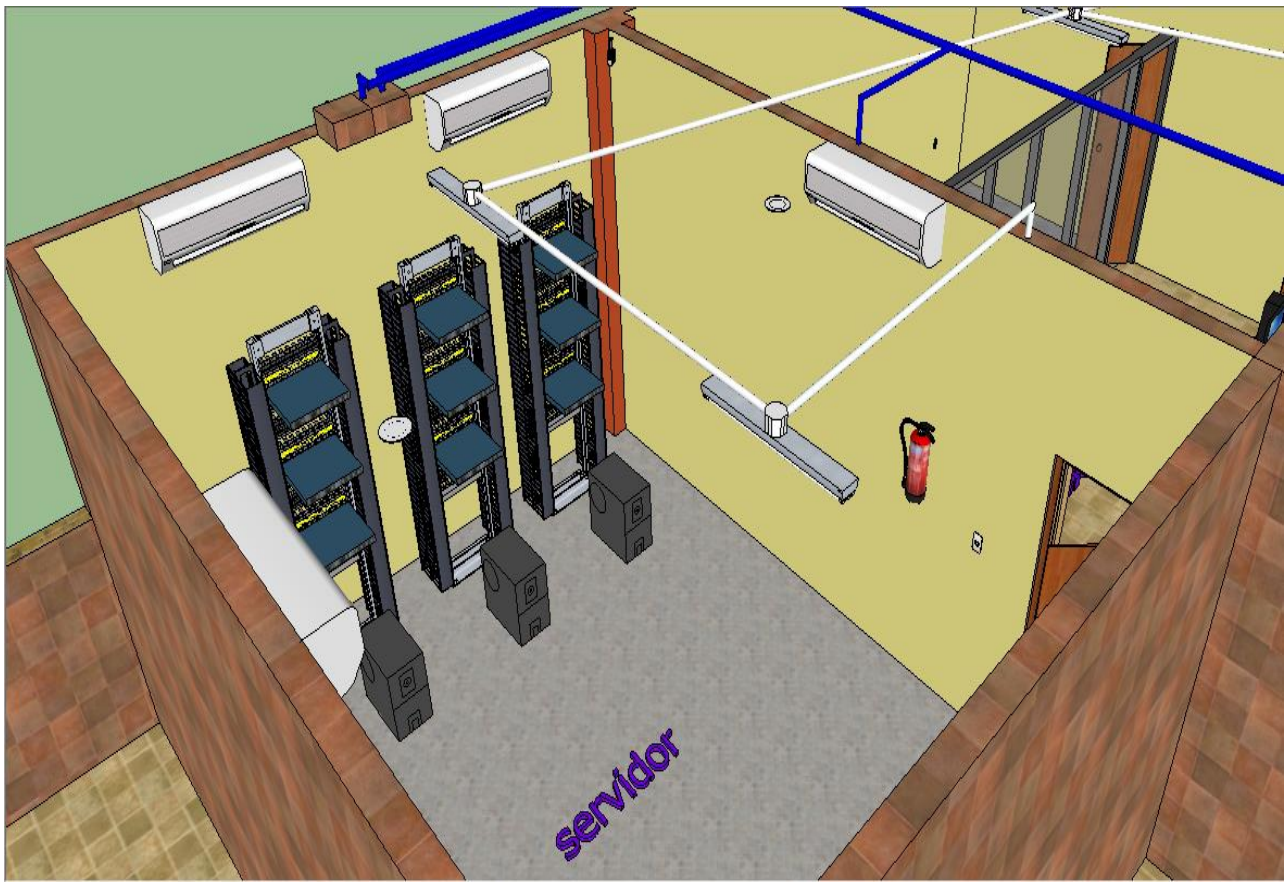



*Fig. N° 5 Cuarto de Equipo*

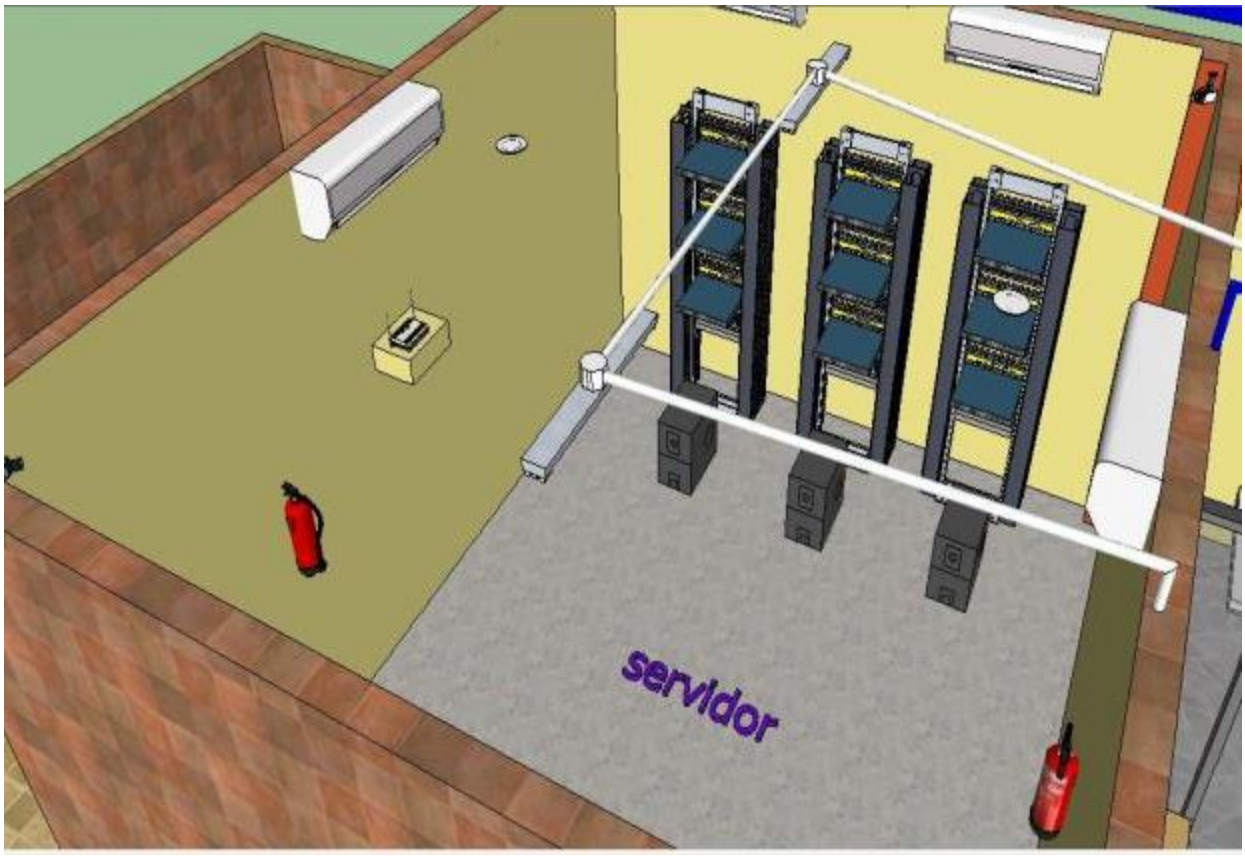



*Fig. N° 6 Cuarto de Equipo*

Asimismo, la **Seguridad Informática.** En la DRELP el personal que labora en dicha institución no cuenta con usuarios respectivos ya que la falta de eso hace que la información este desprotegida y un tercero pueda acceder a dicha información, tampoco cuenta con correos institucionales.

Asimismo, la **Seguridad Física** Como podemos observar la red no cuenta con ningún tipo de protección ante amenazas externas e internas, además se encuentra dentro de un mismo grupo de red, lo cual permitiría a personas no autorizas a manipular la información:



*Fuente: Diseño Propio*

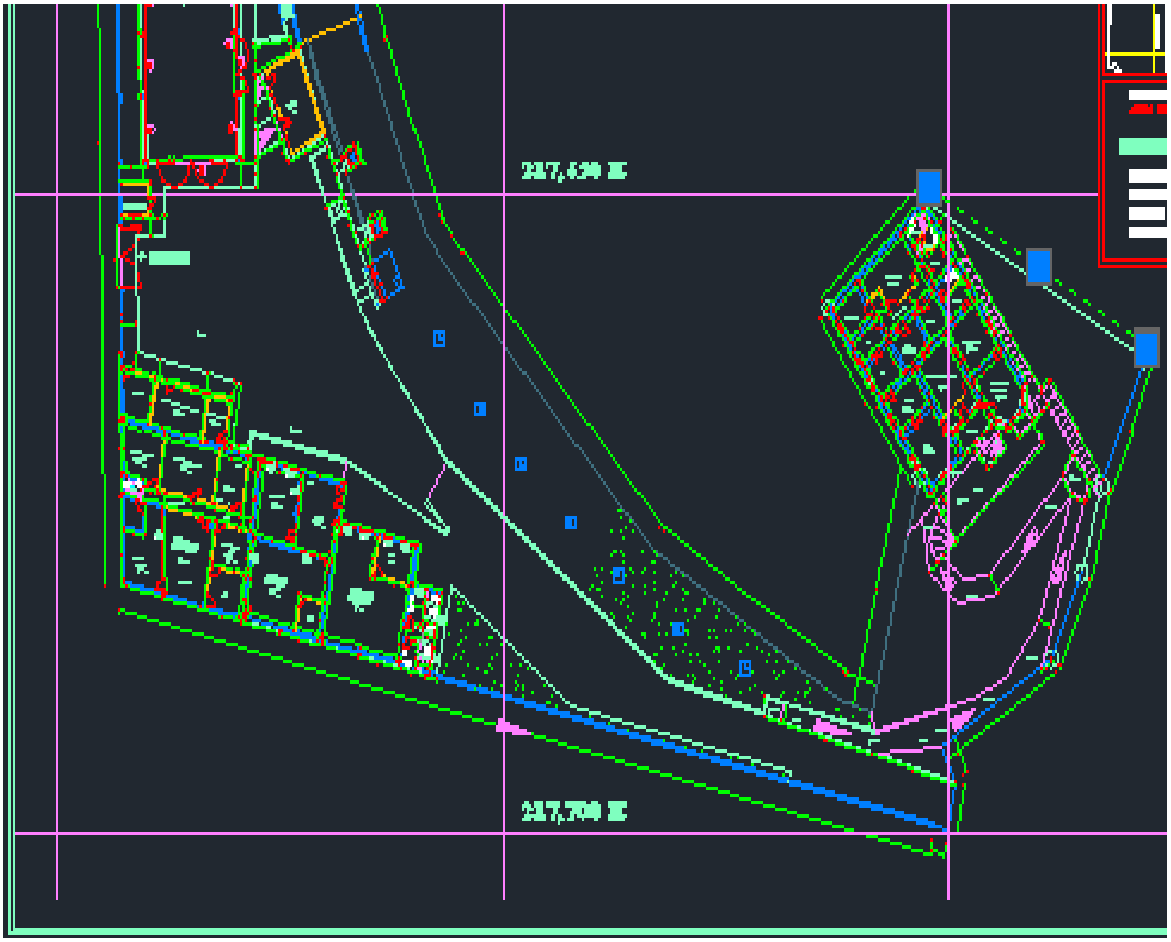


*Fig. N° 7 Diseño de la Red Actual*

**Diseño de red con la propuesta del rediseño de la DRELP**

El diseño lógico del cableado estructurado siguiendo las recomendaciones de los estándares y normas antes mocionadas para su implementación y adecuación, es el siguiente:

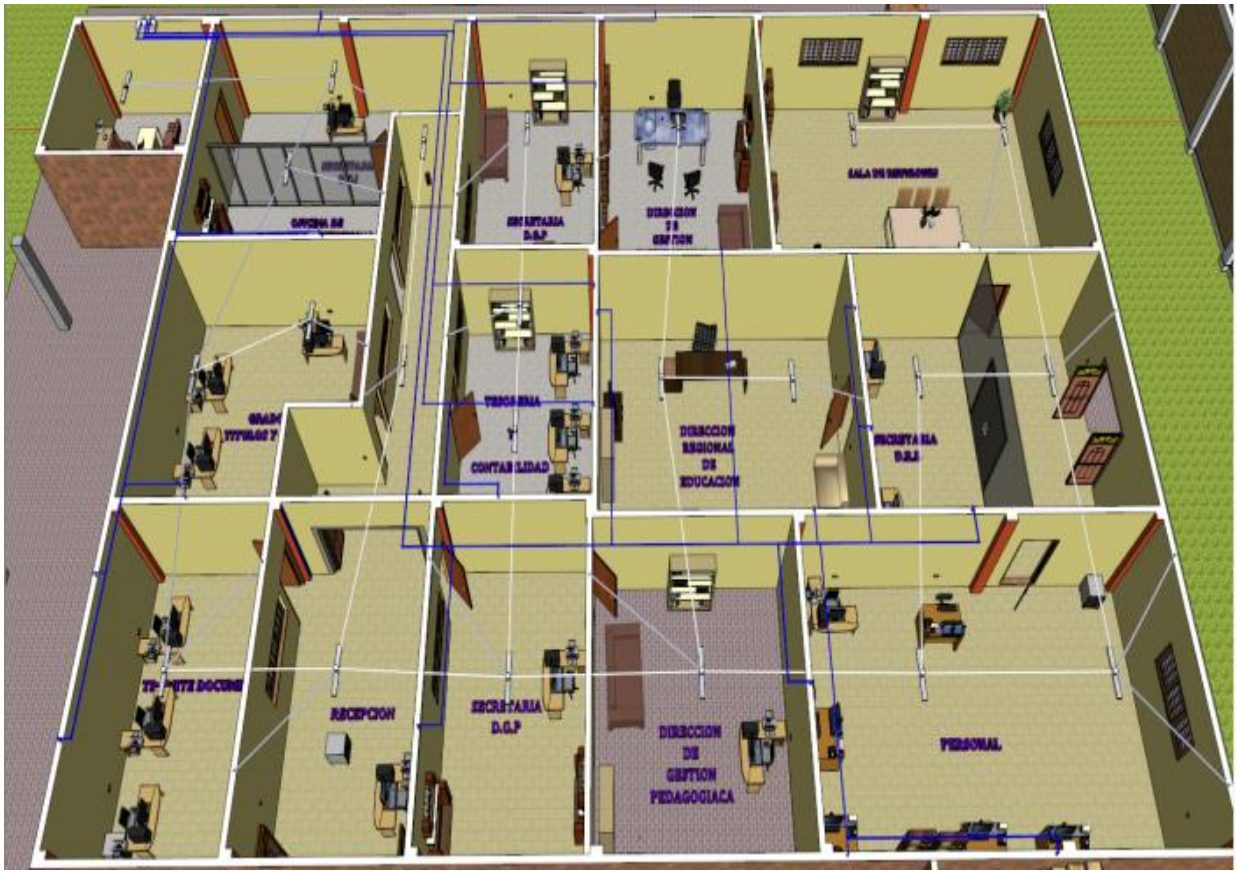



*Fig. N° 8 Red propuesta del 1° piso*

*Fig. N° 9 Lado Frontal de la Red propuesta del 1 piso*


*Fig. N° 10 Red propuesta del 2° piso*

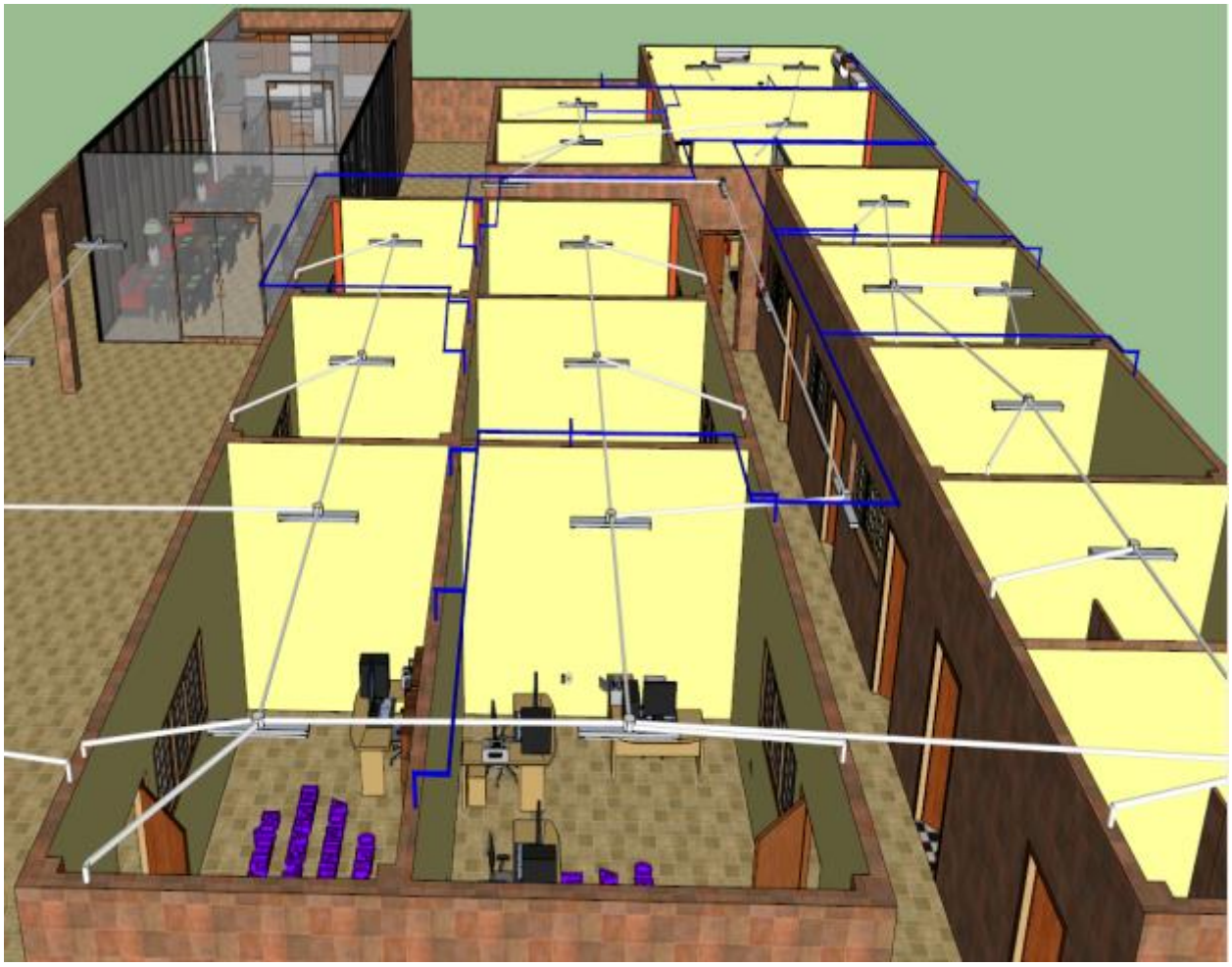


*Fig. N° 11 Lado Frontal de la Red propuesta del Segundo piso*

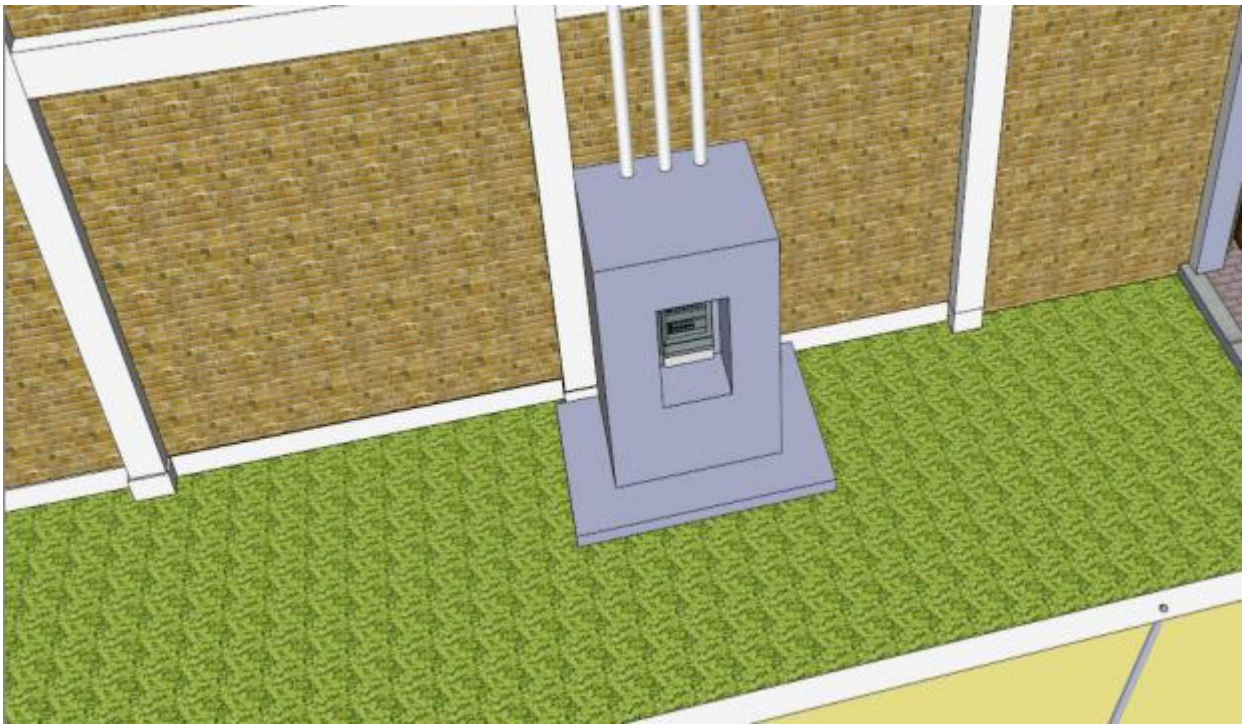


*Fig. N° 12 Tablero*

- ✓ Según los Estándares debe de contar con:
    - Antes de la instalación de los equipos de cómputo, es indispensable que el área competente realice cálculos de la carga eléctrica requerida en la instalación, en los tableros de distribución eléctrica, así como de los circuitos y conexiones que deben soportar la carga adicional proyectada.
    - Para los equipos de cómputo se deberá contar con circuitos alternos y tableros de distribución eléctrica independientes a cualquier otra conexión.
    - Instalar pozos con puesta a tierra, conectados al sistema eléctrico que alimenta los equipos de cómputo. Asimismo etiquetar el cableado, las extensiones y los tableros de

*Fuente: Diseño Propio*

distribución eléctrica de acuerdo a los estándares internacionales vigentes.

- Efectuar el mantenimiento de los pozos con puesta a tierra mínimo una vez al año, para garantizar que la resistencia eléctrica no exceda los 5 ohmios.
- Asegurar el suministro de energía eléctrica de voltaje estable, con la ayuda de sistemas de estabilización de voltaje, supresores de picos, y unidades de potencia contra cortes fluidos (UPS).
- El cableado está debidamente protegido por canaletas
- El Cableado de fibra óptica.

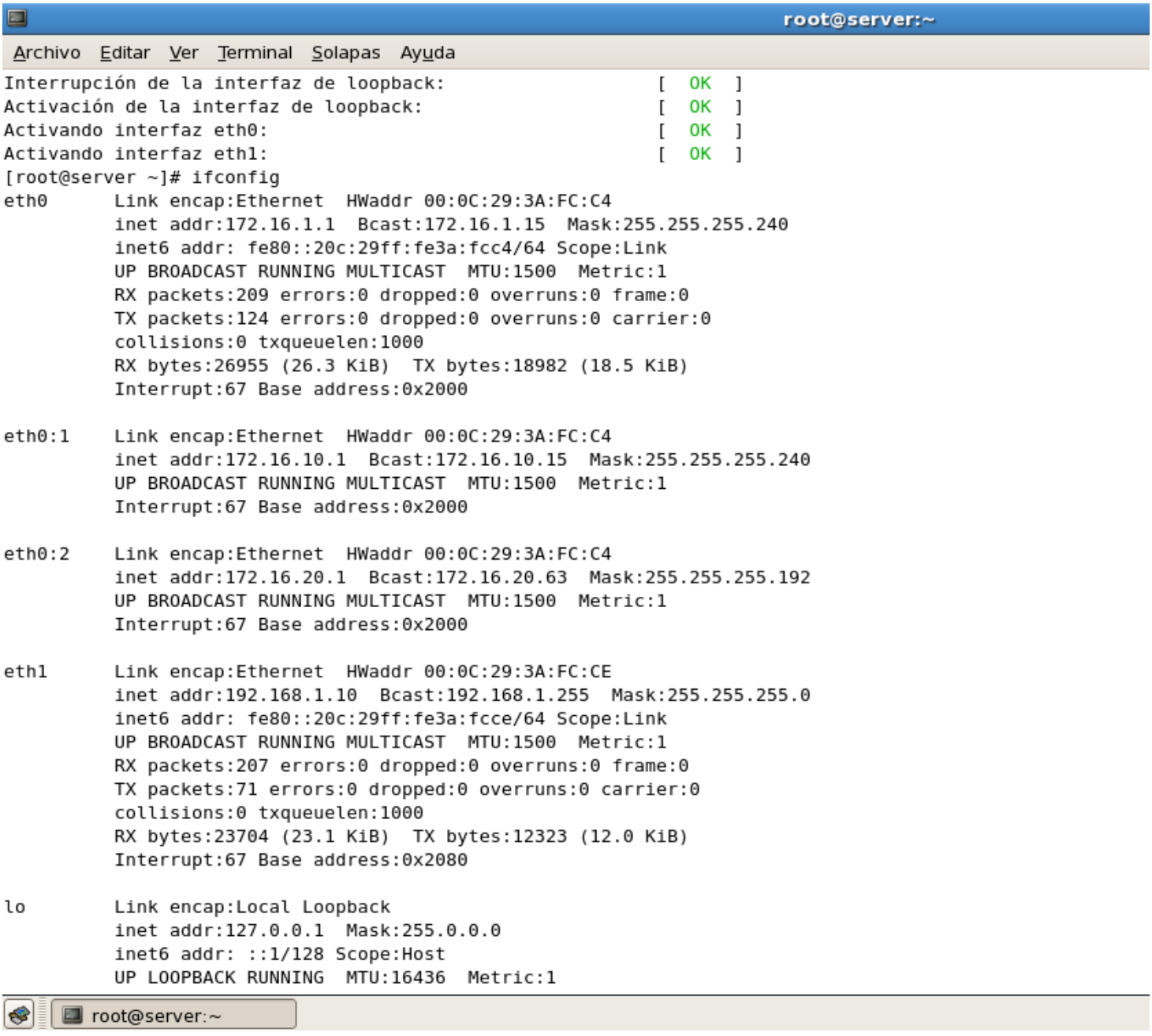



*Fig. N° 13 Control del uso de Equipos*

ETH0: La red que tiene 15 IP la cual estas las áreas de:

- Economía: Contabilidad y Tesorería

ETH01: Es una IP virtual consta de 13 IP donde se encuentran las áreas de:

- Dirección

ETH02: Se encuentras 16 IP las cuales utilizaran:

- Las demás Áreas

ETH1: Se encuentra la red con internet publica

## CONFIGURACION DEL PROXY

root@server:/media/CMA_BLUE/Resp

Archivo Editar Ver Terminal Solapas Ayuda

```
#########################
#CONFIGURACION DEL PROXY DRELP
#########################

#######SUBREDES EN LA DRELP ###############
acl red_direccion src 172.16.1.0/28
acl red_economia  src 172.16.10.0/28
acl red_otras_areas src 172.16.20.0/26
###############################################
 Permitir windowsupdate con IE
acl windowsupdate dstdomain .windowsupdate.com
acl windowsupdate dstdomain .microsoft.com
acl windowsupdate dstdomain .public-trust.com
acl windowsupdate dstdomain .windows.com
acl windowsupdate dstdomain .webiqonline.com
acl windowsupdate dstdomain 207.46.224.158
acl windowsupdate dstdomain .msn.com
always_direct allow windowsupdate

acl palabrasNo url_regex "/etc/squid/acl/palabrasNo.acl"
# Para denegar acceso a ficheros con estas extensiones: .mp3$, .avi$
acl ficherosNo urlpath_regex -i "/etc/squid/acl/ficherosNo.acl"
# Para denegar acceso a dominios completos: sponsoradulto.com
acl sitiosNo dstdomain "/etc/squid/acl/sitiosNo.acl"
# Sitios institucionales para maxima restriccion
acl sitiosSi dstdomain "/etc/squid/acl/sitiosSi.acl"
#Lista Negra
acl listanegra dstdomain "/etc/squid/acl/listanegra.acl"
# Prohibe messenger
acl msn_messenger req_mime_type -i ^application/x-msn-messenger$
# Bloqueamos gateway.dll para versiones viejas de MSN Messenger
acl msn_url url_regex -i gateway.dll
# Bloqueamos el puerto utilizado por todas las versiones
acl msn_port port 1863
# Bloqueamos el metodo POST utilizado por las nuevas versiones de MSN Messenger
acl msn_method method POST
#############################################################################
-- INSERTAR --
```

[root@server:~] [Pantallazo.png] root@server:~ CMA_BLUE R

*Fig. N° 14 Configuración del Proxy*

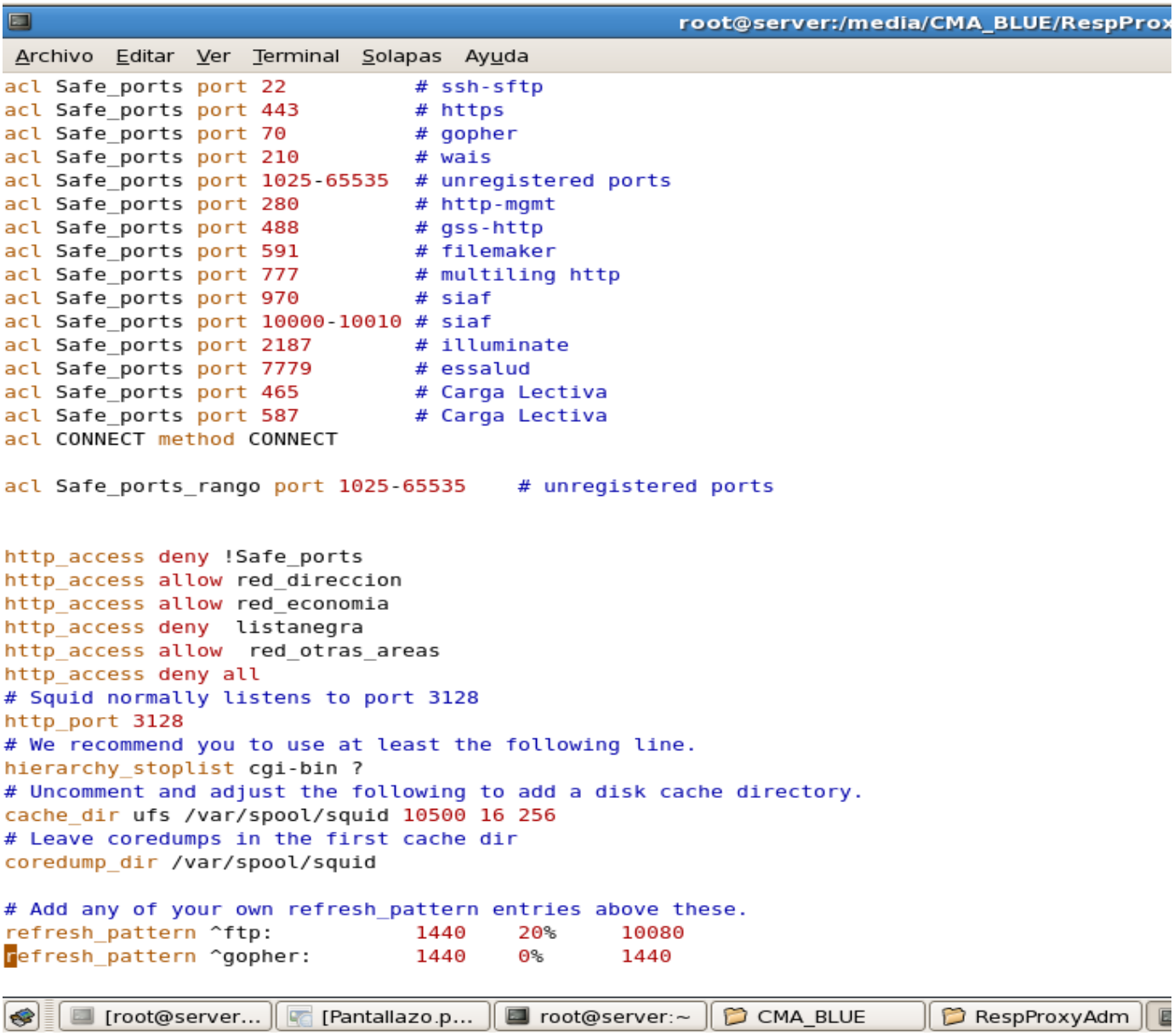



*Fig. N° 15 Configuración del Proxy*

- Que se cumpla el esquema organizacional requerido para la administración de seguridad de la información y poder velar por la implantación de las medidas de administración de seguridad de la información. Igualmente es responsable de desarrollar las tareas necesarias para el mantenimiento de estas medidas.

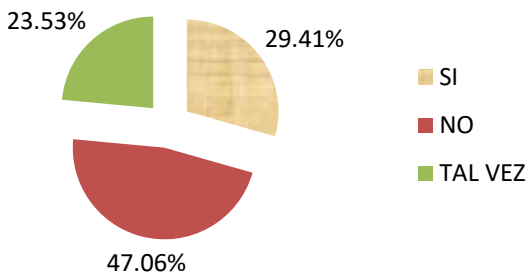
- Se deberá dar a conocer la cultura de seguridad de la información a todos los usuarios del SGSI.
- Se recomienda utilizar como solución antimalware al antivirus BITDEFENDER, ya que este está basado en el ISO 27001 y cuenta con políticas de administración muy interesantes como Informe de Auditoría de Redes e inventario de software y hardware, que en un futuro de ser implementado un Active Directory puede ser de mucha utilidad.

# RESULTADOS

Como punto de partida, ya conociendo nuestros resultados presentamos a continuación un detalle de la encuesta aplicada a los trabajadores, la cual nos sirvió para determinar los requerimientos de seguridad para la red.

**Institución de trabajadores de la DRELP, según opinión Acerca de la RIEGOS del Sistema de Seguridad.**

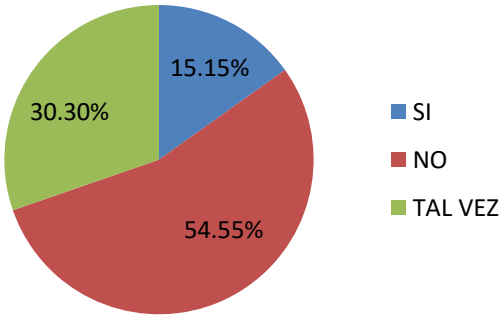
**1. ¿Se ha tenido en cuenta la seguridad de la informacion en la DRELP al realizar el diseño de la red?**




RESULTADO

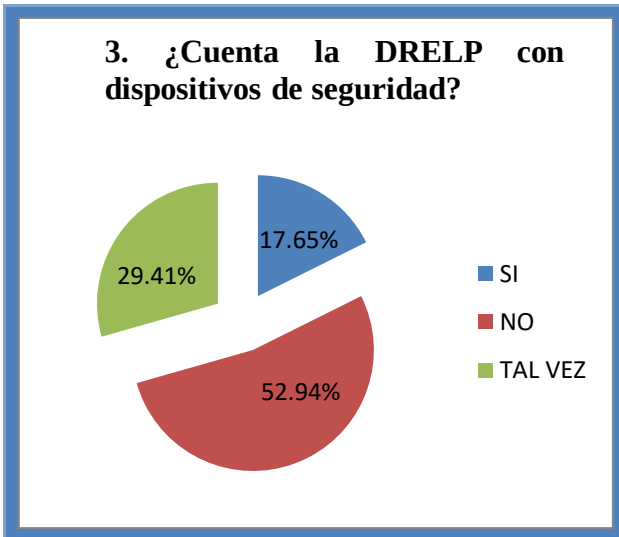
El 47,06% de los trabajadores opinan que No se ha tenido en cuenta la seguridad, mientras el 29,41% dice que sí y el 23,53% dice que tal vez se tuvo en cuenta la seguridad.

**2. ¿Es buena la seguridad fisica en la DRELP?**




RESULTADO

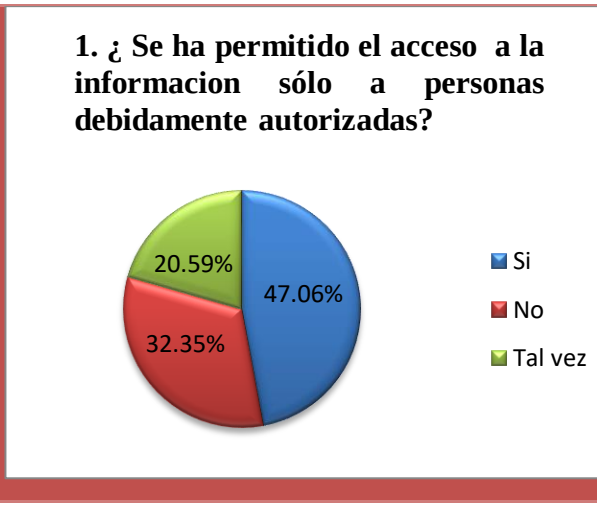
El 54,55% de los trabajadores opina que la seguridad física No es buena, Mientras el 15,15% dice que Si es buena y el 30,30% dice que tal vez.




RESULTADO

Como nos indica el gráfico el 52,94% de los usuarios señalan que la DRELP No cuenta con dispositivos de seguridad suficientes, mientras que el 17,65% dice que si cuenta y el 29,41% dice que tal vez.

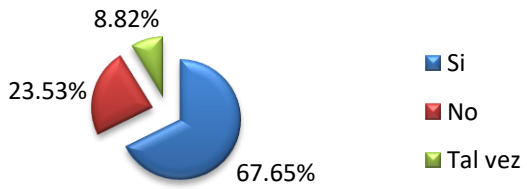
**Institución De Trabajadores De La DRELP Según Opinión Acerca De La CONFIDENCIALIDAD Del Sistema De Seguridad**




RESULTADOS

Este gráfico nos muestra que el 47,06% dice que solo se ha permitido a personas autorizadas, mientras el 32,35% dice que No y el 20,59% dice que tal vez.

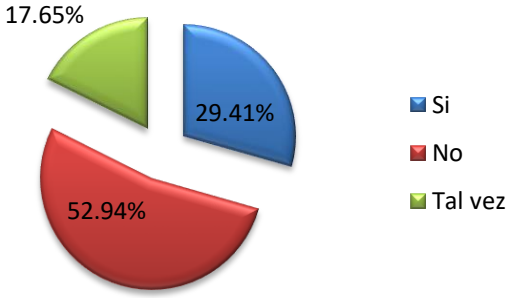
**2. ¿Se ha establecido un control para que los usuarios no modifiquen datos del sistema de información de un modo autorizado?**




RESULTADOS

El 67,65% de los trabajadores dice que Si, el 23,53% dice que No y el 8,82% duda de este control.

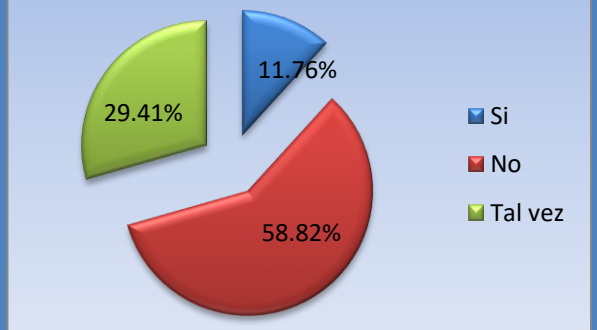
**3. ¿Los usuarios del sistema han podido acceder siempre en todo momento a los datos permitidos para ellos?**




RESULTADOS

El 53% dice que No han tenido problemas al acceder a sus datos, mientras el 29% dice que Si lo tuvo y el 18% dice Tal vez.

**Institución De Trabajadores De La DRELP Según Opinión Acerca Del CUMPLIMIENTO Del Sistema De Seguridad**



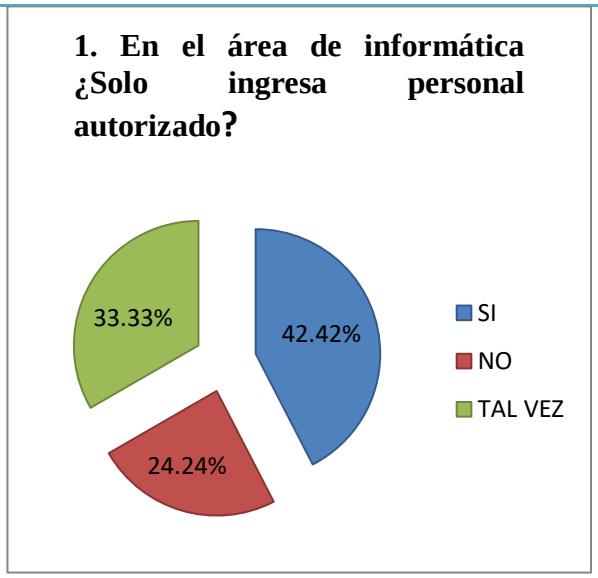

RESULTADOS

El 58,82% de los trabajadores nos dijo que no cuentan con el plan de contingencia, mientras el 11,76% dice que SI y el 29,41% no está seguro.


RESULTADOS

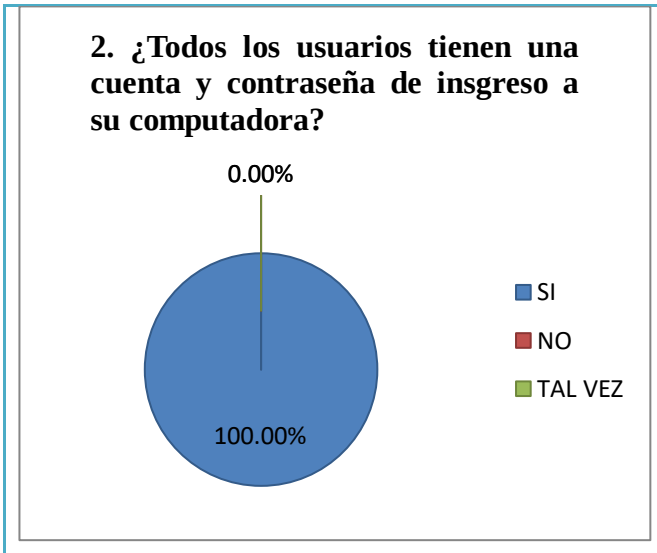
El 38,24% de los trabajadores dice que No, mientras el 20,59% asegura que si lo tienen y el 41,18% duda de esta política.

**Institución De Trabajadores De La DRELP Según Opinión Acerca Del CONTROL Del Sistema De Seguridad**



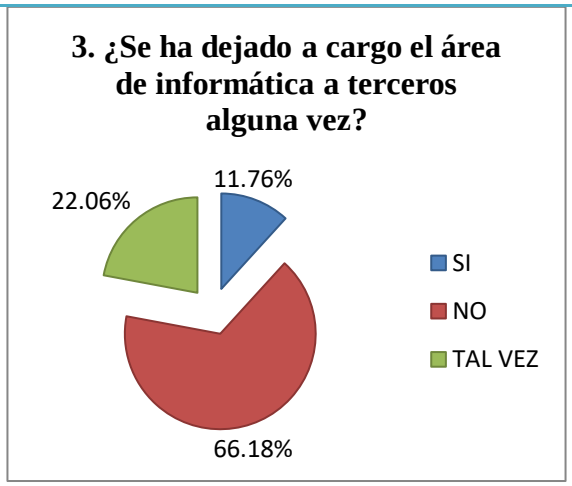

RESULTADOS

El 42,42% dice que esta regla Si se cumple, mientras el 24,24%dice que no, y el 33,33% de los trabajadores duda de esta regla.




RESULTADOS

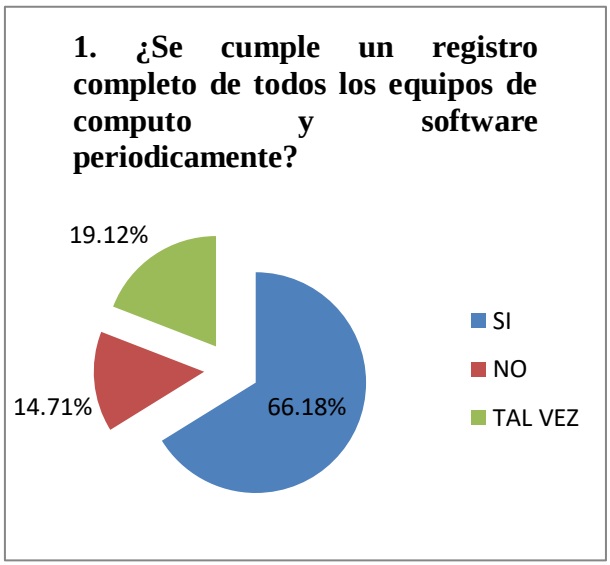
El 100% de los trabajadores confirman que si cuentan con usuarios y contraseñas.




RESULTADOS

El 66,18% de los trabajadores dice que No se dejó a cargo a terceros, mientras, el 11.76%dice que Si y el 22,06% de los trabajadores duda de esta pregunta.

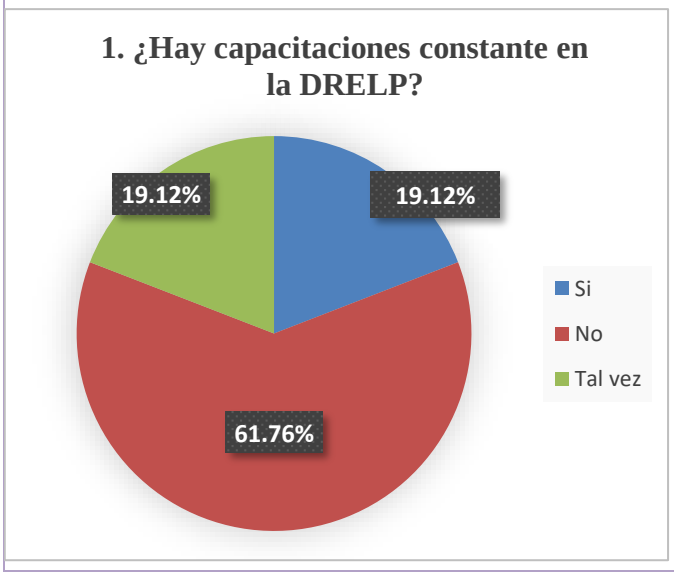
**Institución De Trabajadores De La DRELP Según Opinión Acerca De La AUDITABILIDAD Sistema De Seguridad**




RESULTADOS

El 66,18% de los trabajadores dice que Si se cumple, mientras el 14,71% dice que no y el 19,12% duda de este registro.

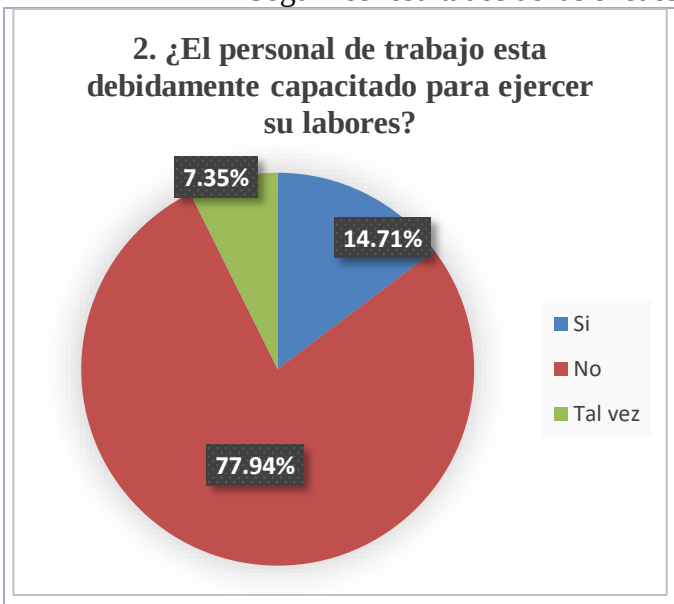
**Institución De Trabajadores De La DRELP Según Opinión Acerca De La CAPACITACION Sistema De Seguridad**




RESULTADOS

El 19,12 % dice que si hay capacitaciones constantes en la DRELP, el 61,76% dice que no, y el 19,12% dice que tal vez hay capacitaciones. Dando como conclusión que las capacitaciones no son constantes en la institución.

- Según los resultados de las encuestas realizadas a los trabajadores nos podemos




RESULTADOS

El 14,71 % dice que el personal de trabajo está debidamente capacitado, el 7,35% dice que no, y el 14,71% dice que tal. Dando como conclusión que los trabajadores de la DRELP no están debidamente capacitados.

dar cuenta que la seguridad física, no es buena en la DRELP, ya que no cuentan con todos los dispositivos y equipos adecuados para una buena protección de

datos y no tuvieron en cuenta la seguridad de información al momento de diseñar la red en la institución.

- De acuerdo a los resultados ya vistos en la encuesta, interpretamos que en la institución si existe un control de acceso y restricción de la información a personas no autorizadas, ya que estos datos pueden ser modificados, borrados, etc., causando una posible fuga o destrucción de la misma. Pero vemos también que no siempre es posible el acceso a todos los datos permitidos.
- Podemos asegurar también mediante los gráficos ya vistos que la DRELP no cuenta con un "plan de contingencia" en caso de desastres naturales y los usuarios no tienen conocimiento si existe una política de restauración de información en caso de ataques informáticos.
- Según los resultados vistos en las encuestas realizadas nos pudimos dar cuenta que en la DRELP existe un control de acceso al área de informática para las personas no autorizadas, pero que no se cumple mucho con esta norma. Todos los usuarios tienen una cuenta y contraseña de acceso a su computador y por otro lado el ingeniero responsable del área de informática pocas veces deja a cargo el área a un tercero.
- Tal como lo muestra el gráfico, podemos decir que la DRELP realiza periódicamente un registro de sus equipos de cómputo y software para llevar un mejor control. (008-95-INEI/SJI I. D., 1995)

# ANÁLISIS Y DISCUSIÓN

De acuerdo a la problemática ya estudiada y analizada, y nuestra propuesta basada en la utilización de estándares como es la norma ISO 27001, se desprende que en la dimensión Riesgos, a pesar de que se tiene establecida como norma en la DRELP, al no aplicarse se tiene que sugerir la implementación de las pautas y disposiciones para su ejecución. Asimismo, respecto a la dimensión confiabilidad hemos observado que en la DRELP la información no ha estado bien resguardada, y esto ocasionaba fugas de información, por lo que sugerimos realizar un control de accesos a la información como se establece según las normas. Respecto a la dimensión de Cumplimiento, hemos detectado que la DRELP no cumple cabalmente con las normas establecidas, por lo que sugerimos haya un mayor control para el cumplimiento de estas normas.

De acuerdo a la dimensión de Control, la DRELP no cumple con las normas respecto a la seguridad física y lógica por lo que existen Riesgos en la seguridad de la institución. Asimismo, respecto a la dimensión de auditabilidad no se está cumpliendo debidamente con lo establecido, ya que no se realizan un registro de los equipos y software periódicamente, por lo que sugerimos un mayor control en la institución.

Finalmente para la dimensión de Capacitación, no se está aplicando constantemente, de modo que no hay un cumplimiento con la norma establecida, por lo que sugerimos que se realicen las debidas capacitaciones cuando fueran necesarias.

# CONCLUSIONES

1. Después de haber analizado podemos concluir que las normas y estándares no se han venido cumpliendo en la institución en el aspecto físico y lógico.

2. Para poder hacer un buen diseño de un sistema de seguridad en una red es necesario realizar previamente un análisis físico y lógico en la institución para conocer al detalle en que aspectos están fallando o se pueden mejorar.

3. El aplicar la Metodología ISO 27001 ayudará a gestionar y proteger la valiosa información.

4. La información tiene una importancia fundamental para el funcionamiento y es incluso decisiva para la supervivencia de la organización trabajando conjuntamente con los equipos como dispositivos de seguridad que ayudarán a tener una información segura.

# RECOMENDACIONES

1.1. Para que la institución y toda empresa tenga una seguridad de información de calidad en los aspectos físicos y lógicos, es necesario que cumplan con las normas y estándares establecidos ya mencionados anteriormente.

1.2. Antes de realizar un diseño de un sistema de seguridad para una red es necesario primero hacer un análisis físico y lógico que nos permita conocer las debilidades que se tiene en la red actual, ya que nos servirá como prototipo para mejorar nuestra propuesta.

1.3. Recomendamos utilizar la metodología ISO 27001 ya que aquí nos indican que normas y estándares aplicar para tener una buena seguridad de información en los aspectos físicos y lógicos.

1.4. La información consideramos que es el bien más preciado de toda institución o empresa, y debe contar con una buena seguridad, y para eso es necesario tener los equipos informáticos adecuados y un diseño de red estructurado cumpliendo las normas y estándares establecidos.

# REFERENCIA BIBLIOGRAFIA


(2009), G. (s.f.). *http://mmujica.files.wordprees.com/2007/07/iso-17799-2005-castellano.pdf*.

008-95-INEI/SJI, I. D. (1995). *Recomendaciones técnicas para la protección física de los equipos y medios de procesamiento de la información en la administración pública.* Obtenido de http://www.ongei.gob.pe/publica/metodologias/lib5082/cap04.htm

008-95-INEI/SJI, I. D. (1995). *Recomendaciones Tecnicas para la proteccion fisica de los equipos ymedios de procesamiento de la informacion en la administracion publica.* Lima.

015-94-INEI/SJI, O. (. (s.f.). *¨Normas Técnicas Para El Almacenamiento Y Respaldo De La Información Que Se Procesa En Las Entidades Del Estado¨.* Obtenido de http://www.ongei.gob.pe/publica/metodologias/lib5082/cap01.htm

27001, I. (2005). Tecnología de la Información– Técnicas de seguridad – Sistemas de gestión de seguridad de la información – Requerimientos.

27001, I. (2005). Tecnología de la Información-Técnicas de Seguridad-Código para la práctica de la gestión de la seguridad de la Información.

500-04, I. (2000). *Mantenimiento de equipos de computación: la Dirección de cada entidad debe establecer políticas respecto al manteniemiento de los equipos de computación que permitan optimizar su rendimiento.* Obtenido de http:/www.unmsn.edu.pe/ogp/ARCHIVOS/NORMAS_TECNICAS_DE_CONTROL_INTERNO.htm#normas 50004

Gnu/Linux. (2009).

ONGEI. (1994). "Normas Para La Prevención, Detección Y Eliminación De Virus Informático En Los Equipos De Cómputo De La Administración Pública", aprobado por Resolución Jefatural Nº 362-94-INEI.

ONGEI. (1994). Directiva Nº 015-94-INEI/SJI ¨Normas Técnicas Para El Almacenamiento Y Respaldo De La Información Que Se Procesa En Las Entidades Del Estado¨.

ONGEI. (1995). Recomendaciones Técnicas Para La Seguridad E Integridad De La Información Que Se Procesa En La Administración Pública", aprobado por Resolución Jefatural Nº O76-95-INEI.

ONGEI. (2007). Norma Tecnica Peruana "NTP-ISO/ IEC 17799: 2007 EDI". En *Tecnologia de la informacion. Código de buenas prácticas para la gestión de la seguridad de la*

*información.* (pág. http://www.ongei.gob.pe/banco/ongei_normas_detalles.asp?pk_id_normas=90). 2a. Edición".

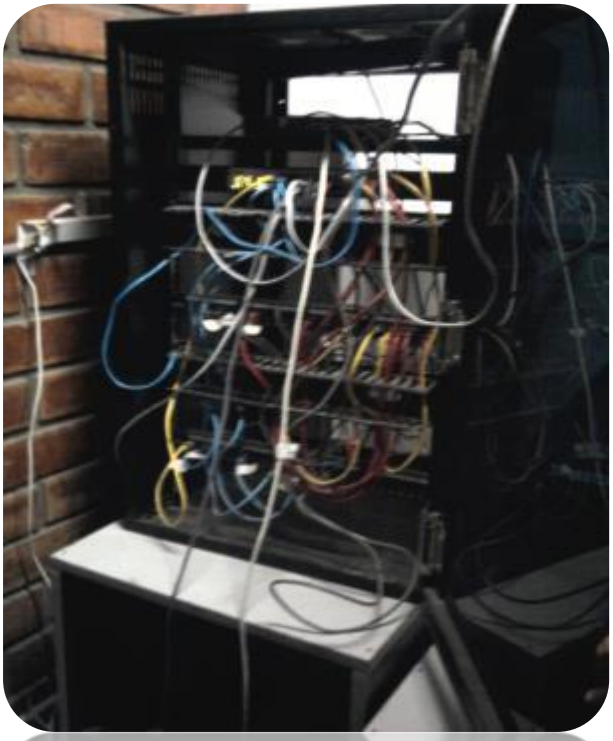
## ANEXO 01: ENCUESTA EN LA DIRECCION REGIONAL DE EDUCACION DE LIMA PROVINCIAS

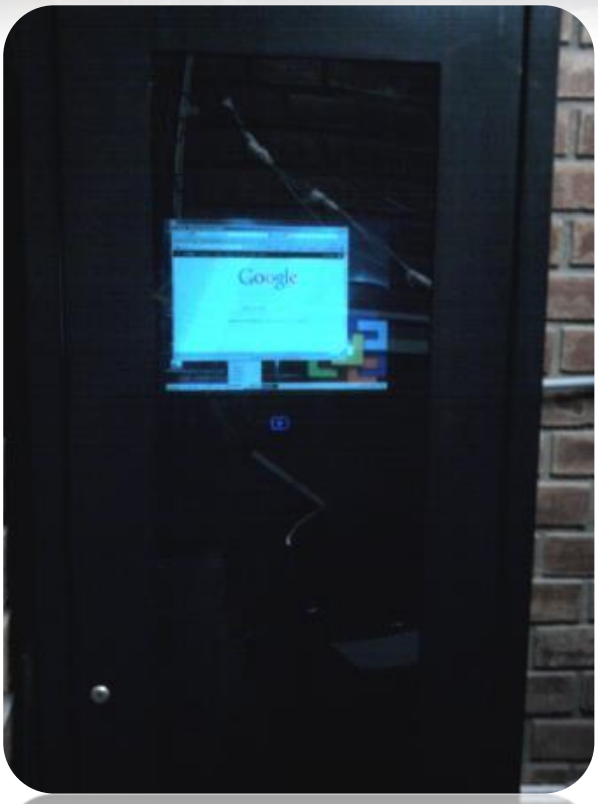
**Objetivo:** Esta encuesta es conocer su nivel de comunicación con la institución.

**Instrucciones:** Lea cuidadosamente los enunciados antes de responder a las proposiciones descritas en las páginas siguientes.

| PREGUNTAS | SI | NO | TAL VEZ |
|---|---|---|---|
| 1. ¿Se ha tenido en cuenta la seguridad de información de la DRELP al realizar el diseño de la red actual? | | | |
| 2. ¿Es buena la seguridad física en la DRELP? | | | |
| 3. ¿Cuenta la DRELP con dispositivos de seguridad (cámaras, detectores de humo, alarmas, etc.)? | | | |
| 4. ¿Se ha permitido el acceso a la información sólo a personas debidamente autorizadas? | | | |
| 5. ¿Se ha establecido un control para que los usuarios no modifiquen datos del sistema de información de un modo no autorizado? | | | |
| 6. ¿Los usuarios del sistema han podido acceder siempre en todo momento a todos los datos permitidos para ellos? | | | |
| 7. ¿Cuenta la DRELP con un plan de contingencias? | | | |
| 8. ¿Se tiene definida una política de restauración de los sistemas de información en caso de ataques informáticos? | | | |
| 9. En el área de informática ¿sólo ingresa el personal autorizado? | | | |
| 10. ¿Todos los usuarios tiene una cuenta y contraseña de ingreso a su computadora? | | | |
| 11. ¿Se ha dejado a cargo el área de informática a terceros alguna vez? | | | |
| 12. ¿Se cumple un registro completo de todos los equipos de cómputo y software periódicamente? | | | |
| 13. ¿Hay capacitaciones constantes en la DRELP? | | | |
| 14. ¿El personal de trabajo está debidamente capacitado para ejercer sus labores? | | | |


PELIGRO
RIESGO
ELECTRICO




Google