FACULTAD DE INGENIERÍA

Carrera de Ingeniería de Sistemas Computacionales

"DISEÑO E IMPLEMENTACIÓN DE UNA RED DE SEGURIDAD INFORMÁTICA PARA MEJORAR LA ADMINISTRACIÓN DE DATOS BASADO EN LA NORMA ISO/IEC 27002:2013, EN LA EMPRESA A.C.E SACO OLIVEROS - SEDE MONTERRICO. LIMA 2021"

Trabajo de suficiencia profesional para optar el título profesional de:

Ingeniero en Sistemas Computacionales

Autor:

Juan Jesús Lino López

Asesor:

Ing. Mg. Franchesca Fiorella Rodríguez Rivera

Lima - Perú

2022

DEDICATORIA

Dedico este trabajo a mi familia, lo más importante en este mundo, en especial a mi hijo, padres y esposa por su gran esfuerzo brindado a lo largo de los años.

AGRADECIMIENTO

Quisiera agradecer a mis maestros y asesores por brindarme el conocimiento profesional. El cual demuestro en el proyecto.

Tabla de contenidos

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN EJECUTIVO

El presente trabajo tendrá como fin la implementación de una red de datos para las aulas hibridas y áreas administrativas. El cual, brindará administración de seguridad informática a una sede modelo basado en los controles de la norma ISO/IEC 27002:2013, en la empresa Asociación Saco Oliveros, con el cual se construirá servicios de seguridad informática.

Actualmente la asociación tiene 40 sedes en lima y provincias, todas sus sedes no cuentan con la seguridad informática adecuada, tienen una red plana e insegura.

En el proyecto se requiere conocer la importancia de la seguridad Informática en las redes locales y externas, permitiendo tener un mayor control en el tráfico de los paquetes de datos por medio de la segmentación de las redes por VLAN.

Se obtuvieron resultados favorables, el servicio de internet estable para las aplicaciones de las áreas administrativas. Se garantizó estabilidad del servicio de red en las aulas hibridas para nuestros alumnos y docentes.

Se concluye el proyecto indicando la importancia de la seguridad de redes en el sector educación basado en la norma ISO/IEC 27002.

Las competencias profesionales aplicadas garantizaron llevar el proyecto con éxito. El presidente de la Institución aprobó replicar el proyecto en sus demás sedes educativas.

CAPÍTULO I. INTRODUCCIÓN

1.1. Realidad problemática

La falta de seguridad informática no es tan sólo una creación artificial, ya que no transcurre un mes sin que se haga pública alguna vulnerabilidad que afecte a la principal herramienta de acceso a Internet: el navegador Internet Explorer, utilizado por más del 90% de los ordenadores. Los reiterados esfuerzos del primer fabricante mundial de software por mejorar esta situación parecen haber sido hasta ahora completamente inútiles. Y se han centrado más en mejorar los mecanismos de distribución de parches y actualizaciones que en mejorar la calidad del software para disminuir el número de vulnerabilidades de seguridad.

El error más desafortunado que comete una empresa es esperar a que ocurra un desastre para adoptar una postura segura. ¿Cuántas organizaciones no han implantado una política de seguridad que defina el uso aceptable de sus recursos informáticos hasta después de una demanda? En seguridad existe una frace: Cuando no ocurre nada, nos quejamos de lo mucho que gastamos en seguridad. Cuando algo sucede, nos lamentamos de no haber invertido más.

De igual modo que se pueden cometer delitos en el mundo físico, dentro del mundo digital también existen: alguien puede substraer dinero de cuentas de Internet, se puede robar documentación importante a través de la red o se puede tirar abajo un servidor Web de comercio electrónico. En suma, existen múltiples delitos dentro del mundo digital, todos ellos ligados a la información que se aloja en sistemas o que se transmite por las redes de comunicaciones. (Álvarez, Marañón, Gonzalo, and García, Pedro Pablo Pérez. España,2004)

Ley de Delitos Informáticos busca mejorar la lucha contra la ciberdelincuencia.

Norma protege atentados contra la integridad, confidencialidad y disponibilidad de datos y sistemas informáticos.

La Oficina Nacional de Gobierno Electrónico e Informática de la Presidencia del Consejo de Ministros (ONGEI-PCM) expresa que la regulación de figuras delictivas recogidas en la Ley de Delitos Informáticos, promulgada el pasado martes 22 de octubre, contribuye a mejorar la lucha contra la ciberdelincuencia. La referida Ley, que busca proteger atentados contra la integridad, confidencialidad y disponibilidad de datos y sistemas informáticos, sanciona las conductas que tengan la intención de vulnerar las medidas de seguridad establecidas y que puedan inducir al tráfico ilegal de datos, interceptación de datos informáticos y los fraudes informáticos. Adicionalmente, se sancionan figuras como las proposiciones a niños, niñas y adolescentes para obtener de ellos material pornográfico o para tener relaciones sexuales; el fraude informático, el cual sanciona la clonación de tarjetas de crédito o débito; la inducción al error a través de páginas web fraudulentas de agencias bancarias para obtener claves e información del usuario; y la suplantación de identidad, en páginas webs de instituciones públicas, privadas y ciudadanos. (ONGEI-PCM, Peru-2013).

Aprueban el Reglamento de la Ley N° 30254, Ley de Promoción para el uso seguro y responsable de las Tecnologías de la Información y Comunicaciones por Niños, Niñas y Adolescentes.

Que, el artículo 1 de la Ley N° 30254, Ley de Promoción para el uso seguro y responsable de las Tecnologías de la Información y Comunicaciones por Niños, Niñas y Adolescentes, precisa que la citada Ley tiene por objeto promover el uso seguro y responsable de las tecnologías de la información y comunicaciones (TIC) por niños,

niñas y adolescentes para protegerlos de los peligros del mal uso del acceso al Internet, para lo cual el Estado, en sus tres niveles de gobierno, genera normas complementarias sobre el uso seguro y responsable de las TIC, con especial atención al uso que realizan los niños, niñas y adolescentes;

Que, la Única Disposición Complementaria Final de la Ley N° 30254 dispone que el Poder Ejecutivo, a través de la Presidencia del Consejo de Ministros, reglamentará la Ley (Decreto Supremo- N° 093-2019-PCM)

Figura 1

Aprobación de ley 30254

Fuente: ISP Optical Network indica aprobación de ley 30254 para velar la seguridad a nuestros alumnos

1.2. Objetivos

- Determinar de qué manera influye el diseño e implementación de una red de seguridad informática para mejorar la administración de datos en la empresa A.C.E Saco Oliveros - Sede Monterrico. Lima 2021
- Identificar los niveles de protección de la Norma ISO27002:2013 en la empresa ACE Saco Oliveros
- Determinar en qué medida el uso de la Norma ISO27002:2013 influye en proteger atentados contra la integridad, confidencialidad y disponibilidad de datos, y sistemas informáticos en los equipos de cómputo de la empresa ACE Saco Oliveros.
- Diseñar e implementar la topología de red para la administración de datos en la empresa ACE Saco Oliveros.

1.3. Justificación

1.3.1. Justificación Teórica

La razón en cuanto a la investigación desde una perspectiva teórica es la de contar con una metodología de implementación y uso de software libre y así también la documentación necesaria en el área de la seguridad de la información a nivel de la capa de red.

Según la revista RISTI indica sobre las vulnerabilidades en una red en los ambientes de aprendizaje virtuales en todas las instituciones educativas a nivel mundial han evolucionado de forma incomparable, tanto información a nivel académico como investigativa, han generado millones de datos y que estos son compartidos por medio

del conocimiento, las instituciones educativas solo miran el funcionamiento, la disponibilidad de los recursos didácticos, pero no se ha pensado que detrás de un servidor orientado al manejo de entornos virtuales pueden estar varios usuarios con un fin nada ético para sabotear la información, accediendo de forma inusual para realizar cambios de notas, denegación de servicios, y lo más preocupante acceder al resto de información de todas las áreas en lo particular áreas financieras y operativas, todo esto marca la posibilidad que los ambientes virtuales de aprendizaje no cuenten con metodologías apropiadas entorno a la seguridad informática, lo que implica tener un alto riesgo de ser las posibles víctimas de un ataque informático.(Diego Fernando Baroja Llanos, Luis David Narváez Erazo, 2017)

Según la revista RISTI revista Ibérica de Sistemas y tecnologías de la información habla sobre las vulnerabilidades en una red en el sector educación indica que se las conoce como una debilidad, revista me ayuda a respaldar mi investigación que es muy importante tener servidores intermediarios.

Según el documento Negocios de internet: Los servidores, indica que los Proxy Service son muy usados por los proveedores de acceso a la internet (ISP) ya que pueden cumplir varias funciones. La principal es disminuir el tiempo requerido con frecuencia, cumpliendo las funciones de una memoria cache de toda la organización.

Cuando uno de los usuarios solicita un documento, el proxy analizará primero si algún otro usuario ya solicitó ese mismo documento, siendo así, lo presentará sin necesidad de buscarlo en la internet o servidores DNS externos, ahorrando tiempo y consumiendo ancho de banda.

Si la URL no es encontrada, entonces sí será solicitado externamente. Debido a que el proxy se instala entre la organización y el mundo externo (internet) puede ser utilizado para verificar todos los pedidos que entran y salen. En otras palabras, al ser el proxy la puerta de entrada o salida, es el lugar apropiado para colocar medidas de seguridad que protejan a la organización

Es entonces cuando aparece el concepto de firewall, que podríamos describir como una barrera que verifica cada pedido, autorizando o no el paso de información. Los firewalls también permiten mantener una historia de pedidos denegados, con lo cual es posible hacer un análisis de cada incidente y determinar posibles intrusos o hackers.

En sus párrafos del documento presenta lo que requiero para la institución educativa SACO OLIVEROS, que es brindar seguridad al alumnado y docente en todas las sedes, cuidando la integridad y además no perjudicando el ancho de banda del internet.

1.3.2. Justificación Práctica

Por medio del presente estudio se podrá utilizar la tecnología para poder aplicarla y solucionar el problema de investigación; la parte práctica reside en la instalación, configuración y administración de una red estrella extendida con Vlan para gestionar las áreas administrativas, laboratorios de cómputo, aulas de nivel primaria y secundaria conectados a un servidor de seguridad en la red de área local de la institución para así lograr una mejora en la seguridad de la información a nivel de la capa de red.

La aplicación del servidor de seguridad en la red de área local del área administrativa y laboratorio de Computo de la ACE Saco Oliveros, seguirá la metodología de desarrollo de proyectos ágiles, que en este caso se centra en la implementación, configuración y administración de una red LAN administrada por medio de VLAN con todos los servicios correspondientes para controlar y gestionar la

seguridad de la información a nivel de la capa de red. También hacemos uso de la metodología empírica para el desarrollo y la aplicación del proyecto de investigación.

Los laboratorios de cómputo contarían con un servicio PROXI CACHE TRANSPARENT en el Router Trendnet Ac3000 permita dar acceso con políticas de Access List a la navegación del internet garantizando las visitas a páginas permitidas administradas, optimizando el uso de los servicios del laboratorio de cómputo, beneficiando que no haya caídas del servicio de internet. Además de mejorar las actividades que desarrollan los decentes.

El servidor PROXI CACHE TRANSPARENT su beneficio es que aloja en su cache paginas URL ya visitas, al momento de realizar una petición al servidor proxy de un URL la solicitud es inmediata porque entrega la información guardada y no tiene que buscar en servidores externos.

1.3.3. Justificación Social.

Que, el artículo 1 de la Ley N° 30254, Ley de Promoción para el uso seguro y responsable de las Tecnologías de la Información y Comunicaciones por Niños, Niñas y Adolescentes, precisa que la citada Ley tiene por objeto promover el uso seguro y responsable de las tecnologías de la información y comunicaciones (TIC) por niños, niñas y adolescentes para protegerlos de los peligros del mal uso del acceso al Internet, para lo cual el Estado, en sus tres niveles de gobierno, genera normas complementarias sobre el uso seguro y responsable de las TIC, con especial atención al uso que realizan los niños, niñas y adolescentes;

Que, la Única Disposición Complementaria Final de la Ley N° 30254 dispone que el Poder Ejecutivo, a través de la Presidencia del Consejo de Ministros, reglamentará la Ley (Decreto Supremo- N° 093-2019-PCM)

1.4. Descripción de la empresa:

La institución educativa "SACO OLIVEROS" se dedica al rubro de la educación inicial, primaria, secundaria y academia, 25 años potenciando el talento, inspirando y transformado vidas. Fundado en el año 1997.

El creador de este sistema es el Ing. Wilmer Carrasco, quien en su trayectoria como docente preuniversitario y tras un profundo diagnóstico sobre la crisis del sistema educativo, desarrolló esta metodología de enseñanza con el objetivo de preparar a los estudiantes para enfrentar las exigencias del mundo moderno. Somos la gran familia Saco Oliveros y Apeiron.

Brindamos una EDUCACIÓN DE CALIDAD para formar personas con liderazgo y alto sentido ético, capaces de enfrentar la vida dignamente.

Figura 2

Presidente Asociación Saco Oliveros

Fuente: Asociación Civil Educativa Saco Oliveros.
Presidente Wilmer Carrasco Beas.

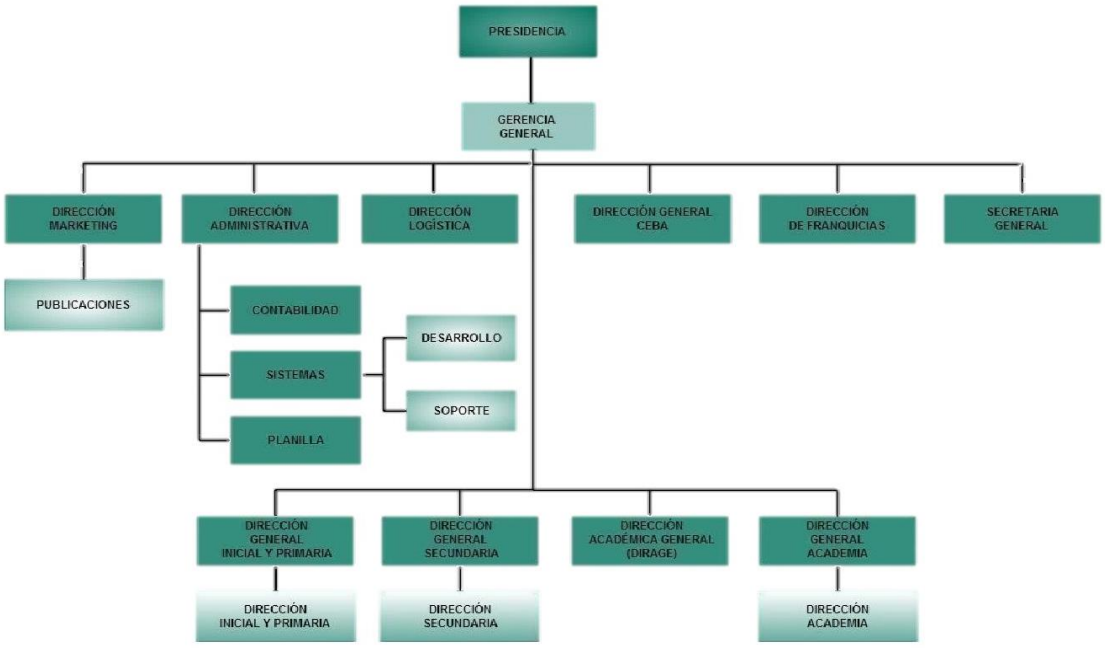
Objetivos

- Motivar e involucrar al estudiante en un nuevo sistema de aprendizaje de alta exigencia.
- Desarrollar sistemas de aprendizaje de acuerdo a la capacidad del estudiante.
- Fomentar el desarrollo de valores y la participación de la familia en la tarea educativa.
- Brindar herramientas adecuadas al estudiante para su ingreso y posterior formación profesional en la universidad o centro superior.

Para ello contamos con un equipo de profesionales altamente calificados y de amplia experiencia que maximizan las competencias de los estudiantes para garantizar una formación integral con excelencia académica.

Figura 3

Organigrama Asociación Saco Oliveros



Fuente: Asociación Civil Educativa Saco Oliveros. La figura ilustra el mapa del organigrama institucional para identificar cada área en la institución.

Las palabras del presidente de la institución en reuniones de gerencia y mensajes hacia los padres de familia indica el uso de las herramientas tecnológicas, el uso del internet como una herramienta principal para nuestro autoaprendizaje y desarrollo personal. Para ello podemos encontrar cursos libres o gratuitos en diversas páginas como www.miriadax.net, en la que podemos encontrar cursos como: coaching personal, inteligencia emocional, comunicación efectiva, y si quieren aprender otros cursos de cualquier índole o materia de las principales universidades podemos ingresar a google a la página Mooc.es y encontraremos un sinfín de alternativas que ayuden a nuestro desarrollo y uso del AULA VIRTUAL SACO OLIVEROS donde todos nuestros alumnos y docentes tendrán acceso a nuestra plataforma.

Actualmente se cuenta con 40 sedes en los diferentes distritos de lima metropolitana y provincias. Con una población de 25.000 alumnos aproximadamente. Su oficina principal está ubicada en el Jr. Manuel Gómez 245 lince - sede de atención en lima.

Figura 4

Sede principal

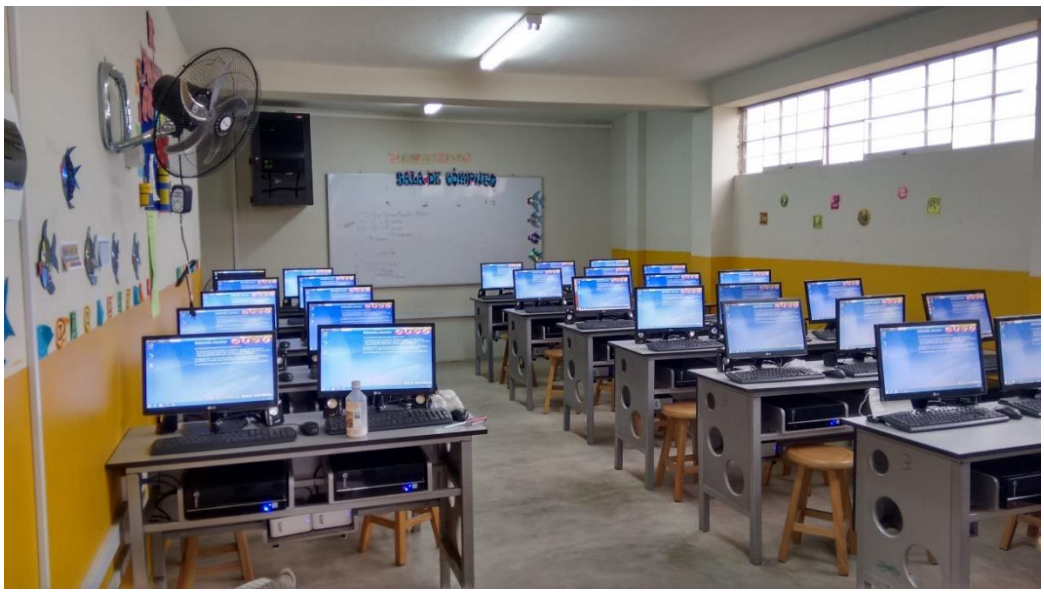
Fuente: Asociación Civil Educativa Saco Oliveros. La figura ilustra la Sede Lince. Sede Principal se encuentran las áreas de presidencia, gerencia, administración, contabilidad, soporte.

Los alumnos y docentes tienen acceso al internet de los Laboratorios de cómputo.

Se tiene 33 Laboratorios de cómputo, cada laboratorio cuenta entre 30 y 40 computadoras totalmente implementadas y equipos de última generación.

Figura 5

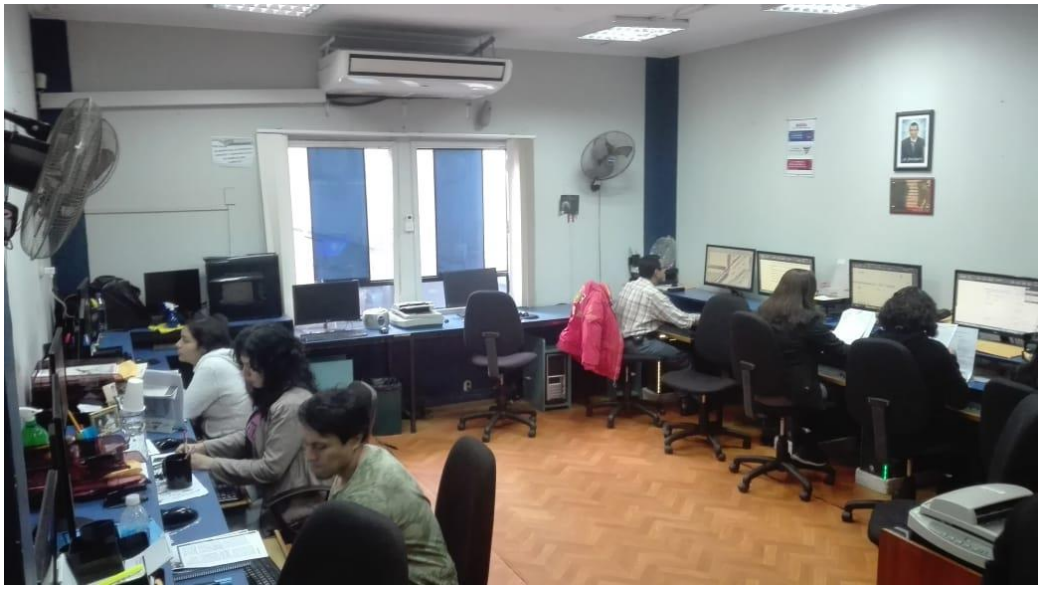
Laboratorio de computo



Fuente: Asociación Civil Educativa Saco Oliveros. La figura ilustra el Laboratorio de cómputo, también incluida en un área de estudio para nuestra investigación.

Figura 6

Área de Publicaciones



Fuente: Asociación Civil Educativa Saco Oliveros, área de Publicaciones, también incluida en un área de estudio para nuestra investigación.

Por la demanda del internet y brindar un valor agregado al servicio que se le brinda a nuestros alumnos, los laboratorios de cómputo cuentan con el servicio de internet. Los alumnos no cuentan con el control debido para la visita a sitios URL, entrando a páginas pornográficas, descarga de videos, música, el cual ocasionan lentitud del servicio de internet a las áreas administrativas de cada sede. Y sobre todo el mal ejemplo que se gana la institución por comentarios externos.

La conexión de internet es abastecida por el ISP. OPTICAL NETWORD, el tendido de su fibra llega directamente a los gabinetes de comunicación de cada laboratorio de cómputo el cual es distribuido por un ROUTER DSL (puerto WAN), por su puerto LAN conecta a los Switches capa 2 que distribuyen el servicio de internet a cada equipo de cómputo.

El ROUTER DSL se instala para separar las redes de los laboratorios de cómputo con las áreas administrativas.

Sin la instalación de un servidor Proxy que ayude como intermediario entre la red WAN-Internet y la red local que son nuestros laboratorios de cómputo, nuestros alumnos y docentes estas propensos a los siguientes problemas:

- Los alumnos y docentes tienen acceso total del internet y ver todo el contenido de páginas web sin tener un servidor de seguridad que filtre el contenido malicioso encontrados en las URL.
- En las búsquedas en internet masiva de todos los alumnos realizan descargas de videos, juegos, música, etc., provocando lentitud del servicio de internet en

las redes administrativas retrasando los sistemas Web locales, sistemas de pagos, control de asistencia personal, dificultad de atención al padre de familia.

- Con el acceso libre al internet se producen descargas de contenido web malicioso, virus, infectando constantemente los equipos de cómputo, ello con lleva a infección de datos y perdida de información.
- La ausencia de un servidor Proxy ocasiona constantemente averías en los equipos del laboratorio de cómputo, muchos casos son reportados al área de Soporte Técnico para su reparación, involucrando tiempo, presupuesto de reparación.

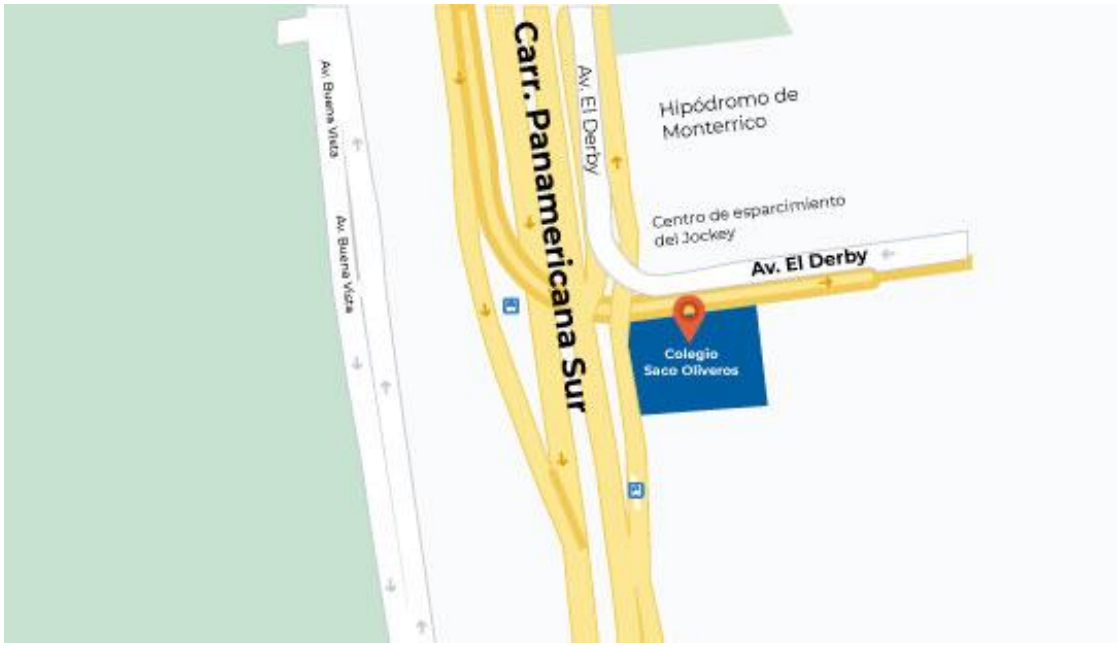
Se expuso a nuestro presidente la necesidad de construir una sede con una Red segura y sea modelo para las demás sedes. El cual se manifestaron los siguientes temas para su implementación:

- Costos y presupuestos
- Tiempos de implementación
- Especialistas elaboración de planos de redes de comunicaciones
- Tipos de implementación del cableado estructurado.
- La Sede asignada será la más moderna de todas las sedes.

Para la sede modelo nuestro presidente nos propuso una sede que sería demolida y edificada con estructuras antisísmicas. La sede asignada es la sede Monterrico, ubicada en el distrito de Santiago de Surco, dirección: Panamericana Sur con Av. El Derby.

Figura 7

Ubicación sede Monterrico



Fuente: Asociación Civil Educativa Saco Oliveros. La figura ilustra la ubicación de la Sede Monterrico.

Figura 8

Proceso constructivo sede Monterrico

Fuente: Asociación Civil Educativa Saco Oliveros. La figura muestra el proceso constructivo de la Sede Monterrico.

Figura 9

Proceso constructivo sede Monterrico

Fuente: Asociación Civil Educativa Saco Oliveros. La figura muestra el proceso constructivo de la Sede Monterrico.

Figura 10

Proyección obra Sede Monterrico

Fuente: Asociación Civil Educativa Saco Oliveros. La figura ilustra la proyección de la Sede Monterrico.

Figura 11

Proyección obra Sede Monterrico

Fuente: Asociación Civil Educativa Saco Oliveros. La figura ilustra la proyección de la Sede Monterrico.

Figura 12

Laboratorio de cómputo sede Monterrico

Fuente: Asociación Civil Educativa Saco Oliveros. La figura ilustra Laboratorio de Cómputo de la Sede Monterrico.

Figura 13

Área de Recepción

Fuente: Asociación Civil Educativa Saco Oliveros. La figura ilustra el área de recepción de la Sede Monterrico.

Figura 14

Áreas administrativas

Fuente: Asociación Civil Educativa Saco Oliveros. La figura ilustra las áreas administrativas de la Sede Monterrico.

Tomando la decisión que bajo esta coyuntura y una visión para el 2022 el inicio de clases semipresenciales. El presidente de la institución decidió entregarme el proyecto de redes a mi persona para construir una red segura y administrada. Teniendo en cuenta que ya había terminado la carrera de ingeniería de sistema. El cual, requería la intervención de un especialista en ingeniería de sistemas.

Adicionalmente se explicó al Presidente las ventajas y desventajas de usar una red cableada

Tabla 1

Ventajas y desventajas de las conexiones cableadas e inalámbricas

	Ventajas	Desventajas
conexión cableada	✓ Mayor estabilidad y escalables de la señal. ✓ Tiene alto rendimiento y velocidad de trasferencia de paquetes. ✓ Son mas seguras y fiables. ✓ Su costo es bajo. ✓ Facil mantenimiento. ✓ Integracion de Señales alambricas e inalambricas.	✓ El tiempo de implementacion es largo.
conexión inalámbrica	✓ Su instalacion es mas rapida y sencilla	✓ Son inestables. ✓ Son inseguras. ✓ El ancho de banda de las redes inalambricas es menor. ✓ La señal inalámbrica puede verse afectada e incluso interrumpida por objetos, árboles, paredes, espejos, etc. ✓ Su costo es elevado. ✓ Requiere de supervision constante del personal de soporte.

*Nota***.** Fuente: Elaboracion propia. Tabla nos indica las ventajas y desventajas de las conexiones cableadas e inalambricas.

CAPÍTULO II. MARCO TEÓRICO

3.4. Antecedentes

Nacionales

1. (Mosquera & Celestino, 2017) La investigación tuvo como finalidad de implementación de un sistema de gestión de la seguridad de la información bajo el ISO 27002 para mejorar la seguridad en cuanto al uso de los activos y tecnologías de la información en la empresa Geosurvey de la ciudad de Lima en el año 2016. El método fue bajo el enfoque cuantitativo, y de tipo aplicativo; porque se utilizó la tecnología para la solución de un problema, así mismo se empleó el diseño pre experimental de pre y post test se llevó a cabo un experimento en condiciones controladas. Tanto la población como la muestra estuvo conformada por 33 trabajadores siendo no probabilística, se tomaron en cuenta todos los trabajadores de las diferentes áreas de la empresa. Para la recolección de datos se utilizó el cuestionario como técnica y el cuestionario de encuesta como instrumento para luego los datos ser procesados en el software estadístico SPSS.

2. (Jaime Fernando Vásquez Escalante – UNMSM – Lima, 2018) En su investigación tuvo como resultado proteger la información en sus tres dimensiones: confidencialidad, integridad y disponibilidad mediante la implementación de una metodología de riesgos que permita identificar las amenazas que atenten contra la seguridad de la información en los procesos de TI de la organización GMD® que administra la plataforma tecnológica y mesa de ayuda de su cliente “ONP”. Las actividades para una correcta implementación del sistema de gestión de seguridad de la información es concienciar al personal en la

importancia de salvaguardar la información que manejan en sus actividades laborales.

3. (Santos Llanos, Daniel Elias – PUCP – Lima, 2016) En su investigación tuvo como resultado cuatro fases cíclicas del SGSI: el establecimiento, donde las bases del sistema se integran a los procesos del negocio; la implementación, que desarrolla los mecanismos para la adecuada administración de la seguridad; el mantenimiento, donde se detectan fallos que pueden existir en la organización o en el propio sistema; y la mejora, que finalmente permite cerrar el ciclo mediante la aplicación de todas las correcciones y optimizaciones significativas que han sido detectadas. Este modelo permite que el sistema opere bajo un principio de mejora continua, que beneficia permanentemente a la organización, propiciando un manejo adecuado de la seguridad de su información.
4. (Tullume Ramos, 2017) En su investigación tuvo como propuesta de Mejora Basada en la Creación de redes virtuales (VLAN) para optimizar la administración de la red de la sede central del Fondo de Cooperación y Desarrollo Social-FONCODES. El incremento exponencial de los equipos informáticos y el uso de internet en las redes de computadoras, representa una gran problemática, ya que podría ocasionar pérdida o mal uso de los activos de la información. La presente propuesta, tiene como finalidad presentar los conceptos para la implementación de redes de área local virtuales, para lograr la segmentación por áreas de trabajo, obtener mayor seguridad y tener un correcto funcionamiento de la red.

Internacionales

1. (Ramos et al., 2017) En su investigación tiene como objetivo principal la opción e implementación de políticas de seguridad de la información teniendo en cuenta la norma 27002:2013, las cuales servirán como guía para proporcionar herramientas que contribuyan a mejorar la gestión de la información obtenida, generada o procesada en CODELCAUCA. , la política de seguridad facilitará la adopción de lineamientos necesarios para garantizar la seguridad de la información teniendo las directrices establecidas en los objetivos de control 5.1.1 y 5.1.2 relacionados con políticas de seguridad y sustentados en los objetivos de la empresa.
2. (Figueroa Leyton, 2019) El presente trabajo de investigacion tiene como objetivo desarrollar un plan de seguridad informática basado en la norma ISO 27002 para el departamento de Tecnologías de la Información y la Comunicación de la Universidad Regional Autónoma de Los Andes. Se implementó además el Diseño Metodológico y Diagnóstico de la investigación y se aplicó una encuesta a estudiantes y docentes de la Uniandes. Finalmente, se planteó una propuesta el desarrollo de un plan de seguridad informática basado en la norma ISO 27002.
3. (Ruano Chinguercela, 2016) En su investigación tuvo como resultado la implementación de calidad de servicio (QOS) en redes locales virtuales (VLAN) mediante las normas 802.1d y 802.1q. Una VLAN (Red de área local virtual o LAN virtual) es una red de área local que agrupa un conjunto de equipos de manera lógica y no física. Efectivamente, la comunicación entre los diferentes equipos en una red de área local está regida por la arquitectura física. Gracias a las redes virtuales (VLAN), es posible liberarse de las limitaciones de la arquitectura física (limitaciones geográficas, limitaciones de dirección, etc.), ya que se define una

segmentación lógica basada en el agrupamiento de equipos según determinados criterios (direcciones MAC, números de puertos, protocolo, etc.)

3.5. Proceso de conectividad de las sedes.

Técnicamente vamos a representar el problema de conectividad LAN que vino pasando la Institución hasta el año 2021, después de culminar la sede modelo se demostró la eficiencia y uso de la tecnología VLAN en una red, optimizando la gestión del ancho de banda del internet, garantizando la mejora continua con las clases semipresenciales (Clases Hibridas) próximas a iniciar.

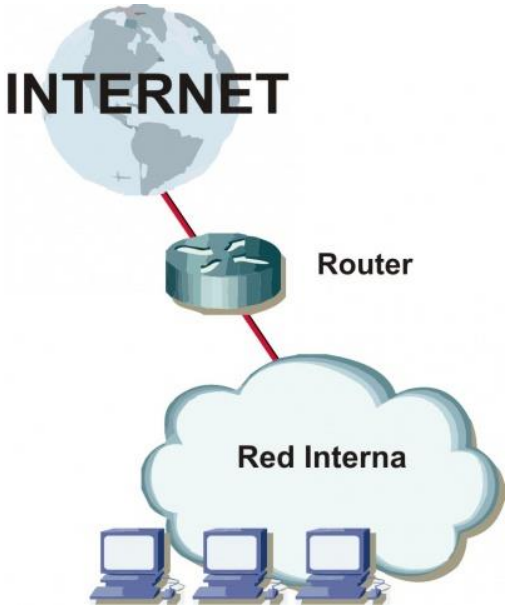
Topología actual de las Sedes - Saco oliveros

Las conexiones de red LAN y el cableado de internet se realizan mediante una Red plana, sin la administración de una red segura:

ISP a ROUTER de ROUTER a SWTICH de SWTICH a PC

Figura 15

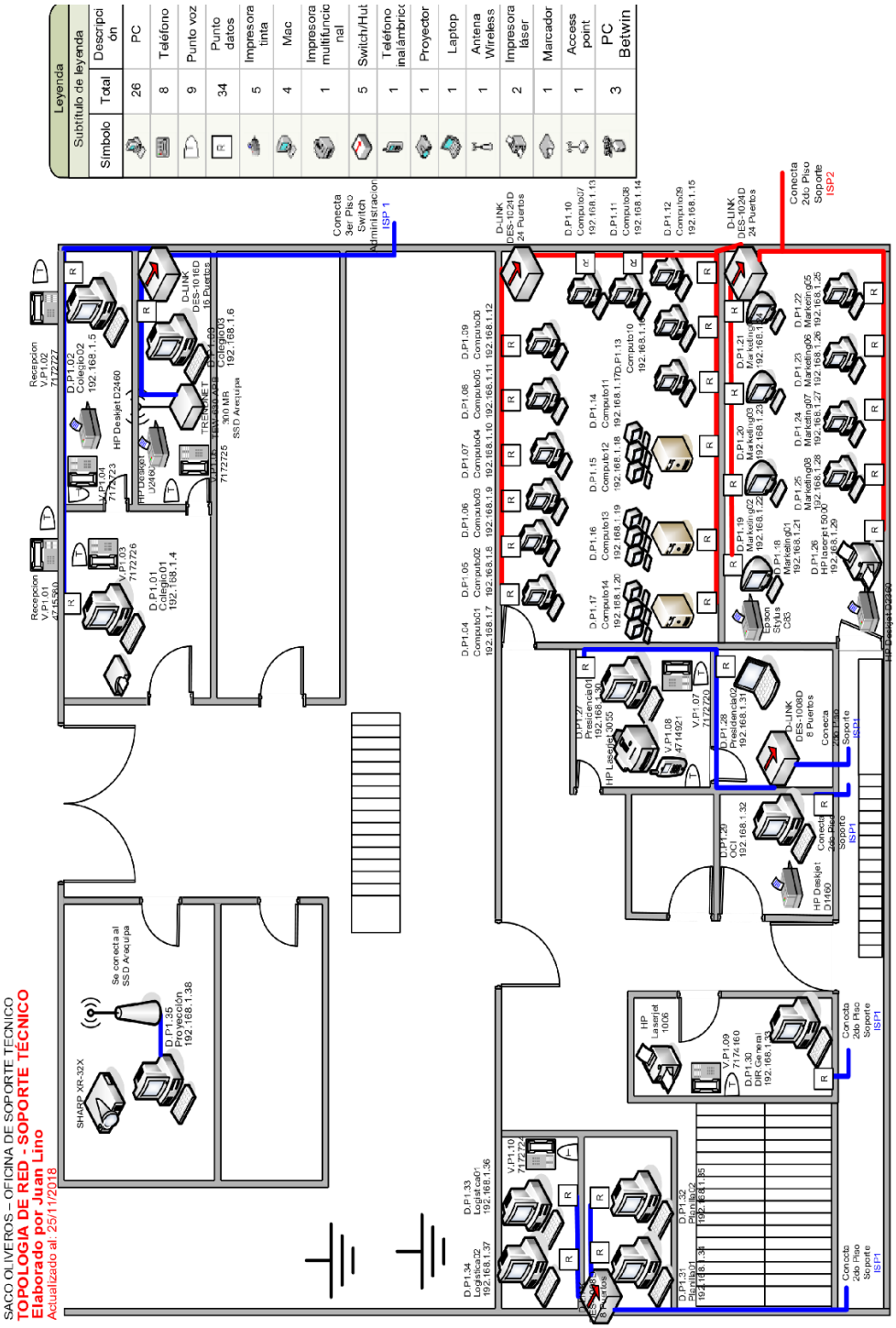
Topología de red – Antes de intervenir



Nota. Fuente: Seguridad informática para empresas y particulares (Gonzalo Álvarez Marañón y Pedro Pablo Pérez García). Esquema Red Básico.

Figura 16

Topología de red Asociación Saco Oliveros



Nota. Fuente: Elaborado por el area de Soporte Tecnico. Topología de RED

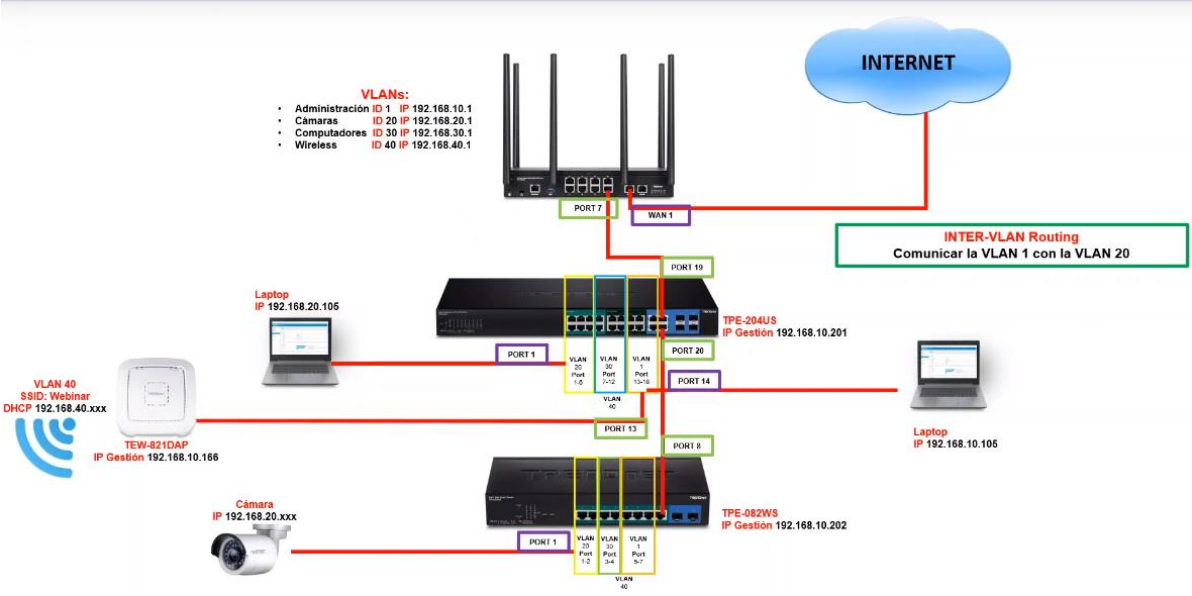
Se detalla las áreas que cuentan con puntos de red LAN. Las áreas involucradas que conforman cada sede son las siguientes:

- Director de Secundaria y Primaria: Usuarios son los responsables de sede, quienes reportan las incidencias de sus diversas áreas a cargo en su sede.
- Tesorería: Gestión de cobros, manejo de sistema Web.
- Secretaria: Realizar informes
- Psicología: Supervisión alumnos
- Coordinación Tutoría: Supervisión alumnos
- Tutoría: Supervisión alumnos
- Laboratorio de cómputo: Soporta el uso diario de clases de informática.
- Puntos de Red Telefonía IP: Todas las sedes cuentan con 3 líneas telefónicas conectadas a la red LAN.
- POS: Equipos POS ubicados en Tesorería para cobros
- Impresoras de red: impresoras ubicadas en secretaria y dirección
- Cámaras IP: Implementación de CCTV IP

Según lo detallado se identifica el problema por la cantidad de equipos informáticos conectados en una red plana no administrada. El resultado del estudio previo presentado a nuestro presidente de la institución es el siguiente:

Figura 17

Topología de red implementada con VLAN



Nota. Segmentación topológica

3.6. Bases Teóricas.

1. **Topologías de red:** Es la propiedad que indica la forma física de la red, es decir, el modo en que se colocan los equipos y el sistema de cableado que los interconectan para cumplir con su función.(*Abad Domingo y E-libro - 2013 - Redes locales..pdf*, s. f.)
2. **PROXY:** Es un intermediario de red entre el cliente solicitante y el servidor que lo brinda.(*Abad Domingo y E-libro - 2013 - Redes locales..pdf*, s. f.)
3. **OSI:** Es el modelo de referencia de una arquitectura de capas para redes de ordenadores y sistemas distribuidos, propuesta por ISO como estándar de interconexión de sistemas abiertos.(*Abad Domingo y E-libro - 2013 - Redes locales..pdf*, s. f.)
4. **VLAN:** Es un método que crea una red Lógica dentro de una red física, de esta forma se logra que la información que se crea dentro de cada una de las redes

virtuales solo sea recibida por el host de la propia red lógica y no por la red física.(Ribes, 2013)

5. **IP:** Mueve los datos de un ordenador a otro. Los paquetes pueden ir por caminos distintos. El receptor los reordena. Si un paquete llega mal, se retransmite sólo ese paquete. **ISP:** El proveedor de servicios de Internet (ISP, por la sigla en inglés de Internet service provider) es la empresa que brinda conexión a Internet a sus clientes. Un ISP conecta a sus usuarios a Internet a través de diferentes tecnologías como DSL, cablemódem, GSM, dial-up, etcétera.(Barcell, s. f.)
6. **TCP/IP:** Los protocolos IP (Protocolo de Internet) y TCP (Protocolo de Control de Transmisión) se originaron a principios de 1980 y fueron adoptados por la red ARPANET en 1983, que estaba integrada por cientos de computadoras de universidades, centros de investigación militar y algunas empresas.(*sep_art51.pdf*, s. f.)
7. **TCP:** Coordina el movimiento de datos entre ordenadores dividiendo dichos datos en paquetes. (Barcell, s. f.)
8. **UTP:** El cable sólido UTP SATRA Categoría 6 de 4 pares trenzados, diseñado para redes de alta velocidad con alto rendimiento. Cumple y supera los requerimientos descritos en las especificaciones de la norma ANSI/TIA-568-C.2, brindando un ancho de banda (frecuencia de operación) de 250MHz.(*Cables de Cobre U/UTP CM SólidGo Categoría 6 - Satra Perú*, 2021)
9. **U/FTP:** El cable sólido U/FTP SATRA Categoría 6A de 4 pares trenzados, combina el desempeño de 10Gbps con seguridad e inmunidad al ruido. Cumple y supera los requerimientos descritos en las especificaciones de la norma ANSI/TIA-

568-C.2, brindando un ancho de banda (frecuencia de operación) de 500MHz.(*Cables de Cobre U/FTP Sólido Categoría 6A - Satra Perú*, 2021)

10. **LAN:** Es una red de área local, es una grupo de elementos físicos y lógicos que realizan interconexión entre dispositivos de un área privada.(*Abad Domingo y E-libro - 2013 - Redes locales..pdf*, s. f.)
11. **WAN:** Es una red que intercomunica equipos en una área geográfica muy amplia.(Abad Domingo & E-libro, 2013)
12. **DNS:** Es un servicio de red que consta de una base de datos que asocia direcciones ip con nombres de dominio, que son más fáciles que recordar.(Ribes, 2013)

CAPÍTULO III. DESCRIPCIÓN DE LA EXPERIENCIA

4.4. Proceso de ingreso a la empresa:

El ingreso a la institución Saco Oliveros fue por la vía de convocatoria en el año 2005. El cual, solicitaban especialistas en electrónica y sistemas para la reparación de equipos informáticos y administración de las redes de comunicaciones. El área de Soporte era constituida por el Jefe del área de Publicaciones y 3 técnicos.

En año 2007, el jefe de Publicaciones me asigna el cargo de Coordinador del área de soporte para liderar y gestionar todas las incidencias de las sedes, el año 2007 se contaba con 25 sedes en las diversas zonas.

4.5. Funciones Coordinador de Soporte

Se detalla el Rol y las funciones que realizo como coordinador de Soporte y demás involucrados en la gestión de incidencias. Se uso la herramienta IBM RSA para de modelado de negocio.

La institución educativa “SACO OLIVEROS” se dedica al rubro de la educación inicial, primaria, secundaria y academia, Su oficina principal está ubicada en el Jr. Manuel Gómez 245 lince - sede de atención en lima y provincias.

Se realizan las actividades de soporte técnico de acuerdo a lo siguiente: El Director hace el reporte de una incidencia al coordinador de soporte quien recibe la atención y la clasifica si es un servicio o la adquisición de un producto. Si fuera un servicio programa, si fuera adquisición se deriva el requerimiento al jefe de logística.

El Director hace el reporte de una incidencia al coordinador de soporte quien recibe la atención y la clasifica como un servicio, durante la atención el técnico verifica que se trata de un componente dañado, y realiza una solicitud mediante un formato de conformidad de trabajo autorizada por el Director de la sede. Dicha solicitud realizada por el técnico llega al coordinador de soporte para detallar en un formato de requerimiento de bienes al jefe de logística. El jefe de Logística

Entrega el requerimiento con una guía de remisión al coordinador de soporte y/o director de sede, quien asigna un técnico para revisión e instalación del requerimiento abastecido. Finalmente, el director firma una conformidad de culminación de servicio al técnico quien a su vez entrega sus conformidades de trabajo al coordinador.

4.6. Objetivos del coordinador de Soporte

- ✓ Administrar y garantizar el buen funcionamiento de las redes de comunicaciones.
- ✓ Prevención y/o solución de problemas técnicos de hardware y software en las computadoras. Mediante el acceso remoto y acceso presencial.
- ✓ Atención oportuna en casos de contingencias al 100%.
- ✓ Garantizar la operación de los sistemas de información de forma rápida, oportuna mediante tareas rutinarias al 100 %.

4.7. Modelado de Negocio

4.7.1. Lista de Casos de Uso de Negocio

Tabla 2

Lista casos de uso de negocio incidencias y abastecimiento

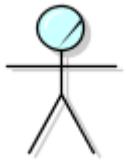
Caso de uso del negocio	Descripción
CUN01 – [Proceso de Incidencias del CUN01]	*Este proceso es enviado por el responsable de la sede (Director).* *La incidencia llega al coordinador de soporte técnico mediante correos, llamadas telefónicas.* *Coordinador verifica prioridad de la incidencia* *Coordinador asigna si el caso de incidencia es presencia o no presencial.* *Coordinador asigna personal técnico para cubrir incidencias* *Coordinador reporta caso de atención al usuario.*
CUN02 – [Abastecimiento de Componentes del CUN02]	*Las reparaciones que implique cambio de componentes, implementaciones de nuevas áreas, o alguna compra de artículos son derivadas al área de Logística. Vía documentación (requerimiento, conformidad de trabajo), Documentos son aprobados por directores responsables.* *El jefe de Logística se encarga de aprobar requerimientos enviados por el coordinador de Soporte Técnico* *El jefe de Logística verifica su stock, si tuviera stock envía abastecimiento a sede o área de producción. Sino tiene stock cotiza a proveedor, proveedor abastece almacén de Logística y Logística abastece a sedes o áreas de producción.*

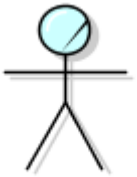
Nota. Fuente: Elaboracion propia. Tabla nos indica lista de casos de uso del proceso incidencias y abastecimiento.

4.7.2. Lista de Actores del Negocio

Tabla 3

Lista actores de negocio

Actor del Negocio	Descripción
 Director	*Representa a los usuarios de las diferentes sedes de lima y provincias, dichos usuarios son los responsables de sede, quienes reportan las incidencias de sus diversas áreas a cargo en su sede.*

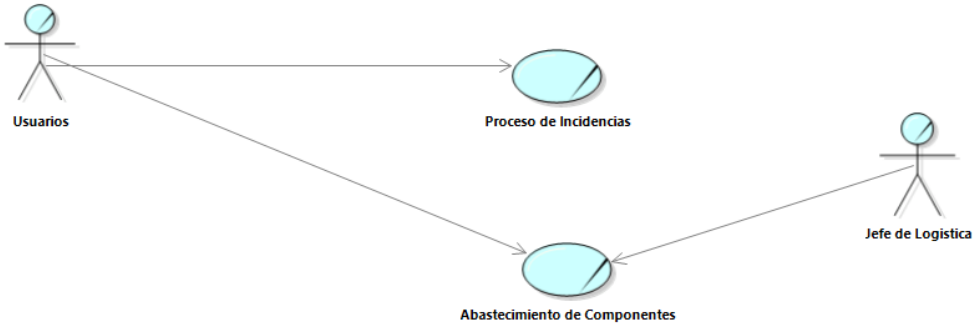
 Jefe de Logistica	*Representa al jefe de Logística, el cual se encargará de abastecer los requerimientos a las diversas sedes y a Soporte Técnico.* *La recepción de requerimientos es verificada por los usuarios el cual firman la guía de remisión dando conformidad a lo requerido.*

Nota. Fuente: Elaboracion propia. Tabla nos indica lista de actores de negocio

4.7.3. Diagrama General de Caso de Uso del Negocio

Figura 18

Diagrama General de Caso de Uso del Negocio



Fuente: Elaboración propia

4.7.4. Lista de Trabajadores de Negocio

Tabla 4

Lista de trabajadores de negocio

Trabajador del Negocio	Descripción
 Coordinador de Soporte	*Recepciona reporte de incidencias y la programación de actividades de los técnicos*
 Tecnicos	*Atienden las incidencias de las diversas sedes de la institución.*

Nota. Fuente: Elaboracion propia. Tabla nos indica lista de trabajadors de negocio área soporte

4.7.5. Lista de Entidades de Negocio

Tabla 5

Lista de entidades de negocio

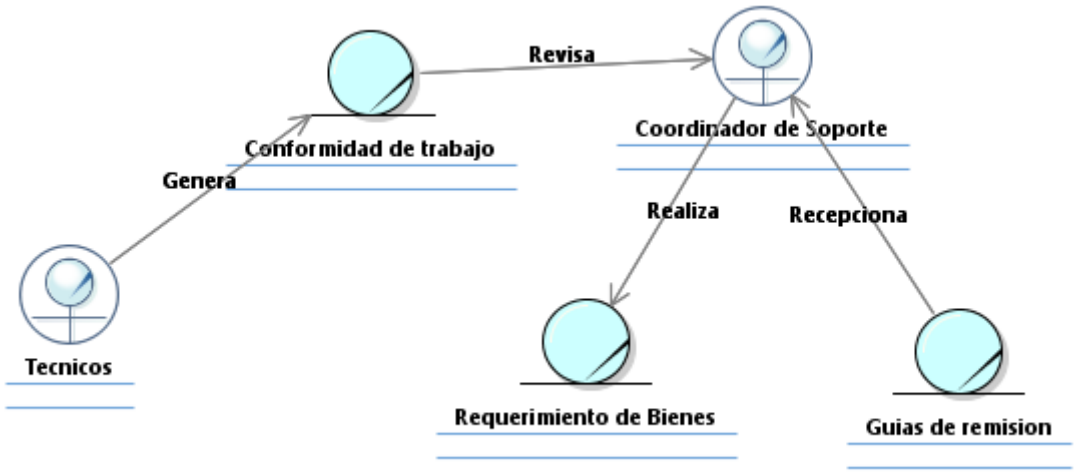
Entidad del Negocio	Descripción
	- *Generado por el Coordinador de Soporte.* - *Recepcionado por el Jefe de Logística.*
	- *Generado por el Director de sede.*
	- *Emitido por el jefe de Logística*
	- *Registrador por el coordinador de Soporte Técnico.*
	- *Generado por los técnicos responsables de cubrir cada incidencia.*

Nota. Fuente: Elaboracion propia. Tabla nos indica lista de entidades de negocio

4.7.6. Diagrama de Clases de Negocio

Figura 19

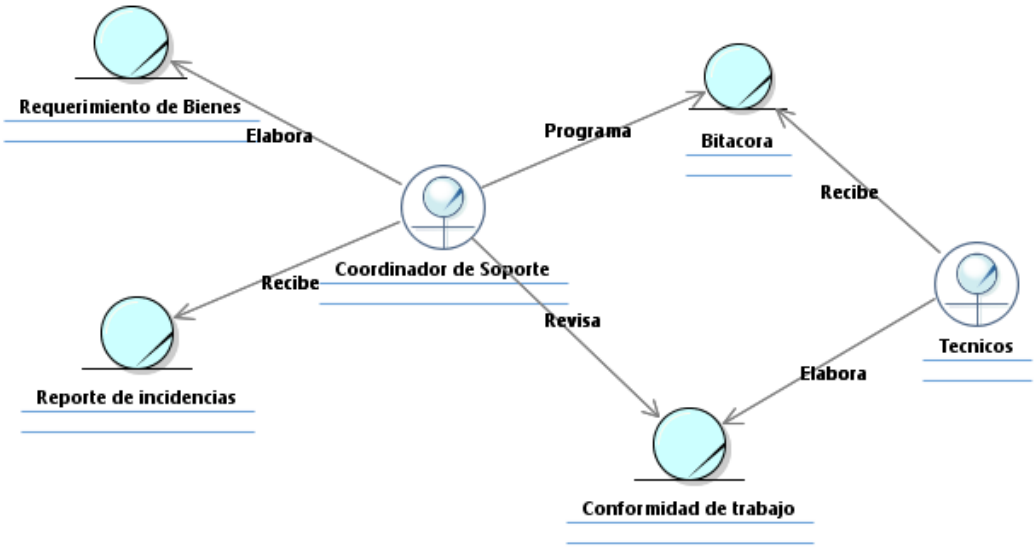
DCN_Abastecimiento de Componentes



Fuente: Elaboración propia

Figura 20

DCN_Reporte de Incidencias

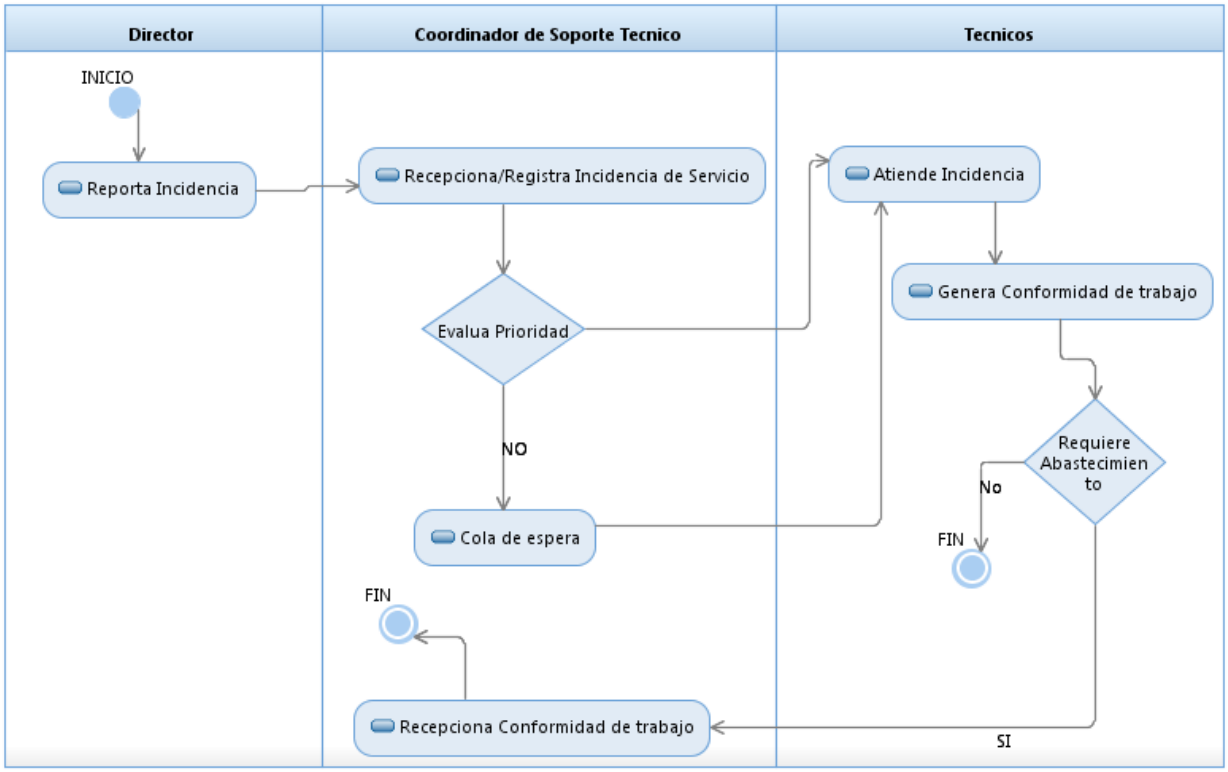


Fuente: Elaboración propia

4.7.7. Diagrama de Actividades de Negocio

Figura 21

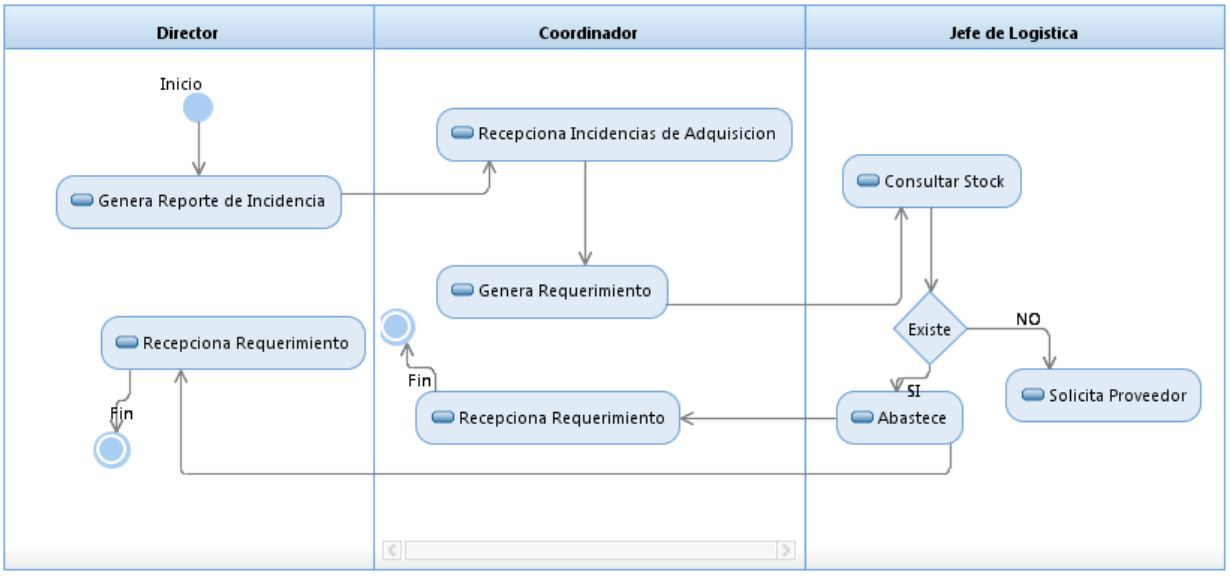
DAN_Reporte de Incidencias



Fuente: Elaboración propia

Figura 22

DAN_Abastecimiento de Componentes



Fuente: Elaboración propia

El presente proyecto corresponde al I.E.P Colegio Saco Oliveros de Monterrico ubicado en Panamericana Sur con av. El Derby, Monterrico, Distrito de Santiago de Surco, provincia y departamento de Lima. La construcción consta de 5 módulos de 4 niveles conformada por aulas, oficinas administrativas, 02 laboratorios de cómputo, biblioteca y auditorio.

El desarrollo del proyecto inicia en la sede Monterrico, una de las sedes con categoría alta económicamente. Entre su población de alumnado se tienen los niveles de inicial, primaria y secundaria. La sede se demolió en diciembre del 2020 para edificar una nueva construcción antisísmica. Nuestro presidente de la Institución Saco Oliveros me entrego la responsabilidad para ejecutar los trabajos de conectividad de redes y seguridad informática en la sede Monterrico.

Para el siguiente proyecto usaremos como metodología de procesos, el ciclo de Deming más conocido como el ciclo PHVA (Planificar, Hacer, Verificar, Actuar).

Se realizará comparativas de conexiones alámbrica(cableado) y conexión inalámbrica (wifi).

Para llevar a cabo el proyecto no debe de afectar los procesos u operaciones de las actividades actuales y proyectos del área de Soporte.

La presente planificación del proyecto de actividades tendrá como fin. El Diseño e implementación de la conexión cableada e inalámbrica de red (internet) para computadora del docente y punto de red para gestionar el proyector de las aulas. Asimismo, las conexiones de red para las áreas administrativas, Laboratorios de cómputo, cámaras IP segmentado atravez de VLAN.

Actualmente la institución no cuenta en sus sedes con la conexión de red de datos administrada en sus diversas áreas. Es por ello, el consumo excesivo del internet, siendo perjudicial a las aplicaciones contables de la red administrativa.

Por lo cual, en la nueva construcción de la sede Monterrico se realizó el cableado estructurado de red, audio y video en las aulas, laboratorios y áreas administrativas.

Objetivos del Coordinado de Soporte

Objetivo General:

- Determinar e implementar aulas con conexiones de red y acceso a internet, garantizando mejora continua a los alumnos y docentes.
- Garantizar estabilidad del cableado estructurado.
- Comparar el uso de conexiones cableadas e inalámbricas.
- Evaluar tiempos de actividades del personal de soporte.

Planificación del Proyecto.

Desde un enfoque de gestión e impulsar su optimización continua a través del tiempo que nos demandara el proyecto, usaremos la metodología PHVA para alinear los procesos de las actividades y medir tiempos que al personal de Soporte le demandara.

Por medio del presente estudio del proyecto se podrá usar la tecnología para poder aplicarla y solucionar problemas. El propósito de la planificación es alcanzar nuestros objetivos, y medir el progreso de los objetivos.

NORMAS DE ESTÁNDARES INTERNACIONALES PARA LA CONSTRUCCIÓN Y DISEÑO DE LAS REDES DE COMUNICACIÓN

Se cuenta con una red de comunicación tipo estrella extendida donde las estaciones están conectadas directamente a un punto central y todas las comunicaciones se hacen

necesariamente a través de ese punto (conmutador, repetidor o concentrador). Usando el modelo de referencia OSI.

Ventajas:

- Posee un sistema que permite agregar nuevos equipos fácilmente
- Reconfiguración rápida de cada daño
- Fácil de prevenir daños y/o conflictos, ya que no afecta a los demás equipos si ocurre algún fallo.
- Centralización de la red.
- Fácil de encontrar fallas de cada uno de ellos

Proveedor de internet(ISP)

- El servicio del local educativo presenta las siguientes características:
- Proveedor del servicio de Internet (ISP): Optical Networks
- Razón Social: Optical Technologies Sac
- Ruc: 20552504641
- Medio físico de transporte local: fibra óptica
- Ancho de banda: 40 Mbps
- Overbooking: 100% garantizado 1:1

Tipo de servicio de telefonía:

- Central Virtual de Respuestas de voz interactivas (IVR).
- Proveedor del servicio de telefonía: Optical Networks
- Número Asociado: (01) 680 5300 Anexo 251,252.

Tabla 6

Estado sede

Estado actual sede	Estado deseado sedes	Observación
- Identificar cantidad de aulas en sedes	-Tener identificado la cantidad de aulas por sede. El cual serán trabajadas	Validar si todas las aulas serán usadas
- Ausencia de conexión de red e internet en aulas	- Las aulas deben tener conexiones estables de audio, video y red, sea cableado o inalámbrica	La conexión cableada tiene mayor estabilidad
- Diseñar plano topológico de red	- Estudio estructural de la obra	
-	-	
Habilitar oficina de ingeniería	Habilitar espacio de 25 m2	Espacio servirá para estudio de planos, almacén de herramientas

Nota. Fuente: Elaboracion propia. Tabla nos indica el estado actual y el estado deseado de las sedes.

Para la distribucion del personal de soporte asignado a realizar actividades en la obra sede Monterrico, se realizo el estudio de trabajos y proyectos que altualmente se ejecutaban.

En el area de Soporte contamos con 12 profesionales en sistemas y electronica.

Tabla 7

Resumen de actividades personal del área de soporte

Estado actual actividades	Personal de Soporte	Fecha inicio	Fecha fin	Observación
- Gestión, distribución de actividades	- Juan Lino		Hasta la actualidad	
- Atención remota a docentes y personal administrativo, en equipos institucionales en calidad de préstamo y equipos personales	- Javier Apeña - Dante Uribe - Gustavo Tornero - Luis García		Dic-2021	

- Reparación presencial de equipos de cómputo. Validar estado de equipos	- Dante Uribe - Gustavo Tornero - Luis García		Dic-2021	
- Obra Monterrico: Gestión, diseño, canalización, cableado estructurado de red, video, audio, cámaras, sensores de seguridad,	- Juan Lino - Manuel Flores - Arturo Chávez - Nicanor Ventura - Diego Maldonado - Fernando Castillo - Elías Huaripuma	Mar 2021	Dic-2021	-Proceso de canalización tuberías en aulas y áreas administrativas, troncales-buzones. -Cableado, conexiones de redes, audio, video, cámaras, sensores. - Instalación y configuración de equipos.
-Obra Ate: Gestión, diseño de planos, canalización, cableado estructurado de red, video, audio, cámaras.	- Juan Lino - Manuel Flores - Arturo Chávez - Nicanor Ventura - Diego Maldonado - Fernando Castillo - Elías Huaripuma			En ejecución, Falta levantamiento de planos
- Mantenimiento, reparación de equipos proyectores, sistema de audio, Ecran en sede.	- Juan Lino - Manuel Flores - Arturo Chávez - Nicanor Ventura - Diego Maldonado - Fernando Castillo - Elías Huaripuma - Javier Apeña - Dante Uribe - Gustavo Tornero - Luis García	Nov2021	Feb 2021	Actualmente 863 proyectores en aulas, mantenimiento electrónico interno de componentes. Estando próximos a las clases, se realizará el mantenimiento preventivo y correctivo de los equipos multimedia
- Mantenimiento de equipos de cómputo.	- Juan Lino - Manuel Flores - Arturo Chávez - Nicanor Ventura	Nov2021	Feb 2022	Estando próximos a las clases, se realizará el

- Retorno de equipos de cómputo a sedes de origen	- Diego Maldonado - Fernando Castillo - Elías Huaripuma - Javier Apeña - Dante Uribe - Gustavo Tornero - Luis García - Juan Lino - Manuel Flores - Arturo Chávez - Nicanor Ventura			mantenimiento preventivo y correctivo de los equipos de cómputo.
- Mantenimiento de equipos de comunicación, redes Lan, Wan, cometidas	- Diego Maldonado - Fernando Castillo - Elías Huaripuma - Javier Apeña - Dante Uribe - Gustavo Tornero - Luis García - Juan Lino - Manuel Flores - Arturo Chávez - Nicanor Ventura	Nov2021	Feb 2022	Estando próximos a las clases, se realizará el mantenimiento preventivo y correctivo de los equipos de comunicación
-Mantenimiento de cámaras de seguridad	- Diego Maldonado - Fernando Castillo - Elías Huaripuma - Javier Apeña - Dante Uribe - Gustavo Tornero - Luis García	Nov2021	Feb 2022	Mantenimiento preventivo y correctivo de las cámaras de seguridad.
- Configuración de Tablet	- Dante Uribe - Luis García			

Nota. Fuente: Elaboracion propia. Tabla nos indica el estado actual, programación de las actividades del personal del area de soporte.

Teniendo como referencia las activiades del personal de Soporte que actualmente realizan y las actividades que se estan por programar. Se detalla descripcion del proceso, tiempos de ejecucion por procesos en la obra sede Monterrico.

Tabla 8

Procesos de actividades sede Monterrico

N° Proceso	FECHA INICIO	FECHA FIN	DESCRIPCION	OBSERVACION
1er Proceso	02/01/2021	30/01/2021	Diseño, estudio de planos de comunicaciones REDES	Compatibilizar con planos de arquitectura, estructurales, eléctricos, gasfitería. Sede Monterrico se divide en 5 módulos
2do Proceso	01/03/2021	30/08/2021	Canalización de tuberías de REDES en aulas y áreas administrativas, troncales- buzones.	La ejecución de canalización de redes es programada según llenado de techos y muros. Avance del área de ingeniería civil
3er Proceso	01/09/2021	30/09/2021	Cableado estructurado conexiones de redes	Cableado de red en aulas, laboratorios de cómputo, áreas administrativas, cámaras ip
4to Proceso	01/10/2021	30/10/2021	Instalación de equipos de comunicaciones	Instalación de equipos de comunicación en Data Center, gabinetes, ponchado de puntos de red en 5 módulos construidos, perímetros
5to Proceso	01/11/2021	05/11/2021	Pruebas de calidad y control de conectividad	Pruebas de enlaces entre trocales de cada módulo y data center, pruebas de aulas con gabinetes
6to Proceso	15/11/2021	27/11/2021	Configuración de equipos de comunicaciones	Configuración de equipos VLAN:-ROUTER TRENDNET TEW-829DRU/AC3000- Smart Switch Gbe 16puertos Trendnet Teg-204ws 4sfp-Rackeable
7mo Proceso	01/12/2021	15/12/2021	Instalación de quipos informáticos	Instalación y configuración de equipos información en diversas áreas

Nota. Fuente: Elaboracion propia. Tabla nos indica los procesos ejesutados en la sede Monterrico

1er Proceso: Diseño, estudio de planos de comunicaciones REDES.

La elaboración de planos se realizó en el programa AutoCAD, versión 2021. El área de Arquitectura Liderado por la Arq. Liliana Carrasco nos entregó los planos de arquitectura. El cual, se añadió el dibujo de redes

Se realizó el diseño de topología estrella extendida, correspondientes a 5 módulos, cada módulo cuenta con 4 pisos. Ver anexos n.° 3 - n.° 6. Planos del 1er al 4er piso, canalización y conectividad de redes.

Figura 23

Compatibilidad de planos de redes de datos

Fuente: La figura ilustra lectura de planos de ingeniería compatibilizados con diversas especialidades.

2do Proceso: Canalización de tuberías de REDES en aulas y áreas administrativas, troncales- buzones.

La canalización empotrada en muros y techo por medio de tuberías pvc Sap 3⁄4 marca pavco en laboratorio de cómputo y recepción. Se acondicionaron troncales (Unión de módulos) por medio de buzones excavación en piso usando tuberías de 4” sap pvc. Todas las aulas cuentan con red e internet.

La canalización de Redes, se gestionó requerimientos al área de logística para el envió de material.

Figura 24

Sistema de requerimiento Saco Oliveros

It.	Cantidad	Stock	Código	Nombre Articulo	Und Med	Tipo Requer.
0001	150,00		02180920008	TUBO SAP DE 3/4"	UND	
0002	50,00		02180920002	TUBO SAP DE 1 1/4"	UND	
0003	50,00		02180920003	TUBO SAP DE 1"	UND	
0004	30,00		02180920001	TUBO SAP DE 1 1/2"	UND	
0005	150,00		02180890017	CURVA SAP DE 3/4"	UND	
0006	30,00		02180890010	CURVA SAP DE 1 1/2"	UND	
0007	40,00		02180890012	CURVA SAP DE 1"	UND	
0008	30,00		02180890011	CURVA SAP DE 1 1/4"	UND	
0009	150,00		02180890008	CONECTOR SAP DE 3/4"	UND	
0010	30,00		02180890026	UNION SAP DE 3/4"	UND	

Fuente: Figura muestra la solicitud de requerimientos al área de Logística

Los trabajos de canalización de tuberías de redes de datos en techos y muros se realizaron con las medidas de seguridad contando con EPP para trabajos.

Figura 25

Canalización de redes de datos

Fuente: Figura muestra, técnicos realizando la canalización de redes de comunicaciones

Figura 26

Canalización de cajas de pase redes de datos

Fuente: Figura muestra, técnicos realizando la canalización de redes de comunicaciones

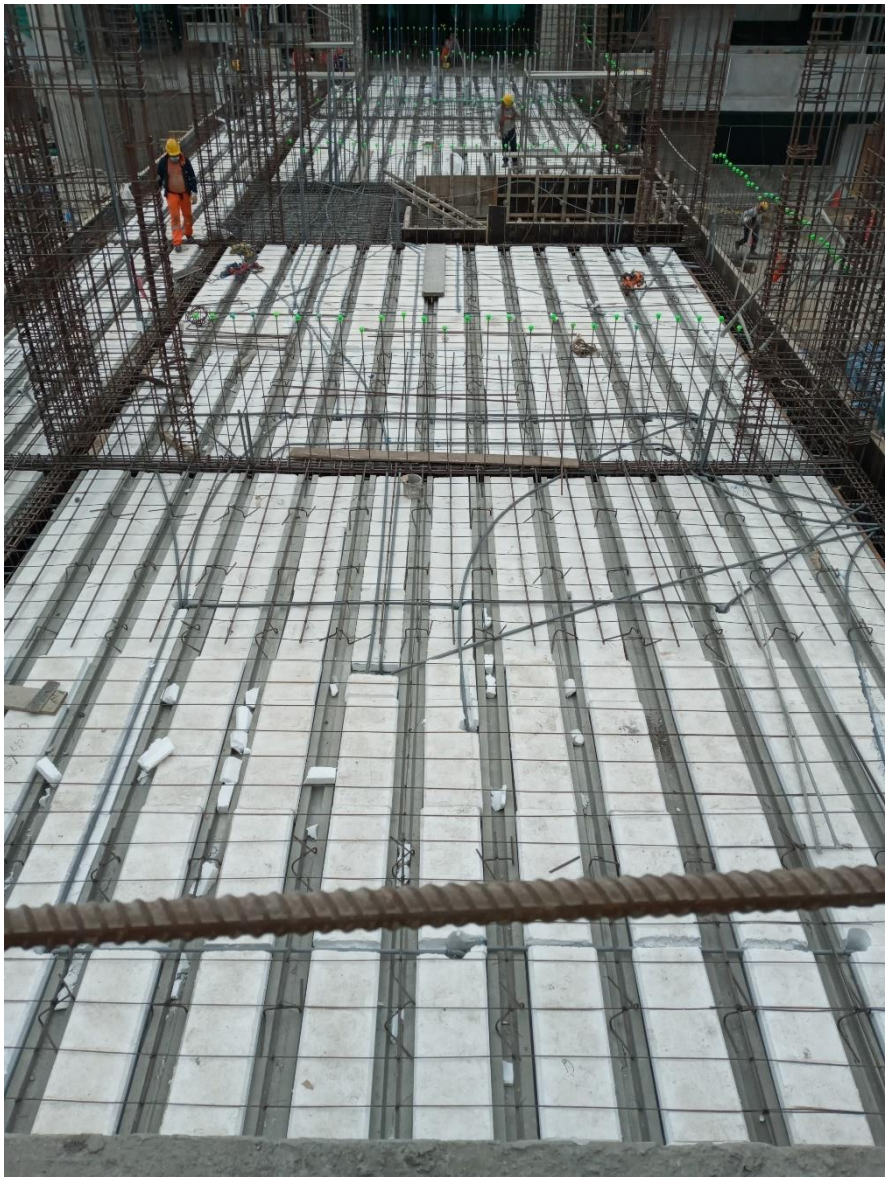
Figura 27

Canalización de cajas de pase redes de datos

Fuente: Figura muestra, técnicos realizando la canalización de redes de comunicaciones

Figura 28

Canalización de tuberías de REDES de datos para aulas



Fuente: Figura muestra la canalización de redes de datos en aulas, según plano.

3er Proceso: Cableado estructurado conexiones de redes.

El Cableado de red se ejecutó en 31 aulas 02 puntos de red, 02 laboratorios de cómputo cada laboratorio 30 puntos de red, 32 puntos de red en áreas administrativas, 25 puntos de red para cámaras IP.

Tipo de cables:

- UTP: Marca Dixon modelo 9020 multifilar cat6 TIA/EIA-586B.2, usado para conexión de equipos de cómputo, telefonía, marcador de huella y cámaras. Cable UTP cat6 marca SATRA sólido gris. Cumple con la norma ANSI/TIA-568-C.2

- U/FTP: Cable Solido U/FTP LSZH Categoría 6A de 4 pares trenzados, combina el desempeño de 10Gbps con seguridad e inmunidad al ruido. Cumple y supera los requerimientos descritos en las especificaciones de la norma ANSI/TIA-568-C.2, brindando un ancho de banda (frecuencia de operación) de 500MHz.

Figura 29

Cableado estructurado – UTP cat6A

Fuente: Cableado estructurado Data Center - Sede Monterrico

Figura 30

Instalación de gabinete de piso de 44ru – Data Center

Fuente: Figura muestra instalación de Gabinete de piso 44ru

Figura 31

Ponchado de puntos de red en Patch panel

Fuente: Figura muestra ponchado de puntos de RED - Data Center

Figura 32

Instalación de Switches de RED

Fuente: Figura muestra instalacion de equipos de comunicación(Switches, Patch panel, Orgizadores)

4to Proceso: Instalación de equipos de comunicaciones.

Instalación de equipos de comunicación en Data Center, gabinetes, ponchado de puntos de red en 5 módulos construidos, perímetros.

El personal de soporte realiza la instalación de los gabinetes anclándolos en muros y pisos con anclajes de expansión, según especificación del fabricante, brindando seguridad a los

usuarios. Todos los equipos de comunicación son instalados en los gabinetes para no estar expuestos.

- Gabinetes de Pared: GABINETE DE PARED 6RU (30 X 60 X 40CM),son ideales para instalaciones donde el espacio disponible es limitado. Los gabinetes de pared son la solución perfecta para cualquier instalación estándar de 19 pulgadas de cables para dar a las instalaciones un aspecto profesional, seguro y organizado. Se usan comúnmente con paneles de interconexión y de distribución. Basados en las normas: EIA – 310D de 19” DIN41494 parte 1 - 7 IEC60297 parte 1 – 2

Figura 33

Instalación de gabinetes de pared en módulos 1B, 3, 4, 5.

Fuente: Figura ilustra instalación de gabinetes de redes en módulos para la red de las aulas.

- Gabinete de Piso: Gabinete de Piso 44RU (Alt. 214 x Anch. 61 x Prof. 100 cm). Gabinete de 44RU, de estructura metálica, óptimo para la instalación de sus servidores. Disponen de

una puerta frontal, posterior y laterales. Cuenta con rieles de perforaciones cuadradas que permitirán la instalación de servidores toolless o instalar equipos que cuenten con otras perforaciones utilizando pernos enjaulados. Diseñados para para Centros de Datos. Carga máxima hasta 1000Kg. Basado en la norma. EIA/ECA – 310-E. DIN41494 parte 1 - 7 IEC 60297-3-100 ASTM A366, ASTM E-136 y ASTM E-84 clase A ASTM B 633 ASTM 1008

Figura 34

Implementación de gabinete de red 44RU – Data Center

Fuente: Figura muestra la culminación del gabinete de 44RU

- **Rack de pared de 6 RU:** Basados en las normas EIA-310D de 19". DIN41494 parte 1 - 7. IEC60297 parte 1 - 2. Certificados JIS G-3141-SPCC ASTM 1008 (Reemplaza a la norma ASTM A-366). Dimensiones (Profundidad 30.5 cm x Ancho 50 cm x Alto 26.2 cm)

CARACTERÍSTICAS:

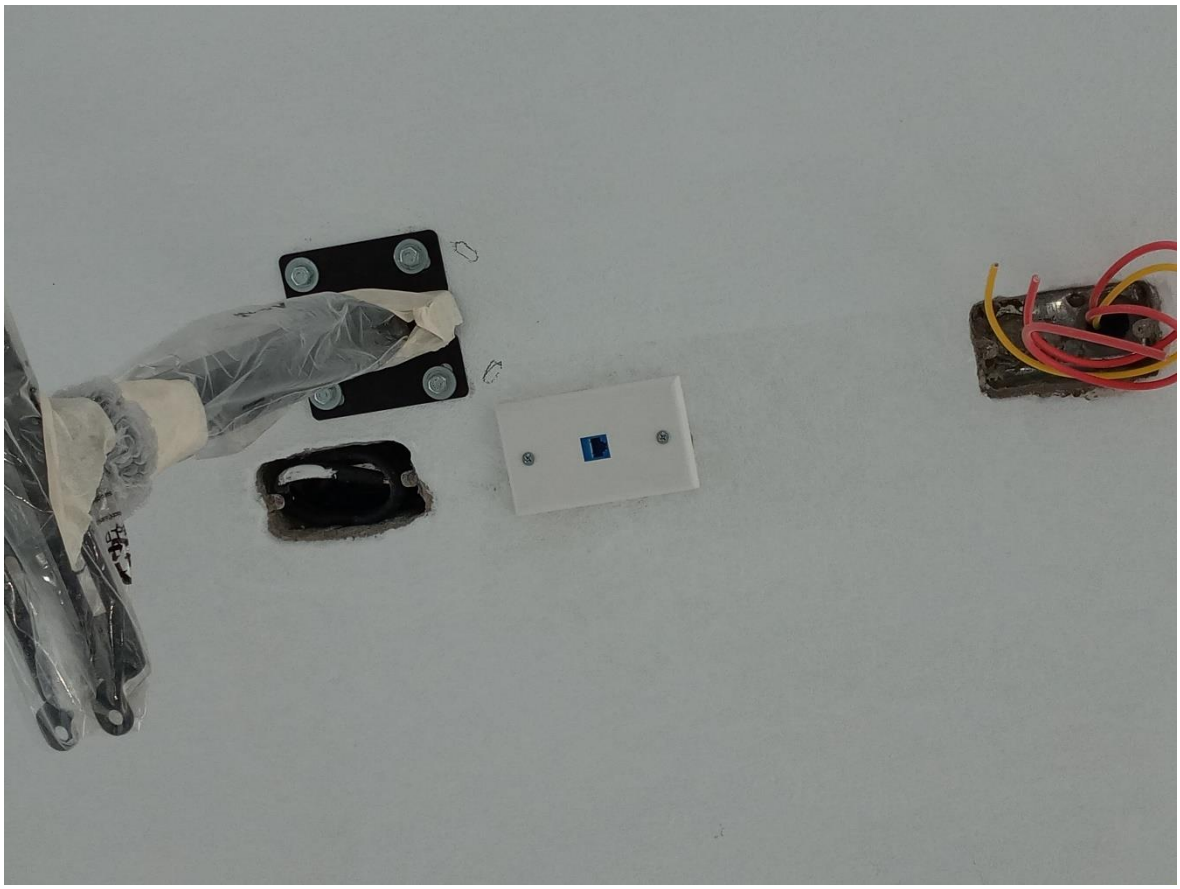
- Acabado Pintura en polvo electrostático de 70 a 80 micras,
- color negro texturizado.
- Espesor de la estructura 1.2mm.
- Ventilación Kit de 2 ventiladores.
- Entrada de cable (orificio 7.8 cm diámetro).
- Seguridad 2 chapas (1 puerta y 1 marco).
- 2 llaves.

Distribución de Gabinetes:

- Módulo 1b: Tutoría: Gabinete de pared de 6 RU.
- Módulo 1A: Sin construir.
- Módulo 2: Laboratorio de cómputo: gabinete de piso de 44RU (Data Center).
- Módulo 3: Gabinete de pared de 6 RU.
- Módulo 4: rack de pared de 6 RU.
- Módulo 5: Gabinete de pared de 6 RU.

Figura 35

Puntos de red en techos de aulas – VLAN proyectores



Fuente: Figura muestra punto de red en techo con previa canalización y cableado

PATCH PANEL:

-24 puertos modular CAT 6, Los patch panel SATRA están diseñados para cumplir y exceder las especificaciones de rendimiento exigidas por la norma ANSI/TIA-568 C.2, tanto para las categorías 5e, 6 y 6A. Asegure el máximo desempeño y logre una instalación sencilla con una terminación estandarizada tipo T568A/B en cumplimiento con la norma y realice el etiquetado de los puntos de red para una mejor administración de cableado.

- Patch Panel Categoría 6A Blindado:

- Paneles de parcheo con 24 RJ-45.

- Óptimo para Ethernet a 10Giga bit por segundo – 10GBase-T.

- Diseño modular para patch panel categoría 6A para transmisiones de datos superiores a 500MHZ.

- **PATCH CORD:** CAT 6 SATRA multifilar

- **Patch Cord S/FTP Categoría 6A LSZH**

- **BANDEJAS FIJAS: 1 RU**

- **SISTEMA DE VENTILACIÓN:** 2 ventiladores marca SATRA

- **POWER RACK:** 8 tomas universales

5to Proceso: Pruebas de calidad y control de conectividad

Pruebas de enlaces entre trocales de cada módulo y data center, pruebas de aulas con gabinetes

6to Proceso: Configuración de equipos de comunicaciones (Red)

Configuración de equipos VLAN:

- ROUTER: Se cuenta con 2 routers, uno del ISP y el otro en el laboratorio de cómputo. El cual, gerena VLAN para separar las redes del laboratorio de cómputo, aulas, cámaras ip y las áreas administrativas.

Figura 36

ROUTER TRENDNET TEW-829DRU/AC3000

Router wireless AC3000 tribanda Gigabit WAN dual VPN SMB

TEW-829DRU (Version v1.0R)

- Los puertos WAN dual admiten modos de balance de carga y fail-over
- 8 puertos gigabit LAN, 1 puerto de consola
- Admite SSL, IPsec, PPTP y L2TP con IPsec para VPN
- Enrutamiento IEEE 802.1Q inter-VLAN
- Las tres bandas WiFi concurrentes maximizan las velocidades de trabajo en red de los dispositivos
- Tribanda AC3000: Bandas 1733Mbps (5GHz1) + 867Mbps (5GHz2) + 400Mbps (2.4GHz)
- WiFi preencriptado para ofrecerle la mayor comodidad
- Aislamiento de cliente wireless
- Administración por navegador web y CLI
- Notificación de firmware y actualización por Internet
- QoS para aplicaciones de VoIP y difusión continua de contenidos audiovisuales
- Servicio avanzado de filtrado de contenidos web por Router Limits™

Fuente: Figura muestra el Router AC3000, para generar la administración de VLAN

- SWICHT: El gabinete del laboratorio de cómputo cuenta con 1 switch administrable para generar VLAN, garantizando la seguridad de los datos y separación de broadcast en la red., 01 switch POE, 5 switch de 24 puertos no administrables capa 2 para la conectividad de los 2 host del laboratorio de cómputo, áreas administrativas.

En los módulos 1b, módulo 3, modulo 4 y módulo 5 cuenta con 01 switch administrable de 16 puertos y 1 switch de 16 puertos no administrables capa 2.

Smart Switch Gbe 16puertos Trendnet Teg-204ws 4sfp- Rackeable

Figura 37

Switch administrable

Fuente: Figura muestra el switch administrable instalado en cada gabinete

Router ISP: Web filtering

El filtro de páginas web se realiza por categorías y subcategorías que son actualizadas de manera automática con los servicios de Fortiguard y pueden revisar el origen de las categorías de las urls desde la siguiente página web: http://fortiguard.com/webfilter

Se recomienda que se nombre el grupo de webfiltering igual al del grupo que se le aplicara el perfil y además podremos agregar excepciones si una web está contenida dentro de una categoría. Revisar las pestañas de Perfiles de seguridad.

Figura 38

Grupo de webfiltering

Grupo	Call Center	Gerencia	Servidores
IPs/rango/Subred	192.168.168.1.0/24	192.168.2.10, 192.168.2.11	192.168.2.50-192.168.2.60
Puertos / Servicios	TCP/UDP 80, 443, 53	ALL	ALL
Garantizado / Max Mbps	10 / 15	5 / 15	6 / 20
AV	-	-	SI
Web Filtering	Call Center	Gerencia	Servidores

Fuente: Elaboración propia. Grupo de webfiltering.

Figura 39

Categorías para el filtro de páginas web

CATEGORIAS BLOQUEO DE PAGINAS URL: ASOCIACION CIVIL EDUACTIVA SACO OLIVEROS				
ISP: OPTICAL NETWORD		GENERAL(Ejemplo)	Grupo_2	Grupo_
	MARCAR CON X PARA BLOQUEAR		Secretarias / Computo	Directo
Filtro de Aplicaciones	Skype			
	P2P	X		
	Game	X	X	x
	Update	X	X	x
	Social Networking			
	Media (audio/video)	X	X	
	MARCAR CON X PARA BLOQUEAR			
Filtro Web	**Potentially Liable**		X	X
	Child Abuse	x	X	X
	Discrimination	X	X	X
	Hacking	X	X	X
	Proxy Avoidance	X	X	X
	Adult/Mature Content	X		
	Pornography	X	X	x
	Sex Education	X		
	Freeware and Software Downloads	X		
	Internet Radio and TV	X	X	
	Peer-to-peer File Sharing	X		
	Streaming Media and Download		X	

Fuente: Formato ISP Optical. categorías para el filtro de páginas web

7mo Proceso: Instalación de quipos informáticos
Instalación y configuración de equipos información en diversas áreas

- **Access point:** En recepción, áreas administrativas, biblioteca.
- **Proyector Epson** PowerLite x39: LAN – RJ45 x 1 (10/100)
- **PC:** Las computadoras cuentan con tarjeta de red integrada Chip Realtek® GbE LAN LAN (10/100/1000 Mbit):

Cantidades: la sede de Saco Oliveros Monterrico cuenta con 60 computadoras en los laboratorios de cómputo, 11 computadoras en el área administrativas. 31computadoras en las aulas del nivel primaria y secundaria

- **Camaras IP:** Se habilitaron 21 puntos de red para instalación de cámaras IP.

- **MARCADOR DE ASISTENCIA:** Terminal multi biométrica para control de asistencia y acceso con reconocimiento facial en luz visible. Modelo G4 ZKTECO que es administrado por BioTime 7.0. Con sensor de huella, pantalla táctil y cámara binocular.

Para cubrir nuestro primer objetivo de investigación usaremos el domino 13, objetivo de control 13.1 y del control 13.1.2.

Determinar de qué manera influye el diseño e implementación de una red de seguridad informática para mejorar la administración de datos en la empresa A.C.E Saco Oliveros - Sede Monterrico. Lima 2021

Tabla 9

Dominio 13, objetivos 13.1, control alineado a la investigación 13.1.2

ISO/IEC 27002/2013	No	Descripción
Dominio	13	SEGURIDAD EN LAS TELECOMUNICACIONES.
Adjetivos de Control	13.1	Gestión de la seguridad en las redes.
	13.1.1	Control de red.
Controles	13.1.2	Mecanismos de seguridad asociados a servicios en red.

Nota. Fuente: ISO/IEC 27002:2013. Dominio es aplicado para mecanismos de gestión en redes

Se deberían controlar los accesos a servicios internos y externos conectados en red.

El acceso de los usuarios a redes y servicios en red no debería comprometer la seguridad de los servicios en red si se garantizan:

a) que existen interfaces adecuadas entre la red de la Organización y las redes públicas o privadas de otras organizaciones.

b) que los mecanismos de autenticación adecuados se aplican a los usuarios y equipos.

c) el cumplimiento del control de los accesos de los usuarios a los servicios de información.

Mantenga el equilibrio entre controles de seguridad perimetrales (LAN/WAN) e internos (LAN/LAN), frente a controles de seguridad en aplicaciones (defensa en profundidad).

Prepare e implante estándares, directrices y procedimientos de seguridad técnicos para redes y herramientas de seguridad de red como IDS/IPS (detección y prevención de intrusiones), gestión de vulnerabilidades, etc.

Para cubrir nuestro segundo objetivo de investigación usaremos el domino 18, objetivo de control 18.1 y del control 18.1.3.

Identificar los niveles de protección de la Norma ISO27002:2013 en la empresa ACE Saco Oliveros.

Tabla 10

Dominio 18, objetivos 18.1, control alineado a la investigación 18.1.3

ISO/IEC 27002/2013	No	Descripción
Dominio	18	CUMPLIMIENTO
Adjetivos de Control	18.1	Cumplimiento de los requisitos legales y contractuales.
Controles	18.1.3	Protección de los registros de la organización.

Nota. Fuente: ISO/IEC 27002:2013. Dominio es aplicado el uso seguro y responsable de las TIC, según Ley 30254

Protección de los registros de la organización: Los registros se deberían proteger contra pérdidas, destrucción, falsificación, accesos y publicación no autorizados de acuerdo con los requisitos legislativos, normativos, contractuales y comerciales.

En el ANEXO n.° 3. Se indica la Ley N° 30254, Ley de Promoción para el uso seguro y responsable de las Tecnologías de la Información y Comunicaciones por Niños, Niñas y Adolescentes.

La ley tiene como objetivo el uso seguro y responsable de las tecnologías de información y comunicaciones (TIC), para proteger de los peligros en internet a los Niños, Niñas y Adolescentes. El estado peruano genera normas complementarias sobre el uso seguro y responsable de las TIC (Ley N° 30254).

Se implemento 02 alternativas de solución para cubrir con dicha Ley.

Primera. Servidor Firewall, gestionado por el área de Soporte Técnico.

Segunda. Servicio en la Nube propuesto por ISP Optical.

Para cubrir nuestro Quinto objetivo específico de investigación usaremos el domino 6, objetivo de control 6.1 y del control 6.1.5.

Determinar en qué medida el uso de la Administración de seguridad informática influye en la gestión de políticas de seguridad para recursos informáticos en la empresa ACE Saco Oliveros.

Tabla 11

Dominio 6, objetivos 6.1, control alineado a la investigación 6.1.5

ISO/IEC 27002/2013	No	Descripción
Dominio	6	ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACION.
Objetivos de Control	6.1	Organización interna.
Controles	6.1.5	Seguridad de la información en la gestión de proyectos.

Nota. Fuente: ISO/IEC 27002:2013. Dominio es aplicado la gestión de proyectos independientes o por terceros.

Se debería establecer una estructura de gestión con objeto de iniciar y controlar la implantación de la seguridad de la información dentro de la Organización.

Si fuera necesario, en la Organización se debería establecer y facilitar el acceso a una fuente especializada de consulta en seguridad de la información. Deberían desarrollarse contactos con especialistas externos en seguridad, que incluyan a las administraciones pertinentes, con objeto de mantenerse actualizado en las tendencias de la industria, la evolución de las normas y los métodos de evaluación, así como proporcionar enlaces adecuados para el tratamiento de las incidencias de seguridad.

Debería fomentarse un enfoque multidisciplinario de la seguridad de la información, que, por ejemplo, implique la cooperación y la colaboración de directores, usuarios, administradores, diseñadores de aplicaciones, auditores y el equipo de seguridad con expertos en áreas como la gestión de seguros y la gestión de riesgos.

6.1.5 Seguridad de la información en la gestión de proyectos: Se debería contemplar la seguridad de la información en la gestión de proyectos e independientemente del tipo de proyecto a desarrollar por la organización.

Como la norma indica la institución Saco oliveros dispone de un área de Soporte técnico actualmente para el desarrollo de proyectos en la seguridad informática.

Actualmente contamos con 12 profesionales especiales en Redes y comunicaciones, profesionales en electrónica y computación.

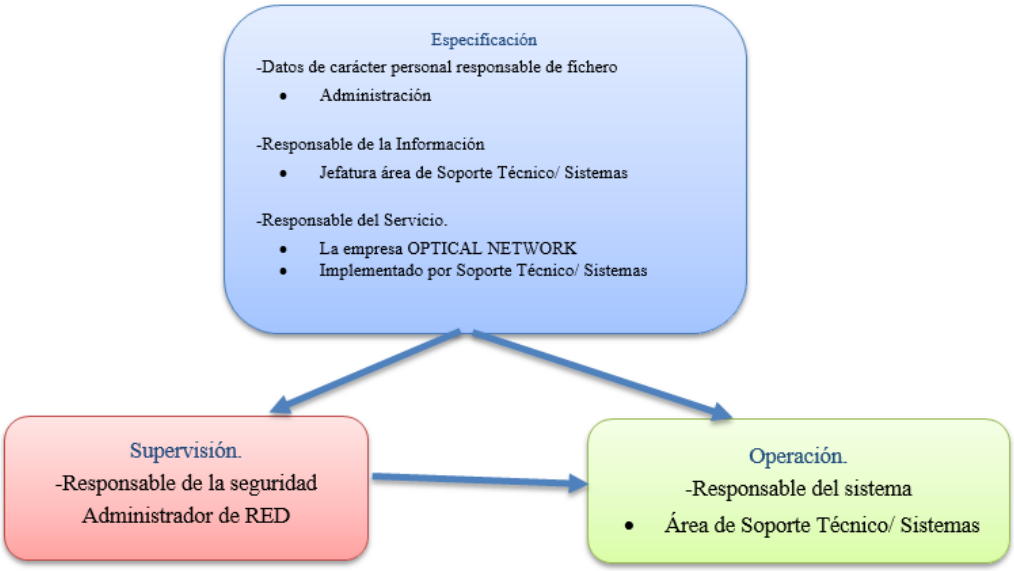
Para cubrir las 40 sedes y brindar la seguridad informática requerida. El personal es distribuido por zonas para velar por la integridad de cada sede. La Empresa

OPTICAL NETWORK actualmente nos brinda capacitaciones en seguridad informática.

Con la ayuda de nuestra bibliográfica la estructura propuesta diferencia 3 bloques de responsabilidad

Figura 40

bloques de responsabilidad para la seguridad de la información.



Fuente: Elaboración Propia. La imagen ilustra áreas responsables para la seguridad de la información.

CAPÍTULO IV. RESULTADOS

Tabla 12

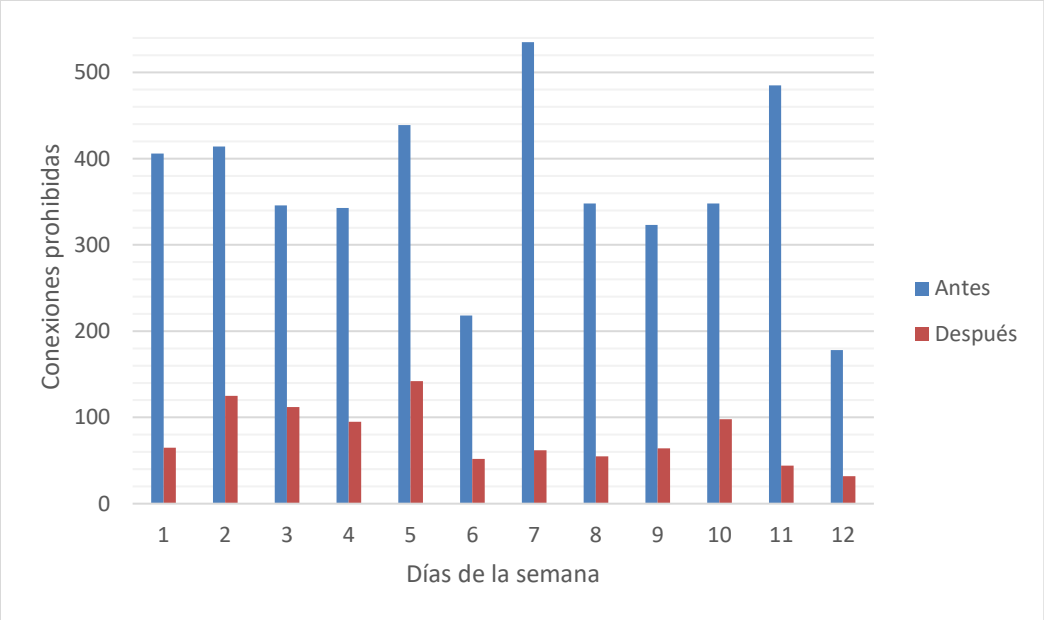
Comparación Antes – Después de la cantidad de páginas no autorizadas visitadas al día, de lunes a sábado durante 12 días.

Días de la semana	Antes	Después
Día 01	406	65
Día 02	414	125
Día 03	346	112
Día 04	343	95
Día 05	439	142
Día 06	218	52
Día 07	535	62
Día 08	348	55
Día 09	323	64
Día 10	348	98
Día 11	485	44
Día 12	178	32
TOTAL	4383	946

Nota. Fuente: Elaboracion propia.

Figura 41

Comparación de paginas no autorizadas



Fuente: Elaboración propia. Comparación Antes – Después de la cantidad de páginas no autorizadas visitadas al día lunes a sábado durante 12 días.

Como se puede apreciar se presenta una disminución total de hasta el 80% de visitas de páginas web no autorizadas. Esto se debe a las configuraciones de las ACL implementadas en el servidor proxy. Lo ideal sería una reducción del 100% pero hay excepciones a través de solicitudes y/o páginas que aún se han definido o agregado a la base de datos.

Tabla 13

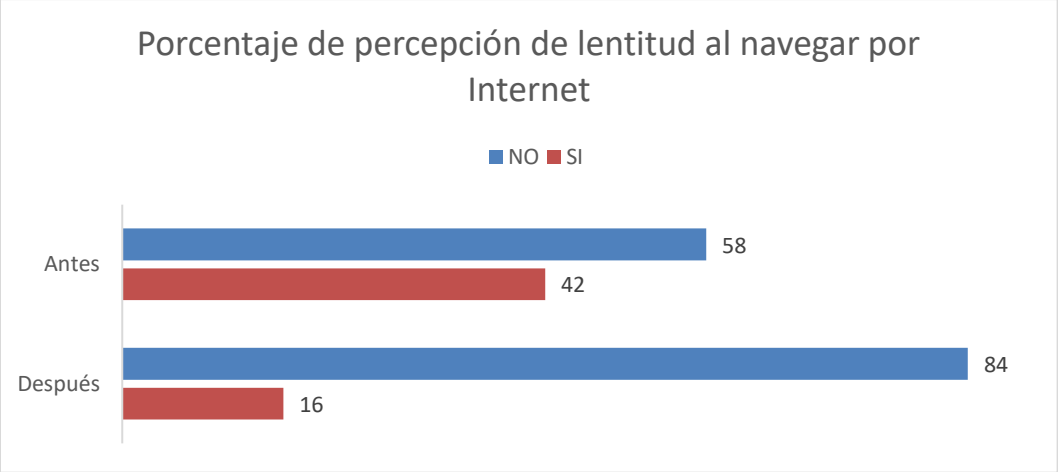
Comparación Antes – Después de la percepción de disminución de velocidad de navegación en Internet

Disminución de velocidad de Internet	Antes	Después
SI	42 %	16 %
NO	58 %	84 %

Nota. Fuente: Elaboracion propia.

Figura 42

Comparación velocidad de navegación



Fuente: Elaboración propia. Comparación Antes – Después de la percepción de disminución de velocidad de navegación en Internet.

Para el control se entrevistó a la misma persona encargada de enviar la documentación contable a las otras sedes y se le consultó su percepción de la velocidad de internet a lo largo de 2 semanas; dando como resultado una mejor percepción de la red a comparación del antes, dado que hay menos páginas visitadas

y existe menor carga en el tráfico de datos. Hay que tener en cuenta también que la percepción es algo subjetivo, pero a la vez sirve para mantener al usuario final satisfecho.

Tabla 14

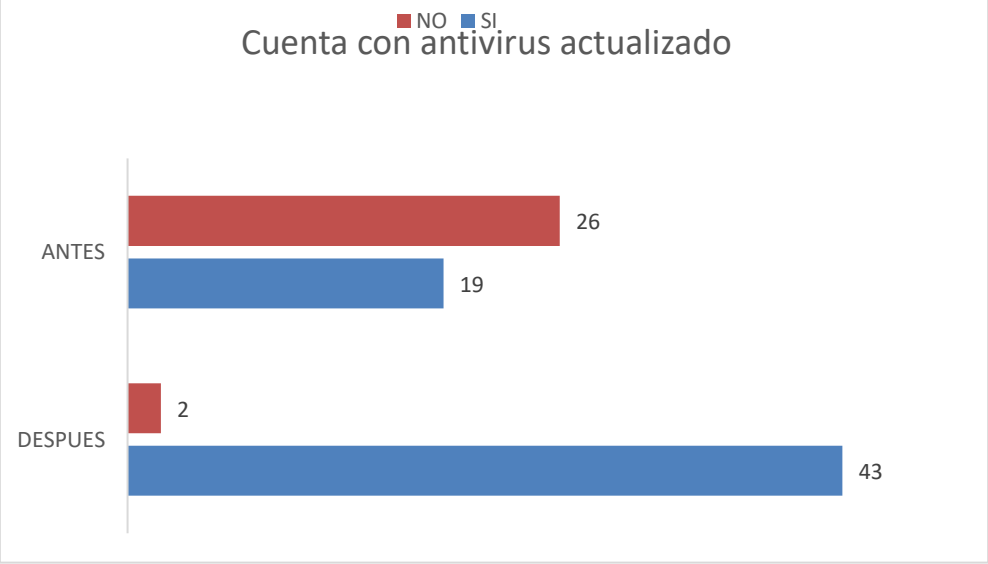
Comparación Antes – Después su equipo cuenta con antivirus actualizado.

		ANTES	DESPUES
SI		19	43
NO		26	2
	total	45	45

Nota. Fuente: Elaboracion propia.

Figura 43

Comparación análisis de antivirus



Fuente: Elaboración propia. Comparación Antes – Después su equipo cuenta con antivirus actualizado

De un total de 45 equipos se realizó el control, para definir y actualizar el antivirus, dando como resultado que luego de la implementación se lograron tener el 95% de los equipos con antivirus actualizado.

Tabla 15

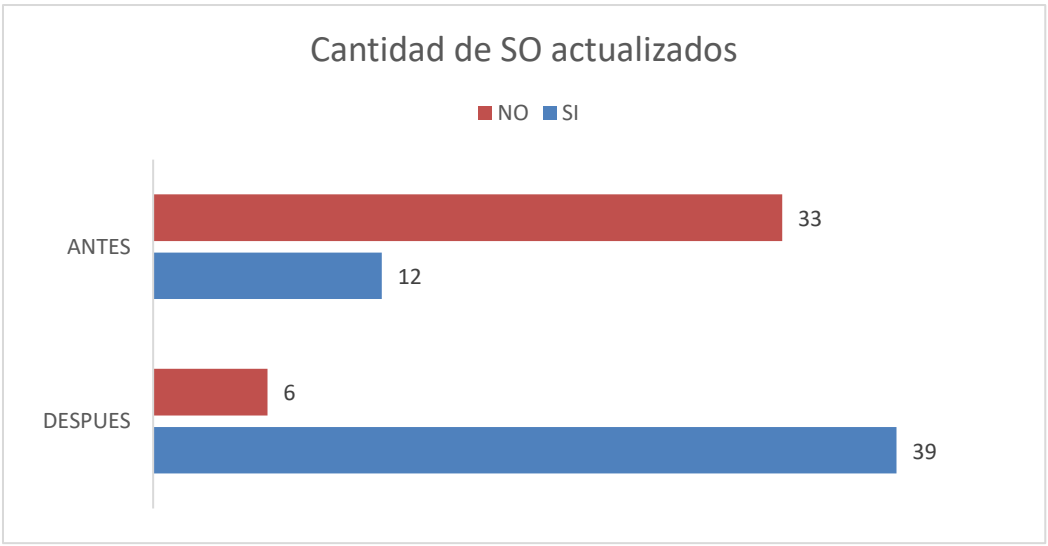
Comparación Antes – Después el sistema operativo de su equipo esta actualizado.

	ANTES	DESPUES
SI	12	39
NO	33	6

Nota. Fuente: Elaboracion propia.

Figura 44

Comparación análisis sistema operativo actualizado



Fuente: Elaboración propia. Comparación Antes – Después el sistema operativo de su equipo esta actualizado.

Se reactivó las actualizaciones automáticas en Windows para mantener el equipo actualizado y con la menor cantidad de vulnerabilidades posibles. Se planea implementar un servidor WSUS para aligerar el tráfico de la red.

Tabla 16

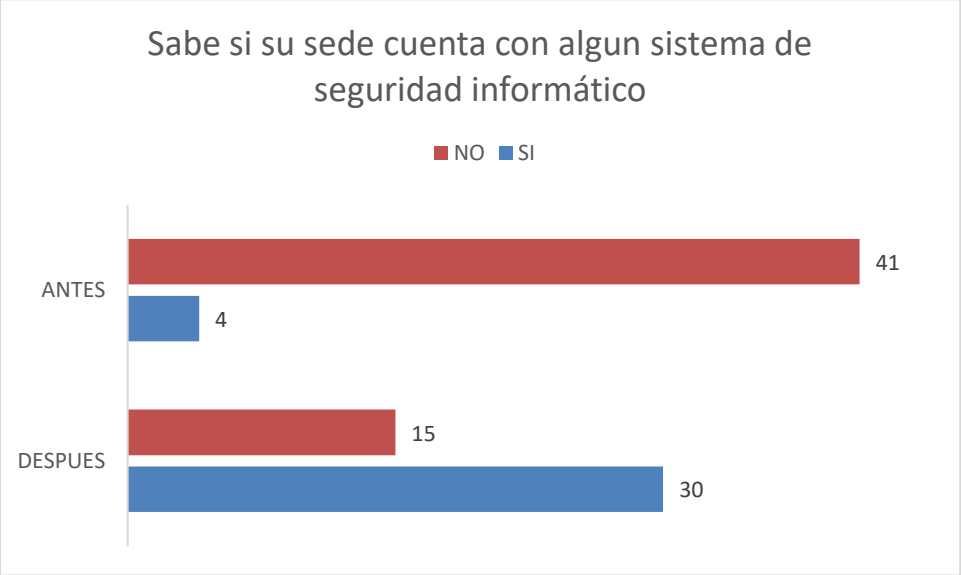
Comparación Antes – Después conocimiento si su equipo cuenta con un sistema de seguridad informático.

	DESPUES	ANTES
SI	30	4
NO	15	41

Nota. Fuente: Elaboracion propia.

Figura 45

Comparación sistema de seguridad informático



Fuente: Elaboración propia. Comparación Antes – Después conocimiento si su equipo cuenta con un sistema de seguridad informático.

Con la charla brindada a los colaboradores sobre la seguridad de la información se percibe que se logró concientizar a más del 67% de los usuarios y conocer más de las medias de control y seguridad.

Resultado y comparación de costos según controladores trabajados:

Propuesta del Proveedor OPTICAL NETWORK.

En el punto 1.5.2 Justificación Practica, se indica como propuesta la construcción de un servidor Firewall, para controlar la seguridad en la navegación de internet de las áreas administrativas y laboratorio de cómputo. El cual se indican los precios.

Tabla 17

Costo implementación de Firewall.

IMPLEMENTO	CARACTERISTICAS	COSTO UNI.($)	COSTO TOTAL($)
SOFTWARE	- LINUX	0	0
HARDWARE	- COMPUTADORA	0	0
	- D-LINK 10/100/1000	$15	$15
IMPLEMENTACION	- Bonos, Movilidad	$140	$140
TOTAL	40 Sedes	$155	$6200

Nota. Fuente: Elaboracion propia.

Tabla 18

Resultados comparación de costos.

	Tipo de implementación	Costo por 40 Sede	Costo Anual
Proveedor Optical Networks	Seguridad en la nube	$800 (Pago mensual)	$9600
Area Soporte Técnico	Firewall	$6200 (único pago)	$6200 (único pago)

Nota. Fuente: Elaboracion propia.

En la tabla comparación de costos se logra apreciar que existe una disminución de costo en la implementación de un servidor Firewall, en comparación del servicio que nos brindaría la empresa Optical Networks. Para brindar mayor seguridad de opto:

1ro. Brindar seguridad por segmentación por medio AC3000 gestionado por el personal de soporte Saco Oliveros

2do. La empresa Optical Networks gestionara por medio de la modalidad L2L contratado.

CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones

En la norma ISO 27002:2013 los controladores de seguridad aplicados en la administración de URL a la institución educativa Saco Oliveros, permitió escoger los controladores adecuados para la investigación.

Por tal motivo implementar herramientas o servicios que permitan administrar el flujo con el cual se accede a los servicios del Internet, permitirá tener un ambiente controlado al detalle de quienes intentan acceder a la información.

Se maximizo la producción del personal administrativo, ejecutan políticas de seguridad y se minimizo el consumo de internet, garantizando estabilidad en los sistemas web administrativos.

El servicio del ISP fue más costoso, en comparación a la implementación por el mismo personal de Soporte.

Es indispensable que la institución tenga un servidor de seguridad para garantizar la confidencialidad, integridad de nuestros alumnos y personal administrativos, con la aplicación de la norma ISO/IEC 27002.

5.2. Recomendaciones

Se debe continuar con las capacitaciones de uso y resguardo de la información relevante a todos los usuarios.

Gestionar 2 servicio de internet para garantizar la estabilidad del servicio que se brinda con las clases hibridas – semipresenciales.

Replicar trabajos de implementación de Redes de comunicación administradas a sus demás sedes (39 sedes).

REFERENCIAS

Abad Domingo, A., & E-libro, C. (2013). *Redes locales.* McGraw-Hill Espaa.

Abad Domingo y E-libro—2013—Redes locales..pdf. (s. f.). Recuperado 13 de marzo de 2022, de https://d1wqtxts1xzle7.cloudfront.net/44956517/2Redes_Locales-with-cover-page-v2.pdf?Expires=1647225304&Signature=YyavVaqr0wmsU3GoIa710wCCwHs2iNUSyr6kgq0Ql7L4v5xRAfG3XKigc2Tp97A2d-RmNvFqnyEsmODtmtM583klIZdozlTJbKTcPO~mrv5jWPkm8QxDSiu08Zl9g-v7KWs~NhJ5A8JpdQUam~Xvm1KT6Y6gmu~5SKuxiXqrieMJO4M2vywZ~E4wfIrawOn50qr49LHsBjKYaHn-E-rkKEYp9LN4Gyv30r7KXT7RITrgIG4hTZEikOpMSo5WzqvKVPOAkbiKZ8qsCeoCqfr5D3mlj4QQNdttkPnQwko7moK7coor-ZSKoXvS5OvTr~n9VhG5RdGay4t697oozw~~CA__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA

Barcell, M. F. (s. f.). *DEPARTAMENTO DE INGENIERÍA INFORMÁTICA*. 25.

Cables de Cobre U/FTP Sólido Categoría 6A - Satra Perú. (2021, julio 5). https://satranet.com/cables-de-cobre-u-ftp-solido-categoria-6a/, https://satranet.com/cables-de-cobre-u-ftp-solido-categoria-6a/

Cables de Cobre U/UTP CM Sólido Categoría 6—Satra Perú. (2021, julio 5). https://satranet.com/cables-de-cobre-u-utp-cm-solido-categoria-6/, https://satranet.com/cables-de-cobre-u-utp-cm-solido-categoria-6/

Figueroa Leyton, J. L. (2019). *Plan de seguridad informática basado en la norma ISO 27002 y la gestión de la información para el departamento de TIC de la Uniandes extensión Babahoyo*. https://dspace.uniandes.edu.ec/handle/123456789/9751

Mosquera, V., & Celestino, E. (2017). DISEÑO E IMPLEMENTACIÓN DE UN SGSI ISO 27001 PARA LA MEJORA DE LA SEGURIDAD DEL AREA DE RECURSOS HUMANOS DE LA EMPRESA GEOSURVEY DE LA CIUDAD DE LIMA. *Universidad de Huánuco*. http://localhost:8080/xmlui/handle/123456789/809

Ramos, Y., Urrutia, O., Bravo, A., & Ordoñez, D. (2017). Adoptar una política de seguridad de la información basados en un dominio del estándar NTC ISO/IEC 27002:2013 para la Cooperativa Codelcauca. *Memorias de Congresos UTP; 2017: 4to Congreso Internacional AmITIC 2017, Aplicando nuevas tecnologías; 88-95*, 8.

Ribes, R. J. C. (2013). *Redes locales*. Macmillan Iberia, S.A. https://elibro.bibliotecaupn.elogim.com/es/ereader/upnorte/43257

Ruano Chinguercela, D. F. (2016). *Propuesta de implementación de calidad de servicio (QOS) en redes locales virtuales (VLAN) mediante las normas 802.1d y 802.1q. Aplicado a la empresa Sinergy Hard*. http://repositorio.puce.edu.ec:80/xmlui/handle/22000/13150

Sep_art51.pdf. (s. f.). Recuperado 13 de marzo de 2022, de https://www.ru.tic.unam.mx/bitstream/handle/123456789/791/sep_art51.pdf?sequence=1

Tullume Ramos, L. M. (2017). *Propuesta de Mejora Basada en la Creación de Redes Virtuales (VLAN) para Optimizar La Administración de la Red de la Sede Central del Fondo de Cooperación y Desarrollo Social (FONCODES)*. http://repositorio.untels.edu.pe//handle/123456789/268

ANEXOS

ANEXO n.° 1. Ley N° 30254, Ley de Promoción para el uso seguro y responsable de las Tecnologías de la Información y Comunicaciones por Niños, Niñas y Adolescentes

DIARIO OFICIAL DEL BICENTENARIO

El Peruano

FUNDADO EL 22 DE OCTUBRE DE 1825 POR EL LIBERTADOR SIMÓN BOLÍVAR

Aprueban el Reglamento de la Ley N° 30254, Ley de Promoción para el uso seguro y responsable de las Tecnologías de la Información y Comunicaciones por Niños, Niñas y Adolescentes

DECRETO SUPREMO

N° 093-2019-PCM

EL PRESIDENTE DE LA REPÚBLICA

CONSIDERANDO:

Que, el artículo 1 de la Ley N° 30254, Ley de Promoción para el uso seguro y responsable de las Tecnologías de la Información y Comunicaciones por Niños, Niñas y Adolescentes, precisa que la citada Ley tiene por objeto promover el uso seguro y responsable de las tecnologías de la información y comunicaciones (TIC) por niños, niñas y adolescentes para protegerlos de los peligros del mal uso del acceso al Internet, para lo cual el Estado, en sus tres niveles de gobierno, genera normas complementarias sobre el uso seguro y responsable de las TIC, con especial atención al uso que realizan los niños, niñas y adolescentes;
Que, la Única Disposición Complementaria Final de la Ley N° 30254 dispone que el Poder Ejecutivo, a través de la Presidencia del Consejo de Ministros, reglamentará la Ley;

Que, de conformidad con el Reglamento que establece disposiciones relativas a la publicidad, publicación de proyectos normativos y difusión de normas legales de carácter general aprobado por Decreto Supremo N° 001-2009-JUS, mediante Resolución Ministerial N° 246-2015-PCM, se dispuso la publicación del proyecto de Reglamento de la Ley N° 30254, Ley de Promoción para el uso seguro y responsable de las Tecnologías de la Información y Comunicaciones por Niños, Niñas y Adolescentes y su exposición de motivos, otorgando un plazo de treinta (30) días calendario contados a partir del día siguiente de su publicación, a efectos de recibir las sugerencias de la ciudadanía en general;

Que, habiéndose procesado los comentarios recibidos, resulta necesario aprobar el Reglamento de la Ley N° 30254, Ley de Promoción para el uso seguro y responsable de las Tecnologías de la Información y Comunicación por Niños, Niñas y Adolescentes, para su correcta y oportuna implementación;

De conformidad con lo establecido en el numeral 8) del artículo 118 de la Constitución Política del Perú; en el numeral 3) del artículo 11 de la Ley N° 29158, Ley Orgánica del Poder Ejecutivo; y, en la Única Disposición Complementaria Final de la Ley N° 30254, Ley de Promoción para el uso seguro y responsable de las Tecnologías de la Información y Comunicaciones por Niños, Niñas y Adolescentes;

DECRETA:

Artículo 1.- Aprobación
Apruébase el Reglamento de la Ley N° 30254, Ley de Promoción para el uso seguro y responsable de las Tecnologías de la Información y Comunicaciones por Niños, Niñas y Adolescentes, que consta de tres (03) Títulos, diez (10) Artículos, y Tres (03) Disposiciones Complementarias Finales, cuyo texto forma parte integrante del presente Decreto Supremo.

Fuente: Diario el Peruano

ANEXO n.° 2. Dominio y Controles del ISO/IEC 27002:2013

ISO/IEC 27002:2013. 14 DOMINIOS, 35 OBJETIVOS DE CONTROL Y 114 CONTROLES

5. POLÍTICAS DE SEGURIDAD.
- 5.1 Directrices de la Dirección en seguridad de la información.
  - 5.1.1 Conjunto de políticas para la seguridad de la información.
  - 5.1.2 Revisión de las políticas para la seguridad de la información.

6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.
- 6.1 Organización interna.
  - 6.1.1 Asignación de responsabilidades para la segur. de la información.
  - 6.1.2 Segregación de tareas.
  - 6.1.3 Contacto con las autoridades.
  - 6.1.4 Contacto con grupos de interés especial.
  - 6.1.5 Seguridad de la información en la gestión de proyectos.
- 6.2 Dispositivos para movilidad y teletrabajo.
  - 6.2.1 Política de uso de dispositivos para movilidad.
  - 6.2.2 Teletrabajo.

7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.
- 7.1 Antes de la contratación.
  - 7.1.1 Investigación de antecedentes.
  - 7.1.2 Términos y condiciones de contratación.
- 7.2 Durante la contratación.
  - 7.2.1 Responsabilidades de gestión.
  - 7.2.2 Concienciación, educación y capacitación en segur. de la informac.
  - 7.2.3 Proceso disciplinario.
- 7.3 Cese o cambio de puesto de trabajo.
  - 7.3.1 Cese o cambio de puesto de trabajo.

8. GESTIÓN DE ACTIVOS.
- 8.1 Responsabilidad sobre los activos.
  - 8.1.1 Inventario de activos.
  - 8.1.2 Propiedad de los activos.
  - 8.1.3 Uso aceptable de los activos.
  - 8.1.4 Devolución de activos.
- 8.2 Clasificación de la información.
  - 8.2.1 Directrices de clasificación.
  - 8.2.2 Etiquetado y manipulado de la información.
  - 8.2.3 Manipulación de activos.
- 8.3 Manejo de los soportes de almacenamiento.
  - 8.3.1 Gestión de soportes extraíbles.
  - 8.3.2 Eliminación de soportes.
  - 8.3.3 Soportes físicos en tránsito.

9. CONTROL DE ACCESOS.
- 9.1 Requisitos de negocio para el control de accesos.
  - 9.1.1 Política de control de accesos.
  - 9.1.2 Control de acceso a las redes y servicios asociados.
- 9.2 Gestión de acceso de usuario.
  - 9.2.1 Gestión de altas/bajas en el registro de usuarios.
  - 9.2.2 Gestión de los derechos de acceso asignados a usuarios.
  - 9.2.3 Gestión de los derechos de acceso con privilegios especiales.
  - 9.2.4 Gestión de información confidencial de autenticación de usuarios.
  - 9.2.5 Revisión de los derechos de acceso de los usuarios.
  - 9.2.6 Retirada o adaptación de los derechos de acceso
- 9.3 Responsabilidades del usuario.
  - 9.3.1 Uso de información confidencial para la autenticación.
- 9.4 Control de acceso a sistemas y aplicaciones.
  - 9.4.1 Restricción del acceso a la información.
  - 9.4.2 Procedimientos seguros de inicio de sesión.
  - 9.4.3 Gestión de contraseñas de usuario.
  - 9.4.4 Uso de herramientas de administración de sistemas.
  - 9.4.5 Control de acceso al código fuente de los programas.

10. CIFRADO.
- 10.1 Controles criptográficos.
  - 10.1.1 Política de uso de los controles criptográficos.
  - 10.1.2 Gestión de claves.

11. SEGURIDAD FÍSICA Y AMBIENTAL.
- 11.1 Áreas seguras.
  - 11.1.1 Perímetro de seguridad física.
  - 11.1.2 Controles físicos de entrada.
  - 11.1.3 Seguridad de oficinas, despachos y recursos.
  - 11.1.4 Protección contra las amenazas externas y ambientales.
  - 11.1.5 El trabajo en áreas seguras.
  - 11.1.6 Áreas de acceso público, carga y descarga.
- 11.2 Seguridad de los equipos.
  - 11.2.1 Emplazamiento y protección de equipos.
  - 11.2.2 Instalaciones de suministro.
  - 11.2.3 Seguridad del cableado.
  - 11.2.4 Mantenimiento de los equipos.
  - 11.2.5 Salida de activos fuera de las dependencias de la empresa.
  - 11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.
  - 11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.
  - 11.2.8 Equipo informático de usuario desatendido.
  - 11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.

12. SEGURIDAD EN LA OPERATIVA.
- 12.1 Responsabilidades y procedimientos de operación.
  - 12.1.1 Documentación de procedimientos de operación.
  - 12.1.2 Gestión de cambios.
  - 12.1.3 Gestión de capacidades.
  - 12.1.4 Separación de entornos de desarrollo, prueba y producción.
- 12.2 Protección contra código malicioso.
  - 12.2.1 Controles contra el código malicioso.
- 12.3 Copias de seguridad.
  - 12.3.1 Copias de seguridad de la información.
- 12.4 Registro de actividad y supervisión.
  - 12.4.1 Registro y gestión de eventos de actividad.
  - 12.4.2 Protección de los registros de información.
  - 12.4.3 Registros de actividad del administrador y operador del sistema.
  - 12.4.4 Sincronización de relojes.
- 12.5 Control del software en explotación.
  - 12.5.1 Instalación del software en sistemas en producción.
- 12.6 Gestión de la vulnerabilidad técnica.
  - 12.6.1 Gestión de las vulnerabilidades técnicas.
  - 12.6.2 Restricciones en la instalación de software.
- 12.7 Consideraciones de las auditorías de los sistemas de información.
  - 12.7.1 Controles de auditoría de los sistemas de información.

13. SEGURIDAD EN LAS TELECOMUNICACIONES.
- 13.1 Gestión de la seguridad en las redes.
  - 13.1.1 Controles de red.
  - 13.1.2 Mecanismos de seguridad asociados a servicios en red.
  - 13.1.3 Segregación de redes.
- 13.2 Intercambio de información con partes externas.
  - 13.2.1 Políticas y procedimientos de intercambio de información.
  - 13.2.2 Acuerdos de intercambio.
  - 13.2.3 Mensajería electrónica.
  - 13.2.4 Acuerdos de confidencialidad y secreto.

ISO27002.es PATROCINADO POR:

GES CONSULTOR
GOBIERNO T.I. - RIESGO - CUMPLIMIENTO

14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.
- 14.1 Requisitos de seguridad de los sistemas de información.
  - 14.1.1 Análisis y especificación de los requisitos de seguridad.
  - 14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.
  - 14.1.3 Protección de las transacciones por redes telemáticas.
- 14.2 Seguridad en los procesos de desarrollo y soporte.
  - 14.2.1 Política de desarrollo seguro de software.
  - 14.2.2 Procedimientos de control de cambios en los sistemas.
  - 14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
  - 14.2.4 Restricciones a los cambios en los paquetes de software.
  - 14.2.5 Uso de principios de ingeniería en protección de sistemas.
  - 14.2.6 Seguridad en entornos de desarrollo.
  - 14.2.7 Externalización del desarrollo de software.
  - 14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.
  - 14.2.9 Pruebas de aceptación.
- 14.3 Datos de prueba.
  - 14.3.1 Protección de los datos utilizados en pruebas.

15. RELACIONES CON SUMINISTRADORES.
- 15.1 Seguridad de la información en las relaciones con suministradores.
  - 15.1.1 Política de seguridad de la información para suministradores.
  - 15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.
  - 15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.
- 15.2 Gestión de la prestación del servicio por suministradores.
  - 15.2.1 Supervisión y revisión de los servicios prestados por terceros.
  - 15.2.2 Gestión de cambios en los servicios prestados por terceros.

16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.
- 16.1 Gestión de incidentes de seguridad de la información y mejoras.
  - 16.1.1 Responsabilidades y procedimientos.
  - 16.1.2 Notificación de los eventos de seguridad de la información.
  - 16.1.3 Notificación de puntos débiles de la seguridad.
  - 16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.
  - 16.1.5 Respuesta a los incidentes de seguridad.
  - 16.1.6 Aprendizaje de los incidentes de seguridad de la información.
  - 16.1.7 Recopilación de evidencias.

17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.
- 17.1 Continuidad de la seguridad de la información.
  - 17.1.1 Planificación de la continuidad de la seguridad de la información.
  - 17.1.2 Implantación de la continuidad de la seguridad de la información.
  - 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.
- 17.2 Redundancias.
  - 17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.

18. CUMPLIMIENTO.
- 18.1 Cumplimiento de los requisitos legales y contractuales.
  - 18.1.1 Identificación de la legislación aplicable.
  - 18.1.2 Derechos de propiedad intelectual (DPI).
  - 18.1.3 Protección de los registros de la organización.
  - 18.1.4 Protección de datos y privacidad de la información personal.
  - 18.1.5 Regulación de los controles criptográficos.
- 18.2 Revisiones de la seguridad de la información.
  - 18.2.1 Revisión independiente de la seguridad de la información.
  - 18.2.2 Cumplimiento de las políticas y normas de seguridad.
  - 18.2.3 Comprobación del cumplimiento.

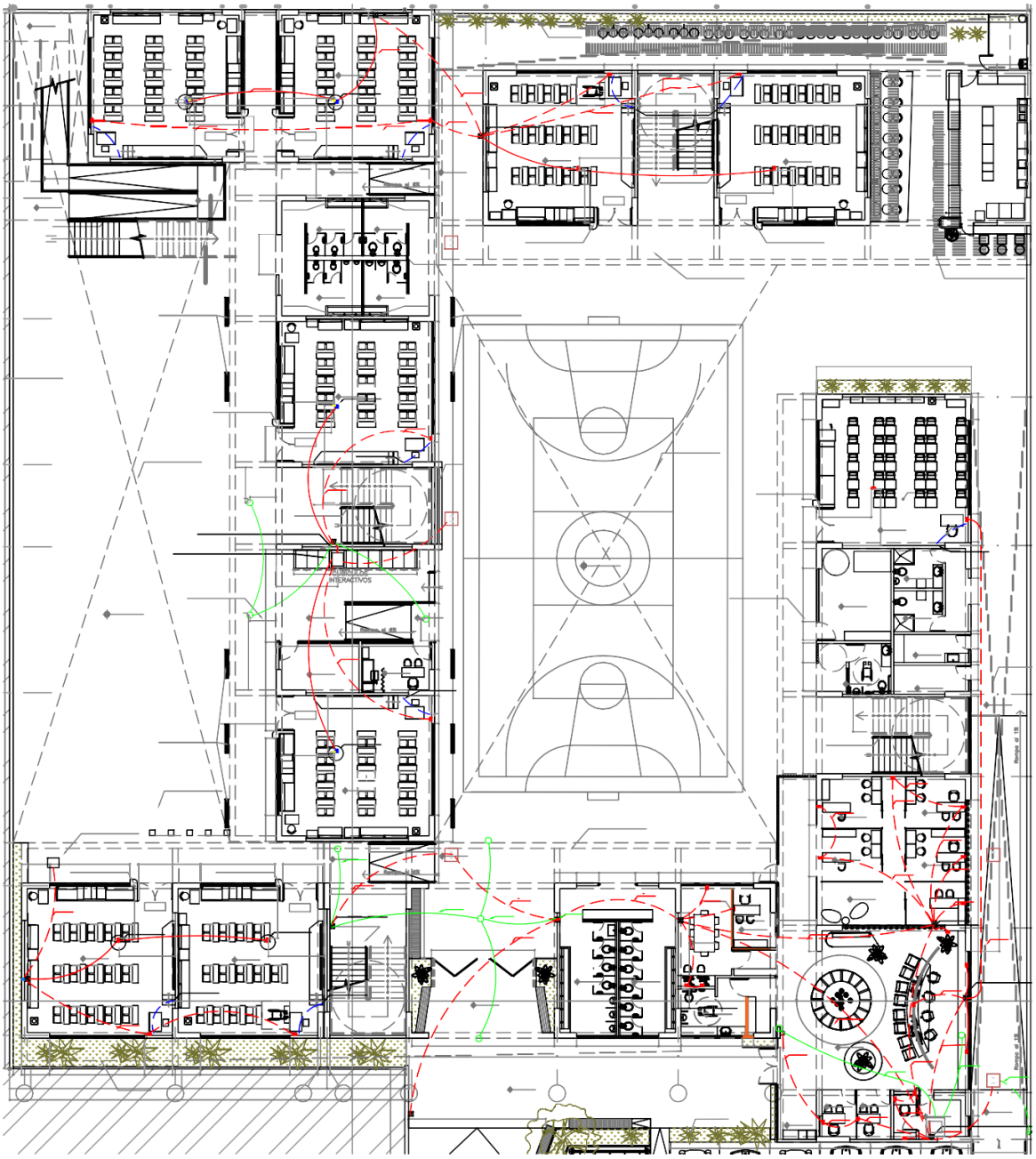
ISO27000

Iso27000.es: Documento sólo para uso didáctico. La norma oficial debe adquirirse en las entidades autorizadas para su venta.

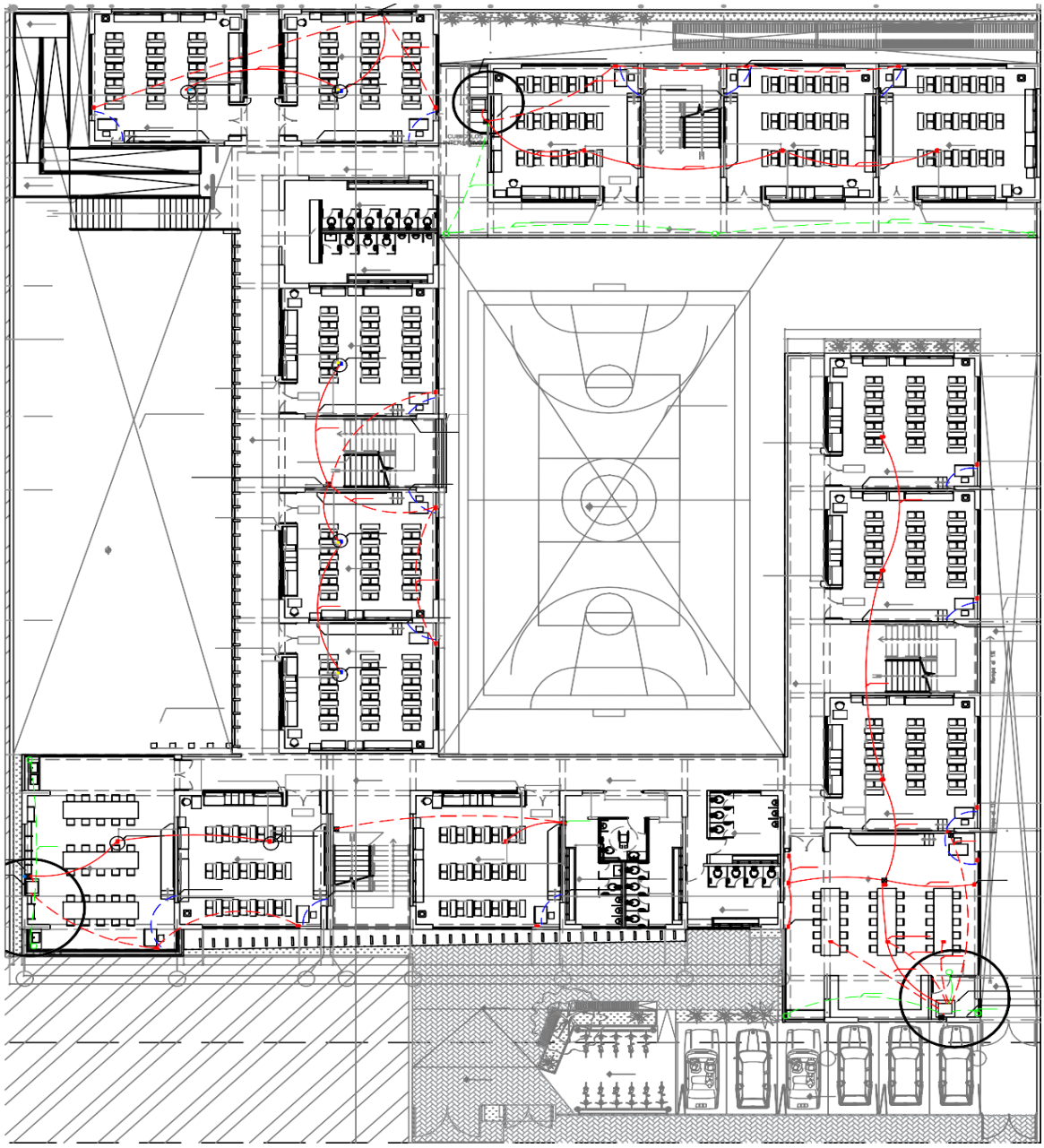
Octubre-2013

Fuente: ISO27002:2013

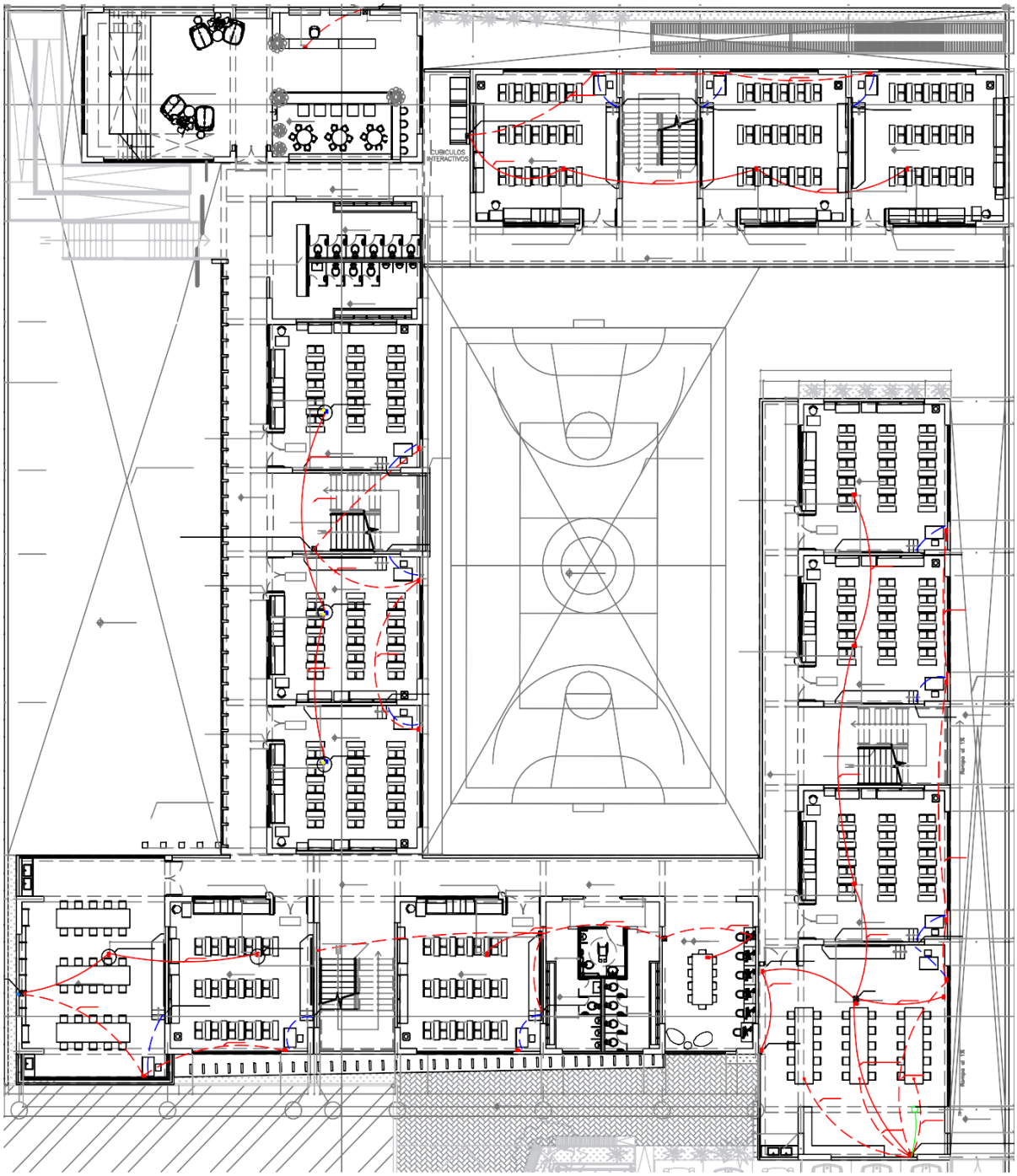
ANEXO n.° 3. Plano 1er piso, canalización y conectividad de redes.



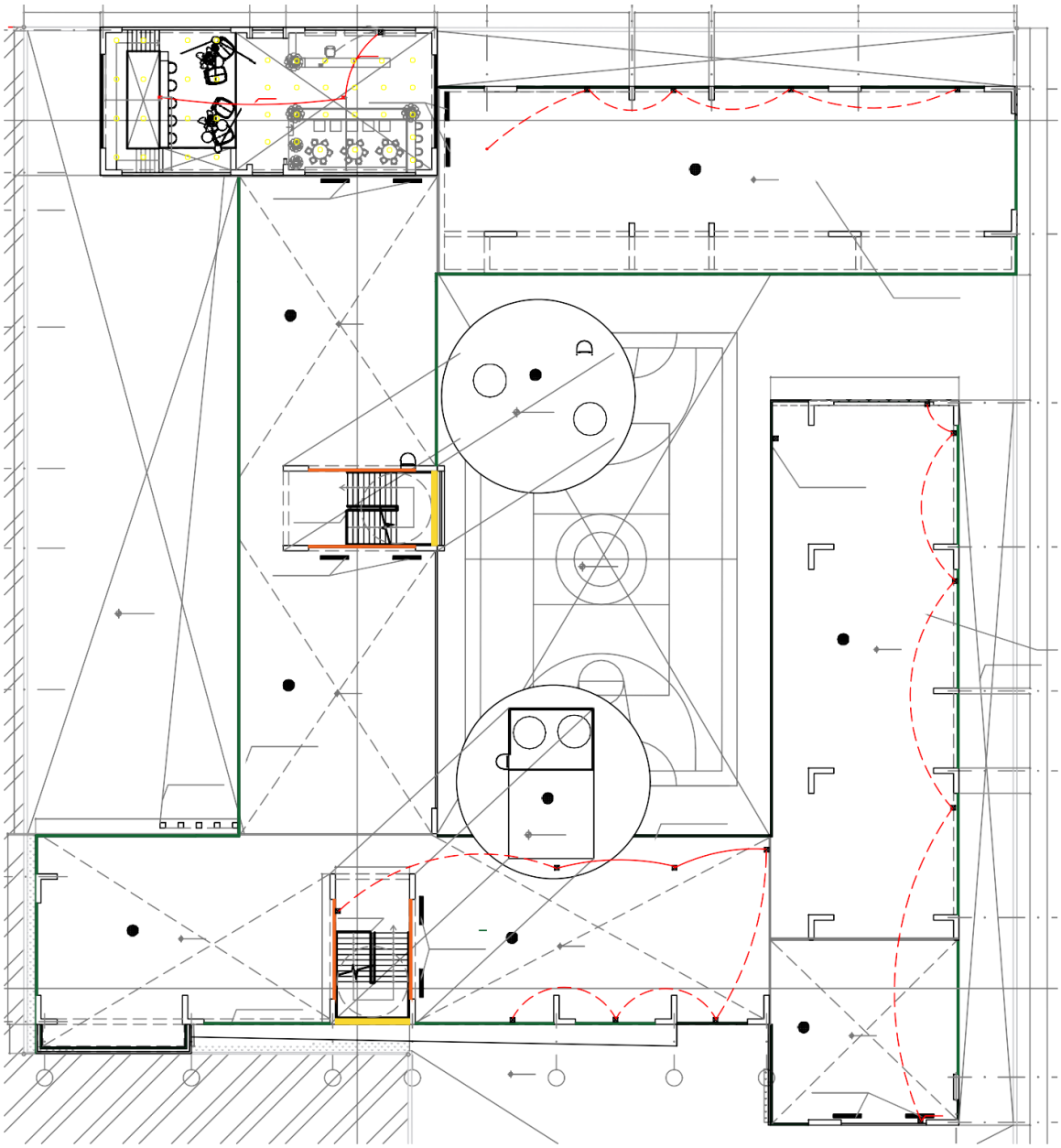
ANEXO n.° 4. Plano 2er piso, canalización y conectividad de redes.

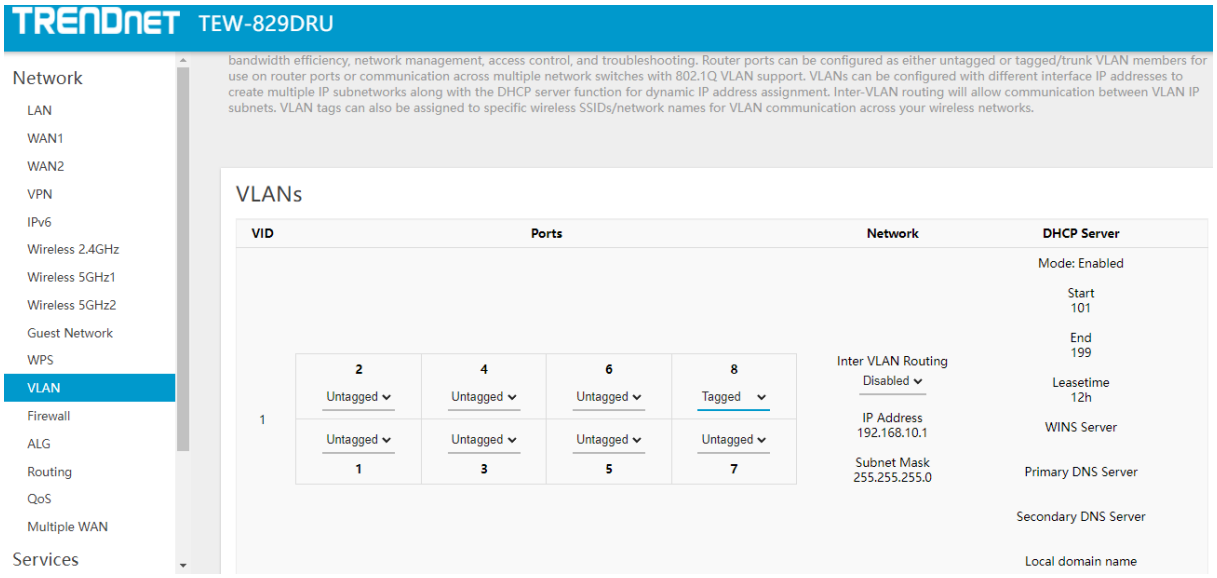


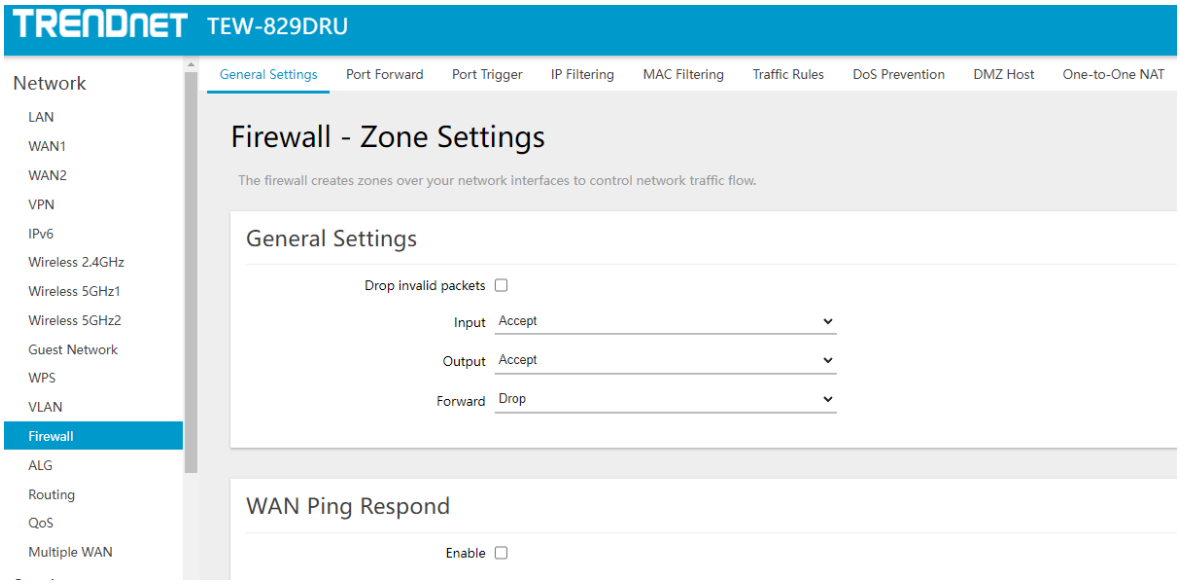
ANEXO n.° 5. Plano 3er piso, canalización y conectividad de redes.

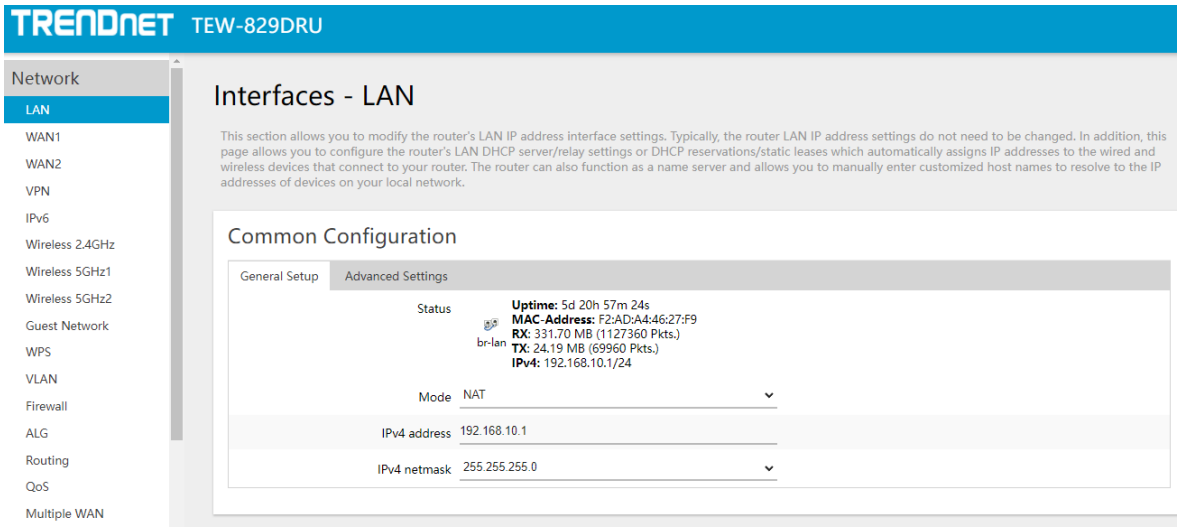


ANEXO n.° 6. Plano 4er piso, canalización y conectividad de redes.




TRENDNET TEW-829DRU
Network
LAN
WAN1
WAN2
VPN
IPv6
Wireless 2.4GHz
Wireless 5GHz1
Wireless 5GHz2
Guest Network
WPS
VLAN
Firewall
ALG
Routing
QoS
Multiple WAN
Services
bandwidth efficiency, network management, access control, and troubleshooting. Router ports can be configured as either untagged or tagged/trunk VLAN members for use on router ports or communication across multiple network switches with 802.1Q VLAN support. VLANs can be configured with different interface IP addresses to create multiple IP subnetworks along with the DHCP server function for dynamic IP address assignment. Inter-VLAN routing will allow communication between VLAN IP subnets. VLAN tags can also be assigned to specific wireless SSIDs/network names for VLAN communication across your wireless networks.
VLANs
VID
Ports
Network
DHCP Server
1
2 Untagged
4 Untagged
6 Untagged
8 Tagged
Untagged 1
Untagged 3
Untagged 5
Untagged 7
Inter VLAN Routing
Disabled
IP Address
192.168.10.1
Subnet Mask
255.255.255.0
Mode: Enabled
Start
101
End
199
Leasetime
12h
WINS Server
Primary DNS Server
Secondary DNS Server
Local domain name


TRENDnet TEW-829DRU
Network
LAN
WAN1
WAN2
VPN
IPv6
Wireless 2.4GHz
Wireless 5GHz1
Wireless 5GHz2
Guest Network
WPS
VLAN
Firewall
ALG
Routing
QoS
Multiple WAN
General Settings
Port Forward
Port Trigger
IP Filtering
MAC Filtering
Traffic Rules
DoS Prevention
DMZ Host
One-to-One NAT
Firewall - Zone Settings
The firewall creates zones over your network interfaces to control network traffic flow.
General Settings
Drop invalid packets
Input Accept
Output Accept
Forward Drop
WAN Ping Respond
Enable


TRENDnet TEW-829DRU
Network
LAN
WAN1
WAN2
VPN
IPv6
Wireless 2.4GHz
Wireless 5GHz1
Wireless 5GHz2
Guest Network
WPS
VLAN
Firewall
ALG
Routing
QoS
Multiple WAN
Interfaces - LAN
This section allows you to modify the router's LAN IP address interface settings. Typically, the router LAN IP address settings do not need to be changed. In addition, this page allows you to configure the router's LAN DHCP server/relay settings or DHCP reservations/static leases which automatically assigns IP addresses to the wired and wireless devices that connect to your router. The router can also function as a name server and allows you to manually enter customized host names to resolve to the IP addresses of devices on your local network.
Common Configuration
General Setup
Advanced Settings
Status
br-lan
Uptime: 5d 20h 57m 24s
MAC-Address: F2:AD:A4:46:27:F9
RX: 331.70 MB (1127360 Pkts.)
TX: 24.19 MB (69960 Pkts.)
IPv4: 192.168.10.1/24
Mode
NAT
IPv4 address
192.168.10.1
IPv4 netmask
255.255.255.0