



Planificación para la implementación de un laboratorio de Ciberdefensa en la Escuela de Comunicaciones del Ejército.

Armijos Herrera, Javier Alexander

Departamento de Eléctrica, Electrónica y Telecomunicaciones

Carrera de Tecnología Superior en Redes y Telecomunicaciones

Trabajo de Unidad de Integración Curricular, previo a la obtención del título de Tecnólogo Superior en Redes y Telecomunicaciones

Ing. Caicedo Altamirano, Fernando Sebastián

15 de febrero del 2023





Latacunga

Reporte de Verificación de Contenido

Document Information

Analyzed document	MONOGRAFIA ARMUJOS JAVIER.pdf (D158349291)
Submitted	2/10/2023 3:06:00 PM
Submitted by	Juan Carlos Altamirano
Submitter email	jc.altamiranoc@uta.edu.ec
Similarity	2%
Analysis address	jc.altamiranoc.uta@analysis.arkund.com

Sources included in the report

SA	Tesis JIMENEZ-SAMANIEGO.docx Document Tesis JIMENEZ-SAMANIEGO.docx (D22386241)		1
SA	TESIS MERO SUAREZ IRVING JOEL.docx Document TESIS MERO SUAREZ IRVING JOEL.docx (D143089673)		1
SA	TESIS 10 DE NOV DE 2014 wendy.pdf Document TESIS 10 DE NOV DE 2014 wendy.pdf (D12254523)		1
W	URL: https://www.rbracing-rsr.com/downloads/wiring_pdfs/navair_manual.pdf Fetched: 1/6/2022 10:27:12 PM		3



Ing. Caicedo Altamirano, Fernando Sebastián

Director



Departamento de Eléctrica, Electrónica y Telecomunicaciones
Carrera de Tecnología Superior en Redes y Telecomunicaciones

Certificación

Certifico que el trabajo de Unidad de Integración Curricular: "Planificación para la implementación de un laboratorio de Ciberdefensa en la Escuela de Comunicaciones del Ejército" fue realizada por el señor Armijos Herrera, Javier Alexander, el mismo que cumple con los requisitos legales, teóricos, científicos, técnicos y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, además fue revisada y analizada en su totalidad por la herramienta de prevención y/o verificación de similitud de contenidos; razón por la cual me permito acreditar y autorizar para que se la sustente públicamente.

Latacunga, 15 de febrero de 2023

Ing. Caicedo Altamirano, Fernando Sebastián

C. C. 180393502-0



Departamento de Eléctrica y Electrónica y Telecomunicaciones
Carrera de Tecnología Superior en Redes y Telecomunicaciones

Responsabilidad de Autoría

Yo, **Armijos Herrera, Javier Alexander**, con cédula de ciudadanía n° 172460256-8, declaro que el contenido, ideas y criterios del trabajo de Unidad de Integración Curricular: **Planificación para la implementación de un laboratorio de Ciberdefensa en la Escuela de Comunicaciones del Ejército** es de mi autoría y responsabilidad, cumpliendo con los requisitos legales, teóricos, científicos, técnicos, y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, respetando los derechos intelectuales de terceros y referenciando las citas bibliográficas.

Latacunga, 15 de febrero de 2023

Armijos Herrera, Javier Alexander

C.C.: 172460256-8

Autorización de Publicación



Departamento de Eléctrica, Electrónica y Telecomunicaciones
Carrera de Tecnología Superior en Redes y Telecomunicaciones

Autorización de Publicación

Yo **Armijos Herrera, Javier Alexander** con cédula de ciudadanía n° 172460256-8, autorizo a la Universidad de las Fuerzas Armadas ESPE publicar el trabajo de Unidad de Integración Curricular: **Planificación para la implementación de un laboratorio de Ciberdefensa en la Escuela de Comunicaciones del Ejército** en el Repositorio Institucional, cuyo contenido, ideas y criterios son de mi responsabilidad.

Latacunga, 15 de febrero de 2023

Armijos Herrera, Javier Alexander

C.C.: 172460256-8

Dedicatoria

Mi trabajo de titulación se lo dedicó a Dios por ser quien cada día me brinda salud y vida, a través del espíritu santo me da la dirección para hacer las cosas de la mejor manera y la fortaleza para poder sobrellevar las adversidades que cada día se presentan.

A mi querida madre que siempre ha creído en mí y me apoyado en cada sueño que he tenido, por su ejemplo de superación a base de sacrificio, humildad y sencillez, por cada día brindarme sus consejos porque gracias a ellos he sabido discernir entre lo bueno y lo malo, a su apoyo incondicional que me a permitido lograr un objetivo más en mi vida.

Y a mis compañeros que durante el tiempo de estudio hemos compartido momentos buenos y malos, que nos enseñan que a veces se gana, a veces se pierde, pero siempre se aprende.

Armijos Herrera, Javier Alexander

Agradecimiento

Al Padre Celestial por cada día permitirme ver un nuevo amanecer, por darme un hogar, una hermosa familia, por las bendiciones que me colma día a día y por permitirme hacer un sueño realidad.

A mis docentes por su loable labor de dar catedra la misma que me ha permitido crecer profesional y personalmente.

A mi tutor de tesis, Ingeniero Fernando Caicedo por guiarme con paciencia y sabiduría, por siempre estar predispuesto a solventar las inquietudes y por todos los conocimientos impartidos en el transcurso de estos dos años que me ha permitido finalizar la carrera.

Al Glorioso Ejército Ecuatoriano por darme la oportunidad y las facilidades de prepararme académicamente, de superarme profesionalmente y en un futuro no muy lejano poder compartir los conocimientos adquiridos en las unidades militares.

Armijos Herrera, Javier Alexander

ÍNDICE DE CONTENIDOS

Carátula	1
Reporte de Verificación de Contenido.....	2
Certificación	3
Responsabilidad de Autoría.....	4
Autorización de Publicación	5
Dedicatoria	6
Agradecimiento.....	7
Índice de Contenidos.....	8
Índice de Figuras	13
Índice de Tablas	16
Resumen.....	17
Abstract	18
Capítulo I: Introducción.....	19
Antecedentes.....	19
Planteamiento del problema.....	20
Justificación	21
Objetivos.....	22
<i>Objetivo General</i>	22
<i>Objetivos Específicos.....</i>	22
Alcance	22
Capítulo II: Marco Teórico	24
Generalidades.....	24
Seguridad de la Información.....	24

Objetivos de la seguridad de la información.....	24
Ciberseguridad	25
<i>Dominios de ciberseguridad</i>	26
Amenaza	26
<i>Amenaza Física</i>	27
<i>Amenaza Lógica</i>	28
Vulnerabilidad.....	31
<i>Vulnerabilidades y exposiciones comunes</i>	31
<i>Clasificación de vulnerabilidades</i>	31
Riesgo	32
Ciberguerra.....	32
Ciberataques.....	33
<i>Tipos de ataques informáticos</i>	33
Cyber kill chain.....	34
Herramientas de seguridad informática	34
<i>Software Antivirus</i>	35
<i>Firewall perimetral de red</i>	35
<i>Servidor proxy</i>	35
<i>End Point Disk Encryption</i>	35
<i>Escáner de vulnerabilidades</i>	35
Sistemas operativos orientados a la ciberseguridad	36
<i>Kali Linux</i>	36
<i>Parrot Security OS</i>	37
<i>BackBox Linux</i>	38
<i>BlackArch Linux</i>	39
<i>Pentoo</i>	39

<i>Metasploit</i>	40
<i>Cortafuegos de próxima generación (NGFW)</i>	40
Red Informática	41
<i>Tipos de Redes Informáticas</i>	42
<i>Topología de Red</i>	44
Protocolos de red.....	51
<i>Modelo OSI</i>	51
<i>Modelo TCP/IP</i>	51
<i>Suites de Protocolos</i>	53
VLAN	56
<i>Tipos de VLAN</i>	56
VPN para seguridad	57
<i>Tipos de VPN</i>	57
Power over Ethernet (PoE)	58
<i>Clases de PoE</i>	59
<i>Estándares POE</i>	60
EtherChannel	61
Port Channel	63
Enrutamiento	64
<i>Tipos de protocolos de enrutamiento dinámico</i>	64
<i>Protocolos básicos de enrutamiento</i>	66
VLSM	66
Cableado Estructurado	67
<i>Características del cableado estructurado</i>	67
<i>Elementos del Cableado Estructurado</i>	68
<i>Ventajas del Cableado Estructurado</i>	68

<i>Componentes del cableado estructurado</i>	68
Tipos de cable	75
<i>Coaxial</i>	75
<i>Par Trenzado</i>	76
<i>Fibra Óptica</i>	79
Elementos para el cableado estructurado	80
<i>RJ-45</i>	80
<i>Faceplate</i>	81
<i>Patch Panel</i>	81
<i>Patch Cord</i>	82
<i>Canaletas</i>	83
<i>Rack</i>	84
Normativa de cableado estructurado	84
<i>Estándar</i>	86
Capítulo III: Desarrollo del Tema	88
Metodología	88
<i>Tipo de Investigación</i>	88
<i>Nivel de investigación</i>	88
Información de la Escuela de Comunicaciones	88
<i>Estructura Organizacional</i>	89
<i>Misión</i>	90
<i>Visión</i>	90
Análisis de Requisitos técnicos	91
Requisitos técnicos en software y hardware del cliente	91
<i>Requisitos técnicos en software del cliente</i>	91

<i>Requisitos técnicos en hardware del cliente</i>	97
Requisitos técnicos en software y hardware del servidor	100
<i>Requisitos técnicos en software del servidor</i>	100
<i>Requisitos técnicos en hardware del servidor</i>	101
Diseño del Proyecto	103
Instructivo para la instalación del cableado estructurado	123
Capitulo IV:.....	125
Conclusiones y Recomendaciones	125
Conclusiones.....	125
Recomendaciones.....	126
Bibliografía	127
Anexos.....	143

ÍNDICE DE FIGURAS

Figura 1 <i>Principios de la seguridad de la información</i>	25
Figura 2 <i>Tipos de amenaza</i>	27
Figura 3 <i>Amenaza Física</i>	28
Figura 4 <i>Amenaza Lógica</i>	28
Figura 5 <i>Identificación de una CVE</i>	31
Figura 6 <i>Cyber Kill Chain</i>	34
Figura 7 <i>Entorno de Kali Linux</i>	37
Figura 8 <i>Sistema Operativo Parrot</i>	38
Figura 9 <i>Distribución BackBox</i>	38
Figura 10 <i>Distribución BlackArch Linux</i>	39
Figura 11 <i>Distribución Pentoo</i>	39
Figura 12 <i>Interfaz de Metasploit</i>	40
Figura 13 <i>Firewall de nueva generación vs. firewall como servicio</i>	41
Figura 14 <i>Red LAN</i>	42
Figura 15 <i>Red MAN</i>	43
Figura 16 <i>Red WAN</i>	44
Figura 17 <i>Topología de Anillo</i>	45
Figura 18 <i>Topología en Árbol</i>	46
Figura 19 <i>Topología de Bus</i>	47
Figura 20 <i>Topología en Estrella</i>	48
Figura 21 <i>Topología en Malla</i>	49
Figura 22 <i>Topología Híbrida</i>	50
Figura 23 <i>Modelo OSI</i>	51
Figura 24 <i>Modelo IP/TCP</i>	52
Figura 25 <i>Interacción de Protocolos</i>	53

Figura 26 <i>Protocolos de comunicación</i>	53
Figura 27 <i>Modelo OSI y TCP/IP</i>	54
Figura 28 <i>Ejemplo de una Red con VLAN</i>	56
Figura 29 <i>Funcionamiento de una VPN</i>	57
Figura 30 <i>VPN de acceso remoto</i>	57
Figura 31 <i>VPN de sitio a sitio</i>	58
Figura 32 <i>Dispositivos conectados mediante PoE</i>	59
Figura 33 <i>Alimentación de energía directamente con el cable de red</i>	59
Figura 34 <i>Clases de PoE</i>	60
Figura 35 <i>Clases, tipos y estándares para PoE</i>	61
Figura 36 <i>EtherChannel</i>	62
Figura 37 <i>Protocolos para agregación de enlaces</i>	63
Figura 38 <i>Port Channel</i>	63
Figura 39 <i>Protocolos de enrutamiento dinámico</i>	64
Figura 40 <i>Cableado de red</i>	67
Figura 41 <i>Cableado vertical</i>	71
Figura 42 <i>Cuarto de Telecomunicaciones</i>	72
Figura 43 <i>Cableado Horizontal</i>	73
Figura 44 <i>Distancias Máximas para el Cableado Horizontal</i>	73
Figura 45 <i>Toma corriente equipado con adaptador</i>	74
Figura 46 <i>Permisos en el área de trabajo</i>	75
Figura 47 <i>Cable coaxial</i>	76
Figura 48 <i>Par Trenzado</i>	77
Figura 49 <i>Fibra Óptica</i>	80
Figura 50 <i>Cable directo</i>	80
Figura 51 <i>Cable cruzado</i>	81

Figura 52 <i>Faceplate doble</i>	81
Figura 53 <i>Patch panel</i>	82
Figura 54 <i>Paneles de parcheo</i>	82
Figura 55 <i>Cable de red</i>	83
Figura 56 <i>Canaleta</i>	83
Figura 57 <i>Modelos de rack</i>	84
Figura 58 <i>Organismos</i>	85
Figura 59 <i>Organigrama Escuela de Comunicaciones</i>	90
Figura 60 <i>Características de ESXi</i>	100
Figura 61 <i>Distribución del gabinete</i>	103
Figura 62 <i>Ubicación del laboratorio</i>	104
Figura 63 <i>Conversión de unidades</i>	105
Figura 64 <i>Área de trabajo</i>	105
Figura 65 <i>Diseño de los escritorios</i>	106
Figura 66 <i>Ubicación de los computadores</i>	106
Figura 67 <i>Puntos de red dobles</i>	107
Figura 68 <i>Tendido del cable de red</i>	108
Figura 69 <i>Puntos de red</i>	108
Figura 70 <i>Cantidad de cables</i>	109
Figura 71 <i>Formato de etiquetado Faceplate</i>	110
Figura 72 <i>Etiquetado faceplate</i>	114
Figura 73 <i>Etiquetado faceplate</i>	114
Figura 74 <i>Etiquetado en el Patch panel</i>	116

ÍNDICE DE TABLAS

Tabla 1 <i>Comparación entre RIP, OSPF y EIGRP</i>	66
Tabla 2 <i>Características del cable UTP</i>	77
Tabla 3 <i>Tabla comparativa de los programas de virtualización</i>	92
Tabla 4 <i>Tabla comparativa de los sistemas operativos</i>	93
Tabla 5 <i>Tabla comparativa programas de criptografía</i>	95
Tabla 6 <i>Tabla comparativa de firewall</i>	96
Tabla 7 <i>Requerimientos técnicos</i>	98
Tabla 8 <i>Requerimientos del servidor</i>	102
Tabla 9 <i>Etiquetado del faceplate</i>	110
Tabla 10 <i>Etiqueta para identificación del panel de conexiones</i>	115
Tabla 11 <i>Etiquetado de un extremo del cable que va al Patch panel</i>	117
Tabla 12 <i>Etiquetado del otro extremo del cable que va al faceplate</i>	120

Resumen

En la actualidad en varias instituciones públicas y privadas surge la problemática que el activo más importante con el que cuentan estas entidades (información) es vulnerable es decir está en riesgo debido a la gran cantidad de delitos informáticos que son ocasionados por ciberdelincuentes que buscan obtener información personal, con el pasar de los años los métodos de hackeo han ido evolucionando. Es por ello que el objetivo general de la presente investigación es la planificación para la implementación de un laboratorio de ciberdefensa que tiene como propósito realizar el bosquejo del laboratorio y del cableado estructurado basado en normas internacionales para que en un futuro no muy lejano se pueda implementar dicho laboratorio y de esta forma dar las facilidades para que el personal de alumnos militares que realicen el curso de ciberdefensa ponga en prácticas los conocimientos teóricos adquiridos. El proyecto está conformado por un marco teórico el cual sustenta la investigación realizada, en el desarrollo del tema se explica cómo se realizó el diseño del laboratorio, el recorrido del cableado, la ubicación de los equipos, así como el análisis técnico para poder determinar los equipos y sistemas operativos idóneos para cada computador y/o servidor. Con el diseño realizado se logró establecer conclusiones y recomendaciones que sirva de guía para una futura implementación por parte de las autoridades competentes.

Palabras Clave: Delito informático, Ciberdelincuente, Laboratorio de ciberdefensa, Cableado estructurado, Sistemas Operativos

Abstract

Nowadays in several public and private institutions the problem appears that the most important asset that these entities have (information) is vulnerable, that is to say, it is at risk due to the large amount of computer crimes that are caused by cybercriminals who seek to obtain personal information, over the years hacking methods have evolved. That is why the general objective of this research is the planning for the implementation of a cyber defense laboratory whose purpose is to make the outline of the laboratory and structured cabling based on international standards so that in the not too distant future this laboratory can be implemented and thus provide the facilities for the personnel of military students taking the cyber defense course to put into practice the theoretical knowledge acquired. The project is made up of a theoretical framework which supports the research carried out, in the development of the topic it is explained how the design of the laboratory was carried out, the wiring route, the location of the equipment, as well as the technical analysis to determine the equipment and operating systems suitable for each computer and / or server. With the design made it was possible to establish conclusions and recommendations that will serve as a guide for future implementation by the competent authorities.

Keywords: Computer crime, Cyber offender, Cyber defense laboratory, Structured cabling, Operating systems

Capítulo I

Introducción

Antecedentes

El ciberespacio se ha convertido en una nueva dimensión de confrontación para las naciones, los últimos 20 años el avance de las tecnologías de la información y la comunicación han sido exponencial, lo que empezó siendo una herramienta para ayudar y optimizar los procesos administrativos es ahora un instrumento estratégico de la defensa.

Los sistemas informáticos de las diferentes instituciones ya sean públicas o privadas a nivel mundial son vulnerables y corren el riesgo de recibir ataques informáticos, es por ello que el 12 de septiembre del 2014 por el Acuerdo Ministerial No. 281 se creó el Comando de Ciberdefensa dentro de las Fuerzas Armadas, organismo que tiene como misión defender, explotar el dominio cibernético y responder ante incidentes o amenazas que atenten la infraestructura crítica estratégica digital de FF.AA y del estado (COCIBER, 2014).

Hernández Linares y Jiménez Montañez en su artículo “Importancia de la implementación de un laboratorio de ciberdefensa” desarrollado en la Escuela Militar de Cadetes “General José María Córdova” del Ejército de Colombia, identifica las nuevas amenazas a la seguridad nacional planteadas por la expansión e intensificación de la actividad del ciberespacio en todos los niveles; también, destaca la necesidad de que los Estados modernos se preparen para la acción defensiva en este nuevo campo de batalla conocido como ciberespacio; y para finalizar, llama la atención sobre la necesidad de un orden jurídico internacional más eficaz a la luz de esta alarmante realidad contemporánea (2020).

Según Cardona Zapata y Sánchez Piedrahita en su trabajo de investigación “Diseño de un Laboratorio de Seguridad de la Información para el Tecnológico de Antioquia” la ayuda de los recursos que brinda este espacio en cuanto a infraestructura, calidad, diseño, docentes y casos de estudio que simulan con éxito ciberataques, buscó proponer una guía para la

implementación de un laboratorio de prácticas de seguridad informática, promover el desarrollo y aprendizaje académico a través de la realización de la praxis (2019).

En consecuencia, se puede verificar el gran interés que existe actualmente por parte de los investigadores en mejorar la preparación en el ámbito de la ciberseguridad, formación que tiene como finalidad contribuir contingente capacitado y que proteja el activo más importante que existe hoy en día que son los datos.

Planteamiento del problema

Aproximadamente en el mes de febrero del 2020 en Ecuador empezó la pandemia del COVID-19 lo que conllevó a un confinamiento nacional motivo por el cual la población tuvo que realizar teletrabajo y el estudio de forma virtual, particularidad que fue aprovechada por los ciberdelincuentes para robar información personal, propagación de malware y ataques orientados a ciertos sectores, en América Latina hubo un incremento del 25% en ataques de código malicioso (Dávalos, 2021).

El aumento de ataques en Ecuador no fue la excepción y varias instituciones se vieron afectadas, el 16 de abril del 2022 el Municipio de Quito recibió un ataque de ransomware y fue perjudicado con el 15% de su información, lo cual afectó a los servicios en línea y la ciudadanía tuvo que realizar los trámites por ventanilla (Mantilla, 2022).

Otro acontecimiento nefasto sucedió el 10 de marzo del 2022, la plataforma del centro de inteligencia fue hackeada, información de Fuerzas Armadas e inteligencia de la Policía Nacional se vio afectada (Televistazo, 2022).

Existen serios vacíos en la identificación de riesgos en Ecuador, acontecimientos descritos anteriormente y puesto que los ataques cibernéticos son inevitables el Ministerio de Telecomunicaciones elabora la Estrategia Nacional de Ciberseguridad con la finalidad que la ciudadanía acceda a los servicios en línea de forma más segura. Estos sucesos hacen que el

Estado cree el Comando de Ciberdefensa para protegerse de ataques cibernéticos (Saumeth, 2021)

En la actualidad el Comando de Educación y Doctrina del Ejército mediante la Escuela de Comunicaciones tiene como finalidad la especialización, perfeccionamiento y capacitación continua de sus miembros impartiendo dos cursos de perfeccionamiento y dos cursos de especialización al año, iniciando esta modalidad el 28 de marzo del 2022 con el primer curso de Ciberdefensa bajo responsabilidad de la ESCOM, sin embargo, la problemática surge en la práctica de dichos aprendizajes debido a que los alumnos que desarrollan este curso no cuentan con un laboratorio donde puedan poner en práctica todo lo aprendido, es por esto que en su gran mayoría se genera un déficit en el aprendizaje y por ende mala práctica profesional.

Por ello al continuar año tras año con la problemática planteada se dificulta que la ESCOM pueda llevar a cabo el curso, una vez que se ha identificado la problemática se establece que la Escuela de Comunicaciones requiere de la planificación de un laboratorio de ciberdefensa que permita a los alumnos adquirir todos los conocimientos, destrezas y aptitudes con ayuda de la praxis del curso en mención.

Justificación

Para la Escuela de Comunicaciones es muy importante tener un laboratorio que cuente con todas las herramientas necesarias tanto hardware como software puesto que aporta a que los alumnos adquieran las destrezas durante el proceso de aprendizaje.

El presente trabajo tiene como finalidad la planificación de un laboratorio de ciberdefensa lo cual garantiza que en cualquier momento se pueda implementar el laboratorio y de esta manera los próximos cursos que se desarrollen en la Escuela de Comunicaciones cuenten con la infraestructura adecuada lo que conlleva a una mejora en la calidad educativa y en el rendimiento de los alumnos.

La consecuencia de no planificar la implementación de un laboratorio de ciberdefensa en estos momentos agrava el desarrollo de los próximos cursos porque no contarían con la infraestructura adecuada para poder recibir las clases, de continuar con el problema se dificultaría impartir el conocimiento por parte de los instructores, a los alumnos poder desarrollar las prácticas de las diferentes asignaturas generando vacíos que no garantizan que desempeñen correctamente las funciones que le corresponden.

Los beneficiarios de esta investigación serán la Escuela de Comunicaciones, los instructores y alumnos de los diferentes cursos que harían uso del laboratorio de ciberdefensa y sus dependientes indirectos.

Objetivos

Objetivo General

- Realizar una planificación para la implementación de un laboratorio de Ciberdefensa en la Escuela de Comunicaciones del Ejército.

Objetivos Específicos

- Investigar los requisitos técnicos para la implementación de un laboratorio de Ciberdefensa en la escuela de Comunicaciones del Ejército
- Planificar el despliegue para el cableado estructurado y equipos, siguiendo normativas internacionales.
- Implementar un instructivo para la puesta en marcha de equipos y sistemas informáticos requeridos para el laboratorio

Alcance

El presente trabajo de investigación tiene como propósito realizar la planificación para la implementación de un laboratorio de ciberdefensa para lo cual será necesario realizar una investigación técnica, se empezará con el análisis de los requisitos técnicos los cuales dan a conocer las características, condiciones, cantidad, calidad de los recursos que debe cumplir el

laboratorio, posteriormente se planifica el despliegue del cableado estructurado y los equipos en referencia a las normativas internacionales, finalmente para demostrar el desarrollo de la investigación se realizará un instructivo que facilite la puesta en marcha de equipos y sistemas informáticos requeridos para el laboratorio de ciberdefensa en la Escuela de Comunicaciones.

Capítulo II

Marco Teórico

Generalidades

En el siguiente capítulo se detallan todos los contenidos teóricos relacionados a ciberseguridad y a su vez los requerimientos técnicos esenciales a tener en cuenta en la implementación de un laboratorio de ciberseguridad, conceptos que ayudan a una comprensión general del tema de investigación.

Seguridad de la Información

Es el conjunto de normas de seguridad asignadas por una empresa u organización con la finalidad de salvaguardar información sensible y proteger su privacidad es decir resguardar los activos de la información (Silva, 2021).

Objetivos de la seguridad de la información

La finalidad de la seguridad de la información es mantener la integridad, disponibilidad y confidencialidad de la información.

- **Integridad:** los recursos y la información no se modifica permanece intacta, solo personal autorizado puede realizar cambios.
- **Disponibilidad:** la información y los medios están disponibles en cualquier momento.
- **Confidencialidad:** garantiza que los datos están protegidos y solo personal habilitado tienen acceso (Gomez, 2022).

Figura 1

Principios de la seguridad de la información



Nota. En la figura se puede observar los principios básicos de la seguridad de la información.

Recuperado de (Martínez Ramírez, 2020)

- **Autenticidad:** este objetivo se relaciona con el usuario, se obtiene el seguimiento de quien tiene acceso, permisos, quien puede modificar y quien no.
- **No repudio:** permite visualizar quien tuvo acceso a un archivo y si realizó alguna modificación (ISO 27001, 2018).

Ciberseguridad

Es la praxis de defender las redes, programas y los sistemas de los diferentes ataques en línea. Los ataques digitales pretenden chantajear a los usuarios a cambio de dinero o interferir con las operaciones comerciales (CISCO, 2022).

La ciberseguridad está enfocada en la información digital es por ello que hay apogeo en la ciberseguridad la mayoría de las personas utiliza diariamente dispositivos móviles, computadoras, tablet, para transacciones bancarias, ingreso a portales institucionales, pago de servicios básicos, registro de notas, etc.

Dominios de ciberseguridad

Una estrategia sólida dentro de la seguridad cibernética incluye capas de defensa que protegen contra el delito cibernético, incluido los ataques cibernéticos que quieren acceder, modificar o destruir datos extorsionar a los usuarios o a la organización o interrumpir las operaciones comerciales normales (IBM, 2020). Las contramedidas deben estar dirigidas a:

- **Seguridad de la red:** Las conexiones Wi-Fi y por cable se encuentran entre las medidas de seguridad que se utilizan para mantener una red de sistemas segura frente a los extraños. De acuerdo con la Universidad Católica San Pablo hay varias capas a considerar cuando se trata de ciberseguridad en una organización. Los ataques pueden acontecer en cualquier capa del modelo de capa de seguridad de la red, por lo que el hardware, el software y las políticas de seguridad de la red deben diseñarse para cada área. (UCSP, 2022)
- **Seguridad de las aplicaciones:** Son precauciones que se adoptan para evitar que los datos o el código sea hurtado, también se toma en cuenta las políticas de seguridad al momento de desarrollar aplicaciones (Vmware, 2022).
- **Seguridad de cloud:** Es el respaldo a la privacidad del cliente específicamente encripta los datos en la nube mientras está en reposo, en movimiento y en uso (IBM, 2020).

Amenaza

Es un ente que puede explotar una vulnerabilidad, también es algo o alguien que identifica una vulnerabilidad específica para explotarla y usarla en contra (Incibe, 2020).

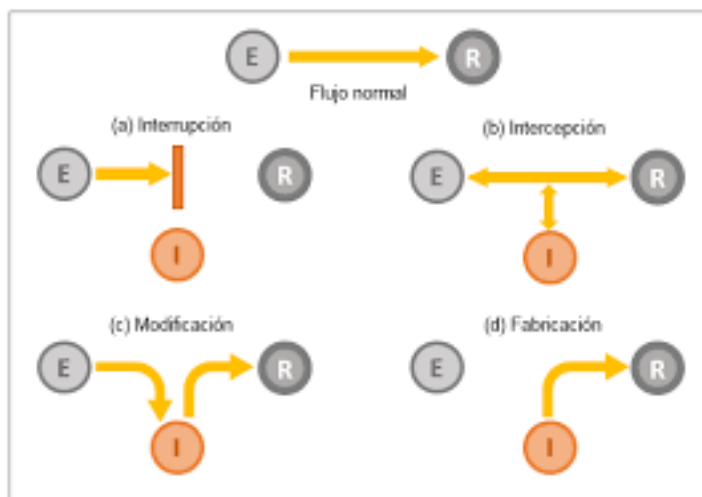
En general, se pueden utilizar cuatro categorías para clasificar las amenazas según el factor de seguridad.

- **Interrupción:** Un recurso del sistema se destruye o deja de estar disponible en este ataque contra la disponibilidad.

- **Intercepción:** Una violación de la confidencialidad en la que una parte no autorizada accede a un recurso.
- **Modificación:** Se compone de la manipulación no autorizada de los recursos, lo cual es un atentado a la integridad.
- **Suplantación o fabricación:** Una parte no autorizada inserta elementos falsos en un sistema en este ataque a la autenticidad del objeto (vlex, 2019).

Figura 2

Tipos de amenaza



Nota. En la figura se visualiza los tipos de amenazas que existen. Recuperado de (Solano, 2017)

Amenaza Física

Es cualquier acto de la naturaleza o daño causado por el hombre de forma intencional o no intencional en el hardware del computador (Jurado, 2019).

Figura 3

Amenaza Física



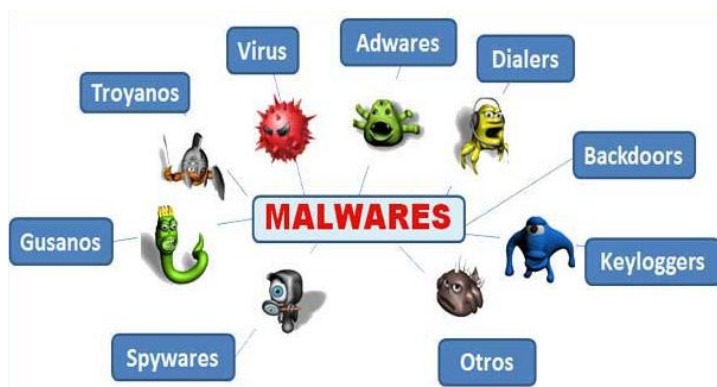
Nota. En la figura se puede observar las causas de las amenazas físicas. Recuperado de (Maribel, 2017)

Amenaza Lógica

Están asociadas con el software que daña los sistemas informáticos, ya sea a propósito o no (Maribel, 2017).

Figura 4

Amenaza Lógica



Nota. En la figura se observa los tipos de amenazas lógicas. Recuperado de (UNAD, 2022)

Los siguientes grupos serían las amenazas lógicas más significativas.

- **Malware:** es un software malicioso que va en archivos adjuntos al correo electrónico trabaja de forma sigilosa para sustraer información o a su vez borra datos, el spyware, el ransomware, los virus y los gusanos son ejemplos de software malicioso (Tokio, 2022).
- **Ransomware:** El acceso a los datos o equipos de los usuarios está restringido por software malicioso. En esencia, es la incautación de datos o equipos que requiere el pago de una determinada suma para recuperarlos. Una de las formas más comunes en que los delincuentes extorsionan a clientes y empresas es a través de este ataque. Pueden infiltrarse en las computadoras de varias maneras, más comúnmente utilizando estrategias de ingeniería social o fallas de software para instalarse con éxito en la máquina del usuario (CISCO, 2022).
- **Gusano:** este tipo de malware se incrementa indefinidamente por sí mismo y se expande por el ordenador sin causar ningún daño, pero por cantidad que se clonan consumen espacio y recursos (Fernández Y. , 2020).
- **Virus:** este tipo de malware es todo lo contrario a los gusanos, el virus afecta el rendimiento del equipo siempre y cuando el usuario autorice (Fernández Y. , 2020).
- **Troyano:** es todo lo contrario al gusano es decir no se multiplica por si solo, necesita ser ejecutado por el usuario para poder esparcirse al igual que el virus, con la diferencia que se oculta como si fuera una aplicación legítima con la peculiaridad que ingresan al sistema por la puerta trasera o también conocida como backdoor (Digicert, 2017).
- **Ingeniería social:** Se refiere a una variedad de estrategias y tácticas utilizadas por piratas informáticos para engañar a las personas e inconscientemente revelen información íntima, o a su vez al hacer clic en enlaces de sitios web maliciosos. Para eludir las precauciones típicas de seguridad cibernética y acceder a la computadora o la información personal de la víctima, estos piratas informáticos engañan a sus víctimas

para que deshabiliten las medidas habituales de seguridad cibernética y de esta manera obtener una ganancia monetaria (Softwarelab, 2021).

Muchos piratas informáticos solo confían en la voluntad de cooperación de sus víctimas potenciales para llevar a cabo ataques de ingeniería social exitosos. De manera similar, podrían intentar sacar provecho de la ignorancia de sus víctimas en lo que respecta a la tecnología. La mayoría de las veces, los piratas informáticos investigarán un objetivo viable y permisible. Para objetivos específicos, esto implica revisar cuidadosamente sus cuentas de redes sociales para buscar cualquier información personal que puedan haber compartido, como sus cumpleaños, direcciones de correo electrónico, números de teléfono o ubicaciones concurridas frecuentemente (Softwarelab, 2021).

- **Phishing:** también conocido como suplantación de identidad pretende robar información secreta como lo es usuario y contraseña de las personas por medio del correo electrónico (IBM, 2022).
- **Spyware:** es un programa espía cuya función principal es recopilar la mayor cantidad de información del usuario en secreto, cabe recalcar que se instala sin el consentimiento de la persona (G4s, 2020).
- **Adware:** también conocido como publicidad no deseada su objetivo es mostrar anuncios a través de ventanas emergentes mientras se navega en internet (Aleph, 2021).
- **Rootkit:** software utilizado por los hackers para robar información sin ser detectados a través de un acceso remoto (ICA, 2022).
- **Ataques DoS:** su objetivo es sobrecargar el servidor con tráfico hasta el punto en que no pueda dar contestación al requerimiento de servicios por parte de los usuarios (Cámara Valencia, 2018).

Vulnerabilidad

Es un error o una falla en el sistema de información que amenaza con el activo más importante de una empresa, organización o persona permitiendo que el atacante comprometa la integridad, disponibilidad o confidencialidad de la información, es importante poder localizar estas vulnerabilidades y deshacerse tan pronto como se pueda. Estas brechas pueden originarse en una variedad de lugares, como un mal diseño, una configuración incorrecta o la falta de procedimientos (Incibe, 2020).

Vulnerabilidades y exposiciones comunes

El término "vulnerabilidad" suele estar estrechamente asociado con CVE en el contexto de la seguridad informática. Encontrar vulnerabilidades en un sistema informático se puede hacer de innumerables formas. Sin embargo, se puede acceder a los detalles de CVE para encontrar una lista completa de vulnerabilidades disponibles públicamente. Además, utilizando el formato de la figura 5, todos y cada uno de los CVE deben estar correctamente identificados.

Figura 5

Identificación de una CVE



Nota. Formato de CVE para identificar una vulnerabilidad. Recuperado de (Nextvision, 2022)

Clasificación de vulnerabilidades

De acuerdo con la gravedad y el alcance de sus efectos, las vulnerabilidades se pueden clasificar en cuatro categorías principales:

- **Crítico:** Las vulnerabilidades de nivel crítico permiten a un atacante acceder a información confidencial o ejecutar código arbitrario. Se recomienda corregir estas debilidades de inmediato debido a lo peligrosas que son.
- **Alto:** Los problemas con una calificación de gravedad alta brindan a los atacantes acceso a los recursos y datos de la aplicación vulnerable, lo que les permite robar datos de sesión o datos privados de la aplicación y el servidor. En esta situación, también se recomienda reparar de inmediato las vulnerabilidades en este nivel porque pueden alentar a los atacantes a descubrir otras fallas más graves.
- **Medio:** Los errores y deficiencias en la configuración de la aplicación suelen ser los culpables de las vulnerabilidades encontradas en este nivel. Los atacantes tienen acceso a los datos privados del servidor o de la aplicación aprovechando estas fallas de seguridad.
- **Bajo:** La fuga de información, la configuración incorrecta y la falta de medidas de seguridad son vulnerabilidades en este nivel. Estos se distinguen por tener un impacto menor que los niveles observados anteriormente (crítico, alto y medio) (Atlassian, 2022).

Riesgo

Es la probabilidad que una amenaza explote una vulnerabilidad y el impacto se refleja en la empresa sea fuga o pérdida de información (ISO 27001, 2018).

Ciberguerra

Son ataques digitales que reciben las naciones diariamente, el objetivo de las agencias militares es identificar brechas de seguridad en las redes o sistemas informáticos del adversario para vulnerar, lanzar un ataque, robar información y datos confidenciales. En este escenario, el campo de batalla es el ciberespacio y las armas son los programas o aplicaciones informáticas (Sain, 2016).

Ciberataques

Es el intento de atacar los sistemas informáticos de determinada organización con la finalidad de robar información. Las personas que realizan estas actividades se les conoce como atacantes cibernéticos, piratas informáticos o hackers (González, 2018). Los ataques informáticos se pueden dividir en:

- **Ataques pasivos:** En este tipo de ataque, el atacante simplemente observa la comunicación para recopilar datos sobre lo que se transmite en lugar de cambiarlo. Debido al hecho de que no alteran ningún dato, los ataques pasivos son muy difíciles de identificar. En este ataque se localiza al emisor y el receptor de la comunicación, verifica el horario cuando existe mayor movimiento y cantidad de intercambio de datos. Sin embargo, al cifrar los datos y usar otros métodos, es posible evitar que tenga éxito.
- **Ataques activos:** Esta ofensiva cambian la serie de datos transmitidos de alguna manera o producen un flujo de datos inexistente. La usurpación de identidad, la reactuación es decir el reenvío de mensajes supuestamente de buena reputación, la alteración de mensajes o la obstrucción de un servicio haciéndolo imposible de usar (DoS) son ciertas maneras de ataques activos (Itca, 2022).

Tipos de ataques informáticos

Existen gran cantidad ataques informáticos, pero se pueden agrupar en cuatro categorías considerando su función.

- **Cibercrimen:** actividad que está dirigida a un dispositivo final con la finalidad de obtener fines de lucro.
- **Hacktivism:** acción que se realiza en forma de protesta en contra del gobierno irrumpiendo sus sitios web.
- **Ciberespionaje:** implica el robo de información importante de todas las personas que conforman una organización.

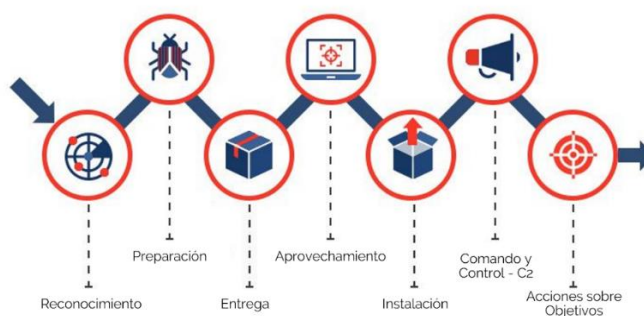
- **Ciberterrorismo:** está encaminado a gobiernos o naciones enteras y tiene un impacto significativo en la infraestructura y los servicios como la defensa o el sistema de salud (Caser, 2017).

Cyber kill chain

Es el ciclo de vida del ataque cibernético y detalla cada una de las etapas que utilizan los ciberdelincuentes para llevar a cabo un ciberataque exitoso (Netskope, 2022). En la figura 6 se visualiza las siete fases.

Figura 6

Cyber Kill Chain



Nota. La figura muestra el ciclo de vida del ataque cibernético está conformado por siete etapas. Recuperado de (Martinez, 2020)

Herramientas de seguridad informática

La formación de los empleados sobre cómo manejar los datos de la empresa, los protocolos de actuación y reacción ante las ciberamenazas y, por supuesto, el uso de software y otras herramientas de seguridad digital proporcionadas por diferentes proveedores son formas de conseguir la seguridad informática. En esta investigación, veremos algunas de las herramientas de seguridad informática más intrigantes disponibles en la actualidad, qué pueden hacer por nosotros y por qué deberíamos usarlas en el trabajo para proteger nuestros archivos (Castellnou, 2021).

Software Antivirus

Debe haber un buen programa antivirus instalado en cada computadora comercial conectada a la red. La detección de malware u otros elementos maliciosos se ve frustrada de manera efectiva por el software antivirus, que también elimina las amenazas potenciales y tiene la capacidad de poner el dispositivo en cuarentena para evitar que empeoren los problemas (Castellnou, 2021).

Firewall perimetral de red

El firewall forma parte de los equipos más importantes para la seguridad de la información. Solo escanea paquetes de red, decidiendo si bloquearlos o no en base a las reglas que el administrador ha establecido previamente. Los cortafuegos permiten examinar el tráfico web, reconocer a los usuarios, evitar el acceso no autorizado y realizar muchas otras tareas (Castellnou, 2021).

Servidor proxy

Es una pieza de equipo que se interpone entre las conexiones del navegador a Internet y filtra los paquetes que viajan entre los dos. Los sitios web que se consideran peligrosos o cuya visita está prohibida en el trabajo se bloquean gracias al proxy. El proxy también ayuda a definir un sistema de autenticación que restringe el acceso a la red externa (Castellnou, 2021).

End Point Disk Encryption

Este método de codificación de datos, también conocido como cifrado de punto final, evita que cualquier persona que no posea la clave de descifrado pueda leerlos. Al inhibir los ficheros almacenados en computadoras, servidores y otros puntos finales, protege los sistemas operativos de los archivos de instalación corruptos (Castellnou, 2021).

Escáner de vulnerabilidades

Para todos los tipos de empresas, independientemente del tamaño o la industria, el escáner de vulnerabilidades es una herramienta de seguridad informática fundamental. El escáner es una pieza de software que localiza, evalúa y controla las vulnerabilidades del

sistema. El tiempo que lleva resolver los conflictos se reduce significativamente al enviar alertas en tiempo real cuando se detectan problemas (Castellnou, 2021).

Sistemas operativos orientados a la ciberseguridad

Todas las empresas deberían tener herramientas y sistemas operativos de ciberseguridad, por varias razones, aquí están algunos parámetros a tomar en cuenta, como resultado de la aceleración de la digitalización de la pandemia, la cantidad de datos que manejan las empresas ha aumentado a un ritmo exponencial. Debido a esto, la seguridad en las organizaciones se ha convertido en un componente crucial, no solo para cumplir con los requisitos legales, sino también por su honorabilidad mediante la protección de datos privados y de tipo reservado. Sin embargo, lo más preocupante es que una persona promedio tarda 5,4 meses en darse cuenta de que ha sido pirateada, según datos de la Oficina Europea de Estadística (Bello, 2022).

Kali Linux

Para una amplia gama de temas de seguridad, incluidos análisis de red, ataques inalámbricos, análisis forense y otros, Kali Linux es la mejor opción, es una distribución de Linux basada en el sistema operativo Debian (Altube, 2021).

Con más de 600 herramientas de seguridad diferentes, Kali Linux se utiliza principalmente para pruebas de penetración y análisis forense digital. La distribución de Linux escanea computadoras y redes en busca de posibles fallas, decodifica claves y cifra los datos, asimismo evalúa el estado del sistema de seguridad. En el caso de que la información o los ficheros se hayan eliminado siempre y cuando no estén sobrescritos se puede recuperar (IONOS, 2022).

Figura 7

Entorno de Kali Linux



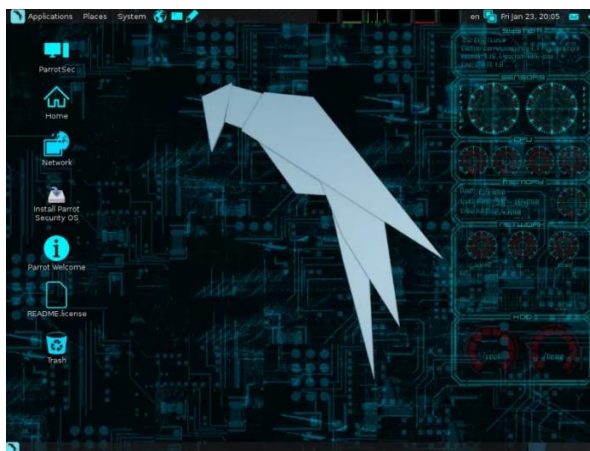
Nota. Para sistemas operativos tipo UNIX, Xfce es un entorno de escritorio liviano. Recuperado de (Kali, 2022)

Parrot Security OS

La distribución Parrot está basada en Debian, este sistema operativo cuenta con una gran variedad de herramientas para diagnosticar la protección de los equipos, con la ayuda de este programa los expertos en seguridad pueden ejecutar maniobras de ciberseguridad (Altube, 2021).

Figura 8

Sistema Operativo Parrot



Nota. En la figura se visualiza la interfaz del sistema operativo Parrot. Recuperado de (Ávila, 2020)

BackBox Linux

Esta distribución está fundada en Ubuntu y su objetivo es realizar evaluaciones de seguridad para determinar vulnerabilidades en la red (Velasco, 2019).

Figura 9

Distribución BackBox



Nota. En la figura se observa la interfaz del sistema operativo BackBox. Recuperado de (Ávila, 2020)

BlackArch Linux

Este sistema operativo tiene la finalidad de realizar pruebas de penetración, cuenta con más de 2000 herramientas para realizar análisis forense (Keepcoding, 2022).

Figura 10

Distribución BlackArch Linux



Nota. En la figura se observa la interfaz del sistema operativo BlackArch. Recuperado de (Ávila, 2020)

Pentoo

Es una distribución pioneras en el ámbito de la ciberseguridad, está enfocada en realiza evaluaciones de seguridad y pruebas de penetración (Ávila, 2020).

Figura 11

Distribución Pentoo



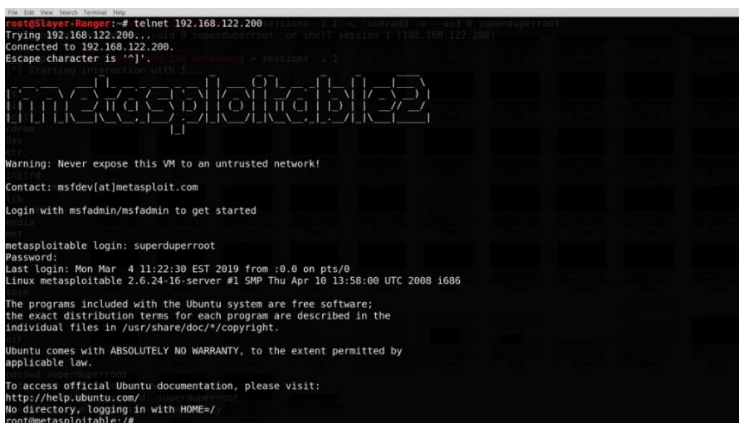
Nota. En la figura se visualiza la interfaz del sistema operativo Pentoo. Recuperado de (Ávila, 2020)

Metasploit

De acuerdo con la Universidad Complutense de Madrid el proyecto de seguridad informática de código abierto Metasploit difunde conocimientos sobre fallas de seguridad, ayuda en las pruebas de penetración y ayuda en la creación de firmas del sistema de detección de intrusos. Es una herramienta GNU que utiliza varios lenguajes de programación diferentes, incluidos C, Python, ASM, etc., para la creación, prueba, desarrollo y penetración de varios sistemas, incluido Windows (UCM, 2022).

Figura 12

Interfaz de Metasploit.



```
metasploit> telnet 192.168.122.200
Trying 192.168.122.200...
Connected to 192.168.122.200.
Escape character is '^]'.

  _____
 /  _  _  _  \
|  _ \| | | | | | |
| |_) | | | | |
|  _ \| | | | |
|_| \_|_|_|_|_|

Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started

metasploitable login: superduperr00t
Password:
Last login: Mon Mar  4 11:22:30 EST 2019 from :0.0 on pts/0
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:50:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No directory, logging in with HOME=/
root@metasploitable:/#
```

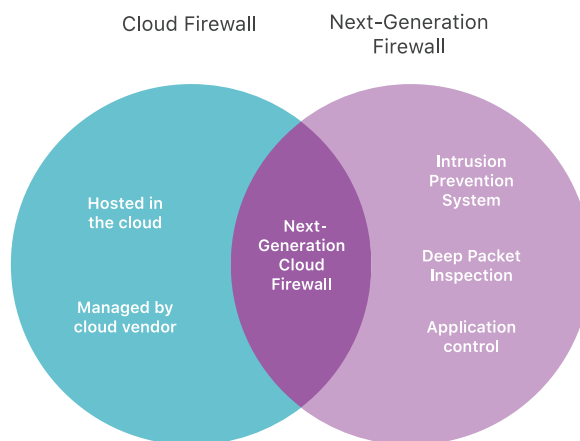
Nota. En la figura se visualiza la interfaz del sistema operativo Metasploit. Recuperado de (Xringarchy, 2019)

Cortafuegos de próxima generación (NGFW)

La tercera generación de tecnología de cortafuegos, que se puede utilizar como hardware o software, incluye un cortafuegos de próxima generación (NGFW). Al hacer cumplir las normas de seguridad en los diferentes niveles de aplicación nivel 7 del modelo OSI, puerto y protocolo, puede reconocer y frustrar ataques complejos, mientras que los firewalls que se utiliza hoy en día solo operan en las capas 3 y 4 (IT, 2021).

Figura 13

Firewall de nueva generación vs. firewall como servicio



Nota. En la figura se visualiza que un NGFW está equipado con un conjunto particular de herramientas de seguridad mientras que el FWaaS es un cortafuego que brinda sus servicios en la nube. Recuperado de (Cloudflare, 2022)

Los firewalls tradicionales son inadecuados para la sólida protección contra amenazas que requiere el panorama actual de ciberamenazas. Los NGFW tienen la capacidad de frustrar amenazas persistentes avanzadas y pueden inmovilizar al malware (Zscaler, 2022).

Red Informática

Es el conjunto de equipos informáticos conectados a través de un medio guiado o no guiado y pueden compartir datos, además son sistemas de comunicación en los que varios dispositivos alternan los roles de transmisor y receptor (Implika, 2021). Estos son los componentes de las redes informáticas:

- **Servidores:** son los que concentran el control de la red y tratan el flujo de datos.
- **Clientes:** se refiere a dispositivos en la red que no son servidores pero que aún se usan para acceder a la red.
- **Medios de transmisión:** la transmisión de información es posible gracias al cableado.

- **Elementos de hardware:** son los componentes que hacen posible construir la red físicamente.
- **Elementos de software:** son las aplicaciones necesarias para controlar todo el sistema operativo (Implika, 2021).

Tipos de Redes Informáticas

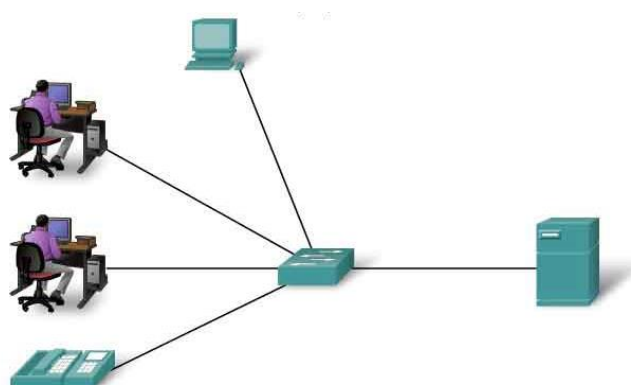
Las redes informáticas se clasifican por su tamaño y por su forma. Según su tamaño: LAN, MAN, WAN, y según la forma en que se conecten los equipos: bus, malla en estrella y en anillo (Áreatecnológica, 2022).

Redes de Área Local (LAN)

Una LAN es una red que se aloja en un área compacta, generalmente en el interior del mismo edificio. Un ejemplo de LAN son las redes WiFi en hogares y redes de pequeñas organizaciones. Un enrutador sirve como concentrador para la mayoría de las conexiones LAN a Internet. Las LAN domésticas emplean con frecuencia un único enrutador, mientras que las LAN en áreas más grandes también pueden hacer uso de más conmutadores de red para una entrega de paquetes más rápida (Hwang, 2021).

Figura 14

Red LAN



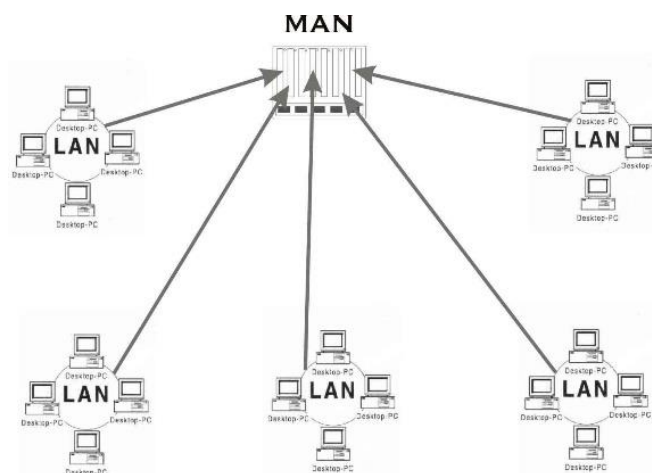
Nota. En la figura se visualiza la comunicación que existe en una red LAN. Recuperado de (UAEH, 2022)

Redes de Área metropolitana (MAN)

La red de área metropolitana trabaja a altas velocidades, cubre un área considerable y tiene la cualidad de incorporar servicios de datos, voz y video a través de medios de transmisión guiados. El significado de LAN ha evolucionado hacia el concepto de red de área metropolitana, que tiene un alcance mayor (Cisco, Red de Área Metropolitana, 2022).

Figura 15

Red MAN



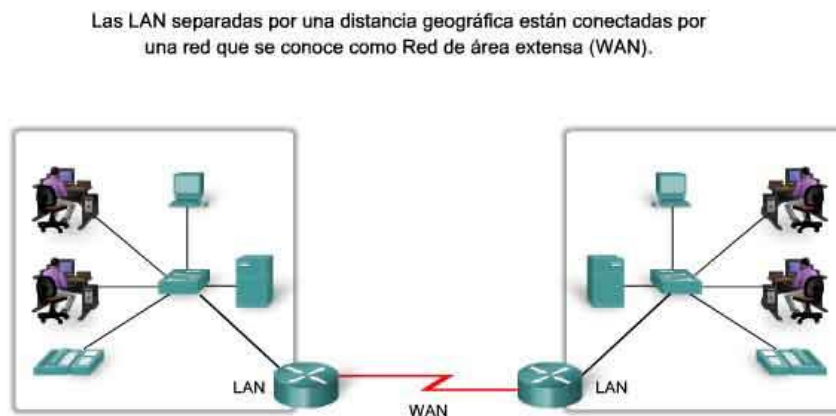
Nota. En la figura se puede observar la comunicación que existe en una red MAN. Recuperado de (UAEH, 2022)

Redes de Área Amplia (WAN)

Es una conexión entre dos o más redes de área local (LAN) que están separadas físicamente entre sí, pero le dan la sensación de estar en una conexión local. Para que una gran cantidad de computadoras funcionen en este tipo de red, deben estar conectadas entre sí a través de algún tipo de transmisión, generalmente por cable o fibra óptica, para poder comunicarse con una estación central ubicada a varios cientos de kilómetros (Higo, 2022).

Figura 16

Red WAN



Nota. En la figura se puede visualizar la comunicación que existe en una red WAN. Recuperado de (UAEH, 2022)

Topología de Red

Según la Universidad Internacional de La Rioja es el método por el cual instalaremos el cableado que unirá los equipos que componen una red. Al diseñar redes informáticas, la topología de la red es una idea crucial a considerar. Debido a que estos tipos de topología de red definen cómo se conectan las computadoras entre sí, es crucial estar familiarizado con ellos. Algunos ejemplos incluyen malla, estrella, árbol, bus y anillo (UNIR, 2022). Básicamente, hay dos niveles en una topología de red:

- **Físico:** Determina las conexiones físicas entre terminales y dispositivos, incluido el uso de cables y antenas.
- **Lógico:** Es el diagrama más completo de cómo se mueven los datos dentro de una red.

Disponer de una red bien estructurada tanto física como lógicamente es fundamental para garantizar el correcto desempeño de todos los dispositivos conectados (UNIR, 2022).

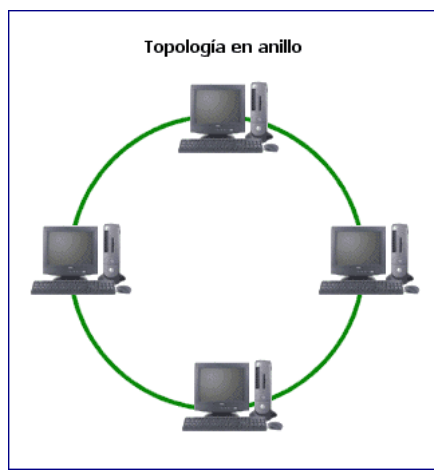
Topología de Anillo

Es un sistema interconectado de computadoras que están instaladas en forma de anillo y unidas entre sí por cables. En una estación se recibe un mensaje, se verifica la información

de envío, y si el destinatario que allí figura no es el que realmente lo está recibiendo, pasa el paquete al siguiente destinatario, y así sucesivamente, hasta que llega a su destino, en otras palabras, la información viaja a través de cada computadora antes de llegar al destinatario (Limonos, 2021).

Figura 17

Topología de Anillo



Nota. En la figura se observa el diseño físico de la red en anillo. Recuperado de (Tinet, 2022)

Ventajas

- Todas las computadoras tienen el mismo acceso al sistema.
- Incluso cuando la red se usa mucho, el rendimiento permanece constante.
- Flujo de datos sencillo.

Desventajas

- En comparación con otras topologías la transmisión de datos es más lenta, dado que la información debe pasar por cada estación intermedia antes de llegar a la ubicación final.
- Antes de que llegue a la estación de destino, las estaciones intermedias pueden ver el archivo si se está enviando.
- Con la expansión de la red, el canal normalmente se deteriora.

- Inconvenientes al momento de determinar y reparar problemas en la red (Apuntesjulio, 2022).

Topología en Árbol

Dado que dispone de un dispositivo central al que se conectan los nodos, en este caso compartiendo el mismo canal de comunicación, este tipo de topología con modelo jerárquico podría describirse como la unión de las topologías estrella y bus. Todos los nodos reciben la información, pero se propaga desde una raíz (Limonos, 2021).

Figura 18

Topología en Árbol



Nota. En la figura se observa el diseño físico de la red en árbol. Recuperado de (Tinet, 2022)

Ventajas

- Para segmentos individuales, se utiliza cableado punto a punto.
- Respaldo por muchos proveedores de hardware y software.
- Sencillez en la resolución de problemas

Desventajas

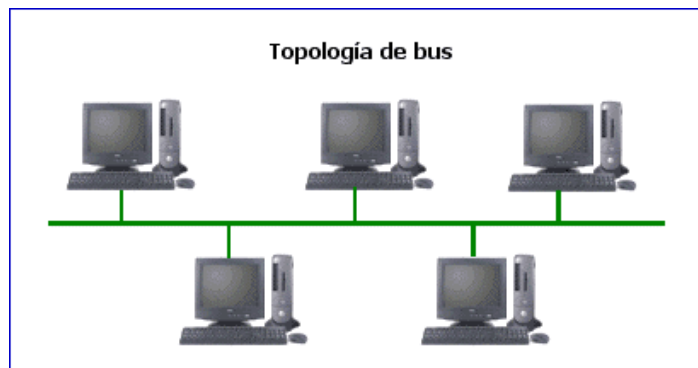
- Se necesita mucho cable.
- Todo el segmento se viene abajo si el segmento principal cae.
- Su configuración es más compleja (Apuntesjulio, 2022).

Topología de Bus

En esta topología, todos los dispositivos conectados comparten un único canal de comunicación para la transmisión de datos. Sus beneficios incluyen una fácil instalación, requisitos mínimos de cableado y un alto grado de flexibilidad con respecto a la cantidad de nodos que se pueden agregar o quitar. Sin embargo, si hay un inconveniente en el cable, entre los equipos no habrá comunicación. Si uno de los dispositivos falla, los demás seguirán funcionando con normalidad (Limonos, 2021).

Figura 19

Topología de Bus



Nota. En la figura se visualiza el diseño físico de la red en bus. Recuperado de (Tinet, 2022)

Ventajas

- Simplicidad de crecimiento y despliegue.
- Sencillez en la construcción.
- Es una red compacta.

Desventajas

- Dependiendo de la calidad de la señal, se puede utilizar una cierta cantidad de equipos.
 - A medida que la red se expande, el rendimiento disminuye.
 - Bastantes pérdidas de transmisión provocadas por colisiones de mensajes
- (Apuntesjulio, 2022).

Topología en Estrella

En contraste con la topología de bus, donde todos los dispositivos compartirían un solo canal de comunicación, cada dispositivo de red en esta topología tiene un canal separado. A diferencia de las topologías anteriores (bus y anillo), si un nodo falla o se avería, no afectará a los demás, pero si falla el switch, toda la red se paralizará. La organización de la red también mejora ya que agregar nodos se vuelve simple porque todo lo que se requiere es conectarlos al switch (Limonos, 2021).

Figura 20

Topología en Estrella



Nota. En la figura se observa el diseño físico de la red en estrella. Recuperado de (Tinet, 2022)

Ventajas

- Dado que una falla no afectará al otro equipo, los daños y/o conflictos son fáciles de evitar.
- Se puede añadir nuevos equipos rápidamente gracias a su sistema.
- La red no se detiene por completo cuando se interrumpe una conexión.

Desventajas

- Si el conmutador central no funciona correctamente, toda la red pierde la comunicación.

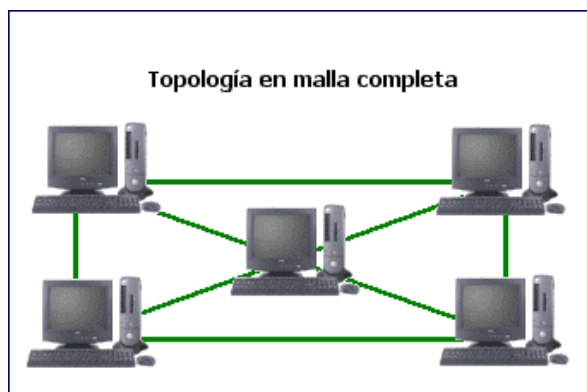
- A diferencia de las topologías de bus o anillo, requiere más cables, lo que lo hace más costoso (Apuntesjulio, 2022).

Topología en Malla

Cada nodo está conectado entre sí, se encargan de enviar los mensajes por la ruta más corta y cada uno tiene conexiones en todas las direcciones. La entrega del mensaje a su destinatario es su principal prioridad, pero en caso de que uno no tenga éxito, buscan otro más lejano (Limonos, 2021).

Figura 21

Topología en Malla



Nota. En la figura se visualiza el diseño físico de la red en malla. Recuperado de (Tinet, 2022)

Ventajas

- Enviar el mensaje a través de varios caminos o rutas
- Ausencia de interrupciones en la comunicación.
- En términos de rendimiento, es mucho más efectivo que los modelos anteriores.

Desventajas

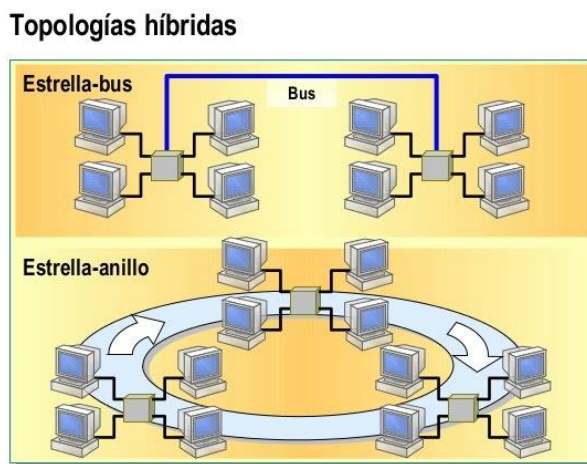
- Debido al costo y la dificultad de la instalación, solo se puede usar con una pequeña cantidad de nodos (Apuntesjulio, 2022).

Topología Híbrida

Se refiere al uso de dos o más topologías en combinación por una red de una empresa con necesidades particulares. En consecuencia, recibe los beneficios y los inconvenientes de las topologías que se incluyen (Limonas, 2021).

Figura 22

Topología Híbrida



Nota. En la figura se observa el diseño físico de la red híbrida. Recuperado de (Google, 2022)

Ventajas

- Fiable debido a la sencillez de la detección de errores y la resolución de problemas.
- Escalable, ya que las nuevas redes informáticas se pueden conectar a las existentes utilizando varias topologías de red.
- Gestiona mucho tráfico.

Desventajas

- Este tipo de red es costosa.
- El boceto de la red híbrida es extremadamente complejo.
- Para vincular la topología a otra topología, hay una modificación de hardware (Acervolima, 2021).

Protocolos de red

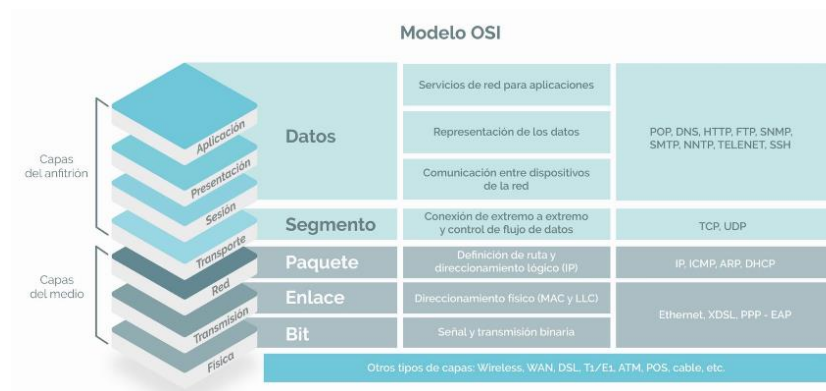
Los protocolos de red establecen un formato estándar y un conjunto de pautas para el intercambio de mensajes entre dispositivos, es necesario comprender como se comunican las computadoras, Hypertext Transfer Protocol (HTTP), el protocolo de control de transmisión (TCP) y el protocolo de Internet (IP) son algunos de los protocolos de red más populares (CISCO, 2019).

Modelo OSI

La Organización Internacional de Estandarización (ISO) creó el modelo OSI (Interconexión de Sistemas Abiertos) el cual es una referencia para las redes informáticas que utiliza protocolos para conectar diferentes sistemas de comunicación (Cloudflare, 2022). El modelo OSI está conformado por siete niveles que se representa en la figura 23.

Figura 23

Modelo OSI



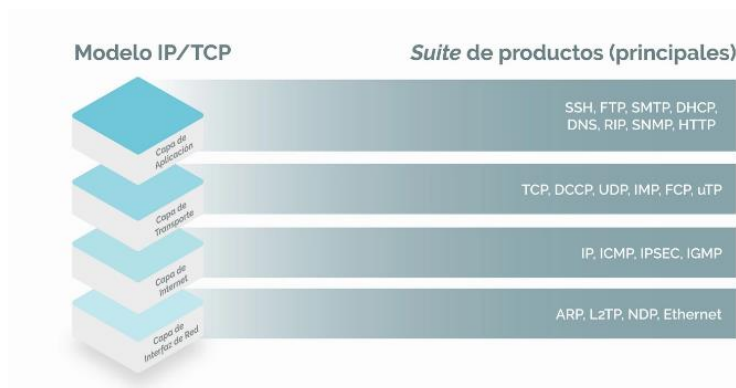
Nota. En la figura se muestra las 7 capas del modelo OSI. Recuperado de (Process, 2022)

Modelo TCP/IP

Actualmente es el modelo que se usa para las comunicaciones informáticas, está constituido por protocolos que permiten la comunicación entre equipos (Robledano, 2019). En la figura 24 se plasma las cuatro capas del modelo TCP/IP que deben tenerse en cuenta.

Figura 24

Modelo IP/TCP



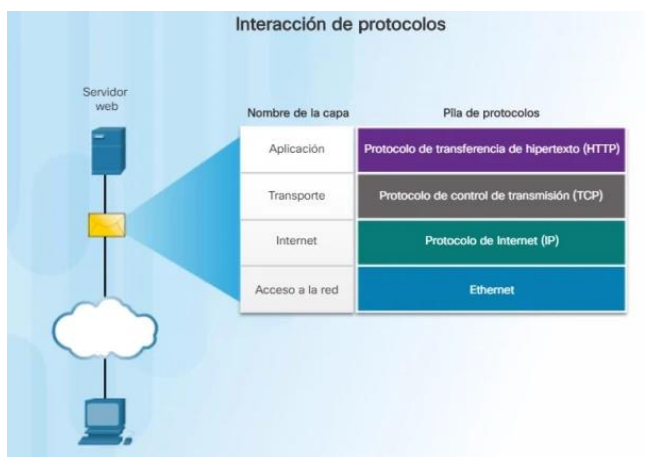
Nota. En la figura se muestra las 4 capas del modelo IP/TCP. Recuperado de (Process, 2022)

Una ilustración de cómo interactúan los diferentes protocolos es la comunicación entre un servidor web y un cliente web.

- **HTTP:** protocolo de aplicación que controla la comunicación entre un servidor web y un cliente web.
- **TCP:** gestionar conversaciones individuales a través de un protocolo de transporte.
- **IP:** crea paquetes a partir de segmentos TCP, asigna direcciones y los envía al host de destino.
- **Ethernet:** hace posible la transmisión física de datos a través de medios de red (CISCO, 2019).

Figura 25

Interacción de Protocolos



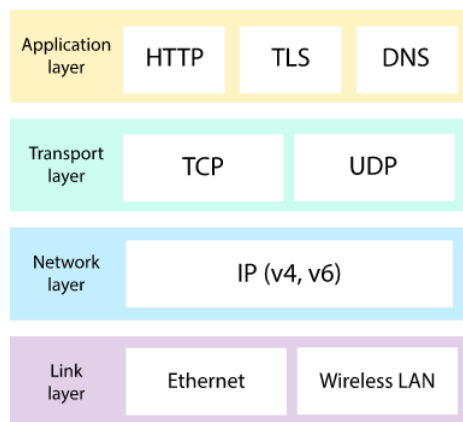
Nota. En la figura se observa la interacción entre los protocolos. Recuperado de (Educa Sistemas, 2018)

Suites de Protocolos

Es un conjunto de protocolos que realizan un esfuerzo conjunto para ofrecer servicios de comunicación de red (CISCO, 2019). Existen varios protocolos de comunicación entre los más utilizados están:

Figura 26

Protocolos de comunicación



Nota. En la figura se muestra la clasificación de los protocolos según las capas del modelo IP/TCP. Recuperado de (Khan Academy, 2022)

Figura 27*Modelo OSI y TCP/IP*

Modelo OSI	Conjunto del protocolo TCP/IP	Modelo TCP/IP
Aplicación	HTTP, DNS, DHCP, FTP	Aplicación
Presentación		
Sesión		
Transporte	TCP, UDP	Transporte
Red	IPv4, IPv6, ICMPv4 e ICMPv6	Internet
Enlace de datos	PPP, retransmisión de tramas, Ethernet	Acceso a la red
Física		

Nota. En la figura se observa una comparación entre el modelo OSI y el modelo TCP/IP.

Recuperado de (Walton, 2017)

Capa de aplicación: Establece las aplicaciones de red y servicios de Internet disponibles para el usuario.

- HTTP
- FTP
- SMTP
- SSH
- SNMP
- DNS

Capa de presentación: Asegura que los datos se representen de una manera común.

- AFP
- NFS

Capa de sesión: ayuda a la capa de presentación a administrar el intercambio de datos y organizar la conversación.

- NetBIOS

- ISNS
- FTP
- SAP

Capa de transporte: delimita los servicios de segmentación, transferencia y vuelve armar los datos.

- UDP
- TCP

Capa de red: proporciona a los terminales que han sido identificados servicios para intercambiar las porciones de datos específicos a través de la red.

- IP
- RIP
- IGP
- IPX / SPX

Capa de enlace de datos: Ofrece formas para que los dispositivos conectados por un medio común intercambien tramas de datos.

- Ethernet
- FDDI
- ARP
- PPP

Capa de física: representa los modos de transmitir bits a través de conexiones físicas (CISCO, 2019).

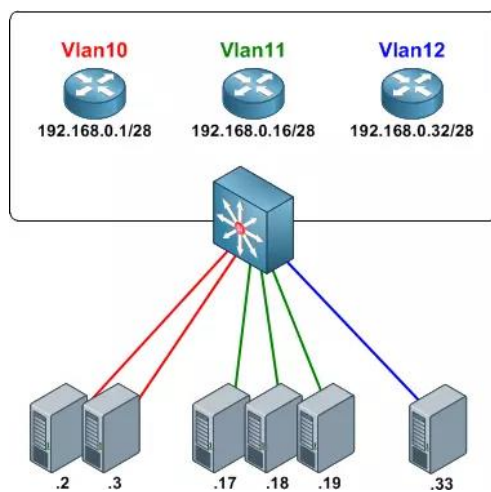
- DLS
- ISDN
- Bluetooth
- USB

VLAN

Es una técnica que permite dividir o segmentar redes independientes a partir de los diversos grupos de usuarios de red que componen una red física, es decir dentro del mismo conmutador un usuario puede tener varias VLAN (TokioSchool, 2021).

Figura 28

Ejemplo de una Red con VLAN



Nota. En la figura se observa un ejemplo de VLAN. Recuperado de (De Luz, 2022)

Tipos de VLAN

- **VLAN de datos o de usuario:** para transmitir únicamente el tráfico de datos creado por los usuarios.
- **VLAN Predeterminada:** La VLAN estándar en Cisco es la VLAN 1 la cual no se puede borrar, se transporta tráfico de control de capa 2 y al encender el conmutador esta VLAN es la VLAN predeterminada para todos los dispositivos.
- **VLAN nativa:** conectado a un puerto de tipo troncal 802.1Q. Todo el tráfico que se coloca en esta VLAN no se etiqueta con otra VLAN.
- **VLAN de administración:** Está configurado para tener acceso a la gestión de los conmutadores.

- **VLAN de Voz:** Permite mantener el nivel de servicio de telefonía VoIP. Este tráfico con etiquetas de VLAN tiene prioridad sobre otros tipos de tráfico, como los datos de Internet (De Luz, 2022).

VPN para seguridad

Una VPN es un tipo de red que transforma una red privada en pública, a través de un túnel privado los usuarios crean una conexión segura y encriptada (Kaspersky, 2022).

Figura 29

Funcionamiento de una VPN



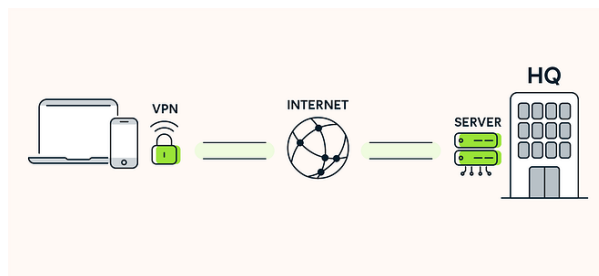
Nota. En la figura se muestra el funcionamiento de una VPN. Recuperado de (Surfshark, 2023)

Tipos de VPN

- **VPN de acceso remoto:** se puede conectar a una red diferente por medio de un túnel privado y seguro (Empey y Latto, 2020).

Figura 30

VPN de acceso remoto

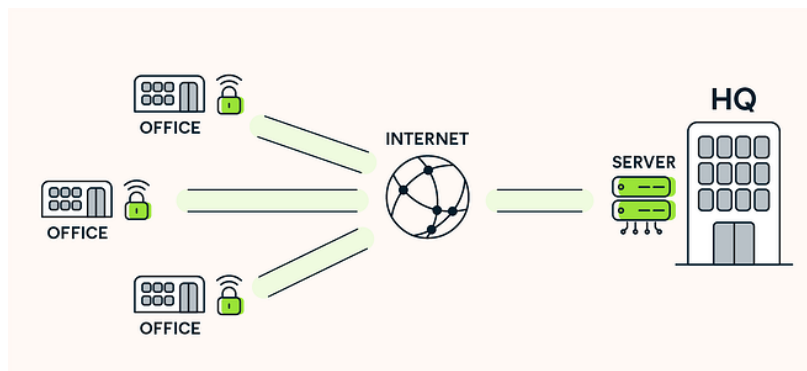


Nota. En la figura se visualiza el funcionamiento de una VPN de acceso remoto. Recuperado de (Empey y Latto, 2020)

- **VPN de sitio a sitio:** se utiliza en entornos empresariales, cuando una corporación tiene varias agencias en diferentes ciudades. Este tipo de VPN genera una red interna segura que permite conexiones entre varios sitios (Empey y Latto, 2020).

Figura 31

VPN de sitio a sitio



Nota. En la figura se visualiza el funcionamiento de una VPN de sitio a sitio. Recuperado de (Empey y Latto, 2020)

Power over Ethernet (PoE)

Los estándares IEEE 802.3af y 802.3at definen Power over Ethernet como una función de red, mediante el uso de PoE los cables Ethernet pueden alimentar dispositivos de red conectados para transferir datos y energía a los dispositivos que no cuentan con una fuente de alimentación cerca, el dispositivo de red es el que suministra la energía puede ser un switch, router, punto de acceso, etc. La única diferencia entre ellos es la cantidad de energía que pueden suministrar, (Arguello, 2022).

Figura 32

Dispositivos conectados mediante PoE.



Nota. En la figura se observa el esquema de varios dispositivos conectados mediante PoE.

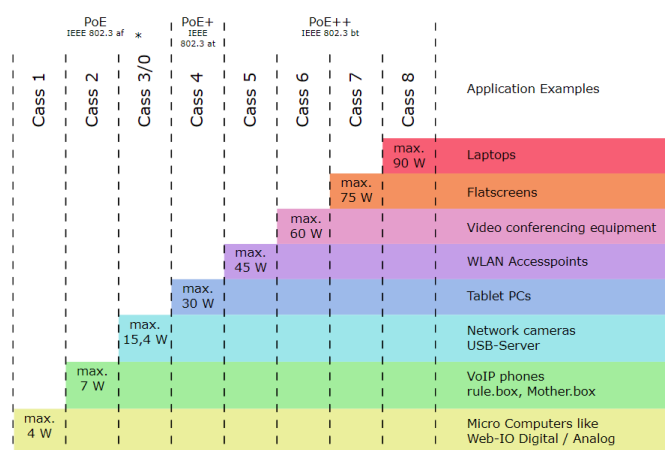
Recuperado de (Wut, 2023)

Clases de PoE

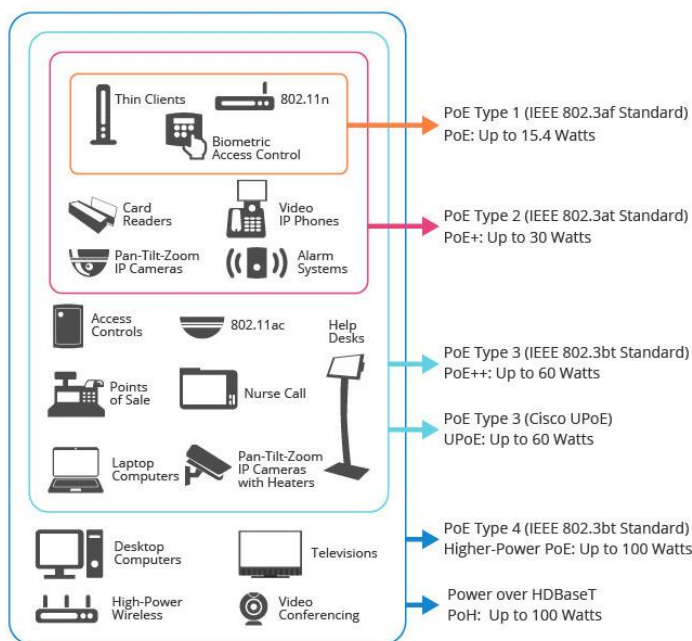
El equipo de alimentación especial en forma de interruptores e inyectores PoE proporciona la fuente de alimentación necesaria. Según la cantidad de energía que necesitan reciben una clase que va de 1 a 8.

Figura 33

Alimentación de energía directamente con el cable de red



Nota. En la figura se visualiza las clases de los puertos PoE. Recuperado de (Wut, 2023)

Figura 34*Clases de PoE*

Nota. En la figura se visualiza la clasificación de los puertos PoE. Recuperado de (Migelle, 2022)

Estándares POE

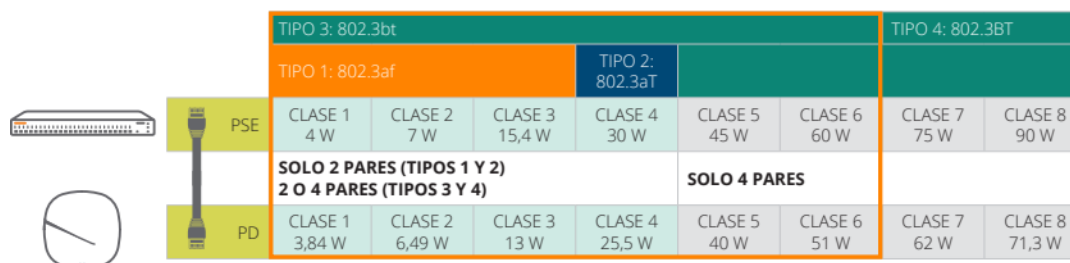
Existen tres tipos de estándares que especifican la cantidad recomendada de energía que puede manejar el equipo de fuente de alimentación. Estos son: 802.3af, 802.3at y 802.3bt.

- **802.3af:** La potencia de salida máxima de un puerto en este estándar es de 15,4 W. Hay una pequeña pérdida en el cable Ethernet durante la transmisión.
- **802.3at:** La potencia de salida mínima asegurada en cada puerto de un equipo de fuente de alimentación es de 25W, pero puede suministrar hasta 30W de potencia en cada puerto.
- **802.3bt:** Este estándar se divide en el tipo 3 y 4.
 - Tipo 3 a pesar de tener una salida máxima de 60 vatios, en realidad solo se reciben 51 vatios.

- Tipo 4 la potencia real recibida es de 71 vatios a pesar de una salida de potencia máxima de 100 vatios (Fernández L. , 2023).

Figura 35

Clases, tipos y estándares para PoE



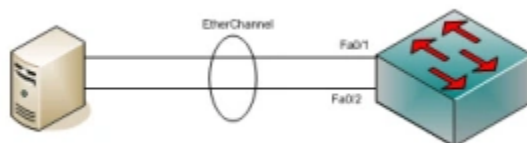
TIPO 3: 802.3bt				TIPO 2: 802.3at				TIPO 4: 802.3BT	
TIPO 1: 802.3af									
CLASE 1 4 W	CLASE 2 7 W	CLASE 3 15,4 W	CLASE 4 30 W	CLASE 5 45 W	CLASE 6 60 W	CLASE 7 75 W	CLASE 8 90 W		
SOLO 2 PARES (TIPOS 1 Y 2)				SOLO 4 PARES					
2 O 4 PARES (TIPOS 3 Y 4)									
CLASE 1 3,84 W	CLASE 2 6,49 W	CLASE 3 13 W	CLASE 4 25,5 W	CLASE 5 40 W	CLASE 6 51 W	CLASE 7 62 W	CLASE 8 71,3 W		

Nota. En la figura se puede observar las clases, tipos y estándares de los puertos PoE.

Recuperado de (Aruba, 2018)

EtherChannel

La agregación de enlaces es el proceso de combinar varios enlaces físicos entre dos dispositivos para formar un único enlace lógico. Un canal lógico permite la redundancia y la distribución de carga en caso de que falle uno o más de los enlaces del canal. EtherChannel se puede utilizar para conectar clientes LAN, servidores, enrutadores y conmutadores a través de fibra monomodo y multimodo o cableado de par trenzado (Cisco, Configuración de EtherChannel en Switches Catalyst, 2022).

Figura 36*EtherChannel*

Nota. En la figura se visualiza la agregación de un enlace lógico. Recuperado de (Todopacketracer, 2017)

PAgP

- Es un protocolo exclusivo de CISCO utilizado para establecer canales Ethernet.
- Se puede acoplar 8 interfaces del mismo tipo usando PAgP. No se pueden combinar diferentes interfaces de velocidad.
- Todos los mensajes de control son enviados por PAgP cada 30 segundos.

LACP

- IEEE 802.3ad, es el protocolo abierto para crear canales Ethernet.
- LACP solo puede unir 8 de las 16 interfaces disponibles del mismo tipo.
- No se pueden combinar diferentes interfaces de velocidad (Todopacketracer, 2017).

Figura 37

Protocolos para agregación de enlaces

	LACP		PAgP		Estático
	Active	Passive	Desirable	Auto	
LACP Active	Canal	Canal	NO	NO	NO
Passive	Canal	NO	NO	NO	NO
PAgP Desirable	NO	NO	Canal	Canal	NO
Auto	NO	NO	Canal	NO	NO
Estático	NO	NO	NO	NO	Canal

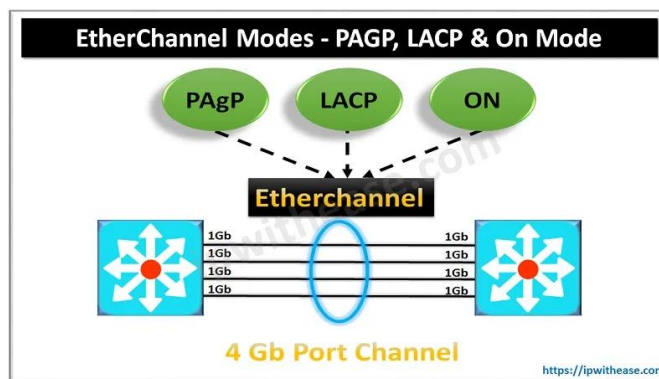
Nota. En la figura se representa los protocolos para agregación de enlaces. Recuperado de (Gerometta, 2019)

Port Channel

Es un método que permite equilibrar el tráfico entre varios puertos, es decir se crea un puerto lógico ofrece enlaces confiables y de alto rendimiento. (Collado, 2020).

Figura 38

Port Channel



Nota. En la figura se representa un port channel. Recuperado de (Bhardwaj, 2020)

Enrutamiento

Es el proceso de toma de decisiones para elegir una ruta de transferencia de información entre una o más redes, factores como la métrica, la distancia administrativa, el ancho de banda se debe tener en cuenta para encontrar la ruta más eficiente (Cloudflare, 2022). Existen dos tipos de enrutamiento, enrutamiento estático y dinámico.

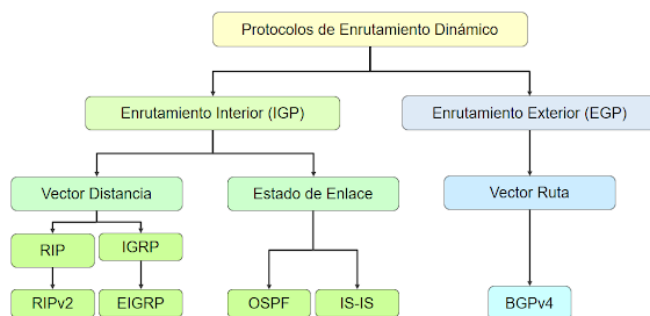
- **Enrutamiento estático:** es útil cuando el diseño o los parámetros de la red permanecerán constantes, el administrador configura y elige rutas de red de forma manual.
- **Enrutamiento dinámico:** el router intenta determinar la ruta más rápida desde el origen hasta el destino, crea las tablas de enrutamiento y las actualiza constantemente (AWS, 2023).

Tipos de protocolos de enrutamiento dinámico

Existen varias opciones de enrutamiento dinámico, todo depende de las características de la red y las necesidades del servicio. La elección de un protocolo de enrutamiento es muy necesario y en la figura 39 se detalla la clasificación.

Figura 39

Protocolos de enrutamiento dinámico



Nota. En la figura se representa los protocolos de enrutamiento dinámico. Recuperado de (Gerometta, Protocolos de enrutamiento dinámico, 2017)

- **Protocolos de Borde Interior (IGP):** dirige el tráfico de red en una misma empresa.

IGP tiene 2 categorías de protocolos:

- ❖ **Vector Distancia:** este grupo incluye los protocolos RIP y EIGRP que determinan la ruta a la red de destino en función de una dirección.
 - **RIP:** determina la mejor ruta a una red de destino en función del número de saltos.
 - **EIGRP:** determina la mejor ruta a una red de destino en función de la métrica.
- ❖ **Estado de Enlace:** consiste en los protocolos OSPF e IS-IS los cuales calculan el costo de la red de destino y verifican las adyacencias entre vecinos de manera regular.
 - **OSPF:** determina la mejor ruta en base al costo, la mejor ruta es la de menor costo, trabaja en la capa de red.
 - **IS-IS:** determina la mejor ruta de forma idéntica a OSPF con la diferencia que trabaja en las capas física y de enlace de datos.
- **Protocolos de Borde Exterior (EGP):** permite la comunicación entre enrutadores de borde de varios sistemas autónomos, un ejemplo de este protocolo es dirigir el tráfico de red entre diferentes empresas. (Telecapp, 2022). En la tabla 1 se realiza una comparación de los protocolos más utilizados.

Protocolos básicos de enrutamiento

Tabla 1

Comparación entre RIP, OSPF y EIGRP

Características	RIP	OSPF	EIGRP
Tipo	Vector distancia	Estado de enlace	Vector distancia, Estado de enlace
Tiempo de Convergencia	Lento	Rápido	Rápido
Soporta VLSM	No	Si	Si
Consumo de ancho de banda	Alto	Bajo	Bajo
Consumo de Recursos	Bajo	Bajo	Bajo
Mejor escalamiento	No	Si	Si
De libre uso o propietario	Libre uso	Libre uso	Propietario

Nota. En la figura se visualiza la comparación entre los protocolos RIP, OSPF y EIGRP.

Recuperado de (Mier Ruiz y Mier Ruiz, 2008)

VLSM

Máscara de Subred de Longitud Variable se desarrolló para usar el espacio de direcciones de una red de manera más efectiva y evitar que las direcciones IP se desperdicien,

cada subred recibe una máscara diferente según la cantidad de hosts que se van a utilizar (Arcadio, 2019).

Cableado Estructurado

Está conformado por un sistema de cables, accesorios y otros elementos, asimismo cumple con normas y reglamentos establecidos. Un sistema de cableado estructurado es una red de un único cable que incluye bloques de conexión, cables terminados en una variedad de conectores, adaptadores y diferentes tipos de cable (Escobar, 2022).

Figura 40

Cableado de red



Nota. Recuperado de (VCS, 2022)

Características del cableado estructurado

- **Modularidad:** posibilita montar una red mucho más extensa.
- **Flexibilidad:** Permite la expansión de la red sin afectar a los componentes ya presentes.
- **Compatibilidad:** Cumple con los requerimientos de la industria a nivel universal.
- **Integración de servicios:** Se combinan datos, telefonía, audio, video, seguridad, etc. dentro de una sola infraestructura, servicios.
- **Diseño:** Simplicidad en la instalación y el mantenimiento (Google, 2022).

Elementos del Cableado Estructurado

Para el diseño del cableado estructurado se debe considerar varios componentes, sus características, el bosquejo del lugar donde se colocarán y el potencial de crecimiento futuro de la instalación. En consecuencia, el número de cables que se tiendan debe ser suficiente para dar cabida a este crecimiento potencial (CAD & LAN, 2020).

Ventajas del Cableado Estructurado

- Gestión Centralizada
- Alto desempeño
- Seguridad
- Larga vida útil
- Escalabilidad
- Facilidad de Mantenimiento
- Disminución de costos (Laucol, 2020)

Componentes del cableado estructurado

- Cuarto de Entrada de Servicios
- Cuarto de Equipos
- Cableado Vertical
- Sala de Telecomunicaciones
- Cableado Horizontal
- Área de Trabajo (Informática VIP, 2022)

Los siguientes principios de diseño se aplican a todos los espacios de telecomunicaciones, incluida la sala de equipos, las salas de telecomunicaciones y la sala de entrada de servicio.

- Las puertas deben deslizarse hacia un lado, girar hacia afuera o ser desmontables, independientemente del marco de la puerta. Sus dimensiones mínimas son de 0,91 m. de ancho por 2 m de alto
- Al menos dos enchufes de diferentes circuitos deben proporcionar la electricidad. Esto es independiente de los requisitos eléctricos impuestos a la habitación por el equipo que está presente.
- Debe haber 500 lx de iluminación y el interruptor debe estar cerca de la entrada.
- En estas zonas no puede haber cielo raso.
- Cualquier agujero perforado en las paredes resistentes al fuego debe sellarse para detener la propagación del fuego.
- Toda la ruta del tendido de red debe estar libre de toda perturbación electromagnética.
- Dar fiel cumplimiento de la norma ANSI/TIA/EIA 607 la cual hace énfasis en los requisitos para puesta a tierra y seguridad en edificaciones comerciales.

Cuarto de entrada de servicios

Es la entrada del servicio de telecomunicaciones al edificio en este lugar es donde se encuentra el sitio de demarcación y el cablea ingresa a la edificación, según el estándar se debe encontrar en un lugar seco cerca de del cableado vertical, por lo general, reside en el primer piso o en el sótano, puede demandar una entrada alternativa, las paredes deben tener al menos 20 mm de espesor de A-C plywood (Santiago, 2022).

Cuarto de equipos

En el cuarto central de distribución se encuentra los router o switch de capa 3 que enrutan tráfico entre redes, los servidores principales de toda la red y el punto de presencia (POP) que es la entrada del tendido de red que viene desde la red pública hasta el edificio. Este centro principal de equipos al igual que los intermedios deben cumplir con ciertas recomendaciones que se especifican en la norma 569A como son:

- Los sistemas HVAC deben usarse para regular constantemente la temperatura en la habitación. La temperatura y la humedad relativa deben estar entre 18 y 24 grados centígrados y 30% a 55% respectivamente. Se recomienda instalar un sistema de filtro de aire para proteger la maquinaria de contaminantes como el polvo.
- Es importante tomar precauciones contra terremotos y temblores.
- Dado que la entrada debe ser lo suficientemente espaciosa para que se pueda acceder fácilmente al equipo, se recomienda tener dos puertas.
- Para evitar daños por inundaciones, la habitación debe estar elevada por encima del agua.
- Es posible que la sala de equipos y la sala de entrada de servicio sean una misma.

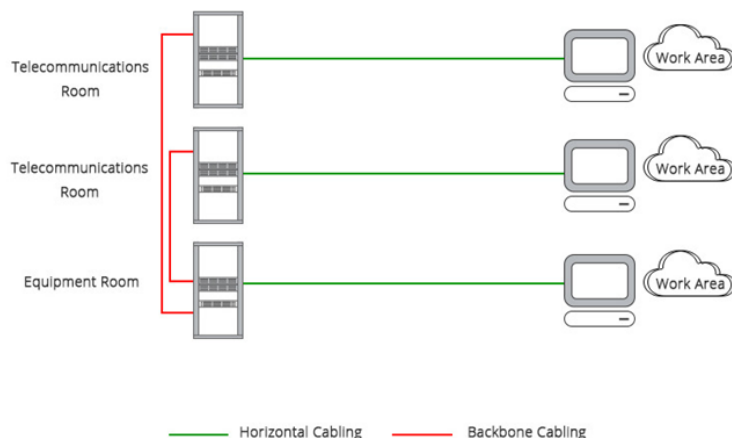
En el centro de equipos principal (MDF) pueden estar router, switch multicapa, servidores y punto de presencia, aunque dependiendo de las posibilidades del edificio se les puede separar en habitaciones distintas o por lo menos el punto de presencia separarlo de los servidores principales de tal forma de que si existe algún problema con el servicio del proveedor de internet y debe ir algún técnico al lugar no esté trabajando en el mismo espacio donde existe puntos críticos para el funcionamiento de la red (Santiago, 2022).

Cableado vertical

A todo el cableado que comunica los cuartos de telecomunicaciones intermedios con el cuarto de equipos o de distribución principal es lo que se denomina cableado vertical o cableado backbone, para este cableado es recomendable utilizar cable UTP categoría 6 o directamente fibra óptica para asegurar una buena capacidad de canal, la función del cableado vertical es la interconexión entre los diferentes gabinetes de los cuartos de telecomunicaciones y el Data Center (Santiago, 2022).

Figura 41

Cableado vertical



Nota. En la figura se visualiza el cableado vertical que está con líneas de color rojo.

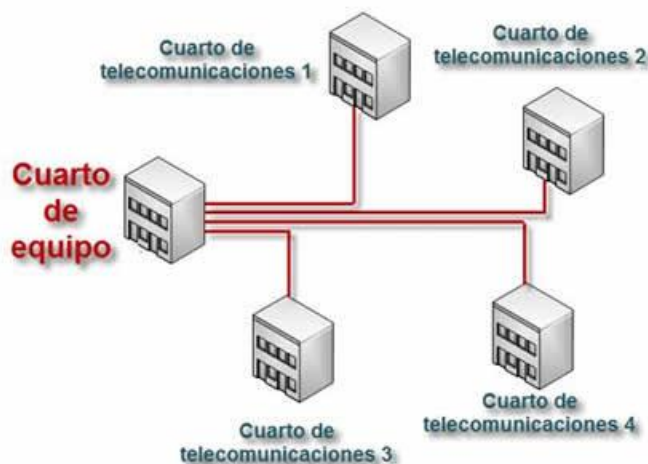
Recuperado de (Worton, 2019)

Sala de telecomunicaciones

Dentro del marco de distribución intermedio (IDF) el cableado que está protegido y viene de la zona de trabajo no se conecta directamente al switch, sino que pasa por un elemento intermedio como es el patch panel el mismo que sirve como organizador de las conexiones y además protege los puertos del switch evitando que tenga daños por una constante conexión de cables. Los cables se colocan con una pinza de impacto y siguiendo el código de colores estandarizado y desde el patch panel se conecta un patch cord pequeño al switch, de esta manera se protege el cableado, los puertos de los elementos activos y se minimiza el tiempo al momento de cambiar un cable. Dependiendo del tamaño del edificio y las redes que se manejen probablemente se usa más de un cuarto de telecomunicaciones, si el edificio es de varias plantas debe tener varios centros de distribución intermedios conectados a uno principal o uno cada 1000 m² de área utilizable (Santiago, 2022).

Figura 42

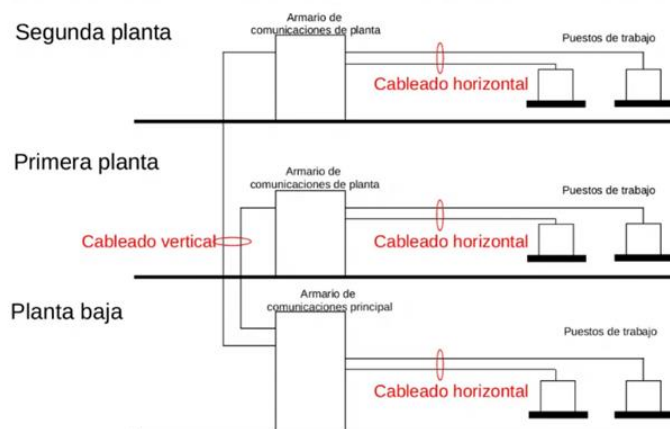
Cuarto de Telecomunicaciones



Nota. Los cuartos de telecomunicaciones están acoplados al cuarto de equipos. Recuperado de (Uhi, 2022)

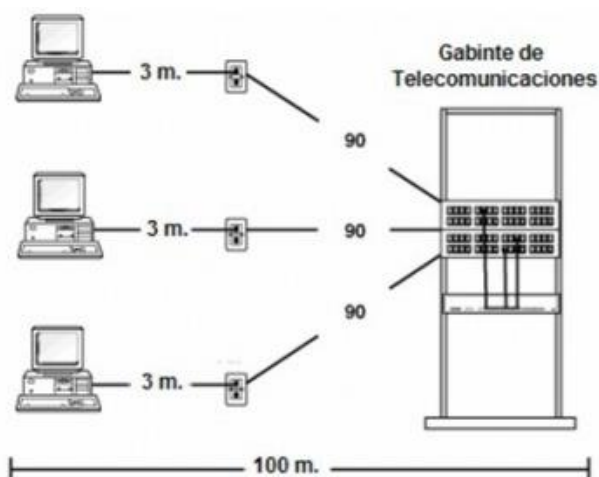
Cableado horizontal

Debe estar protegido por ductos, canaletas o bandejas aéreas, este cableado termina en el switch, el switch no debe estar ubicado en cualquier parte sino en un cuarto de telecomunicaciones o en un IDF, el marco de distribución intermedio puede ser una habitación o un espacio designado para un rack ya sea abierto o cerrado o incluso algún gabinete pequeño para montar en la pared eso depende de la magnitud de la red. El IDF es donde se debe encontrar el switch en una zona protegida correctamente ventilado como establecen las normas (Santiago, 2022).

Figura 43*Cableado Horizontal*

Nota. en la figura se puede observar el cableado horizontal que está representado por círculos de color rojo. Recuperado de (beron, 2020)

El total del cableado horizontal no debe superar los 100m de longitud, dentro del rack los cables deben estar organizados y etiquetados e incluso usar diferentes colores puede ser una opción para identificarlos fácilmente.

Figura 44*Distancias Máximas para el Cableado Horizontal*

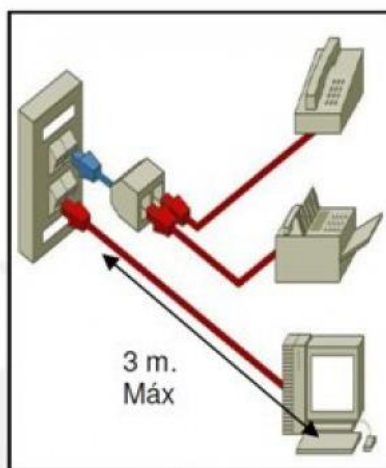
Nota. Independientemente del cable que se utilice, no puede tener más de 90 m., pero hay un buffer de 10 metros. Recuperado de (bracamontedatcenters, 2022)

Área de trabajo

Lugar donde los operarios van a trabajar en los equipos, se debe considerar que debe haber un área de trabajo cada 5m cuadrados, para conectar las áreas de trabajo se debe dividir el cableado en 3 tramos, el primer tramo comprende desde el computador al terminal RJ45 de la pared el cual no debe ser mayor a 3 metros, el segundo tramo va desde el terminal de pared hasta un patch panel el cual debe estar protegido por medio de canaletas o bandejas portacables y el último tramo desde el patch panel hasta el switch. Si existe un solo tramo puede provocar dificultades y pérdida de tiempo a la hora de cambiar y reparar, así mismo al momento de arreglar un cable muy largo se tiene acceso al switch y esta zona debe tener acceso restringido es por ello que se divide el cableado en tramos logrando de esta manera minimizar las posibilidades de que se rompa ya que la única parte visible del cable que estaría al alcance de los trabajadores es el tramo 1, el resto del cableado se encuentra por ductos o bandejas aéreas que hace difícil que se rompa accidentalmente (Santiago, 2022).

Figura 45

Toma corriente equipado con adaptador



Nota. El enchufe o punto de conexión es donde comienza el cableado. Recuperado de (bracamontedatcenters, 2022)

El cable de red que se utiliza en los puestos de trabajo y en el cableado horizontal es el cable ethernet estandarizado RJ45, este cable también es conocido como UTP es un cable de 8 hilos presentado en 4 pares trenzados, existen varias categorías de cable y se recomienda categoría 6 o 6A es lo óptimo en velocidad y transferencia. Dependiendo de la categoría del cable debe estar separado del cableado de la corriente por lo menos unos 20 cm para evitar interferencias en la señal y aislado de campos electromagnéticos como motores eléctricos o un aire acondicionado (Santiago, 2022).

Figura 46

Permisos en el área de trabajo



Nota. En la figura se observa que para llegar al área de trabajo existe una parte de cableado que es de acceso restringido y otra que es protegido. Recuperado de (Santiago, 2022)

Tipos de cable

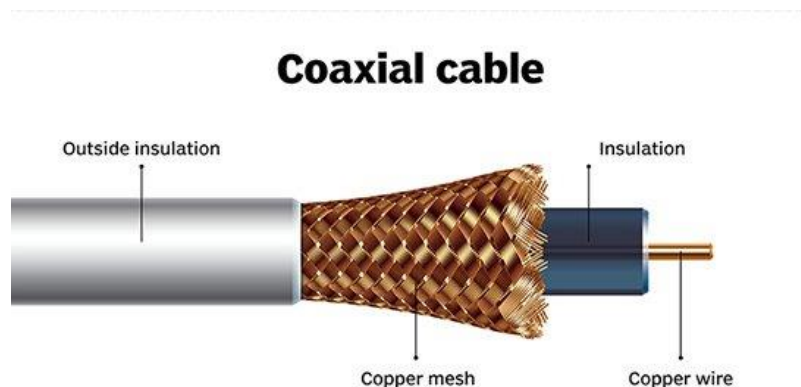
Coaxial

Para transmitir señales de radiofrecuencia, se desarrolló el cable coaxial en la década de 1930. La peculiaridad de este tipo de cable es que sus dos conductores están dispuestos de forma concéntrica en un mismo eje. Los conductores eléctricos y el material aislante se superponen en círculos concéntricos sobre cables coaxiales. Con este diseño, se garantiza que

las señales estén contenidas dentro del cable y protegidas del ruido eléctrico. (Fernández Y. , 2022).

Figura 47

Cable coaxial



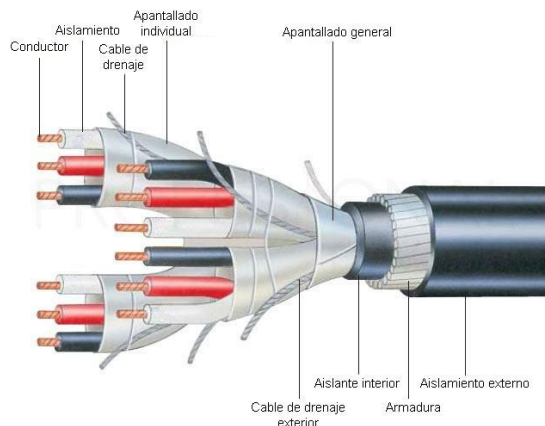
Nota. En la figura se visualiza las partes del cable coaxial. Recuperado de (Novelec, 2020)

Par Trenzado

Desde el desarrollo de las redes de datos, el cable de par trenzado se ha convertido en una de las conexiones más populares. Su diseño inteligente pero sencillo le permitió alcanzar distancias más largas al soportar mejor la interferencia y transportar más datos, lo que sin duda representó una revolución en la industria. Los cables de par trenzado están formados por pares de hilos que se entrelazan para crear un bucle en espiral. Cada conductor está hecho de aluminio o cobre y está protegido por un aislador de plástico. El nombre de par trenzado se debe porque cada cable incluye varios de estos pares en un encapsulado general, generalmente cuatro para redes LAN (Castillo, 2020).

Figura 48

Par Trenzado



Nota. En la figura se visualiza las partes del cable par trenzado. Recuperado de (Castillo, 2020).

Categorías de cable estructurado

El cableado estructurado ha mejorado significativamente con el objetivo de admitir velocidades más rápidas y arquitecturas de red más complejas que permitan una gestión eficaz para edificios inteligentes (CAD & LAN, 2020).

Tabla 2

Características del cable UTP

Categoría UTP	Estándar	Velocidad	Frecuencia	Distancia	Observación
Cat. 5	100Base-Tx	100Mbps	100 MHz	100 m	Descontinuado
Cat. 5e	1000Base-TX	1000Mbps	100 MHz	100 m	Vigente
Cat. 6	EIA/TIA 568B2.1	1Gbps	250 MHz	55 m	Vigente

Categoría UTP	Estándar	Velocidad	Frecuencia	Distancia	Observación
Cat. 6A	10GBase-T	10 Gbps	500 MHz	100 m	Uso especializado para telecomunicaciones
Cat. 7	10GBase-T	10 Gbps	600 MHz	100 m	Uso especializado para telecomunicaciones
Cat. 7A	10GBase-T	10 Gbps	1000 MHz	40 m	Uso especializado para telecomunicaciones
Cat. 8	40GBase-T	40 Gbps	1600-2000 MHz	30 m	Uso para Data Center

Nota. En la tabla se observa las características del cable UTP según su categoría. Recuperado de (CAD & LAN, 2020)

Tipos de Apantallamientos

También hay tres o cuatro letras visibles en la envoltura de plástico de la categoría del cable. Estos hablan del blindaje o protección electromagnética de los hilos de cobre que forman el cable.

- **UTP (Unshielded Twisted Pair):** Los cables no blindados se utilizan con frecuencia en entornos domésticos, pero no se recomiendan cuando los cables muy largos deben ir dentro de una pared.
- **FTP (Foiled Twisted Pair):** Los pares de cables también están trenzados y sin blindaje, pero al mismo tiempo están blindados como un todo. También se recomiendan para uso en el hogar.

- **STP (Shielded Twisted Pair):** Para que sirva de blindaje, se coloca una malla conductora sobre cada par de cables trenzados por separado. Se recomiendan para instalaciones de pared a pared.
- **SFTP (Shield Foiled Twisted Pair):** Estos cables se utilizan típicamente en instalaciones entre paredes largas; son más caros, pero también más seguros. Las mallas protectoras individuales que protegen cada par trenzado de cable se cubren con un revestimiento universal que protege todos los cables (Pablo, 2021).

Fibra Óptica

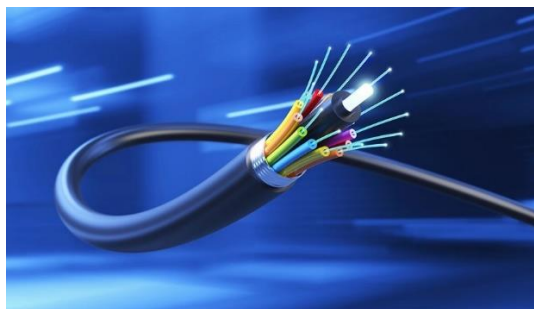
Es un medio de transferencia típicamente utilizado en redes de datos y telecomunicaciones que permite la transmisión de una cantidad significativa de datos a larga distancia se conoce como fibra óptica. Es un filamento transparente muy fino, que puede ser de vidrio o plástico, por medio del cual se envían los datos a transmitir en forma de pulsos de luz.

La fibra óptica tiene como características:

- Mayor ancho de banda.
- Mejor rapidez de transmisión.
- Inmune a interferencias.
- Menores pérdidas (Gallinas, 2022).

Figura 49

Fibra Óptica



Nota. Recuperado de (Citelia, 2020)

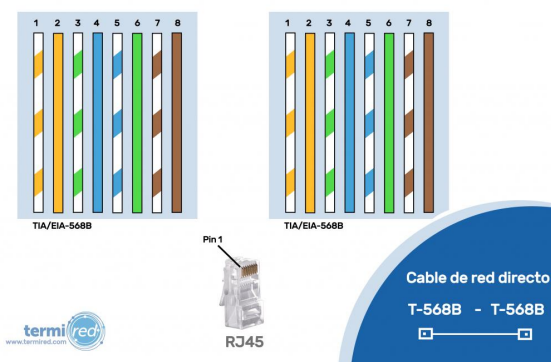
Elementos para el cableado estructurado

RJ-45

Es un conector que se utiliza para conectar computadoras a través de la tarjeta de red utilizando un cable de 4 pares de hilos de diferentes colores, según el código de colores el cable puede ser directo o cruzado como se muestra en la figura 50 y 51 (Geeknetic, 2020).

Figura 50

Cable directo

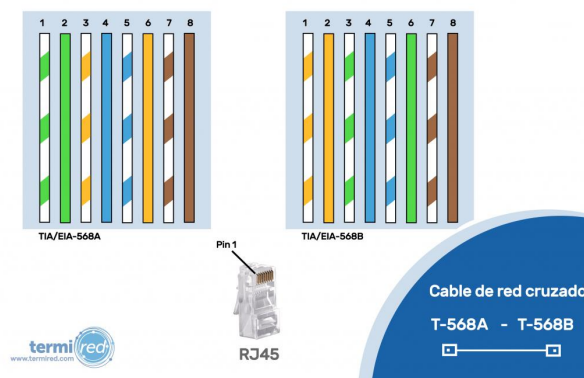


Nota. Se utiliza para conexiones entre equipos que trabajan en diferente capa del modelo OSI.

Recuperado de (Termired, 2021)

Figura 51

Cable cruzado



Nota. Se utiliza para conexiones entre equipos que trabajan en la misma capa del modelo OSI.

Recuperado de (Termired, 2021)

Faceplate

Son cubiertas de plástico que por lo general están ubicadas en la pared y por medio de un cable de red permite la conexión de voz y datos (Daga, 2020).

Figura 52

Faceplate doble



Nota. Recuperado de (Daga, 2020)

Patch Panel

Es un dispositivo de red que se instala en el rack y es el responsable de concentrar el cableado horizontal, en la parte externa del patch panel se conecta dispositivos como switch,

servidores, hub, etc, que permiten interconectar la red, mientras que por la parte posterior se enlaza los nodos de red como visualiza en la figura 53 (John, 2021).

Figura 53

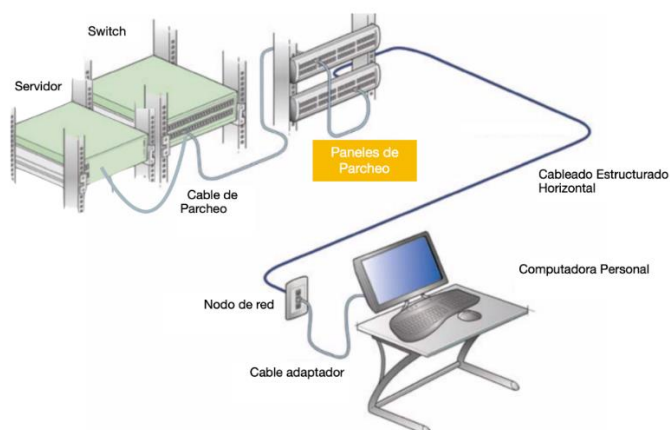
Patch panel



Nota. Recuperado de (IEEDES, 2022)

Figura 54

Paneles de parcheo



Nota. Recuperado de (Sanchez, 2019)

Patch Cord

También conocido como cable de red permite conectar dispositivos al Patch panel o elementos de una red (Sanchez, 2021).

Figura 55

Cable de red



Nota. En la figura se visualiza las características de un cable de red. Recuperado de (Daga, 2020)

Canaletas

Son ductos de plástico por los que pasan los cables, proveen de seguridad ante las perturbaciones y permite su distribución en cada área de trabajo ya sea de forma vertical u horizontal (Leroy Merlin, 2022).

Figura 56

Canaleta



Nota. En la figura se visualiza los diferentes tipos de canaletas según sus dimensiones.

Recuperado de (Hoy, 2022)

Rack

O también llamado gabinete o armario de telecomunicaciones es una estructura metálica que aloja dispositivos de red como router o switch, el tamaño lo determina de acuerdo a las necesidades (Gtlan, 2019).

Figura 57

Modelos de rack



Nota. En la figura se visualiza los diferentes modelos de racks de telecomunicaciones.

Recuperado de (Cristhian, 2021)

Normativa de cableado estructurado

Unitel-Sistemas de Telecomunicaciones se basa en una serie de Estándares de Cableado Estructurado que han sido establecidos por las organizaciones involucradas en su desarrollo. Estas Normas se utilizan para garantizar una infraestructura, instalación o proyecto que involucre un sistema de cableado (UNITEL, 2020).

- **ANSI (American Instituto Nacional de Normalización):** es una empresa sin fines de lucro que gestiona la creación de estándares para bienes, servicios, procedimientos y sistemas en los Estados Unidos. La Comisión Electrotécnica Internacional (IEC) y la Organización Internacional de Normalización (ISO) reconocen a ANSI como miembro. Para que los productos de EE. UU. se utilicen globalmente, la organización también coordina los estándares de EE. UU. con los estándares internacionales (ANSI, 2022).

- **TIA (Asociación de la Industria de Telecomunicaciones):** Para crear estándares de la industria para productos de tecnología de la información y la comunicación (TIC) como torres de telefonía móvil, terminales móviles, datos, dispositivos de VoIP, satélites, equipos de terminales telefónicas y muchos más, la Asociación de la Industria de las Telecomunicaciones (TIA) es una asociación comercial reconocida por la ANSI (Tiaonline, 2022).
- **ISO (Organización Internacional de Normalización):** La función principal de la ISO es la creación de medidas tecnológicas internacionales. El adelanto, la elaboración y el abastecimiento de bienes y servicios se hacen más productivos, seguros y claros con la ayuda de las normas ISO (Fundibeq, 2022).
- **EIA (Alianza de Industrias Electrónicas):** Asociación estadounidense que en el 2011 cerró sus puertas, fue quien motivo a la creación de normas para el tendido de red con la finalidad de tener una estructura homogénea es decir que los fabricantes desarrollen dispositivos compatibles (Atlas, 2019).
- **IEEE (Instituto de Ingenieros Eléctricos y de Electrónica):** Este instituto tiene la finalidad publicar los avances tecnológicos en los campos de Electrónica, Informática y áreas relacionadas a favor del ser humano (IEEE, 2022).

Figura 58

Organismos



Nota. Recuperado de (UNITEL, 2020)

Estándar

Según la ISO un estándar es un acuerdo escrito que comprende detalles técnicos que sirven como normas o pautas para garantizar que los servicios cumplan con su finalidad (MINTIC, 2019).

Estándares TIA/EIA

- **TIA/EIA-568-B:** esta norma de cableado se enfoca en el proceso de instalación del cableado y para su facilidad se segmenta en 3 grupos que son:
 - TIA/EIA-568-B.1 Muestra los requerimientos generales.
 - TIA/EIA-568-B.2 Componentes de cableado de Par Trenzado Balanceado.
 - TIA/EIA-568-B.3 Componentes de fibra óptica (UNITEL, 2020).
- **TIA/EIA-569-A:** El siguiente estándar se enfoca en las rutas que debe seguir cada componente del cableado estructurado así mismo busca identificar el material que se encuentre en mejores condiciones para su uso (Peralta, 2017).
- **TIA/EIA 570:** Norma de Cableado Residencial e Iluminación Comercial.
- **TIA/EIA 606-A:** El objetivo de esta norma es ofrecer un plan de gestión estandarizado con cuatro clases y que de esta manera que no se vea afectado por las diversas aplicaciones a las que puede someterse el sistema de cableado de un edificio durante su vida útil (Peralta, 2017).
- **TIA/EIA 607-A:** Se ocupa de los requisitos y procedimientos en la instalación de puesta a tierra con la finalidad de garantizar una protección eléctrica a los equipos y velar por la integridad de las personas (Alarcón, 2018).

Estándares Internacionales

- **ISO/IEC 11801:** Tecnología Información – Cableado Genérico para Cableado Estructurado de Clientes.

- **ISO/IEC 18010:** Tecnología Información – Rutas y Espacios para Cableado Estructurado de Clientes.
- **CENELEC EN 50173:** Tecnología Información – Sistemas de Cableado Genérico.
- **CENELEC EN 50174:** Tecnología Información – Instalación de Cableado – Especificación y Garantía de Calidad.

Capítulo III

Desarrollo del Tema

Metodología

Se considera práctico utilizar las siguientes técnicas de investigación para lograr cada uno de los objetivos establecidos para el desarrollo del siguiente proyecto:

Tipo de Investigación

Investigación bibliográfica

En el presente proyecto se utiliza referencias entregadas por parte de la Escuela de Comunicaciones “CRNL. EDUARDO CORNEJO” y fuentes documentales como lo son revistas, artículos científicos, libros, tesis que abordan el tema, entre otros con el fin de respaldar el presente proyecto.

Investigación de campo

Las instalaciones de la Escuela de Comunicaciones ubicada en la ciudad de Quito sector la Kennedy serán el escenario de la investigación de campo de este proyecto, que servirá para la planificación del diseño del laboratorio de ciberdefensa, asimismo para recopilar información crucial sobre tamaño del aula, puntos de red, cableado estructurado, cantidad de computadoras y que tipos de software se van a utilizar.

Nivel de investigación

Investigación descriptiva

Es la que permite explicar las características del fenómeno de estudio estableciendo atributos de su estado real, recolectando información relacionada con el estado actual.

Información de la Escuela de Comunicaciones

Reseña Histórica

Los inicios de la Escuela se remontan hacia el 16 de junio de 1922 con la creación de las Escuela para oficiales Ingenieros Militares, posteriormente en 1931 se conforma la Escuela

de Telegrafistas, para llegar al 25 de septiembre de 1943 mediante decreto Ejecutivo N° 1484 se dispone la creación de la Escuela de Transmisiones anexa a la Escuela de Artillería e Ingenieros Militares en Quito, que constituiría la primera y principal fuente de formación de personal técnico militar especializado en transmisiones.

Posteriormente el 1 de junio de 1962 la Escuela se anexa al Batallón de Transmisiones, conformando así el Batallón Escuela de Transmisiones N° 81 del Ejército.

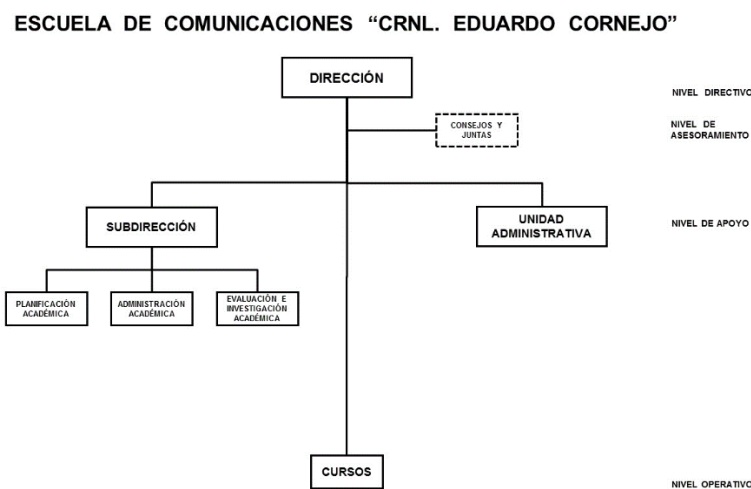
En 1987 el Batallón Escuela de Transmisiones N° 81, cambia de numeración por la de Batallón Escuela N° 1. Seguidamente en 1997 el arma de Transmisiones cambia su denominación por Comunicaciones, por lo que a partir de 1998 la unidad toma el nombre de Batallón Escuela de Comunicaciones N° 1 "Rumiñahui".

En el año 2003 la Escuela de Comunicaciones se crea como unidad independiente subordinada al Comando de Educación y Doctrina Militar Terrestre y en el año 2009 toma el nombre de "CRNL. EDUARDO CORNEJO" en honor a unos de los pioneros del arma del mando.

Actualmente la escuela está encargada de la capacitación, perfeccionamiento y apoyo a la formación de personal profesional del arma del enlace y mando, entregando personal capacitado con herramientas técnicas que demandan en la actualidad, cumplir eficientemente la misión asignada (Ejercito Ecuatoriano, 2012).

Estructura Organizacional

La escuela de comunicaciones se basa en un modelo organizacional de tipo lineal como se visualiza en la figura 59 cada nivel cuenta con una autoridad.

Figura 59*Organigrama Escuela de Comunicaciones*

Nota. En la figura se visualiza el organigrama de la Escuela de Comunicaciones. Recuperado de (Ludueña, 2022)

Misión

Especializar y perfeccionar al talento humano del Sistema de Comunicaciones del Ejército, con estándares de calidad y excelencia, a través de un proceso de enseñanza holístico; sujeto al modelo educativo de fuerzas armadas, entregando personal idóneo de apoyo en el área de comunicaciones e informática a las unidades del ejército y al país (Ludueña, 2022).

Visión

Ser un instituto líder en educación militar, basado en un modelo de gestión efectivo, que cuente con certificaciones avaladas por organismos nacionales e internacionales que, utilizando tecnología de punta, con docentes capacitados y planta física adecuada, enrumbe la especialización y perfeccionamiento del talento humano de comunicaciones e informática acorde a los nuevos escenarios y efectividad operacional (Ludueña, 2022).

Análisis de Requisitos técnicos

El curso de ciberdefensa que imparte la Escuela de comunicaciones a través de sus instructores tiene como tareas formadoras crear un par de llaves públicas, privadas y remitir al correo electrónico del instructor de forma cifrada, también realizar la exposición de una herramienta de búsqueda de información y la verificación práctica por grupos, como tarea integradora identificar la IP de un servidor C2 que tiene un malware alojado en un archivo infectado e intenta conectarse al servidor C2, es por ello que se sugiere la utilización de ciertos programas los cuales ayudaran al estudiante a poner en práctica los conocimientos adquiridos.

Para la implementación del laboratorio de ciberdefensa se recomienda la utilización de un programa de virtualización, distribuciones que cuenten con herramientas de hacking que permitan ver las vulnerabilidades que existen en los diferentes equipos y un firewall.

Requisitos técnicos en software y hardware del cliente

Requisitos técnicos en software del cliente

Las computadoras pueden usar Windows 10 o superior como su sistema operativo principal.

Virtualización

Para las prácticas de ciberdefensa se recomienda crear máquinas virtuales para ello se sugiere la utilización de un programa de virtualización, a continuación, se realiza una comparación para determinar que programa es beneficioso para los alumnos.

Tabla 3

Tabla comparativa de los programas de virtualización

	VMware	VirtualBox	Hyper-V
Facilidad de uso	Medio	Fácil	Complicado
Rendimiento	Bueno	Medio	Bueno
Instantáneas	Si	Si	No
Compartir archivos	Si	Si	Si, pero complicado.
Integración con Windows	Si	Si	No
Cifrado	Si	Si (a través de Guest Additions)	Si
Sistemas compatibles	Windows, Linux, macOS	Windows, Linux, macOS	Windows y Linux (este con limitaciones)
Precio	Gratis / De pago	Gratis	Gratis
Otros	Excelente seguridad	OpenSource	Solo en Windows 10 Pro Soporte WSL y WSL2 W

Nota. En la tabla se representa una comparación de los programas de virtualización.

Recuperado de (Velasco, 2022)

Se propone la utilización del programa VMware se conoce que es una edición de pago por las diferentes funcionalidades que tiene, sería una buena inversión por parte de la Escuela de Comunicaciones por los diferentes cursos que desarrolla, al momento que los alumnos realicen las prácticas no habría limitaciones en lo que concierne a la virtualización, rendimiento, compartir archivos, etc sino todo lo contrario se utilizaría los recursos de las diferentes máquinas.

Sistemas Operativos

Para elegir los programas que utilizaran las máquinas virtuales, se realiza una tabla comparativa de los diferentes sistemas operativos que se podría utilizar.

Tabla 4

Tabla comparativa de los sistemas operativos

	Parrot OS	Kali Linux	BackBox
RAM	320 MB	1GB	1 GB
GPU	No necesita	Si necesita	Si necesita
Almacenamiento	16 GB	20 GB	20 GB
Interfaz Gráfica	Ubuntu-Matte-Desktop-Environment	Gnome	Gnome
Compilador e IDE	Varios compiladores, IDE instalados	Compiladores y los IDE no están instalados	Compiladores y los IDE no están instalados

	Parrot OS	Kali Linux	BackBox
Interfaz de usuario	Fácil de usar	Fácil de usar	Fácil de usar
Almacenamiento y rendimiento del sistema operativo	Ligero	Lento	Ligero
Herramientas	Posee las herramientas de Kali y agrega otras propias	Tiene herramientas básicas	Tiene menos herramientas que Kali Linux
Procesador	Dual-core de 1 Ghz	Intel i5 o i7	Intel i5-4590 / AMD Ryzen 5 1500X ó superior
Respaldo	Comunidad	Offensive Security	Comunidad

Nota. En la tabla se observa la comparación de los sistemas operativos orientados a la ciberseguridad. Recuperado de (Altube, 2021)

En la tabla 4 se considera 3 sistemas operativos con sus diferentes características y requisitos de hardware para determinar que existen varios sistemas operativos de seguridad

informática sin embargo se recomienda usar Kali Linux porque es de código abierto, gratuito, fácil de utilizar, es respaldado por Offensive Security que es una de las empresas de seguridad más importante del mundo, para certificaciones internacionales como el OSCP de Offensive Security recomiendan usar Kali Linux.

Criptografía

A continuación, se realiza una tabla comparativa de los programas de criptografía para poder establecer que aplicación es la más idónea y que los estudiantes puedan realizar las prácticas de cifrado.

Tabla 5

Tabla comparativa programas de criptografía

safeDES,	Aesphere	GenRSA	SAMcript
	Aplicación de uso		
Es un programa diseñado para técnicas de encriptación DES en formato ANSI y hexadecimal, así como ataques de fuerza bruta al algoritmo DES (Muñoz, 2003).	educativo que explica el cifrado AES en los modos de cifrado CBC, ECB y CTR. También hay una sección donde puedes atacar para averiguar la clave de cifrado utilizada para	Software gratuito simplifica la comprensión y el uso del algoritmo RSA, un tipo de criptografía asimétrica ampliamente utilizado (Velasco, 2017).	Se utiliza un programa de soporte llamado SAMCRIPT para manejar cálculos de cifras grandes para criptografía simple (Díaz M. N., 2018).

safeDES,	Aesphere	GenRSA	SAMcript
cifrar un mensaje			
(Díaz A. , 2020).			

Nota. En la tabla se muestra la comparación de programas de criptografía.

En la tabla 5 se visualiza el análisis de 4 programas de criptografía, se toma en cuenta las diferentes utilidades que ofrece como es cifrar, descifrar y crear claves de forma manual o automática, es por ello que se sugiere utilizar dos herramientas que se considera de uso educativo como lo es AESphere y genRSA.

Firewall

Posteriormente se sugiere la administración del firewall para ello se realiza una analogía entre varios programas para recomendar el más idóneo.

Tabla 6

Tabla comparativa de firewall

	PFsense	IPFire	OPNSense
Procesador	600 MHz	1GHz	1 GHz i386
RAM	512	1GB	1GB
Almacenamiento	4GB	4GB	4GB
Tarjeta de red	2 mínimo (WAN y LAN)	2 mínimo (WAN y LAN)	2 mínimo (WAN y LAN)
	- NAT	- IDS/IPS	- Proxy
	- Alta	- VPN	- VPN
Características	disponibilidad	- Proxy	- DNS
	- Multi WAN	- Servidor	- DHCP
	- Balanceo de carga	DHCP	- Soporte para plugins
		- DNS	

	PFsense	IPFire	OPNSense
	- VPN		
	- Servidor PPPoE		
	- Monitoreo gráfico y por logs	- DNS - QoS	
Características	- DNS dinámico	- Filtrado	- Compatibilidad
	- Portal cautivo	GeoIP	con VLAN 802.1Q
	- Servidor DHCP y DHCP Relay	(Álvarez, 2021)	
	(Drivemeca, 2018)		

Nota. En la tabla se representa una comparación de los programas de firewall.

Los 3 programas destacan en diferentes características como se representa en la tabla 6 motivo por el cual se sugiere utilizar el enrutador y cortafuegos pfSense puesto que presenta ventajas en las herramientas de monitoreo y seguridad perimetral, asimismo pfSense tiene más tiempo en el mercado, hay más información en línea disponible y la comunidad ha crecido.

Requisitos técnicos en hardware del cliente

En referencia a los programas anteriormente mencionados se sugiere que los equipos informáticos PC de escritorio cumplan con ciertos requisitos como son:

Tabla 7*Requerimientos técnicos*

Requerimientos de la computadora	
Pantalla	24" HD IPS Touchscreen
Procesador	Intel Core i7 8-Core (10th Gen o superior)
DDR4 Memory	16 GB
SSD	256 GB
Disco Duro	1TB

Nota. En la tabla se representa los requerimientos técnicos en hardware del cliente.

Pantalla

Se sugiere que la pantalla sea de 24 pulgadas porque el estudiante al momento de realizar las practicas se ve en la necesidad de trabajar de forma multitarea, es decir tener varias ventanas abiertas, el tener una pantalla con esa dimensión ayuda a realizar diversas tareas al mismo tiempo, también se considera la NTP 251 la cual indica que la distancia que debe existir entre computadora y persona debe ser mayor a 40cm de esta manera se reduce el dolor de cuello e incluso la tensión ocular y ayuda a que la visualización sea mejor.

Procesador

Los sistemas operativos y las máquinas virtuales se actualizan constantemente, esos cambios requieren mayor velocidad y potencia es por ello que se recomienda un procesador de 2.0 GHz Intel Core i7 8-Core de 10ma generación o superior, también por las diferentes actividades que van a realizar los estudiantes en las computadoras se necesita ejecutar programas y que la mayor cantidad de tareas se completen lo más rápido posible.

Memoria RAM

Asimismo, debido a la cantidad de datos que se va a gestionar se sugiere utilizar una memoria DDR4 de 16 GB porque permite ejecutar la mayor cantidad de tareas posibles y cambiar entre tareas rápidamente consume menos energía.

Puertos

El llevar a la práctica los conocimientos adquiridos de las diferentes asignaturas del curso de ciberdefensa, extensos grupos de datos requieren ser transportados, con el auge de varias aplicaciones y de la computación en la nube la velocidad del internet es crucial es por ello que se recomienda que los puertos de red de todos los equipos de red sean 10 Gigabit Ethernet de esta forma se descarta posibles cuellos de botella y ofrece una forma práctica de satisfacer las demandas de alta velocidad.

La virtualización es otro aspecto importante que se ha considerado para recomendar la tecnología 10 gigabit ethernet, el uso de máquinas virtuales conlleva al consumo significativo en la cantidad de recursos de red y por medio de 10 gigabit ethernet los efectos de este aumento en el consumo se lograrán mitigar.

A largo plazo si se ve en la necesidad de utilizar fibra óptica no va existir ningún impedimento ya que los equipos tendrían puertos 10 gigabit ethernet y se aprovecharía todo el potencial de la fibra óptica, es primordial tener en consideración que se debe utilizar cable par trenzado de categoría 6A en adelante.

Se recomienda utilizar switches administrables porque permite realizar configuraciones de forma remota o por su interfaz, crear vlan, dar seguridad a los puertos, conectar equipos basado en la dirección MAC, monitorear la red, gestionar enlaces redundantes, etc (Cardenas, 2022).

Otra característica que se recomienda al switch aparte de que cuenten con tecnología 10 gigabit ethernet es que sean POE+ dado que tienen una potencia de salida máxima de 30

vacios por puerto, lo que permite a futuro conectar un Access Point o una cámara según las necesidades de la Escuela de Comunicaciones (Luz, 2020).

También se debe tener en cuenta el número de puertos que debe tener el switch y pensar que la red se puede expandir, hay switch desde 4 hasta 48 puertos, asimismo se debe tener en consideración la velocidad de dichos puertos que debe ser 10 gigabit ethernet (Franklin, 2019). Simultáneamente, se recomienda que el conmutador tenga puertos Uplink para poder conectar con otros switch y puertos SFP+ para tener conexión por fibra óptica (Reyes, 2019).

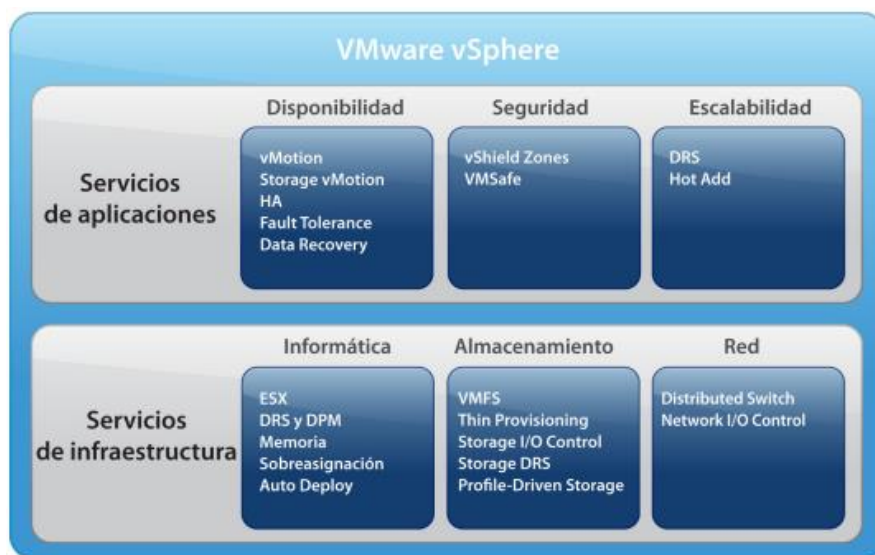
Requisitos técnicos en software y hardware del servidor

Requisitos técnicos en software del servidor

A continuación, en la figura 60 se muestra una gama completa de servicios de infraestructura y aplicaciones del hipervisor ESXi.

Figura 60

Características de ESXi



Nota. En la tabla se representa los servicios de aplicaciones e infraestructura que provee VMware. Recuperado de (VMware, 2022)

Se considera el hipervisor ESXi para que sea instalado en el servidor físico, dentro de sus características se encuentran es el más apto por su rentabilidad, disponibilidad, escalabilidad, seguridad, el apoyo que tiene de la comunidad y otro aspecto muy relevante es que el modo de operación se lo puede hacer por interfaz gráfica o líneas de comandos en el ámbito de la ciberseguridad la mayor parte del tiempo se trabaja por medio del símbolo del sistema entonces el modo de funcionamiento no habría inconvenientes.

En el sistema operativo ESXi se puede instalar máquinas virtuales y trabajar con varios sistemas operativos entre ellos de software libre que es fomentado como política de gobierno porque permite utilizar sin restricciones de datos y se ahorra en gastos de licencias (Subsecretaría de Informática, 2009).

Requisitos técnicos en hardware del servidor

En referencia al análisis realizado anteriormente se ha tomado en consideración las características de las computadoras que van a utilizar los alumnos, el almacenamiento de los entornos virtuales en conjunto con el procesamiento, el sistema operativo para las máquinas virtuales, entre otros recursos que en el transcurso del curso se puede llegar a utilizar, es por ello que en la tabla 8 se plantea las características que debe tener el servidor.

Tabla 8*Requerimientos del servidor*

Requerimientos del servidor	
Procesador	Procesador Intel Xeon o AMD Opteron
Memoria RAM	DDR4 de 32 GB
Almacenamiento	2 SSD de 2 TB
Red	Una o más tarjetas 10 Gb Ethernet

Nota. En la tabla se representa los requerimientos técnicos en hardware del servidor.

Se recomienda un procesador Intel Xeon o AMD Opteron que tenga características como escalabilidad, redundancia en la información, virtualización, que estén diseñados para trabajar 24/7, que tengan memoria caché L3 y tenga la cualidad de encontrar cualquier error en los paquetes y repararlos.

Se ha considerado una memoria RAM DDR4 de 32 GB en función de la cantidad de equipos que se ha planificado para el laboratorio así mismo el sistema operativo que se va a utilizar, esto permitirá ejecutar más programas, además genera menos calor, prolonga la vida útil de la batería y reduce el consumo de energía.

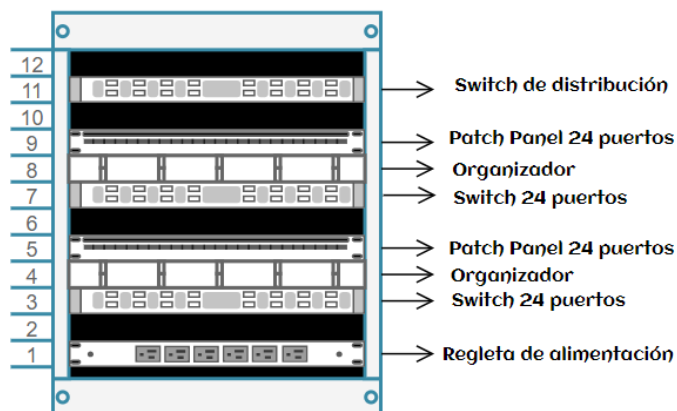
El modelo jerárquico de red se compone de tres capas que son: el núcleo, distribución y acceso, es por ello que se recomienda un switch de distribución robusto administrable con la finalidad que la red se encuentre utilizable durante las etapas de mantenimiento o cuando exista errores de software o hardware. Igualmente, por medio del modelo jerárquico se obtiene redundancia, escalabilidad, confiabilidad y seguridad.

Al tratarse de una red pequeña y que el área es menor a 100m² se sugiere utilizar un gabinete de pared de 12 unidades como indica la norma TIA/EIA-569-A, el gabinete alojara una regleta de alimentación de 8 tomas, un switch de distribución, dos switches de 24 puertos, dos

organizadores y dos Patch panel de 24 puertos. Se considera dos conmutadores de 24 puertos debido a la cantidad de usuarios que estarán conectados, asimismo por la facilidad de mantenimiento y por precaución si se llega a dañar un switch.

Figura 61

Distribución del gabinete



Nota. La figura muestra la distribución del gabinete con los equipos de red.

Diseño del Proyecto

La planificación del laboratorio de ciberdefensa se desarrolla para la Escuela de Comunicaciones en el primer piso del edificio de los laboratorios, exactamente en el aula “CBOS JACINTO O. CORTEZ J.”

Figura 62

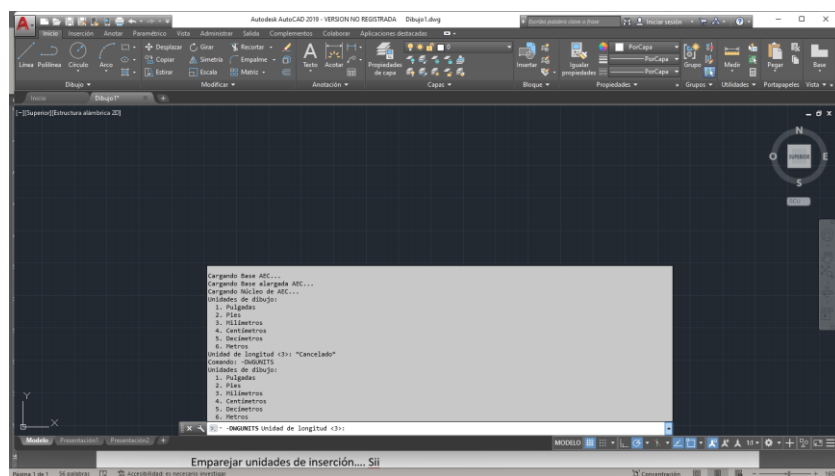
Ubicación del laboratorio



Nota. La figura muestra la ubicación del futuro laboratorio de ciberdefensa.

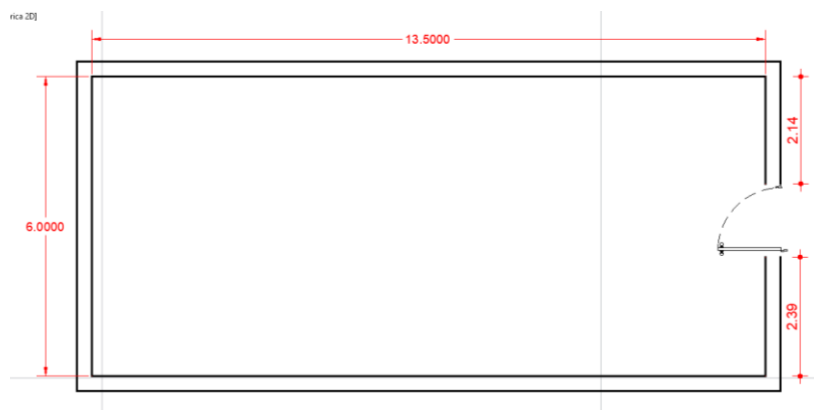
A continuación, para el levantamiento de información se realiza las mediciones del lugar donde se quiere implementar el laboratorio, se tiene como área de trabajo 81m^2 , posteriormente con la ayuda de AutoCAD, software de diseño que permite la creación y edición de planos, se realiza el boceto del laboratorio con los equipos, escritorios, equipos de red y el esquema del cableado estructurado.

En AutoCAD se inicia con la configuración de unidades de longitud a través del comando "DWGUNITS", este comando permite realizar la conversión de unidades imperiales a unidades métricas.

Figura 63*Conversión de unidades*

Nota. La figura muestra la inicialización de AutoCAD para el diseño del laboratorio de ciberdefensa.

Por organización el diseño se realiza mediante capas, a las cuales se les designa nombres que describen su contenido, en la capa “Muros” se realiza las paredes del laboratorio, con la ayuda del comando “LÍNEA” y el comando “DESFASE”, el aula mide 13.500 metros de largo por 6 metros de ancho, en la figura 64 se visualiza las 4 paredes del laboratorio con su respectiva puerta.

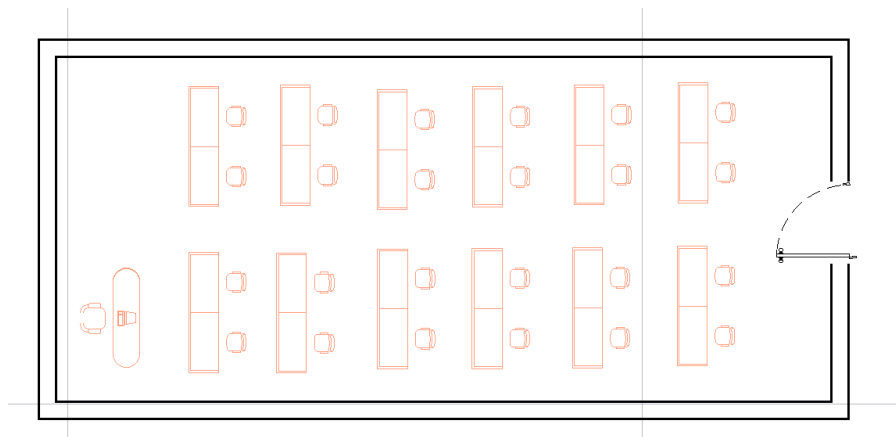
Figura 64*Área de trabajo*

Nota. La figura muestra el diseño de las paredes del futuro laboratorio de ciberdefensa.

En la capa “inmobiliario” se diseñan los escritorios que servirán de soporte a los computadores, se sitúa 25 escritorios, 12 computadores por cada ala y uno para el docente.

Figura 65

Diseño de los escritorios

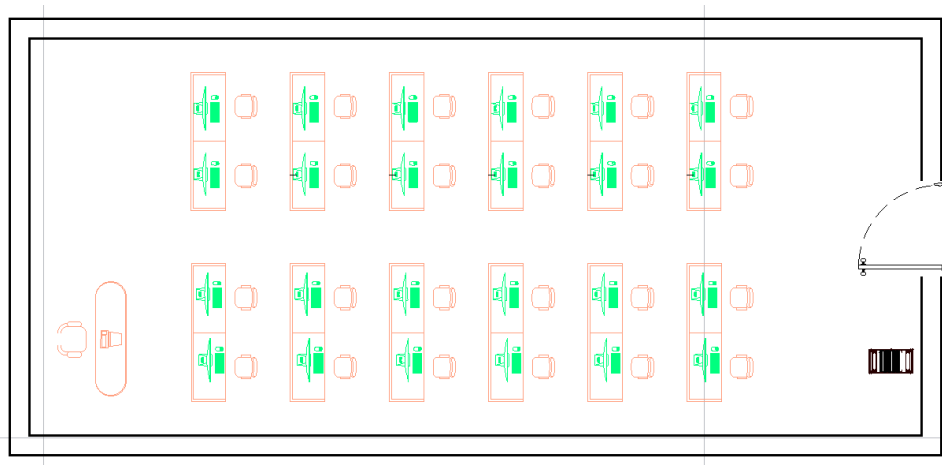


Nota. La figura muestra la ubicación de los escritorios.

En la capa “Hardware” se grafica los computadores sobre los escritorios los mismos que servirán para que los alumnos realicen sus prácticas, en la capa “Rack” se diseña el gabinete.

Figura 66

Ubicación de los computadores

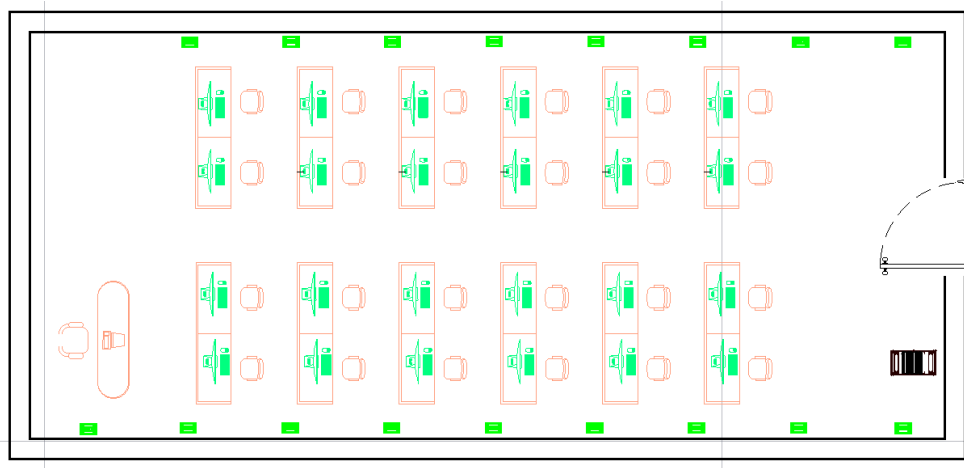


Nota. La figura muestra la ubicación de los computadores.

En la figura 67 se visualiza un total de 17 puntos de red dobles, este diseño se lo realiza en la capa “Faceplate”, la distancia entre cada faceplate es de 1,50 metros y están ubicados a una altura de 40 cm del piso 13 puntos de red lo ocupan las computadoras y 4 puntos de red están de reserva.

Figura 67

Puntos de red dobles

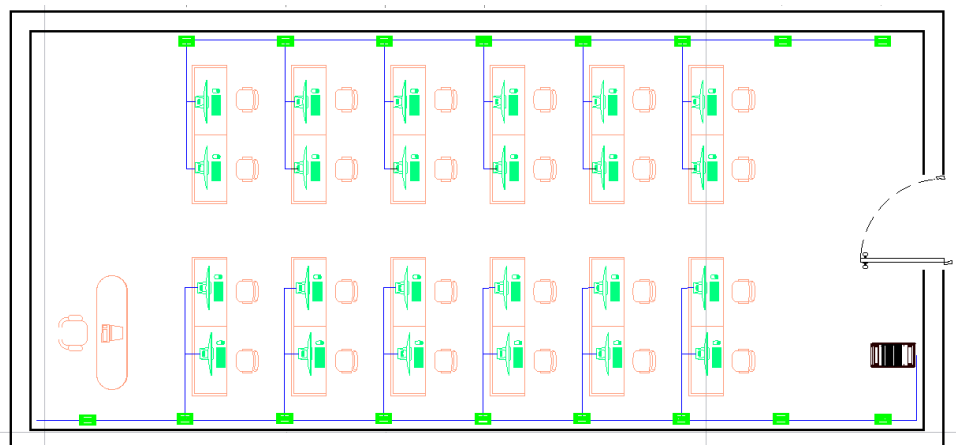


Nota. La figura muestra la ubicación de los puntos de red.

En la figura 68 se visualiza la capa de “Cableado”, en esta etapa se diseña el tendido del cable de red que es representado por una línea azul, 16 cables UTP pasan por el ala norte y 18 cables UTP en el ala sur, se utiliza la topología estrella por los beneficios que esta ofrece como son: añadir nuevos dispositivos, mayor seguridad, rápida configuración y mantenimiento, beneficios que son amparados en la norma EIA/TIA 568-B.

Figura 68

Tendido del cable de red.

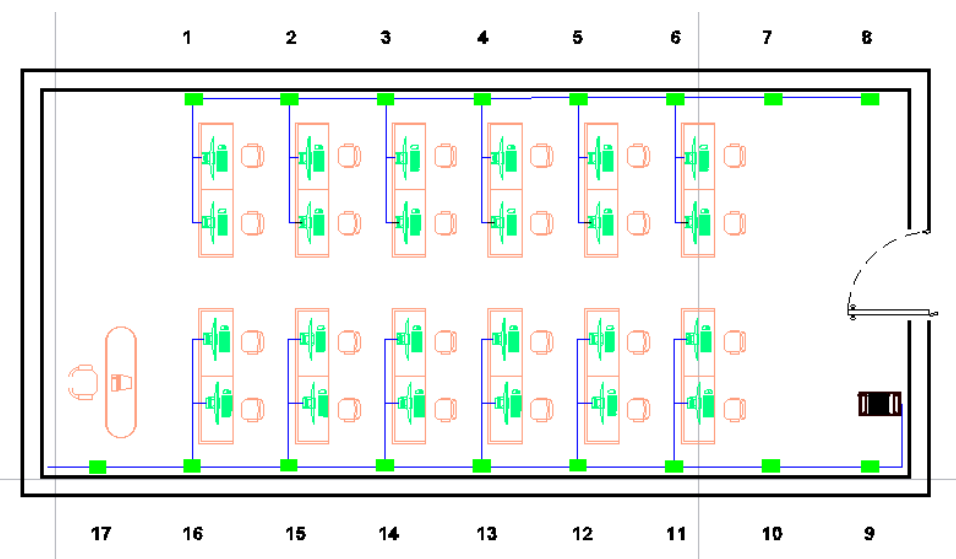


Nota. La figura muestra el tendido del cable de red.

Para simplificar la administración se ha enumerado los faceplate y de esta manera se obtiene un mejor control e identificación de los puntos de red, en la figura 69 se observa el orden que están enumerados.

Figura 69

Puntos de red



Nota. La figura muestra la identificación de los faceplate que se lo hace por medio de numeración.

En base a la norma TIA/EIA 569A que hace referencia a las rutas de cableado horizontal, se sugiere utilizar rutas perimetrales (canaletas) porque ayudan a llegar hasta el lugar de trabajo, por la cantidad de cable UTP que se utilizará se recomienda usar canaletas plásticas de 60 x 40 como lo muestra la figura 50, así mismo en base a la norma anteriormente indicada se aconseja llenar las canaletas del 40% al 60% de su capacidad total, con el fin de evitar calentamiento de los cables por contacto.

Figura 70

Cantidad de cables

Guía para seleccionar canaletas de superficie

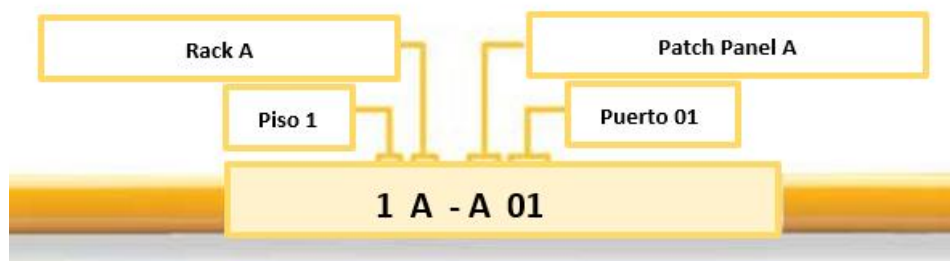
ALTURA (mm)	DIMENSIONES (mm)	Cantidad de cables que acepta según tipo				Comunicación		Fibra Óptica		
		12 AWG	14 AWG	16 AWG	18 AWG	UTP	RS56	RG 58	Fibra Óptica	Fibra Óptica Multiplex
10	10x10	2	2	3	3	1	1	1	1	
7	13x7	2	2	3	3	1				
12	20x12	4	5	11	12	3	4	3	7	1
	32x12	6	8	18	20	5	6	3	11	2
13	32x12 cd	6	8	16	18	4	5	3	10	2
	60x13	4	8	12	14	4	4	4	8	4
16	60x16 cd	13	28	35	38	10	11	8	26	4
20	20x20	8	9	15	17	6	7	4	12	2
25	25x25	9	11	20	20	8	9	5	18	3
	40x25	17	26	35	49	13	14	8	29	4
	40x25 cd	16	26	36	46	12	13	8	27	4
40	40x40	35	49	71	77	20	21	13	46	7
	60x40	66	81	120	149	30	31	20	70	10
45	60x40 cd	61	76	117	142	28	29	20	68	10
	100x45	105	140	220	240	50	51	32	116	17

Nota. La figura muestra la cantidad de cables que puede ir en las canaletas según sus dimensiones. Recuperado de (FCM, 2021)

La norma internacional ISO/IEC 14763-1 y la norma europea EN 50174-1 dan libre albedrío al técnico para realizar los trabajos de etiquetado, pero el estándar ANSI/TIA/EIA 606C establece las normas de administración e identificación de un sistema de cableado estructurado, es por ello que se recomienda utilizar el formato de etiquetado establecido en dicho estándar, en la figura 71 se visualiza el formato de etiquetado para el faceplate.

Figura 71

Formato de etiquetado Faceplate



Nota. La figura muestra el etiquetado que va en el faceplate, en donde 1 representa el piso, la primera letra identifica al rack, la segunda letra representa al Patch panel y el último número el puerto.

En la tabla 9 se muestra el listado de etiquetado de los faceplate del laboratorio y en la figura 72 se representa un ejemplo del etiquetado ya impreso.

Tabla 9

Etiquetado del faceplate

Etiquetado faceplate					
Número del Piso	Rack	Patch Panel	Número del Puerto	Ejemplo	Significado
1	A	A	01	1A-A01	Piso 1, Rack A, Patch Panel A Puerto 01
1	A	A	02	1A-A02	Piso 1, Rack A, Patch Panel A Puerto 02
1	A	A	03	1A-A03	Piso 1, Rack A, Patch Panel A Puerto 03

Número del Piso	Rack	Patch Panel	Número del Puerto	Ejemplo	Significado
1	A	A	04	1A-A04	Piso 1, Rack A, Patch Panel A Puerto 04
1	A	A	05	1A-A05	Piso 1, Rack A, Patch Panel A Puerto 05
1	A	A	06	1A-A06	Piso 1, Rack A, Patch Panel A Puerto 06
1	A	A	07	1A-A07	Piso 1, Rack A, Patch Panel A Puerto 07
1	A	A	08	1A-A08	Piso 1, Rack A, Patch Panel A Puerto 08
1	A	A	09	1A-A09	Piso 1, Rack A, Patch Panel A Puerto 09
1	A	A	10	1A-A10	Piso 1, Rack A, Patch Panel A Puerto 10
1	A	A	11	1A-A11	Piso 1, Rack A, Patch Panel A Puerto 11
1	A	A	12	1A-A12	Piso 1, Rack A, Patch Panel A Puerto 12
1	A	A	13	1A-A13	Piso 1, Rack A, Patch Panel A Puerto 13
1	A	A	14	1A-A14	Piso 1, Rack A, Patch Panel A Puerto 14

Número del Piso	Rack	Patch Panel	Número del Puerto	Ejemplo	Significado
1	A	A	15	1A-A15	Piso 1, Rack A, Patch Panel A Puerto 15
1	A	A	16	1A-A16	Piso 1, Rack A, Patch Panel A Puerto 16
1	A	A	17	1A-A17	Piso 1, Rack A, Patch Panel A Puerto 17
1	A	A	18	1A-A18	Piso 1, Rack A, Patch Panel A Puerto 18
1	A	A	19	1A-A19	Piso 1, Rack A, Patch Panel A Puerto 19
1	A	A	20	1A-A20	Piso 1, Rack A, Patch Panel A Puerto 20
1	A	A	21	1A-A21	Piso 1, Rack A, Patch Panel A Puerto 21
1	A	A	22	1A-A22	Piso 1, Rack A, Patch Panel A Puerto 22
1	A	A	23	1A-A23	Piso 1, Rack A, Patch Panel A Puerto 23
1	A	A	24	1A-A24	Piso 1, Rack A, Patch Panel A Puerto 24
1	A	B	01	1A-B01	Piso 1, Rack A, Patch Panel B Puerto 01

Número del Piso	Rack	Patch Panel	Número del Puerto	Ejemplo	Significado
1	A	B	02	1A-B02	Piso 1, Rack A, Patch Panel B Puerto 02
1	A	B	03	1A-B03	Piso 1, Rack A, Patch Panel B Puerto 03
1	A	B	04	1A-B04	Piso 1, Rack A, Patch Panel B Puerto 04
1	A	B	05	1A-B05	Piso 1, Rack A, Patch Panel B Puerto 05
1	A	B	06	1A-B06	Piso 1, Rack A, Patch Panel B Puerto 06
1	A	B	07	1A-B07	Piso 1, Rack A, Patch Panel B Puerto 07
1	A	B	08	1A-B08	Piso 1, Rack A, Patch Panel B Puerto 08
1	A	B	09	1A-B09	Piso 1, Rack A, Patch Panel B Puerto 09
1	A	B	10	1A-B10	Piso 1, Rack A, Patch Panel B Puerto 10

Nota. La tabla representa el etiquetado de todos los faceplate.

Figura 72

Etiquetado faceplate



Nota. La figura muestra un ejemplo de etiquetado en el faceplate.

El etiquetado en el Patch panel se basa en el formato que se puede observar en la figura 73, en la tabla 10 se detalla el etiquetado de cada puerto del Patch panel y en la figura 74 se visualiza un ejemplo de cómo quedaría el etiquetado ya impreso en el Patch panel.

Figura 73

Formato de etiquetado Patch Panel



Nota. La figura muestra el etiquetado que va en el Patch panel, en donde el primero número representa el laboratorio, el siguiente número identifica a la toma y el último número representa al puerto.

Tabla 10*Etiqueta para identificación del panel de conexiones*

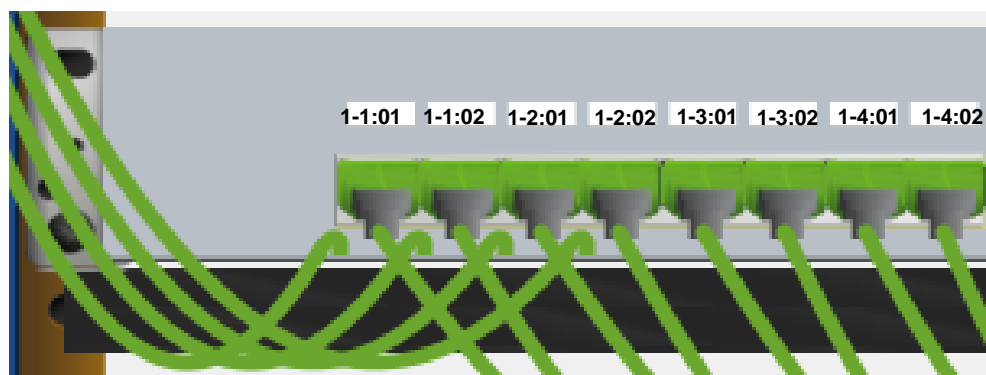
Etiquetado del Patch Panel				
N.º	Dependencia	N.º Toma	Nombre Etiqueta	Significado
1		1	1-1:01	Laboratorio, Toma 1 Puerto 01.
2		1	1-1:02	Laboratorio, Toma 1 Puerto 02.
3		2	1-2:01	Laboratorio, Toma 2 Puerto 01.
4		2	1-2:02	Laboratorio, Toma 2 Puerto 02.
5		3	1-3:01	Laboratorio, Toma 3 Puerto 01.
6		3	1-3:02	Laboratorio, Toma 3 Puerto 02.
7		4	1-4:01	Laboratorio, Toma 4 Puerto 01.
8		4	1-4:02	Laboratorio, Toma 4 Puerto 02.
9	Laboratorio	5	1-5:01	Laboratorio, Toma 5 Puerto 01.
10	de	5	1-5:02	Laboratorio, Toma 5 Puerto 02.
11	Ciberdefensa	6	1-6:01	Laboratorio, Toma 6 Puerto 01.
12		6	1-6:02	Laboratorio, Toma 6 Puerto 02.
13		7	1-7:01	Laboratorio, Toma 7 Puerto 01.
14		7	1-7:02	Laboratorio, Toma 7 Puerto 02.
15		8	1-8:01	Laboratorio, Toma 8 Puerto 01.
16		8	1-8:02	Laboratorio, Toma 8 Puerto 02.
17		9	1-9:01	Laboratorio, Toma 9 Puerto 01.
18		9	1-9:02	Laboratorio, Toma 9 Puerto 02.
19		10	1-10:01	Laboratorio, Toma 10 Puerto 01.
20		10	1-10:02	Laboratorio, Toma 10 Puerto 02.

N.º	Dependencia	N.º Toma	Nombre Etiqueta	Significado
21		11	1-11:01	Laboratorio, Toma 11 Puerto 01.
22		11	1-11:02	Laboratorio, Toma 11 Puerto 02.
23		12	1-12:01	Laboratorio, Toma 12 Puerto 01.
24		12	1-12:02	Laboratorio, Toma 12 Puerto 02.
25		13	1-13:01	Laboratorio, Toma 13 Puerto 01.
26		13	1-13:02	Laboratorio, Toma 13 Puerto 02.
27		14	1-14:01	Laboratorio, Toma 14 Puerto 01.
28		14	1-14:02	Laboratorio, Toma 14 Puerto 02.
29		15	1-15:01	Laboratorio, Toma 15 Puerto 01.
30		15	1-15:02	Laboratorio, Toma 15 Puerto 02.
31		16	1-16:01	Laboratorio, Toma 16 Puerto 01.
32		16	1-16:02	Laboratorio, Toma 16 Puerto 02.
33		17	1-17:01	Laboratorio, Toma 17 Puerto 01.
34		17	1-17:02	Laboratorio, Toma 17 Puerto 02.

Nota. La tabla representa el etiquetado en el patch panel.

Figura 74

Etiquetado en el Patch panel



Nota. La figura muestra un ejemplo de etiquetado en el Patch panel.

En la tabla 11 se detalla el etiquetado de un extremo del cable, el extremo que va al patch panel y en la tabla 12 se especifica el etiquetado del otro extremo del cable, el extremo que va al faceplate.

Tabla 11

Etiquetado de un extremo del cable que va al Patch panel

Etiquetado de un extremo del cable				
N.º	Dependencia	N.º Toma	Nombre Etiqueta	Significado
1		1	1A-A:01/1- 1:01	Rack A, Patch Panel A Puerto 01, Laboratorio, Toma 1 Puerto 01.
2		1	1A-A:02/1- 1:02	Rack A, Patch Panel A Puerto 02, Laboratorio, Toma 1 Puerto 02.
3		2	1A-A:03/1- 2:01	Rack A, Patch Panel A Puerto 03, Laboratorio, Toma 2 Puerto 01.
4	Laboratorio	2	1A-A:04/1- 2:02	Rack A, Patch Panel A Puerto 04, Laboratorio, Toma 2 Puerto 02.
5	de Ciberdefensa	3	1A-A:05/1- 3:01	Rack A, Patch Panel A Puerto 05, Laboratorio, Toma 3 Puerto 01.
6		3	1A-A:06/1- 3:02	Rack A, Patch Panel A Puerto 06, Laboratorio, Toma 3 Puerto 02.
7		4	1A-A:07/1- 4.01	Rack A, Patch Panel A Puerto 07, Laboratorio, Toma 4 Puerto 01.
8		4	1A-A:08/1- 4.02	Rack A, Patch Panel A Puerto 08, Laboratorio, Toma 4 Puerto 02.

N.º	N.º Toma	Nombre Etiqueta	Significado
9	5	1A-A:09/1- 5.01	Rack A, Patch Panel A Puerto 09, Laboratorio, Toma 5 Puerto 01.
10	5	1A-A:10/1- 5.02	Rack A, Patch Panel A Puerto 10, Laboratorio, Toma 5 Puerto 02.
11	6	1A-A:11/1- 6.01	Rack A, Patch Panel A Puerto 11, Laboratorio, Toma 6 Puerto 01.
12	6	1A-A:12/1- 6.02	Rack A, Patch Panel A Puerto 12, Laboratorio, Toma 6 Puerto 02.
13	7	1A-A:13/1- 7.01	Rack A, Patch Panel A Puerto 13, Laboratorio, Toma 7 Puerto 01.
14	7	1A-A:14/1- 7.02	Rack A, Patch Panel A Puerto 14, Laboratorio, Toma 7 Puerto 02.
15	8	1A-A:15/1- 8.01	Rack A, Patch Panel A Puerto 15, Laboratorio, Toma 8 Puerto 01.
16	8	1A-A:16/1- 8.02	Rack A, Patch Panel A Puerto 16, Laboratorio, Toma 8 Puerto 02.
17	9	1A-A:17/1- 9.01	Rack A, Patch Panel A Puerto 17, Laboratorio, Toma 9 Puerto 01
18	9	1A-A:18/1- 9.02	Rack A, Patch Panel A Puerto 18, Laboratorio, Toma 9 Puerto 02
19	10	1A-A:19/1- 10.01	Rack A, Patch Panel A Puerto 19, Laboratorio, Toma 10 Puerto 01.

N.º	Dependencia	N.º Toma	Nombre Etiqueta	Significado
20		10	1A-A:20/1- 10.02	Rack A, Patch Panel A Puerto 20, Laboratorio, Toma 10 Puerto 02
21		11	1A-A:21/1- 11.01	Rack A, Patch Panel A Puerto 21, Laboratorio, Toma 11 Puerto 01
22		11	1A-A:22/1- 11.02	Rack A, Patch Panel A Puerto 22, Laboratorio, Toma 11 Puerto 02.
23		12	1A-A:23/1- 12.01	Rack A, Patch Panel A Puerto 23, Laboratorio, Toma 12 Puerto 01
24		12	1A-A:24/1- 12.02	Rack A, Patch Panel A Puerto 24, Laboratorio, Toma 12 Puerto 02
25		13	1A-B:01/1- 13.01	Rack A, Patch Panel B Puerto 01, Laboratorio, Toma 13 Puerto 1.
26		13	1A-B:02/1- 13.02	Rack A, Patch Panel B Puerto 02, Laboratorio, Toma 13 Puerto 2
27		14	1A-B:03/1- 14.01	Rack A, Patch Panel B Puerto 03, Laboratorio, Toma 14 Puerto 1
28		14	1A-B:04/1- 14.02	Rack A, Patch Panel B Puerto 04, Laboratorio, Toma 14 Puerto 2.
29		15	1A-B:05/1- 15.01	Rack A, Patch Panel B Puerto 05, Laboratorio, Toma 15 Puerto 1
30		15	1A-B:06/1- 15.02	Rack A, Patch Panel B Puerto 06, Laboratorio, Toma 15 Puerto 2

N.º	Dependencia	N.º Toma	Nombre Etiqueta	Significado
31		16	1A-B:07/1- 16.01	Rack A, Patch Panel B Puerto 07, Laboratorio, Toma 16 Puerto 1.
32		16	1A-B:08/1- 16.02	Rack A, Patch Panel B Puerto 08, Laboratorio, Toma 16 Puerto 2
33		17	1A-B:09/1- 17.01	Rack A, Patch Panel B Puerto 09, Laboratorio, Toma 17 Puerto 1
34		17	1A-B:10/1- 17.02	Rack A, Patch Panel B Puerto 10, Laboratorio, Toma 17 Puerto 2

Nota. La tabla representa el etiquetado de un extremo del cable que va al Patch panel.

Tabla 12

Etiquetado del otro extremo del cable que va al faceplate

Etiquetado del otro extremo del cable				
N.º	Dependencia	N.º Toma	Nombre Etiqueta	Significado
1		1	1-1:01/1A- A:01	Laboratorio, Toma 1 Puerto 01. Rack A, Patch Panel A Puerto 01
2	Laboratorio de	1	1-1:02/1A- A:02	Laboratorio, Toma 1 Puerto 02. Rack A, Patch Panel A Puerto 02
3	Ciberdefensa	2	1-2:01/1A- A:03	Laboratorio, Toma 2 Puerto 01. Rack A, Patch Panel A Puerto 03
4		2	1-2:02/1A- A:04	Laboratorio, Toma 2 Puerto 02. Rack A, Patch Panel A Puerto 04

N.º	N.º Toma	Nombre Etiqueta	Significado
5	3	1-3:01 /1A- A:05	Laboratorio, Toma 3 Puerto 01. Rack A, Patch Panel A Puerto 05
6	3	1-3:02/1A- A:06	Laboratorio, Toma 3 Puerto 02. Rack A, Patch Panel A Puerto 06
7	4	1-4.01/1A- A:07	Laboratorio, Toma 4 Puerto 01. Rack A, Patch Panel A Puerto 07
8	4	1-4.02/1A- A:08	Laboratorio, Toma 4 Puerto 02. Rack A, Patch Panel A Puerto 08
9	5	1-5.01/1A- A:09	Laboratorio, Toma 5 Puerto 01. Rack A, Patch Panel A Puerto 09
10	5	1-5.02/1A- A:10	Laboratorio, Toma 5 Puerto 02. Rack A, Patch Panel A Puerto 10
11	6	1-6.01/1A- A:11	Laboratorio, Toma 6 Puerto 01. Rack A, Patch Panel A Puerto 11
12	6	1-6.02/1A- A:12	Laboratorio, Toma 6 Puerto 02. Rack A, Patch Panel A Puerto 12
13	7	1-7.01/1A- A:13	Laboratorio, Toma 7 Puerto 01. Rack A, Patch Panel A Puerto 13
14	7	1-7.02/1A- A:14	Laboratorio, Toma 7 Puerto 02. Rack A, Patch Panel A Puerto 14
15	8	1-8.01/1A- A:15	Laboratorio, Toma 8 Puerto 01. Rack A, Patch Panel A Puerto 15

N.º	N.º Toma	Nombre Etiqueta	Significado
16	8	1-8.02/1A- A:16	Laboratorio, Toma 8 Puerto 02. Rack A, Patch Panel A Puerto 16
17	9	1-9.01/1A- A:17	Laboratorio, Toma 9 Puerto 01. Rack A, Patch Panel A Puerto 17
18	9	1-9.02/1A- A18	Laboratorio, Toma 9 Puerto 02. Rack A, Patch Panel A Puerto 18
19	10	1-10.01/1A- A:19	Laboratorio, Toma 10 Puerto 01. Rack A, Patch Panel A Puerto 19
20	10	1-10.02/1A- A:20	Laboratorio, Toma 10 Puerto 02. Rack A, Patch Panel A Puerto 20
21	11	1-11.01/1A- A:21	Laboratorio, Toma 11 Puerto 01. Rack A, Patch Panel A Puerto 21
22	11	1-11.02/1A- A:22	Laboratorio, Toma 11 Puerto 02. Rack A, Patch Panel A Puerto 22
23	12	1-12.01/1A- A:23	Laboratorio, Toma 12 Puerto 01. Rack A, Patch Panel A Puerto 23
24	12	1-12.02/1A- A24	Laboratorio, Toma 12 Puerto 02. Rack A, Patch Panel A Puerto 24
25	13	1-13.01/1A- B:01	Laboratorio, Toma 13 Puerto 1. Rack A, Patch Panel B Puerto 01
26	13	1-13.02/1A- B:02	Laboratorio, Toma 13 Puerto 2. Rack A, Patch Panel B Puerto 02

N.°	Dependencia	N.° Toma	Nombre Etiqueta	Significado
27		14	1-14.01/1A- B:03	Laboratorio, Toma 14 Puerto 1. Rack A, Patch Panel B Puerto 03
28		14	1-14.02/1A- B:04	Laboratorio, Toma 14 Puerto 2. Rack A, Patch Panel B Puerto 04
29		15	1-15.01/1A- B:05	Laboratorio, Toma 15 Puerto 1. Rack A, Patch Panel B Puerto 05
30		15	1-15.02/1A- B:06	Laboratorio, Toma 15 Puerto 2. Rack A, Patch Panel B Puerto 06
31		16	1-16.01/1A- B:07	Laboratorio, Toma 16 Puerto 1. Rack A, Patch Panel B Puerto 07
32		16	1-16.02/1A- B:08	Laboratorio, Toma 16 Puerto 2. Rack A, Patch Panel B Puerto 08
33		17	1-17.01/1A- B:09	Laboratorio, Toma 17 Puerto 1. Rack A, Patch Panel B Puerto 09
34		17	1-17.02/1A- B:10	Laboratorio, Toma 17 Puerto 2. Rack A, Patch Panel B Puerto 10

Nota. En la tabla se observa el etiquetado del otro extremo del cable que va al Patch panel

Instructivo para la instalación del cableado estructurado

De acuerdo al diseño realizado del cableado estructurado se elaboró el instructivo el mismo que contiene información del proceso para la implementación en lo que corresponde al cableado, canaletas, equipos de red y sistemas operativos.

En el instructivo se especifica la instalación de las máquinas virtuales Kali Linux y Metasploit, adicionalmente se realizó las guías de laboratorio con pruebas como es escaneo de

vulnerabilidades por medio de la herramienta nikto, escaneo de vulnerabilidades en aplicaciones web a través de la herramienta ZAP, escaneo de redes, puertos y dispositivos por medio de la herramienta nmap, estos detalles se encuentran en el anexo A.

Una vez finalizado el instructivo se realizó la entrega formal al señor Director de la Escuela de Comunicaciones mi Tcrn de E.M Juan Carlos Ludeña a través de actas de entrega recepción las mismas que se encuentran al final del instructivo.

Capítulo IV

Conclusiones y Recomendaciones

Conclusiones

- Se realizó un análisis comparativo técnico de software y hardware para determinar los programas y equipos idóneos para el laboratorio de ciberdefensa los cuales servirán como base para el aprendizaje de los alumnos que desarrollen el curso de ciberdefensa.
- Se elaboró el despliegue del cableado estructurado basándose en los estándares TIA/EIA-568-B, TIA/EIA-569-A, TIA/EIA-606-A, el cableado horizontal empieza en el gabinete de telecomunicaciones y termina en cada computadora que es el área de trabajo de los estudiantes, es importante recalcar que esta distancia no debe ser mayor de los 90 metros, existe un margen de sistema de 10 metros.
- El laboratorio de ciberdefensa se ha planificado para 32 puntos de red de los cuales 8 puntos de red son de reserva es decir se puede ubicar más equipos conforme a la necesidad que tenga la Escuela de Comunicaciones.
- Se elaboró un instructivo el mismo que contiene todo el procedimiento técnico para la implementación de cableado estructurado, equipos y sistemas operativos el mismo que servirá como documento informativo al momento de dar inicio con la implementación del laboratorio de ciberdefensa.

Recomendaciones

- Para la instalación se recomienda cumplir con los parámetros detallados mismos que cumplen la normativa internacional puesto que de esta manera se garantizan un buen funcionamiento del laboratorio a la par de un buen cuidado y mantenimiento.
- Tener en cuenta a más personal militar al curso de ciberdefensa en vista que el laboratorio cuenta con 8 puntos de red de reserva que tranquilamente pueden ser utilizados por más alumnos aprovechando los recursos que presenta el laboratorio.
- Se sugiere que para las diferentes prácticas se implemente un servidor con diferentes máquinas virtuales las cuáles serán las vulneradas y estarán conectadas mediante una VPN así cada alumno tendrá un objetivo diferente.
- Realizar la planificación para la implementación de un data center que sirva de soporte para los laboratorios de la Escuela de Comunicaciones.

Bibliografía

Acervolima. (2021). *Ventajas y desventajas de la topología hpiibrida*.

<https://es.acervolima.com/ventajas-y-desventajas-de-la-topologia-hibrida/>

Acurio Del Pino, S. (2016). *Delitos informáticos: generalidades*. 26.

Alarcón, L. F. (2018). *Capítulo 7 TIA/EIA-607-A Requerimientos para Aterrizaje y Conexión de Sistemas de Telecomunicaciones de Edificios Comerciales*.

<https://docplayer.es/98575477-Capitulo-7-tia-eia-607-a-requerimientos-para-aterrizaje-y-conexion-de-sistemas-de-telecomunicaciones-de-edificios-comerciales.html>

Aleph. (19 de Marzo de 2021). *¿Qué es un spyware adware y spam?* <https://aleph.org.mx/que-es-un-spyware-adware-y-spam>

Altube, R. (12 de Noviembre de 2021). <https://openwebinars.net/blog/parrot-os-que-es-y-caracteristicas-principales/>

Altube, R. (5 de Noviembre de 2021). *Kali Linux: Qué es y características principales*.

<https://openwebinars.net/blog/kali-linux-que-es-y-caracteristicas-principales/>

Altube, R. (6 de Diciembre de 2021). *Kali vs Parrot, cuál es mejor en Ciberseguridad*.

<https://openwebinars.net/blog/kali-vs-parrot-cual-es-mejor-en-ciberseguridad/>

Álvarez, P. (26 de Marzo de 2021). *IPFire: La distribución de Linux perfecta para crear*

Cortafuegos e implementar Firewall. <https://ciberninjas.com/so-linux-ipfire-redes/>

ANSI. (2022). *American National Standards Institute*. <https://www.ansi.org/>

Apuntesjulio. (12 de Septiembre de 2022). *Topologías de red*.

<https://apuntesjulio.com/topologias-de-red/>

Arcadio. (2019). *Subredes VLSM paso a paso*. <https://arcadio.gq/subredes-vlsm-paso-a-paso.html>

Áreatecnológica. (2022). *Redes Informáticas*. <https://www.areatecnologia.com/redes-informaticas.htm>

Arguello, F. (14 de Diciembre de 2022). *¿Qué es PoE o Power Over Ethernet?* .

<https://www.infoteknico.com/que-es-poe/>

Aruba. (2018). *¿Qué es PoE de alta potencia?*

https://www.arubanetworks.com/assets/_es/tg/TB_High-Power-PoE.pdf

Atlas. (01 de Julio de 2019). *La norma EIA*. [https://atlascomunicaciones.com/norma-](https://atlascomunicaciones.com/norma-eia/#:~:text=La%20Alianza%20de%20Industrias%20Electr%C3%B3nicas,alta%20tecnol)

[eia/#:~:text=La%20Alianza%20de%20Industrias%20Electr%C3%B3nicas,alta%20tecnol](https://atlascomunicaciones.com/norma-eia/#:~:text=La%20Alianza%20de%20Industrias%20Electr%C3%B3nicas,alta%20tecnol)
[og%C3%ADa%20de%20Estados%20Unidos.](https://atlascomunicaciones.com/norma-eia/#:~:text=La%20Alianza%20de%20Industrias%20Electr%C3%B3nicas,alta%20tecnol)

Atlassian. (2022). *Niveles de gravedad de las incidencias de seguridad*.

<https://www.atlassian.com/es/trust/security/security-severity-levels>

Ávila, F. (17 de Enero de 2020). *Conoce los mejores sistemas operativos para hacking ético*.

<http://www.disoftin.com/2020/01/conoce-los-mejores-sistemas-operativos.html>

AWS. (2023). *¿Qué es el enrutamiento?* [https://aws.amazon.com/es/what-](https://aws.amazon.com/es/what-is/routing/#:~:text=Un%20protocolo%20de%20enrutamiento%20es,de%20puerta%20de)

[is/routing/#:~:text=Un%20protocolo%20de%20enrutamiento%20es,de%20puerta%20de](https://aws.amazon.com/es/what-is/routing/#:~:text=Un%20protocolo%20de%20enrutamiento%20es,de%20puerta%20de)
[%20enlace%20exterior.](https://aws.amazon.com/es/what-is/routing/#:~:text=Un%20protocolo%20de%20enrutamiento%20es,de%20puerta%20de)

Bello, E. (20 de Octubre de 2022). *Conoce las herramientas de ciberseguridad para proteger tu*

empresa. <https://www.iebschool.com/blog/herramientas-ciberseguridad-digital-business/>

beron, S. (27 de Agosto de 2020). *Calcular longitud de cable horizontal*.

<https://soportelan.com/2020/08/26/calcular-longitud-de-cable-horizontal/>

Bhardwaj, R. (9 de Septiembre de 2020). *Modos EtherChannel: modo PAGP, modos LACP y*

modo activado. <https://ipwithease.com/etherchannel-modes-pagp-lACP-and-on/>

Bodnar, D. (29 de Octubre de 2020). *Ingeniería social y cómo protegerse*.

<https://www.avast.com/es-es/c-social-engineering#topic-3>

bracamontedatcenters. (2022). *Subsistema de Cableado Horizontal*.

<http://bracamontedatcenters.weebly.com/cableado-horizontal.html>

Btnet. (2007). *TIA/EIA-568-B*.

<https://bibdigital.epn.edu.ec/bitstream/15000/9268/5/Cap%204.pdf>

CAD & LAN. (17 de Agosto de 2020). *Cableado estructurado: definición, elementos y tipologías.*

<https://www.cadlan.com/noticias/todo-lo-que-debes-saber-sobre-el-cableado-estructurado/>

Cámara Valencia. (12 de Noviembre de 2018). *Qué es un ciberataque y qué tipos existen.*

<https://ticnegocios.camaravalencia.com/servicios/tendencias/que-es-un-ciberataque-y-que-tipos-existen/#Malware>

Cardenas, M. O. (31 de Agosto de 2022). *¿Cómo elegir el mejor switch de red para su*

proyecto? <https://tecnosinergia.zendesk.com/hc/es/articles/8109824869403--C%C3%B3mo-elegir-el-mejor-switch-de-red-para-su-proyecto->

Cardona Zapata, D. E., & Sánchez Piedrahita, A. M. (2019). *Diseño de un Laboratorio de Seguridad de la Información para el Tecnológico de Antioquia Tesis de Ingeniería Tecnológico de Antioquia.*

Caser. (2017). *¿Qué es un ciberataque y qué tipos hay?* <https://www.caser.es/seguros-empresas/articulos/que-es-un-ciberataque-y-tipos>

Castellnou, R. (10 de Mayo de 2021). *Las herramientas de seguridad informática que protegerán tu empresa.* <https://www.captio.net/blog/herramientas-seguridad-informatica>

Castillo, J. A. (12 de Septiembre de 2020). *Cable par trenzado – Características, construcción, tipos y categorías.* https://www.profesionalreview.com/2020/09/12/cable-par-trenzado-caracteristicas/#Categorias_de_cable_par_trenzado

CISCO. (2019). *Protocolos y comunicación de red.*

https://www.uv.mx/personal/angelperez/files/2019/02/CCNA_ITN_Ch3.pdf

CISCO. (Marzo de 2022). *¿Qué es la ciberseguridad?*

https://www.cisco.com/c/es_mx/products/security/what-is-cybersecurity.html#~:tipos-de-amenazas

Cisco. (Marzo de 2022). *Configuración de EtherChannel en Switches Catalyst.*

https://www.cisco.com/c/es_mx/support/docs/lan-switching/etherchannel/10024-6.html

Cisco. (2022). *Red de Área Metropolitana*.

http://ciscoredes.mex.tl/frameset.php?url=/1950700_MAN---RED-DE--REA-METROPOLITANA-.html

Citelia. (18 de Agosto de 2020). *Tipos de Fibra Óptica*. <https://citelia.es/blog/tipos-fibra-optica-internet/>

Cloudflare. (2022). *¿Qué es el modelo OSI?* <https://www.cloudflare.com/es-es/learning/ddos/glossary/open-systems-interconnection-model-osi/>

Cloudflare. (2022). *Firewall de nueva generación (NGFW) vs. firewall como servicio (FWaaS)*. <https://www.cloudflare.com/es-es/learning/cloud/ngfw-vs-fwaas/>

COCIBER. (2014). *Sobre Nosotros*. <https://cociber.cffaa.mil.ec/quienes-somos/>

Collado, E. (9 de Noviembre de 2020). *Cisco vPC (virtual Port Channel)*.

<https://www.eduardocollado.com/2020/11/09/cisco-vpc-virtual-port-channel/>

Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros. (19 de julio de 2019). *Gobierno de México*. <https://www.gob.mx/condufef/articulos/aguas-con-los-fraudes>

Consejo Argentino para las Relaciones Internacionales. (noviembre de 2013). *cari*.

https://www.cari.org.ar/pdf/ciberdefensa_riesgos_amenazas.pdf

Consejotecnologico. (6 de Marzo de 2019). *Las 10 mejores herramientas de hacking Wifi de Kali Linux*. <https://consejotecnologico.com/las-10-mejores-herramientas-de-hacking-wifi-de-kali-linux/>

Cristhian. (11 de Mayo de 2021). *Armario rack*. <https://conceptoabc.com/armario-rack/>

Cybersecurity. (22 de Mayo de 2022). *Alien Vault OSSIM*.

<https://cybersecurity.att.com/products/ossim>

Daga. (27 de Junio de 2020). *Face Plate*. <https://www.daga-sa.com/index.php/cat-cableado-estructurado/qst-0024/16-cableado-estructurado->

ESIC Business & Marketing School. (2020). Definición de la ciberseguridad y su riesgo. *ESIC*.

<https://www.novasec.co/blog/67-gestion-de-activos-de-informacion#:~:text=Un%20activo%20de%20informaci%C3%B3n%20en,por%20lo%20tanto%20debe%20proteger%E2%80%9D>.

f5.com. (2019). *¿Qué es la seguridad de las aplicaciones web?*

https://www.f5.com/es_es/services/resources/glossary/web-application-security

FCM. (11 de Octubre de 2021). *Canaletas de superficie y piso*.

<https://www.fcmsolutionsperu.com/blogs/noticias/canaletas-dexson>

Fernández, L. (09 de Enero de 2023). *Power over Ethernet: Qué es, cómo funciona y tipos de*

PoE. <https://www.redeszone.net/tutoriales/redes-cable/power-over-ethernet-poe-que-es/>

Fernández, Y. (2 de Junio de 2020). [https://www.xataka.com/basics/cual-es-la-diferencia-](https://www.xataka.com/basics/cual-es-la-diferencia-malware-virus-gusanos-spyware-troyanos-ransomware-etccetera)

[malware-virus-gusanos-spyware-troyanos-ransomware-etccetera](https://www.xataka.com/basics/cual-es-la-diferencia-malware-virus-gusanos-spyware-troyanos-ransomware-etccetera)

Fernández, Y. (2 de Junio de 2020). [https://www.xataka.com/basics/cual-es-la-diferencia-](https://www.xataka.com/basics/cual-es-la-diferencia-malware-virus-gusanos-spyware-troyanos-ransomware-etccetera)

[malware-virus-gusanos-spyware-troyanos-ransomware-etccetera](https://www.xataka.com/basics/cual-es-la-diferencia-malware-virus-gusanos-spyware-troyanos-ransomware-etccetera)

Fernández, Y. (30 de Junio de 2022). *Cable Coaxial: qué es, para qué sirve, tipos y cuál elegir*.

<https://www.xataka.com/basics/cable-coaxial-que-sirve-tipos-cual-elegir>

Franklin. (30 de Julio de 2019). *Qué debes saber a la hora de elegir un switch*.

<https://www.4netonline.com/ws/que-debes-saber-a-la-hora-de-elegir-un-switch/#:~:text=Los%20switch%20com%C3%BAmente%20vienen%20con,16%20puertos%20deber%C3%ADa%20ser%20suficiente>.

Fundibeq. (2022). *¿Qué es ISO?* <https://www.fundibeq.org/informacion/infoiso/que-es-iso>

G4s. (16 de Noviembre de 2020). *¿qué son los spyware y adware?* [https://www.g4s.com/es-](https://www.g4s.com/es-pe/g4s-te-informa/boletines-informativos-g4s/2020/11/16/que-son-los-spyware-y-adware)

[pe/g4s-te-informa/boletines-informativos-g4s/2020/11/16/que-son-los-spyware-y-adware](https://www.g4s.com/es-pe/g4s-te-informa/boletines-informativos-g4s/2020/11/16/que-son-los-spyware-y-adware)

Gallinas, B. (24 de Noviembre de 2022). *¿Qué es la fibra óptica? Aprende todo lo que necesitas*

saber. <https://roams.es/companias-telefonicas/blog/internet/que-es-fibra-optica/>

Ganuzá, N. (2020). *Guía de Ciberdefensa*. Canadá.

Geeknetic. (08 de Octubre de 2020). *¿Qué es RJ45 y para qué sirve?*

<https://www.geeknetic.es/RJ45/que-es-y-para-que-sirve>

Gerometta, O. (18 de Octubre de 2017). *Protocolos de enrutamiento dinámico.*

<http://librosnetworking.blogspot.com/2017/10/protocolos-de-enrutamiento-dinamico.html>

Gerometta, O. (4 de Mayo de 2019). [http://librosnetworking.blogspot.com/2019/05/port-](http://librosnetworking.blogspot.com/2019/05/port-aggregation-etherchannel.html)

[aggregation-etherchannel.html](http://librosnetworking.blogspot.com/2019/05/port-aggregation-etherchannel.html)

Gomez, F. P. (2022). *Objetivos de la seguridad informática.* [https://www.fpgenrede.es/Seguridad-](https://www.fpgenrede.es/Seguridad-Informatica-I/objetivos_de_la_seguridad_informtica.html)

[Informatica-I/objetivos_de_la_seguridad_informtica.html](https://www.fpgenrede.es/Seguridad-Informatica-I/objetivos_de_la_seguridad_informtica.html)

González. (8 de octubre de 2018). *Qué es un ciberataque y qué tipos existen.*

<https://ayudaleyprotecciondatos.es/2018/10/08/ciberataque/>

González, P. (18 de Mayo de 2015). *Generando Payloads en Base64 en Metasploit.*

<https://www.flu-project.com/2015/05/generando-payloads-en-base64-en.html>

Google. (2022). *Cableado estructurado.* [https://sites.google.com/site/redeslocalesyglobales/2-](https://sites.google.com/site/redeslocalesyglobales/2-aspectos-fisicos/6-elementos-de-la-instalacion-fisica/3-cableado-estructurado)

[aspectos-fisicos/6-elementos-de-la-instalacion-fisica/3-cableado-estructurado](https://sites.google.com/site/redeslocalesyglobales/2-aspectos-fisicos/6-elementos-de-la-instalacion-fisica/3-cableado-estructurado)

Google. (2022). *Topología Híbrida.* [https://sites.google.com/site/tecnologia4a16/tipos-de-](https://sites.google.com/site/tecnologia4a16/tipos-de-redes/redes-lan/conceptos-necesarios/topologia-hibrida)

[redes/redes-lan/conceptos-necesarios/topologia-hibrida](https://sites.google.com/site/tecnologia4a16/tipos-de-redes/redes-lan/conceptos-necesarios/topologia-hibrida)

Gtlan. (5 de Noviembre de 2019). *Armarios rack, la importancia de esta «caja metálica»:*

definición y usos. <https://www.gtlan.com/armarios-rack-la-importancia-de-esta-caja-metalica-definicion-y-usos/>

Hernández Linares, F. A., & Jiménez Montañez, J. A. (2020). *Importancia de la implementación de un laboratorio de ciberdefensa. Brújula Semilleros de Investigación.*

<https://brujuladesemilleros.com/index.php/bs/article/view/36>

Higo. (4 de Julio de 2022). *Red WAN ¿Qué es y cómo funciona?* [https://higo.io/glosario-](https://higo.io/glosario-contable/r/red-wan-que-es-y-como-funciona/)

[contable/r/red-wan-que-es-y-como-funciona/](https://higo.io/glosario-contable/r/red-wan-que-es-y-como-funciona/)

Hoy. (20 de Septiembre de 2022). *Canaletas: ¿Qué son y cuáles son sus beneficios?* .

<https://hoy.com.do/canaletas-que-son-y-cuales-son-sus-beneficios/>

Hwang, D. (2021). *Red de área local o LAN*.

<https://www.computerweekly.com/es/definicion/Red-de-area-local-o-LAN>

IBM. (2020). *¿Qué es la ciberseguridad?* <https://www.ibm.com/es-es/topics/cybersecurity>

IBM. (2022). *¿Qué es un ciberataque?* <https://www.ibm.com/es-es/topics/cyber-attack>

ICA. (2022). *Los 9 tipos ciberataque que deberías conocer*. <https://www.grupoica.com/blog/-/blogs/9-tipos-ciberataque-debes-conocer>

IEEDES. (31 de Agosto de 2022). *¿Qué es un patch panel y para qué sirve?*

<https://www.ieedes.com/patch-panel/>

IEEE. (29 de Enero de 2022). *¿Qué es el IEEE?* <https://edu.ieee.org/mx-uami/que-es-el-ieee/>

Implika. (14 de Abril de 2021). *Formación en Nuevas Tecnologías*.

<https://www.implika.es/blog/que-son-redes-informaticas>

Incibe. (22 de Diciembre de 2020). *Amenaza vs vulnerabilidad: cómo diferenciarlos*.

<https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-diferenciarlos#:~:text=Definici%C3%B3n%20de%20vulnerabilidad%20y%20amenaza&text=Una%20cuesti%C3%B3n%20es%20tener%20la,si%20somos%20o%20no%20vulnerables.>

Informática VIP. (2022). *Cableados Estructurados Datos*.

<https://www.informaticavip.com.ar/implementaciones/cableados-estructurados-datos>

infosecuritymexico. (2022). *Ciberseguridad*.

<https://www.infosecuritymexico.com/es/ciberseguridad.html>

IONOS, D. G. (22 de Junio de 2022). *Kali Linux: ¿qué es Linux para hackers?*

<https://www.ionos.es/digitalguide/servidores/configuracion/kali-linux/>

ISO 27001. (2018). *Referencias Normativas ISO 27000*. <https://normaiso27001.es/referencias-normativas-iso-27000/#def361>

IT, I. (8 de Diciembre de 2021). *NGFW: ¿Qué es el Next Generation Firewall?*

<https://www.internationalit.com/post/ngfw-que-es-el-next-generation-firewall?lang=es>

Itca. (2022). *Ataques pasivos vs ataques activos*.

https://virtual.itca.edu.sv/Mediadores/cms/u46_ataques_pasivos_vs_ataques_activos.html

John. (6 de Julio de 2021). *¿Qué es un patch panel y por qué lo necesitamos?*

<https://community.fs.com/es/blog/what-is-a-patch-panel-and-why-use-it.html>

Jurado, Á. (09 de Julio de 2019). *Amenazas de seguridad física para los sistemas de información*. <https://www.inesem.es/revistadigital/gestion-integrada/amenazas-seguridad-fisica-sistemas-de-informacion/>

Kali. (26 de Noviembre de 2022). *La distribución de pruebas de penetración más avanzada*.

<https://www.kali.org/>

Kaspersky. (Diciembre de 2021). *¿Qué es la ciberseguridad?*

<https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security>

Kaspersky. (2022). *¿Qué es una VPN y cómo funciona?* <https://latam.kaspersky.com/resource-center/definitions/what-is-a-vpn>

KeepCodin, R. (8 de Septiembre de 2022). *¿Qué es Suricata en ciberseguridad?*

<https://keepcoding.io/blog/que-es-suricata-en-ciberseguridad/>

Keepcoding. (26 de Septiembre de 2022). *¿Qué es BlackArch Linux?*

<https://keepcoding.io/blog/que-es-blackarch-linux/>

Khan Academy. (2022). *La suite de protocolos de Internet*.

<https://es.khanacademy.org/computing/ap-computer-science-principles/the-internet/x2d2f703b37b450a3:the-internet-protocol-suite/a/the-internet-protocols>

Laucol. (13 de Diciembre de 2020). *Funciones del Cableado estructurado*.

<https://laucol.com.ec/novedades-y-publicaciones/leviton/funciones-del-cableado-estructurado/>

Leroy Merlin. (11 de Agosto de 2022). *Canaleta*. <https://www.leroymerlin.es/bricopedia/canaleta>

Limones, E. (7 de Abril de 2021). *Topología de redes informáticas*.

<https://openwebinars.net/blog/topologia-de-redes-informaticas/>

Linux, K. (5 de Agosto de 2022). *Documentación de la herramienta*.

<https://www.kali.org/tools/reaver/>

López, J. G. (2014). *Hackers. Aprende a atacar y defenderte. 2ª Adición Actualizada*. Ra-Ma.

Low, J. (29 de julio de 2022). *WebHostingSecretRevealed.net*.

<https://www.webhostingsecretrevealed.net/es/blog/security/cybersecurity-statistics/>

Ludueña, T. d. (19 de Septiembre de 2022). Organigrama. (J. Cbos de Com Armijos, Entrevistador)

Luz, S. d. (27 de Marzo de 2020). *Los mejores switches: consejos para comprar tu switch*.

https://www.redeszone.net/mejores/switches/?_gl=1%2a18y0gp%2a_up%2aMQ..%2a_ga%2aMTQyODA0NjQzNS4xNjcyMzYwMTM3%2a_ga_THC18XR4S2%2aMTY3MjM2MDEzNi4xLjAuMTY3MjM2MDEzNi4wLjAuMA..

malwarebytes. (20 de Diciembre de 2018). *Todo acerca del malware*.

<https://es.malwarebytes.com/malware/>

Mantilla, I. (18 de Abril de 2022). *Municipio de Quito suspende trámites digitales por ataque de hackers*. <https://www.elcomercio.com/actualidad/municipio-quito-ataque-hacker-tramites.html>

Maribel. (11 de Mayo de 2017). *Amenazas Físicas y Lógicas*.

<https://sites.google.com/site/seguridadinformaticafpb/tipos-de-amenazas/11amenazasfisicasylogicas>

Martínez Ramírez, C. (18 de Junio de 2020). *Confidencialidad, integridad y disponibilidad*.

<https://es.linkedin.com/pulse/confidencialidad-integridad-y-disponibilidad-martinez-ramirez>

Martinez, J. (28 de Julio de 2020). *Seguridad Cibernética*. <https://grupocsf.com/tag/seguridad-cibernetica/>

Mier Ruiz, E. E., & Mier Ruiz, G. D. (2008). *Protocolos de Enrutamiento*.

<https://biblioteca.utb.edu.co/notas/tesis/0045016.pdf>

Migelle. (12 de Enero de 2022). <https://community.fs.com/es/blog/what-is-power-over-ethernet-and-how-to-add-poe-in-network.html>

MINTIC. (2019). *Estándares y Tecnologías*. [https://mintic.gov.co/portal/inicio/Atencion-y-Servicio-a-la-Ciudadania/Preguntas-frecuentes/5236:Estandares-y-Tecnologias#:~:text=Un%20est%C3%A1ndar%20\(como%20lo%20define,servicios%20cumplan%20con%20su%20proposito%22](https://mintic.gov.co/portal/inicio/Atencion-y-Servicio-a-la-Ciudadania/Preguntas-frecuentes/5236:Estandares-y-Tecnologias#:~:text=Un%20est%C3%A1ndar%20(como%20lo%20define,servicios%20cumplan%20con%20su%20proposito%22).

Moris. (15 de Julio de 2021). *Introducción a la interfaz RJ45*.

<https://community.fs.com/es/blog/introduction-of-the-rj45-interface.html>

Muñoz, M. A. (05 de Junio de 2003). *safeDES: Software de Ataque a la Fortaleza del Estándar DES*. <https://www.abcdatos.com/programa/ataque-fortaleza-estandar-des.html>

Netskope. (18 de Octubre de 2022). *¿Qué es Cyber Security Kill Chain (cadena de exterminio de la ciberseguridad)?* <https://www.netskope.com/es/security-defined/cyber-security-kill-chain>

Nextvision. (9 de julio de 2022). *CVE: Vulnerabilidades junio 2022*. <https://nextvision.com/cve-vulnerabilidades-junio-2022-2/>

Novelec, E. G. (16 de Noviembre de 2020). *Cable coaxial: Tipos y características*.

<https://blog.gruponovelec.com/redes-vdi/cable-coaxial-tipos-y-caracteristicas/>

ORACLE. (s.f.). *oracle*. <https://www.oracle.com/es/database/security/que-es-el-malware.html#:~:text=Malware%20es%20un%20t%C3%A9rmino%20gen%C3%A9rico,c> contenido%20activo%20y%20otro%20software.

Oscarfmdc. (02 de Marzo de 2020). *Apache Hive: Introducción*.

[https://aprenderbigdata.com/apache-](https://aprenderbigdata.com/apache-hive/#:~:text=Hive%20proporciona%20una%20estructura%20basada,las%20divisiones%20de%20las%20particiones)

[hive/#:~:text=Hive%20proporciona%20una%20estructura%20basada,las%20divisiones%20de%20las%20particiones](https://aprenderbigdata.com/apache-hive/#:~:text=Hive%20proporciona%20una%20estructura%20basada,las%20divisiones%20de%20las%20particiones).

- Pablo. (24 de Junio de 2021). *El cable Ethernet, nuestra conexión básica a internet*.
<https://blog.orange.es/consejos-y-trucos/tipos-de-cable-ethernet/>
- Parra Correa, C. A., & Porras Díaz, H. (2007). Las Amenazas informáticas: peligro latente para las organizaciones actuales. 87. <https://core.ac.uk/download/pdf/230227206.pdf>
- Peralta, P. F. (27 de abril de 2017). *Estándar EIA/TIA. Cableado estructurado*.
<https://silo.tips/download/estandar-eia-tia-cableado-estructurado>
- Pérez Porto, J., & Gardey, A. (2014). *Definicion.de*. <https://definicion.de/cableado-estructurado/>
- Process. (3 de Mayo de 2022). *Protocolo de red: qué es y sus características*.
<https://autmix.com/blog/que-es-protocolo-red#que-es-un-protocolo-de-red>
- Project, T. (2014). *The Hive una plataforma de respuesta a incidentes de seguridad 4 en 1*.
<https://thehive-project.org/>
- Quezada, A. E. (19 de Junio de 2014). *Ataque de Envenenamiento ARP utilizando Ettercap*.
https://www.reydes.com/d/?q=Ataque_de_Envenenamiento_ARP_utilizando_Ettercap
- Ramiro, R. (8 de Septiembre de 2018). *Un trio perfecto con TheHive, Cortex y MISP*.
<https://ciberseguridad.blog/un-trio-perfecto-con-thehive-cortex-y-misp/>
- RedesLocales. (2022). *Comparativa OSI frente TCP/IP*.
<https://sites.google.com/site/redeslocales2marta/home/transmision-de-datos-en-las-redes/osi-frente-tcp-ip>
- Reyes, G. (1 de Septiembre de 2019). *¿Qué debo considerar antes de comprar un switch?*
<https://quanti.com.mx/articulos/que-debo-considerar-antes-de-comprar-un-switch/>
- Robledano, A. (18 de Junio de 2019). *Qué es TCP/IP*. <https://openwebinars.net/blog/que-es-tcpip/>
- Sain, G. (27 de Febrero de 2016). *¿Qué es la ciberguerra? Pensamiento Penal*, 1.
<https://www.pensamientopenal.com.ar/doctrina/42952-es-ciberguerra>

- Sanchez, D. (4 de Octubre de 2019). *¿Qué es un panel de parcheo en cableado estructurado y para qué sirve?* <https://info.ita.tech/blog/que-es-un-panel-de-parcheo-en-cableado-estructurado>
- Sanchez, D. (12 de Junio de 2021). <https://info.ita.tech/blog/que-es-un-cable-de-parcheo-patch-panel>
- Sánchez, R. (27 de Mayo de 2020). *¿Qué es un cable invertido (cruzado) y para qué sirve?* <https://resethn.wordpress.com/2012/05/27/qu-es-un-cable-invertido-y-para-qu-sirve/>
- Santiago, P. (21 de Marzo de 2022). *Cableado Horizontal y Vertical [Video]*. https://www.youtube.com/watch?v=Y_B88Xgifyw
- Saumeth, E. (5 de Marzo de 2021). *Ecuador crea el Comando de Ciberdefensa para blindar al país ante ataques cibernéticos*. <https://www.infodefensa.com/texto-diario/mostrar/3056658/ecuador-crea-comando-ciberdefensa-blindar-pais-ante-ataques-ciberneticos>
- Silva, D. d. (23 de Agosto de 2021). *¿Qué es la seguridad de la información?* <https://www.zendesk.com.mx/blog/que-es-seguridad-de-informacion/>
- SoftwareLab. (23 de Junio de 2021). *¿Qué es la ingeniería social? Los 5 ejemplos principales*. <https://softwarelab.org/es/que-es-ingenieria-social/>
- Solano, D. O. (2017). *Análisis de Vulnerabilidades y acciones correctivas sobre un sistema web*. <https://www.dspace.espol.edu.ec/retrieve/45e4491d-5352-4463-8569-19d44988922c/D-106382.pdf>
- Subsecretaría de Informática. (Enero de 2009). *Estrategia Implantación de Software Libre en la Administración Pública Central de Ecuador*. https://cti.gobiernoelectronico.gob.ec/ayuda/manual/decreto_1014.pdf
- Surfshark. (3 de Enero de 2023). *¿Qué es una VPN y cómo funciona una red privada virtual?* <https://surfshark.com/es/learn/que-es-vpn>
- Syscom. (2020). *Herramientas*. <https://www.syscom.mx/producto/CWST-PANDUIT-75309.html>

Taque, M. P. (Junio de 2011). Delito en el Comercio Electrónico. *Prisma Jurídico*, 209-224.

<https://www.redalyc.org/pdf/934/93420939012.pdf>

Telecapp. (2022). *Protocolos de enrutamiento*. <https://telecapp.com/protocolos-enrutamiento>

Televistazo. (10 de Marzo de 2022). *Otra plataforma informática del Centro de Inteligencia Estratégica fue vulnerada por "hackers"*.

<https://www.ecuavisa.com/noticias/ecuador/otra-plataforma-informatica-del-centro-de-inteligencia-estrategica-fue-vulnerada-por-hackers-FE1431153>

Termired. (26 de Febrero de 2021). *Estándares T568A y T568B*. <https://termired.com/codigos-de-colores-rj45/>

Tiaonline. (28 de Noviembre de 2022). *Telecommunications Industry Association*.

<https://tiaonline.org/>

Tinet. (2022). *Tipos de redes*.

https://usuaris.tinet.cat/acl/html_web/redes/topologia/topologia_2.html

Todopacketracer. (15 de Septiembre de 2017). *Ethernet Channel*.

<https://todopacketracer.wordpress.com/2017/09/07/ethernet-channel-y-port-channel/>

Tokio. (19 de Agosto de 2022). *Tipos de ataques informáticos: ¿cuáles son y cómo operan?*

<https://www.tokioschool.com/noticias/tipos-ataques-informaticos/>

TokioSchool. (9 de Junio de 2021). *Red VLAN: ¿En qué consiste?*

<https://www.tokioschool.com/noticias/que-es-vlan/>

Tops. (2022). *IDS-IPS*. <https://www.tops.hk/en/pfsense-firmware-os/ids-ips.html>

UAEH. (2022). *Tipos de Redes (LAN, MAN, WAN)*.

http://cidecame.uaeh.edu.mx/lcc/mapa/PROYECTO/libro27/136_tipos_de_redes_lan_man_wan.html

UCM. (2022). *Proyecto de Innovación Software libre para ciencias e ingenierías*.

<https://www.ucm.es/pimcd2014-free-software/metasploit>

- UCSP. (17 de Junio de 2022). *Todo lo que tienes que saber sobre la seguridad de redes*.
<https://postgrado.ucsp.edu.pe/articulos/que-es-seguridad-redes/>
- Ulhi. (2022). *Condiciones de instalación del cableado Vertical, backbone*.
https://ikastaroak.ulhi.net/edu/es/IEA/ICTV/ICTV10/es_IEA_ICTV10_Contenidos/website_251_condiciones_de_instalacin_del_cableado_vertical_backbone.html
- UNAD. (2022). *Seguridad Informática*.
<https://soniaespitia.github.io/LecturasSeguridadInformatica/>
- Unión Internacional de Telecomunicaciones. (2008). Recomendación UIT-T X.1205. 3.
- UNIR. (4 de Enero de 2022). *Topología de red: qué es y cuáles son los tipos más habituales*.
<https://ecuador.unir.net/actualidad-unir/topologia-red/>
- UNITEL. (2020). *Normas sobre Cableado Estructurado*. <https://unitel-tc.com/normas-sobre-cableado-estructurado/>
- VCS. (2022). *Cableado Estructurado*. <https://vcs-proyectos.com.pe/cableado-estructurado/>
- Velasco, R. (22 de Octubre de 2017). *genRSA, una completa herramienta para generar y atacar claves RSA*. <https://www.redeszone.net/2017/10/22/genrsa-generar-atacar-claves-rsa/>
- Velasco, R. (17 de Junio de 2019). *BackBox Linux 6 disponible; llega la nueva suite de hacking ético con nuevas herramientas y mejoras internas*.
<https://www.redeszone.net/2019/06/17/backbox-linux-6-hacking-etico/>
- Velasco, R. (01 de Diciembre de 2022). *VMware, VirtualBox o Hyper-V – ¿Qué programa es mejor?* <https://www.softzone.es/programas/utilidades/diferencias-vmware-virtualbox-hyper-v/>
- vlex. (2019). *Clasificación y tipos de ataques contra sistemas de información*.
<https://doi.org/https://vlex.es/vid/clasificacion-tipos-ataques-sistemas-102081>
- Vmware. (15 de Diciembre de 2022). *Seguridad de las aplicaciones*.
<https://www.vmware.com/latam/topics/glossary/content/application-security.html>

VMware. (2022). *VMware vSphere*. <https://www.vmware.com/files/es/pdf/VMware-vSphere-Entreprise-Edition-Datasheet.pdf>

Walton, A. (17 de Noviembre de 2017). *Modelos TCP/IP y OSI*.

<https://ccnadesdecero.es/modelos-tcp-ip-osi-caracteristicas/>

Worton. (16 de Junio de 2019). *Cableado de la red troncal vs. el cableado horizontal*.

<https://community.fs.com/es/blog/structured-cabling-backbone-cabling-vs-horizontal-cabling.html>

Wut. (2023). *PoE – Power over Ethernet*. <https://www.wut.de/e-5773w-01-thes-000.php>

Xringarchy. (23 de Marzo de 2019). *Consejo de piratería: persistencia y pivoteo para principiantes en Metasploitable 2*.

<https://xringarchy.wordpress.com/2019/03/23/hacking-tip-persistence-in-metasploitable-2/>

Yanes, J. (10 de noviembre de 2017). *bbvaopenmind*.

<https://www.bbvaopenmind.com/tecnologia/mundo-digital/la-historia-de-los-virus-informaticos/>

Zscaler. (2022). *¿Qué es un cortafuegos de próxima generación?*

<https://www.zscaler.es/resources/security-terms-glossary/what-is-next-generation-firewall>

Anexos