UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

Integración de materiales didácticos en una plataforma educativa para el curso de Redes de Datos Seguras

TESIS

Que para obtener el título de

Ingeniero en Computación

P R E S E N T A N

Alberto Saavedra León
Luis Fernando Resendiz Cruz

DIRECTOR(A) DE TESIS

M.C. Ma. Jaquelina López Barrientos

Ciudad Universitaria, Cd. Mx., 2021

Índice

Índice de figuras

Índice de tablas.

Introducción

En la actualidad la mayoría de las comunicaciones se realizan por medio de dispositivos electrónicos, esto ha sido gracias al avance del ser humano en los campos de la ciencia y la tecnología. Pero a pesar de que las comunicaciones siguen avanzando día a día siempre existirá una base común que permite su funcionamiento, ese es el caso de las Redes de Datos que llegó a darle un impulso sorprendente al desarrollo y evolución de la sociedad permitiendo comunicar más información de una manera rápida y eficaz.

En 1969 fue implementada la primera red de computadoras, ARPANET, la cual constaba de cuatro nodos distribuidos por la costa oeste de los Estados Unidos, en la actualidad estas redes han evolucionado a un nivel que supera los 4.000 millones de usuarios diariamente, además, las Redes de Datos se han convertido en una parte esencial de los gobiernos, empresas y organizaciones a tal punto que no es permisible que sus redes tengan algún problema, falla o que no cumplan con sus requisitos de operatividad.

Las Redes de Datos transportan una gran cantidad de información de todo tipo, desde información personal hasta información sensible de empresas y gobiernos, por ello, las Redes de Datos se han convertido en el nuevo blanco de actividades maliciosas como lo son el robo de información, la suplantación de identidad, ciberterrorismo, y ciberguerras entre otras. Como dato importante en México se han registrado más de 300 millones de ataques cibernéticos en el último año (octubre 2018 al mismo mes del 2019) [1] lo que quiere decir que la implementación de mecanismos de seguridad es importante e imprescindible para salvaguardar la información y con ello a los usuarios.

Por la misma importancia que tienen las Redes de Datos, el conocerlas, implementarlas de manera correcta y, en especial, procurando la seguridad es el motivo de que las siguientes generaciones de Ingenieros en Computación se

[1] Hernández Armenta , Mauricio. (2019, 21 noviembre). México registró 9.5 ataques de malware por segundo en 2019. Recuperado 16 de junio de 2020, de https://www.forbes.com.mx/mexico-registro-9-5-ataques-de-malware-por-segundo-en-2019/

formen con el conocimiento necesario a fin de solventar los problemas que a la sociedad aquejan.

Así, las nuevas generaciones de Ingenieros en Computación necesitan adquirir los conocimientos para diseñar, implementar, actualizar y mantener la seguridad de las Redes de Datos, para ello requieren de materiales didácticos que les permitan afianzar sus conocimientos y conozcan sus debilidades incluyendo temas referentes a seguridad.

Además, cabe mencionar que en esta era de Tecnologías de la Información, es imprescindible que los estudiantes cuenten con material didáctico a su alcance en todo momento y desde cualquier lugar, por lo que sería altamente recomendable que el material se albergara en una plataforma donde siempre se pueda acceder a través de Internet.

El objetivo principal del proyecto presentado en este documento es la implementación de una plataforma educativa en la cual se integren el material didáctico, el material de apoyo y los videos del laboratorio de Redes da Datos Seguras, en un sitio centralizado y disponible desde cualquier lugar tanto para los docentes como para los alumnos.

Para cumplir con el objetivo principal del proyecto es necesario alcanzar los siguientes objetivos particulares:

● Desarrollar material didáctico tomando como base los contenidos que indica el programa de estudio de la asignatura, así como el material didáctico que se ha desarrollado para la asignatura.

● Investigación y selección de una plataforma educativa que se adapte lo mejor posible a las necesidades de integración de los materiales y de los videos.

● Implementación de un ambiente piloto para la instalación, personalización y pruebas de la plataforma para su posterior migración a los servidores de la Academia de Redes.

● Creación de la documentación requerida para una adecuada administración por la Academia de Redes

Capítulo 1. Análisis

En este capítulo se muestra el proceso de análisis que se llevó a cabo para realizar la implementación de la página de estudio.

1.1 Análisis del Programa de estudio.

Para generar el material didáctico que ayude a los estudiantes en su formación académica en esta área es importante comprender y entender cuáles son los conocimientos previos que se requieren para la asignatura de Redes de Datos Seguras, para ello se tomó en cuenta el mapa curricular de la carrera de Ingeniería en Computación del plan de estudios 2016 (véase la figura 1.1).

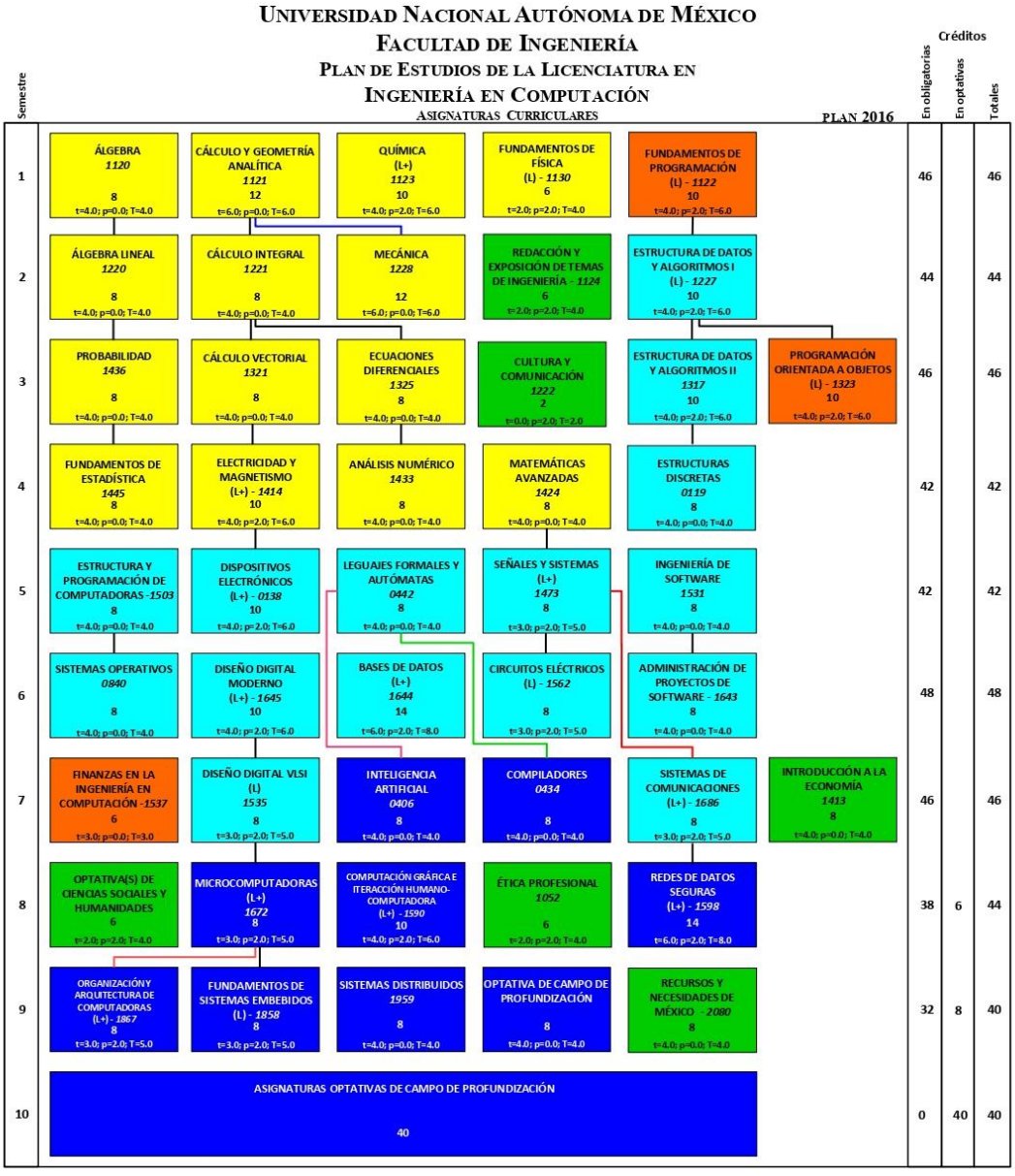


Figura 1.1. Plan de estudios de la carrera de Ingeniería en Computación.

Como se aprecia en la figura 1.1 la asignatura Redes de Datos Seguras se ubica en el octavo semestre en color azul y sus antecedentes son las asignaturas de Sistemas de Comunicación, Señales y Sistemas, y Matemáticas Avanzadas. Además, se realizó un análisis del programa de estudio vigente de la asignatura (véase **Anexo 1**)

En este programa se observa que la asignatura consta de nueve temas principales que están divididos en subtemas, a grandes rasgos se identifica que los temas uno y dos están enfocados en los conocimientos generales de la asignatura que los estudiantes deben dominar antes de entrar más a fondo en las Redes de Datos y que los temas del tres al nueve están enfocados cada uno en una de las 7 capas del modelo OSI *(Open System Interconection)* el cual es el pilar de estudio principal de las Redes de Datos.

Así mismo, se analizó cada tema detenidamente, ya que estos a su vez se dividen en subtemas los cuales se enfocan en los aspectos fundamentales de la capa que se está estudiando. Siguiendo el análisis se identificó que existe en la mayoría de los temas, al menos un subtema enfocado en la seguridad, esta es una premisa importante y que cabe destacar, debido a que es uno de los propósitos principales del curso de Redes de Datos Seguras, el cual corresponde a cubrir los aspectos de seguridad de la información tanto en la parte física como en la parte lógica de las Redes de Datos con lo cual es importante resaltarlo en el material de estudio.

Una vez realizado el análisis del programa de estudio también se debe de comprender y estudiar cada uno de los temas para generar el material adecuado al conocimiento que se busca que obtengan los estudiantes en él, para esto se revisaron los temas a tratar en apuntes de semestres anteriores, libros (mismos que recomienda el plan de estudios de la asignatura), además de libros recomendados por estudiantes y profesores y especialmente en el material de apoyo que se desarrolló como parte del proyecto que lleva a la realización del presente trabajo para obtener el conocimiento sobre el curso.

1.2 Identificación de conocimientos que se buscan en cada tema.

Tema 1. Conceptos básicos.

En el primer tema del curso de Redes de Datos Seguras se identificó que se trata de un tema teórico enfocado en los conceptos básicos que los estudiantes deben de adquirir o que tal vez ya conocen y lo que se busca es que reflexionen sobre ellos y valoren la importancia de las Redes de Datos y su seguridad en el mundo actual.

Debido a que la enseñanza que se busca en este primer tema es la adquisición de conocimientos básicos para identificar la diferencia entre conceptos utilizados en el campo de las redes y la ciberseguridad para así tener un mejor criterio al momento de tomar decisiones sobre cómo actuar ante un incidente o las medidas necesarias a tomar al momento del diseño e implementación de una red. La forma para evaluar el aprendizaje de este tema es mediante reactivos que comprueben la adquisición de los conocimientos teóricos básicos y su reflexión sobre las Redes de Datos Seguras.

Tema 2. Estándares y arquitecturas.

El segundo tema de la asignatura de Redes de Datos Seguras trata sobre estándares y arquitecturas, se busca que el estudiante conozca a cierta profundidad los principales estándares y arquitecturas que rigen las Redes de Datos y comunicaciones para su correcta implementación. La importancia de este conocimiento radica en que las empresas y organizaciones deben de apegarse a estándares los cuales son probados y respaldados por instituciones de confianza, en caso contrario existirían un sin número de formas de implementación de Redes de Datos lo cual resultaría en problemas de incompatibilidad y a su vez esto provocaría que los usuarios no pudieran conectarse y hacer uso de las Redes de Datos.

Los conocimientos de este tema son teóricos, se enfocan en la adquisición del conocimiento sobre los estándares que rigen el campo de las Redes de Datos, así como de los organismos que los promueven, además también se busca dar a

conocer al estudiante los distintos modelos de comunicaciones, entre ellos el modelo OSI que tiene relevancia debido a que a partir de este modelo se lleva a cabo el estudio de la asignatura y cada una de sus capas se desarrollan en los siguientes temas. Los reactivos de este tema serán formulados con el objetivo de evaluar la adquisición del conocimiento teórico que el estudiante ha adquirido.

Tema 3. Capa física.

El tercer tema de la asignatura trata sobre la primera capa del modelo OSI que es la capa física, en este tema se busca que el estudiante adquiera los conocimientos sobre los distintos medios de transmisión que se utilizan para las comunicaciones en la red, así como los distintos estándares que rigen sobre la capa física.

El conocimiento en este tema es teórico/práctico ya que es necesario conocer los estándares que dictan las normas para llevar a cabo instalaciones de cableado así como de redes inalámbricas, conocimientos que se complementan con actividades prácticas en el laboratorio de Redes, por lo cual los reactivos creados para este tema deben de validar la adquisición de este conocimiento mediante preguntas que se enfoquen a promover el conocimiento de los distintos medios de transmisión de datos, sus ventajas y desventajas, así como el conocimiento de cableado estructurado que es importante debido a que la capa física es la base de una red de datos. En esta capa se definen características como son el rendimiento, la latencia y la tasa de error por esta razón es importante el conocimiento adquirido en esta capa para lograr la implementación que permita el mejor desempeño posible.

Tema 4. Capa de enlace de datos.

En el cuarto tema de la asignatura de Redes de Datos aborda los distintos protocolos, métodos y dispositivos electrónicos que se utilizan en la capa de enlace de datos del modelo OSI. La importancia del conocimiento que se espera que el alumno a quiera puede hallarse en el objetivo de la capa el cual es el de transportar una serie de bits mediante los servicios de la capa física, para lograr esto, la capa debe de manejar los errores de transmisión, regular el flujo de datos

y proporcionar una interfaz de servicio bien definida. Si esta capa no es correctamente diseñada afectará al rendimiento general de la red de datos.

En este tema el conocimiento que se busca adquiera el estudiante es la comprensión de los protocolos de enlace para redes tanto alámbricas (Ethernet) como inalámbricas (Wi-Fi), aprender sobre HDLC *(Higt Data Link Control)* y SDLC que son protocolos propios de la capa de enlace y conocer sobre los dispositivos físicos de interconexión, por lo tanto, los reactivos realizados deben de tener un enfoque que verifiquen la adquisición de los conocimientos relacionado con los distintos protocolos de la capa de enlace, comprensión del método de handshaking y la identificación de dispositivos como el switch, bridge y NIC que operan en esta capa del modelo OSI.

Tema 5. Capa de red.

El quinto tema trata sobre la capa de red del modelo OSI, se busca que el estudiante aplique métodos y estándares para diseñar y configurar Redes de Datos. Estudiar esta capa es importante debido a que es la que se encarga de llevar paquetes de datos de extremo a extremo de la comunicación, y para hacer esto es necesario que se conozca la topología de la red para escoger la ruta óptima, procurando no sobrecargar las líneas de comunicación y los enrutadores. También se encarga de la comunicación entre distintas redes, por todo lo anterior, es importante que el alumno conozca el diseño de la capa de red para su correcta implementación y gestión.

El conocimiento que se desea que el estudiante posea al término de este tema es comprender sobre algoritmos y protocolos de enrutamiento estáticos y dinámicos, también sobre servicios orientados y no orientados a conexión. Además, aprenderá sobre el protocolo IP y con ellos sobre CIDR, VLSM y sumarización de rutas. Los reactivos creados para este tema buscan comprobar la adquisición del conocimiento mediante preguntas y con ejercicios para el apartado de subnetting que se estudia en este tema y que tienen importancia en el momento de realizar configuraciones en las redes para su correcto funcionamiento.

Tema 6. Capa de transporte.

En el sexto tema de la asignatura se estudia la capa de transporte del modelo OSI, el objetivo es que el estudiante logre identificar los diferentes tipos de protocolos, métodos y estándares que ese utilizan en esta capa, esto mediante el análisis del funcionamiento de los protocolos TCP y UDP. La importancia de este tema es el cómo funcionan los protocolos de esta capa, estos proveen un nivel de abstracción para que las aplicaciones sean capaces de realizar sus funciones, el objetivo principal de la capa es el de transportar datos de un proceso en la máquina origen a un proceso de la máquina destino, por ello se debe conocer esta capa para realizar la elección del protocolo a utilizar en la red de datos.

El conocimiento que se busca transmitir es el comprender los servicios propios de la capa, el manejo de paquetes, puertos lógicos y los métodos de control de flujo como lo son stop-wait y ventana deslizante. También se estudian los protocolos TCP y UDP los cuales son los principales para esta capa. Los reactivos desarrollados para este tema buscan verificar la compresión de los variados conocimientos mediante preguntas y, para el caso de los métodos de control de flujo, se pueden desarrollar ciertos ejercicios.

Tema 7. Capa de sesión.

El séptimo tema de la asignatura de Redes de Datos Seguras se estudia la capa de sesión, esta capa es la primera orientada a la aplicación, se encarga principalmente de permitir el diálogo entre el emisor y el receptor mediante el establecimiento de sesiones, logrando así el intercambio ordenado de datos y controlando las desconexiones o interrupciones por fallos de la red. Es importante que el estudiante conozca esta capa porque hay aplicaciones que hacen uso de los servicios de esta capa y es importante identificar cuando hacer uso de estos servicios al momento de diseñar o implementar una aplicación. Teniendo esto en cuenta, los reactivos generados se enfocan en comprobar que los conocimientos antes mencionados hayan sido adquiridos.

Tema 8. Capa de presentación.

En el octavo tema de la asignatura de Redes de Datos Seguras se estudia sobre la capa de presentación, se busca que el estudiante conozca sobre los distintos protocolos que trabajan en esta capa, así como la representación, las técnicas de compresión y cifrado de datos, este último se divide en el análisis de algoritmos de cifrado simétrico y asimétrico los cuales son importantes para la implementación de seguridad de la información. La importancia de que el alumno adquiera el conocimiento al respecto de la capa de presentación radica en que es necesario, al momento de diseñar o implementar una aplicación, conocer qué servicios se ofrecen para hacer el correcto uso de estos.

Los reactivos desarrollados para este tema se enfocan en promover el conocimiento sobre los distintos algoritmos de cifrado, los formatos en los que es representada la información y los distintos tipos de compresión de datos tanto con cómo sin pérdida de información.

Tema 9. Capa de aplicación.

En el último tema de la asignatura de Redes de Datos Seguras se estudia sobre la capa de aplicación, en este tema se tiene como objetivo que el estudiante sea capaz de identificar y poner en práctica distintos tipos de aplicaciones, todo esto orientado a las necesidades y requerimientos que pueden tener los usuarios en una red. La importancia de esta capa radica en que cuando se requiere implementar una aplicación, es indispensable conocer cómo funciona esta y si cubre las necesidades de la organización en la que se implementa.

Los reactivos de este tema tienen como objetivo el fomentar el conocimiento de las distintas aplicaciones pertenecientes a esta capa, en qué puertos lógicos trabajan habitualmente, qué alternativa se tiene de una aplicación de acuerdo al sistema operativo y para qué tipo de tarea puede ser usada cada aplicación para que así el estudiante sea capaz de escoger entre las distintas alternativas la aplicación que más se adapte a los requerimientos de los usuarios para el correcto funcionamiento de las operaciones en una red de datos.

1.3 Software de implementación.

Debido a que el material didáctico que se generó debe estar disponible en todo momento al público en general que esté interesado en la asignatura de Redes de Datos Seguras se ha tomado la decisión de implementarlo mediante un LMS (Learning Management System) esto con el fin de proporcionar el material a los estudiantes, a su vez se asientan las bases de una plataforma a través de la cual el Laboratorio de Redes y Seguridad ponga a disposición de académicos y estudiantes todo el material didáctico que se desarrolla para la adquisición del conocimiento en esta área.

Un Learning Management System (LMS, Sistema de manejo de aprendizaje traducido del inglés) es un software basado en servicios web, el cual permite crear, implementar y desarrollar un proceso de aprendizaje, todo esto a distancia. Por lo general un LMS consta de dos elementos: un servidor donde se aloja la infraestructura del LMS y una interfaz con la cual es posible que los administradores, educadores y alumnos puedan interactuar con el contenido de los cursos.

Con esto en mente se han analizado las posibles LMS que pueden ser utilizadas para cumplir con el fin de proporcionar el material didáctico.

1.3.1. Sakai

Figura 1.3. 1 Logo Sakai Proyect

Sakai es una plataforma de acceso libre con herramientas enfocas al aprendizaje, la docencia, la investigación y la colaboración. Se inicio en 2003 en un proyecto conjunto entre varias universidades de Estados Unidos principalmente la universidad de Michigan y la universidad de Indiana. El proyecto Sakai esta diseñado para apoyar los trabajos de colaboración.

El objetivo del Proyecto Sakai es crear un entorno de colaboración y aprendizaje para la educación superior, que pueda competir con sus equivalentes comerciales Blackboard / WebCT y que mejore otras iniciativas de código abierto como Moodle.

La plataforma integra bibliotecas, cursos, proyectos de investigación, sitios electrónicos, además de que tiene la ventaja de poseer herramientas integradas que facilitan el aprendizaje, como también poder incorporar herramientas procedentes de otras plataformas.

Este proyecto fue un pionero del modelo de código fuente comunitario en el desarrollo de software, porque gran parte de la inversión inicial para su creación provino de la colaboración y la contribución de individuos, escuelas y universidades. El apoyo de la comunidad le da estabilidad al proyecto y marca su dirección ya que se establecen prioridades.

Al tratarse de un código abierto, Sakai puede ser descargado por cualquier usuario sin costo alguno, además de poder ser implementado, modificado y distribuido para cualquier propósito.

Ventajas:

- Es un sistema autónomo para el aprendizaje, la docencia, la investigación y la colaboración, ofrece un diverso catálogo de características que se pueden utilizar para cursos y proyectos.
- Se adapta a las necesidades pedagógicas o de enseñanza de cada institución.
- Permite personalizar el ambiente de acuerdo con las necesidades institucionales.
- Control de actualizaciones. Con el continuo desarrollo del código por su comunidad es un proyecto en constante desarrollo y evolución.
- Es una plataforma que se puede instalar en sistemas propios o proporcionados por terceros.

- Es un sistema que se puede aplicar a distintos tamaños de comunidades sin generar costos adicionales.
- Su comunidad está conformada por 350 instituciones que apoyan a millones de estudiantes en los EUA y 4 millones de estudiantes a nivel mundial, lo cual contribuye a la mejora continua de la plataforma.
- Ofrece la oportunidad de forjar un sistema solida de aprendizaje que apoye a su institución en el tránsito hacia el futuro y los nuevos sistemas de educación a distancia.

Desventajas

- Se pueden llegar a encontrar diferentes deficiencias que pueden tardar en ser arregladas debido a su sistema de establecer prioridades.
- La interfaz de usuario puede llegar a ser compleja para algunas personas.
- Al ser un proyecto escrito en leguaje Java obliga a los suaurios a instalar software adicional.
- La documentación esta desorganizada, dispersa, es abundante y en ocasiones redundante u obsoleta.
- Debido al punto anterior puede ser complicado encontrar información relacionada a problemas tanto para los administradores como para los usuarios.
- La curva de aprendizaje para la administración de la plataforma es bastante grande por lo que puede ser tardado tener una administración adecuada.
- Pese al tamaño de su comunidad esta es pequeña en comparación con otras plataformas.

Conclusión.

Sakai fue un pionero para el termino de proyecto colaborativo lo que ha permitido satisfacer las necesidades de distintas instituciones educativas, con ayuda de herramisntas de aprendizaje, la enseñanza y la colaboración para las investigaciones.

Gracias al trabajo comunitario, la plataforma mejora de manera progresiva, por lo que sus deficiencias y problemas pueden ser eliminadas en las versiones subsecuentes y también se puede adaptar a los nuevos enfoques educativos.

1.3.2. Chamilo.

Figura 1.3. 2 Logo Chamilo e-Learning & Colaboration Software

Chamilo es un sistema de gestión de aprendizaje o LMS (Learning Management System), diseñado para apoyar a la educación en línea. Es una plataforma de software libre escrita en PHP, cuyo propósito es mejorar la educación y su acceso a ella a nivel mundial. Este software gratuito es fruto de la colaboración de varias empresas, organizaciones e individuos de acuerdo con el modelo de código abierto bajo estrictos valores éticos. Se distribuye bajo la Licencia Pública General de GNU/GPLv3. Este tipo de licencias para software está destinada a garantizar la libertad para compartir y cambiar todas las versiones de un programa, lo cual asegura que sea gratuito para todos sus usuarios, permitiendo instalar, modificar y crear elementos complementarios para poder adaptarse a las necesidades específicas de cada proyecto de e-learning. Es por este motivo, por el que sus creadores escogieron el nombre Chamilo, que surge del diminutivo de la expresión en inglés Chameleon.

El origen de esta plataforma se encuentra en la Asociación Chamilo, una organización sin ánimo de lucro cuyo objetivo principal es mantener la plataforma y asegurar su continuidad.

Ventajas.

- Simplicidad de uso para el docente y el alumno
- Cuidado estético y fácil creación de contenidos

- Soporte multi idiomas
- Portabilidad y rapidez con instalación sencilla y rápida
- Opciones útiles visibles
- Seguimiento de cursos y usuarios mediante detallados informes de actividad
- Comunicación síncrona y asíncrona, también videoconferencias
- Herramientas de autor para creación de nuestros propios cursos
- Gran capacidad de gestión documental

Desventajas.

- Mayor esfuerzo y dedicación por parte del profesor
- La plataforma precisa ser actualizada constantemente.
- Se pueden llegar a encontrar diferentes deficiencias que pueden tardar en ser arregladas debido a su sistema de establecer prioridades.
- La interfaz de usuario puede llegar a ser compleja para algunas personas.
- Pese al tamaño de su comunidad esta es pequeña en comparación con otras plataformas.

Conclusiones.

De acuerdo con los testimonios de diferentes instituciones que han implementado la plataforma Chamilo destaca por ser sencilla, intuitiva y estructurada. Además, su diseño es visualmente atractivo y no saturado con demasiadas opciones, muy bien enfocada a la experiencia de los usuarios.

Chamilo cuenta con las herramientas necesarias para la comunicación y la colaboración entre sus usuarios, la creación y reutilización de contenidos, la planeación didáctica y la evaluación de los estudiantes en los cursos.

Chamilo puede ser utilizada para operar cursos en línea o como apoyo para un curso presencial.

1.3.3. ATutor.

Figura 1.3. 3 Logo ATutor

ATutor es un sistema de gestión de contenidos de aprendizaje de código abierto. La principal finalidad de esta herramienta es ofrecer un nivel de accesibilidad y adaptabilidad elevado en la web. Al ser de código abierto, lo convierte en una herramienta rentable para organizaciones pequeñas y grandes que desarrollan contenido educativo y ofrecen cursos en la web. En este sentido se puede copiar, distribuir y modificar ATutor atendiendo a los términos de la Licencia Pública General GNU (GPL).

ATutor es el primer sistema de gestión de contenidos de aprendizaje que cumple las condiciones de accesibilidad del World Wide Web Consortium WCAG 1.0 en el nivel de AA+, permitiendo el acceso a todos los estudiantes potenciales, instructores, y administradores, incluyendo a aquellos que tienen algún tipo de discapacidad como, por ejemplo, la visual. La conformidad con el estándar XHTML 1.0 del World Wide Web Consortium asegura que ATutor esté constantemente presente en cualquier tecnología compatible con los estándares.

Ventajas.

- Promueve una pedagogía constructivista social (colaboración, actividades, reflexión crítica, etc.).
- Apropiada para el 100% de las clases online, así como también para complementar el aprendizaje presencial.
- Tiene una interfaz de navegador de tecnología sencilla, ligera, eficiente y compatible.
- Es fácil de instalar en casi cualquier plataforma que soporte PHP. Sólo requiere que exista una base de datos (y la puede compartir).

- Con su completa abstracción de bases de datos, soporta las principales marcas de bases de datos (excepto en la definición inicial de las tablas).
- La lista de cursos muestra descripciones de cada uno de los cursos que hay en el servidor, incluyendo la posibilidad de acceder como invitado.
- Los cursos pueden clasificarse por categorías y también pueden ser buscados - un sitio ATutor puede albergar miles de cursos.
- Se ha puesto énfasis en una seguridad sólida en toda la plataforma. Todos los formularios son revisados, las cookies encriptadas, etc.
- La mayoría de las áreas de introducción de texto (recursos, mensajes de los foros etc.) pueden ser editadas usando el editor HTML, tan sencillo como cualquier editor de texto de Windows.

Desventajas.

- Los foros, actividades y recursos están separados.
- La interfaz en la que crea el profesor es diferente a la del alumno.
- No cuenta con la posibilidad de crear itinerarios de aprendizaje.
- No se pueden poner tareas offline/online.
- No cuenta con documentación adecuada.
- La solución de problemas puede complicarse demasiado debido a la falta de documentación.

Conclusiones.

ATutor es una herramienta de código abierto cuya mayor deficiencia es la falta de soporte por parte de su comunidad ya que esta es bastante reducida, por lo cual resulta complicado tenerla en un nivel funcionamiento optimo. Como la plataforma ATutor requiere de un equipo técnico especializado esto lo pone en desventaja en comparación con otras plataformas que no requieren un conocimiento técnico avanzado para ser implementadas.

Asimismo, la plataforma requiere de mantenimiento constante ya que puede presentar vulnerabilidades si las actualizaciones no las realiza un equipo técnico especializado.

Pese a que no es la mejor opción para implementar por la curva de aprendizaje que conlleva su mejor cualidad es que esta plataforma puede ser utilizada por personas con discapacidades audiovisuales lo cual es un gran plus a sus funcionalidades.

1.3.4. Moodle

Figura 1.3. 4 Logo Moodle

Moodle es una plataforma de código abierto dedicada al aprendizaje, tiene como objetivo brindarle a educadores, administradores y estudiantes un sistema integrado único, robusto y seguro. Moodle está disponible en más de 100 idiomas y tienen la confianza de instituciones y organizaciones grandes y pequeñas.

Debido a que Moodle es una herramienta de código abierto permite a los desarrolladores el crear plugins e integrar aplicaciones externas para lograr funcionalidades específicas, además es constantemente revisada y mejorada por la comunidad de Moodle lo que permite que la plataforma se adapte a las necesidades actuales y cambiantes de los usuarios.

Moodle cuenta con dos formas de implementarlo, Moodle que necesita descargar y realizar el procedimientos de instalación este es totalmente gratuito, y Moodle Cloud que es la versión en la nube de Moodle que permite utilizarlo sin la necesidad de realizar todo el proceso de instalación, esta versión también es gratuita pero está limitada a 50 usuarios y 200 MB de almacenamiento para archivos aunque si se paga una cuota anual se obtiene más capacidad de almacenamiento y de usuario además de funciones extras.

Con respecto a los cuestionarios estos están formados por preguntas contenidas en una base de datos, estas preguntas son creadas mediante alguna de las plantillas que ya contiene la plataforma o es posible crear una plantilla personalizada de acuerdo a las necesidades particulares de cada profesor o bien utilizar algún plugin creado por la comunidad para crear una pregunta con un formato en particular.

La primera versión de Moodle se lanzó en 2001 comenzando como un blog y a lo largo del tiempo continuó desarrollándose hasta convertirse en lo que hoy se conoce como plataformas e-learning, su última versión estable es la 3.8 compilación 9 que data de marzo de 2020.

A diferencia de nuestras dos posibles alternativas Moodle no es una herramienta única de cloud, debido a que provee la opción de ser instalada dentro de la intranet de la organización con el fin de capacitar a sus integrantes o usarlo como portal para almacenar información de la organización a modo de una base de conocimientos

Su objetivo de desarrollo es brindar una opción de aprendizaje gratuito como lo indican en su web oficial:

"Moodle es un sistema de gestión de aprendizaje en línea gratuito que brinda a los educadores de todo el mundo una solución de código abierto para el aprendizaje electrónico que es escalable, personalizable y segura con la mayor selección de actividades disponibles. Moodle cuenta con el respaldo de una red activa de Socios certificados de Moodle para ayudar con el soporte y una comunidad activa de desarrolladores, usuarios y seguidores."[2]

[2] *Acerca de Moodle - MoodleDocs*. (s. f.). Moodle. Recuperado 18 de agosto de 2020, de https://docs.moodle.org/all/es/Acerca_de_Moodle

Las versiones anteriores de Moodle aún se encuentran disponibles para su uso, pero incluso la web oficial de Moodle recomienda no hacer uso de estas ya que no cuentan con soporte o utilizan software muy antiguo o no compatible con equipos actuales.

Ventajas:

- Es una plataforma relativamente sencilla de usar para los profesores y estudiantes.
- Es altamente personalizable.
- Es fácilmente escalable.
- Tiene gran compatibilidad con cualquier navegador web.

Desventajas:

- La versión Cloud tiene varias limitaciones.
- Actualmente no tiene compatibilidad con celulares inteligentes.
- Se requiere una capacitación para los administradores y profesores.
- La versión estándar de Moodle necesita de ciertos requerimientos de software y hardware para su implementación.

Conclusión.

En la actualidad Moodle es una plataforma libre la cual cuenta comuna comunidad más amplia, la cual actualiza y mejora constante mente la plataforma, si se realiza una búsqueda de la palabra Moodle en Google Search se encuentran alrededor de 66 millones de resultados una gran diferencia a comparación con las demás plataformas como Chamilo con 478 mil resultados.

Esto posiciona a Moodle como la plataforma libre con más contenido, desarrollo y mantenimiento pese a que su documentación esta dispersa y no completamente estructurada, los foros son una fuente de conocimientos y soluciones a problemas

de administración e integración de materiales, por lo que no resulta tan complicado solucionar problemas.

1.3.5. Claroline

Figura 1.3. 5 Logo Claroline

Claroline es una plataforma de aprendizaje y software colaborativo de código abierto y gratuito. Lleva una licencia GNU y está publicado bajo la licencia de código abierto GPLv2. Permite a cientos de instituciones de todo el mundo (universidades, colegios, asociaciones, empresas...) crear y administrar cursos y espacios de colaboración en línea.

Reutiliza códigos disponibles en la extensa biblioteca del GLP open source. Thomas De Praetere creó Claroline en UCLouvain (Universidad Católica de Lovaina), con la ayuda financiera de Fondation Louvain, Hugues Peeters (quién dio el conocido nombre "Claroline") y Christopher Gesché, financiado por UCL también (Fonds de développement pédagogique).

Ventajas

- Es un poderoso entrenador. Posibilita hacer diferentes pruebas como preguntas de opción múltiple, de selección, emparejamientos, tablas o clasificaciones.
- Ofrece variedad de recursos múltiples. Permite crear contenidos que ayuden a la adquisición de competencias, por ejemplo, vídeos, foros, cuestionarios, o evaluaciones.

- Tiene caminos de aprendizaje. Le proporciona al estudiante seguir un camino lógico y simple a través de las rutas de aprendizaje con contenidos.
- Es un gestor de habilidades. Permite crear repositorios de habilidades, los cuales, se pueden enlazar a los cursos o personas, para ver la evolución de esas habilidades.
- Es una plataforma abierta y sencilla.
- Permite conformar cada sector, para conseguir aspectos y estilos personalizados y flexibles.
- Posibilita administrar cursos virtuales en entornos de aprendizaje en línea de forma rápida.

Desventajas

- Es poco modificable.
- No se pueden exportar los cursos.
- Tiene escasos módulos y pocos plugins para descargar.
- Las personalizaciones son un poco difíciles.
- La comunidad de los usuarios españoles es reducida.

1.3.6. Selección de la plataforma.

Entre las opciones mostradas existe un universo gigante de plataformas LMS tanto de código libre como de pago por licencias que se pueden adaptar a nuestras necesidades, sin embargo, consideramos únicamente plataformas de código libre, y que ya sean implementadas por la universidad para reducir el número de plataformas a considerar.

Y una vez realizado el análisis de las posibles LMS que poseen la capacidad de crear y alojar los videos del laboratorio, los materiales de apoyo y didácticos, se llegó a la decisión de utilizar la plataforma de Moodle debido a que es una de las opciones más completas en cuanto a desarrollo de cursos en línea por la cantidad de herramientas desarrolladas por su comunidad, con lo cual se tendría una mayor cantidad de opciones al momento de desarrollar y gestionar los cursos, pese a que

las demás plataformas también podrían ser una alternativa, no se implementaron debido a la escases de documentación comparada a la cantidad con la que cuenta Moodle.

Otro motivo por el cual se seleccionó la plataforma de Moodle es que en la facultad existe registro de que esta plataforma es viable para ser usada como apoyo a la enseñanza de la asignatura de Redes De datos Seguras, y es el caso de la plataforma de EDUCAFI la cual está construida con este LMS. Además, de que otras instituciones educativas también hace uso de Moodle como es el caso de la Nepal Open University, la Royal College of Art, la Dulwich College International, la Universitat Politècnica de Catalunya, la Louisiana State University, entre otras.

Además de esto otro de los motivos para seleccionar Moodle es que es una plataforma que se ha utilizado anteriormente como estudiante, tomando cursos en esta plataforma y se ha tenido una experiencia satisfactoria debido a que el enfoque que tienen la plataforma es la de facilitar la impartición de conocimiento tanto para profesores como para los estudiantes. Por último, como esta herramienta es de código abierto no se tiene que realizar una inversión monetaria y es posible realizar modificaciones a nivel de código u obtener actualizaciones oficiales.

Capítulo 2. Diseño.

En este capítulo se desarrolla el diseño del material didáctico, las formas en las cuales se encuentran los reactivos y se muestra el diseño para la integración de los materiales en la plataforma seleccionada (Moodle).

2.1 Diseño de preguntas.

Se desarrollaron distintos estilos de preguntas para que los cuestionarios que forman parte del material didáctico se adapten a lo que se busca evaluar en cada uno de los temas, por ello se diseñaron los siguientes tipos de reactivos:

Tipo 1. Pregunta de opción múltiple con única respuesta correcta.

En el tipo 1 de pregunta (véase la figura 2.1) se realiza un cuestionamiento o se pide completar alguna sentencia con el fin que el estudiante seleccione una sola opción, este tipo de pregunta cuenta con una única respuesta correcta y dos o más respuestas incorrectas v que funcionan como distractores.

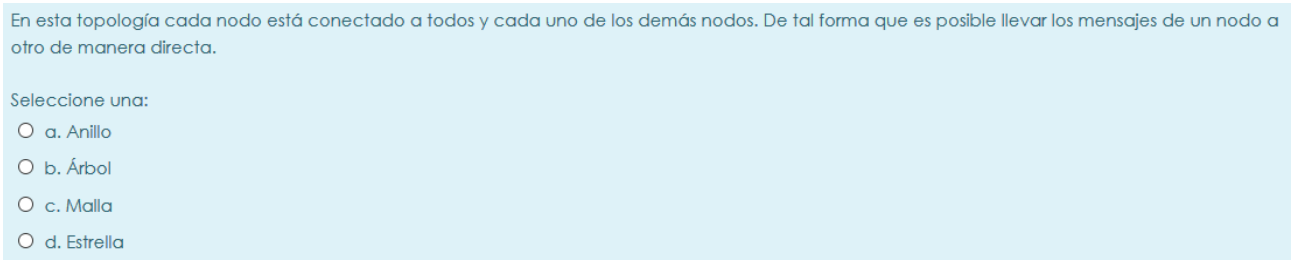


Figura 2.1. Ejemplo de cómo luce una pregunta del tipo 1, opción múltiple con única respuesta.

Este tipo de preguntas se realiza principalmente para evaluar cuestiones teóricas del tema donde el estudiante debe de tener el conocimiento sobre algún concepto en específico.

Tipo 2. Pregunta de opción múltiple con múltiples respuestas correctas.

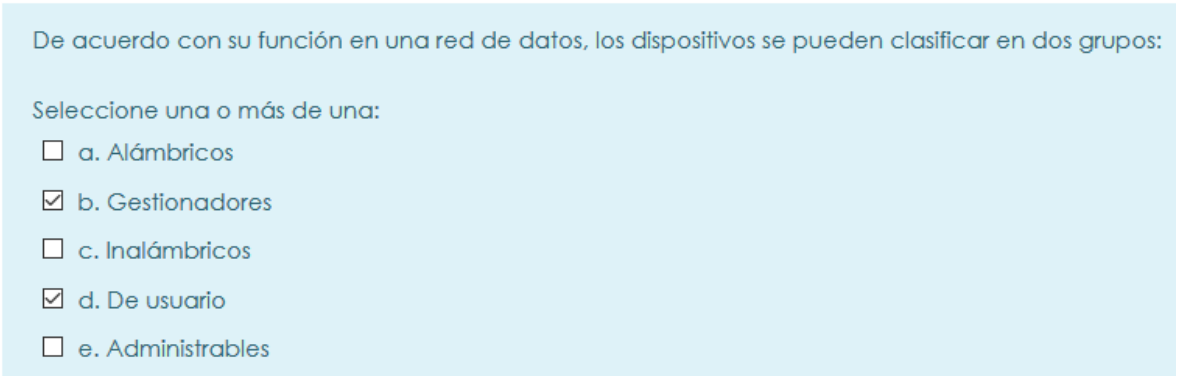


Figura 2.2. Ejemplo de cómo luce una pregunta del tipo 2, opción múltiple con múltiples respuestas correctas.

En el tipo 2 de pregunta (véase figura 2.2) se realiza un cuestionamiento con el fin de que el estudiante seleccione dos o más opciones, este estilo cuenta con dos o más respuestas correctas y dos o más respuestas incorrectas.

Se realiza este tipo de reactivo cuando se quiere evaluar una cuestión teórica pero el conocimiento evaluado se relaciona con distintos conceptos a la vez.

Tipo 3. Pregunta de relación de columnas.

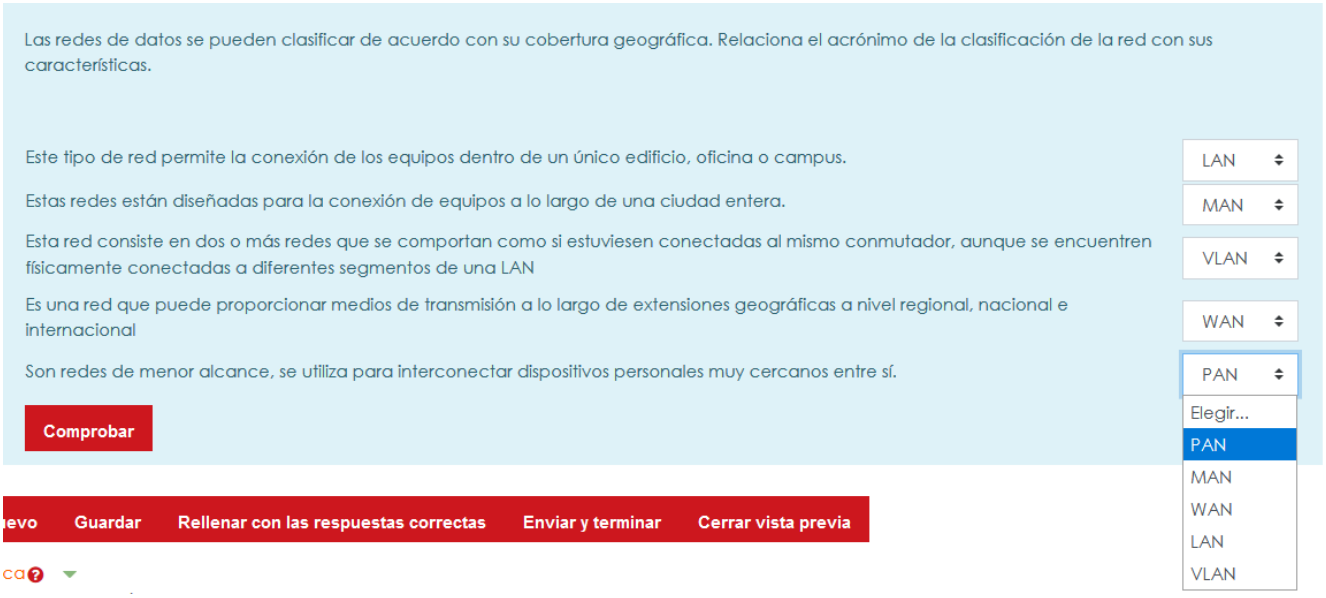


Figura 2.3 Ejemplo de cómo luce una pregunta tipo 3, relacion de columnas

En el tipo 3 de pregunta (véase figura 2.3) se le solicita al estudiante que combine una columna con otra, esta relación es de uno a uno o bien de uno a muchos.

Este tipo de pregunta se utiliza principalmente para evaluar cuestiones teóricas en las cuales se considera necesario comprobar que el estudiante es capaz de distinguir y relacionar un concepto con su correcta definición.

Tipo 4. Preguntas de respuesta cierto o falso.

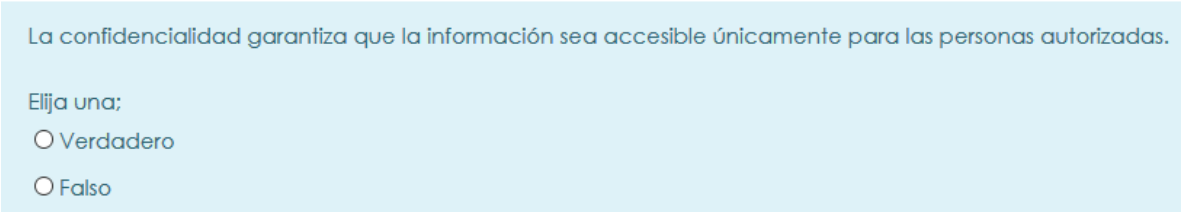


Figura 2.4. Ejemplo de cómo luce una pregunta tipo 4, cierto o falso

En el tipo 4 de pregunta (véase figura 2.4) se cuestiona al estudiante sobre un concepto o alguna afirmación donde tendrá que diferir si es cierta o falsa.

Este tipo de pregunta es utilizado para evaluar cuestiones teóricas donde se considera importante que el estudiante sea capaz de identificar una definición o una descripción de un concepto en particular.

Tipo 5. Arrastrar y soltar.

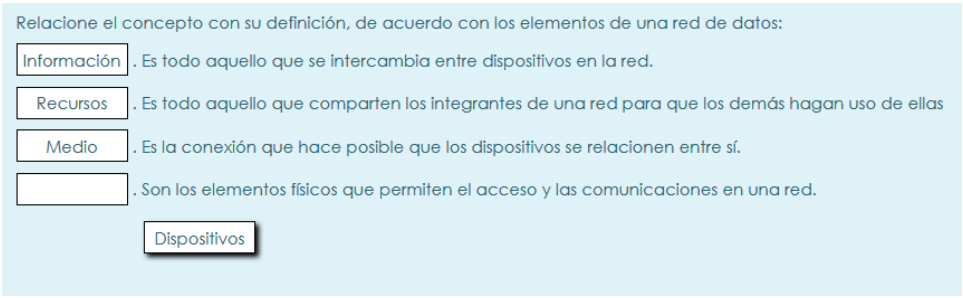


Figura 2.5. Ejemplo de cómo luce una pregunta del tipo 5, arrastrar y soltar

En el tipo 5 de pregunta (véase figura 2.5) son utilizadas como alternativa a la relación de columnas, se trata de que el estudiante relacione un concepto con su correcta definición, la principal diferencia es en cómo lucen las preguntas para que no se sientan las preguntas monótonas al realizar una acción distinta a la habitual.

Tipo 6. Respuesta libre.

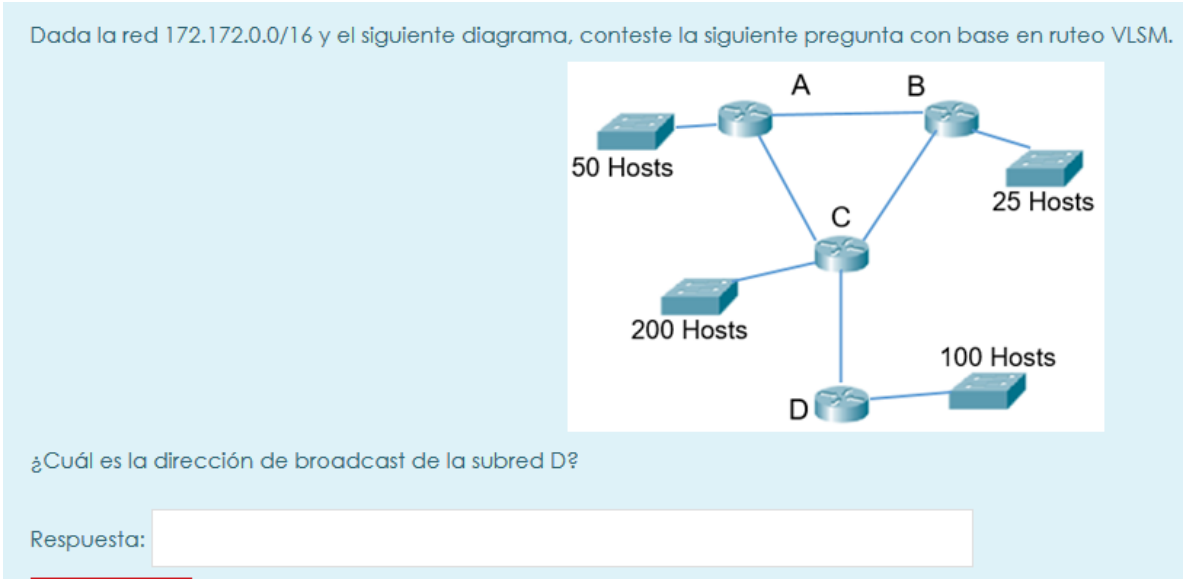


Figura 2.6. Ejemplo de cómo luce una pregunta del tipo 6, Respuesta libre.

En el tipo 6 de pregunta (véase figura 2.6) se le cuestiona al estudiante sobre una respuesta exacta sin darle alguna opción. Y se utiliza para validar conocimiento que involucra la resolución de problemas, para ello se plantea un ejercicio que el estudiante debe contestar de manera correcta.

Tipo 7. Múltiples respuestas libres.

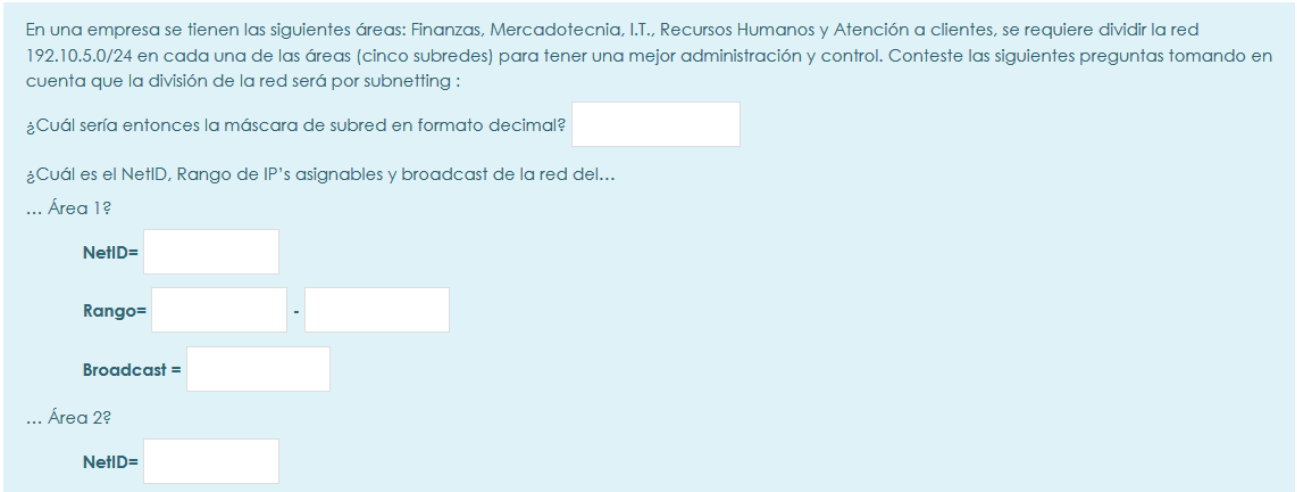


Figura 2.7. Ejemplo de cómo luce una pregunta del tipo 7, Múltiples respuestas libres.

En el tipo 7 de pregunta (véase figura 2.7) el estudiante rellena cada recuadro conforme realiza la resolución del ejercicio propuesto. Es utilizada para evaluar conocimiento relacionado con la resolución de problemas, pero a diferencia del tipo 6 de pregunta, cada una de las respuestas están en cierta medida relacionadas, en el caso de que el estudiante conteste incorrectamente a alguna de ellas será capaz de identificar en qué punto se equivocó.

2.2 Diseño de cuestionarios.

Para cada tema se ha creado un cuestionario en la plataforma de Moodle, cada cuestionario cuenta con diez preguntas tomadas de manera aleatoria de una base de datos que contiene todos los reactivos formulados para cada tema. Estos cuestionarios no tienen un límite de tiempo para ser solucionados con el fin de darle la oportunidad al estudiante de revisar distintos materiales en caso de que no esté seguro de su respuesta y con ello repase los conceptos que le sean necesarios. Además, el estudiante será capaz de resolver las veces que desee un cuestionario y con el beneficio de resolver distintas preguntas debido a la selección aleatoria que se hace del banco de preguntas desarrollado.

El número total de reactivos almacenados en la base de datos de cada cuestionario se determinó de acuerdo a la relevancia del tema y al número de horas que se ha establecido en el programa para su estudio (véase tabla 2.1).

Tabla 2.1. Cantidad de reactivos creados por cuestionario.

Tema	Cantidad de preguntas.
Tema 1. Conceptos básicos.	50
Tema 2. Estándares y arquitecturas.	50
Tema 3. Capa física.	50
Tema 4. Capa de enlace de datos.	50

Tema 5. Capa de red.	62
Tema 6. Capa de transporte.	51
Tema 7. Capa de sesión.	29
Tema 8. Capa de presentación.	31
Tema 9. Capa de aplicación.	61

2.3 Diseños de integración de materiales en la plataforma seleccionada.

Para la integración de los materiales es importante identificar el tipo de material (material de apoyo, reactivos o vídeos de prácticas del laboratorio) así como de las herramientas de las cuales dispone la plataforma para que estos materiales se pongan a disposición de los estudiantes de la asignatura de Redes de Datos Seguras.

2.3.1 Material de apoyo.

El material de apoyo que se pone a disposición de los estudiantes es en su totalidad textos, los cuales tienen las opciones de ser presentados de las siguientes formas:

2.3.1.1 Libro de Moodle.

Moodle cuenta con un recurso llamado “Libro” el cual se pude editar para presentar la información en un formato parecido a un libro virtual con la capacidad de agregar texto, imágenes, enlaces externos y contenido multimedia.

Figura 2.8. Ejemplo de cómo se ve un libro de Moodle.

Ventajas.

- El contenido de los libros de Moodle es más dinámico que los que habitualmente se usan debido a la capacidad de usar recursos como audios o videos.
- La navegación por este recurso es sencillo e intuitivo, se utilizan las flechas para recorrer la información de manera secuencial o bien mediante la tabla de contenidos para ir directamente al subtema deseado.
- Una vez conocido el funcionamiento de Moodle es sencillo crear este recurso.
- Se tiene la opción de imprimir el libro, ya sea completo o solo algunos subtemas, esto es posible directamente en papel o bien en un archivo PDF para ser usado fuera de línea.

Desventajas.

- Para crear un libro se requiere de cierto conocimiento de Moodle he incluso de lenguaje HTML.

- La presentación de material de este tipo está limitada a lo que se pueda hacer en HTML.
- La apariencia alcanzada con esta opción es inferior.

2.3.1.2 Disposición de archivos de texto.

Moodle tienen la capacidad de albergar archivos en distintos formatos para que puedan ser consultados por los estudiantes.

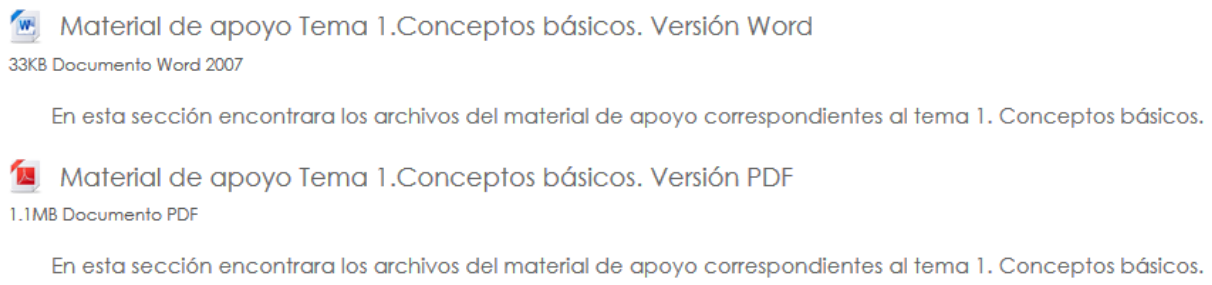


Figura 2.9. Ejemplo de cómo lucen los archivos subidos a Moodle.

Ventajas.

- Es posible abrir los archivos desde el mismo navegador, sin la necesidad de descargar software extra, siempre y cuando el buscador lo soporte como es el caso de los archivos PDF.
- Posee la opción de definir la actividad que realiza con los archivos como puede ser abrirlos en una ventana nueva, incrustarlos en el mismo Moodle o bien que solo se descargue.
- La edición del archivo depende del software con el que es creado, esto da la posibilidad de que el material tenga una presentación más acorde a lo que se necesite.

Desventajas.

- Cuando el contenido es descargado, se depende de que el estudiante tenga el software necesario para abrirlo.
- Con esta opción no es posible realizar la combinación de contenido multimedia con texto como en los libros de Moodle

- Para actualizar la información en un archivo se requiere eliminar el actual y subir nuevamente el archivo en su versión actualizada que, dependiendo del archivo y la conexión, es un proceso tardado y lento.

2.3.1.3 Forma de integración del material de apoyo.

Se analizaron las dos opciones presentadas y mediante una consulta a la persona responsable del material se llegó a la decisión de utilizar la opción de subir el material a la plataforma, esto es debido a que el material de apoyo únicamente es texto ya presente en una serie de archivos PDF los cuales ya cuentan con un diseño realizado con cuidado. El material se podrá visualizar directamente para su lectura en una ventana nueva sin menús y con la opción de descargar, esto es con la finalidad de disminuir los distractores y dar la posibilidad de guardar el material por si se requiere su consulta sin la necesidad de tener conexión a internet.

2.3.2 Videos de prácticas del laboratorio.

Es posible presentar los videos de las practicas del laboratorio mediante dos posibles opciones:

2.3.2.1 Alojamiento externo.

Los videos son alojados en una plataforma ajena a la que contiene el Moodle, como son las plataformas de You Tube, Vimeo y Wistia las cuales son la que tienen mayor compatibilidad con Moodle.

Práctica 6 del laboratorio de redes de datos seguras (You Tube)

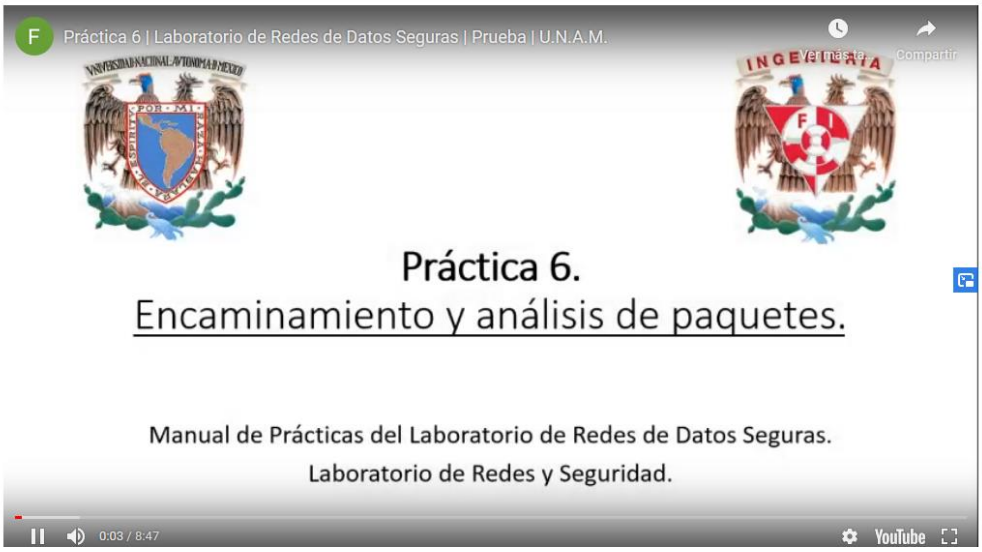


Figura 2.10. Ejemplo de cómo se vería un video incrustado en Moodle, pero alojado en una plataforma externa (Youtube).

Ventajas.

- Cómo es alojado en una plataforma externa no se requiere de espacio adicional para guardar estos videos.
- La calidad que es ofrecida depende de la plataforma y del video subido a ella, en caso de que se necesite reducir la calidad del video es posible sin tener que rehacer el video. Pero siempre la plataforma busca presentar el video con la máxima calidad posible.
- El tráfico de red de la trasmisión del video es soportado por la plataforma que aloja el material.

Desventajas.

- Se tiene una dependencia de la disponibilidad de la plataforma seleccionada, si la plataforma no está disponible tampoco lo están los videos.

- Los videos tienen una marca de agua que redirecciona a la plataforma que aloja el material, dentro de esta plataforma no se tiene control del resto de contenido disponible.
- En ciertas plataformas se tiene que pagar para tener el servicio de alojamiento como es en los casos de Vimeo y Wistia.

2.3.2.2 Alojamiento interno.

En este caso el video es almacenado directamente en el servidor del laboratorio y es puesto a la disposición del estudiante como un archivo incrustado para que pueda ser visualizado desde un curso de Moodle.

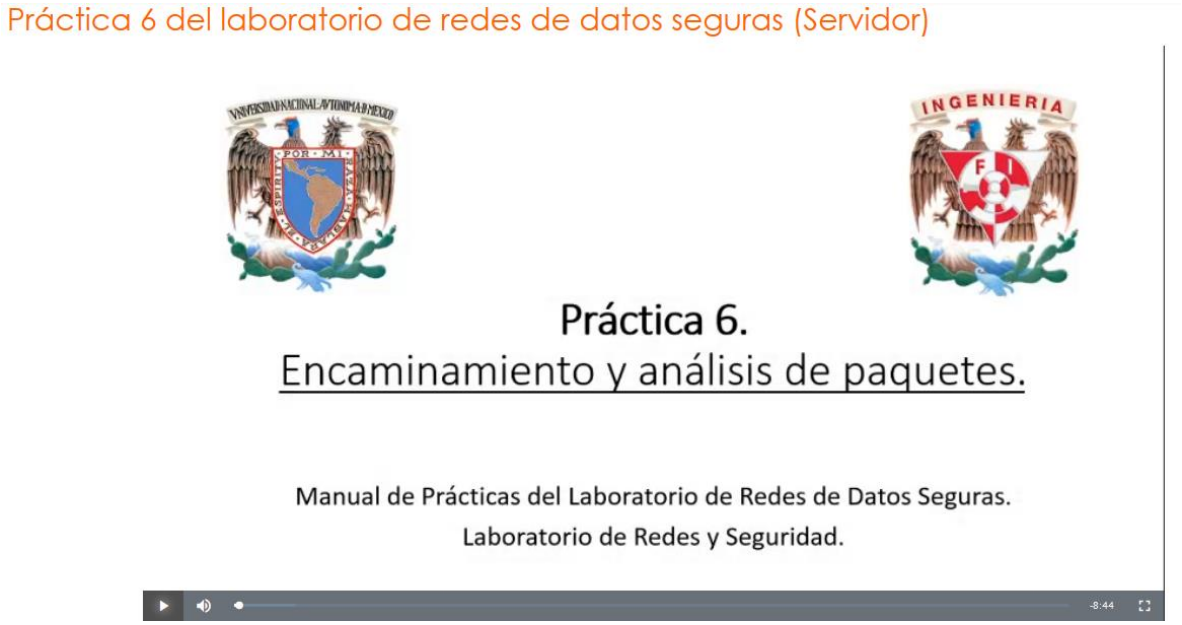


Figura 2.6. Ejemplo de cómo se vería un video incrustado en Moodle y que está alojado en el mismo servidor.

Ventajas.

- Al estar almacenado en el servidor de Moodle se tiene control total de este material.
- La calidad del video depende únicamente de la producción de este.
- Este método de presentar videos evita las distracciones que existen en otras plataformas debido a que solo se muestra contenidos de la materia.

Desventajas.

- Se requiere de más capacidad de almacenamiento disponible en el servidor que alberga Moodle para también guardar los videos.
- El servidor que almacena Moodle deberá de ser capaz de soportar el tráfico generado por la reproducción de los videos.

2.3.2.3 Forma de integración de los videos del laboratorio.

Después de observar las opciones disponibles se ha optado por el alojamiento interno de los videos del laboratorio de la asignatura de redes de datos seguras. Esto es porque se busca tener el control total de este material y no depender de una plataforma externa la cual también puede provocar distracciones debido a que en estas plataformas se presentan contenido ajeno a la materia.

Además, esta opción nos permite presentar los videos manteniendo la calidad con la que han sido creados ayudando a su correcta presentación hacia los estudiantes.

Capítulo 3. Desarrollo e implementación.

Con base en los capítulos anteriores, en éste se muestra el desarrollo y la implementación de los cuestionarios, así como la integración de los materiales de apoyo y los videos del laboratorio de Redes de Datos Seguras, todo ello contenido en la plataforma de Moodle.

3.1. Infraestructura base.

Para la implementación de la plataforma es necesario contar con un equipo el cual cumpla con las especificaciones requeridas por Moodle para funcionar adecuadamente.

Los requisitos que Moodle recomienda son los siguientes:

Hardware

- **Espacio en disco:** 200 MB para el código de Moodle mas lo que sea requerido por los recursos cargados.
- **Procesador:** 1 GHz (mínimo), 2 GHz dual core recomendado.
- **Memoria RAM:** 512 MB (mínimo), 1 GB recomendado

Nota: Se recomienda tener un habiente distribuido entre la interfaz web y la base de datos para una mayor seguridad.

Estos requisitos son únicamente para el funcionamiento de la plataforma ya que no consideran los recursos adicionales que se cargaran en la plataforma, el administrador es el encargo de corroborar los requisitos requeridos para uso en su infraestructura. Pero con base en estos requisitos, en este tema abordaremos las consideraciones que se tomaron en cuenta para realizar la implementación de Moodle y la selección de proveedor para probar la instalación.

3.1.1. Requisitos Moodle y selección de proveedor.

Moodle funciona en sistemas operativos tanto Windows como Linux, pero de acuerdo con la documentación oficial de Moodle es preferible el uso de Linux haciendo uso de una estructura LAMP (Linux, Apache, MySQL/MariaDB y PHP).

Existe una gran variedad de proveedores de “cloud computing” como puede ser Digital Ocean, Amazon Web Services, Microsoft Azure, por nombrar algunos que ofrecen el servicio de maquinas virtuales en la nube. Para hacer una selección de proveedor, fue necesario revisar si estos proveedores cuentan equipos que

cuenten con equipos que cumplan las características mínimas necesarias, se tomó en cuenta nuestra experiencia con estos proveedores en proyectos escolares, sí contaban con algún plan gratuito y sí las máquinas que ofrecen cubren con los requisitos de Moodle. Los principales proveedores analizados son los siguientes:

- **Amazon Web Services**

Amazon Web Services (AWS) es una colección de servicios de cómputo en la nube pública (también llamados servicios web) que en conjunto forman una plataforma de cómputo en la nube, estos servicios web son ofrecidos a través de internet por Amazon.com. Es usado en aplicaciones como Dropbox, Foursquare, HootSuite.

Este proveedor ofrece un plan de gratuito en Elastic Compute Cloud (EC2) los cuales son equipos de propósito general, este plan gratuito ofrece 750 horas de uso de la computadora durante 12 meses. Este plan ofrece máquinas del tipo t2.micro el cual cuenta con un sistema operativo Linux, un procesador virtual Intel Xeon, 1 GB de RAM y 500 GB de almacenamiento HDD o 1GB de almacenamiento SSD.

- **Microsoft Azure**

Microsoft Azure es un servicio de cómputo en la nube creado por Microsoft para construir, probar, desplegar y administrar aplicaciones y servicios mediante el uso de sus centros de datos. Proporciona software como servicio (SaaS), plataforma como servicio (PaaS) e infraestructura como servicio (IaaS).

Azure tiene un plan gratuito similar al que ofrece AWS el cual pone a disposición una máquina de propósito general que es llamado como “burstable” (B - series), el plan ofrece 750 horas de uso al mes por 12 meses, además ofrece $200 créditos para ser usados en el primer mes de suscripción. La máquina que ofrece es una B1S el cual posee un vCPU, 1 GB de RAM y 4 GB de almacenamiento SSD.

- **Google Cloud Plataform**

Google Cloud Plataform (GCP) es una plataforma que reúne todas las aplicaciones de desarrollo web que ofrece Google. Es utilizada para crear ciertos tipos de soluciones a través de la tecnología almacenada en la nube como puede ser computación en la nube, bases de datos, almacenamiento de información, aplicaciones relacionadas con inteligencia artificial, entre otros.

GCP ofrece planes gratuitos distintos a los vistos anteriormente, este plan ofrece una máquina f1-micro cada mes de por vida, además, para los nuevos usuarios ofrece una prueba gratuita de $300 créditos por 90 días para ser usado en cualquier servicio. La máquina f1-micro tiene 1 vCPU, 0.6 GB de RAM y 30 GB de almacenamiento HDD.

Con base en la información recabada de los proveedores de cloud computing y en particular de los planes gratuitos que ofrecen, así como de las máquinas a la que se tienen acceso en estos planes, se realizó un análisis comparativo entre los distintos proveedores para tomar la decisión y seleccionar el que se utilizó en el desarrollo del presente proyecto (véase tabla 3.1).

Tabla 3.1. Comparación entre las distintas empresas que ofrecen cómputo en la nube.

Tabla 2.1. Comparación de plataformas

	Plan gratuito	Plan de prueba	Cumple con los requisitos de Moodle.
Microsoft Azure	Si, 750 hrs/mes durante12 mese	Si, $200 por 30 días	Si
Google Cloud Plataform	Si, 1 instancia cada mes	Si, $300 por 90 días	Si
Amazon Web Services	Si, 750 hrs/mes durante12 mese	No	Si

Cada una de las plataformas cumplen con el punto de poseer un plan gratuito y ofrecer en ese plan una máquina que cumpla con los requisitos mínimos para instalar Moodle (véase tabla 3.1). Para hacer nuestra selección tomamos en cuenta un factor que difiere de acuerdo con el proveedor que es la prueba gratuita. En el caso de AWS no se cuenta con una prueba gratuita, en los casos de Azure y GCP cuentan con una prueba gratuita la cual es distinta en la cantidad de créditos y tiempo que ofrecen.

Para el proyecto se necesita un tiempo amplio para realizar la implementación de Moodle y la integración de los materiales, por eso mismo, el proveedor seleccionado fue GCP debido a que ofrece un máximo de 3 meses, tiempo que es duplicable debido a que somos dos personas que podemos crear una cuenta cada uno. Además, el crédito que disponemos es mayor al que ofrece Microsoft Azure esto permite solicitar una máquina con especificaciones un tanto mayores a los que necesita Moodle para así realizar toda la implementación sin complicaciones relacionadas con el hardware.

3.1.2 Máquina Virtual.

Una vez seleccionado el proveedor se procedió a solicitar una máquina la cual tenga especificaciones que superen a los requeridos por Moodle, pero sin que supere la cantidad de créditos que factura durante el periodo de pruebas. Esta máquina tiene las siguientes especificaciones:

- Tipo de máquina: n1-estándar-1.
- CPU: 1 CPU virtual.
- RAM: 4 Gb.
- Tipo de Almacenamiento: Disco duro mecánico.
- Capacidad de Almacenamiento: 10 Gb.
- Memoria persistente: Si.
- Sistema operativo: Debian 9 Stretch.
- IP Publica: 34.94.93.240.

3.2. Implementación de la plataforma

Una vez que se seleccionó la máquina virtual y se comprobó que efectivamente podía soportar la implementación de software adicional y la implementación de material didáctico dentro de la plataforma, se procedió a la instalación de la estructura LAMP necesaria para el funcionamiento.

3.2.1. Software Adicional

Como se mencionó anteriormente, es necesaria una estructura LAMP dentro de la máquina virtual a utilizar para el funcionamiento de la plataforma con lo cual el software seleccionado se basó en las recomendaciones de instalación de Moodle.

- Linux: no tiene ninguna preferencia por alguna versión del sistema operativo, así que utilizamos el que venía por defecto en la máquina virtual de Google Cloud Debian 9 Stretch.
- Apache: Utilizamos la última versión de Apache que corresponde a la 2.4.43.
- PHP: la recomendación es a partir de PHP 5.0 pero utilizamos la versión 7.0 de PHP ya que a partir de Moodle V3 es la versión mínima requerida.
- Base de Datos: Moodle es compatible con diferentes servidores de base datos. En este caso nosotros utilizamos MySQL server 8.0.20.

3.2.2. Instalación de Moodle.

Para realizar la instalación de Moodle es recomendable seguir alguna de las guías que están a la disposición del público en la página oficial de Moodle.

Para realizar la instalación se siguieron los siguientes pasos:

Se instaló la estructura LAMP previamente mencionada (véase figura 3.1) utilizando el siguiente comando:

```
sudo apt install apache2 mysql-client mysql-server php liabapache2-mod-
php
```

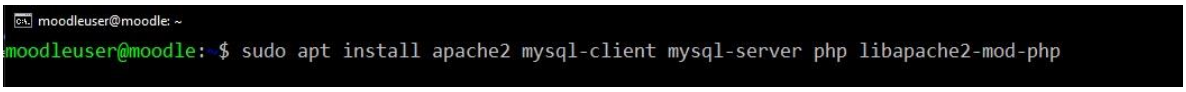


Figura 3.1. Instalación de LAMP

Posterior a ello se instalaron algunos programas que requiere Moodle para su funcionamiento (véase figura 3.2) con el siguiente comando:

```
sudo apt install graphviz aspell ghostscript clamav php-pspell php-curl
php-gd php-intl php-mysql php-xml php-xmlrpc php-ldap php-zip php-soap
php-mbstring
```

Figura 3.2. Instalación de programas adicionales para el funcionamiento de Moodle.

Se ejecutó el comando mysql_secure_installation para realizar algunas configuraciones seguras del manejador de bases de datos (véase figura 3.3).

```
sudo mysql_secure_installation
```

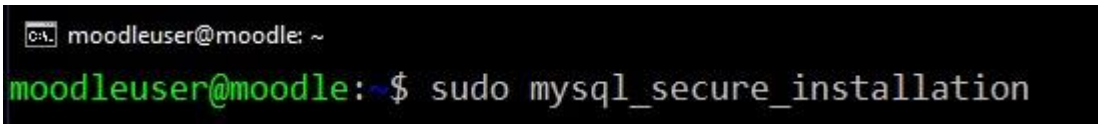


Figura 3.3. Aseguramiento del manejador de bases de datos.

Después de ello se realizó una clonación del repositorio de Moodle en la carpeta opt (véase figura 3.4).

```
sudo git clone git://git.moodle.org/moodle.git
```

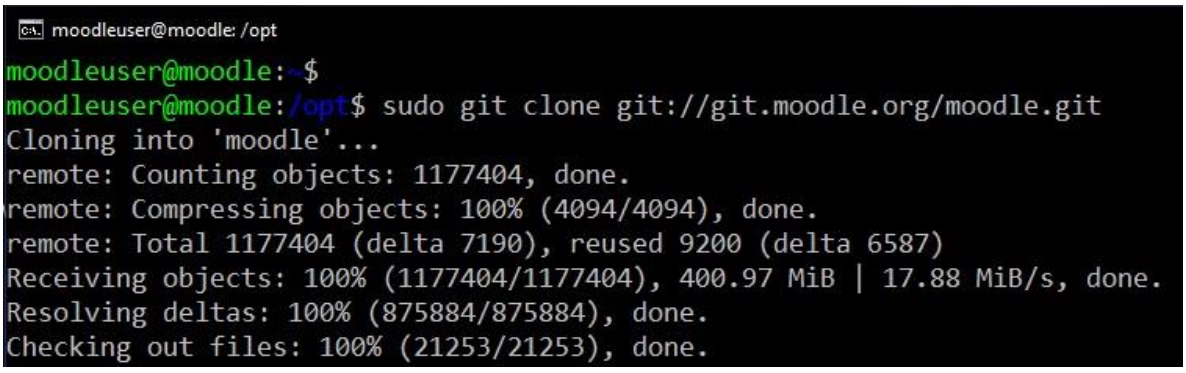


Figura 3.4. Clonación del repositorio de Moodle

A continuación fue necesario seleccionar la rama que se quiere del repositorio de acuerdo a la version de Moodle que se desea instalar, en este caso la versión más actual es la 3.9 (véase figura 3.5) ejecutamos el siguiente comando en la dirección /opt/moodle/.

```
sudo git branch --track MOODLE_39_STABLE origin/MOODLE_39_STABLE
```

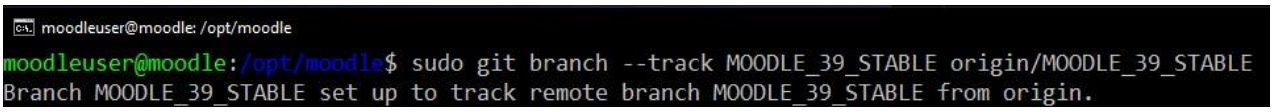


Figura 3.5. Selección del Branch.

Verificamos que la rama fuese la mas reciente (véase figura 3.6) ejecutamos el siguiente comando en la dirección /opt/moodle/.

```
sudo git checkout MOODLE_39_STABLE
```

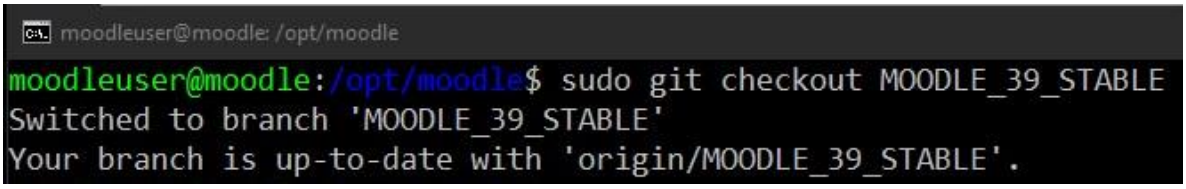


Figura 3.6. Verificación de la rama.

Después se crearon los archivos que se requieren para usar Moodle (véase figura 3.7) para ello se usaron los siguientes comandos en la dirección /opt/moodle/.

```
sudo mkdir /var/www/html/RedesDeDatosSeguras
sudo cp -R /opt/Moodle/* /var/www/html/RedesDeDatosSeguras/
sudo mkdir /var/www/html/RedesDeDatosSeguras
sudo mkdir /var/www/html/RedesDeDatosSeguras
sudo mkdir /var/moodledata
sudo chown -R www-data /var/moodledata
sudo chmod -R 777 /var/moodledata
sudo chmod -R 0755 /var/www/html/RedesDeDatosSeguras/
```

Figura 3.7. Creación de archivos y asignación de permisos.

Antes de proceder con la instalacion de Moodle necesitamos crear una base de datos para esta plataforma (véase figura 3.8).

```
sudo mysql -u root -p
CREATE DATABASE moodle DEFAULT CHARACTER SET utf8mb4 COLLATE
utf8mb4_unicode_ci;
create user 'usermood'@'localhost' IDENTIFIED BY 'password';
GRANT SELECT,INSERT,UPDATE,DELETE,CREATE,CREATE TEMPORARY
TABLES,DROP,INDEX,ALTER ON moodle.* TO 'usermood'@'localhost';
quit;
```

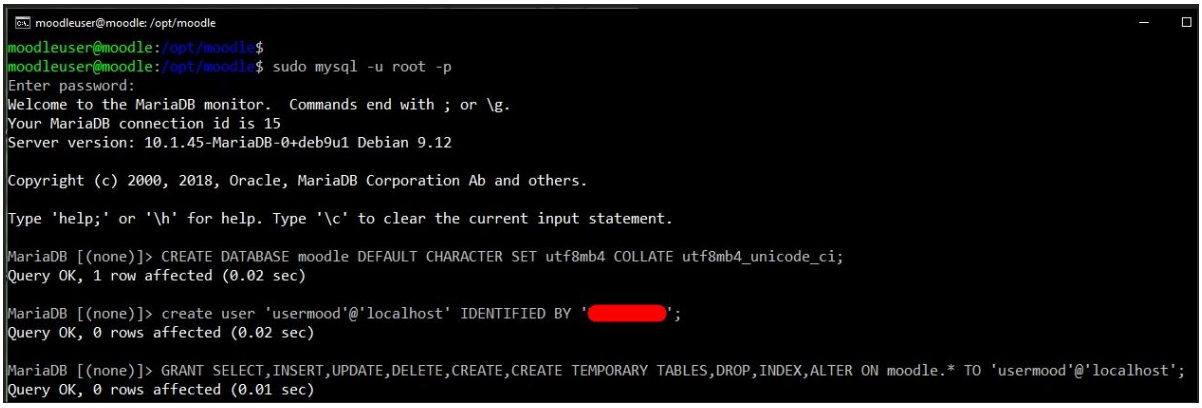


Figura 3.8. Creación de base de datos para Moodle.

Una vez creada la base de datos se puede proceder al navegador y comenzar con la instalación (véase figura 3.9).

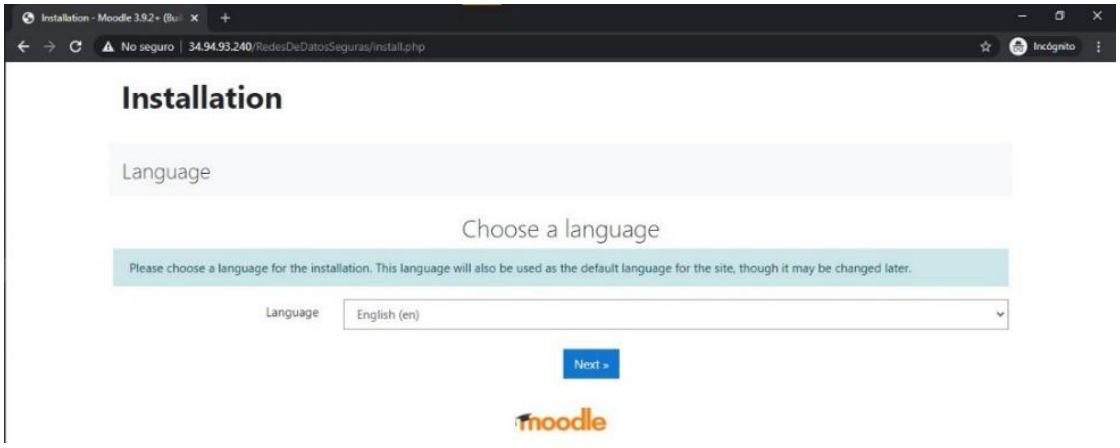


Figura 3.9. Instalación de Moodle.

Una vez terminada la instalación fue necesario hacer configuraciones administrativas para finalizar y entonces trabajar en Moodle.

3.3 Disposición de los materiales.

Los materiales están divididos en tres grupos: materiales de apoyo, cuestionarios, y videos del laboratorio, por ello se crearon tres cursos para que cada uno aloje un tipo de material en específico. Para crear un curso se entra a la plataforma con alguna cuenta que tenga permisos de administración y se dirige *Site administration* > *Courses* >*Manage courses and categories* > *Add a new course* (véase figura 3.10) en esta sección se proporciona la información necesaria para crear los cursos que almacenan el material.

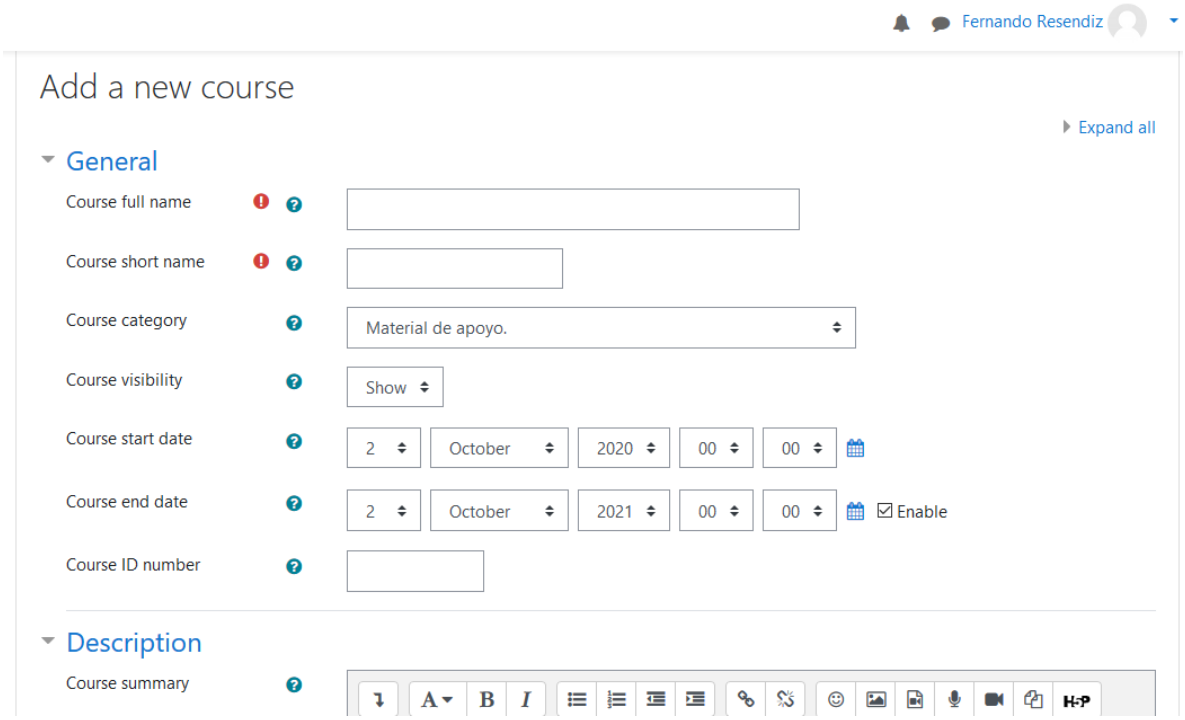


Figura 3.10. Sección para agregar un curso.

Una vez creados los cursos, estos se muestran en la página principal de Moodle (véase figura 3.1). Se muestra el título del curso, que es el material que alberga, una imagen para una fácil distinción y una pequeña descripción de lo que se encuentra en cada curso.

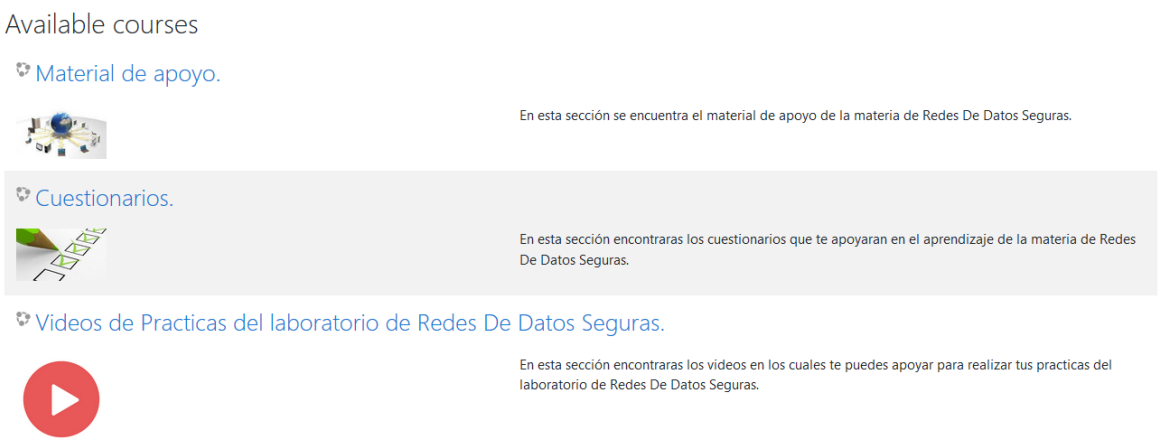


Figura 3.11. Presentación de los cursos que alojan los materiales correspondientes.

3.3.1 Material de apoyo

Figura 3.12. Muestra de cómo se presenta el material de apoyo.

Como se decidió anteriormente, el material de apoyo se pondrá a disposición del estudiante en forma de un documento PDF (véase figura 3.12) que el alumno es capaz de consultar directamente en el navegador o bien que sea capaz de descargarlo para su posterior consulta. Para ello se utilizó la opción de Moodle

que permite agregar un recurso, para nuestro caso un archivo, en el curso de “Material de apoyo” con el fin de anexar todo el material de apoyo desarrollado (véase figura 3.13).

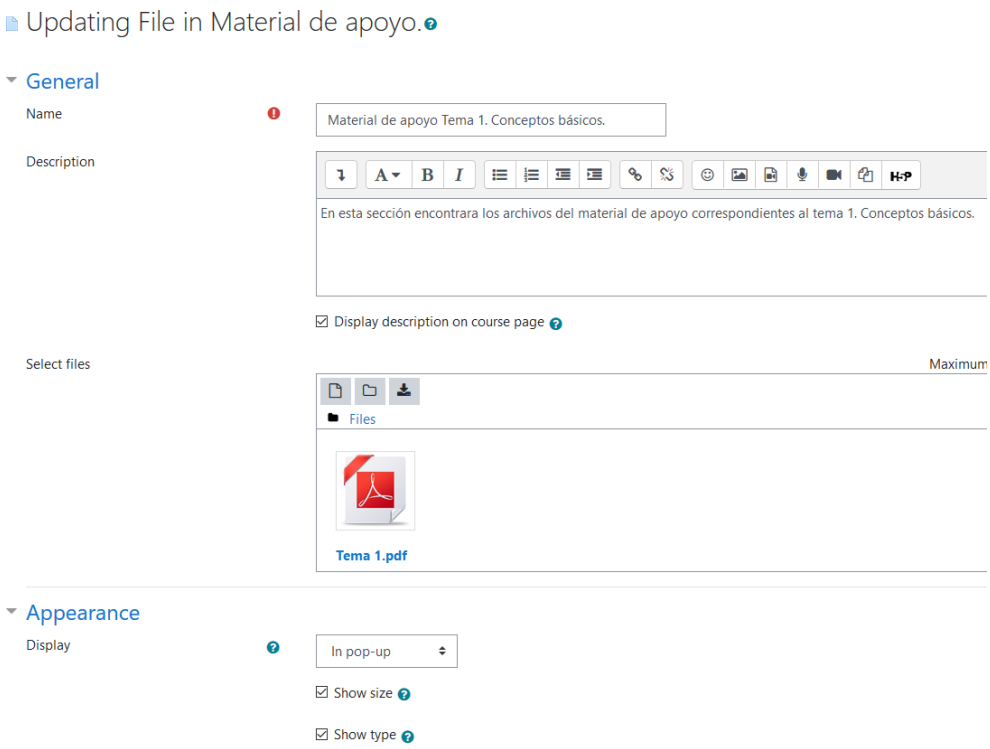


Figura 3.13. Configuración de los archivos del material de apoyo.

Una característica para destacar es la opción *Display* en la sección de *Appearence*, donde se puede seleccionar la forma en que se muestra el documento y se estableció como *In pop-up*, esto nos permite que cada vez que un estudiante consulte el material éste se habrá en una ventana distinta, lo permite continuar con la navegación del sitio y a la vez tener el archivo abierto.

3.3.2 Cuestionarios

3.3.2.1 Desarrollo de reactivos.

Una vez que se ha determinado la cantidad de reactivos que contendrá cada cuestionario y su diseño, se procedió al desarrollo de los reactivos tomando en cuenta apuntes de la materia, así como el material de apoyo desarrollado para la asignatura. Un punto que destacar fue el definir con qué tipo de pregunta se relaciona cada reactivo, por ello en la redacción de las preguntas (que es

consultable en el **Anexo 2** de este documento) se observa el tipo con el cual será implementada cada pregunta. Además, cada reactivo se ha revisado con el apoyo de la profesora M.C. María Jaquelina López Barrientos para que estas preguntas estén dentro del rango del conocimiento que se espera posean los estudiantes.

En el **Anexo 2** se presenta el conjunto de preguntas organizadas de acuerdo con el tema al que pertenecen. Cada pregunta esta enumerada y clasificada respecto al tipo de pregunta con la que es implementada. Por último, es posible encontrar cada pregunta junto con su respuesta correcta subrayada en color amarillo.

3.3.2.2 Implementación de cuestionarios.

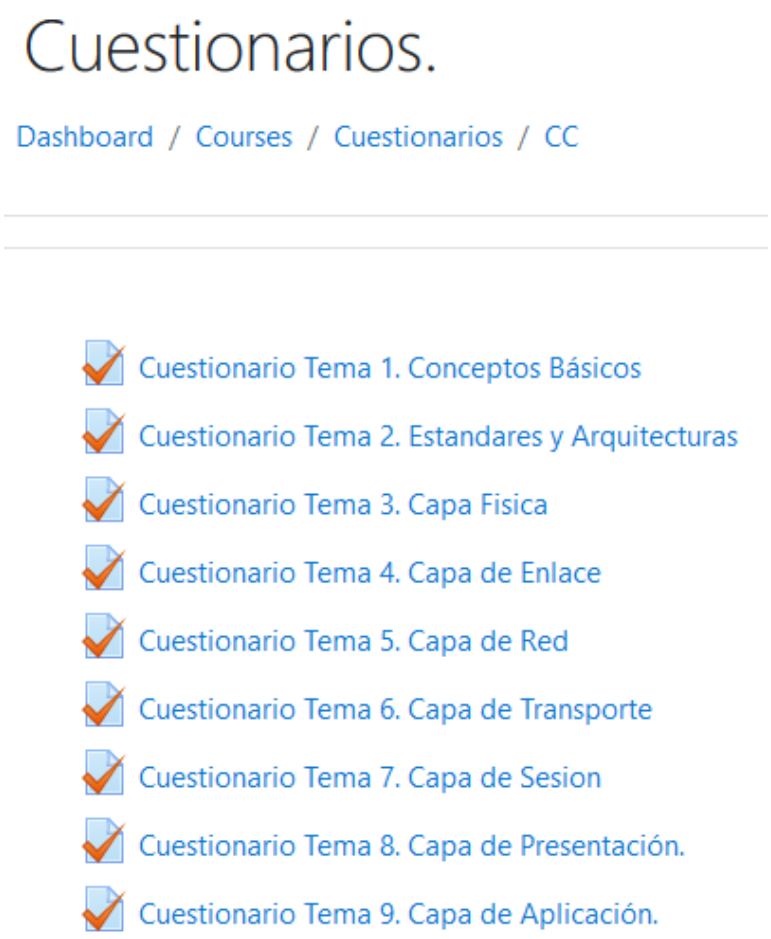


Figura 3.14. Muestra de cómo se presentan los cuestionarios.

Los cuestionarios son implementados mediante la función de exámenes que contiene Moodle, este tipo de recurso permite crear cuestionarios a partir de las

preguntas que están contenidas en el banco de preguntas de cada tema. Estos cuestionarios solo muestran el título del tema al que pertenecen sin ninguna información extra para tener una presentación limpia y sencilla de ellos (véase figura 3.12).

Banco de preguntas

Cada banco de preguntas cuenta con distintos tipos de reactivos los cuales han sido implementados de la siguiente manera:

- **General.**

Todas las preguntas elaboradas cuentan con una sección general, en esta se definen características comunes como es la categoría a la que pertenece la pregunta, nombre de la pregunta, texto de la pregunta y un ID para identificarla (véase la figura 3.15). Después de las características generales vienen las características propias de cada tipo de pregunta.

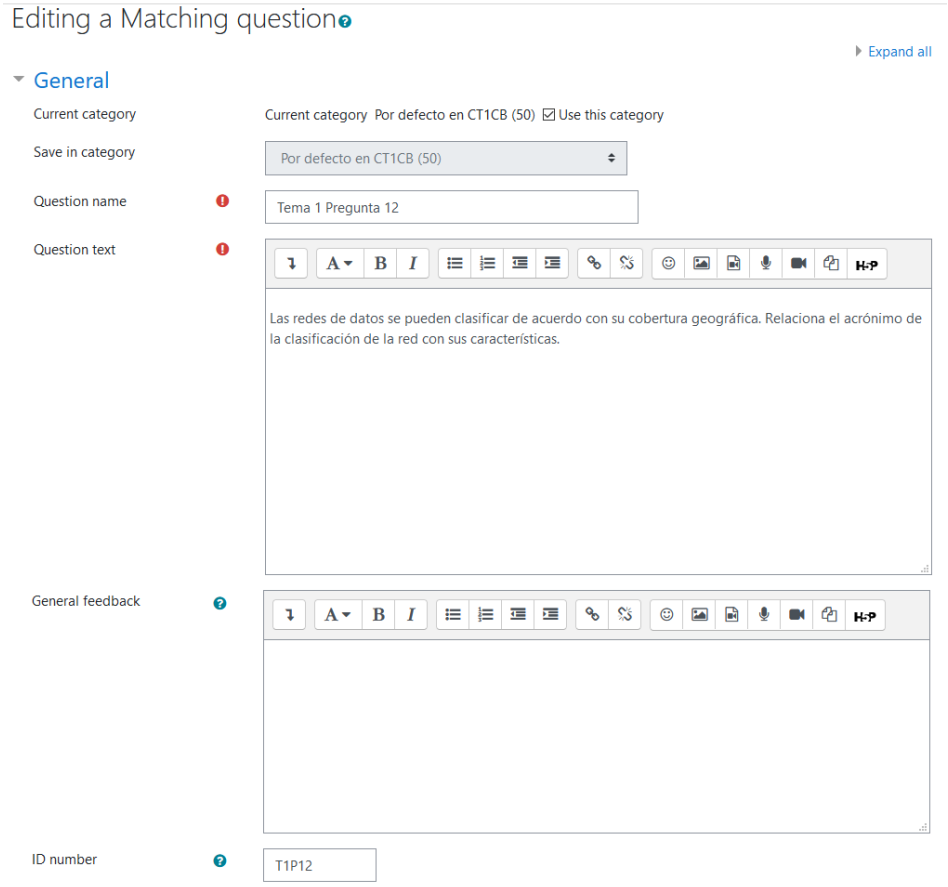


Figura 3.15. Características generales de las preguntas

- **Tipo 1. Pregunta de opción múltiple con única respuesta correcta.**

Para crea este tipo de preguntas se selecciona la opción de *"Multiple choice"* en el menú de *"Choose a question type to add"* (véase figura 3.16.), menú que es desplegado en el momento que se crea una pregunta.

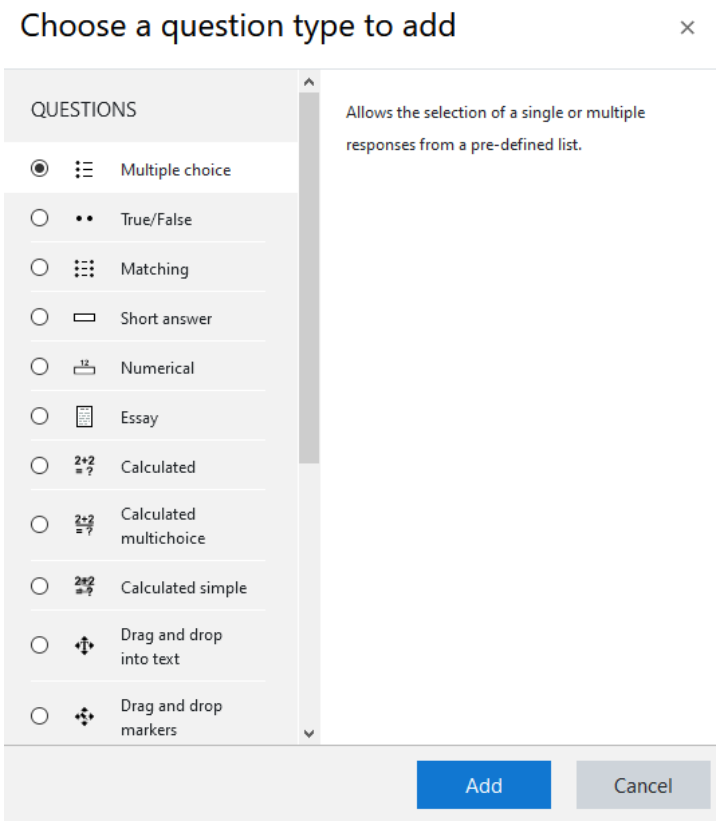


Figura 3.16. Selección de pregunta de opción múltiple.

Para crear el tipo de pregunta de selección múltiple con única opción correcta, ¿en la sección "One or multiple answers?" se selecciona *"One answer only"*, esto permite que solo una respuesta sea la correcta. Posteriormente se colocan las opciones de las cuales una debe de tener el porcentaje de 100% la cual es la respuesta correcta (véase figura 3.17).

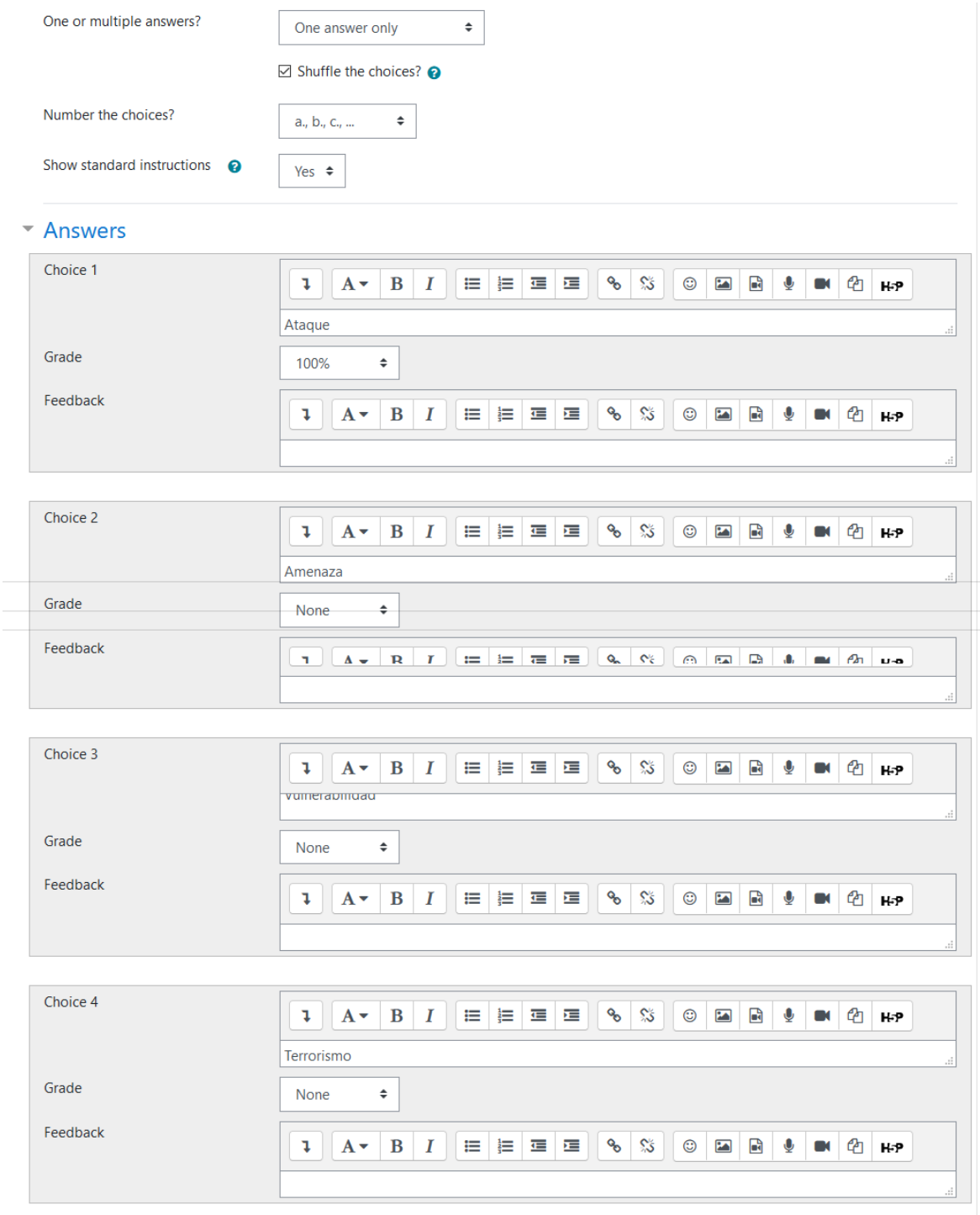


Figura 3.17. Creación de pregunta de opción múltiple con única respuesta correcta.

- **Tipo 2. Pregunta de opción múltiple con múltiples respuestas correctas.**

Para crear este tipo de pregunta se selecciona la misma opción que en el caso del tipo 1 de preguntas. Donde, en la sección *"One or multipleanswers?"* ahora se selecciona *"Multiple answers allowed"*, además, en la sección de *"Answers"* las respuestas pueden tener distintos porcentajes siempre y cuando la suma de estos no supere el 100% (véase figura 3.18.).

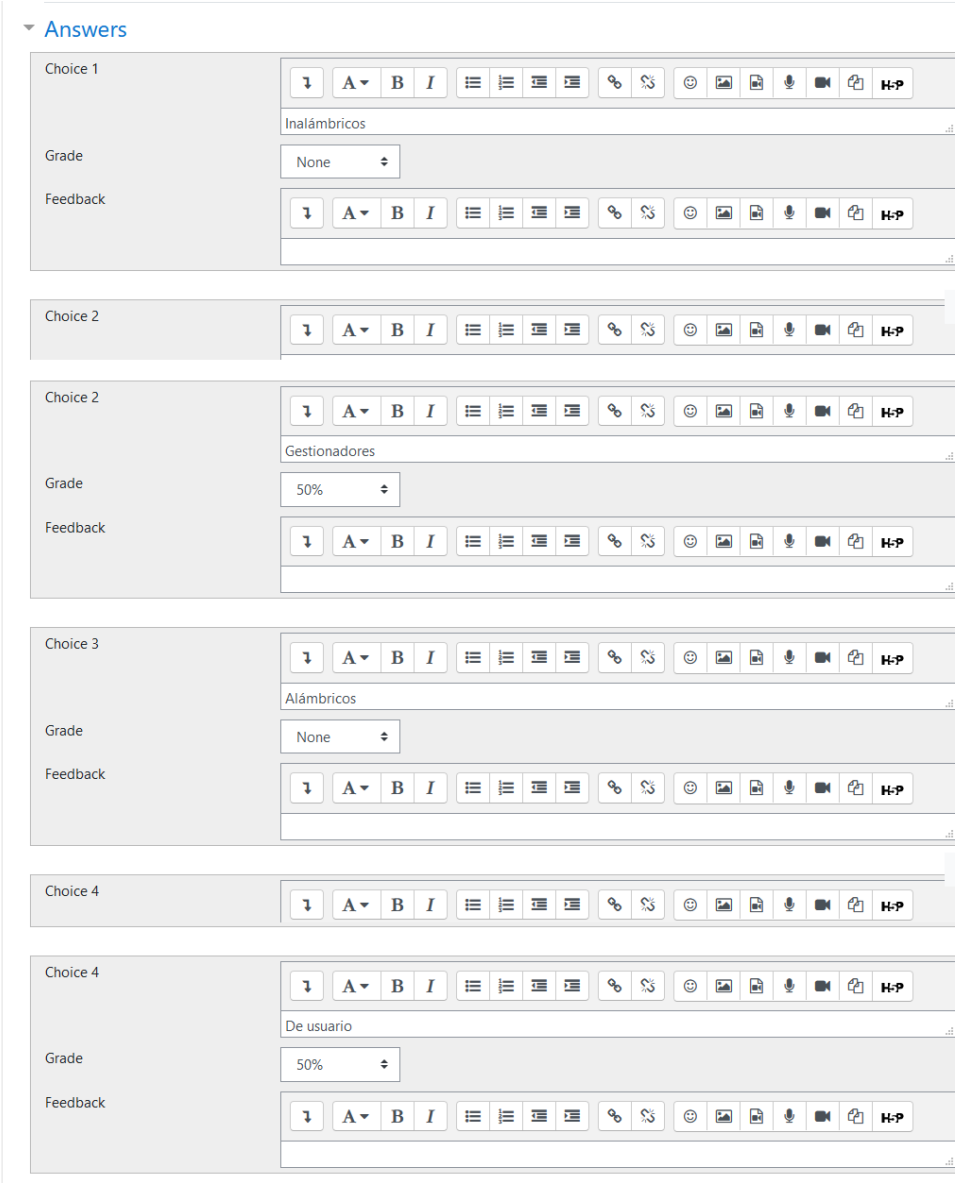


Figura 3.18. Creación de pregunta de opción múltiple con múltiples respuestas correctas.

Tipo 3. Pregunta de relación de columnas.

Para crea este tipo de preguntas se selecciona en el menú de *"Choose a question type to add"* la opción de *"Matching"* (véase figura 3.19), esta opción permite crear preguntas del tipo relación de columnas.

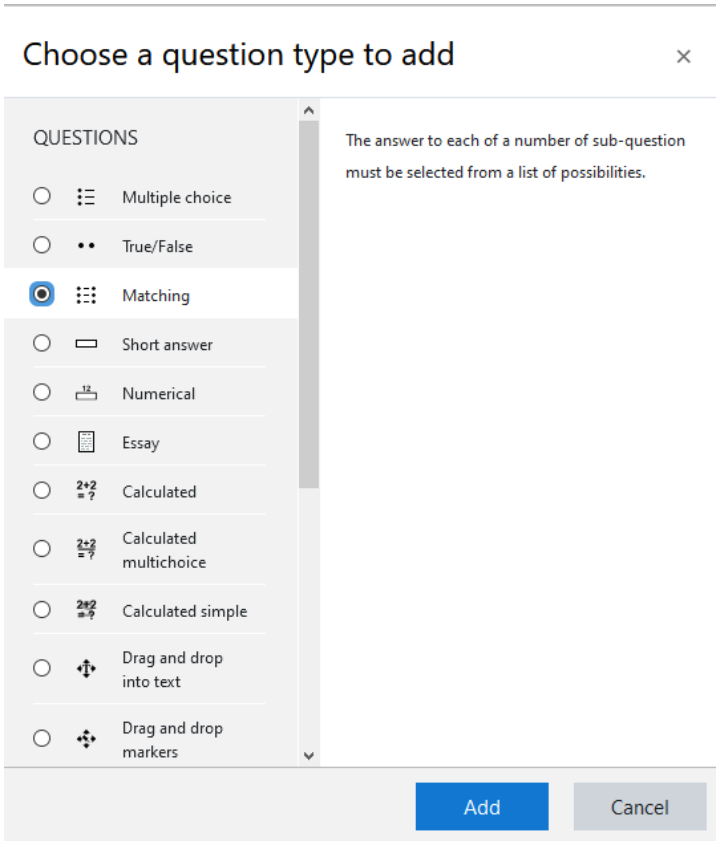


Figura 3.19. Creación de pregunta de opción múltiple con múltiples respuestas correctas.

En este tipo de preguntas es necesario colocar el concepto con su respectiva definición para que sean las columnas a relacionar, además, es posible agregar conceptos sin definición, esto es para que funcionen como distractores y agregar un cierto nivel de dificultad (véase figura 3.20).

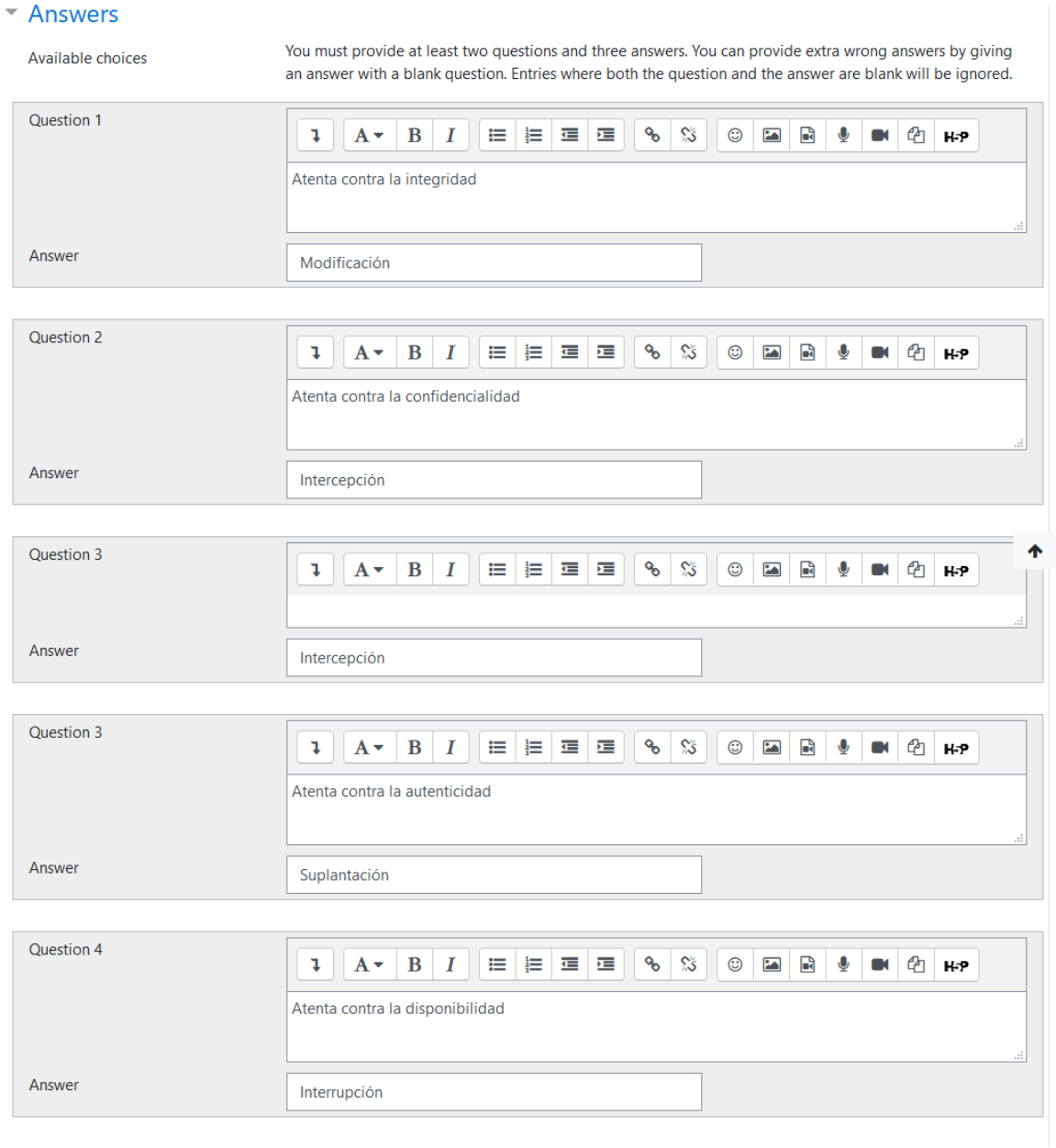


Figura 3.20. Creación de pregunta relación de columnas.

Tipo 4. Preguntas de respuesta cierto o falso.

Para elaborar este tipo de preguntas, en el menú de *"Choose a question type to add"* se selecciona la opción de *"True/False"* (véase figura 3.21), con esta opción es posible formular preguntas del estilo cierto o falso.

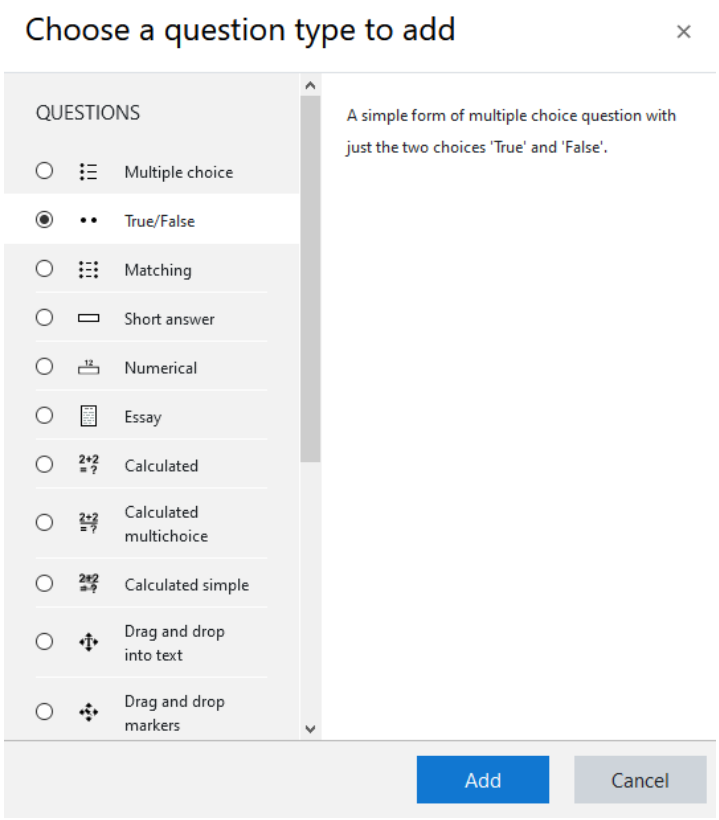


Figura 3.21. Selección de pregunta del tipo cierto o falso.

La implementación de este tipo de preguntas es sencilla debido a que la respuesta esperada solo puede ser una de dos opciones, así que en el campo de *"Correct Answer"* seleccionamos la respuesta, además tenemos la opción de agregar una retroalimentación más específica (véase figura 3.22).

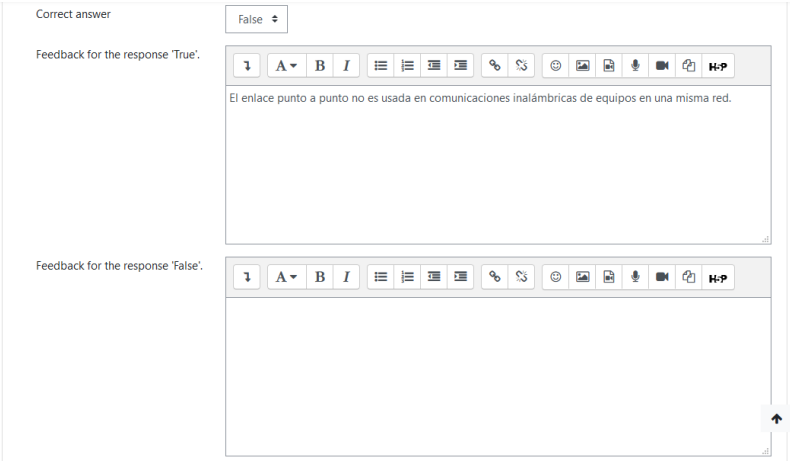


Figura 3.22. Creación de pregunta de cierto o falso.

Tipo 5. Arrastrar y soltar.

En el menú de *"Choose a question type to add"* se selecciona la opción de *"Drag and drop into text"* (véase figura 3.23.) para elaborar las preguntas del tipo arrastrar y soltar en textos.

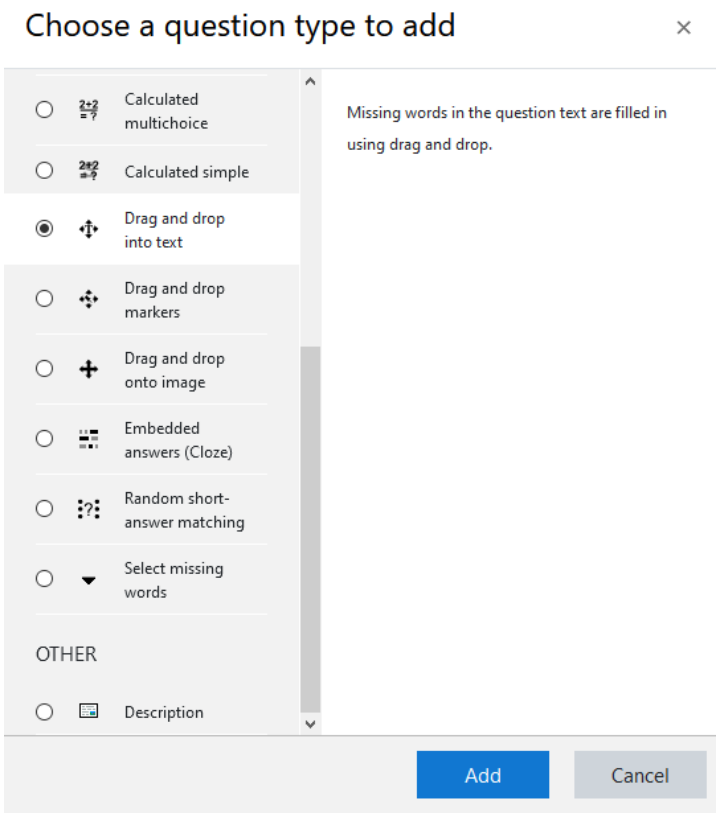


Figura 3.23. Selección de pregunta del tipo arrastrar y soltar.

Este tipo de preguntas son un poco distintas a las demás en su sección de *"General"* desde el momento de redactar el cuerpo de la pregunta se debe de colocar [[*n*]] donde n es un número (véase figura 3.24), en esta marca es donde se colocarán las respuestas.

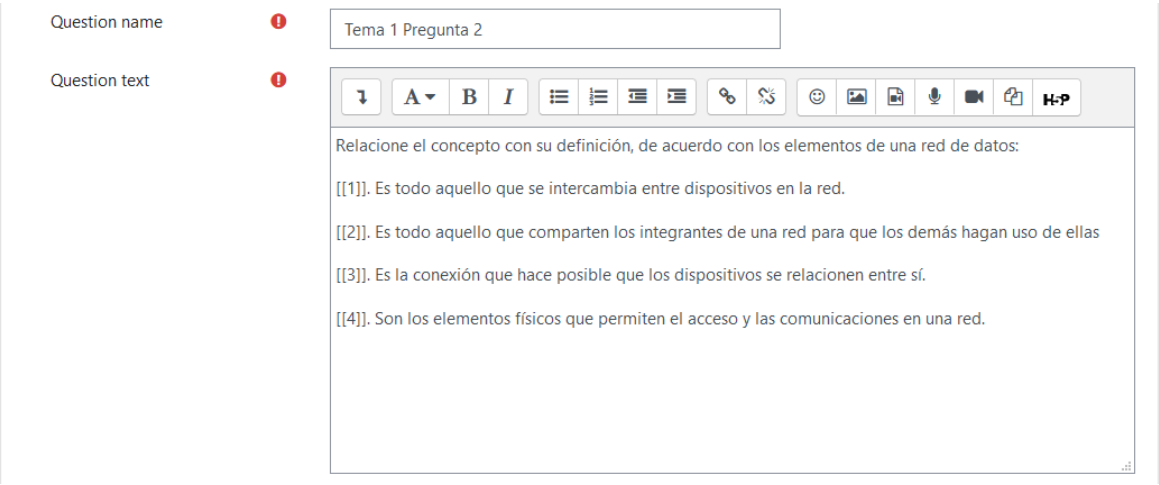


Figura 3.24. Sección general de una pregunta del tipo arrastrar y soltar.

En la sección de *"Choices"* es donde se define qué respuesta va en qué etiqueta de las colocadas previamente en el cuerpo de la pregunta (véase figura 3.25).

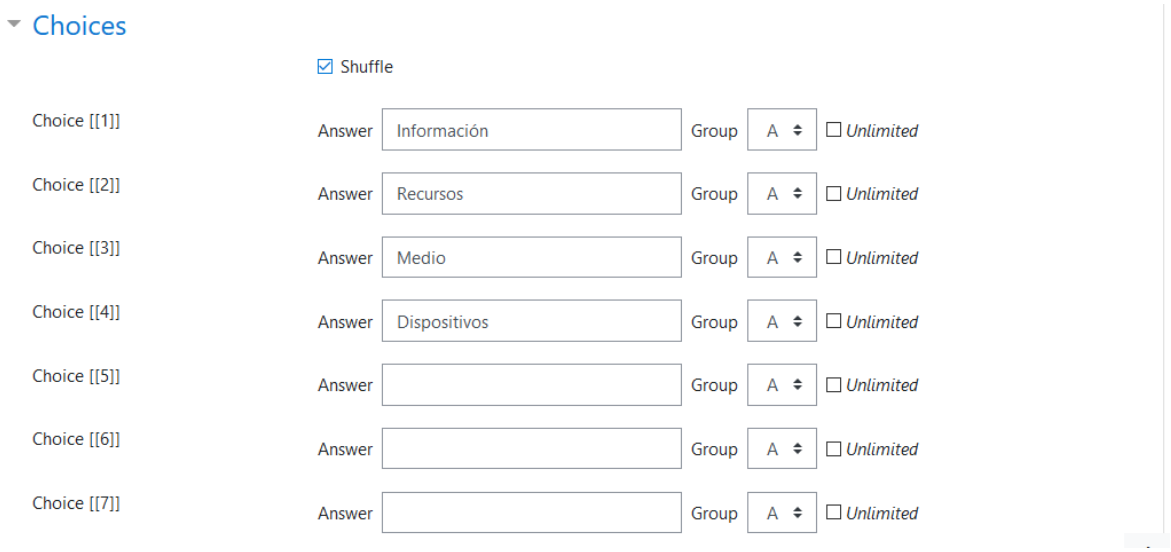


Figura 3.25. Relación de respuestas con su correspondiente etiqueta.

Tipo 6. Respuesta libre.

Para crear una pregunta con respuesta libre en el menú de *"Choose a question type to add"* se selecciona la opción de *"short answer"* (véase figura 3.26) esta opción permite realizar una pregunta sin darle alguna opción al estudiante, para que este escriba la respuesta correcta.

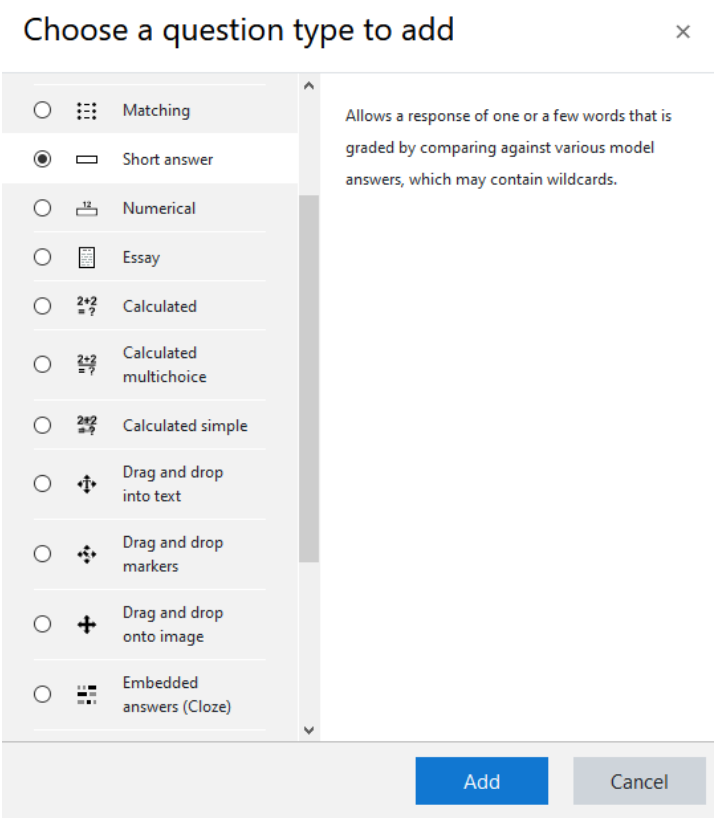


Figura 3.26. Selección de la opción que permite crear preguntas del tipo respuesta abierta.

Para este tipo de preguntas la respuesta debe de ser ingresada, en caso necesario se puede definir si es sensible a mayúscula, además, se pueden definir más respuestas correctas para el caso en el que el alumno o alumna ingrese una respuesta y esta sea muy cercana a la que se esperaba (véase figura 3.27).

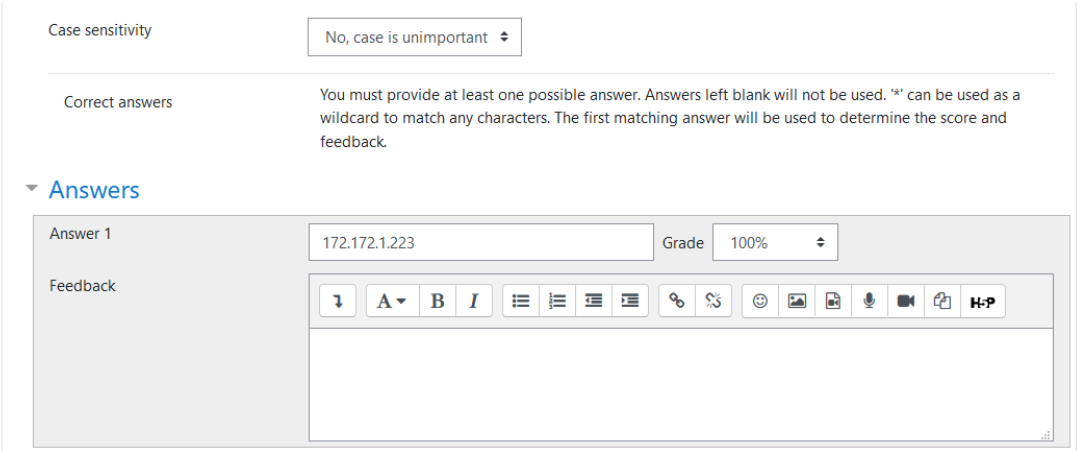


Figura 3.27. Creación de una pregunta con respuesta abierta.

Tipo 7. Múltiples respuestas libres.

Para realizar este tipo de preguntas en el menú de *"Choose a question type to add"* se selecciona la opción *"Embedded answers (Cloze)"* (véase figura 3.28), este tipo de preguntas permite reestructurar un tipo de pregunta utilizando código que puede interpretar Moodle.

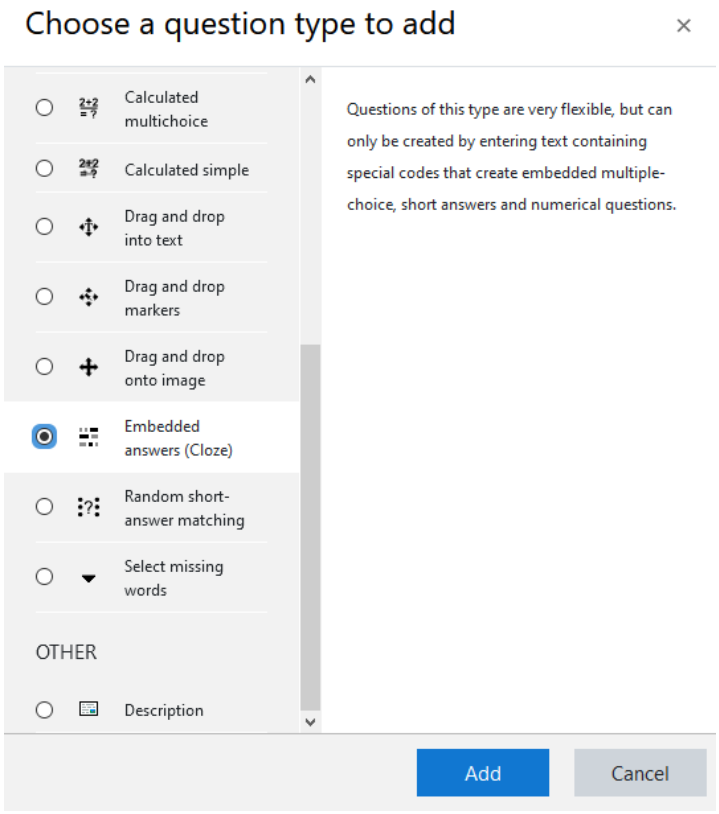


Figura 3.28. Selección del tipo Embedded para crear preguntas con múltiples respuestas libres.

Para este caso es necesario modificar el cuerpo de la pregunta, agregando entre llaves el código el cual interpretara Moodle, este código está compuesto por el valor de esa pregunta, el tipo de pregunta, para nuestro caso respuesta libre, y por último la respuesta correcta (véase figura 3.29), de esta manera podemos implementar una pregunta que espera varias respuestas libres.

Figura 3.29. Creación de pregunta con múltiples respuestas libres.

3.3.3 Videos del laboratorio.

Para la integración de los videos del laboratorio dentro del curso *"Videos de Prácticas del Laboratorio de Redes de Datos Seguras."* se agrega un nuevo recurso del tipo *"Page"* (véase figura 3.30).

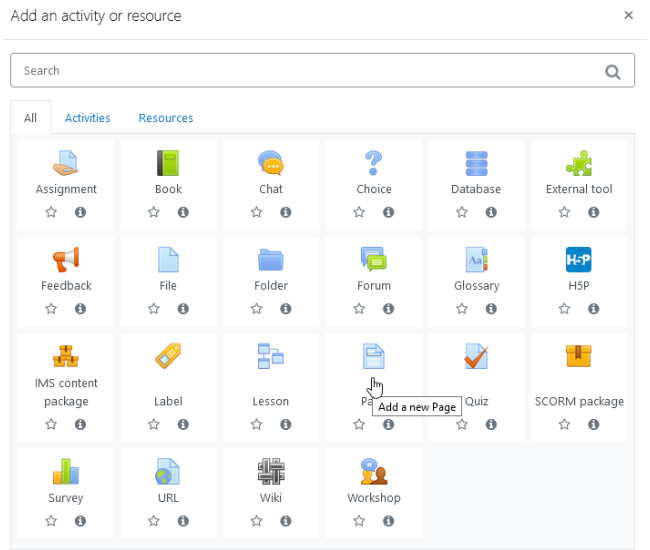


Figura 3.30. Creación de un recurso del tipo "Page"

Debemos de poner un nombre a la página, en este caso el nombre corresponde al nombre de la práctica a la que hace alusión el video guardado. Una vez puesto el nombre modificamos el contenido de la página insertando el video correspondiente (véase figura 3.31).

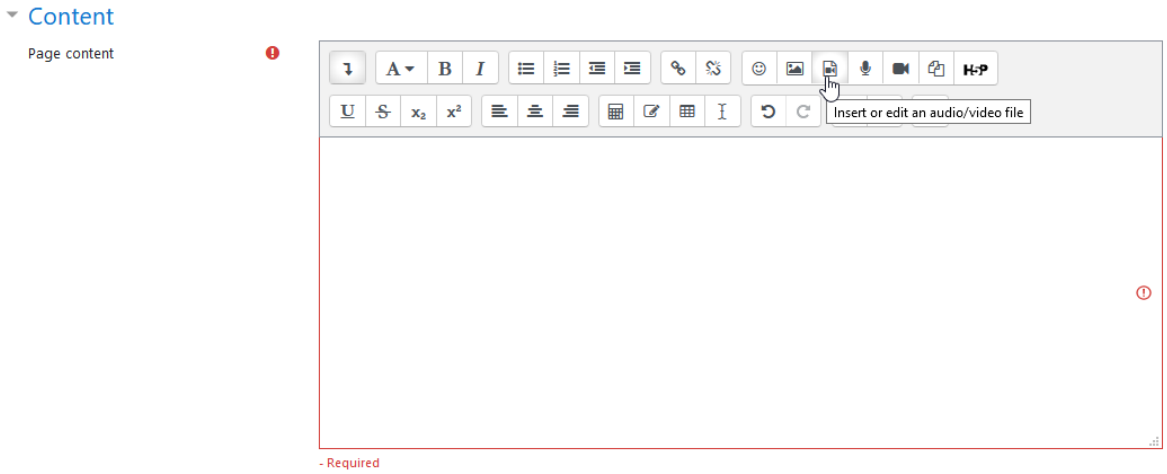


Figura 3.31. Modificación del contenido de la página.

Al escoger esta opción, desplegará una pantalla para la inserción de material del tipo multimedia, nos dirigimos a la sección de video (véase figura 3.32).

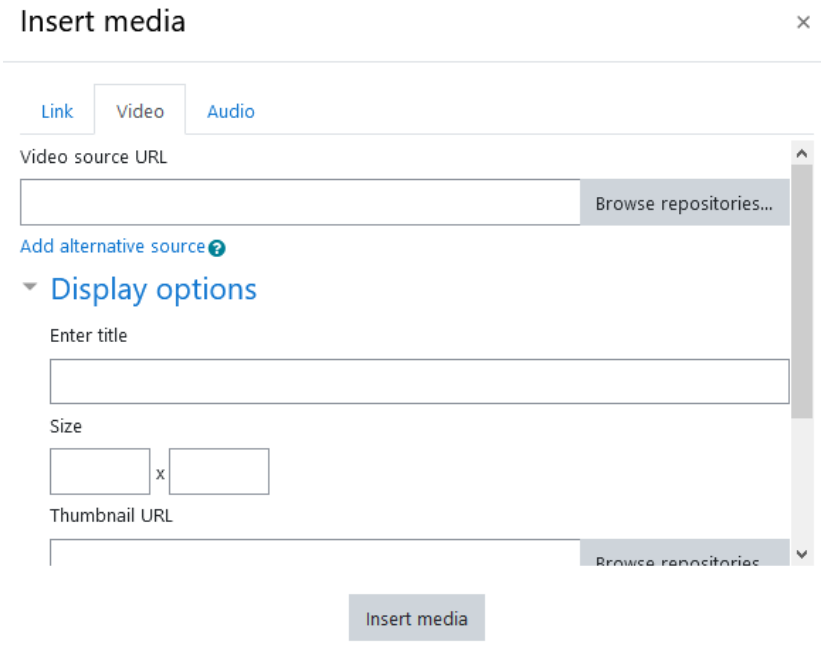


Figura 3.32. Pantalla de inserción de multimedia, pestaña de video.

En esta pestaña se debe subir el video, para ello se selecciona *"Browse repositories"* el cual presentará una pantalla donde se selecciona subir un archivo (véase figura 3.33).

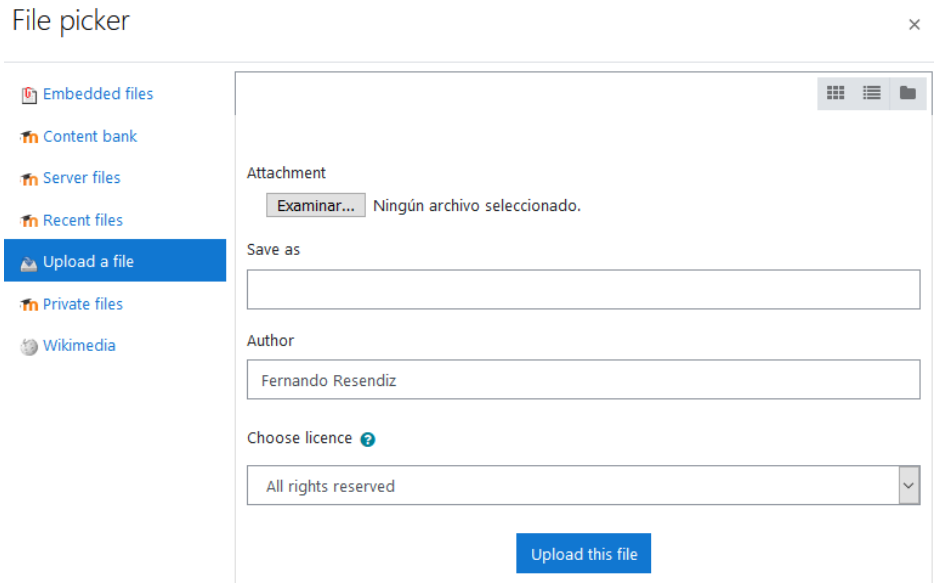


Figura 3.33. Pantalla de subida de archivos.

Agregamos el video en la parte de Examinar, además, de la información general sobre el video (véase figura 3.34).

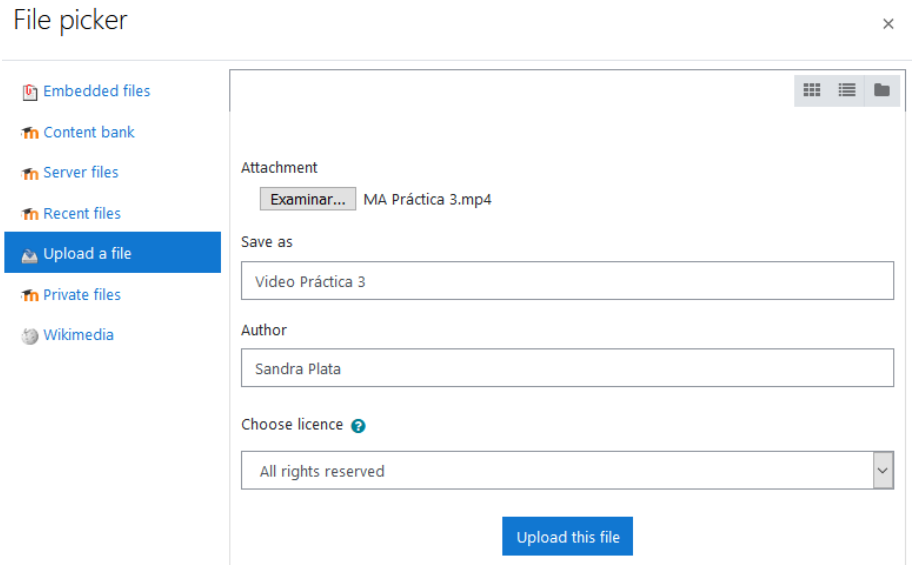


Figura 3.34. Información básica del video subido.

Una vez terminada la subida del video, se debe colocar información como el nombre del video, así como las dimensiones con las que se muestra en pantalla (véase figura 3.35).

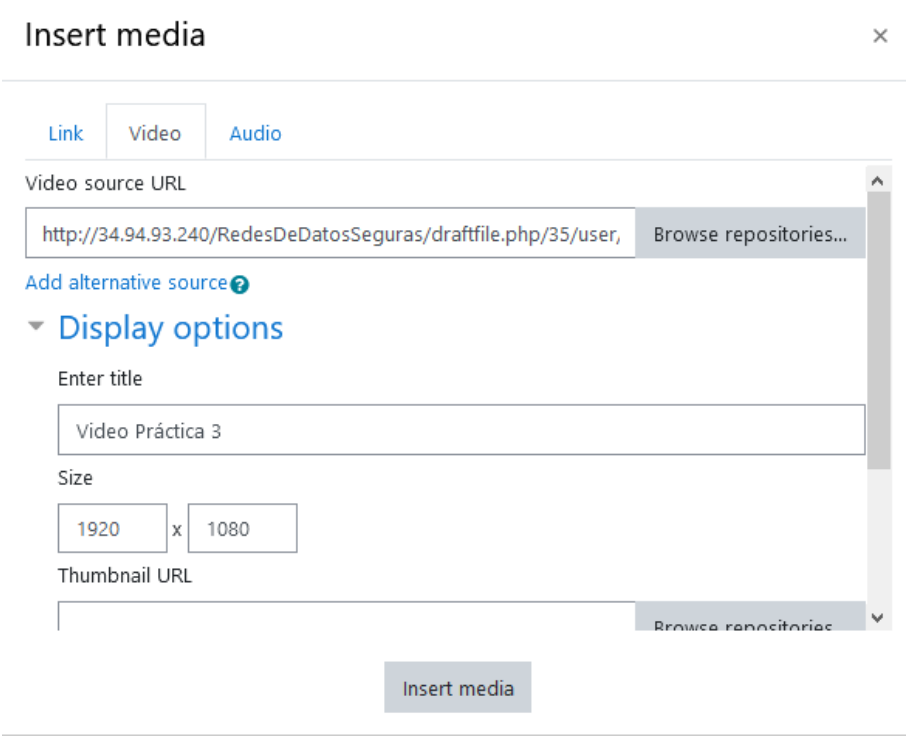


Figura 3.35. Información sobre la presentación del video.

Finalmente, el video ha quedado listo para que el usuario pueda verlo cuando lo desee.

Capítulo 4. Pruebas.

En este capítulo se muestran las pruebas realizadas, en la primera fase se revisaron los reactivos para los cuestionarios, en la segunda fase se implementaron los cuestionarios y se integraron con el resto de los materiales en una plataforma la cual fue probada con los estudiantes para recibir una retroalimentación que ayudó a la mejora de la plataforma para su despliegue definitivo.

4.1 Descripción de las fases de pruebas.

La primera fase de pruebas consistió en las revisiones realizadas a los cuestionarios. En estas actividades se verificaba que los reactivos formulados fueran redactados de tal forma que el estudiante comprendiera la pregunta, que el reactivo tuviera relación con el programa de estudios y con el material de apoyo y, además, que contara con la ortografía y formalidad necesarias para ser presentados como material oficial a los alumnos. En caso que el reactivo no se considerara adecuado este era corregido en los aspectos necesarios para formar parte de los cuestionarios y posteriormente implementarlo en la plataforma.

La segunda fase de pruebas consistió en presentar la plataforma a los estudiantes de distintas asignaturas relacionadas con las Redes de Datos Seguras como son Administración de Redes, Laboratorio de Administración de Redes, Redes de Datos, Laboratorio de Redes de Datos y los estudiantes tanto de teoría como de laboratorio de la misma asignatura de Redes de Datos Seguras.

El objetivo de la presentación fue que los alumnos utilizaran la plataforma en un ambiente de pruebas como es el que se creó en la nube de Google. Otro aspecto que se buscó poner a prueba fue que los estudiantes accedieran a los tres rubros desarrollados que son el material de apoyo, los cuestionarios y los videos del laboratorio para que posteriormente pudieran proveer de una retroalimentación mediante una encuesta implementada en Moodle.

Además, se acordó con los profesores de los grupos proporcionar las listas de los estudiantes que participaron en la prueba, para ello se implementó un sistema de contraseñas para que cuando un estudiante accedería a los materiales se registraran en su grupo de manera automática.

Los profesores que se seleccionaron para las pruebas fueron aquellos que anteriormente han seguido el avance del desarrollo de la plataforma y que tenían conocimiento debido a su participación en la revisión del material de apoyo que se aloja en la plataforma que fue creada en Moodle.

Se tomaron como resultado de las pruebas las respuestas y recomendaciones dadas por los estudiantes que participaron en este proceso y que vertieron en la plataforma y que en total fueron 135 participantes. Con estos resultados se realizaron los ajustes pertinentes a la plataforma con el objetivo que la implementación que se alojará en el servidor de la Facultad de Ingeniería se encuentre corregida y sea posible utilizarla.

4.2 Encuesta.

Como se comentó con anterioridad se crea una encuesta que fue aplicada a los estudiantes para que, una vez terminada su exploración en la plataforma, lograran enviarnos a sus respuestas y recomendaciones.

Para crear esta encuesta se hace uso del plugin “Questionaire” (véase figura 4.1) el cual requiere de instalación debido que no es un plugin que venga con la plataforma por defecto.

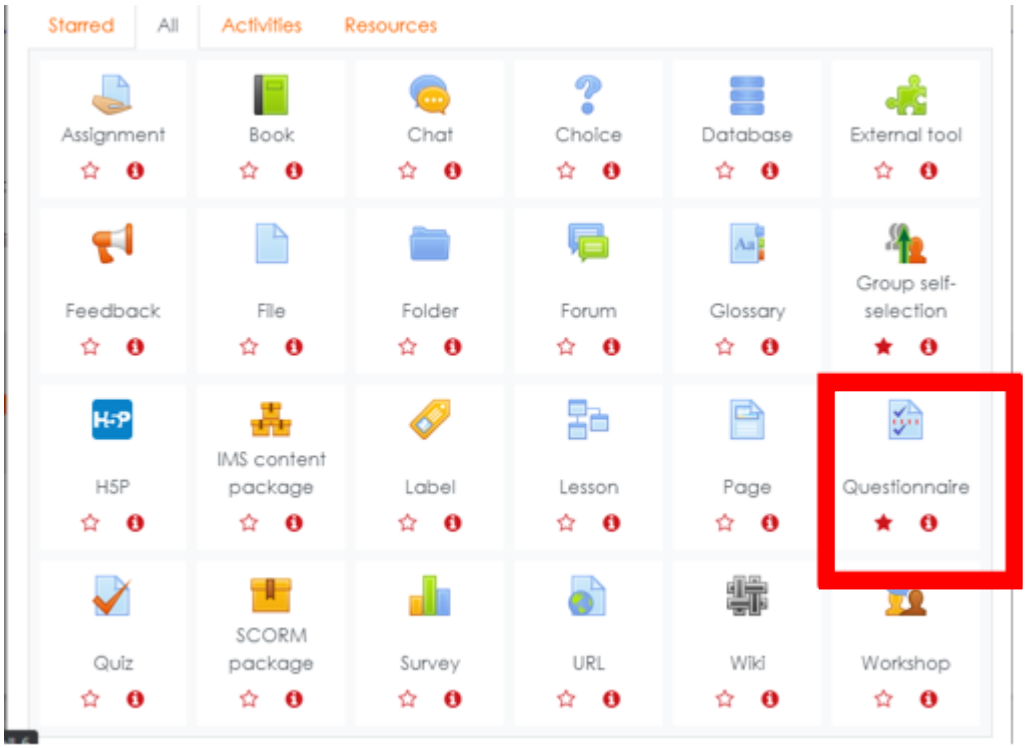


Figura 4.1. Ubicación del módulo questionaire.

Para crear la encuesta se solicita cierta información. Lo primero que se necesita es contar con los datos básicos como el nombre y la descripción de la encuesta (véase figura 4.2).

Figura 4.2. Datos generales de la encuesta.

Para nuestra aplicación del módulo es necesario establecer una fecha de terminación para que los estudiantes no sigan contestando la encuesta después del periodo establecido (véase figura 4.3).

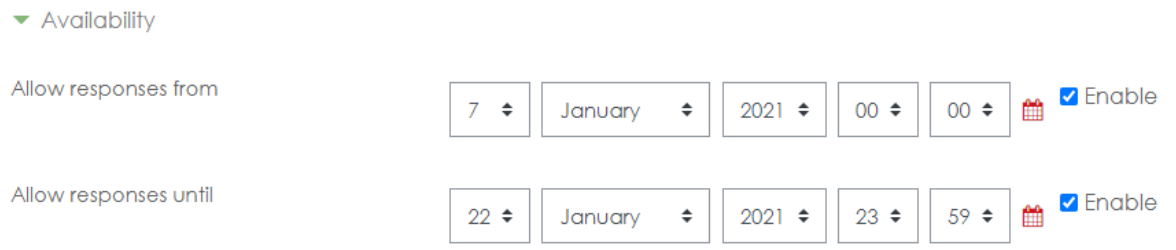


Figura 4.3. Límite de tiempo de la encuesta.

Posteriormente debemos de configurar las opciones propias del módulo (véase figura 4.4) .

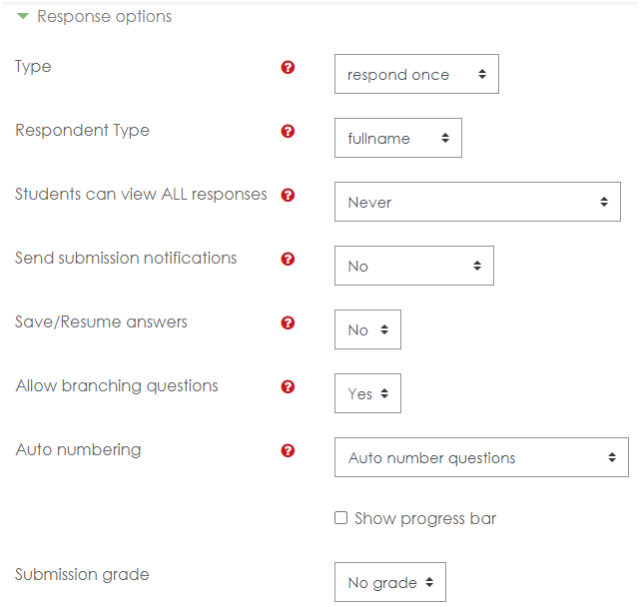


Figura 4.4.Configuraciones de la encuesta.

Una vez creada la encuesta debemos ingresar las preguntas que deseamos que los estudiantes contesten. En la figura 4.5 podemos apreciar como se presenta la encuesta a los estudiantes.

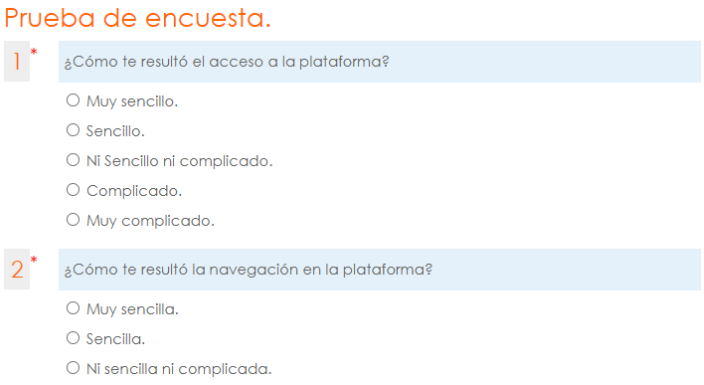


Figura 4.5. Preview de la encuesta.

4.3 Resultados.

Una vez terminado el periodo en el que era posible contestar la encuesta, el módulo es capaz de generar gráficas de los resultados de la encuesta. En la figura

4.6 podemos ver los resultados de la primera pregunta la cual buscaba conocer como percibía el usuario el acceso a la plataforma.

1 ¿Cómo te resultó el acceso a la plataforma?

Response	Average	Total
Muy sencillo.	47%	64
Sencillo.	41%	55
Ni Sencillo ni complicado.	7%	10
Complicado.	4%	6

Figura 4.6. Resultados de la primera pregunta.

En la figura 4.7 podemos observar los resultados de la segunda pregunta cuyo objetivo es conocer como percibía el usuario la navegación en la plataforma.

2 ¿Cómo te resultó la navegación en la plataforma?

Response	Average	Total
Muy sencilla.	40%	54
Sencilla.	39%	53
Ni sencilla ni complicada.	13%	18
Complicada.	7%	10

Figura 4.7. Resultados de la segunda pregunta.

En la figura 4.8 se observan los resultados de la tercera pregunta cuyo objetivo es el conocer como percibía el usuario la presentación de los materiales de apoyo.

3 ¿Qué tan de acuerdo estas con la forma en la que se presenta el material de apoyo?

Response	Average	Total
Totalmente de acuerdo.	66%	89
Algo de acuerdo.	30%	40
Ni de acuerdo ni en desacuerdo.	3%	4
Algo en desacuerdo.	1%	2

Figura 4.8. Resultado de la tercera pregunta.

En la figura 4.9 podemos apreciar los resultados de la cuarta pregunta cuyo objetivo es conocer como percibía el usuario la presentación de los videos del laboratorio.

4 ¿Qué tan de acuerdo estas con la forma en la que se presentan los videos del laboratorio?

Response	Average	Total
Totalmente de acuerdo.	56%	75
Algo de acuerdo.	35%	47
Ni de acuerdo ni en desacuerdo.	5%	7
Algo en desacuerdo.	4%	5
Totalmente en desacuerdo.	1%	1

Figura 4.9. Resultado de la cuarta pregunta.

En la figura 4.10 se aprecian los resultados de la quinta pregunta cuyo objetivo es el conocer como percibía el usuario la presentación de los cuestionarios.

5 ¿Qué tan de acuerdo estas con la forma en la que se presentan los cuestionarios?

Response	Average	Total
Totalmente de acuerdo.	61%	82
Algo de acuerdo.	31%	42
Ni de acuerdo ni en desacuerdo.	7%	9
Totalmente en desacuerdo.	1%	2

Figura 4.10. Resultado de la quinta pregunta.

En la figura 4.11 se observan los resultados de la sexta pregunta cuyo objetivo es el conocer como percibía el usuario el nivel de dificultad de los cuestionarios.

6 El nivel de dificultad de los cuestionarios es...

Response	Average	Total
Muy fácil.	5%	7
Fácil.	24%	33
Ni fácil ni difícil.	64%	87
Difícil.	5%	7
Muy difícil.	1%	1

Figura 4.11. Resultado de la sexta pregunta.

En la figura 4.12 podemos observar los resultados de la séptima pregunta cuyo objetivo es el conocer como percibía el usuario la redacción de las preguntas.

7 La forma en que se plantean las preguntas del cuestionario es...

Response	Average	Total
Clara.	73%	99
Algo clara.	26%	35
Nada clara.	1%	1

Figura 4.12. Resultado de la séptima pregunta.

En la figura 4.13 se presentan los resultados de la octava pregunta cuyo objetivo es conocer como percibía el usuario en general la plataforma.

8 En general, ¿Cómo evaluarías la paltaforma?

Response	Average	Total
Muy buena.	33%	44
Buena.	59%	79
Regular.	8%	11
Muy mala.	1%	1

Figura 4.13. Resultado de la octava pregunta.

Además de estas preguntas existe una novena pregunta la cual es libre y se pide que escriban los comentarios y recomendaciones que consideren necesarias tanto para la plataforma como para el contenido actual. En general, observando los resultados de las preguntas, así como de los comentarios, considera se necesitan hacer ciertas modificaciones antes de realizar la migración del ambiente de pruebas al servidor de la facultad.

Conclusiones.

El principal objetivo de esta tesis era el diseño, desarrollo e implementación de material didáctico esto con el fin de apoyar a los estudiantes y profesores de la carrera de Ingeniería en computación, en la asignatura de Redes de Datos Seguras. Con este objetivo en mente se desarrolló la implementación de una plataforma de estudios que contiene una base de conocimiento basada en el temario de la asignatura, esta base conocimientos consta de una serie materiales didácticos, de apoyo y videos con los cuales se apoya a los estudiantes a repasar los temas vistos en clase.

Para el cumplimiento del objetivo principal fue necesario la adquisición de conocimientos relacionados con LMS, para seleccionar el sistema que proporciona más ventajas al proyecto como lo es la escalabilidad y el soporte que reciben para que así, con el paso del tiempo, la plataforma pueda continuar con su funcionalidad mediante el aumento de materiales, su actualización o bien para que la plataforma crezca ofreciendo medios para la realización de exámenes.

Además, para lograr realizar el trabajo de manera simultánea a pesar de la distancia, se adquirió conocimientos sobre computo en la nube para la implementación de la plataforma y realizar la integración de los materiales desarrollados sin importar la ubicación geográfica, ya sea para nosotros como desarrolladores, sino también para los alumnos que nos ayudaron con sus comentarios durante la fase de pruebas.

Por último, a futuro esta plataforma virtual se puede seguir desarrollando y creciendo mediante el aumento y actualización de las preguntas que están contenidas en la base de conocimientos de Moodle, todo esto de acuerdo a la evolución de los temarios de la asignatura, además, al tener la base de la estructura de Moodle ya instalada se puede usar para la impartición de otras asignaturas en las cuales se requieran hacer entregas de materiales de estudio, de manera audiovisual como texto, o bien realizar exámenes para la evaluación de los alumnos, informes, avisos ,entrega de tareas o poner a su disposición materiales de interés que los ayuden en sus estudios.

Con todo lo anterior podemos dar por cubiertos los objetivos planteados para la realización de este proyecto y los que surgieron durante su desarrollo, ya que con esto se logra una contribución hacia la comunidad de la Facultad de Ingeniería integrada tanto por los académicos como por los alumnos.

Anexo 1. Programa de estudio de la asignatura de Redes de Datos Seguras.

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO
FACULTAD DE INGENIERÍA

PROGRAMA DE ESTUDIO

REDES DE DATOS SEGURAS	1598	8	14
Asignatura	Clave	Semestre	Créditos

INGENIERÍA ELÉCTRICA	INGENIERÍA EN COMPUTACIÓN	INGENIERÍA EN COMPUTACIÓN
División	Departamento	Licenciatura

Asignatura:		Horas/semana:		Horas/semestre:	
Obligatoria	X	Teóricas	6.0	Teóricas	96.0
Optativa		Prácticas	2.0	Prácticas	32.0
		Total	8.0	Total	128.0

Modalidad: Curso teórico-práctico

Seriación obligatoria antecedente: Sistemas de Comunicaciones

Seriación obligatoria consecuente: Ninguna

Objetivo(s) del curso:
El alumno integrará los conocimientos de protocolos, métodos y estándares sobre redes de datos dentro de las siete capas del modelo OSI, considerando medidas de seguridad en cada una de las capas de acuerdo a los estándares ISO 7498-1 e ISO 7498-2.

Temario

NÚM.	NOMBRE	HORAS
1.	Conceptos básicos	6.0
2.	Estándares y arquitecturas	6.0
3.	Capa física	16.0
4.	Capa de enlace de datos	16.0
5.	Capa de red	20.0
6.	Capa de transporte	8.0
7.	Capa de sesión	6.0
8.	Capa de presentación	6.0
9.	Capa de aplicación	12.0
		96.0
	Actividades prácticas	32.0
	Total	128.0

275

4/6/2015 17:38

1 Conceptos básicos

Objetivo: El alumno explicará las funciones principales de las redes de datos a través de las principales estructuras y posibles formas de enviar información.

Contenido:

1.1 Redes de comunicaciones de datos. Panorama general

1.2 Beneficios de las redes locales. Usos y aplicaciones

1.3 Topologías. Importante consideración de diseño.

- **1.3.1** Estrella.
- **1.3.2** Árbol.
- **1.3.3** Anillo.
- **1.3.4** Bus.
- **1.3.5** Malla.
- **1.3.6** Híbridas.

1.4 Evolución de las redes de datos. Principales características: cobertura geográfica, velocidad, control de errores, enlaces, historia ALOHA y X.25.

- **1.4.1** LAN.
- **1.4.2** MAN.
- **1.4.3** PAN.
- **1.4.4** WAN.
- **1.4.5** VLAN.

1.5 Fundamentos de seguridad.

- **1.5.1** Conceptos generales.

2 Estándares y arquitecturas

Objetivo: El alumno explicará los estándares y protocolos de redes de datos a tráves de los diferentes modelos de comunicaciones.

Contenido:

2.1 Organismos de estandarización. Objetivos, miembros, grupos de trabajo, organismos, etc.

- **2.1.1** ISO.
- **2.1.2** IEEE.
- **2.1.3** NOM.
- **2.1.4** TIA.
- **2.1.5** EIA.
- **2.1.6** ANSI.
- **2.1.7** ITU.
- **2.1.8** BROADBAND FORUM.

2.2 Modelo OSI de acuerdo al estándar 7498-1.

- **2.2.1** Definición de sistemas abiertos.
- **2.2.2** Capas del modelo OSI.

2.3 Arquitectura de seguridad de OSI estándar 7498-2.

- **2.3.1** Servicios de seguridad.
- **2.3.2** Mecanismos de seguridad.

2.4 Modelo TCP/IP.

2.4.1 Capas del modelo TCP/IP.

2.4.2 Capa física o hardware.

2.4.3 Capa de enlace o interfaz de red.

2.4.4 Capa de red o internet.

2.4.5 Capa de transporte.

2.4.6 Capa de aplicación.

2.4.7 Seguridad en TCP/IP.

2.5 Otros modelos (SNA, DNA, Netware, Appletalk).

3 Capa física

Objetivo: El alumno explicará los diferentes medios de transmisión y las ventajas de cada uno de ellos mediante los estándares IEEE y ANSI/TIA/EIA involucrados en la capa física.

Contenido:

3.1 Medios de transmisión terrestres o guiados.

3.1.1 Cable coaxial.

3.1.2 Par trenzado.

3.1.3 Fibra óptica.

3.2 Medios de transmisión aéreos o no guiados.

3.2.1 Redes inalámbricas.

3.2.2 Microondas.

3.2.3 Enlaces satelitales.

3.2.4 Rayo láser.

3.2.5 Infrarrojo.

3.3 Estándares de la capa física: RS-232, RS-422, RS-449.

3.4 Cableado estructurado.

3.4.1 Estándar EIA/TIA 568.

3.4.2 Estándar EIA/TIA 569.

3.4.3 Estándar EIA/TIA 598 /A.

3.4.4 Estándar EIA/TIA 606.

3.5 Dispositivos de interconexión.

3.5.1 Repetidor y Hub.

3.6 Conexiones a nivel WAN.

3.6.1 ATM.

3.6.2 Frame Relay.

3.7 Seguridad a nivel de capa física.

3.7.1 Confidencialidad en modo con conexión.

3.7.2 Confidencialidad del flujo de datos.

4 Capa de enlace de datos

Objetivo: El alumno analizará los diferentes tipos de protocolos, métodos y estándares utilizados en la capa de enlace, así como su aplicación en dispositivos físicos de esta capa.

Contenido:

4.1 Hand-shaking.

4.2 Transmisión asíncrona y síncrona.

4.3 Protocolos HDLC y SDLC.

4.4 Control de acceso al medio.

- **4.4.1** CSMA/CD y CSMA/CA.
- **4.4.2** Token.
- **4.4.3** FDDI.

4.5 Protocolo LLC y MAC del estándar IEEE 802 para redes de área local.

- **4.5.1** Capa LLC (IEEE 802.2).
- **4.5.2** Ethernet (IEEE 802.3).
- **4.5.3** Token Bus y Token Ring (IEEE 802.4 y 802.5).
- **4.5.4** Redes inalámbricas.
- **4.5.5** MAC Address.

4.6 Técnicas de conmutación.

- **4.6.1** Conmutación de circuitos.
- **4.6.2** Conmutación de mensajes.
- **4.6.3** Conmutación de paquetes.

4.7 Dispositivos de interconexión.

- **4.7.1** Puente.
- **4.7.2** Switch.
- **4.7.3** Control de congestión.
- **4.7.4** NIC (Network Interface Card).

4.8 Seguridad a nivel de capa enlace.

- **4.8.1** Confidencialidad en modo con conexión.
- **4.8.2** Confidencialidad en modo sin conexión.

5 Capa de red

Objetivo: El alumno resumirá los diferentes tipos de protocolos, métodos y estándares utilizados en la capa de red, a través de aplicaciones para su configuración en dispositivos físicos de esta capa, así como el funcionamiento del protocolo IP.

Contenido:

5.1 Protocolos del nivel red.

- **5.1.1** Protocolos.
- **5.1.2** Protocolo IPX.
- **5.1.3** DLS.

5.2 Redes y subredes.

- **5.2.1** Subneting.
- **5.2.2** VLSM.
- **5.2.3** CIDR.

5.3 Tablas de ruteo.

5.4 Protocolos de enrutamiento.

5.4.1 Algoritmos de enrutamiento estático.

5.4.2 Algoritmos de enrutamiento dinámico.

5.5 Servicios orientados a conexión.

5.6 Servicios no orientados a conexión.

5.7 Ruteadores.

5.7.1 Control de la congestión.

5.8 Seguridad a nivel de capa red.

5.8.1 Autenticación de participantes.

5.8.2 Autenticación del origen de datos.

5.8.3 Servicio de control de acceso.

5.8.4 Confidencialidad en modo conexión.

5.8.5 Confidencialidad en modo sin conexión.

5.8.6 Confidencialidad del flujo de datos.

5.8.7 Integridad en modo con conexión sin recuperación.

5.8.8 Integridad en modo sin conexión.

5.8.9 IPSec.

6 Capa de transporte

Objetivo: El alumno analizará los diferentes tipos de protocolos, métodos y estándares utilizados en la capa de transporte del modelo OSI mediante el análisis del funcionamiento de los protocolos TCP y UDP.

Contenido:

6.1 Servicios de la capa transporte.

6.2 Manejo de paquetes.

6.2.1 Fragmentación de paquetes.

6.2.2 Secuenciamiento.

6.2.3 Reensamble de paquetes.

6.3 Control de flujo.

6.3.1 Solicitud de respuesta automatica (ARQ).

6.3.2 Parada y espera (Stop-wait).

6.3.3 Venta deslizante.

6.4 Protocolos del nivel transporte.

6.4.1 Protocolo TCP.

6.4.2 Protocolo UDP.

6.5 Seguridad a nivel de capa transporte.

6.5.1 Autenticación de participantes.

6.5.2 Autenticación del origen de datos.

6.5.3 Servicio de control de acceso.

6.5.4 Confidencialidad en modo conexión.

6.5.5 Confidencialidad en modo sin conexión.

6.5.6 Integridad en modo con conexión con recuperación.

6.5.7 Integridad en modo con conexión sin recuperación.

6.5.8 Integridad en modo sin conexión.

7 **Capa de sesión**

Objetivo: El alumno analizará los diferentes tipos de protocolos, métodos y estándares revisando los mismos en la capa sesión del modelo OSI.

Contenido:

7.1 Uso de puertos de comunicación.

7.2 Hand shaking entre aplicaciones.

7.3 Servicios de nivel sesión.

7.4 Llamadas a procedimientos remotos (RPC).

8 Capa de presentación

Objetivo: El alumno analizará los diferentes tipos de protocolos, representación de datos, técnicas de compresión y criptografía a través de los estándares utilizados en la capa de presentación del modelo OSI.

Contenido:

8.1 Representaciones comunes de los datos.

8.1.1 ASCII 7 bits.

8.1.2 ASCII 8 bits.

8.1.3 Unicode.

8.2 Compresión de datos.

8.2.1 Formatos de compresión con pérdidas.

8.2.2 Formatos de compresión sin pérdidas.

8.3 Criptografía.

8.3.1 Algoritmos simétricos.

8.3.2 Algoritmos asimétricos.

8.4 Seguridad a nivel de capa presentación.

8.4.1 Confidencialidad en modo con conexión.

8.4.2 Confidencialidad en modo sin conexión.

8.4.3 Confidencialidad selectiva por elementos.

9 Capa de aplicación

Objetivo: El alumno clasificará los diferentes tipos de protocolos mediante las aplicaciones de la capa de aplicación del modelo OSI.

Contenido:

9.1 HTTP y HTTPS.

9.2 Compartir archivos.

9.2.1 SMB.

9.2.2 NFS.

9.3 Sesión remota.

9.3.1 Telnet.

9.3.2 SSH.

9.4 Transferencias de archivos.
- **9.4.1** FTP.
- **9.4.2** SFTP.
- **9.4.3** VSFTP.
- **9.4.4** TFTP.

9.5 Correo electrónico.

9.6 Protocolo de autenticación.
- **9.6.1** Páginas amarillas (yp).
- **9.6.2** LDAP.
- **9.6.3** Kerberos.
- **9.6.4** Radius.
- **9.6.5** Portal captivo o cautivo.

9.7 Redes sociales.

9.8 RFC 1700.

9.9 Seguridad a nivel de capa de aplicación.
- **9.9.1** Autenticación de participantes.
- **9.9.2** Autenticación del origen de datos.
- **9.9.3** Servicio de control de acceso.
- **9.9.4** Confidencialidad en modo conexión.
- **9.9.5** Confidencialidad en modo sin conexión.
- **9.9.6** Confidencialidad selectiva por elementos.
- **9.9.7** Confidencialidad del flujo de datos.
- **9.9.8** Integridad en modo con conexión con recuperación.
- **9.9.9** Integridad en modo con conexión sin recuperación.
- **9.9.10** Integridad en modo con conexión selectiva por elementos.
- **9.9.11** Integridad en modo sin conexión.
- **9.9.12** Integridad en modo sin conexión selectiva por elementos.
- **9.9.13** No repudio del origen.
- **9.9.14** No repudio del destino.

Bibliografía básica	**Temas para los que se recomienda:**
ARIGANELLO, Ernesto *Guia de estudio para la certificación CCNA 640-802* 2a. edición México Alfaomega, 2011	1, 2, 3, 4, 5
COMER, Douglas E. *Computer Networks and Internets* 6th edition Boston Massachusetts	Todos

Pearson, 2014

FOROUZAN, Behrouz
Transmisión de datos y redes de comunicaciones Todos
2a. edición
España
McGraw-Hill, 2002

GALLO, Michael, HANCOCK, William
Comunicación entre computadoras y tecnologías de redes Todos
México
Thomson, 2002

PETERSON, Larry L., DAVIE, Bruce S.
Computer Networks: A Systems Approach Todos
5th Edition
Boston
The Morgan Kaufmann, 2012

PETERSON, Larry, DAVIE, Bruce
Computer Networks Todos
2nd edition
USA
Morgan Kaufman Publishers, 2000

STALLINGS, William
Comunicaciones y redes de computadores Todos
6a. edición
España
Prentice Hall, 2000

TANENBAUM, Andrew S
Redes de computadoras Todos
4a. edición
México
Pearson Educación, 2003

Bibliografía complementaria **Temas para los que se recomienda:**

HALSALL, Fred
Comunicaciones de datos, redes y computadores y sistemas abiertos México Todos
Pearson Educación, 1998

KUROSE, James F., ROSS, Keith W.
Computer Networking: A Top-Down Approach Todos

6th Edition
USA
PEARSON, 2012

LEÓN-GARCÍA, Alberto, WIDJAJA, Indra
Redes de comunicación. Conceptos fundamentales y arquitecturas básicas España
McGraw-Hill, 2002

WHITE, Curt
Data Communications and Computer Networks: A Business Users Approach 7th Edition
Boston
Cengage Learning, 2012

Todos

Todos

Sugerencias didácticas

Exposición oral	X	Lecturas obligatorias	X
Exposición audiovisual	X	Trabajos de investigación	X
Ejercicios dentro de clase	X	Prácticas de taller o laboratorio	X
Ejercicios fuera del aula	X	Prácticas de campo	
Seminarios	X	Búsqueda especializada en internet	X
Uso de software especializado		Uso de redes sociales con fines académicos	
Uso de plataformas educativas			

Forma de evaluar

Exámenes parciales	X	Participación en clase	X
Exámenes finales	X	Asistencia a prácticas	X
Trabajos y tareas fuera del aula	X		

Perfil profesiográfico de quienes pueden impartir la asignatura

Licenciatura en Ingeniería en Computación, Ciencias de Computación, Ingeniería Eléctrica Electrónica, Ingeniería en Telecomunicaciones, Matemáticas Aplicadas o una carrera similar. Deseable haber realizado estudios de posgrado, contar con conocimientos y experiencia en el área de Redes y/o Seguridad, contar con experiencia docente o haber participado en cursos o seminario de iniciación en la práctica docente.

Anexo 2. Reactivos.

Preguntas Tema 1. Conceptos básicos.

1) <Tipo 2> De acuerdo con su función en una red de datos, los dispositivos se pueden clasificar en dos grupos:

Respuesta:

a) Inalámbricos.
b) Gestionadores.
c) Alámbricos.
d) De usuario.
e) Administrables.

2) <Tipo 5> Relacione el concepto con su definición de acuerdo con los elementos de una red de datos:

a) Dispositivos.	(c) Es todo aquello que se intercambia entre dispositivos en la red.
b) Medio.	(d) Es todo aquello que comparten los integrantes de una red para que los demás hagan uso de ellas
c)Información.	(b) Es la conexión que hace posible que los dispositivos se relacionen entre sí.
d) Recursos.	(a) Una de sus funciones es permitir el acceso y las comunicaciones en una red.

3) <Tipo 4> Como elemento de una red de datos el medio se define como “La vía por la cual se logra la transmisión de datos entre los equipos de una red”.

a) Cierto.
b) Falso.

4) <Tipo 1> Es un elemento de una red que está presente en dispositivos tanto de gestión y comunicación como de usurario y es todo aquello que se intercambia en la red.

a) Dispositivos.
b) Medio.
c) Información.
d) Recursos.
e) Enlaces.

5) <Tipo 1> Al implementar una red de área local nos brinda de varios beneficios, ¿cuál de los siguientes es un beneficio de una red local?

- Procesos de respaldo más efectivos.
- Equipos periféricos compartidos.
- Comunicación personal más eficiente.
- Acceso simultáneo a programas e información.

a) Todos los anteriores.
b) La primera y tercera opción
c) La segunda y cuarta opción.
d) Solo la primera y última opción.
e) Ninguna de las anteriores.

6) <Tipo 1> Cuando se empieza el diseño de una red es importante considerar su topología, ¿Cuál de las siguientes no es una topología de red?

a) Túnel.
b) Estrella.
c) Hibrida.
d) Malla.
e) Árbol.

7) <Tipo 3> Cada topología recibe su nombre a partir de la manera en que esta se conecta. A continuación, relacione la definición con la topología correspondiente con las topologías que la poseen.

a) Estrella.
b) Árbol.
c) Anillo.
d) Bus.
e) Malla.
f) Hibrida.

(e) es una topología de red en la que cada nodo está conectado a todos los nodos. De esta manera es posible llevar los mensajes de un nodo a otro por distintos caminos.

(b) es una topología de red parecida a una serie de redes en estrella interconectadas salvo en que no tiene un concentrador central.

(f) es una topología de red que se deriva de la unión de dos o más topologías.

(a) es una topología de red donde las estaciones están conectadas directamente a un punto central y todas las comunicaciones se hacen necesariamente a través de ese punto.

(c) es una topología de red en la que cada estación tiene una única conexión de entrada y otra de salida ya que la información solo viaja en un sentido.

(d) es una topología de red donde cada computadora está conectada a un segmento común de cable de red.

8) <Tipo 1> En esta topología los equipos están conectados a un nodo central y todas las comunicaciones se realizan mediante este nodo central.

a) Bus.
b) Árbol.
c) Estrella.
d) Hibrida.
e) Malla.
f) Anillo.

9) <Tipo 1> Esta topología es parecida a una serie de redes de estrella interconectadas entre sí

a) Bus.
b) Árbol.
c) Estrella.
d) Hibrida.
e) Malla.
f) Anillo.

10) <Tipo 1> En esta topología cada nodo está conectado a todos y cada uno de los demás nodos. De tal forma que es posible llevar los mensajes de un nodo a otro de manera directa.

a) Árbol.
b) Estrella.
c) Hibrida.
d) Malla.
e) Anillo.
f) Bus.

11) <Tipo 1> Esta topología combina las características de dos o más topologías distintas y suele usarse para conectar diferentes redes entre sí,

a) Árbol.
b) Estrella.
c) Híbrida.
d) Malla.
e) Anillo.
f) Bus.

12)<Tipo 3> Las redes de datos se pueden clasificar de acuerdo con su cobertura geográfica. Relaciona el acrónimo de la clasificación de la red con sus características.

a) PAN.
b) LAN.
c) VLAN.
d) MAN.
e) WAN.

(e) Es una red que puede proporcionar medios de transmisión a lo largo de extensiones geográficas a nivel regional, nacional e internacional

(c) Esta red consiste en dos o más redes que se comportan como si estuviesen conectadas al mismo conmutador, aunque se encuentren físicamente conectadas a diferentes segmentos de una LAN

(a) Son redes de menor alcance, se utiliza para interconectar dispositivos personales muy cercanos entre sí.

(d) Estas redes están diseñadas para la conexión de equipos a lo largo de una ciudad entera.

(b) Este tipo de red permite la conexión de los equipos dentro de un único edificio, oficina o campus.

13)<Tipo 4> Las Personal Area Networks tienen una distancia entre procesadores de aproximadamente un metro. Un ejemplo de estas redes es el Bluethoot

a) Cierto.
b) Falso.

14)<Tipo 4> Las Local Area Networks son redes que tienen una distancia de alcance desde 100 metros a un 1 kilómetro, abarcan el área de una oficina o un edificio y pueden ser implementadas de manera virtual (VLAN).

a) Cierto.
b) Falso.

15)<Tipo 4> Las redes de Área local están restringidas a pequeñas áreas como pueden ser una casa, departamento u oficina

a) Cierto.
b) Falso.

16)<Tipo 2> Estas redes superan el alcance de un kilómetro suelen usarse para interconectar varias redes LAN.

a) PAN.
b) LAN.
c) VLAN.
d) MAN.
e) WAN.

17)<Tipo 1> La comunicación entre los nodos de una red puede ser de varias formas, ¿cuál de ellas solo permite el envío de información en un solo sentido?, de manera análoga es parecida a la comunicación que se realiza por un dispositivo de Walkie Talkie.

a) Full dúplex.
b) Punto a punto.
c) Multipunto.
d) Half dúplex.
e) Síncrono.

18)<Tipo 1> La comunicación entre los nodos de una red puede ser de varias formas, ¿cuál de ellas permite el envío de información de manera simultánea sin que ninguno de los nodos involucrados en la comunicación tenga que esperar a que el otro nodo termine enviar su información?

a) Full dúplex.
b) Punto a punto.
c) Multipunto.
d) Half dúplex.
e) Asíncrono.

19)<Tipo 4> Existen diferentes tipos de enlaces para la comunicación entre un nodo de una red con otro dispositivo de la misma red. Uno de ellos es el enlace Punto a Punto usualmente usado para comunicaciones inalámbricas.

a) Cierto.
b) Falso.

20)<Tipo 5> Existen diferentes tipos de enlaces para la comunicación entre un nodo de una red con otro dispositivo de la misma red. Uno de ellos es el enlace _____ usualmente usado para comunicaciones inalámbricas.

a) Full dúplex.
b) Punto a punto.
c) Multipunto.
d) Half dúplex.
e) Ninguna de las anteriores.

21)<Tipo 1> Se utiliza para conectar una o varias computadoras a una red privada a través de internet en un canal cifrado.

a) VPN.
b) Proxy.
c) Enrutamiento estático.
d) Enrutamiento dinámico.

22)<Tipo 1> Cualquier medida que impida la ejecución de operaciones no autorizadas sobre un sistema informático o red de datos que puedan afectar su información.

a) Seguridad Informática.
b) Seguridad de la información.
c) Seguridad en routers.
d) Políticas y normas.

23)<Tipo 2> ¿Cuáles son los tres elementos que conforman la famosa “Triada de la seguridad”?

1) Disponibilidad.
2) Integridad.
3) Confidencialidad.
4) Accesibilidad.
5) Velocidad.

24)<Tipo 4> La confidencialidad garantiza que la información sea accesible únicamente para las personas autorizadas.

a) Cierto.
b) Falso.

25)<Tipo 4> La integridad garantiza que la información no podrá ser modificada por “entes” que no tengan los permisos requeridos.

a) Cierto.
b) Falso.

26)<Tipo 4> La Disponibilidad garantiza el acceso a la información en cualquier momento que se requiera consultar.

a) Cierto.
b) Falso.

27)<Tipo 1> Es el método por el cual un individuo, mediante un sistema informático logra tomar el control, desestabilizar o dañar otro sistema informático (computadora, red).

1) Ataque.
2) Amenaza.
3) Vulnerabilidad.
4) Terrorismo.

28)<Tipo 1> Es el método por el cual un individuo, mediante un sistema informático intenta tomar el control, desestabilizar o dañar otro sistema informático (computadora, red).

5) Ataque.
6) Amenaza.
7) Vulnerabilidad.
8) Terrorismo.

29)<Tipo 2> ¿Cuáles son las categorías en las que se clasifican los ataques?

a) Intercepción.
b) Modificación.
c) Interrupción.
d) Suplantación.
e) Falsificación.
f) Robo de identidad.
g) Phishing.
h) Virus.
i) Gusanos.

30)<Tipo 3> Relaciona las siguientes columnas

a) Intercepción.	(b) Atenta contra la integridad.
b) Modificación.	(a) Atenta contra la confidencialidad.
c) Interrupción.	(d) Atenta contra la autenticidad.
d) Suplantación.	(c) Atenta contra la disponibilidad.

31)<Tipo 1> Es un defecto o falla en un sistema informático que puede poner en riesgo la seguridad de la información.

a) Vulnerabilidad.
b) Falla.
c) Riesgo.
d) Amenaza.

32)<Tipo 1> Es la probabilidad de que ocurra un evento no deseado

a) Riesgo.
b) Falla.
c) Vulnerabilidad.
d) Amenaza.

33)<Tipo 1> Se aprovecha de la o las vulnerabilidades de un sistema informático para atentar contra el mismo.

a) Amenaza.
b) Riesgo.
c) Vulnerabilidad.
d) Falla.

34)<Tipo 5>Relaciona las siguientes columnas.

a) Vulnerabilidad.	(b) Es la probabilidad de que ocurra un evento no deseado.
b) Riesgo.	(c) Se aprovecha de la vulnerabilidad de un sistema para atentar contra.
c) Amenaza.	(a) Es un defecto o falla en un sistema informático que puede poner en riesgo la seguridad del mismo.

35)<Tipo 1> Consiste en el robo de información mediante la suplantación de una entidad de confianza.

a) Virus.
b) Phishing.
c) Gusano.
d) Ingeniería Social.

36)<Tipo 1> Su motivación es encontrar fallas y vulnerabilidades en sistemas informáticos y notificarlos a la empresa o hacerlos públicos con el fin de que estas sean resueltas lo más rápido posible.

a) Hacker de sombrero blanco.
b) Hacker de sombrero gris.
c) Hacker de sombrero negro.
d) Hacker de sombrero morado.
e) Hacker de sombrero rojo.

37)<Tipo 1> Su motivación es encontrar fallas y vulnerabilidades en sistemas informáticos con el fin de explotarlas para acceder a la información y obtener algún beneficio de esta.

a) Hacker de sombrero blanco.
b) Hacker de sombrero gris.
c) Hacker de sombrero negro.
d) Hacker de sombrero morado.
e) Hacker de sombrero rojo.

38)<Tipo 1> Su motivación es encontrar fallas y vulnerabilidades en sistemas informáticos con el fin de venderlas al mejor postor, sin importar el uso que se les dé a estas.

a) Hacker de sombrero blanco.
b) Hacker de sombrero gris.
c) Hacker de sombrero negro.
d) Hacker de sombrero morado.
e) Hacker de sombrero rojo.

39)<Tipo 1> Es una persona fuera de alguna empresa de consultoría de ciberseguridad contratado por la empresa para buscar vulnerabilidades en sus productos (redes, programas, equipos) antes de su lanzamiento, para poder corregirlas.

a) Hacker de sombrero blanco.
b) Hacker de sombrero gris.
c) Hacker de sombrero negro.
d) Hacker de sombrero morado.
e) Hacker de sombrero rojo.

40)<Tipo 1> Es una persona que se caracteriza por utilizar, promover y mejorar el software libre.

a) Hacker de sombrero blanco.
b) Hacker de sombrero gris.
c) Hacker de sombrero negro.
d) Hacker de sombrero morado.
e) Hacker de sombrero rojo.

41)<Tipo 4> Se considera “Cracker” a una persona que posee un nivel elevado de conocimientos de programación y redes de datos.

a) Cierto.
b) Falso.

42)<Tipo 4> Se considera “Cracker” a la persona que posee un elevado conocimiento en programación y redes de datos y lo utiliza para explotar un sistema con el fin de obtener algún beneficio.

a) Cierto.
b) Falso.

43)<Tipo 1> Conjunto de reglas y principios para lograr la seguridad, tener un orden y hacer buen uso de los elementos que conforman la red de la empresa u organización.

a) Políticas de seguridad.
b) Normas de seguridad.
c) Reglas de seguridad.
d) Reglamento de trabajo.

44)<Tipo 1> Es la práctica de obtener información confidencial a través de la manipulación de los usuarios y no de los sistemas informáticos.

a) Ingeniería Social.
b) Phishing.
c) Suplantación.
d) Robo.

45)<Tipo 4> Los ataques se clasifican en activos y pasivos

a) Cierto.
b) Falso.

46)<Tipo1> Estos ataques no implican la modificación del flujo de datos entre los dispositivos, sino que se enfocan en monitorear la red para obtener la información que necesitan.

a) Ataques pasivos.
b) Ataques activos.
c) Ataques Man in the middle.
d) Ataques de inyección.

47)<Tipo 1> Estos ataques implican algún tipo de modificación del flujo de datos transmitido o la creación de un falso flujo de datos para acceder a la información.

a) Ataques Pasivos.
b) Ataques Activos.
c) Inyección de SQL.
d) Troyano.

48)<Tipo 1> Son personas que utilizan programas desarrollados por alguien más (sin saber cómo funcionan en realidad) para atacar sistemas informáticos.

a) Script Kiddie.
b) Newbie.
c) Samurai.
d) Ninja.

49)<Tipo 1> Son crackers que saben exactamente lo que buscan, donde encontrarlo y como obtenerlos.

a) Script Kiddie.
b) Newbie.
c) Samurái.
d) Ninja.

50)<Tipo 1> Son aquellos que están comenzando en el mundo del hacking.

a) Script Kiddie.
b) Newbie.
c) Samurái.
d) Ninja.

Preguntas Tema 2. Estándares y arquitecturas.

1. <Tipo 4> La estandarización asegura que un producto o servicio siga ciertas reglas que serán aceptadas por cualquiera que quiera hacer uso del mismo, contando con calidad, seguridad, eficiencia e interoperabilidad y sobre todo a un costo aceptable.

   ¿Esta definición es correcta?

   a) Cierto
   b) Falso

2. <Tipo 1> La estandarización asegura ‘cuatro’ cualidades que tendrá el producto o servicio que se esté ofreciendo:

   Indica cuales son estas cuatro cualidades

   I. Calidad
   II. Seguridad
   III. Eficiencia
   IV. interoperabilidad
   V. Disponibilidad
   VI. Control de calidad
   VII. Eficiencia
   VIII. Eficacia

   1) I, II, III, IV
   2) V, VI, VII, VIII
   3) I, II, V, VI
   4) III, IV, VII, VIII
   5) Ninguna de las anteriores

3. <Tipo 1> Cuáles son las siglas de la organización encargada de la estandarización en México?
    a) NOM
    b) ISO
    c) ANSI
    d) IEEE
    e) IFT

4. <Tipo 1> Indica cuales son las siete capas del modelo OSI
    a) Física, enlace, red, transporte, sesión, presentación y aplicación.
    b) Física, comunicación, enlace, login, sesión, presentación, Interfaz.
    c) Física, enlace, transporte, comunicación, presentación, aplicación, interfaz.
    d) Red Física, Vinculo de datos, Internet, Transporte y Aplicación.

5. <Tipo 1> La estandarización asegura que un producto o servicio siga ciertas reglas que serán aceptadas por cualquiera que quiera hacer uso del mismo, contando con _____, _____, _____, _____ y sobre todo a un costo aceptable.

    I. Calidad
    II. Seguridad
    III. Eficiencia
    IV. interoperabilidad
    V. Disponibilidad
    VI. Control de calidad
    VII. Eficiencia
    VIII. Eficacia

    a) I, II, III, IV
    b) V, VI, VII, VIII
    c) I, II, V, VI
    d) III, IV, VII, VIII

6. <Tipo 4> Un protocolo es un conjunto de reglas que se deben de seguir para realizar la comunicación de dos o más elementos de red.

    a) Cierto.
    b) Falso.

7. <Tipo 4> Un protocolo es un conjunto de estándares que se deben de seguir para realizar la comunicación de dos o más elementos de red.

    a) Cierto.
    b) Falso.

8. <Tipo 2> ¿Cuáles son las dos interfaces que provee un protocolo?

    a) Interfaz de servicio.
    b) Interfaz peer to peer.
    c) Estado de servicio.
    d) Calidad de conexión.

9. <Tipo 4> Una ventaja de la estandarización es la interoperabilidad entre los diferentes tipos de equipos, asegurándonos que todos funcionarán de manera correcta independientemente de su fabricante

    a) Cierto.
    b) Falso.

10. <Tipo 3> Relaciona la capa con la función que desempeña.

a) Controla la transmisión de la cadena de bits sobre el medio físico.
b) Capa responsable de la confiabilidad en cuanto al envío de la información por parte de la capa física, se encarga de iniciar, mantener y terminar una comunicación entre punto a punto.
c) Establece la ruta a seguir para el envío de información entre dos nodos sobre una red de datos.
d) garantiza la confiabilidad del enlace en la red. Provee la corrección de errores y el control de flujo entre los dos puntos finales conectados en la red.
e) Establece, administra y termina la conexión a nivel usuario y administra la interacción entre los sistemas finales.
f) Realiza la transformación de datos para proveer una interfaz común para la aplicación del usuario.
g) Provee directamente el servicio solicitado.

(a) Física.
(b) Enlace.
(c) Red.
(d) Transporte.
(e) Sesión.
(f) Presentación.
(g) Aplicación.

11. <Tipo 1> El “encoding” es la forma en que la información es transmitida en términos de bits. ¿En qué capa se da esta operación?

a) Física.
b) Enlace.
c) Red.
d) Transporte.
e) Sesión.
f) Presentación.
g) Aplicación.

12. <Tipo 1>El “framing” es la segmentación de paquetes para su envío a través de la red ¿En qué capa se realiza esta operación?

    a) Física.
    b) Enlace.
    c) Red.
    d) Transporte.
    e) Sesión.
    f) Presentación.
    g) Aplicación.

13. <Tipo 2>El “error detecting” es la detección de errores en la transmisión de la información, esta operación se realiza en tres capas. Indica cuáles capas detectan errores de transmisión.

    a) Física.
    b) Enlace.
    c) Red.
    d) Transporte.
    e) Sesión.
    f) Presentación.
    g) Aplicación.

14. <Tipo 1> “Reliable Trasmision” es la seguridad de que toda la información será recibida. Indica en qué capa se realiza esta operación.

    a) Física.
    b) Enlace.
    c) Red.
    d) Transporte.
    e) Sesión.
    f) Presentación.
    g) Aplicación.

15. <Tipo 2> El framing es la fragmentación de información para ser enviada a través de la red, esta de da de dos maneras, indica cuáles son las maneras de fragmin.

    a) Byte Oriented.
    b) Bit Oriented.
    c) Sentinel.
    d) Counting.
    e) HDLC.
    f) SDLC.

16. <Tipo 1> Este protocolo es uno de los más importantes dentro de la capa de enlace, ya que a partir de él surgen protocolos más sofisticados como Frame Relay e ISDN entre otros.

    a) Byte Oriented.
    b) Bit Oriented.
    c) Sentinel.
    d) Counting.
    e) HDLC.
    f) SDLC.

17. <Tipo 1> Cuáles son las tres técnicas más comunes utilizadas para la detección de errores de envío de información.

    a) 2-D Parity Checking.
    b) Checksum.
    c) Cyclic Redundancy Check.
    d) Duplicate information.
    e) information encryption.
    f) decryption of information.

18. <Tipo 4>Los algoritmos de ruteo permiten conocer la red, es decir, nos dan la ruta por la cual la información debe pasar.

a) Cierto.
b) Falso.

19. <Tipo 1> El protocolo IP (internet protocol) se apoya en los protocolos _____ y _____ para permitir la comunicación entre dos elementos de la red.

a) TCP y UDP.
b) TCP y HDLC.
c) UDP y SDLC.
d) UDP y HDLC.
e) TCP y SDLC.

20. <Tipo 5>Relaciona las capas de modelo TCP/IP con la función que desempeñan.

a) Los protocolos de este nivel proporcionan los medios para que el sistema envíe la información a los otros elementos de la red.
b) Capa responsable de la confiabilidad en cuanto al envío de información, inicia, mantiene y termina una comunicación entre punto y punto.
c) IP da el servicio básico de envío de paquetes sobre el cual se construyen las redes TCP/IP, toda la información fluye a través de IP sin importar el destino final.
d) Esta capa incluye todos los procesos que usan los protocolos de nivel de transporte para enviar la información.

(a) Capa Física.
(b) Capa de Enlace.
(c) Capa de Internet.
(d) Capa de aplicación.

21. <Tipo 1> Este protocolo proporciona un servicio de envío de datos confiable con detección y corrección de errores de extremo a extremo.

    a) TCP.
    b) UDP.
    c) HDLC.
    d) SDLC.

22. <Tipo 1> Este protocolo proporciona un servicio de envío de datagramas con menos información de control y sin conexión.

    a) TCP.
    b) UDP.
    c) HDLC.
    d) SDLC.

23. <Tipo 4> Aunque los protocolos TCP y UDP funcionan de manera diferente, su objetivo es el mismo, el cual es el envío de información entre las capas de enlace e internet del modelo TCP/IP.

    a) Cierto.
    b) Falso.

24. <Tipo 5> Relaciona el protocolo con el tipo de información que envía

a) Protocolo para realizar una conexión remota a un elemento, nodo o servidor.	(a) Telnet
b) Protocolo para el envío de archivos.	(b) FTP
c) Protocolo para el envío de correo electrónico.	(c) SMTP
d) Protocolo para el envío de páginas de Hipertexto.	(d) HTTP
e) Protocolo para la autoadministración de la red IP.	(e) SNMP

25. <Tipo 2> La capa uno del modelo OSI se encarga de la comunicación a través de un medio _____ y una interfaz.

a) Físico.
b) Electrónico.
c) Eléctrico.
d) Magnético.

26. <Tipo 4> "*El estándar ISO 7498-2 proporciona una descripción de los servicios de seguridad y mecanismos asociados, con el fin de garantizar la seguridad de los sistemas abiertos o las transferencias de datos en dichos sistemas."* La anterior oración es…

a) Cierta.
b) Falsa.

27. <Tipo 1> A continuación se muestran mecanismos de seguridad ¿Cuáles de estos mecanismos son de seguridad específicos?

I. Mecanismo de cifrado.
II. Mecanismo de etiquetas de seguridad.
III. Mecanismo de detección de eventos.
IV. Mecanismo de control de acceso.
V. Mecanismo de certificación.
VI. Mecanismo de recuperación de seguridad.
VII. Mecanismo de firma digital.

a) I, IV, V, VII
b) I, III, VI, VII
c) I, II, III, V, VII
d) I, IV, V, VI, VII
e) I, II, IV, V, VII

28. <Tipo 2> El estándar 7498-2 define cinco servicios de seguridad ¿Cuáles de los siguientes servicios son los que define?

a) Servicios de certificación.
b) Servicios de autenticación.
c) Servicios de no repudio.
d) Servicios de cifrado.
e) Servicios de firma digital.
f) Servicios de confidencial de datos.

29. <Tipo 1> Este servicio definido en el estándar ISO 7498-2 se encarga de corroborar la veracidad de la fuente de una unidad de datos.

a) Servicio de autenticación.
b) Servicio de control de acceso.
c) Servicio de confidencialidad de datos.
d) Servicio de integridad de datos.
e) Servicio de no repudio.

30. <Tipo 1> Este servicio definido en el estándar ISO 7498-2 se utiliza para evitar el uso no autorizado de los recursos.

a) Servicio de autenticación.
b) Servicio de control de acceso.
c) Servicio de confidencialidad de datos.
d) Servicio de integridad de datos.
e) Servicio de no repudio.

31. <Tipo 1> Este servicio definido en el estándar ISO 7498-2 proporciona protección contra la revelación deliberada o accidental de los datos en una comunicación.

a) Servicio de autenticación.
b) Servicio de control de acceso.
c) Servicio de confidencialidad de datos.
d) Servicio de integridad de datos.
e) Servicio de no repudio.

32. <Tipo 1> Este servicio definido en el estándar ISO 7498-2 garantiza que los datos que recibe un receptor sean los mismos que han sido enviados por el emisor.

a) Servicio de autenticación.
b) Servicio de control de acceso.
c) Servicio de confidencialidad de datos.
d) Servicio de integridad de datos.
e) Servicio de no repudio.

33. <Tipo 1> Este servicio definido en el estándar ISO 7498-2 proporciona las pruebas ante una tercera parte de que cada una de las entidades comunicantes han participado en una comunicación.

a) Servicio de autenticación.
b) Servicio de control de acceso.
c) Servicio de confidencialidad de datos.
d) Servicio de integridad de datos.
e) Servicio de no repudio.

34. <Tipo 1> Este modelo consta de las capas de aplicación, presentación, sesión, transporte, red, enlace de datos y física, es un modelo de referencia desarrollado en 1984 y proporcionó a los fabricantes un conjunto de estándares que aseguraron una mayor compatibilidad e interoperabilidad entre los distintos tipos de tecnología de red.

a) Modelo TCP/IP.
b) Modelo OSI.
c) Modelo SNA.
d) Modelo DNA.
e) Modelo ISO.

35. <Tipo 1> Este modelo consta de las capas de aplicación, transporte, red, enlace y física, es usado para comunicaciones en redes y describe un conjunto de guías generales de operación para permitir que un equipo pueda comunicarse en una red. Fue implementado en la red ARPANET.

a) Modelo TCP/IP.
b) Modelo OSI.
c) Modelo SNA.
d) Modelo DNA.
e) Modelo ISO.

36. <Tipo 1> En el modelo TCP/IP en la capa de _____ es donde se especifican las características que se utilizarán para el hardware.

a) Capa física.
b) Capa de enlace.
c) Capa de red.
d) Capa de transporte.
e) Capa de aplicación.

37. <Tipo 1> En el modelo TCP/IP en la capa de _____ se define en qué forma los datos se enrutan, además, esta capa admite los datagramas IP y los transmite como tramas a través de un hardware específico.

a) Capa de hardware.
b) Capa de interfaz de red.
c) Capa de internet.
d) Capa de transporte.
e) Capa de aplicación.

38. <Tipo 1> En el modelo TCP/IP en la capa de _____ es donde se coloca el paquete en un datagrama de IP, a su vez se coloca una cabecera y una cola de datagrama y se decide a donde se enviará el datagrama.

a) Capa de hardware.
b) Capa de interfaz de red.
c) Capa de internet.
d) Capa de transporte.
e) Capa de aplicación.

39. <Tipo 1> En el modelo TCP/IP en la capa de _____ se brinda los datos de enrutamiento, junto con los mecanismos que permiten conocer el estado de la transmisión.

a) Capa física.
b) Capa de enlace.
c) Capa de red.
d) Capa de transporte.
e) Capa de aplicación.

40. <Tipo 1> En el modelo TCP/IP en los programas de la capa de _____ envían mensajes o corrientes de datos a uno de los protocolos de la capa de transporte de internet, ya sea UDP o TCP.

a) Capa física.
b) Capa de enlace.
c) Capa de red.
d) Capa de transporte.
e) Capa de aplicación.

41. <Tipo 2> Los protocolos TCP/IP pueden ser vulnerados con base en dos conceptos inherentes a su diseño. ¿Cuáles son esos conceptos? (Selecciona los dos correctos).

a) El modo en que se realiza el direccionamiento.
b) Los programas de la capa de aplicación son volubles.
c) El formato de los paquetes de los diferentes protocolos.
d) El modo de funcionamiento de los protocolos.
e) El formato del datagrama de cabecera.

42. <Tipo 4> “Systems Network Architecture (SNA) es una arquitectura de red diseñada y utilizada por Digital Equipment Corporation (DEC) para la conectividad con sus hots o mainframes” La anterior sentencia es…

    a) Cierta.
    b) Falsa.

43. <Tipo 1> Esta arquitectura de red fue creado por Digital Equipment Corporation (DEC) en 1975, fue diseñada para servidores DEC’s fuera de línea y provee dos formas de implementación.

a) TCP/IP.
b) OSI.
c) ISO.
d) SNA.
e) DNA.
f) Netware.
g) Appletalk.

44. <Tipo 1> Fue desarrollado por Novell Corporation, es un producto de software que corre sobre distintos tipos de LAN’s, desde Ethernet a IBM con topología de anillo.

a) TCP/IP.
b) OSI.
c) ISO.
d) SNA.
e) DNA.
f) Netware.
g) Appletalk.

45. <Tipo 1> Este modelo define una serie de especificaciones que describen las conexiones de computadoras Macintosh, impresoras y otros recursos o computadoras dentro de una red.

a) TCP/IP.
b) OSI.
c) ISO.
d) SNA.
e) DNA.
f) Netware.
g) Appletalk.

46. <Tipo 4> *SNA posee seis capas de operación las cuales son:*

- *Física*
- *Control de enlace de datos (DLC- Data Link Control).*
- *Control de Ruta (Path control).*
- *Control de flujo de datos (Data flow control).*
- *Servicios de presentación (Presentation services).*
- *Servicios de transacción (Transaction services).*

Lo anterior escrito es…

a) Correcto.
b) Incorrecto.

47. <Tipo 2> La arquitectura DNA provee dos opciones de implementación, la aplicación así y la aplicación DNA, en esta última usa se reemplaza unas capas por la capa de control de sesión ¿Cuáles son estas capas que son sustituidas?

a) Física.
b) Enlace de datos.
c) Red.
d) Transporte.
e) Sesión.
f) Presentación.
g) Aplicación.

48. <Tipo 2> Netware implementa distintos protocolos en sus capas, ¿cuáles de los siguientes protocolos conforman a Netware?

a) UDP.
b) UTP.
c) SPX.
d) AppleShare.
e) DLC.
f) NCP.
g) ATP.
h) IPX.

49. <Tipo 2> ¿Cuáles de los siguientes protocolos implementa Appletalk?

a) UDP.
b) NCP.
c) ATP.
d) NBP.
e) ZIP.
f) SNA.

50. <Tipo 5> Relacione el protocolo con la organización que lo diseñó.

a) OSI.
b) TCP/IP.
c) SNA.
d) DNA.
e) Netware.
f) Appletalk.

(e) Novell Corporation.
(a) International Organization for Standardization.
(b) Defense Advanced Research Projects Agency.
(c) International Business Machines Corporation.
(f) Apple.

Preguntas Tema 3. Capa Física

1. <Tipo 1> ¿Cuáles son los medios físicos de transmisión más comunes?

a) Terrestres y Aéreos.
b) Espaciales y Aéreos.
c) Terrestres y Espaciales.
d) Cableado y Radiofrecuencia.
e) Electrónicos y transmisores de luz.
f) Ninguna de las anteriores.

2. <Tipo 2> ¿Cuál de las siguientes opciones son medios de transmisión terrestre?

a) Par trenzado.
b) Cable coaxial.
c) Fibra óptica.
d) Microondas.
e) Rayo infrarrojo.
f) Rayo láser.

3. <Tipo 2> ¿Cuál de las siguientes opciones son medios de transmisión aérea?

a) Par trenzado.
b) Cable coaxial.
c) Fibra óptica.
d) Microondas.
e) Rayo infrarrojo.
f) Rayo láser.

4. <Tipo 2> Existen dos tipos de cable coaxial, ThinLAN y ThickLAN. Indica cuales son las diferencias entre ambos.

a) Longitud de transmisión sin repetidores.
b) Ancho de banda.
c) Resistencia eléctrica.
d) Diámetro de los hilos conductores.
e) Material de fabricación.
f) Tipos de conectores.

5. <Tipo 2> ¿Cuale son los dos modelos de cable coaxial que se utilizan en redes de datos?

a) ThinLAN.
b) ThickLAN.
c) ThinEthernet.
d) ThickEthernet.
e) Ethernet.
f) Par trenzado.
g) UTP.

6. <Tipo 1> ¿Cuál es la distancia máxima de transmisión de un cable thinLAN sin utilizar repetidores?

a) 185 [m].
b) 500 [m].
c) 200 [m].
d) 100 [m].
e) 85 [m].

7. <Tipo 1> ¿Cuál es la distancia máxima de transmisión de un cable ThickLAN sin utilizar repetidores?

a) 185 [m].
b) 500 [m].
c) 200 [m].
d) 100 [m].
e) 85 [m].

8. <Tipo 4> El cable UTP es comúnmente utilizado en redes de datos, debido a que posee una longitud de transmisión sin repetidores de hasta 100 m, además de que sus cables vienen en pares trenzados en forma helicoidal para evitar la interferencia de pares trenzados cercanos.

a) Cierto.
b) Falso.

9. <Tipo 3> Relaciona las columnas

A. Medios de transmisión aéreos.	(B) Par trenzado.
B. Medios de transmisión terrestre.	(B) Cable coaxial.
	(B) Fibra óptica.
	(A) Microondas.
	(A) Rayo infrarrojo.
	(A)Rayo láser.

10. <Tipo 2> ¿Cuáles son los dos tipos de cable de par trenzado que existen?

a) UTP.
b) STP.
c) FTP.
d) SMNP.
e) UDP.
f) Ninguna de las anteriores.

11. <Tipo 1> ¿Cuál es la distancia máxima de transmisión de un cable UTP sin utilizar repetidores?

a) 100 [m].
b) 200 [m].
c) 50 [m].
d) 185 [m].
e) 250 [m].

12. <Tipo 1> ¿Cuál es la distancia máxima de transmisión de un cable STP sin utilizar repetidores?

a) 100 [m].
b) 200 [m].
c) 50 [m].
d) 185 [m].
e) 250 [m].

13. <Tipo 2> ¿Cuáles son las diferencias entre las categorías 3, 4, 5 y 6 del cable UTP?

a) El número de trenzas por pie.
b) La velocidad de transmisión.
c) El número de pares trenzados.
d) El número de hilos conductores.
e) No existe diferencia.

14. <Tipo 1> ¿Cuál es el tipo de conectores utilizados en líneas telefónicas?

a) RJ45.
b) RJ11.
c) BNC.
d) Banana.
e) Ninguna de las anteriores.

15. <Tipo 1> ¿Cuál es el tipo de conectores utilizados en líneas ethernet?

a) RJ45.
b) RJ11.
c) BNC.
d) Banana.
e) Ninguna de las anteriores.

16. <Tipo 4>La fibra óptica consiste en un medio de vidrio, forrado por un aislante plástico, en el cual la información viaja en forma de luz.

a) Cierto.
b) Falso.

17. <Tipo 2> ¿Cuáles son los dos tipos de fibra óptica que existen?

a) Monomodo.
b) Multimodo.
c) Unimodo.
d) Vidrio.
e) Plástico.
f) Ninguna de las anteriores.

18. <Tipo 4> En las fibras monomodo la información viaja únicamente en una dirección, lo que permite distancias de transmisión mayores.

a) Cierto.
b) Falso.

19. <Tipo 4> En las fibras multimodo la información viaja reflejándose en la fibra, con lo cual permite enviar diversos haces de luz a través de la fibra, pero la distancia es menor que en una fibra monomodo.

a) Cierto.
b) Falso.

20. <Tipo 1> ¿Entre qué frecuencias se transmiten las microondas?

a) Entre 300 [MHz] y 30 [GHz].
b) 3 [MHz] y 30 [MHz].
c) 30 [MHZ] y 300[MHz].
d) menor a 15[Hz].
e) mayor a 30 [GHz].

21. <Tipo 2>La interfaz RS-232 es un conjunto de estándares que especifican tres interfaces. ¿Cuáles son estas interfaces?

a) Eléctrica.
b) Funcional.
c) Mecánica.
d) Electrónica.
e) Comunicación.

22. <Tipo 4>La interfaz RS-449 es una extensión de la interfaz RS-232, con la cual aumentó la velocidad de transmisión y la distancia máxima de transmisión.

a) Cierto.
b) Falso.

23. <Tipo 4>Los elementos pasivos de una red de datos únicamente retransmiten la información que reciben.

a) Cierto.
b) Falso.

24. <Tipo 4>Los elementos pasivos de una red de datos generan y/o modifican las señales.

a) Cierto.
b) Falso.

25. <Tipo 4>Los elementos activos de una red de datos generan y/o modifican las señales.

a) Cierto.
b) Falso.

26. <Tipo 4> Los elementos activos de una red de datos únicamente transmiten la información que reciben.

a) Cierto.
b) Falso.

27. <Tipo 4> “El cableado estructurado es la infraestructura de cable destinada a transportar a lo largo y ancho de una red LAN los datos que requieran compartir los usuarios.”

    La anterior sentencia es…

    a) Correcta.
    b) Incorrecta.

28. <Tipo 2> ¿Cuáles son los subsistemas del cableado estructurado?

a) Entrada al edificio.
b) Cuarto de equipos.
c) Switch.
d) Backbone - cableado vertical.
e) Armarios de telecomunicaciones.
f) ISP - Internet Service Provider.
g) Cableado horizontal.
h) Área de trabajo.
i) Rack.

29. <Tipo 1> Este subsistema consta de los cables, hardware de conexión, dispositivos de protección, hardware de transición y equipos para conectar e instalar los servicios externos con la red local.

a) Entrada al edificio.
b) Cuarto de equipos.
c) Backbone - cableado vertical.
d) Armarios de telecomunicaciones.
e) Cableado horizontal.
f) Área de trabajo.

30. <Tipo 1> Este subsistema conecta los cuartos de telecomunicaciones, armarios e instalaciones de entrada.

a) Entrada al edificio.
b) Cuarto de equipos.
c) Backbone - cableado vertical.
d) Armarios de telecomunicaciones.
e) Cableado horizontal.
f) Área de trabajo.

31. <Tipo 1> Este subsistema conecta la entrada del edificio con el backbone.

a) Entrada al edificio.
b) Cuarto de equipos.
c) Backbone - cableado vertical.
d) Armarios de telecomunicaciones.
e) Cableado horizontal.
f) Área de trabajo.

32. <Tipo 1> Este subsistema es la transición entre el cableado vertical y el cableado horizontal.

a) Entrada al edificio.
b) Cuarto de equipos.
c) Backbone - cableado vertical.
d) Armarios de telecomunicaciones.
e) Cableado horizontal.
f) Área de trabajo.

33. <Tipo 1> Este subsistema une la salida del armario de telecomunicaciones en cada piso con el área de trabajo.

a) Entrada al edificio.
b) Cuarto de equipos.
c) Backbone - cableado vertical.
d) Armarios de telecomunicaciones.
e) Cableado horizontal.
f) Área de trabajo.

34. <Tipo 1> En este subsistema es donde el ocupante interactúa con los dispositivos de telecomunicaciones.

a) Entrada al edificio.
b) Cuarto de equipos.
c) Backbone - cableado vertical.
d) Armarios de telecomunicaciones.
e) Cableado horizontal.
f) Área de trabajo.

35. <Tipo 1> En el cableado horizontal se definen las medidas que deben de tener cada conexión. ¿Cuáles son estas medidas?

a) Son 10 metros del backbone al switch, 10 metros de la roseta al equipo de trabajo y 100 metros del patch panel a la roseta.
b) Son 5 metros del backbone al switch, 5 metros de la roseta al equipo de trabajo y 80 metros del patch panel a la roseta.
c) Son 5 metros del backbone al switch, 5 metros de la roseta al equipo de trabajo y 90 metros del patch panel a la roseta.
d) Son 10 metros del backbone al switch, 10 metros de la roseta al equipo de trabajo y 90 metros del patch panel a la roseta.

36. <Tipo 4> *"El estándar del cableado de telecomunicaciones en edificios comerciales EIA/TIA 569 determina dos estándares (A y B) para el cableado de ethernet 10Base-T, determinando qué color corresponde a cada pin del conector RJ45."*

    La anterior sentencia es…

    a) Correcta.
    b) Incorrecta.

37. <Tipo 1> El estándar EIA/TIA 569 para ductos y espacios de telecomunicaciones en edificios comerciales que puedan soportar un ambiente de productos y proveedores múltiples define ciertos elementos para espacios y recorridos de telecomunicaciones ¿Cuáles de los siguientes NO lo define el estándar EIA/TIA 569?

a) Recorridos entre los edificios.
b) Tomas de Telecomunicaciones.
c) Recorridos horizontales.
d) Armado de un Patch cord
e) Armarios de comunicación.

38. <Tipo 1> Este estándar define el modo de agrupación de las fibras para los cables de fibra óptica.

a) EIA/TIA 606.
b) EIA/TIA 598A.
c) EIA/TIA 569.
d) EIA/TIA 568A.
e) EIA/TIA 568B.

39. <Tipo 3> Relacione cada dispositivo de interconexiones con su descripción.

a)	Repetidos.	(d) Es el equipo donde principalmente se agrupan los hubs, patch panels, switchs y routers.
b)	Patch cord.	(c) Su función es alojar equipo electrónico, informático y de comunicaciones.
c)	Gabinete.	(a) Es un dispositivo para regenerar una señal entre dos nodos de una red.
d)	Rack.	(g) Elemento metálico o plástico que brinda protección a los cables instalados.
e)	Patch panel.	(e) Elemento de red que protege los puertos de los equipos activos.
f)	Conector RJ45.	(f) Es una interfaz física usada comúnmente para conectar redes de cableado estructurado.
g)	Canaleta.	(b) Es el cable que va de la roseta a la estación de trabajo.

40. <Tipo 1> Es un protocolo de conmutación alternativa para datos de formato mixto, La tecnología de este protocolo se basa en la multiplicación y conmutación de celda o pequeños paquetes de longitud fija, combinando los beneficios de la conmutación de circuitos con los de la conmutación de paquetes.

a) ATM.
b) Frame Relay.
c) HDLC.
d) HNAS.
e) X.25.

41. <Tipo 2> ¿Cuáles son las principales características del protocolo ATM?

a) No hay control de flujo ni recuperación de errores.
b) Utiliza paquetes de longitud variable.
c) Opera en modo orientado a conexión.
d) Opera únicamente en redes LAN y en la capa física del modelo TCP/IP.
e) Utiliza paquetes de longitud fija.

42. <Tipo 1> Este protocolo está orientado a la tecnología de conmutación de paquetes ofrecido por las compañías telefónicas. Define el proceso para enviar datos sobre la red pública, constituye una tecnología de enlace de datos orientado a la conexión de alto rendimiento y eficacia.

a) ATM.
b) Frame Relay.
c) HDLC.
d) HNAS.
e) X.25.

43. <Tipo 2> Desde una vista de seguridad, en la capa física debemos preocuparnos por impedir que terceros no autorizados ingresen a las instalaciones. ¿qué medidas podemos implementar?

a) Utilización de sistemas biométricos.
b) Implementación de certificados SSL.
c) Monitoreo mediante cámaras y sistemas de CCTV.
d) Implementación de firmas digitales.
e) Utilización de guardias.
f) Utilización de Firewalls.

44. <Tipo 2> ¿Cuáles son las amenazas a las que puede estar expuesta la capa física de un sistema de red?

a) Incendios
b) Robo de identidad.
c) Usuarios no autorizados.
d) Phishing.
e) Terremotos.
f) Robo de datos.

45. <Tipo 1> Los terremotos son una amenaza que atenta en contra de la capa física ¿Cuáles de las siguientes medidas no va enfocada a mantener la seguridad de la parte física de los sistemas?

a) Colocar los equipos sobre plataformas de goma para que esta absorba las vibraciones.
b) No colocar elementos móviles sobre los equipos para evitar que caigan sobre ellos.
c) Utilizar fijaciones para elementos críticos.
d) No situar equipos en sitios altos para evitar caídas.
e) Señalizar las salidas de emergencia.

46. <Tipo 4> *“Las inundaciones son una de las causas de desastres en centros de cómputo. Además de las causas naturales de inundaciones, puede existir la posibilidad de una inundación provocada por la necesidad de apagar un incendio en un piso superior. Para evitar este inconveniente se pueden tomar las siguientes medidas:*

    - *Construir un techo impermeable para evitar el paso de agua desde un nivel superior*
    - *Acondicionar las puertas para contener el agua que bajase por las escaleras.”*

    Lo anterior descrito es…

a) Cierto.
b) Falso.

47. <Tipo 1> Las barreras antifuego tienen distintas clasificaciones. Las barreras que limita el aumento de temperatura pertenecen a la clasificación...

a) Clasificación A.
b) Clasificación F.
c) Clasificación T.
d) Clasificación L.
e) Clasificación M.

48. <Tipo 1> Las barreras antifuego tienen distintas clasificaciones. Las barreras que no permiten que las llamas pasen a través de ellas pertenecen a la clasificación...

a) Clasificación A.
b) Clasificación F.
c) Clasificación T.
d) Clasificación L.
e) Clasificación M.

49. <Tipo 1>Las barreras antifuego tienen distintas clasificaciones. Las barreras que barrera provee una detección efectiva de humo pertenecen a la clasificación

a) Clasificación A.
b) Clasificación F.
c) Clasificación T.
d) Clasificación L.
e) Clasificación M.

50. <Tipo 1> Las barreras de tipo _____ consisten en componentes elastoméricos pre-fabricados moldeados para ajustarse alrededor de cables estándar, tubos y conductos.

a) Mecánico.
b) Antifuego.
c) Contención.
d) No-mecánico.
e) Firestopping.

Preguntas Tema 4. Capa de Enlace

1. <Tipo 1> Esta capa del modelo OSI es la responsable del intercambio de datos entre un host cualquiera, y la red a la que está conectado. Su principal objetivo es la de proveer una comunicación segura entre dos nodos pertenecientes a una misma red o subred, para ello se encarga de la notificación de errores, del modo de transferencia de datos y el control del flujo en la transmisión de las tramas.

a) Física.
b) Enlace.
c) Red.
d) Transporte.
e) Sesión.
f) Presentación.
g) Aplicación.

2. <Tipo 4> ¿Cierto o falso? Hand-Shaking es el proceso de intercambio de información privada entre un cliente o usuario y un servidor, esto ocurre cuando el cliente quiere acceder a una página web.

a) Cierto.
b) Falso.

3. <Tipo 1> Escoja el orden correcto en el que se realiza un Hand-shaking.

   I. El browser comprueba la autenticidad y avisa si existe algún problema.
   II. Se realiza la conexión entre el servidor y el cliente.
   III. El cliente envía al servidor datos sobre el número de cliente, el cifrado, clave aleatoria y más datos que requieren los servidores.
   IV. El servidor reenvía los datos recibidos, así como su certificado digital.

a) I, II, III y IV.
b) III, IV, I y II.
c) IV, III, I y II.
d) II, III, IV y I.

4. <Tipo 4> *"La transmisión asincrónica se refiere al envío de un grupo de caracteres en un flujo continuo de bits."*

   La anterior sentencia es …

a) Correcta.
b) Incorrecta.

5. <Tipo 2> Escoge tres características de la transmisión asincrónica.

   a) Se le denomina de "start-stop".
   b) Los bloques que se envían tienen un tamaño que oscila entre 128 y 1,024 bytes.
   c) Es usada en velocidades de modulación de hasta 1,200 baudios.
   d) Su rendimiento de transmisión es de 99% cuando se transmiten 1,024 bytes y se usan no más de 10 bytes de cabecera y terminación.
   e) Los equipos terminales en este modo de transmisión se denominan como "Terminales en modo carácter".
   f) La señal de sincronismo puede ser generada por el equipo terminal de datos o por el modem.

6. <Tipo 4> *“La transmisión síncrona es aquella que se transmite o se recibe un carácter, bit por bit añadiendo bits de inicio, y bits que indican el término de un paquete de datos, para separar así los paquetes que se van enviando/recibiendo para sincronizar el receptor con el transmisor.”*

   La anterior sentencia es …

a) Correcta.
b) Incorrecta.

7. <Tipo 2> Escoge tres características de la transmisión síncrona.

a) Se le denomina de “start-stop”.
b) Los bloques que se envían tienen un tamaño que oscila entre 128 y 1,024 bytes.
c) Es usada en velocidades de modulación de hasta 1,200 baudios.
d) Su rendimiento de transmisión es de 99% cuando se transmiten 1,024 bytes y se usan no más de 10 bytes de cabecera y terminación.
e) Los equipos terminales en este modo de transmisión se denominan como “Terminales en modo carácter”.
f) La señal de sincronismo puede ser generada por el equipo terminal de datos o por el modem.

8. <Tipo 1> El Control Síncrono de Enlace De Datos (SDLC por sus siglas en inglés) es un protocolo utilizado para transferir información sincrónica, ¿Cuáles de las siguientes opciones es correcta?

a) Fue creado en 1973, fue el soporte para la comunicación entre cajeros automáticos, presente en componentes de comunicación de IBM.
b) Fue creado en 1963, fue el soporte para la comunicación de equipos militares, creado por el ejército de los EE. UU.
c) Fue creado en 1973, se utilizó para la intercomunicación de satélites, desarrollado por la NASA para su posterior uso de bancos.
d) Fue creado en 1963, se utilizó para la intercomunicación de corporativos, principalmente de IBM

9. <Tipo 1> High Level Data Control (HDLC) es …

a) Estándar.
b) Norma.
c) Protocolo.
d) Control.
e) Guía.

10. <Tipo 3> Selecciona la respuesta correcta para cada enunciado.

a) Estación Primaria.	(b) Las tramas que genera se denominan respuestas.
b) Estación Secundaria.	(a) Es el responsable de controlar el funcionamiento del enlace.
c) Estación Combinada.	(c) Esta estación puede generar tramas del tipo respuesta y orden.
	(b) Funciona bajo el control de cualquier otra estación.
	(a) Las tramas que genera se denominan órdenes.

11. <Tipo 1> _____ : se forma por una estación primaria y una o más secundarias. Permite transmisión full dúplex y half duplex.

a) Configuración no balanceada.
b) Configuración balanceada.
c) Modo de respuesta normal (NRM por sus siglas en inglés).
d) Modo balanceado asíncrono (ABM por sus siglas en inglés).
e) Modo de respuesta asíncrono (ARM por sus siglas en inglés).

12. <Tipo 1> _____: consiste en dos estaciones combinadas. Permite transmisión full dúplex y half duplex.

a) Configuración no balanceada.
b) Configuración balanceada.
c) Modo de respuesta normal (NRM por sus siglas en inglés).
d) Modo balanceado asíncrono (ABM por sus siglas en inglés).
e) Modo de respuesta asíncrono (ARM por sus siglas en inglés).

13. <Tipo 1> _____: permite que la estación primaria inicie la transferencia de datos hacia la secundaria, pero la secundaria solo puede transmitir datos con base en respuestas a las órdenes emitidas por la primaria.

a) Configuración no balanceada.
b) Configuración balanceada.
c) Modo de respuesta normal (NRM por sus siglas en inglés).
d) Modo balanceado asíncrono (ABM por sus siglas en inglés).
e) Modo de respuesta asíncrono (ARM por sus siglas en inglés).

14. <Tipo 1> _____: permite que cualquier estación combinada pueda iniciar la transmisión sin necesidad de pedir permiso por parte de la otra estación combinada.

a) Configuración no balanceada.
b) Configuración balanceada.
c) Modo de respuesta normal (NRM por sus siglas en inglés).
d) Modo balanceado asíncrono (ABM por sus siglas en inglés).
e) Modo de respuesta asíncrono (ARM por sus siglas en inglés).

15. <Tipo 1> _____: permite que la estación secundaria puede iniciar la transmisión sin tener permiso explícito de la primaria. La estación primaria sigue teniendo la responsabilidad del funcionamiento de la línea, incluyendo la iniciación, la recuperación de errores y la desconexión lógica.

a) Configuración no balanceada.
b) Configuración balanceada.
c) Modo de respuesta normal (NRM por sus siglas en inglés).
d) Modo balanceado asíncrono (ABM por sus siglas en inglés).
e) Modo de respuesta asíncrono (ARM por sus siglas en inglés).

16. <Tipo 2> HDLC implica tres fases, ¿Cuáles son?

a) Inicio.
b) Comprobación de certificado.
c) Aviso de problemas.
d) Transferencia de datos.
e) Desconexión.
f) Conexión.

17. <Tipo 5> Relacione la trama con sus características.

I) Frame-I
S) Trama-S
U) Trama-U

(I) En esta trama se incluye la información para el control ARQ de errores y de flujo.
(I) Transporta los datos del usuario.
(S) Proporciona el mecanismo de ARQ cuando no se usa la incorporación de las confirmaciones en las tramas de información.
(U) Proporciona funciones complementarias para controlar el enlace.

18. <Tipo 2> En la primera fase del funcionamiento de HDLC se solicita el inicio de la conexión mandando una orden para fijar el modo en que van a trabajar las estaciones. ¿Cuáles son los objetivos que tiene esta orden?

a) Verifica que la conexión se posible.
b) Avisa al otro extremo sobre la solicitud de la iniciación.
c) Define el cifrado que se va a utilizar.
d) Especifica cuál de los tres modos se está solicitando.
e) Comprueba la identidad de la otra estación y define en qué modo opera.
f) Indica si se van a utilizar números de secuencia de 3 o de 7 bits.

19. <Tipo 4> *"En la fase de desconexión de HDLC debe ser iniciada únicamente por la estación que pidió la conexión esto es para evitar errores en la transmisión, la desconexión puede darse tanto por iniciativa propia o tras la petición de capas superiores"*

La anterior sentencia es …

a) Cierta.
b) Falsa.

20. <Tipo 1> En el protocolo denominado _____ todas las estaciones intervienen en la circulación de un paquete especial de un paquete especial que indica que lo posee que puede disponer del medio de transmisión.

a) CSMA/CA.
b) CSMA.
c) CSMA/CD.
d) Token.
e) FDDI.

21. <Tipo 1> _____: se diseñó para cumplir los requerimientos de redes individuales de alta velocidad, y conexiones de alta velocidad entre redes individuales. Este estándar está basado en el cable de fibra óptica, tiene una velocidad de 100 Mbps y utiliza el método de acceso de paso de testigo.

a) CSMA/CA.
b) CSMA.
c) CSMA/CD.
d) Token.
e) FDDI.

22. <Tipo 1> En este tipo de redes donde se utiliza FDDI se usan para interconectar computadoras mainframe y grandes dispositivos de almacenamiento de datos, que requieren altas velocidades de transferencia de datos.

a) Redes Locales Especializadas.
b) Redes profesionales de alta velocidad.
c) Redes locales troncales.
d) Redes WAN.
e) Ninguna de las anteriores.

23. <Tipo 1> Con la llegada del procesamiento de gráficos e imágenes al lugar de trabajo aumentó la necesidad de redes de alta velocidad en las cuales se utiliza FDDI ¿A qué redes hacemos referencia?

a) Redes Locales Especializadas.
b) Redes profesionales de alta velocidad.
c) Redes locales troncales.
d) Redes LAN.
e) Ninguna de las anteriores.

24. <Tipo 1> Esta red tiene una alta capacidad y se usa para conectar redes de área local de muy baja capacidad. El aumento del uso de aplicaciones de procesamiento distribuido y computadoras personales ha llevado a la necesidad de una estrategia flexible para la conexión de redes locales.

a) Redes Locales Especializadas.
b) Redes profesionales de alta velocidad.
c) Redes locales troncales.
d) Redes LAN.
e) Ninguna de las anteriores.

25. <Tipo 2> ¿Cuáles son los componentes de FDDI?

a) Control de acceso al medio (MAC).
b) Acceso múltiple con escucha de señal portadora (CSMA).
c) Capa física (PHY).
d) Control de Enlace Lógico (LLC).
e) Capa dependiente del medio físico (PMD).
f) Control de Enlace Lógico con Control de Colisiones (CSMA/CD).
g) Capa de manejo de estación (SMT).

26. <Tipo 4> La principal función de la capa de enlace es: “iniciar, mantener y terminar una comunicación entre punto y punto a lo largo de la comunicación y detectar errores”

    La sentencia anterior es:

a) Cierto.
b) Falso.

27. <Tipo 1> ALOHA es un método de transmisión que hace posible enviar información a través del medio cuando el usuario lo desee sin importar si este está disponible u ocupado, ni tampoco la cantidad de información que envíe

    ¿Cuál es el principal problema que presenta este método?

a) Colisión de paquetes.
b) Tiempos de espera muy largos.
c) No ocurre ningún problema.
d) Saturación de la red.

28. <Tipo 1> El método ALOHA está divido en dos métodos principales. Indica cuales son estos métodos

a) ALOHA y slotted ALOHA.
b) slot ALOHA y slotted ALOHA.
c) ALOHA y P-ALOHA.
d) sinc ALOHA y asin ALOHA.

29. <Tipo 1> ¿Cuál fue la mejora que se implementó en el método slotted ALOHA?.

a) cada cierto intervalo de tiempo envía una señal para indicar que el medio está disponible.
b) fragmenta la información y la transmite por diferentes medios.
c) transmite la información de manera síncrona.
d) transmite la información de manera asíncrona.

30. <Tipo 4> La tecnología ethernet está basada en slotted ALOHA.

a) Cierto.
b) Falso.

31. <Tipo 1> El método de comunicación CSMA/CD se utiliza en la tecnología.

a) Ethernet.
b) Bluetooth.
c) wi-fi.
d) Infrarrojo.

32. <Tipo 1> El método de comunicación CSMA/CA se utiliza en la tecnología

a) Ethernet.
b) Bluetooth.
c) wi-fi.
d) Infrarrojo.

33. <Tipo 4> El método CSMA/CD verifica que el medio esté disponible antes de enviar información y en caso de colisión notifica a lo nodos que enviaron la información

a) Cierto.
b) Falso.

34. <Tipo 4> El método CSMA/CD verifica que el medio está disponible antes de enviar información y evita colisiones notificando a los nodos su intención de transmitir

a) Cierto.
b) Falso.

35. <Tipo 4> El método CSMA/CD verifica que el medio está disponible antes de enviar información y evita colisiones notificando a los nodos su intención de transmitir

a) Cierto.
b) Falso.

36. <Tipo 4> El método CSMA/CD verifica que el medio esté disponible antes de enviar información y en caso de colisión notifica a lo nodos que enviaron la información

a) Cierto.
b) Falso.

37. <Tipo 2> La capa de enlace está dividida en dos subcapas. indica cuales son estas capas

a) LLC.
b) MAC.
c) IP.
d) Internet.
e) Red.

38. <Tipo 2> la subcapa “logical link control” se encarga de:

a) La lógica de la comunicación.
b) El control de flujo de la comunicación.
c) La identificación del protocolo de comunicación utilizado en capa 3.
d) El cifrado de datos.
e) El descifrado de datos.

39. <Tipo 4> La subcapa “Media Access Control” no está definida en ningún estándar IEEE 802 ya que depende de la tecnología o el producto usado.

a) Cierto.
b) Falso.

40. <Tipo 5> Relaciona las columnas.

a) LLC.	(a) Es la subcapa superior de la capa 2, que se encarga de la comunicación como es el control de flujo y el identificador de protocolo de comunicación utilizado en capa 3.
b) MAC.	(b) Esta subcapa no está definida en ningún estándar de la IEEE, pero se encarga de cómo se utiliza y comparte el medio físico, además de identificar cada nodo de la red a la que se hace referencia.

41. <Tipo 1> ¿Cuál es la cantidad máxima de nodos que se permiten en una red Ethernet?

a) 1024.
b) 2048.
c) 512.
d) 10000.

42. <Tipo 1> ¿Cuál es la distancia máxima permitida entre nodos finales en una red de Ethernet con UTP?

a) 500 [m].
b) 2500 [m].
c) 3000 [m].
d) 5000 [m].

43. <Tipo 1> El estándar IEEE 802.11 hace referencia a tecnologías:

a) wi-fi.
b) wi-max.
c) Infrarrojo.
d) Ethernet.
e) WPAN.
f) Bluetooth.

44. <Tipo 1> El estándar IEEE 802.16 hace referencia a tecnologías:

a) wi-fi.
b) wi-max.
c) Infrarrojo.
d) Ethernet.
e) WPAN.
f) Bluetooth.

45. <Tipo 1> El estándar IEEE 802.3 hace referencia a tecnologías:

a) wi-fi.
b) wi-max.
c) Infrarrojo.
d) Ethernet.
e) WPAN.
f) Bluetooth.

46. <Tipo 1>El estándar IEEE 802.15 hace referencia a tecnologías:

a) wi-fi.
b) wi-max.
c) Infrarrojo.
d) Ethernet.
e) WPAN.
f) Bluetooth.

47. <Tipo 1> Este es un elemento de hardware que trabaja únicamente en capa 2.

a) Bridge.
b) Router.
c) Switch.
d) Hub.
e) Ninguna de las anteriores.

48. <Tipo 1> ¿Cuáles son los elementos de una tabla de direcciones correspondiente a un bridge?

a) Dirección MAC, puerto.
b) Interfaz de origen, interfaz de destino, dirección IP de origen, dirección IP de destino, máscara de subred, Gateway.
c) Interfaz de destino, IP de destino, máscara de subred, Gateway.
d) No utiliza ninguna tabla de direccionamiento.

49. <Tipo 4> Frame relay es una tecnología de redes WAN que trabaja por medio de Packet-Switching, utilizando circuitos lógicos virtuales para la conexión de usuarios finales.

a) Cierto.
b) Falso.

50. <Tipo 4> Cell Relay es una tecnología basada en celdas de tamaño fijo para la transmisión de información generando así una mayor velocidad de propagación.

a) Cierto.
b) Falso.

Preguntas Tema 5. Capa de Red

1. <Tipo 1> Esta capa del modelo OSI es la encargada de encontrar la mejor ruta para que los paquetes de datos lleguen a su destino. Para realizar este transporte se realizan los siguientes procesos:

    - Direccionamiento.
    - Encapsulamiento.
    - Enrutamiento.
    - Desencapsulamiento.

a) Física.
b) Enlace.
c) Red.
d) Transporte.
e) Sesión.
f) Presentación.
g) Aplicación.

2. <Tipo 2> ¿Cuáles son las principales actividades de la capa de red? (Seleccione las tres opciones correctas).

a) Buscar el mejor camino por paquete o por mensaje.
b) Preparar los paquetes para su transmisión.
c) Realizar las funciones de encaminamiento que permitan a múltiples dispositivos lograr enlaces de datos exitosos en una red.
d) Controlar el acceso a los medios físicos.
e) Realizan un direccionamiento lógico.
f) Establecer una sesión de comunicación temporal entre dos aplicaciones.

3. <Tipo 1> Este protocolo de capa de red tiene como objetivo entregar datagramas a través de la red y ofrecer la fragmentación y el reensamblado de datagramas para soportar los enlaces de datos de tamaños diferentes de las MTU.

a) ICMP.
b) IP.
c) ARP.
d) RARP.
e) IGMP.

4. <Tipo 4> "*El protocolo IPv4 utiliza 128 bits para representar una dirección IP, los cuales son divididos en 8 grupos de 4 dígitos en hexadecimal.*"

   La anterior sentencia es…

a) Correcta.
b) Incorrecta.

5. <Tipo 3> Relacione cada clase con sus características.

Clase A.	(A) El rango del 1er octeto va de 1 a 127, cuenta con un octeto para el ID de la red, tres octetos para el identificador de host y su máscara de red es 255.0.0.0.
Clase B.	(B) El rango del 1er octeto va de 128 a 191, cuenta con dos octetos para el ID de la red, dos octetos para el identificador de host y su máscara de red es 255.255.0.0.
Clase C.	(C) El rango del 1er octeto va de 192 a 223, cuenta con tres octetos para el ID de la red, un octeto para el identificador de host y su máscara de red es 255.255.255.0.

6. <Tipo 4> “Las subredes son las divisiones de una red en varias partes para su uso interno de una organización, pero con la capacidad de actuar como una sola red ante el mundo externo. Para implementar las subredes se hace uso de una máscara de red que identifique la división”

   La anterior sentencia es…

a) Correcta.
b) Incorrecta.

7. <Tipo 4> *“Una máscara de red se trata de una sucesión de unos que abarca la porción del identificador de red y adicionalmente la porción que será tomada del Identificador de host para utilizarse como Identificador de subred.”*

   La anterior sentencia es…

a) Correcta.
b) Incorrecta.

8. <Tipo 4> “*Se hace una suma lógica NAND entre la dirección IP y la máscara para determinar la subred a la que se hace referencia y la máquina dentro de esa subred a la que se dirige el paquete.”*

   La anterior sentencia es…

a) Correcta.
b) Incorrecta.

9. <Tipo 2> IPv6 es la versión del protocolo IP que está destinada a sustituir al estándar IPv4. ¿Cuáles son sus características? (Seleccione tres).

a) Mayor espacio de direcciones, de 32 bits a 128 bits.
b) Mantiene el mismo formato de cabecera que su antecesor IPv4.
c) Seguridad con el protocolo IPsec.
d) Posibilidad de paquetes con un payload de 1,500 bytes.
e) Capacidad de etiquetas de flujos.

10. <Tipo 1> ¿Cuál es el funcionamiento del Network Address Translation?

a) Transmitir la información de direccionamiento para el encaminamiento de paquetes.
b) Entregar mensajes IP.
c) Mapear de una dirección IP a una dirección física de un equipo que esté en una red de área local.
d) Permite a los nodos de una red IP obtener sus parámetros de configuración automáticamente.
e) Traduce direcciones IP “locales” dentro de una empresa en una dirección real para dirigirse al exterior.

11. <Tipo 1> ¿Cuál es el funcionamiento del Address Resolution Protocol?

a) Transmitir la información de direccionamiento para el encaminamiento de paquetes.
b) Entregar mensajes IP.
c) Mapea de una dirección IP a una dirección física de un equipo que esté en una red de área local.
d) Permite a los nodos de una red IP obtener sus parámetros de configuración automáticamente.
e) Traduce direcciones IP “locales” dentro de una empresa en una dirección real para dirigirse al exterior.

12. <Tipo 4> *"El ICMP es parte del Modelo TCP/IP. Los mensajes ICMP son usados "fuera de banda" exclusivamente para conocer la operación de la red. Los paquetes entregados ICMP son fiables, así que los hosts pueden contar un paquete recibido ICMP para cualquier problema de la red."*

    La anterior sentencia es…

a) Correcta.
b) Incorrecta.

13. <Tipo 1> Este protocolo se utiliza para intercambiar información acerca del estado de pertenencia entre routers IP que admiten la multidifusión y miembros de grupos de multidifusión.

a) IPv4.
b) IGP.
c) NAT.
d) ICMP.
e) IGMP.

14. <Tipo 4> *"Los protocolos EGP pueden ser divididos en dos categorías, una de ellas es Vector - distancia, el cual tienen en cuenta la cantidad de saltos al tomar la decisión del camino que debe atravesar un datagrama para llegar a destino, sin tener en cuenta las características del salto.*

    La anterior sentencia es...

a) Correcta.
b) Incorrecta.

15. <Tipo 4> *"Los protocolos IGP pueden ser divididos en dos categorías, una de ellas es Estado – Enlace, la cual tiene en cuenta diversos parámetros como el ancho de banda de los links que se atraviesan, para tomar la decisión del camino que debe seguir un datagrama.*

    La anterior sentencia es...

a) Correcta.
b) Incorrecta.

16. <Tipo 1> Este tipo de protocolo se utiliza para intercambiar información de ruteo entre diferentes SA. El único protocolo de este tipo utilizado hoy en día es BGP (Border Gateway Protocol).

a) EGP.
b) IGP.
c) Estado-Enlace.
d) Vector-Distancia.
e) IP.
f) NAT.

17. <Tipo 1> Este protocolo forma un vector que contiene todos los números de SA que ha atravesado dicho anuncio, y por ende indica el camino que toma el paquete en la red (Saltos de SA).

a) BGP.
b) IP.
c) RIP.
d) DHCP.
e) ICMP.
f) EGP.

18. <Tipo 1> Es un protocolo de encaminamiento interno usado por distintos routers para intercambiar información y así conocer por donde deberían enrutar un paquete para hacer que éste llegue a su destino.

a) BGP.
b) IP.
c) RIP.
d) DHCP.
e) ICMP.
f) EGP.

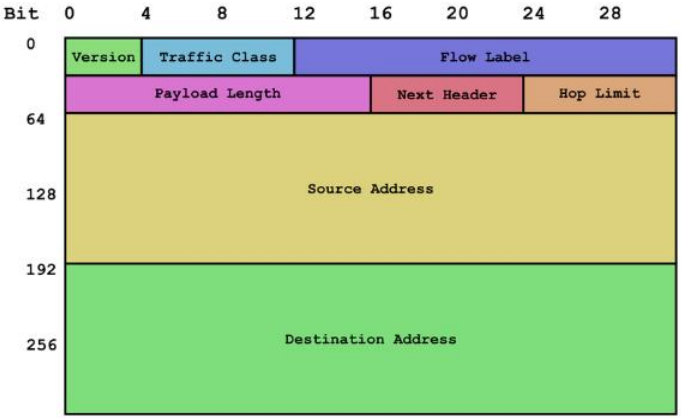
19. <Tipo 1> Es un protocolo de red de tipo cliente/servidor en el que generalmente un servidor posee una lista de direcciones IP dinámicas y las va asignando a los clientes conforme éstas van estando libres, sabiendo en todo momento quien ha estado en posesión de esa IP, cuánto tiempo la ha tenido, a quien se la ha asignado después.

a) BGP.
b) IP.
c) RIP.
d) DHCP.
e) ICMP.
f) EGP.

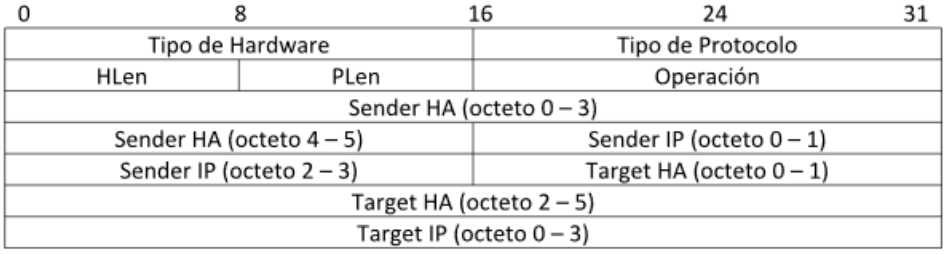
20. <Tipo 5> Relacione la cabecera con su protocolo.

a)

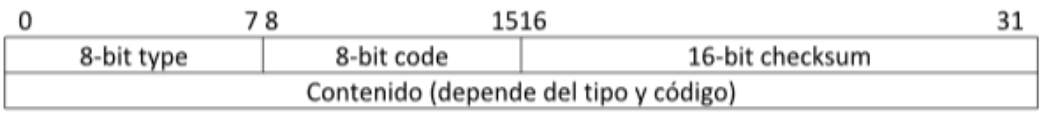
b)



c)



d)



(A) IP (B) NAT (C) ARP (D) ICMP

21. <Tipo 1> Se introdujo en 1993 para brindar flexibilidad al dividir rangos de direcciones IP para crear subredes, de manera que no sea necesario asignar bloques de direcciones en los límites de los octetos, sino solo utilizar el número de bits necesarios para el número de subredes que se requieran.

a) CIDR.
b) VLSM.
c) IP.
d) DHCP.
e) EGP.
f) IGP.

22. <Tipo 1> Se diseñó para maximizar la eficiencia del direccionamiento.

    Entre sus características se encuentran:

    - Se utilizan múltiples máscaras.
    - Las subredes que se crean no tienen el mismo número de equipos.
    - Se tiene una organización del espacio de direcciones más acorde con las necesidades reales.
    - El desaprovechamiento de direcciones IP es mínimo.

a) CIDR.
b) VLSM.
c) IP.
d) DHCP.
e) EGP.
f) IGP.

23. <Tipo 7> En una facultad se tienen la red 192.168.10.0/24 y se desea colocar tres salas de cómputo: una sala en el conjunto norte con 45 hosts, una sala en el conjunto sur con 64 hosts y una última en el posgrado con 30 hosts. Conteste las siguientes preguntas tomando en cuenta que la división de la red será por VLSM:

¿Cuál es la máscara de red en formato decimal, NetID, Rango de IP's asignables y broadcast de la red del…

...conjunto sur?

Mascara de red= 255.255.255.128

NetID= 192.168.10.0

Rango= 192.168.10.1 **-** 192.168.10.126

Broadcast = 192.168.10.127

...conjunto norte?

Mascara de red= 255.255.255.192

NetID= 192.168.10.128

Rango= 192.168.10.129 **-** 192.168.10.190

Broadcast = 192.168.10.191

...posgrado?

Mascara de red= 255.255.255.224

NetID= 192.168.11.192

Rango= 192.168.11.193 **-** 192.168.11.222

Broadcast = 192.168.11.223

24. <Tipo 7> En una empresa se tienen las siguientes áreas: Finanzas, Mercadotecnia, I.T., Recursos Humanos y Atención a clientes, se requiere dividir la red 192.10.5.0/24 en cada una de las áreas para tener una mejor administración y control. Dado el caso conteste las siguientes preguntas:

    ¿Cuál sería la máscara de subred en formato decimal?

    R= 255.255.255.224

    ¿Cuál es el NetID, Rango de IP's asignables y broadcast de la red de…

    … Área 1?

    NetID= 192.10.5.0

    Rango= 192.10.5.1 **-** 192.10.5.30

    Broadcast = 192.10.5.31

    … Área 2?

    NetID= 192.10.5.32

    Rango= 192.10.5.33 **-** 192.10.5.62

    Broadcast = 192.10.5.63

    … Área 3?

    NetID= 192.10.5.64

    Rango= 192.10.5.65 **-** 192.10.5.94

    Broadcast = 192.10.5.95

    … Área 3?

    NetID= 192.10.5.96

Rango= 192.10.5.97 **-** 192.10.5.126

Broadcast = 192.10.5.127

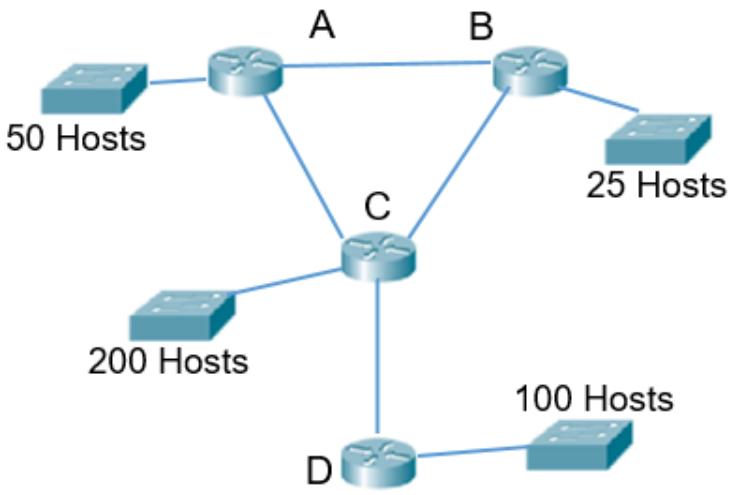
… Área 5?

NetID= 192.10.5.128

Rango= 192.10.5.129 **-** 192.10.5.158

Broadcast = 192.10.5.159

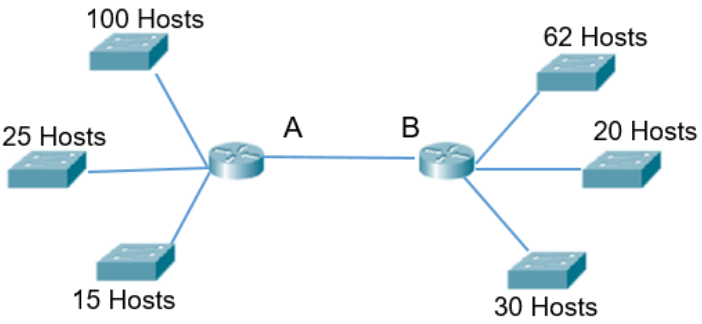
25. <Tipo 6> Dada la red 172.172.0.0/16 y el siguiente diagrama, conteste la siguiente pregunta con base en ruteo VLSM.



¿Cuál es la dirección de broadcast de la subred D?

R= 172.172.1.223

26. <Tipo 6> Dada la red 192.168.14.0/23 y el siguiente diagrama, conteste la siguiente pregunta con base en ruteo VLSM.



¿Cuál es la dirección de broadcast de la última subred que tiene hosts instalados?

R= 192.168.15.63

27. <Tipo 1> Cuando un servicio marca la ruta que todos los paquetes deben recorrer. Se está hablando de:

a) Un servicio orientado a conexión.
b) Un servicio no orientado a conexión.
c) Un enrutamiento estático.
d) Un enrutamiento dinámico.

28. <Tipo 1> Cuando un servicio no determina una ruta específica por la cual los paquetes deben llegar a su destino. Se está hablando de:

a) Un servicio orientado a conexión.
b) Un servicio no orientado a conexión.
c) Un enrutamiento estático.
d) Un enrutamiento dinámico.

29. <Tipo 1> Su principal problema se presenta cuando dos o más sistemas quieren establecer una conexión a un sistema común ya que se pueden presentar colisiones de información.

a) Servicio orientado a conexión.
b) Servicio no orientado a conexión.
c) Enrutamiento estático.
d) Enrutamiento dinámico.

30. <Tipo 1> Su principal problema se basa en la pérdida de información al no determinar una ruta específica entre sistemas.

a) Servicio orientado a conexión.
b) Servicio no orientado a conexión.
c) Enrutamiento estático.
d) Enrutamiento dinámico.

31. <Tipo 1> Es un dispositivo de hardware que opera en la Capa 3 del modelo OSI.

a) Router.
b) Bridge.
c) Switch.
d) HUB.

32. <Tipo 1> El router es un dispositivo de hardware que opera en la capa ___ del modelo OSI.

a) 3.
b) 5.
c) 1.
d) 2.

33. <Tipo 1> Este dispositivo se encarga de procesar la información de origen y destino de los datagramas para transferir los paquetes por la mejor ruta.

a) Router.
b) Switch.
c) Bridge.
d) HUB.

34. <Tipo 1> Un conmutador opera en la capa ___ del modelo OSI.

a) 1.
b) 2.
c) 3.
d) 5.

35. <Tipo 1> Cual es la principal diferencia entre un conmutador y un enrutador.

a) El conmutador opera basado en direcciones MAC y el router con IP.
b) Los protocolos con los cuales operan son diferentes.
c) No hay ninguna diferencia.

36. <Tipo 4> El router no es capaz de comunicar redes con protocolos diferentes, este siempre debe ser equipado con los dispositivos de hardware requeridos para soportar los protocolos con los cuales se trabajará.

a) Cierto.
b) Falso.

37. <Tipo 4> El router es capaz de comunicar redes con protocolos diferentes, debido a que este es capaz de traducir los datos de un protocolo a otro.

a) Cierto.
b) Falso.

38. <Tipo 4> Los routers se consideran dispositivos activos.

a) Cierto.
b) Falso.

39. <Tipo 4> Los routers se consideran dispositivos pasivos.

a) Cierto.
b) Falso.

40. <Tipo 4> La funcionalidad del router se puede clasificar de la siguiente manera.

- Permitir la unión de redes heterogéneas (diferentes).
- Asegurar que las redes sean capaces de manejar el tráfico de carga.
- Escoger la mejor ruta de comunicación a través de la red.

a) Cierto.
b) Falso.

41. <Tipo 4>Cómo se realiza el direccionamiento dentro de la capa de enlace de datos.

a) Con el mapeo realizado en la capa de red y utilizando esquemas de resolución de direcciones.
b) Mediante la especificación de los saltos que deben dar los paquetes.
c) Únicamente especificando la dirección de destino de los paquetes.

42. <Tipo 4> En qué consiste el método Source Quench.

a) El router monitorea el ancho de banda y cuando supera el promedio de uso, este envía un paquete de saturación para que los dispositivos conectados disminuyan o paren su transmisión.
b) El administrador de red monitorea el uso de ancho de banda, cuando este supera el promedio detiene el flujo de datos del sistema que más ancho de banda consume.
c) El router monitorea el ancho de banda, cuando supera el promedio de uso, ente detiene el flujo de datos del sistema que más ancho de banda consume.

43. <Tipo 2> Un router trabaja con tres elementos principalmente. Indica cuales son.

a) Interfaz de red.
b) Tabla de ruteo.
c) Algoritmo de ruteo.
d) Dirección IP de origen.
e) Dirección IP de destino.
f) Dirección MAC.

44. <Tipo 4> La interfaz de red es aquella que se forma a partir de un algoritmo de ruteo.

a) Cierto.
b) Falso.

45. <Tipo 4> La interfaz de red se encarga de conectar el router a una o más redes que utilicen protocolo de capa tres.

a) Cierto.
b) Falso.

46. <Tipo 4> ¿La tabla de ruteo es aquella que se forma a partir de un algoritmo de ruteo?

a) Cierto.
b) Falso.

47. <Tipo 4> La tabla de ruteo se encarga de conectar el router a una o más redes que utilicen protocolos de capa tres.

a) Cierto.
b) Falso.

48. <Tipo4> ¿El protocolo IP es un protocolo de capa tres?

a) Cierto.
b) Falso.

49. <Tipo 1> El protocolo IP es un protocolo de capa ___.

a) 3.
b) 2.
c) 5.
d) 4.

50. <Tipo 4> El Internet Protocol (IP) está constituido por:

- Un espacio de direcciones globales independientes de las capas 1 y 2.
- Trabaja bajo el sistema Connectionless.
- Soporta fragmentación automática.
- IP es un protocolo capa 3, corre en cada host y router en internet.

a) Cierto.
b) Falso.

51. <Tipo 4> La fragmentación se basa en la separación del mensaje en paquetes menores o iguales al MTU de la red local en la que se está trabajando, tomando en cuenta el tamaño que tiene el header de IP (generalmente 20 Bytes).

a) Cierto.
b) Falso.

52. <Tipo 1> La cabecera IP tiene una longitud de ___.

a) 20 bytes.
b) 30 bytes.
c) 40 bytes.
d) 50 bytes.

53. <Tipo 1> ¿La dirección 192.158.2.48/28 es asignable en CIDR?
a) Si.
b) No, porque es la dirección de Broadcast de la subred.
c) No, porque es el Identificador de red (NetID).
d) No, porque es una dirección reservada.

54. <Tipo 1> ¿La dirección 191.168.7.23/29 es asignable en CIDR?
a) Si.
b) No, porque es la dirección de Broadcast de la subred.
c) No, porque es el Identificador de red (NetID).
d) No, porque es una dirección reservada.

55. <Tipo 1> ¿La dirección 127.72.30.6/26 es asignable en CIDR?
a) Si.
b) No, porque es la dirección de Broadcast de la subred.
c) No, porque es el Identificador de red (NetID).
d) No, porque es una dirección reservada.

56. <Tipo 1> ¿La dirección 193.168.30.33/30 es asignable en CIDR?

a) Si.
b) No, porque es la dirección de Broadcast de la subred.
c) No, porque es el Identificador de red (NetID).
d) No, porque es una dirección reservada.

57. <Tipo 1> ¿La dirección 192.158.2.62/28 es asignable en CIDR?

a) Si.
b) No, porque es la dirección de Broadcast de la subred.
c) No, porque es el Identificador de red (NetID).
d) No, porque es una dirección reservada.

58. <Tipo 1> ¿La dirección 127.127.0./28 es asignable en CIDR?

a) Si.
b) No, porque es la dirección de Broadcast de la subred.
c) No, porque es el Identificador de red (NetID).
d) No, porque es una dirección reservada.

59. <Tipo 1> ¿La dirección 200.168.7.24/29 es asignable en CIDR?

a) Si.
b) No, porque es la dirección de Broadcast de la subred.
c) No, porque es el Identificador de red (NetID).
d) No, porque es una dirección reservada.

60. <Tipo 1> ¿La dirección 195.100.10.63/27 es asignable en CIDR?

a) Si.
b) No, porque es la dirección de Broadcast de la subred.
c) No, porque es el Identificador de red (NetID).
d) No, porque es una dirección reservada.

61. <Tipo 1> ¿La dirección 200.200.10.10/31 es asignable en CIDR?

a) Si.
b) No, porque es la dirección de Broadcast de la subred.
c) No, porque es el Identificador de red (NetID).
d) No, porque es una dirección reservada.

62. <Tipo 1> ¿La dirección 192.168.10.25/29 es asignable en CIDR?

a) Si.
b) No, porque es la dirección de Broadcast de la subred.
c) No, porque es el Identificador de red (NetID).
d) No, porque es una dirección reservada.

63. <Tipo 1> ¿La dirección 192.168.0.155/26 es asignable en CIDR?

a) Si.
b) No, porque es la dirección de Broadcast de la subred.
c) No, porque es el Identificador de red (NetID).
d) No, porque es una dirección reservada.

Preguntas Tema 6: Capa de Transporte

1. <Tipo 1> Esta capa del modelo OSI es la encargada de llevar los datos a su destino, asegurando que lleguen en la secuencia correcta, coordina múltiples aplicaciones para que interactúen en la red simultáneamente de tal forma que los datos enviados por una aplicación sean recibidos por la aplicación correspondiente.

a) Física.
b) Enlace.
c) Red.
d) Transporte.
e) Sesión.
f) Presentación.
g) Aplicación.

2. <Tipo 2> ¿Cuáles de las siguientes opciones son servicios que brinda la capa de transporte?

a) Realizar el direccionamiento lógico.
b) Provee comunicación lógica entre aplicaciones corriendo en diferentes máquinas.
c) Seguimiento de la comunicación individual entre aplicaciones en los hosts origen y destino.
d) Buscar la mejor ruta por paquete o por mensaje.
e) Prepara los paquetes para su transmisión.
f) Valida que los protocolos de esta capa solo corran en los sistemas finales.

3. <Tipo 2> ¿Cuáles son los protocolos que trabajan en la capa de transporte?

a) IP.
b) TCP.
c) ARP.
d) IGMP.
e) UDP.
f) NAT.
g) IGP.

4. <Tipo 4> *"UDP: es un servicio sin conexión, no se establece una sesión entre los hosts, pero garantiza y confirma la entrega de datos secuenciado."*

   La anterior sentencia es…

a) Correcta.
b) Incorrecta.

5. <Tipo 4> *"TCP: es un servicio orientado a la conexión, se establece una sesión entre los hosts, garantiza la entrega de los bloques de datos mediante el uso de confirmaciones y la entrega secuenciada de datos."*

   La anterior sentencia es…

a) Correcta.
b) Incorrecta.

6. <Tipo 2> ¿Cuáles son las responsabilidades que cumple la capa de transporte?

a) Fragmentación de paquetes.
b) Cálculo de la mejor ruta para enviar los paquetes.
c) Secuenciamiento.
d) Proveer una comunicación segura entre dos nodos.
e) Reensamblado de paquetes.
f) Notificación de errores.

7. <Tipo 4> *“EL control de flujo trata de que el emisor no sature el buffer del receptor, esto puede ser debido a que la aplicación es lenta para leer el buffer, por ello se hace uso del servicio de acoplado de velocidades que consiste en ajustar la velocidad del receptor con la tasa de consumo de la aplicación.”*

   La anterior sentencia es…

a) Correcta.
b) Incorrecta.

8. <Tipo 1> ¿Que es ARQ?

a) Protocolos utilizados para el control de errores en la transmisión de datos garantizando la integridad de estos.
b) Protocolo que se encarga del encapsulamiento de las tramas que se van a enviar y recibir.
c) Protocolos que se encargan del control del secuenciamiento de los paquetes.
d) Protocolo que realiza el acoplado de velocidades en una transmisión.

9. <Tipo 6> Dado los datos 11100101 y un G(x) igual a 10101. ¿Cuál es el CRC?

   R = 0011

10. <Tipo 6> Dado los datos 1100101001 y un G(x) igual a 11001. ¿Cuál es el CRC?

    R = 0111

11. <Tipo 6> Dado los datos 1110110101 y un G(x) igual a 10011. ¿Cuál es el CRC?

    R = 1100

12. <Tipo 4> *"Stop-wait es un protocolo el cual se asegura de que la información no se pierda, además las tramas o paquetes se reciban en el orden correcto. El emisor envía ráfagas de paquetes y espera una señal de ACK por parte del receptor, si recibe la señal de ACK manda la siguiente ráfaga."*

    La anterior sentencia es…

a) Correcta.
b) Incorrecta.

13. <Tipo 6> Una LAN que utiliza cobre en su canal de propagación opera a una velocidad de 125 Mb/s y tienen una longitud de 8.5 Kilómetros en la cual se transmiten tramas de 5000 bits ¿Cuál es el nivel de su utilización?

    R = 32%

14. <Tipo 6> Una LAN que utiliza cobre en su canal de propagación opera a una velocidad de 75 Mb/s y tienen una longitud de 9.5 Kilómetros en la cual se transmiten tramas de 5000 bits ¿Cuál es el nivel de su utilización?

    R = 41.24%

15. <Tipo 6> Una LAN que utiliza cobre en su canal de propagación opera a una velocidad de 100 Mb/s y tienen una longitud de 10 Kilómetros en la cual se transmiten tramas de 100000 bits ¿Cuál es el nivel de su utilización?

    R = 90.91%

16. <Tipo 4> *“El mecanismo de ventana deslizante es un mecanismo de control de flujo de datos que existen entre un emisor y un receptor en el que el control del flujo de datos se lleva cabo mediante el intercambio de caracteres o tramas de control”*

    La anterior sentencia es…

a) Correcta.
b) Incorrecta.

17. <Tipo 1> ¿Cómo es la transmisión en ventana deslizante?

a) El envío se realiza en ráfagas de paquetes, al final del envío se espera una respuesta del receptor para proceder a enviar la siguiente ráfaga.
b) El envío de realiza en ráfagas de paquetes, durante el envío se puede recibir una señal de retransmisión, si no se recibe tal señal se procede a enviar la siguiente ráfaga.
c) El envió se realiza en tramas individuales, después de que el emisor manda una trama espera una respuesta del receptor para proceder a enviar la siguiente trama.
d) El envió se realiza en tramas individuales, y cada que el emisor manda una trama acciona un temporizador antes de proceder a enviar la siguiente trama.

18. <Tipo 1> ¿Qué es buffer en ventana deslizante?

a) Es donde el emisor guarda todos los paquetes enviados y no validados. Y el receptor coloca los paquetes recibidos correctamente. Su tamaño es igual o superior al de la ventana y se borran los paquetes hasta que reciba un ACK.
b) Es donde el emisor guarda todos los paquetes enviados y el receptor los recibidos. Su tamaño es igual o superior al de la ventana y se borran los paquetes hasta que termina el tiempo del temporizador.
c) Es donde el receptor guarda todos los paquetes recibidos. Su tamaño es igual o superior al de la ventana y se borran los paquetes hasta que el receptor los procesa.
d) Es donde el receptor guarda todos los paquetes recibidos y no validados. Su tamaño es igual o superior al de la ventana y se borran los paquetes hasta que el receptor los valida.
e) Es donde el emisor guarda todos los paquetes enviados. Su tamaño es igual o superior al de la ventana y se borran los paquetes hasta que el receptor los procesa.
f) Es donde el emisor guarda todos los paquetes enviados y no validados. Su tamaño es igual o superior al de la ventana y se borran los paquetes hasta que el receptor los valida.

19. <Tipo 4> *“Un temporizador es asignado a cada uno de los paquetes transmitidos. El temporizador limita el tiempo de espera para recibir la validación de cada paquete. En caso de finalizar el tiempo sin éxito, se reenviará el paquete.”*

    La anterior sentencia es…

a) Correcta
b) Incorrecta

20. <Tipo 1> En esta estrategia de retransmisión el receptor rechaza todos los paquetes recibidos a partir de detectar uno con un error y envía una señal NACK n.

a) Retransmisión Discrecional.
b) Retransmisión No Discrecional.
c) Retransmisión Selectiva.
d) Retransmisión No Selectiva.

21. <Tipo 1> En esta estrategia de retransmisión el receptor sólo descarta el paquete erróneo y acepta los posteriores almacenándolos en el buffer de recepción y envía una señal NACKn.

a) Retransmisión Discrecional.
b) Retransmisión No Discrecional.
c) Retransmisión Selectiva.
d) Retransmisión No Selectiva.

22. <Tipo 6> ¿Cuál es el nivel de utilización en ventana deslizante con los siguientes datos?

Longitud de la trama: 5000 bits.

Velocidad de transmisión:400 KBps.

Retardo de propagación: 250 mseg.

Capacidad de buffer: 321tramas.

R = 100%

23. <Tipo 6> ¿Cuál es el nivel de utilización en ventana deslizante con los siguientes datos?

Longitud de la trama: 4000 bits.

Velocidad de transmisión:600 KBps.

Retardo de propagación: 250 mseg.

Capacidad de buffer: 400tramas.

R =66.56 %

24. <Tipo 2> En la capa de Transporte se puede hablar de dos tipos de servicio

Indica cuales son:

a) Orientado a conexión.
b) No orientado a conexión.
c) Transmisión Selectiva.
d) Transmisión no Selectiva.

25. <Tipo 1> En la capa de Transporte también se habla de los servicios Orientados a conexión y no orientados a conexión. Menciona cual es la diferencia de estos servicios con respecto a la capa de Red

a) No hay diferencia.
b) En la capa de red se encuentran controlados por los elementos de la red por ejemplo routers, mientras que en la de transporte se manejan entre elementos finales.
c) Estos servicios no se encuentran en la capa de RED.
d) Estos servicios no se encuentran en la capa de TRANSPORTE.
e) En la capa de transporte se encuentran controlados por los elementos de la red por ejemplo routers, mientras que en la de transporte se manejan entre elementos finales.

26. <Tipo 3> Relacione la información con el concepto correspondiente.

1) Es un mecanismo que permite convertir un paquete IP en varios bloques de datos _____

2) A todos los procesos de software que requieran acceder a la red se le asigna un número de puerto exclusivo en ese host. Este número de puerto se utiliza en el encabezado de la capa de transporte para indicar que aplicación se asocia en cada parte _____

3) Los protocolos en la capa de transporte describen cómo se utiliza la información del encabezado de la capa para convertir las partes de los datos en un solo bloque de datos _____

a) Fragmentación (1)

b) Secuenciamiento (2)

c) Reensamble (3)

27. <Tipo 1> Debido a que los elementos de red pueden enviar o recibir información a diferentes velocidades de transmisión y la diferente velocidad de procesamiento de estos, se utiliza este método para unir la información como fue enviada

a) Secuenciamiento.
b) Reensamblaje de paquetes.
c) Fragmentación.
d) Cifrado.
e) Descifrado.

28. <Tipo 1> "El emisor, después de enviar una sola trama, no envía las demás hasta que reciba una señal ACK; el receptor, cuando recibe una trama válida (sin errores), envía la señal ACK."

    Indica a qué método hace referencia el enunciado anterior

a) Parada y espera.
b) Ventana Deslizante.
c) Orientado a Conexión.
d) No Orientado a Conexión.

29. <Tipo 1> Es un mecanismo dirigido al control de flujo de datos que existe entre un emisor y un receptor pertenecientes a una red informática. Este mecanismo es un dispositivo de control de flujo de tipo software, es decir, el control del flujo se lleva a cabo mediante el intercambio específico de caracteres o tramas

    Indica a qué método hace referencia el enunciado anterior.

a) Parada y espera.
b) Ventana Deslizante.
c) Orientado a Conexión.
d) No Orientado a Conexión.

30. <Tipo 4> La finalidad del protocolo TCP es:

- Permitir una conexión confiable y transparente entre los puntos terminales de la red.
- Realizar una detección de error de extremo a extremo, así como recuperación y control de flujo de datos.
- Segmentación y reensamblaje de datos de usuarios y protocolos de capas superiores.

La anterior sentencia es:

a) Correcta.
b) Incorrecta.

31. <Tipo 4> El protocolo TCP está formado de la siguiente forma:

- Source Port y Destination Port: identifican la aplicación en cada extremo de la conexión.
- Sequence Number: identifica la posición en la cadena de bytes de este campo de datos.
- ACK number: es la posición de byte más alto que la fuente ha recibido.
- HLeng: es el tamaño del Header dentro de esta unidad de datos.
- Code Bits: es el campo utilizado para diferentes funciones.
- Window: especifica el número de bytes que está preparado a recibir el transmisor.
- Checksum: es utilizado para detección de error en transmisión.
- Urgent Point: indica que se está transmitiendo datos que deben ser suministrados tan rápidos como sea posible.

a) Cierto.
b) Falso.

32. <Tipo 3> Relaciona el concepto con la función que tiene dentro de la cabecera TCP

a) Puerto origen.
b) Puerto destino.
c) Numero de Secuencia.
d) Numero de acuse de Recibo.
e) Hlen.
f) Reservado.
g) Banderas.
h) Ventana.
i) Checksum.
j) Puerto de urgencia.
k) Opciones.

(a) Identifica el número de puerto de un programa de aplicación de origen.
(b) Identifica el número de puerto de un programa de aplicación de destino.
(c) Especifica el número de secuencia del primer byte de datos de este segmento.
(d) Identifica la posición del byte más alto recibido.
(e) especifica el tamaño de la cabecera en palabras de 32 bits.
(f) Espacio reservado para uso futuro.
(g) Indican el estado de la conexión.
(h) Especifica la cantidad de datos que el destino está dispuesto a aceptar.
(i) Verifica la integridad de la cabecera y los datos de segmento.
(j) Indica datos que se deben entregar lo más rápidamente posible.
(k) Poder añadir características no cubiertas por la cabecera fija.

33. <Tipo 3> Relaciona el concepto con la funcion que tiene dentro de la cabecera UDP

a) Puerto Origen.
b) Puerto Destino.
c) Longitud de mensaje.
d) Checksum.

(a) Dirección del puerto de protocolo que envía la información.

(b) Dirección del puerto de protocolo que recibe la información.

(c) Longitud en octetos del datagrama UDP.

(d) Proporciona una comprobación en el datagrama UDP utilizando el mismo algoritmo que IP.

34. <Tipo 1> Identifican la aplicación en cada extremo de la conexión.

Es una función de la cabecera TCP. Indique a qué elemento corresponde

a) Punto de Origen.
b) Número de secuencia.
c) ACK number.
d) HLeng.
e) CodeBits.
f) Ventana.
g) Suma de Verificación.
h) Punto de Urgencia.

35. <Tipo 1> Identifica la posición en la cadena de bytes de este campo de datos.

a) Source Point.
b) Número de secuencia.
c) ACK number.
d) HLeng.
e) CodeBits.
f) Ventana.
g) Suma de Verificación.
h) Punto de urgencia.

36. <Tipo 1> Es la posición de byte más alto que la fuente ha recibido.

a) Source Point.
b) Número de secuencia.
c) ACK number.
d) HLeng.
e) CodeBits.
f) Ventana.
g) Suma de Verificación.
h) Punto de urgencia.

37. <Tipo 1> Es el tamaño del Header dentro de esta unidad de datos.

a) Source Point.
b) Número de secuencia.
c) ACK number.
d) HLeng.
e) CodeBits.
f) Ventana.
g) Suma de verificación.
h) Punto de urgencia.

38. <Tipo 1> Cubre características no cubiertas por la cabecera fija.

a) Source Point.
b) Número de secuencia.
c) ACK number.
d) HLeng.
e) CodeBits.
f) Ventana.
g) Suma de verificación.
h) Punto de urgencia.

39. <Tipo 1> Especifica el número de bytes que está preparado a recibir el transmisor.

a) Source Point.
b) Número de secuencia
c) ACK number.
d) HLeng.
e) CodeBits.
f) Ventana.
g) Suma de verificación.
h) Punto de urgencia.

40. <Tipo 1> es utilizado para detección de error en transmisión.

a) Source Point.
b) Número de secuencia.
c) ACK number.
d) HLeng.
e) CodeBits.
f) ventana.
g) Suma de verificacion.
h) Punto de urgencia.

41. <Tipo 1> Indica que se está transmitiendo datos que deben ser suministrados tan rápidos como sea posible.

a) Source Point.
b) Número de secuencia.
c) ACK number.
d) HLeng.
e) CodeBits.
f) Ventana.
g) Suma de verificación.
h) Punto de urgencia.

42. <Tipo 3> "*Las aplicaciones que utilizan UDP son:*

- *Sistema de nombres de dominios (DNS).*
- *Streaming de Video.*
- *Voz sobre IP (VoIP)".*

La anterior sentencia es:

a) Correcta.
b) Incorrecta.

43. <Tipo 3> El protocolo TCP tiene la siguiente finalidad.

- Envío de mensajes en espera de ack de confirmación.
- Sin control de flujo, los mensajes pueden llegar más rápido de lo que pueden ser procesados.
- Este protocolo utiliza el mismo esquema de numeración de puntos que usa TCP para los protocolos de capas superiores.

La sentencia anterior es:

a) Correcta.
b) Incorrecta.

44. <Tipo 4> El protocolo UDP está formado de la siguiente forma:

- Source Port y Destination Port: identifican la aplicación en cada extremo de la conexión.
- Sequence Number: identifica la posición en la cadena de bytes de este campo de datos.
- ACK number: es la posición de byte más alto que la fuente ha recibido.
- HLeng: es el tamaño del Header dentro de esta unidad de datos.
- Code Bits: es el campo utilizado para diferentes funciones.
- Window: especifica el número de bytes que está preparado a recibir el transmisor.
- Checksum: es utilizado para detección de error en transmisión.
- Urgent Point: indica que se está transmitiendo datos que deben ser suministrados tan rápidos como sea posible.

a) Cierto.
b) Falso.

45. <Tipo 4> El protocolo UDP está formado de la siguiente forma:

    - Source Port y Destination Port: identifican la aplicación en cada extremo de la conexión.
    - HLeng: es el tamaño del Header dentro de esta unidad de datos.
    - Checksum: es utilizado para detección de error en transmisión.

a) Cierto.
b) Falso.

46. <Tipo 1>_____ es un método para evitar que alguien pueda tener acceso a información que se desea preservar. Este método consiste en alterar un mensaje antes de transmitirlo, generalmente mediante la utilización de una clave, de modo que su contenido no sea legible para los que no posean dicha clave.

    Inserte la opción correcta.

a) El cifrado.
b) La encriptación.
c) La codificación.
d) La fragmentación.

47. <Tipo 1> Con este método se evita que el emisor sature el buffer del receptor.

a) Control de Flujo.
b) Stop and Wait.
c) Sliding Window.
d) Orientado a Conexión.
e) No Orientado a Conexión.

48. <Tipo 1> Los puertos _____ están reservados para el sistema operativo y usados por protocolos como son HTTP, POP3/SMTP. Telnet y FTP, su numeración va del 0 al 1023.

a) Bien conocidos.
b) Registrados.
c) Dinámicos.
d) Físicos.
e) Lógicos.

49. <Tipo 1> Los puertos _____ están comprendidos entre 1024 y 49151, pueden ser usados por cualquier aplicación y existe una lista publicada en la página web de la IANA donde se puede consultar que aplicación usa cada puerto.

a) Bien conocidos.
b) Registrados.
c) Dinámicos.
d) Físicos.
e) Lógicos.

50. <Tipo 1> Los puertos _____ están comprendidos entre 49152 y 65535, normalmente se asigna a las aplicaciones de clientes al iniciarse la conexión. Son usados en conexiones Peer to Peer.

a) Bien conocidos.
b) Registrados.
c) Dinámicos.
d) Físicos.
e) Lógicos.

51. <Tipo 3> Ingrese a qué puerto pertenece cada protocolo.

1) IMAP _____(143).
2) SSH _____(22).
3) SMTP _____(25).
4) Telnet _____(23).
5) HTTP _____(80).
6) HTTPS _____(443).
7) POP3 _____(110).
8) Proxy Web _____(8080).
9) FTP _____(21).
10) DNS _____(53).

Preguntas Tema 7: Capa de Sesión

1. <Tipo 1> Esta capa del modelo OSI es la encargada de iniciar, mantener y terminar la comunicación entre origen y destino, sin importar por cuales elementos pase la información o como se realiza el enrutamiento.

a) Física.
b) Enlace.
c) Red.
d) Transporte.
e) Sesión.
f) Presentación.
g) Aplicación.

2. <Tipo 1> *"En la capa de sesión, se le conoce como _____ a derechos que permiten invocar distintos servicios y que se asignan dinámicamente entre los interlocutores. El servicio asociado a un _____ sólo puede ser invocado por su poseedor."*

   ¿Qué palabra es la que falta?

a) Sincronización.
b) Handshake.
c) Testigo.
d) Unidades de diálogo.
e) Privilegios.

3. <Tipo 2> Existen distintos tipos de Token ¿Cuáles de los siguientes **NO** es un tipo de token?

a) De datos.
b) De liberación de Conexión.
c) De sincronización menor.
d) De resincronización.
e) De sincronización mayor y actividad.
f) De unidad de diálogo.

4. <Tipo 1> Estos elementos de la sincronización en la capa de sesión son utilizados para que ciertas actividades, definidas por los participantes de la sincronización, se hagan completamente o no se hagan, delimitan las unidades de diálogo y son siempre confirmados.

a) Tokens.
b) Puntos de sincronización mayores.
c) Puntos de sincronización menores.
d) Señales de sincronización.
e) Señales de resincronización.
f) Unidades de diálogo.

5. <Tipo 1> Estos elementos de la sincronización en la capa de sesión se encargan de sincronizar tareas menos críticas. Se insertan dentro de las unidades de diálogo y pueden ser no confirmados.

a) Tokens.
b) Puntos de sincronización mayores.
c) Puntos de sincronización menores.
d) Señales de sincronización.
e) Señales de resincronización.
f) Unidades de diálogo.

6. <Tipo 1> Las unidades delimitadas por los puntos de sincronización mayores se llaman _____, y generalmente representan partes de trabajo lógicamente significativas.

a) Tokens.
b) Puntos de sincronización mayores.
c) Puntos de sincronización menores.
d) Señales de sincronización.
e) Señales de resincronización.
f) Unidades de diálogo.

7. <Tipo 2> ¿Cuáles son las fases que sigue la capa de sesión en el intercambio de datos?

a) Establecimiento.
b) Sincronización.
c) Utilización.
d) Administración.
e) Control.
f) Liberación.

8. <Tipo 1> En esta fase un usuario de sesión invoca la primitiva S-CONNECT.request con el objeto de establecer una sesión, el proveedor de sesión ejecuta un T-CONNECT.request para establecer una conexión de transporte.

a) Establecimiento.
b) Sincronización.
c) Utilización.
d) Administración.
e) Control.
f) Liberación.

9. <Tipo 1> Durante esta fase se realiza el intercambio de datos entre los participantes de la sesión activa.

a) Establecimiento.
b) Sincronización.
c) Utilización.
d) Administración.
e) Control.
f) Liberación.

10. <Tipo 4> *"Para realizar la liberación del medio en la capa de sesión se utiliza la primitiva T-DISCONNECT.request, que produce una liberación abrupta y puede traer como resultado la pérdida de los datos en tráfico que haya en el momento de la liberación."*

    La anterior sentencia es …

a) Verdadera.
b) Falsa.

11. <Tipo 4> *"Para realizar la liberación del medio en la capa de sesión se utiliza la primitiva S-RELEASE.request que resulta en una liberación ordenada en la cual los datos no se llegan a perder."*

    La anterior sentencia es …

c) Verdadera.
d) Falsa.

12. <Tipo 1> La administración de diálogo es un servicio que ofrece la capa de sesión. ¿En qué consiste este servicio?

a) Consiste en un mecanismo de notificación de errores inesperados.
b) Consiste en permitir que el usuario divida el flujo de mensajes en unidades de lógicas.
c) Consiste en llevar a las entidades de sesión de vuelta a un estado conocido, en caso de que haya un error o algún desacuerdo.
d) Consiste en mantener un seguimiento de a quién le corresponde el turno de comunicarse y hacerlo cumplir.

13. <Tipo 1> La administración de actividades es un servicio que ofrece la capa de sesión. ¿En qué consiste este servicio?

a) Consiste en un mecanismo de notificación de errores inesperados.
b) Consiste en permitir que el usuario divida el flujo de mensajes en unidades de lógicas.
c) Consiste en llevar a las entidades de sesión de vuelta a un estado conocido, en caso de que haya un error o algún desacuerdo.
d) Consiste en mantener un seguimiento de a quien le corresponde el turno de comunicarse y hacerlo cumplir.

14. <Tipo 1> La notificación de excepciones es un servicio que ofrece la capa de sesión. ¿En qué consiste este servicio?

a) Consiste en un mecanismo de notificación de errores inesperados.
b) Consiste en permitir que el usuario divida el flujo de mensajes en unidades de lógicas.
c) Consiste en llevar a las entidades de sesión de vuelta a un estado conocido, en caso de que haya un error o algún desacuerdo.
d) Consiste en mantener un seguimiento de a quien le corresponde el turno de comunicarse y hacerlo cumplir.

15. <Tipo 1> _____: es un protocolo que permite a un programa de computadora ejecutar código en otra máquina remota sin tener que preocuparse por las comunicaciones entre ambos, y además oculta los detalles de implementación de esas llamadas remotas. Implementa la llamada remota mediante un diálogo petición respuesta.

a) RPC.
b) TCP.
c) SSH.
d) UDP.
e) ICMP.
f) Telnet.
g) FTP.

16. <Tipo 1> Es un proceso por medio del cual se realiza una comunicación breve para que cliente y servidor puedan identificarse y establecer una comunicación.

a) Handshaking.
b) Espera y escucha.
c) Ventana deslizante.
d) Retransmisión selectiva.
e) Retransmisión no selectiva.

17. <Tipo 4> La finalidad de RCP es:

- Proporcionar un middleware que simplifique el desarrollo de aplicaciones distribuidas.
- Evitar que el programador tenga que interactuar directamente con el interfaz de Sockets.
- Abstraer (ocultar) los detalles relativos a la red.

- El servidor ofrece procedimiento que el cliente llama como si fueran procedimientos locales.
- Se busca ofrecer un entorno de programación lo más similar posible a un entorno no distribuido.

La sentencia anterior es:

a) Correcta.
b) Incorrecta.

18. <Tipo 1> ¿Cuál es la diferencia entre SCP y RCP?

a) En el protocolo SCP los datos son cifrados durante su transferencia para evitar que potenciales packet sniffers extraigan información útil de los paquetes de datos.
b) En el protocolo RCP los datos son cifrados durante su transferencia para evitar que potenciales packet sniffers extraigan información útil de los paquetes de datos.
c) No existe ninguna diferencia.
d) Son el mismo protocolo bajo diferentes estándares.

19. <Tipo 1> ¿Cuál es la diferencia entre RCP y ASP?

a) ASP es un protocolo intermedio que se basa en la parte superior del protocolo de transacción (ATP) que es original fiable de nivel de sesión.
b) RCP es un protocolo intermedio que se basa en la parte superior de protocolo de transacción (ATP) que es original fiable de nivel sesión.
c) No existe ninguna diferencia.
d) Son el mismo protocolo bajo diferentes estándares.

20. <Tipo 4> La capa de sesión surgió de la necesidad de organizar y sincronizar el diálogo y controlar el intercambio de datos

    La sentencia anterior es:

a) Correcta.
b) Incorrecta.

21. <Tipo 1> ¿Cuál es la finalidad de la capa de sesión?

a) Permite a los usuarios de máquinas diferentes establecer sesiones entre ellos.
b) Se encarga de la representación de la información de manera que distintos equipos puedan tener diferentes representaciones de caracteres.
c) Está encargado de la transferencia libre de errores de los datos entre el emisor y el receptor.
d) Provee servicios para intercambiar secciones de datos individuales a través de la red.

22. <Tipo 2> Son los tipos más comunes de RPC:

a) ONC RPC de Sun.
b) DCE/RPC de OSF.
c) Modelo de Objetos de Componentes Distribuidos de Microsoft DCOM.
d) ASP.
e) SCP.
f) DNS.
g) SSH.
h) SMTP.

23. <Tipo 5> Asigna el servicio a la descripción que le corresponde

a) Control de diálogo.	(a) Este puede ser simultáneo en los dos sentidos o alternado en ambos sentidos.
b) Agrupamiento.	(b) El flujo de datos se puede marcar para definir grupos de datos.
c) Recuperación.	(c) La capa de sesión proporciona un procedimiento que si detecta algún fallo, la capa de sesión es capaz de retransmitir todos los datos desde el último punto de revisión y no desde el inicio.

24. <Tipo 2> La capa de Sesión se encarga de _____, _____ y _____ la comunicación entre origen y destino, sin importar por qué elementos pasa la información o como se realiza el enrutamiento.

a) Iniciar.
b) Mantener.
c) Terminar.
d) Enrutar.
e) Enlazar.
f) Comunicar.

25. <Tipo 4> La capa de sesión se encarga de controlar el diálogo entre las aplicaciones de los sistemas finales. En muchos casos, los servicios de la capa de sesión son parcialmente, o incluso, totalmente prescindibles. No obstante, en algunas aplicaciones su utilización es ineludible.

La sentencia anterior es:

a) Correcta.
b) Incorrecta.

26. <Tipo 4> La capa de transporte se encarga de controlar el diálogo entre las aplicaciones de los sistemas finales. En muchos casos, los servicios de la capa de transporte son parcialmente, o incluso, totalmente prescindibles. No obstante, en algunas aplicaciones su utilización es ineludible.

    La sentencia anterior es:

c) Correcta.
d) Incorrecta.

27. <Tipo 1> Este puede ser simultáneo en los dos sentidos (full-duplex) o alternado en ambos sentidos (half-duplex). Este es un servicio de la capa de sesión que recibe el nombre de:

a) Control de diálogo.
b) Agrupamiento.
c) Recuperación.
d) Flujo de datos.
e) Ninguno de los anteriores.

28. <Tipo 1> El flujo de datos se puede marcar para definir grupos de datos. Es un servicio de la capa de sesión que recibe el nombre de:

a) Control de diálogo.
b) Agrupamiento.
c) Recuperación.
d) Flujo de datos.
e) ninguno de los anteriores.

29. <Tipo 1> La capa de sesión proporciona un procedimiento que si detecta algún fallo, la capa de sesión es capaz de retransmitir todos los datos desde el último punto de revisión y no desde el inicio.

a) Control de diálogo.
b) Agrupamiento.
c) Recuperación.
d) Flujo de datos.
e) ninguno de los anteriores.

Preguntas Tema 8: Capa de Presentación

1. <Tipo 1> Esta capa del modelo OSI es la encargada de traducir el formato y asigna una sintaxis a los datos para su transmisión en la red.

a) Física.
b) Enlace.
c) Red.
d) Transporte.
e) Sesión.
f) Presentación.
g) Aplicación.

2. <Tipo 2> ¿Cuáles son las funciones de la capa de presentación?

a) Iniciar la conexión.
b) Codificación y conversión de datos.
c) Fragmentación de paquetes.
d) Compresión de los datos.
e) Mantener la conexión.
f) Cifrado de los datos.
g) Terminar la transmisión.

3. <Tipo 1> La _____ garantiza que los datos del dispositivo de origen puedan ser interpretados por la aplicación adecuada en el dispositivo de destino.

a) Iniciar la conexión.
b) Codificación y conversión de datos.
c) Fragmentación de paquetes.
d) Compresión de los datos.
e) Mantener la conexión.
f) Cifrado de los datos.
g) Terminar la transmisión.

4. <Tipo 1> La _____ funciona mediante el uso de algoritmos para reducir el tamaño de los archivos. El algoritmo busca patrones de bits repetidos en el archivo y entonces los reemplaza con un token.

a) Iniciar la conexión.
b) Codificación y conversión de datos.
c) Fragmentación de paquetes.
d) Compresión de los datos.
e) Mantener la conexión.
f) Cifrado de los datos.
g) Terminar la transmisión.

5. <Tipo 1> El _____ protege la información durante la transmisión. Las transacciones financieras, por ejemplo, lo utilizan para proteger la información confidencial que se envía a través de Internet.

a) Iniciar la conexión.
b) Codificación y conversión de datos.
c) Fragmentación de paquetes.
d) Compresión de los datos.
e) Mantener la conexión.
f) Cifrado de los datos.
g) Terminar la transmisión.

6. <Tipo 1> Este código fue desarrollado por el Instituto Nacional Norteamericano de Estándares el cual se puede representar 128 símbolos.

a) ANSI.
b) ASCII 7 bits.
c) ASCII 8 bits.
d) UNICODE.
e) UTF-8.

7. <Tipo 1> El lenguaje Java utiliza este código para representar carácteres.

a) ANSI.
b) ASCII 7 bits.
c) ASCII 8 bits.
d) UNICODE.
e) UTF-8.

8. <Tipo 1> ASCII 7 bits tiene las siguientes características:

I. ASCII utiliza un patrón de siete bits que varía de 0000000 a 1111111.
II. El primer patrón (0000000) representa el carácter nulo.
III. El último patrón (1111111) representa el carácter de retorno de carro.
IV. Hay 31 caracteres de control.
V. Los caracteres numéricos se codifican después que las letras.
VI. Las letras mayúsculas (A ... Z) están antes que las letras minúsculas (a ... z).
VII. Los caracteres en mayúsculas y en minúsculas se distinguen sólo por un bit.
VIII. Hay cinco caracteres especiales entre las letras mayúsculas y minúsculas.

¿Cuáles de estas características son incorrectas?

a) II, III y V.
b) II, V y VIII.
c) III, IV y V.
d) III, V y VII.
e) III, V y VIII.
f) Todas las anteriores.
g) Ninguna de las anteriores.

9. <Tipo 4> *“Para hacer que el tamaño de cada patrón sea de 1 byte, a los patrones de ASCII se les aumentó un 0 a la izquierda creando así ASCII 8 bits. el cual, varios fabricantes usaron el bit agregado para crear un sistema de 128 símbolos adicional, este intento fue un éxito para los fabricantes que decidieron realizar este cambio”.*

La anterior sentencia es …

a) Correcta.
b) Incorrecta.

10. <Tipo 1> Una coalición de fabricantes de hardware y software ha diseñado un código llamado _____ que puede representar hasta 65536 símbolos. Diferentes secciones del código se asignan a los símbolos de distintos idiomas en el mundo. Algunas partes del código se usan para símbolos gráficos y especiales.

a) ANSI.
b) ASCII 7 bits.
c) ASCII 8 bits.
d) UNICODE.
e) UTF-8.

11. <Tipo 1> Método de compresión de datos que al comprimir datos y posteriormente descomprimirlos no son exactamente como los originales. Por lo general, este método se utiliza en la compresión de datos multimediales. Cuando se habla de imágenes, sonido y video, suele llamarse también compresión con pérdida de calidad.

a) Compresión con pérdidas.
b) Compresión sin pérdidas.
c) Compresión de espacios en blanco.
d) Compresión simple.
e) Ninguna de las anteriores

12. <Tipo 2> Compresión de imágenes con pérdida de calidad.

a) MP3.
b) Wavelet.
c) Flash.
d) JPEG.
e) MPEG.
f) G.711.
g) AAC.
h) AMR.

13. <Tipo 2> Compresión de videos/animación con pérdida de calidad.

a) MP3.
b) Wavelet.
c) Flash.
d) JPEG.
e) MPEG.
f) G.711.
g) AAC.
h) AMR.

14. <Tipo 2> Compresión de música con pérdida de calidad.

a) MP3.
b) Wavelet.
c) Flash.
d) JPEG.
e) MPEG.
f) G.711.
g) AAC.
h) AMR.

15. <Tipo 2> Compresión de voz con pérdida de calidad.

a) MP3.
b) Wavelet.
c) Flash.
d) JPEG.
e) MPEG.
f) G.711.
g) AAC.
h) AMR.

16. <Tipo 1> Los datos antes y después de efectuar este proceso son exactamente iguales. Por lo que podemos asumir que los datos fueron puestos bajo un proceso de:

a) Compresión sin pérdidas.
b) Compresión simple.
c) Compresión con pérdidas.
d) Compresión sencilla.
e) Los datos no fueron puestos bajo ningún proceso.

17. <Tipo 1>En qué consiste el proceso de compresión sin pérdidas

a) La información no se comprime solo es una manera de llamar a este proceso.
b) La información se comprime y existe pérdida de datos.
c) La información se lee y codifica utilizando la probabilidad de aparición de cada carácter.
d) Ninguna de las definiciones anteriores.

18. <Tipo 2>Compresión de imágenes sin pérdidas

a) PNG.
b) TIFF.
c) GIF.
d) BMP.
e) MP3.
f) Wavelet.
g) Flash.

19. <Tipo 2>Compresión de música/audio sin pérdidas

a) FLAC.
b) AiFF.
c) ALAC.
d) WAV.
e) ACC.
f) MP3.
g) WMA.

20. <Tipo 4>" El *cifrado protege la información durante la transmisión de esta"*

La sentencia anterior es:

a) correcta
b) incorrecta

21. <Tipo 1>La criptología se divide en:

a) Criptoanálisis y criptografía.
b) Esteganografía, criptografía y codificación.
c) criptoanálisis, criptografía y codificación.
d) Esteganografía, criptoanálisis y codificación.
e) ninguna de las anteriores.

22. <Tipo 2>Son técnicas utilizadas en la criptografía.

a) Códigos.
b) Cifrados.
c) Transposición.
d) Sustitución.
e) Ninguna de las anteriores.

23. <Tipo 2> Dos técnicas básicas del cifrado clásico son.

a) Transposición.
b) Sustitución.
c) Monoalfabéticos.
d) Polialfabéticos.
e) Poligramicos.
f) Ninguno de los anteriores.

24. <Tipo 2> Son métodos de cifrado por sustitución.

Selecciona las respuestas correctas.

a) Monoalfabéticos.
b) Polialfabéticos.
c) Poligramicos.
d) Máscaras rotativas.
e) Códigos.
f) Cifrados.

25. <Tipo 1> Son métodos de cifrado por Transposición

Selecciona la respuesta correcta

a) Monoalfabético.
b) Polialfabéticos.
c) Poligrámicos.
d) Transposición.
e) Códigos.
f) Cifrados.
g) Ninguna de la anteriores.

26. <Tipo 4> El cifrado mediante clave simétrica significa que dos o más usuarios poseen una única clave secreta que será la que se utilizará para cifrar y descifrar la información

    La sentencia anterior es:

a) Correcta.
b) Incorrecta.

27. <Tipo 4> El cifrado mediante clave asimétrica significa que dos o más usuarios poseen una única clave secreta que será la que se utilizará para cifrar y descifrar la información.

    La sentencia anterior es:

a) Correcta.
b) Incorrecta.

28. <Tipo 4> El cifrado asimétrico se da mediante la implementación de dos claves de cifrado denominadas clave pública y clave privada.

    La sentencia anterior es:

a) Correcta.
b) Incorrecta.

29. <Tipo 4> El cifrado simétrico se da mediante la implementación de dos claves de cifrado denominadas clave pública y clave privada.

    La sentencia anterior es:

a) Correcta.
b) Incorrecta.

30. <Tipo 2>Si los algoritmos de cifrado que se utilizan son de dominio público, ¿qué garantiza que sean seguros?

a) No son seguros.
b) La clave utilizada para cifrar el mensaje.
c) Las matemáticas del algoritmo.
d) No se utilizan los algoritmos de dominio público.

31. <Tipo 3>Organiza los siguientes algoritmos de cifrado dependiendo si son simétricos o asimétricos.

simétricos	asimétricos
• DES (Data Encryption Standard) • 3DES (Triple Data Encryption Standard) • AES (Advanced Encryption Standard) • SAFER (Secure and Fast Encription Routine) • Blowfish	• RSA (Rivest, Shamir, Adleman) • Diffie-Hellman • ECC (Elliptical Curve Cryptography)

Preguntas Tema 9: Capa de Aplicación

1. <Tipo 1> La capa de _____ ofrece la posibilidad de acceder a los servicios de las demás capas, así como define cuáles son los protocolos que se usarán en la comunicación.

a) Física.
b) Enlace.
c) Red.
d) Transporte.
e) Sesión.
f) Presentación.
g) Aplicación.

2. <Tipo 1> Fue creado por el CERN en 1989, cubrió la necesidad de lograr la comunicación a grandes grupos de científicos y ha sido utilizado en el world wide web desde 1990.

a) HTTP.
b) HTTPS.
c) SSH.
d) TelNet.
e) FTP.
f) SMBS.

3. <Tipo 2> ¿Cuáles de las siguientes opciones corresponden a un servidor que provee http?

a) NCSA.
b) Netscape.
c) Apache.
d) Mosaic.
e) Roxen.
f) Lynx.

4. <Tipo 2> ¿Cuáles de las siguientes opciones corresponden a un cliente de http?

g) NCSA.
h) Netscape.
i) Apache.
j) Mosaic.
k) Roxen.
l) Lynx.

5. <Tipo 1> Este protocolo utiliza un sistema de cifrado basado en SSL para crear un canal seguro entre servidor y cliente. Es usado cuando se necesita enviar o acceder información sensible en un sitio web.

a) HTTP.
b) HTTPS.
c) SSH.
d) TelNet.
e) FTP.
f) SMBS.

6. <Tipo 1> ¿En qué puerto trabaja HTTP?

a) 80.
b) 8080.
c) 443.
d) 21.
e) 23.

7. <Tipo 1> ¿En qué puerto trabaja HTTPS?

a) 80.
b) 8080.
c) 443.
d) 21.
e) 23.

8. <Tipo 1> Es un protocolo que permite compartir archivos dentro de una red LAN. Los clientes que acceden a un servidor de este tipo pueden utilizar los recursos del mismo como si fueran recursos del mismo host cliente. Su funcionamiento está enfocado en sistemas Microsoft Windows.

a) HTTP.
b) HTTPS.
c) SSH.
d) TelNet.
e) FTP.
f) SMB.

9. <Tipo 1> ¿En qué puerto trabaja SMB?

a) 25.
b) 23.
c) 110.
d) 443.
e) 445.
f) 465.

10. <Tipo 1> Este protocolo permite el acceso a sistemas de archivos mediante la red, es nativo de los sistemas Unix.

a) SMB.
b) FTP.
c) SSH.
d) NFS.
e) HTTP.
f) IMAP.

11. <Tipo 1> Samba en el contexto de redes es…

a) Un servidor de SMB para Unix.
b) Un servidor de NFS para Unix.
c) Un servidor de NFS para Windows.
d) Un servidor de SMB para Windows.
e) Un servidor de HTTPS.
f) Un cliente de HTTPS.

12. <Tipo 1> Este es uno de los protocolos más antiguos de Internet y permite interconectar equipos de manera remota, de tal modo que la máquina cliente se comporta como una terminal más de la máquina remota.

a) HTTP.
b) HTTPS.
c) SSH.
d) TelNet.
e) FTP.
f) SMB.

13. <Tipo 4> *"El propósito de TelNet es proporcionar comunicación bastante general, bidireccional. Es previsto que el protocolo se puede también utilizar para comunicación de terminal-terminal (linking) pero no permite comunicación de proceso-proceso (cómputo distribuido)."*

    La anterior sentencia es …

a) Verdadera.
b) Falsa.

14. <Tipo 2> ¿Cuáles son motivos válidos para no recomendar el uso de TelNet en los sistemas modernos?

a) TelNet hace uso de Network Virtual Terminal.
b) TelNet no cifra por defecto las comunicaciones.
c) TelNet no puede realizar comunicación de terminal a terminal.
d) TelNet carece de un esquema de autenticación.
e) TelNet no puede realizar comunicación de proceso a proceso.
f) Ninguna de la anteriores opciones, TelNet siempre es recomendable sin importar para qué es usado.

15. <Tipo 1> ¿En qué puerto trabaja TelNet?

a) 25.
b) 23.
c) 22.
d) 20.
e) 21.
f) 465.

16. <Tipo 1> Es el protocolo moderno que permite la conexión remota a una máquina a través de la red. Permite manejar por completo una computadora mediante un intérprete de comandos.

a) HTTP.
b) HTTPS.
c) SSH.
d) TelNet.
e) FTP.
f) SMB.

17. <Tipo 4> *"Además de la conexión a otros dispositivos, SSH permite copiar datos de forma segura, gestiona únicamente claves RSA para no escribir contraseñas cada vez que se quiera conectar con el dispositivo remoto y enviar los datos de cualquier otra aplicación por un canal seguro tunelizado mediante SSH."*

La anterior sentencia es …

a) Verdadera.
b) Falsa.

18. <Tipo 1> ¿En qué puerto trabaja SSH?

a) 25.
b) 23.
c) 22.
d) 20.
e) 21.
f) 465.

19. <Tipo 1> Este protocolo permite la transferencia de datos entre un cliente y un servidor. Su uso es muy extendido por Internet pese a ser inseguro. Una de sus ventajas es el que ofrece mejor rendimiento y velocidad debido a que no cifra ni descifra la comunicación.

a) SFTP.
b) VSFTPD.
c) TFTP.
d) FTP.
e) SSH.
f) TelNet.

20. <Tipo 2> ¿En qué puertos trabaja FTP?

a) 20.
b) 21.
c) 22.
d) 23.
e) 69.
f) 465.

21. <Tipo 1> Este protocolo trabaja de manera similar a FTP, pero con la importante diferencia de que realiza la transferencia de archivos de mediante una conexión cifrada lo cual lo hace más seguro que FTP, una desventaja que tienen es que no todos los dispositivos son compatibles con este protocolo.

a) SFTP.
b) VSFTPD.
c) TFTP.
d) FTPS.
e) SSH.
f) TelNet.

22. <Tipo 1> En ocasiones se puede confundir SFTP y FTPS ¿Cuál de las siguientes opciones es una diferencia entre estos dos?

a) SFTP es una extensión de FTP en cambio FTPS es un protocolo totalmente construido desde 0.
b) FTPS funciona forzosamente en conjunto con SSH en cambio SFTP puede operar de manera individual.
c) SFTP es el antecesor a FTPS.
d) FTPS es una extensión de FTP en cambio SFTP es un protocolo totalmente construido desde 0.
e) SFTP funciona forzosamente en conjunto con SSH en cambio FTPS puede operar de manera individual.

23. <Tipo 1> Programa que trabaja en segundo plano en los sistemas linux y que no requiere de la intervención del usuario para realizar la transmisión de archivos mediante la red, por lo que a la fecha es considerado uno de los más seguros debido a sus configuraciones predeterminadas. Como referencia opera en los puertos 20 y 21.

a) SFTP.
b) VSFTPD.
c) TFTP.
d) FTPS.
e) SSH.
f) TelNet.

24. <Tipo 4> VSFTPD tiene las siguientes características:

- Soporta direcciones IP virtuales.
- Soporta usuarios virtuales.
- Se ejecuta de manera independiente o a través de inetd.
- Poderosa configuración para cada usuario.
- Soporte para el control de ancho de banda.
- Límites para direcciones IP.
- Soporte para IPv6.
- Soporte de encriptación a través de SSL.

Lo anterior descrito es …

a) Verdadero.
b) Falso.

25. <Tipo 1> Es un protocolo de transferencia de archivos basado en UDP que no proporciona ninguna seguridad. En la mayoría de sistemas está desactivado. Su uso principal es el arranque de estaciones diskless o de routers a través de la red.

a) SFTP.
b) VSFTPD.
c) TFTP.
d) FTPS.
e) SSH.
f) TelNet.

26. <Tipo 1> ¿En qué puerto trabaja TFTP?

a) 20.
b) 21.
c) 22.
d) 23.
e) 69.
f) 465.

27. <Tipo 1> ¿Cuál de las siguientes definiciones se apega al protocolo de IMAP?

a) Este protocolo ofrece la posibilidad de administrar los e-mails directamente en el servidor, es decir, si se elige este protocolo para establecer una cuenta de correo, únicamente se recibirá una lista de los mensajes y sus respectivos asuntos.
b) Este protocolo ofrece la posibilidad de descargar todos los correos desde el servidor, cuando esto ocurre los mensajes son eliminados del servidor de correo.
c) Este protocolo es usado para la transmisión de correo electrónico entre servidores de correo, así como la comunicación entre servidores y clientes de correo.

28. <Tipo 1> ¿Cuál de las siguientes definiciones se apega al protocolo de POP?

a) Este protocolo ofrece la posibilidad de administrar los e-mails directamente en el servidor, es decir, si se elige este protocolo para establecer una cuenta de correo, únicamente se recibirá una lista de los mensajes y sus respectivos asuntos.
b) Este protocolo ofrece la posibilidad de descargar todos los correos desde el servidor, cuando esto ocurre los mensajes son eliminados del servidor de correo.
c) Este protocolo es usado para la transmisión de correo electrónico entre servidores de correo, así como la comunicación entre servidores y clientes de correo.

29. <Tipo 1> ¿Cuál de las siguientes definiciones se apega al protocolo de SMTP?

a) Este protocolo ofrece la posibilidad de administrar los e-mails directamente en el servidor, es decir, si se elige este protocolo para establecer una cuenta de correo, únicamente se recibirá una lista de los mensajes y sus respectivos asuntos.
b) Este protocolo ofrece la posibilidad de descargar todos los correos desde el servidor, cuando esto ocurre los mensajes son eliminados del servidor de correo.
c) Este protocolo es usado para la transmisión de correo electrónico entre servidores de correo, así como la comunicación entre servidores y clientes de correo.

30. <Tipo 1> ¿Cuál de las siguientes opciones no es un protocolo de correo electrónico?

a) SMTP.
b) IMAP.
c) POP.
d) SFTP.

31. <Tipo 1> ¿A través de cuál de los siguientes puertos se utiliza SMTP?

a) 25/tcp.
b) 25/udp.
c) 143/tcp.
d) 143/udp.
e) 110/tcp.
f) 110/udp.

32. <Tipo 1> ¿A través de cuál de los siguientes puertos se utiliza IMAP?

a) 25/tcp.
b) 25/udp.
c) 143/tcp.
d) 143/udp.
e) 110/tcp.
f) 110/udp.

33. <Tipo 1> ¿A través de cuál de los siguientes puertos se utiliza POP?

a) 25/tcp.
b) 25/udp.
c) 143/tcp.
d) 143/udp.
e) 110/tcp.
f) 110/udp.

34. <Tipo 1> La principal ventaja de este sistema de autenticación de usuarios es la posibilidad de utilizar los directorios passwd y/o shadow como bases de datos y permitir el acceso de usuarios a través de cualquier nodo de la red a través de un protocolo seguro

a) NIS.
b) LDAP.
c) Kerberos.
d) Radius.

35. <Tipo 1> La principal ventaja de este sistema de autenticación de usuarios, es la posibilidad que ofrece a los administradores de agregar aplicaciones a sus bases de datos para que puedan acceder a los datos que necesiten, de manera automática y en caso contrario el protocolo permite saber la actividad de la aplicación y para qué utilizó la información

a) NIS.
b) LDAP.
c) Kerberos.
d) Radius.

36. <Tipo 1> ¿Cuál es el protocolo de seguridad para validar usuarios con los servicios de red y evitar el envío de contraseñas a través de la red?

a) NIS.
b) LDAP.
c) Kerberos.
d) Radius.

37. <Tipo 1> ¿Cuál es el protocolo cliente/servidor basado en el protocolo de datagrama de usuario (UDP) y que se considera un servicio sin conexión?

a) NIS.
b) LDAP.
c) Kerberos.
d) Radius.

38. <Tipo 1> ¿A través de cuál de los siguientes puertos se utiliza Kerberos?

a) 88/tcp.
b) 88/udp.
c) 1812/tcp.
d) 1812/udp.
e) 389/tcp.
f) 389/udp.

39. <Tipo 1> ¿A través de cuál de siguientes puertos se utiliza LDAP?

a) 88/tcp.
b) 88/udp.
c) 1812/tcp.
d) 1812/udp.
e) 389/tcp.
f) 389/udp.

40. <Tipo 1> ¿A través de cuál de los siguientes puertos se utiliza Radius?

a) 88/tcp.
b) 88/udp.
c) 1812/tcp.
d) 1812/udp.
e) 389/tcp.
f) 389/udp.

41. <Tipo 1> ¿Cuál es la definición de portal captivo?

a) Es una página de inicio de sesión personalizado en redes empresariales que los usuarios invitados deben pasar antes de poder conectarse a la red.
b) Es una página de inicio de sesión personalizado en redes empresariales que los empleados deben pasar antes de poder conectarse a la red.
c) Es una página de inicio de sesión personalizada en redes privadas para controlar y restringir el acceso a la red.
d) Ninguna de la anteriores.

42. <Tipo 1> Es una página de inicio de sesión personalizado en redes empresariales a través de la cual los usuarios invitados deben ser validados para poder conectarse a la red.

a) Portal captivo.
b) Portal web.
c) Portal de login.
d) ninguna de las anteriores.

43. <Tipo 4> ¿Un certificado digital garantiza la confidencialidad, integridad y disponibilidad de la información?

a) Cierto.
b) Falso.

44. <Tipo 4> ¿La firma digital y el certificado digital aseguran el no repudio?

a) Cierto.
b) Falso.

45. <Tipo 3> Clasifica cada protocolo de acuerdo al tipo.

a) SMTP.
b) IMAP.
c) POP.
d) Radius.
e) Kerberos.
f) NIS.
g) LDAP.

Protocolo de Correo	Protocolos de Autenticación
SMTP. IMAP. POP.	Radius. Kerberos. NIS. LDAP.

46. <Tipo 4> El certificado digital permite que la información transmitida entre emisor y receptor esté cifrada.

a) Cierto.
b) Falso.

47. <Tipo 4> El certificado digital solo se genera si previamente se emitió una firma digital.

a) Cierto.
b) Falso.

48. <Tipo 4> La **firma digital** implica que existe un **certificado** emitido por un organismo a través del cual se valida la propia **firma** y la identidad del firmante. Por su parte, el **certificado digital** o electrónico es el documento mediante el cual se identifica una persona en Internet.

La sentencia anterior es:

a) Correcta.
b) Incorrecto.

49. <Tipo 1> ¿Que protocolo trabaja en el puerto 80?

a) TelNet.
b) HTTPS.
c) SMB.
d) HTTP.
e) SSH.
f) FTP.
g) TFTP.
h) SMTP.
i) IMAP.
j) POP.
k) Kerberos.
l) LDAP.
m) Radius.

50. <Tipo 1> ¿Que protocolo trabaja en el puerto 443?

a) TelNet.
b) HTTPS.
c) SMB.
d) HTTP.
e) SSH.
f) FTP.
g) TFTP.
h) SMTP.
i) IMAP.
j) POP.
k) Kerberos.
l) LDAP.
m) Radius.

51. <Tipo 1> ¿Que protocolo trabaja en el puerto 445?

a) TelNet.
b) HTTPS.
c) SMB.
d) HTTP.
e) SSH.
f) FTP.
g) TFTP.
h) SMTP.
i) IMAP.
j) POP.
k) Kerberos.
l) LDAP.
m) Radius.

52. <Tipo 1> ¿Que protocolo trabaja en el puerto 23?

a) TelNet.
b) HTTPS.
c) SMB.
d) HTTP.
e) SSH.
f) FTP.
g) TFTP.
h) SMTP.
i) IMAP.
j) POP.
k) Kerberos.
l) LDAP.
m) Radius.

53. <Tipo 1> ¿Que protocolo trabaja en el puerto 22?

a) TelNet.
b) HTTPS.
c) SMB.
d) HTTP.
e) SSH.
f) FTP.
g) TFTP.
h) SMTP.
i) IMAP.
j) POP.
k) Kerberos.
l) LDAP.
m) Radius.

54. <Tipo 1> ¿Que protocolo trabaja en el puerto 21?

a) TelNet.
b) HTTPS.
c) SMB.
d) HTTP.
e) SSH.
f) FTP.
g) TFTP.
h) SMTP.
i) IMAP.
j) POP.
k) Kerberos.
l) LDAP.
m) Radius.

55. <Tipo 1> ¿Que protocolo trabaja en el puerto 69?

a) TelNet.
b) HTTPS.
c) SMB.
d) HTTP.
e) SSH.
f) FTP.
g) TFTP.
h) SMTP.
i) IMAP.
j) POP.
k) Kerberos.
l) LDAP.
m) Radius.

56. <Tipo 1> ¿Que protocolo trabaja en el puerto 25?

a) TelNet.
b) HTTPS.
c) SMB.
d) HTTP.
e) SSH.
f) FTP.
g) TFTP.
h) SMTP.
i) IMAP.
j) POP.
k) Kerberos.
l) LDAP.
m) Radius.

57. <Tipo 1> ¿Que protocolo trabaja en el puerto 143?

a) TelNet.
b) HTTPS.
c) SMB.
d) HTTP.
e) SSH.
f) FTP.
g) TFTP.
h) SMTP.
i) IMAP.
j) POP.
k) Kerberos.
l) LDAP.
m) Radius.

58. <Tipo 1> ¿Que protocolo trabaja en el puerto 110?

a) TelNet.
b) HTTPS.
c) SMB.
d) HTTP.
e) SSH.
f) FTP.
g) TFTP.
h) SMTP.
i) IMAP.
j) POP.
k) Kerberos.
l) LDAP.
m) Radius.

59. <Tipo 1> ¿Que protocolo trabaja en el puerto 88?

a) TelNet.
b) HTTPS.
c) SMB.
d) HTTP.
e) SSH.
f) FTP.
g) TFTP.
h) SMTP.
i) IMAP.
j) POP.
k) Kerberos.
l) LDAP.
m) Radius.

60. <Tipo 1> ¿Que protocolo trabaja en el puerto 380?

a) TelNet.
b) HTTPS.
c) SMB.
d) HTTP.
e) SSH.
f) FTP.
g) TFTP.
h) SMTP.
i) IMAP.
j) POP.
k) Kerberos.
l) LDAP.
m) Radius.

61. <Tipo 1> ¿Que protocolo trabaja en el puerto 1812?

a) TelNet.
b) HTTPS.
c) SMB.
d) HTTP.
e) SSH.
f) FTP.
g) TFTP.
h) SMTP.
i) IMAP.
j) POP.
k) Kerberos.
l) LDAP.
m) Radius.

Glosario

A

Activo de información: Es todo aquello con valor para una organización y que necesita protección, tales como información, aplicaciones, procesos, servicios, infraestructura y personal.

ABM (Asynchronous Balanced Mode): Es un modo de comunicación del HDLC y protocolos derivados, apoyado en comunicaciones punto-a-punto entre pares orientada entre dos nodos, cuando uno u otro nodo puede iniciar la transmisión.

Amenazas: Todo aquello que puede causar daño, modificación o pérdida en los activos de una organización.

ANSI (**American National Standards Institute**): Es una organización sin fines de lucro que supervisa el desarrollo de estándares para productos, servicios, procesos y sistemas en los Estados Unidos.

ARM (Asynchronous Response Mode): Es un modo de comunicación del HDLC se utiliza en la configuración no balanceada. La estación secundaria puede iniciar la transmisión sin tener permiso explícito por parte de la primaria.

ARP (Address Resolution Protocol): Protocolo que permite a una fuente encontrar la dirección de hardware de un destino que se encuentre en la misma subred física.

ARP spoofing: Tipo de ataque que consiste en falsificar cualquier dirección MAC en una red de cómputo.

ARQ (Automatic Repeat-reQuest): Son protocolos utilizados para el control de errores en la transmisión de datos, garantizando la integridad de los mismos.

ASP (AppleTalk Session Protocol): Es un protocolo de la capa de sesión en la suite de protocolos AppleTalk que establece y mantiene sesiones entre clientes y servidores AppleTalk.

ASCII (American Standard Code for Information Interchange): Secuencia de 7 u 8 bits que representan símbolos.

Atacante: Individuo o elemento que atentan contra la seguridad de un activo o un sistema.

Ataque: Acciones organizadas e intencionadas causadas por una o más entidades para ocasionar daño o problemas a un sistema o red.

ATM (Asynchronous Transfer Mode): Es un concepto de telecomunicaciones definido por las normas de las organizaciones ANSI y UIT para el transporte de una gama completa de tráfico de usuarios, incluidas las señales de voz, datos y video.
ATP (AppleTalk Transaction Protocol): Protocolo de transacción AppleTalk. Proporciona la conexión de capa de transporte entre Computadoras.
Autenticación. Confirma que la identidad de una o más entidades conectadas a una o más entidades sea verdadera.

B

BGP (Border Gateway Protocol): Es un protocolo escalable de dynamic routing usado en la Internet por grupos de enrutadores para compartir información de enrutamiento.
Bit rate: Tasa de bits que define el número de bits que se transmiten por unidad de tiempo (b/s).
BNC (Bayonet Neill-Concelman): Es un tipo de conector, de rápida conexión/desconexión, utilizado para cable coaxial.
Byte: Unidad de información compuesta generalmente de ocho bits.

C

Cableado estructurado: Infraestructura de cable destinada a transportar a lo largo y ancho de una red LAN los datos que requieran compartir los usuarios.
CERN (Conseil Européen pour la Recherche Nucléaire): Es una organización de investigación europea que opera el laboratorio de física de partículas más grande del mundo.
Certificado digital: Medio que permite garantizar técnica y legalmente la identidad de una persona en Internet, así como cifrar las comunicaciones.
CIDR (Classless Inter-Domain Routing): Protocolo que se introdujo en 1993. Este protocolo permite un uso más eficiente de las direcciones IPv4.

Cifrado: Método para garantizar que la información no es inteligible para individuos, entidades o procesos no autorizados a través de lo cual proporciona confidencialidad a la información.

Confidencialidad. Protege a una entidad contra la revelación deliberada o accidental de cualquier conjunto de datos a entidades no autorizadas.

Control de acceso: Servicio que provee protección contra uso no autorizado de los activos de un sistema, permitiendo que sólo aquellos usuarios autorizados accedan a los recursos del sistema o a la red.

Control de encaminamiento. Permite enviar determinada información por determinadas zonas consideradas clasificadas, así como habilitar la posibilidad de solicitar otras rutas en caso de que se detecten persistentes violaciones de integridad en una ruta determinada.

CRC (Cyclic Redundancy Code): Es un código de detección de errores usado frecuentemente en redes digitales y en dispositivos de almacenamiento para detectar cambios accidentales en los datos.

CSMA (Carrier Sense Multiple Access): Es un protocolo de control de acceso a redes que permite a una estación realizar una escucha para asegurarse de que el medio está libre antes de transmitir información.

CSMA/CD (Carrier Sense Multiple Access with Collision Detection): Variante de CSMA donde es posible detectar una interferencia e interrumpir la transmisión de datos de inmediato, enviando previamente una señal de congestión que notifica la colisión a las demás estaciones que comparten el medio.

CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance): Variante de CSMA donde si el medio está libre tras realizar la escucha, se espera un tiempo aleatorio adicional antes de transmitir, lo cual reduce el número de colisiones.

D

DEC (Digital Equipment Corporation): Fue una compañía estadounidense considerada pionera en la fabricación de minicomputadores.

DHCP (Dynamic Host Configuration Protocol): Protocolo de red que permite a los nodos de una red IP obtener sus parámetros de configuración automáticamente.

Disponibilidad. Asegura que la información sea accedida cuando se requiera por la gente, sistema o proceso que cuente con los permisos necesarios para acceder a ella.

DLC (D**ata** L**ink** C**ontrol):** Dirección que identifica de forma única un nodo de una red. Cada adaptador de red tiene una dirección DLC o identificador DLC.

DNA (Distributed InterNet Application Architecture): Arquitectura de Microsoft para Aplicaciones Web.

DNS (Domain Name System): Protocolo utilizado para resolver nombres de Internet en direcciones IP.

E

E-learning: Es un sistema de formación cuya característica principal es que se realiza a través de internet o conectados a la red

EGP (Exterior Gateway Protocol): Protocolo utilizado para intercambiar información de ruteo entre diferentes sistemas autónomos.

EIA (Energy Information Administration): Es el organismo de estadística y de análisis en el Departamento de Energía de los Estados Unidos.

Estándares: Normas que permiten implementar, brindar o apoyar en un objetivo particular; y deben seguirse para que se cumpla de la mejor forma posible el objetivo.

Exploit: Es el medio que un atacante utiliza para aprovechar una vulnerabilidad con la finalidad de atacar un activo. Puede ser una secuencia de comandos o un fragmento de datos.

F

FDDI (Fiber Distributed Data Interface): Un estándar para transmitir datos por cable de fibra óptica, a la velocidad de alrededor de 100 millones de bits por segundo.

Firewall: Sistema que protege a un computadora o red de computadoras contra intrusiones.

Firma digital: Proceso que implica el cifrado de una cadena comprimida de datos, por medio de una clave secreta del firmante.

FTP (File Transfer Protocol): Protocolo que permite la transferencia de datos entre un cliente y un servidor.

G

Gigabyte: Múltiplo de Byte, unidad de almacenamiento de información. Se utiliza para dispositivos de gran capacidad, como discos duros y DVD. Véase Byte.

Gusano: Es un tipo de virus. Se trata de un programa que se copia a sí mismo hasta ocupar toda la memoria del disco. Para eliminarlo es necesario utilizar un programa antivirus.

H

HDLC (High-Level Data Link Control): es un protocolo de comunicaciones de propósito general punto a punto, que opera a nivel de enlace de datos.

Hash: Algoritmo matemático que transforma cualquier bloque arbitrario de datos en una nueva serie de caracteres con una longitud fija.

HTTP (Hypertext Transfer Protocol): Protocolo para la distribución y colaboración de sistemas de información de hipermedia.

I

ICMP (Internet Control Message Protocol): Protocolo que permite administrar información relacionada con errores de los equipos en red. No permite corregir los errores, sino que los notifica a los protocolos de capas cercanas.

IDS (Intrusion Detection System): Sistema encargado de monitorear el comportamiento de una red para detectar e informar sobre posibles intrusiones no autorizadas, con lo cual se puede prevenir que se vea afectada la integridad de la red.

IEEE (Institute of Electrical and Electronics Engineers): Asociación de profesionales norteamericanos que aportan criterios de estandarización de dispositivos eléctricos y electrónicos.

IFT (Instituto Federal de Telecomunicaciones): Es uno de los Órganos constitucionales autónomos de México, siendo el ente encargado de regular y supervisar las redes y la prestación de servicios de telecomunicaciones y radiodifusión en México.

IGMP (Internet Group Management Protocol): Protocolo que se utiliza para intercambiar información acerca del estado de pertenencia entre routers IP que admiten la multidifusión y miembros de grupos de multidifusión.

IGP (Interior Gateway Protocol): Protocolo responsable responsables de construir y mantener la información de ruteo dentro del dominio administrativo.

IMAP (Internet Message Access Protocol): Protocolo que ofrece la posibilidad de administrar e-mails directamente en el servidor de e-mail, estableciendo una cuenta de correo en el programa de e-mail.

Impacto: Consecuencias o efecto producido por un ataque.

Incidente: Es cualquier evento que afecte la continuidad del negocio y atente contra la confidencialidad, integridad o disponibilidad de la información.

Información: Comprende todo elemento intercambiado entre dispositivos.

Integridad. Asegura que los datos almacenados en los equipos y/o transferidos en una conexión no sean modificados sin la autorización correspondiente.

IP (Internet Protocol): Protocolo que tiene información de direccionamiento para el encaminamiento de paquetes y cuyas responsabilidades son entregar datagramas a través de la red basado en el mejor esfuerzo y ofrecer la fragmentación y el reensamblado de datagramas para soportar los enlaces de datos con tamaños diferentes de las Unidades de Transmisión Máxima (MTU).

IPS (Intrusion Prevention System)): Herramienta muy similar a IDS, pero que además de alertar sobre las detecciones también puede bloquearlas o prevenirlas en el momento de su detección.
IPsec (Internet Protocol security): Protocolo IP que permite a dos o más equipos comunicarse de forma segura.
IPX (Internetwork Packet eXchange): Protocolo de red de NetWare encargado de dirigir y enrutar los paquetes dentro de las LAN y entre ellas. IPX no garantiza que un mensaje llegue completo.
ISDN (Integrated Services Digital Network): Línea telefónica digital utilizada para proporcionar mayor ancho de banda. Es una tecnología ofrecida por las compañías telefónicas más importantes.
ISO (International Organization for Standardization): Organización de carácter voluntario fundada en 1946, que es la responsable de la creación de estándares internacionales en muchas áreas, incluyendo la informática y las comunicaciones.

K

Kerberos: Protocolo de seguridad creado por MIT que usa una criptografía de claves simétricas para validar usuarios con los servicios de red.
Kilobyte: Unidad de almacenamiento múltiplo del byte. Se abrevia como KB, y su equivalencia es: 1KB = 1024B

L

LAN (Local Area Network): Es una red de comunicación de datos que está situada habitualmente en un mismo edificio y que posibilita que las máquinas conectadas transmitan información de unas a otras mediante alguno de los protocolos existentes.
LDAP (Lightweight Directory Access Protocol): Conjunto de protocolos abiertos usados para acceder a la información guardada centralmente a través de la red.
LLC (Logical Link Control): Es uno de los protocolos que maneja la tecnología IrDA-Control. Lleva a cabo ciertas funciones de seguridad en las transferencias.

LMS (*L*earning Management System): Término que se asigna a un sistema informático desarrollado para la gestión de los recursos en línea, la distribución de los materiales del curso y permitir la colaboración entre estudiantes y profesores.

M

MAC (Media Access Control): Es un identificador numérico hexadecimal que identifica de forma única todas las tarjetas de red.

MAN (Metropolitan Area Network): Es la red utilizada en una pequeña población, para interconectar todos sus comercios, hogares y administraciones públicas.

Máscara de red: Sucesión de unos binarios que abarca la porción de Id de red y adicionalmente la porción que será tomada del Id de host para utilizarse como Id de subred.

Mecanismos de seguridad: Dispositivos o elementos para resguardar la información entre la red privada y la red externa.

Medio: Es la conexión que hace posible que los dispositivos se relacionen entre sí.

Modelo OSI (Open System Interconnection): Es un modelo de referencia para los protocolos de la red.

Moodle (Modular Object-Oriented Dynamic Learning Environment): Es una herramienta de gestión de aprendizaje (LMS), de distribución libre, escrita en PHP.

MTU (Maximum Transfer Unit): Es un parámetro que se establece para el protocolo TCP/IP, para definir el tamaño máximo del paquete de datos que puede ser enviado o recibido a través de la conexión, tanto de red local (intranet) como a Internet a través del protocolo.

N

NAT (Network Address Translation): Protocolo que traduce direcciones IP privadas en una dirección pública.

NBP (Name Binding Protocol): Protocolo de la red AppleTalk empleado para realizar la traducción de nombres de dispositivos a direcciones.

NCP (Network Control Protocol): Protocolo para el uso compartido de archivos que controla las comunicaciones de los recursos, los enlaces y las operaciones NDS entre equipos servidor y cliente en una red Novell NetWare.
NFS (Network File System): Protocolo que permite acceso remoto a un sistema de archivos a través de la red.
NIC (Network Interface Card): Dispositivo que permite la conexión en red de varias computadoras.
NIS (Network Information System): Protocolo de servicios de directorios cliente-servidor cuya función principal es el envío de datos de configuración en sistemas distribuidos tales como nombre de usuarios y host entre computadoras en una red.
No repudio. Este servicio protege contra usuarios que quieran negar falsamente haber enviado o recibido un mensaje.
NOM (Normas Oficiales Mexicanas): Son regulaciones técnicas de carácter obligatorio que establecen especificaciones y procedimientos para garantizar que los productos, procesos y servicios cumplan con requisitos mínimos de información, seguridad, calidad, entre otros.
Normas de facto (del hecho): Son normas que aparecieron y se desarrollaron sin ningún plan formal.
Normas de jure (por ley): Estándares formales y legales adaptados por algún organismo de estandarización autorizado.
NRM (Normal Response Mode): Es una configuración no balanceada del protocolos HDLC

O

OSI (Open Systems Interconnection): Modelo de trabajo en red introducido por la ISO para promover la interoperatividad entre múltiples fabricantes. Consiste en una descripción abstracta para el diseño de protocolos de red.

P

PAN (Personal Area Network): Es una red capaz de soportar los segmentos de 10 metros o más de longitud.

Proxy: Es un equipo informático que hace de intermediario entre las conexiones de un cliente y un servidor de destino, filtrando todos los paquetes entre ambos.

R

RARP (Reverse Address Resolution Protocol): Protocolo TCP/IP que sirve para determinar la dirección IP de un nodo de una red de área local conectada a Internet, cuando sólo se conoce la dirección del hardware.

Recurso: Es todo aquel elemento que forma parte de la red, y que puede ser identificado y accedido directamente.

Red de datos: Conjunto de dispositivos y software conectados entre sí mediante vías o medios de transmisión que comparten recursos, datos e información entre ellos de manera segura, eficiente y confiable.

Redes inalámbricas: Término que se utiliza para designar la conexión de los nodos de una red de datos sin necesidad de una conexión física (cables), ésta se da por medio de ondas electromagnéticas.

Riesgo: Posibilidad de la ocurrencia de un evento no deseado. En seguridad informática, es la probabilidad de que una amenaza logre explotar una vulnerabilidad, representando un impacto a la organización.

RIP (Routing Information Protocol): Protocolo usado en sistemas de conexión a internet en el que muchos usuarios se conectan a una red y pueden acceder por lugares distintos.

RPC (Remote Procedure Call): Protocolo que permite a un programa de computadora ejecutar código en otra máquina remota sin tener que preocuparse por las comunicaciones entre ambos.

S

SA (Sistema Autonomo): Es un grupo de redes de direcciones IP que son gestionadas por uno o más operadores de red que poseen una clara y única política de ruteo.

SAAS (Software as a service): Software como servicio (traducido al español) es un término utilizado para referirse a las aplicaciones basadas en la nube con las cuales es posible acceder desde internet.

SCP (Simple Control Protocol): Es un protocolo desarrollado por Microsoft que está optimizado para dispositivos con limitada memoria y poca capacidad de proceso y para redes con baja demanda de ancho de banda, como las económicas transmisiones a través de corrientes portadoras.

SDLC (Synchronous Data Link Control): Es un protocolo que se utiliza para transferir información sincrónica, transparente al código, bit por bit a través de una línea de comunicaciones.

Seguridad: Conjunto de protecciones que permiten resguardar un bien.

Seguridad perimetral: En una red de datos abarca los equipos que van desde el último punto de administración hasta las estaciones finales.

SFTP (Secure File Transfer Protocol): Este protocolo nos permite autenticarnos en los servidores sin usar usuario ni contraseña, sino el método de clave pública/privada.

Shellcode: Es una secuencia de bytes (opcodes) que representan instrucciones en ensamblador. Son parte esencial de muchos exploits, puesto que representan el payload. Se usa para ejecutar un código arbitrario, aunque históricamente se emplea para abrir un Shell en el sistema vulnerado.

Sistema: es un conjunto de elementos con relaciones de interacción e interdependencia que le confieren entidad propia al formar un todo unificado

SMB (Server Message Block): Protocolo de solicitud-respuesta y de cliente-servidor para compartir recursos.

SMTP (Simple Mail Transfer Protocol): Protocolo utilizado para la transferencia de mensajes y archivos adjuntos de correo electrónico.

SNA (Systems Network Architecture): Marco de comunicaciones ampliamente utilizado, desarrollado por IBM para definir funciones de red y establecer estándares que permitan a sus diferentes modelos de equipos intercambiar y procesar datos.

SNMO (Simple** N**etwork** M**anagement** P**rotocol):** Es utilizado entre la consola de administración de red y los dispositivos de la red (enrutadores, puentes y concentradores inteligentes) para colectar e intercambiar información.
SSH (Secure SHell): Protocolo que sirve para acceder a máquinas remotas a través de una red.
SPX (Sequenced Packet Exchange): Es un antiguo protocolo de red de Novell perteneciente al sistema operativo NetWare utilizado para controlar la entrega de datos a través de una red de área local.
Streams: Flujo de información que se transmite entre dispositivos.

T

TCP (Transmission Control Protocol): Servicio orientado a la conexión, se establece una sesión entre los hosts. Garantiza la entrega de los bloques de datos mediante el uso de confirmaciones y la entrega secuenciada de datos.
Telnet (Teletype Network): Protocolo utilizado para conectar con un equipo remoto a través de la red.
TFTP (Trivial** F**ile** T**ransfer** P**rotocol):** Protocolo utilizado para descargar los archivos iniciales necesarios para comenzar el proceso de instalación.
TIA (Telecommunications Industry Association): Es una asociación comercial de los Estados Unidos, que representa casi 600 compañías o empresas.
Topología: Es la forma en que los dispositivos que forman parte de la red están conectados entre sí.
Tráfico de relleno. Consiste en enviar tráfico espurio junto con los datos válidos para que el atacante no sepa si se está enviando información, ni qué cantidad de datos útiles se está transmitiendo.
Trama: Segmento de información enviada o recibida entre dispositivos.

U

UDP (User datagram protocol)): Servicio sin conexión, no se establece una sesión entre los hosts, no garantiza ni confirma la entrega de las unidades de datos y no las secuencia

UIT (Unión Internacional de Telecomunicaciones): Es el organismo especializado en telecomunicaciones de la Organización de las Naciones Unidas, encargado de regular las telecomunicaciones a nivel internacional entre las distintas administraciones y empresas operadoras.

Unicidad. Consiste en añadir a los datos un número de secuencia, la fecha y hora, un número aleatorio, o alguna combinación de los anteriores, que se incluyen en la firma digital o integridad de datos.

V

VLAN (Virtual Local Area Network): Agrupación lógica de hosts en una o varias LAN que permite la comunicación entre hosts como si estuvieran en la misma LAN física.

VLSM (Variable Length Subnet Masking): VLSM permite hacer un uso más eficiente de las redes más grandes y segmentarlas en subredes más pequeñas.

VPN (Virtual Private Network): Extensión de una red privada que abarca vínculos encapsulados, cifrados y autenticados en redes públicas o compartidas. Las conexiones VPN pueden proporcionar acceso remoto y conexiones enrutadas a redes privadas a través de Internet.

VSFTPD (very secure FTP daemon): es un servidor FTP para sistemas basados en Unix, incluido Linux. El programa fue creado para tener una protección muy robusta contra las posibles vulnerabilidades de FTP y soporta IPv6 y SSL.

Vulnerabilidad: Es un defecto o falla de seguridad en los sistemas que una o varias amenazas podrían aprovechar para causar un posible daño a ciertos activos o a toda la organización.

Vulnerabilidad de día cero: Son desconocidas por el fabricante (de una aplicación o sistema) y sus usuarios, hasta el día que se presentan los ataques dirigidos.

W

WAN (Wide Area Network): Es el conjunto de computadoras y dispositivos de red visible en Internet. La red que provee de servicio de conexión a un país o a un continente.

Z

ZIP (Zone Information Protocol): Protocolo que mantiene asignaciones de nombres de zona a números de red en enrutadores de Internet. ZIP es implementado principalmente por enrutadores.

Fuentes de información

¡Talent es lo que nos hace especiales! (s.f.). Recuperado el 22 de Diciembre de 2020, de TalentLMS: https://es.talentlms.com/features

¿En qué consiste un LMS y cómo funciona? (s. f.). Recuperado 28 de diciembre de 2020, de https://www.anahuac.mx/mexico/noticias/En-que-consiste-un-LMS-y-como-funciona

Acerca de Moodle. (7 de Noviembre de 2020). Recuperado el 22 de Diciembre de 2020, de moodle: https://docs.moodle.org/all/es/Acerca_de_Moodle

MoodleCloud Features. (s.f.). Recuperado el 22 de Diciembre de 2020, de MoodleCloud: https://moodlecloud.com/features/

Software como servicio (s.f). Recuperado el 7 de enero de 2020, de Azure Microsoft:https://azure.microsoft.com/es-es/overview/what-is-saas/

Thomas M. Haladyna, R. H. (2018). Preparación de preguntas de opciones múltiples para medir el aprendizaje de los estudiantes. Revista Iberoamericana de Educación, 76(1).

Uriarte Ramírez, J. R., & Arredondo Hernandez, E. P. (s. f.). Licenciatura en Informática del INSTITUTO TECNOLÓGICO DE CULIACÁN. Recuperado 2 de diciembre de 2020, de http://itcelenes.mx.tripod.com/

Universidad Nacional Autonoma de Mexico. (2015). *Plataformas libres para la educacion mediada por las TIC.* Ciudad de Mexico: Espacio Comun de Educacion Superior a distancia.