Asignatura: OPC13 – Cloud Computing

Ensayo de resultados de aprendizaje de la **semana 3**

Temas: Explore el enrutamiento de internet, Explore el hardware y el software, Explore las conexiones en la nube, Explore la redundancia digital

Integrantes:

David Maloof Flores Matrícula: 197589 a197589@uach.mx	Adrian Caleb Jaramillo Flores Matrícula: 367857 a367857@uach.mx	Abel González Mireles Matrícula: 361031 a361031@uach.mx	Ana Rebeca Moreno Reza Matrícula: 367783 a367783@uach.mx	Miguel David Rodríguez Glez. Matrícula: 343786 a343786@uach.mx

1. **Resumen Tema "Explore el enrutamiento de internet"**

   El protocolo Gateway Fronteriza (BGP / Border Gateway Protocol) es la manera en que se comunican los routers para conocer la mejor manera de enviar los paquetes (unidades de datos) hacia su destino específico.

   Los centros de datos son edificios especializados que cuentan con la tecnología para poder ser un centro de datos (alimentación, red y conectividad redundantes), estos crean las zonas de disponibilidad que ofrecen la capacidad de operar aplicaciones de producción y bases de datos que son diseñados para ser disponibles, tolerantes a fallas y escalables. Estos a su vez crean regiones que están compuestas por varias zonas de disponibilidad, estos se encuentran aislados para así tener tolerancia a los errores y estabilidad.

2. **Resumen Tema "Explore el hardware y el software"**

   Para que una computadora produzca una salida útil, su hardware y software deben trabajar en conjunto.

   Hardware: Consiste en los componentes físicos que conforman una computadora. Incluye muchos tipos de periféricos, ya sean externos(monitor, mouse, teclado,etc.) o internos(el disco duro, tarjeta de video, etc.), de entrada(monitor, impresora, etc.) o salida(teclado, mouse)

   Software: Consiste en los programas de la computadora y los datos relacionados que dan instrucciones al hardware de qué hacer y cómo hacerlo. Existen 3 tipos de software:

   Software del sistema: Son aquellos como el sistema operativo, el firmware y drivers.

Software de programación: Son aquellos que incluyen editores, linkers, debuggers y compiladores o intérpretes.

Software aplicado: Incluye programas de procesamiento de texto, software de hojas de cálculo, software de presentaciones, programas de diseño multimedia y editores de imágenes.

Los servicios relacionados a la nube usan máquinas virtuales las que emulan una computadora. Lo que permite ejecutar otros sistemas operativos sin afectar a tu sistema operativo actual.

3. **Resumen Tema "Explore las conexiones en la nube"**

Las tecnologías se vuelven más interdependientes con el paso del tiempo, o sea, cada vez más hay características de ciertas tecnologías dentro de otras tecnologías (por ejemplo, los teléfonos móviles incluyen cámaras digitales dentro de ellos) o hay tecnologías que colaboran entre sí.

Además, las tecnologías ayudan a las personas a trabajar entre ellas. Se han creado herramientas tecnológicas que permiten a la gente comunicarse entre sí, sin importar la distancia; aparte, existen aplicaciones que permiten a diferentes usuarios trabajar de manera síncrona o asíncrona dentro de un proyecto. Las tecnologías también aumentan la productividad de la gente, pues existen aplicaciones que facilitan el manejo de tiempo, además de que la tecnología en sí facilita ciertas tareas.

4. **Resumen Tema "Explore la redundancia digital"**

La conectividad a internet consiste en componentes tanto de software como de hardware. Existen múltiples dispositivos y caminos que los paquetes de datos pueden tomar al viajar. El router/modem de el ISP conecta ambos dispositivos al internet, la conexión puede ser alámbrica, inalámbrica o por fibra óptica, incluso existen cables submarinos que permiten la conexión de cualquier parte del mundo. Los routers son directores de trafico, ya que conectan redes y envían paquetes hasta que alcanzan su destino. Los paquetes pueden tener distintas rutas a un solo destino. Múltiples routers y caminos crean redundancia.

Bit: Es la contracción de "digito binario", es la unidad en que se mide la información en la informática, representada como cero o uno

Paquete: Es la información empaquetada como unidad y transferida de acuerdo al protocolo utilizado.

Dirección IP: Una dirección numérica asignada para cada dispositivo conectado a una red, consiste en un prefijo de red y una interfaz o identificador de host

ISP: Proveedor de servicios de internet (Internet Service Provider por sus siglas en inglés), una organización que provee el acceso a internet, tipicamente, mediante cable o fibra óptica

Modem: Dispositivo que crea una conexión en el hogar y se conecta a la red de un ISP, y por lo tanto, al internet. Mientras que el **Router** conecta una red con otra

Conexión por cable: Tipicamente referida como conexión Ethernet hacia la red

Conexión inalámbrica: Puntos de acceso inalámbricos y routers que entablan conexión inalámbrica, también conocida como WiFi, cuyo nombre era originalmente el nombre de una marca

Fibra óptica: Una conexión óptica de alta velocidad a internet.

Cable submarino: Un cable de comunicación recostado en los mantos acuíferos ubicado entre estaciones terrestres; los cables modernos utilizan fibra óptica para llevar el tráfico de internet.

Protocolos TCP/IP: Son modelos y set de protocolos que proveen comunicación de datos de extremo a extremo. El protocolo **IP** es utilizado para direccionamiento, mientras que el protocolo **TCP** es utilizado para garantizar las entregas de paquetes.

Los routers ayudan a llevar la dirección del tráfico de red, mediante una estructura jerárquica, donde los DNS (Domain Name System por sus siglas en inglés) actúan como un directorio telefónico, pero para el internet, cuando se introduce una dirección web o un URL, un servidor DNS se encarga de traducir dicha dirección a una dirección IP.

Si bien, internet es a día de hoy, una de las herramientas más utilizadas en nuestro día a día, también es necesario tener en cuenta los diversos riesgos y peligros que existen, como por ejemplo, los siguientes ataques maliciosos;

DoS: Un ataque de denegación de servicio (Denial of Service, por sus siglas en inglés), ocurre cuando usuarios legítimos, no son capaces de acceder a los sistemas de información, dispositivos u otros recursos de red, debido a ciber-amenazas de actores maliciosos.

DDoS: Un ataque de denegación de servicios distribuido (Distributed Denial of Service, por sus siglas en inglés) ocurre cuando múltiples máquinas operan juntas para atacar un objetivo, lo que permite enviar de manera exponencial solicitudes al objetivo, por lo tanto, se incrementa el poder de ataque, este tipo de ataques también hacen más complicado identificar el origen del ataque.

Código malicioso: Conocido tambíen como “Malware”, es primariamente una disrupción de un servicio, resultando en la pérdida de productividad y algunas veces pérdida de ingresos. Éstos están diseñados para robar información sensible.

Ransomware: El ransomware es un tipo de malware, diseñado para denegar el acceso a alguna computadora o datos, hasta que un ransom es pagado, típicamente se esparce mediante emails de phishing o por visitas a sitios web infectados.