

Asignatura: OPC13 – Cloud Computing

Ensayo de resultados de aprendizaje de la **semana 6**

Temas: Using the cloud.

Integrantes:

Chacón Orduño Martín
Eduardo
Matrícula: 351840
a351840@uach.mx

Cruz Juárez Guillermo
Matrícula: 352905
a352905@uach.mx

Ruiz Almeida Josue David
Matrícula: 358472
a358472@uach.mx

Mendoza Escarzaga Erick
Matrícula: 357307
a357307@uach.mx

1. Resumen del tema “Privacidad en línea”

En este tema nos damos cuenta de lo poco que sabemos sobre qué pasa con la información que compartimos en internet, lo poco que conocemos sobre lo que sucede con nuestros datos al subirlos a redes sociales. Algunos conceptos que se nos enseñaron en este curso fueron:

Web browser y cookies: Los buscadores web y la ip pueden mostrar tu ubicación. Y las cookies son archivos de texto que están guardados en tu dispositivo que pueden guardar la preferencia del usuario. y además indicar su ubicación.

Apps con acceso a tu ubicación: Algunas veces, cuando descargamos o usamos una aplicación, se nos pide compartir nuestra ubicación..

Dispositivos móviles: Estos dispositivos pueden identificar a cuál torre celular te estás conectando y su GPS puede obtener tu ubicación de manera precisa, además de que el historial de wifi se queda guardado. y revelado cuando nos conectamos a una red pública.

Tomarnos una selfie: pueden revelar nuestra ubicación.

Estos primeros conceptos son sobre cómo podemos revelar nuestra ubicación e información sensible de manera sencilla en la web, luego llegaron los conceptos sobre cómo proteger nuestra información, los cuales son:

HTTPS: El cual es un protocolo HTTP, pero seguro. el candado y el protocolo indican que nuestra información está viajando encriptada., nuestro buscador sabe confiar en sitios con HTTPS por medio de un certificado digital.

Autenticación: Por medio de usuario, contraseña o biométricos.

Requerimientos para contraseñas: que sean mínimo 8 caracteres, que tengan al menos una mayúscula, que contengan un carácter especial; todos estos requerimientos son para que sea más difícil adivinar o descifrar la contraseña.

2. Resumen del tema “Ciberseguridad”

El primer curso toma como principal los siguientes tres puntos para una mayor seguridad:

- **Autenticación:** Se le puede permitir el acceso a un sistema a un usuario mediante algo que sabe (contraseñas o pins), algo que contienen (token mediante correo o teléfono) y algo que son (datos biométricos).
- **Principio de mínimo privilegio:** Establece que los usuarios tienen roles que dependiendo de su posición pueden realizar más acciones o menos.
- **Autenticación multifactor:** Cuando se le pide al usuario que introduzca un código enviado a un correo o teléfono.

En el segundo curso es más extenso y trata sobre los diferentes tipos de ciberataques, y algunas prevenciones.

- **Ingeniería social:** Este tipo de ataque se basa en sacar información sensible al usuario sin que este se de cuenta, ejemplos de este tipo son el phishing (un correo pretendiendo ser alguien más) y man in the middle (Utilizar una red de internet interceptada).
- **Malware:** Se refiere a un programa malicioso que va desde los virus (infectar o dañar un sistema sin el consentimiento del usuario), trojan horse (un programa o herramienta legítimo que oculta malware), spyware (programa que recopila información sin que el usuario se de cuenta) y rootkit (programa que permite al atacante mantener el control del sistema sin ser detectado).

Además se toma en cuenta el modelo de seguridad **CIA Triad** para proteger información, este se conforma de:

- **Confidencialidad:** Solo la información debe ser accesible por personas autorizadas.
- **Integridad:** La información no debe ser alterada de manera no autorizada.
- **Disponibilidad:** Los datos y sistemas siempre deben estar disponibles.

Por último, se hace mención de los tipos de atacantes, white hackers (hacker ético que usa sus habilidades para proteger sistemas) y black hacker (hacker malicioso).

3. Resumen del tema “Seguridad de datos”

En este tema se nos presentan los conceptos clave de la ciberseguridad y cómo se relacionan entre sí a través de la Tríada CID. Lo primero que te dan a conocer son los principios del CID:

- **Confidencialidad:** Se refiere a que la información solo puede ser vista por personas autorizadas.
- **Integridad:** Garantiza que los datos no han sido alterados o manipulados.
- **Disponibilidad:** Asegura que los usuarios tienen acceso a la información cuando la necesitan.

Estos tres conceptos van de la mano, ya que para que un sistema sea seguro, debe proteger estos tres pilares de manera simultánea.

La seguridad de la información se divide en varios conceptos, los cuales son:

- **Confidencialidad:** Se basa en el principio del mínimo privilegio, donde el acceso se da solo a las personas que necesitan la información. Para lograrlo, se utilizan la autenticación (verificar quién eres) y la autorización.
- **Integridad:** Cuando la información se modifica de manera inesperada, se produce una pérdida de integridad. Las funciones hash son una forma de protegerla, ya que convierten las contraseñas en valores difíciles de revertir, evitando que la contraseña real se almacene.
- **Disponibilidad:** Se logra con la tolerancia a fallos, que considera los riesgos de desastres naturales o fallas de hardware. La informática en la nube ayuda a la alta disponibilidad al distribuir la infraestructura en varias regiones.

Y por último, el tema te da información sobre otros conceptos de seguridad como las vulnerabilidades (debilidades en un sistema) y las amenazas (lo que puede explotar esas debilidades).

4. Resumen del tema “Protección de la nube”

Aquí se aborda el tema de la seguridad de los datos, ya que la seguridad de los datos es parte de la ciberseguridad, y es principalmente asegurar la información de manera en que no ocurran cambios que la comprometan o se pierda, existen varias maneras de proteger y prevenir imprevistos, se puede:

- Hacer un respaldo
- Modelo de responsabilidad compartida
- Gestión de Identidad y Acceso
- Autenticación de múltiples factores

También se habla del PoLP(Principle of Least Privilege) que tiene con dar los permisos que necesite el usuario para realizar determinadas tareas sin que haga algo malo.

Además también se menciona que la autenticación de múltiples factores puede ser ya sean preguntas, apps o biométricos

