Asignatura: OPC13 – Cloud Computing

Ensayo de resultados de aprendizaje de la **semana 5**

Temas: Explore la privacidad en línea, Explore la ciberseguridad, Explore la seguridad de datos, Explore la protección de la nube

Integrantes:

Adrian Caleb Jaramillo Flores
Matrícula: 367857
a367857@uach.mx

Ana Rebeca Moreno Reza
Matrícula: 367783
a367783@uach.mx

Abel González Mireles
Matrícula: 361031
a361031@uach.mx

Miguel David Rodríguez González.
Matrícula: 343786
a343786@uach.mx

Docente:

David Maloof Flores
Matrícula: 197589
a197589@uach.mx

1. **Resumen Tema "Explore la privacidad en línea"**

   Si bien el Internet otorga la posibilidad de compartir información con conocidos y amigos, también le brinda esta oportunidad a desconocidos, de los que no se sabe cuál es el uso que le dan a la información que se comparte en el Internet día con día.

   Existen diferentes formas en las que la información de un individuo puede ser vulnerada; por ejemplo, se puede obtener la ubicación de una persona a través de su dirección IP, o a través de rastros que uno mismo deja en fotografías (literalmente mostrando dónde se encuentra alguien, o a través de los metadatos que van en la fotografía).

   No obstante, existen diversas maneras en las que uno puede proteger su información en Internet, por ejemplo el utilizar sitios web HTTPS, los cuales encriptan la información enviada, así como usar VPN mientras se está conectado a una red pública; aparte, se deben de crear contraseñas seguras.

2. **Resumen Tema "Explore la ciberseguridad"**

   Maneras de autenticación para usuarios de servicios en la nube;

   Existen 3 principales formas:

- Usando algo que saben
  - Un ejemplo, podría ser una contraseña, NIP o código

- Usando algo que tienen
    - Podría utilizarse algo como un número de teléfono donde se recibe una llamada o SMS
    - Alguna aplicación de autenticación
    - Un token basado en hardware que funcione de manera offline, etc.
- Usando algo que son
    - Para ésto podrían utilizarse datos biométricos físicos (huellas dactilares, escaneos de retina, etc.)
    - datos biométricos de comportamiento (patrones de escritura, reconocimiento de voz)

Otras formas de ayudar a la prevención de vulnerabilidades una vez que una cuenta de algún usuario ha sido comprometida es minimizar los privilegios, ésto se refiere a cuando un usuario o proceso se le otorga acceso solamente a los recursos necesarios para completar tareas específicas. Existen distintos tipos de privilegios:

- Administrador/Admin:
    - Si lo imaginamos como un árbol, éste se encontraría en la cima, éstos tienen acceso y la capacidad de hacer cambios en masa a lo largo del sistema entero.
- Lectura de información sensible:
    - Se encuentra por debajo del administrador, este tipo de permisos solamente tienen acceso a leer información, no editarla ni crearla, si éste tipo de cuentas fueran vulneradas, los atacantes solamente podrían leer la información que tienen disponible.
- Cuentas de uso común:
    - Este tipo de cuentas es para el uso de actividades de relevancia menor, como alguna clase específica.

Hackers de sombrero negro/black hat:

Son hackers que trabajan para hacer daño a otros.

Hackers de sombrero blanco/white hat

Trabajan en encontrar y arreglar brechas de seguridad

Ataques de phishing

Son aquellos en los que se recibe un email o mensaje de texto que aparenta ser legítimo, pero es en realidad un intento de robar información sensible.

3. Resumen Tema “Explore la seguridad de datos”

La seguridad es un tema de vital importancia al manejar datos que se suben al internet ya que pueden ser vulnerados (vulnerabilidad: debilidad de un sistema que puede ser explotado por una amenaza) en cualquier momento si no se tienen las precauciones adecuadas, esto inclusive si se usan recursos a través de la computación en la nube. Para estos temas de seguridad de la información se usa CID;

C → *confidencialidad* (solo personas autorizadas y autenticadas pueden ver la información precisa para la situación, es decir, estudiante → únicamente puede ver sus calificaciones con controles de acceso específicos para el mismo)

I → *Integridad* (La integridad de los datos no se manipula almacenada ni en tránsito, por ejemplo, con ayuda de HTTPS que cifra la información entre un cliente y un sitio web o un algoritmo HASH para protección de contraseñas)

D → *Disponibilidad* (Disponibilidad en el servicio y los datos con tolerancia a fallos considerando desastres naturales, cortes de energía y fallas de hardware, etc. así como también una alta disponibilidad gracias infraestructuras globales divididas en regiones geográficas)

El nivel de seguridad depende de las necesidades de los usuarios, la app y de la sensibilidad de la información que se encuentra contenida en las bases de datos. El principio de mínimo privilegio permite que únicamente las personas autorizadas y que requieran ver la información lo puedan hacer.

4. **Resumen Tema "Explore la protección de la nube"**

La seguridad de los datos es una parte importante de la ciberseguridad. Nos ayuda a direccionar la seguridad de nuestros datos en orden para prevenir cambios inesperados.

Algunos términos claves son:

Respaldo: Es un duplicado de datos, en caso de la pérdida de los datos principales.

Modelo de responsabilidad compartida: Un servicio de la nube que proporciona herramientas y métodos.

Identificar la gestión de accesos (IAM): Maneja el acceso de los usuarios al sistema.

Autenticación Multifactor (MFA): Esta autenticación requiere 2 o más elementos de autenticación para ser aceptada.

El principio del menos privilegiado (PoLP) está centrado en el concepto de que se debe aplicar el menor número de permisos aplicados a un usuario para añadir, modificar, o eliminar información.