Asignatura: OPC13 – Cloud Computing

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

Temas: Privacidad en línea, Ciberseguridad, Seguridad de datos, Protección de la nube

Integrantes:

Diego Pérez Prieto
Matrícula: 365341
a365341@uach.mx

Jared Alejandro Rosas Molina
Matrícula: 365337
a365337@uach.mx

1. Ensayo Tema "Explore privacidad en línea"

A través de internet, sin darnos cuenta compartimos información sensible tomar en cuenta que esta información es de acceso público, cualquiera puede acceder a ella, lo cual puede llegar a ser perjudicial para nosotros. Existen diversas maneras en las que nosotros compartimos información personal y puede que ni nos demos cuenta de que lo estamos haciendo, como lo son:

- Navegador web y Cookies: El historial de búsqueda y la dirección IP pueden mostrar ubicación, y las Cookies son archivos de texto que pueden almacenar tus preferencias e indicar, de igual manera que el navegador web, la ubicación
- Aplicaciones: Hay veces que hay aplicaciones que piden permisos para acceder al historial, contraseñas, ubicación y otra información del dispositivo
- Dispositivos móviles y relojes inteligentes: Tienen habilitado el GPS para seguir la ubicación, además de que el historial de Wi-Fi puede ser guardada y revelada a otros usuarios cuando un usuario se conecta a un punto de acceso inalámbrico
- Fotografías y redes sociales: En las fotografías queda guardado la metadata, que incluye ubicación, fecha y hora, mientras que en las redes sociales puedes dejar indicios de tu vida, como la ubicación y otros temas sensibles.

Existen diversas maneras en que las páginas web y servicios en la nube protegen tu información, usan características como la encriptación y certificados digitales, esto para que gente que comparte y accede a información sepa que la información está asegurada.

Alguno de los protocolos de seguridad es HTPPS (Hypertext transport protocol secure), que es un conjunto de reglas que permite que dos o más personas se comuniquen entre sí. Hay páginas que tienen un candado al lado izquierdo de la URL, esto indica que la información está encriptada, el navegador sabe que HTTPS sitios web confiar, esto basado en certificados digitales, que estos certificados son documentos que prueban la identidad de un sitio web.

2. Ensayo Tema "Explore la ciberseguridad"

Los desarrolladores, cuando sufren algún ataque que pone en riesgo la información, suelen reaccionar atacando el problema ya conocido. Sin embargo, lo ideal es que, desde la creación de la aplicación, se piense en las posibles vulnerabilidades para prevenir intentos de hackeo, ya que siempre existirán riesgos y amenazas en línea.

Existen varios tipos de amenazas en línea. Por ejemplo:

- Ingeniería social: Consiste en engañar a los usuarios para que proporcionen información sensible. Algunos ejemplos son el phishing y los ataques man-in-the-middle.
- Malware: Es software malicioso diseñado para realizar acciones no autorizadas que afectan la integridad, confidencialidad o disponibilidad de un sistema de información. Algunos ejemplos son los virus, troyanos, spyware y rootkits.

El Internet fue creado principalmente para compartir información y, con la llegada del comercio en línea, se volvió necesario implementar medidas de seguridad. Por ello se desarrolló un modelo diseñado para proteger el hardware, el software, las políticas y los procedimientos: la tríada CIA (Confidentiality, Integrity, Availability). Este modelo busca que la información:

- No sea revelada a usuarios no autorizados (confidencialidad).
- No sea modificada por usuarios no autorizados (integridad).
- Sea accesible para los usuarios autorizados cuando la necesiten (disponibilidad).

Como usuarios, debemos adoptar buenas prácticas para proteger nuestras cuentas. Por ejemplo, usar contraseñas privadas, únicas, largas y complejas para evitar accesos no autorizados.

En la nube existen distintas formas de autenticar la identidad de los usuarios:

- Algo que saben: Contraseña o PIN.
- Algo que tienen: Número de teléfono, mensaje SMS, USB, Bluetooth o NFC.
- Algo que son: Datos biométricos como huellas dactilares o reconocimiento por voz.

Para impedir que un sistema sea vulnerado con facilidad, es necesario incorporar métodos de autenticación adicionales, dificultando así los intentos de acceso no autorizado. Además, es recomendable asignar roles a cada usuario, de modo que cada uno tenga acceso únicamente a la información necesaria para sus funciones. En caso de que un usuario sea comprometido, el acceso del atacante será limitado. En el caso del administrador, se deben aplicar las medidas de seguridad más estrictas para impedir que su cuenta sea hackeada.

3. Ensayo Tema "Seguridad de datos"

Los sistemas en la nube no estan libres de ataques malignos para el robo de información, pueden tener distintas vulnerabilidades, las cuales son debilidades que pueden ser más desarrollados por una o varias amenazas, donde estas amenazas pueden ser generadas dentro de la organización o fuera de esta misma, donde un sistema necesita de seguridad, la cual depende completamente de las necesidades de los usuarios y que tan sensibles es la información. La seguridad se compone de distintas capas, una de ellas es utilizar un marco de seguridad que se llama CID, que por sus siglas significa Confidencialidad, Integridad y Disponibilidad. La confidencialidad de los datos, es aquella que permite que

solo las personas autorizadas puedan ver ciertas cosas, dando acceso a los datos solo a los usuarios que necesitan de esa información mediante un control de acceso, los cuales van a indicar que es lo que un usuario puede hacer y que no.

La integridad de los datos, es aquella que hace que los datos no sean modificados cuando son mandados de un lugar a otro o cuando se guardan, una manera de mantener la integridad es mediante el hashing de contraseñas, lo cual, pasa la contraseña mediante una función matematica, la cual con su resultado no se puede obtener su origen, donde con estos algoritmos permiten guardar la contraseña con un valor hash sin tener que guardar la contraseña de manera legible, por si en dado caso de un ataque, no se tenga acceso a las contraseñas de los usuarios, junto con esto, la conexión HTTPS también cifra la información mandada entre cliente – servidor pero puede ser igual de vulnerable.

La disponibilidad de los datos, permite que la información pueda estar a disposición del cliente que los requiere cuando sea necesario, para lograr esto se tiene que tener una buena tolerancia a los fallos, es decir, prevenir distintos escenarios como son las fallas electricas, falla en el software o hardware de donde se almacenan los datos, o tener una buena seguridad ante ciertos ataques ciberneticos de las personas, y para lograr esta tolerancia, muchas empresas han dividido su infraestructura en distintos puntos alrededor del mundo, donde si uno de estos puntos llega a fallar, los demás contienen la misma información haciendo que se redireccionen hacía ese centro de datos para poder seguir teniendo acceso a los datos.

4. Ensayo Tema “Protección de la nube”

En la protrección de la nube o ciberseguriad, tener los datos de los usuarios es bastante crucial e importante, debido a que esto permite que la información no se pierda o o sufra cambios que no se esperan gracias a un error en el sistema o por una persona o un grupo de personas que intentan hacer un robo de información. Existen distintas maneras de tener una protección de la información:

- Tener un respaldo de los datos: Usualmente es usada para cuando se pierden datos, este es un segundo lugar de guardado de datos y estan siempre disponibles.
- Compartir la responsabilidad: Este se refiere a que los servicios en la nube dan herramientas y métodos para proteger la información, pero el usuario tiene la responsabilidad de implementar la seguridad que el servicio ofrece.
- Gestión de Identidad y Acceso: Permite tener un control sobre los usuarios que necesitan acceder a cierta información, mediante la autenticación de credenciales del usuario, la autorización de las credenciales y que permisos tienen asignados, y a partir de estos permisos que acciones pueden realizar junto a que datos pueden acceder.
- Autenticación multifactor: Este tipo de autenticación, necesita varias partes de información, independientes entre si, para identificar al usuario, como lo es el que son, que tienen o el que saben.

El principio del privilegio minimo (PoLP) se centra en dar la menor cantidad de permisos a las personas para agregar, modificar o eliminar información, lo cual permite tener una seguridad dentro de un proyecto, ya que no cualquier persona tendra el permiso de hacer una modificación dentro de una base de datos, pero puede ser un problema si la cuenta o el dispositivo con el que se tiene acceso se daña o se pierde, lo cual para esto, se puede hacer un respaldo o darle acceso de solo lectura (principio del privilegio minimo) a otra persona para descargar los datos.