

Asignatura: OPC13 – Cloud Computing

Ensayo de resultados de aprendizaje de la **semana 7**

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

Integrantes:

Emiliano Piñón Marín
Matrícula: 367860
a367860@uach.mx

Luisa Fernanda Hernández
Hernández
Matrícula: 368068
a368068@uach.mx

Mauricio Elías Navarrete
Flores
Matrícula: 367785
a367785@uach.mx

1. Resumen Tema “Explore la privacidad en línea”

Es muy fácil compartir información personal en aplicaciones web como redes sociales o foros de internet. Muchas veces se nos puede escapar fácilmente algo personal, así que hay maneras de protegernos de estos errores comunes o impensables. La información personal que solemos exponer incluye:

- Navegador web y cookies: El historial del navegador y la dirección IP pueden mostrar nuestra ubicación. Las cookies pueden almacenar datos precargados de nuestras preferencias, incluyendo datos sensibles como información de tarjetas de crédito o débito.
- Aplicaciones con acceso a la ubicación: Muchas aplicaciones solicitan permisos para acceder a funciones del dispositivo como ubicación, cámara, etc. Debemos ser cuidadosos al momento de conceder estos permisos.
- Redes sociales y fotos: Las líneas de tiempo de fotos y su registro en redes sociales pueden revelar ubicaciones actuales o incluso dónde vivimos.

Las únicas redes seguras son las propias. Al navegar por redes abiertas como las de un café o institución, una forma segura de conectarnos y mantener nuestros datos cifrados es a través de una VPN, es una red privada virtual que nos ayuda a cifrar nuestros datos y mantenerlos seguros en transacciones de datos o consultas en redes abiertas.

Para proteger mejor nuestras cuentas, es recomendable utilizar la autenticación de múltiples factores. Este protocolo hace que cualquier persona que intente acceder necesite aprobar dos o más métodos de verificación, dificultando significativamente el acceso a posibles intrusos, también si lo podemos combinar con una contraseña fuerte y segura, al combinar diferentes caracteres y que no esté ligada a nada personal

2. Resumen Tema “Explore la ciberseguridad (2 cursos)”

El objetivo principal de la ciberseguridad es proteger la confidencialidad, integridad y disponibilidad de la información, conocido como CIA. La confidencialidad evita que los datos sean vistos por personas no autorizadas, la integridad asegura que no se alteren sin permiso, y la disponibilidad garantiza su acceso cuando se necesite. Desafortunadamente, existen numerosas amenazas en línea que buscan vulnerar estos principios.

Los atacantes utilizan diversas estrategias para comprometer nuestros datos y sistemas. Las más frecuentes son:

- Ingeniería Social: Técnicas para engañar a los usuarios y conseguir que revelen información sensible. Dos ejemplos claros son:
- Phishing: Mensajes o correos aparentemente legítimos que buscan robar credenciales como contraseñas, nombres de usuario o datos bancarios.
- Ataque de "Man-in-the-middle": Cuando un atacante intercepta comunicaciones entre dos partes sin ser detectado, como al usar redes Wi-Fi públicas no seguras.
- Malware: Software dañino diseñado para comprometer sistemas. Puede afectar cualquier aspecto de la Tríada CIA. Incluye virus, troyanos, spyware y rootkits.

Para protegernos de estas amenazas, debemos implementar prácticas de seguridad efectivas.

La primera defensa es usar contraseñas seguras. Una buena contraseña debe ser larga y compleja, combinar diversos caracteres y evitar información personal. Para manejar varias contraseñas de forma segura, es mejor utilizar un gestor de contraseñas.

3. Resumen Tema “Explore la seguridad de datos”

Una vulnerabilidad es una debilidad en un sistema, por lo que la seguridad de la información busca preservar la disponibilidad, confiabilidad e integridad de los datos y recursos del sistema.

La Triada CID es un marco de seguridad donde la C significa confidencialidad, la I integridad y la D disponibilidad.

La confidencialidad consiste en que solo las personas autorizadas tienen acceso a la información, para ello se debe autenticar a los usuarios y debe haber un control de acceso. La integridad es porque la información no ha sido manipulada, para ello se usa la criptografía, que se usa en HTTPS (cifra la información enviada entre un cliente y un servidor web), mensajes cifrados y contraseñas hash. La disponibilidad quiere decir que los datos y servicios están disponibles cuando sea necesario

4. Resumen Tema “Explore la protección de la nube”

La seguridad de datos es una parte esencial de la ciberseguridad. Ayuda a tener resguardados nuestros datos y prevenir perdidas o cambios en ellos a causa de errores de los usuarios, hackers o personas que buscan dañar dicha información. Algunas herramientas que nos ayudan con la protección de datos son las siguientes:

- Backups.- una segunda área donde se encuentre una copia de todos los datos importantes y que esté disponible en caso de algún problema con la fuente primaria de la información.
- The shared responsibility model.- ceder parte de las tareas de protección de datos a el proveedor de servicios en la nube con la que se está trabajando.
- IAM.- sistemas de autorización para cada proceso relacionado con las bases de datos. No cualquier persona es apta para realizar ciertas acciones y por tanto es necesario una constante autorización e identificación.
- MFA.- autenticaciones que utilicen más de un recurso independiente del primero para comprobar la identidad de los usuarios.

El principle of least privilege se centra en el concepto de otorgar la mínima cantidad de permisos que necesita cada tipo de usuarios. De esta forma se evita que algunos grupos tengan acceso a herramientas de la base de datos que no les son de utilidad y tener mayormente identificado quienes pudieron haber cometido ciertas acciones.