Ensayo Confidencialidad vs Integridad.

Instrucciones. El alumno deberá de realizar un ensayo de la Confidencialidad vs Integridad (Pag. 22-29), interpretando cada uno de los diagramas que se encuentran en la Sesion02_UC2.

La confidencialidad y la integridad, son dos de las tres características fundamentales de la seguridad informática, necesarias para tener un sistema robusto y mejor protegido ante ataques y vulnerabilidades. Al observar cada uno de los sistemas de cifra de la presentación siendo los sistemas simétricos (cifrado con clave secreta) y asimétricos (cifrado con llave pública), se puede analizar el papel de cada uno de estos conceptos en el cifrado de datos.

En el primer diagrama podemos observar el funcionamiento de los criptosistemas de clave secreta simétricos, un mensaje en texto plano es cifrado a través de una clave única, transmitido a través de un medio, y posteriormente es descifrado por el receptor con dicha clave, pero claro, en base a esto existe el problema de como hacer llegar la clave única al receptor para poder descifrar el mensaje de manera segura, es aquí donde entra la confidencialidad y es que en estos criptosistemas simétricos recae el mantener en secreto las claves privadas para el cifrado y descifrado del mensaje, existe la confidencialidad siempre y cuando dichas claves se mantengan en secreto por lo que es una responsabilidad demasiado grande que cae únicamente en mantener el secreto. Estos sistemas de clave secreta por lo tanto utilizan algoritmos de cifrados para ocultar el mensaje de manera protegida que posteriormente se mueve a través de un medio de transmisión criptograma para ser decodificada y convertida a su estado original de texto base, manteniendo la integridad y confidencialidad.

Para los sistemas con clave pública se cifran los mensajes de manera diferente, primero un mensaje es protegido por el emisor con su llave privada, y se utiliza la llave pública del receptor para mantener el mensaje confidencial, al pasar por este medio se cifra y descifra el contenido con la llave privada del receptor y la llave público del emisor manteniendo la información íntegra.

A diferencia de la confidencialidad, la integridad por su parte, prioriza la rectitud y confiabilidad del mensaje y el evitar posibles alteraciones o inconsistencias en su proceso de envío y recepción, mientras que la confidencialidad, se enfoca en evitar que el mensaje sea interceptado por un intruso.

El funcionamiento de los criptosistemas asimétrico puede definirse como más confiable, ya que utiliza más métodos de seguridad para mantener el mensaje oculto a intrusos, su confidencialidad por lo tanto es mayor a los sistemas simétricos e incluye características para preservar su integridad de manera más compleja.