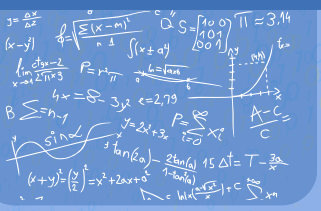
¿QUÉ ES EL HASHING?

UNAM CERT

El hashing es un proceso matemático que toma una entrada y la convierte en una cadena llamada **hash.**

La entrada puede ser texto de diferente longitud, así como documentos, contraseñas, imágenes, archivos multimedia, etc.

La función hash procesa las entradas mediante una serie de operaciones matemáticas para producir un valor.



Existen muchos algoritmos, pero los más populares y seguros son:

SHA-256

Usado en criptomonedas (Bitcoin), verificación de integridad de archivos, firmas digitales.

SHA-3

Usado para de identificadores únicos en sistemas distribuidos o blockchain.

Argon2

Usado para proteger contraseñas.

Con el avance de la computación cuántica, los algoritmos de hashing tradicionales podrían volverse vulnerables a los ataques cuánticos.

El NIST (National Institute of Standards and Technology) está trabajando en el desarrollo de funciones hash seguras para la era cuántica.

El resultado final es una cadena de caracteres alfanuméricos que representan esa entrada, conocida como hash. Cada hash es único.

HOLA → **DA3B5AA765D6154FW44RA**

Las funciones de hash permiten verificar la integridad de archivos descargados. Si el hash de un archivo descargado de internet coincide con el hash original, el archivo no ha sido alterado.

Bibliografía: Neil, I. (2020). CompTIA Security+ : SY0-601 Certification Guide: Complete coverage of the new CompTIA Security+ exam to help you pass on the first attempt (2nd ed.). Packt Publishing.