Parte A

1.

MD5: Sigue siendo usado, principalmente para confirmar la integridad de un archivo. Ya no se usa en muchos campos ya que no es muy seguro.

SHA-2 (256, 384, 512): Se siguen usando en varios campos. Se usan en múltiples protocolos como TSL, SSH entre otros, también es usado en los sistemas unix para el hasheo de las contraseñas. Las cripto monedas también usan este algoritmo para funcionar.

Parte B

1.

Datos que debes ser protegidos:

-Toda la información de los clientes.

-Toda la información que intercambian las unidades de distribución con los servidores.

Esto porque esta es la información que viaja por internet, el resto de información viaja dentro de la oficina que esta protegida por un firewall y los computadores dentro de esta tienen antivirus.

2.

Para la información de los clientes y para la información de las unidades de distribución se necesita confidencialidad, integridad, autenticación y no-repudio.