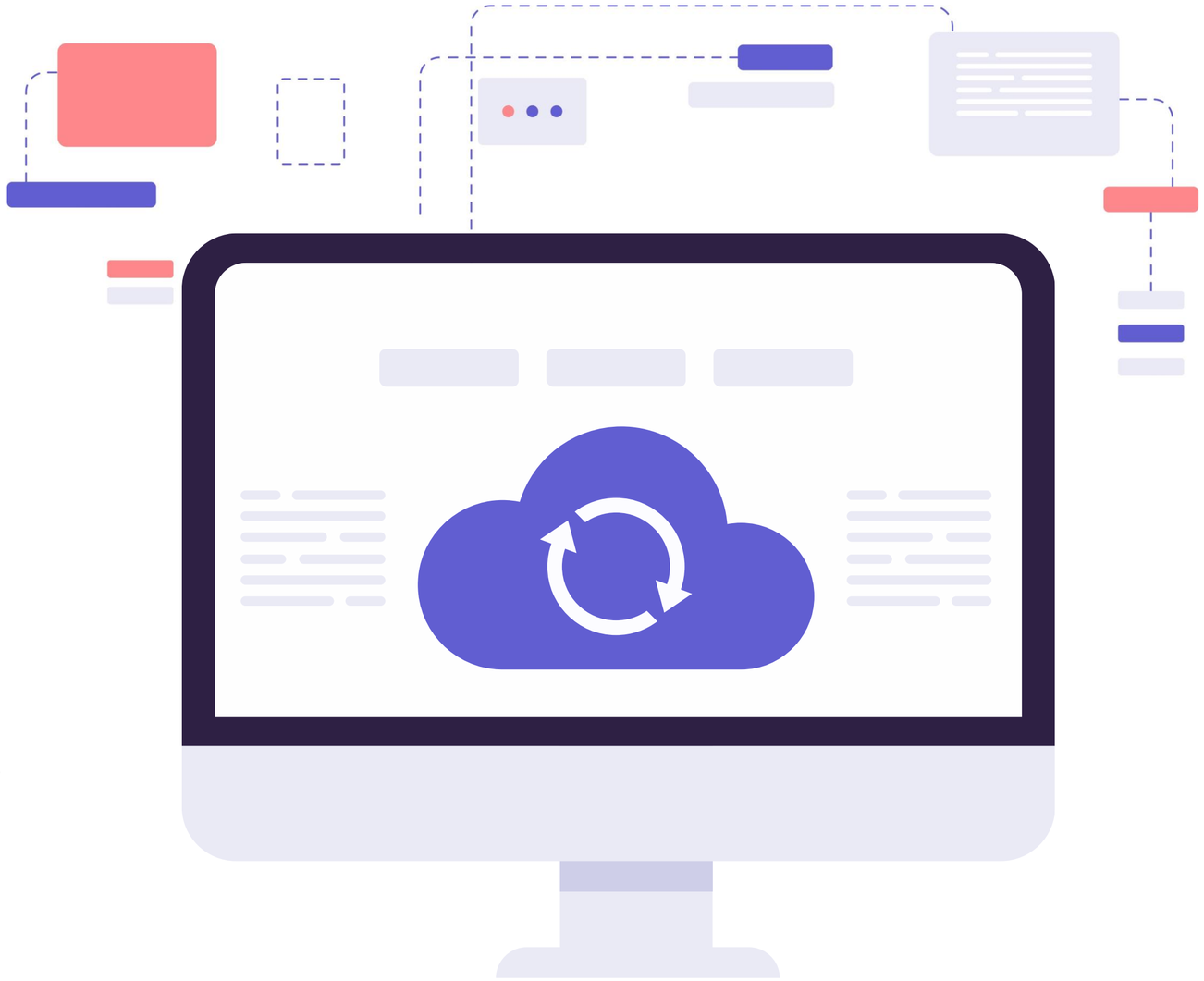
Ministerio de Educación
Gobierno de Chile

UNIVERSIDAD CATÓLICA DE TEMUCO

PROTOCOLOS DE CIFRADO, INTEGRIDAD Y AUTENTICACIÓN



Módulo 8: Sistemas Operativos de Redes.

Telecomunicaciones

Perfil de Egreso - Objetivos de Aprendizaje de la Especialdad

Módulo 1

OA1 Leer y utilizar esquemas, proyectos y en general todo el lenguaje simbólico asociado a las operaciones de montaje y mantenimiento de redes de telecomunicaciones.

Módulo 2

OA6 Realizar mantenimiento y reparaciones menores en equipos ysistemas de telecomunicaciones, utilizando herramientas y pautas de mantención establecidas por el fabricante.

OA7 Aplicar la normativa y los implementos de seguridad y protección relativos almontaje y el mantenimiento de las instalaciones de telecomunicaciones y la normativa del medio ambiente.

Módulo 3

OA2 Instalar equipos y sistemas de telecomunicaciones de generación, transmisión, repetición, amplificación, recepción, y distribución de señal de voz, imagen y datos, según solicitud de trabajo y especificaciones técnicas del proyecto.

OA10 Determinar los equipos y sistemas de comunicación necesarios para una conectividad efectiva y eficiente, de acuerdo a los requerimientos de los usuarios.

Módulo 4

OA9 Detectar y corregir fallas en circuitos de corriente continua de acuerdo a los requerimientos técnicos y de seguridad establecidos.

Módulo 5

OA2 Instalar equipos y sistemas de telecomunicaciones de generación, transmisión, repetición, amplificación, recepción y distribución de señal de voz, imagen y datos, según solicitud de trabajo y especificaciones técnicas del proyecto.

OA4 Realizar medidas y pruebas de conexión y de continuidad de señal eléctrica, de voz, imagen y datos- en equipos, sistemas y de redes de telecomunicaciones, utilizando instrumentos de medición y certificación de calidad de la señal autorizada por la normativa vigente.

Módulo 6

OA8 Instalar y configurar una red inálambrica según tecnologías y protocolos establecidos.

OA7 Aplicar la normativa y los implementos de seguridad y protección relativos al montaje y el mantenimiento de las instalaciones de telecomunicaciones y la normativa del medio ambiente.

Módulo 7

OA5 Instalar y configurar una red de telefonía (tradicional o IP) en una organización según los parámetros técnicos establecidos.

Módulo 8

OA3 Instalar y/o configurar sistemas operativos en computadores o servidores con el fin de incorporarlos a una red laN, cumpliendo con los estándares de calidad y seguridad establecidos.

Módulo 9

OA10 Determinar los equipos y sistemas de comunicación necesarios para una conectividad efectiva y eficiente, de acuerdo, a los requerimientos de los usuarios.

OA6 Realizar el mantenimiento y reparaciones menores en equipos y sistemas de telecomunicaciones, utilizando herramientas y pautas de mantención establecidas por el fabricante.

Módulo 10

No está asociado a Objetivos de Aprendizaje de la Especialidad (AOE), sino a genéricos. No obstante, puede asociarse a un OAE como estrategia didáctica.

Perfil de Egreso – Objetivos de Aprendizaje Genéricos

A- Comunicarse oralmente y por escrito con claridad, utilizando registros de habla y de escritura pertinentes a la situación laboral y a la relación con los interlocutores.	**B-** Leer y utilizar distintos tipos de textos relacionados con el trabajo, tales como especificaciones técnicas, normativas diversas, legislación laboral, así como noticias y artículos que enriquezcan su experiencia laboral.	**C-** Realizar las tareas de manera prolija, cumpliendo plazos establecidos y estándares de calidad, y buscando alternativas y soluciones cuando se presentan problemas pertinentes a las funciones desempeñadas.
D- Trabajar eficazmente en equipo, coordinando acciones con otros in situ o a distancia, solicitando y prestando cooperación para el buen cumplimiento de sus tareas habituales o emergentes.	**E-** Tratar con respeto a subordinados, superiores, colegas, clientes, personas con discapacidades, sin hacer distinciones de género, de clase social, de etnias u otras.	**F-** Respetar y solicitar respeto de deberes y derechos laborales establecidos, así como de aquellas normas culturales internas de la organización que influyen positivamente en el sentido de pertenencia y en la motivación laboral.
G- Participar en diversas situaciones de aprendizaje, formales e informales, y calificarse para desarrollar mejor su trabajo actual o bien para asumir nuevas tareas o puestos de trabajo, en una perspectiva de formación permanente.	**H-** Manejar tecnologías de la información y comunicación para obtener y procesar información pertinente al trabajo, así como para comunicar resultados, instrucciones e ideas.	**I-** Utilizar eficientemente los insumos para los procesos productivos y disponer cuidadosamente los desechos, en una perspectiva de eficiencia energética y cuidado ambiental.
J- Emprender iniciativas útiles en los lugares de trabajo y/o proyectos propios, aplicando principios básicos de gestión financiera y administración para generarles viabilidad.	**K-** Prevenir situaciones de riesgo y enfermedades ocupasionales, evaluando las condiciones del entorno del trabajo y utilizando los elementos de protección personal según la normativa correspondiente.	**L-** Tomar decisiones financieras bien informadas, con proyección a mediano y largo plazo, respecto del ahorro, especialmente del ahorro previsional, de los seguros, y de los riesgos y oportunidades del endeudamiento crediticio así como de la inversión.

Marco de Cualificaciones Técnico Profesional (MCTP) Nivel 3 y su relación con los OAG

HABILIDADES

1. Información

1.Analiza y utiliza información de acuerdo a parámetros establecidos para responder a las necesidades propias de sus actividades y funciones.
2.Identifica y analiza información para fundamentar y responder a las necesidades propias de sus actividades.

2. Resolución de problemas

1.Reconoce y previene problemas de acuerdo a parámetros establecidos en contextos conocidos propios de su actividad o funcion.
2.Detecta las causas que originan problemas en contextos conocidos de acuerdo a parámetros establecidos.
3.Aplica soluciones a problemas de acuerdo a parámetros establecidos en contextos conocidos propios de una función.

3. Uso de recursos

1.Selecciona y utiliza materiales, herramientas y equipamiento para responder a una necesidad propia de una actividad o función especializada en contextos conocidos.
2.Organiza y comprueba la disponibilidad de los materiales, herramientas y equipamiento.
3.Identifica y aplica procedimientos y técnicas específicas de una función de acuedo a parámetros establecidos.

4. Comunicación

4. Comunica y recibe información relacionada a su actividad o función, a través de medios y soportes adecuados en contextos conocidos.

APLICACIÓN EN CONTEXTO

5. Trabajo con otros

1.Trabaja colaborativamente en actividades y funciones coordinándose con otros en diversos contextos.

6. Autonomía

1.Se desempeña con autonomía en actividades y funciones especializadas en diversos contextos con supervisión directa.
2.Toma decisiones en actividades propias y en aquellas que inciden en el quehacer de otros en contextos conocidos.
3.Evalua el proceso y el resultado de sus actividades y funciones de acuerdo a parámetros establecidos para mejorar sus prácticas.
4.Busca oportunidades y redes para el desarrollo de sus capacidades

7. Ética y responsabilidad

1.Actúa de acuerdo a las normas y protocolos que guían su desempeño y reconoce el impacto que la calidad de su trabajo tiene sobre el proceso productivo o la entrega de servicios.
2.Responde por cumplimiento de los procedimientos y resultados de sus actividades.
3.Comprende y valora los efectos de sus acciones sobre la salud y la vida, la organización, la sociedad y el medio ambiente.
4.Actúa acorde al marco de sus conocimientos. experiencias y alcance de sus actividades y funciones

CONOCIMIENTO

8. Conocimientos

1.Demuestra conocimientos especificos de su área y de las tendencias de desarrollo para el desempeño de sus actividades y funciones.

Metodología seleccionada

Demostración guiada

- Esta presentación les ayudará a poder comprender los conceptos necesarios para el desarrollo de su actividad.

Aprendizaje Esperado

- **AE5.** Evalúa la seguridad de una red utilizando técnicas de criptografía, reconocimiento, escaneo, proponiendo recomendaciones en un informe de hallazgos y brechas de seguridad encontrados.

¿Qué vamos a lograr con esta actividad para llegar al Aprendizaje Esperado (AE)?

Identificar cómo se aplican los algoritmos y protocolos de cifrado, integridad y autenticación.

¿Cómo pueden evitar que alguien lea sus archivos personales?

¿Qué es el cifrado de datos?

- En términos simples, es convertir los datos a un formato codificado (ilegible) y esto se utiliza para garantizar la inviolabilidad de la información enviada.

Fuente imagen: https://www.redeszone.net/app/uploads-redeszone.net/2017/02/Herramientas-descifrado-ransomwares.jpg

¿Cuáles son los algoritmos de cifrado?

- En la actualidad existe el cifrado simétrico y asimétrico.

  - **Cifrado Simétrico:** Posee la misma clave para cifrar y descifrar la información.

  Ejemplos:

  1. *DES.*
  2. *3DES.*
  3. *AES.*

Fuente imagen: https://encrypted-tbn0.gstatic.com/images?q=tbn%3AANd9GcTYfM-hgfqENm-bLCWlZ1TFDWIJUKg43n3J2oKzZ3QWNGz6ogSN8kkz_zOeCc_MDRibYJNDpCI8NnbYVz427MNCR3mrR8XtPuqVGw&usqp=CAU&ec=45707744

¿Cuáles son los algoritmos de cifrado?

- **Cifrado asimétrico:** En este caso se generan dos claves, las cuales se relacionan entre sí. Por ejemplo, si tengo clave A y B, si utilizo la clave A para cifrar, utilizaré la clave B para descifrar o viceversa. Es importante que una de estas claves sea privada y la otra pública.

  Ejemplo:

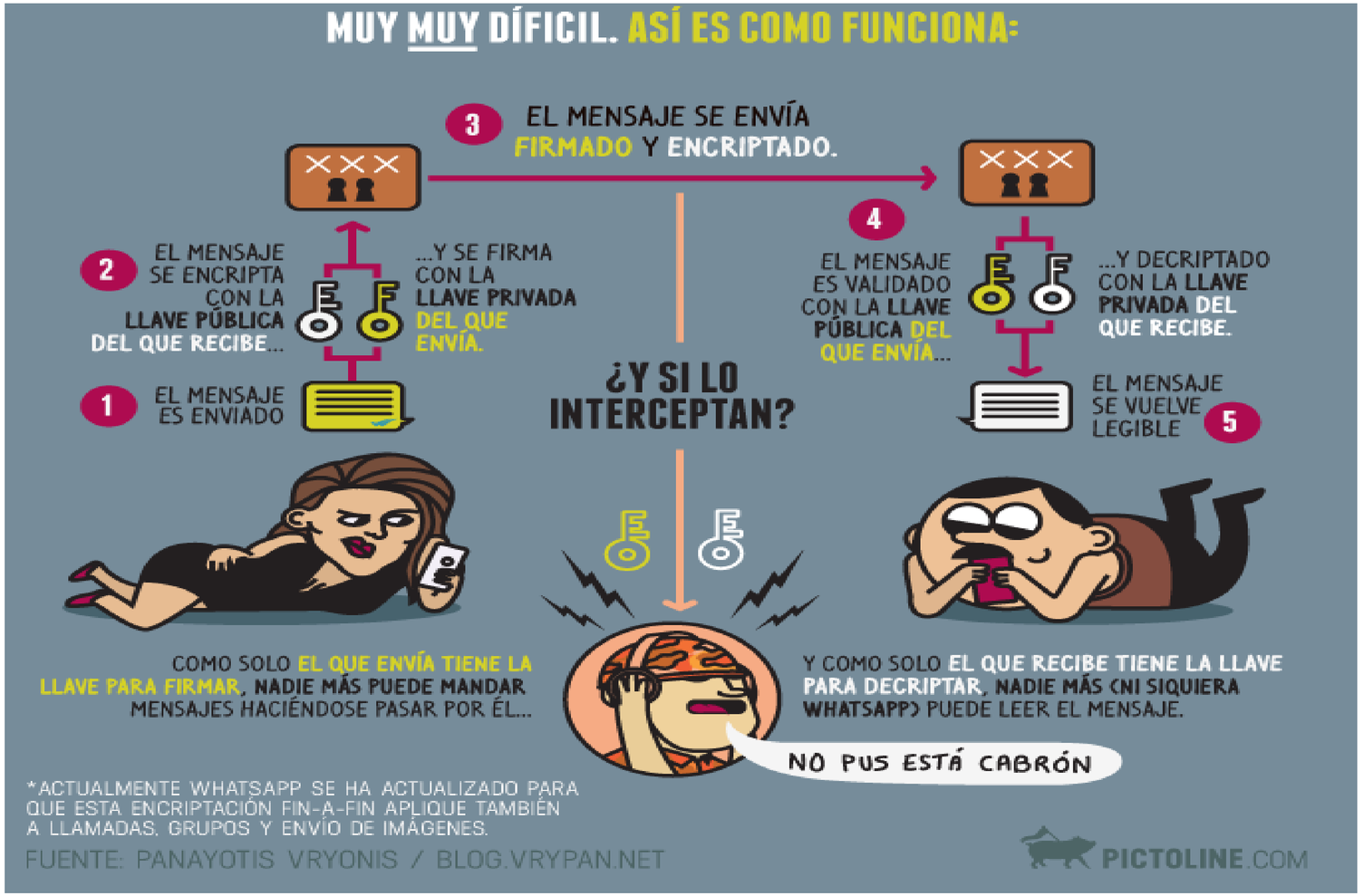
  Algoritmo RSA.

Fuente imagen: https://virtual.itca.edu.sv/Mediadores/cms/cifrado_asimetrico.PNG

Pregunta de Reflexión

¿Qué tan fácil creen ustedes es que se filtren sus conversaciones de Whatsapp?

Respuesta



Fuente imagen:
https://www.altavoz.net/altavoz/blog/desarrollo/que-es-la-criptografia-asimetrica-y-por-que-es-importante

¿Qué se entiende por la integridad a un archivo?

Cuando hablamos de integridad de un archivo, se refiere a que éste no pueda modificarse dado el riesgo que conlleva.

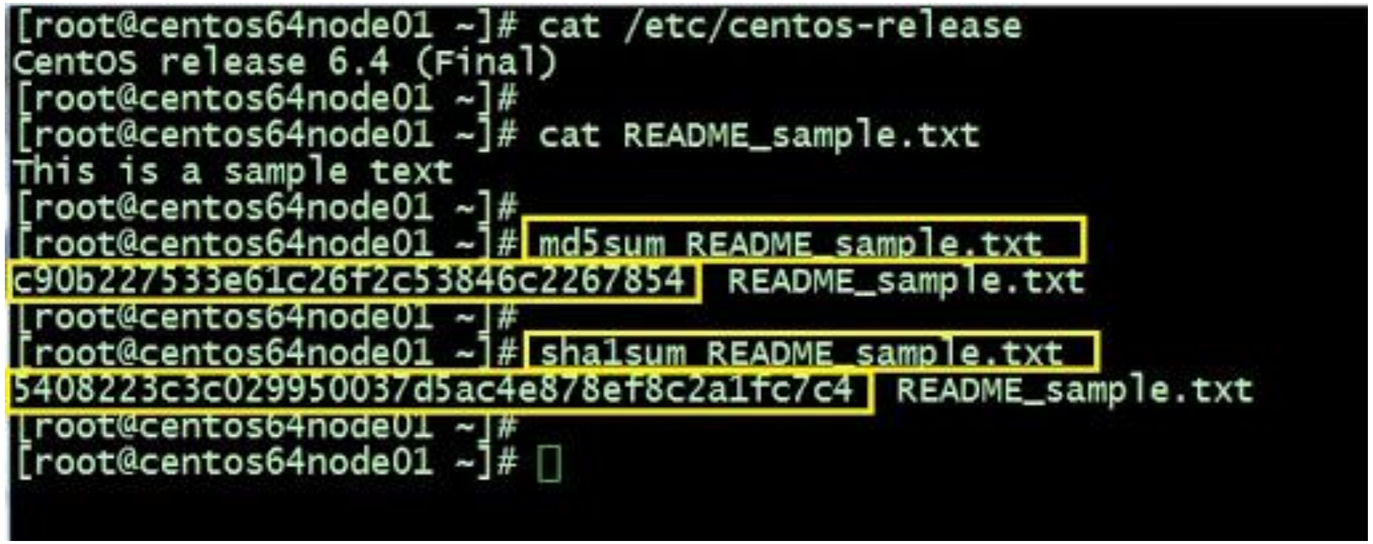
Por ejemplo, si se configura un archivo para levantar un servidor web y este archivo es modificado debido a un ataque, entonces la integridad del archivo se ve afectada. Esto se puede detectar comparando los HASH de ambos archivos.

¿Cuáles son los algoritmos que proporcionan integridad a un archivo ?

Los algoritmos más utilizados para comprobar que un archivo no haya sido modificado y entrega un HASH son:

1. *MD5.*
2. *SHA.*

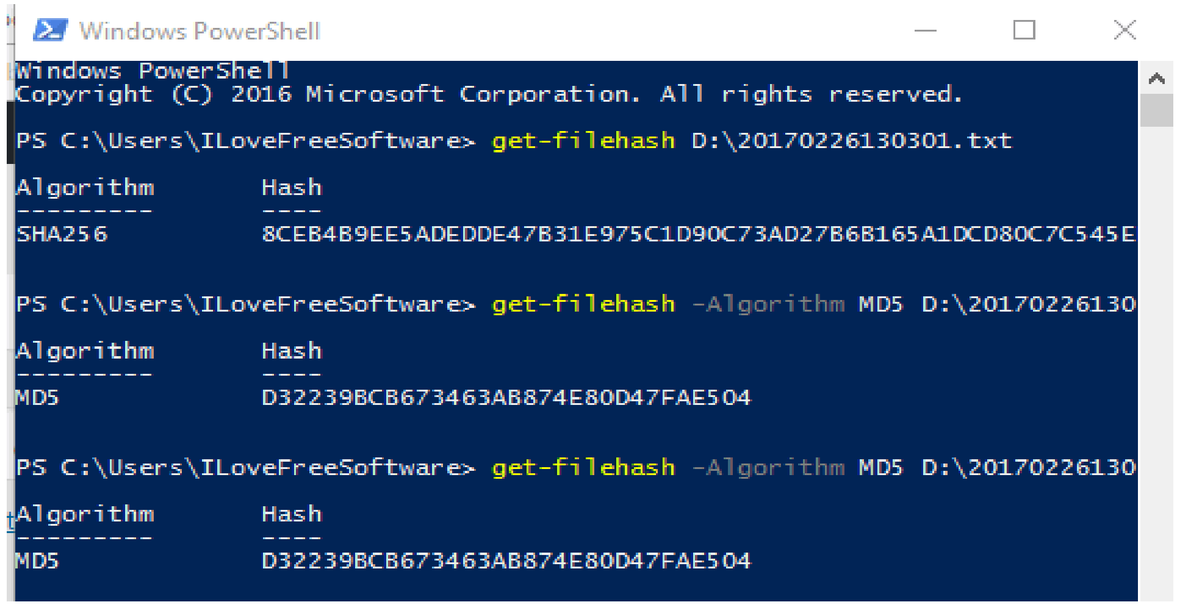
Ejemplos de MD5 Y SHA en Linux



Fuente imagen:
http://geekswing.com/geek/getting-md5-and-sha-1-has-values-on-linux-aix-and-windows/

Como se puede apreciar en la imagen, con el comando MD5 y SHA al aplicarlo al archivo nos entrega un código llamado HASH.

Ejemplos de MD5 Y SHA en Windows



Fuente imagen: *https://www.ilovefreesoftware.com/03/windows-10/calculate-hash-value-file-using-powershell-windows-10.html*

Como se puede apreciar en la imagen, con el comando MD5 y SHA al aplicarlo al archivo nos entrega un código llamado HASH.

Pregunta de reflexión

¿Alguien me puede decir un ejemplo personal donde cree sería necesario aplicar integridad a su información?

¿Qué es la autenticación?

- La autenticación es la forma que permite verificar la identidad de una persona o usuario que requiera acceder a un servicio, aplicación, dispositivo, etc.

- Además, permite identificar un servidor o un servicio y asegura la confidencialidad.

Fuente: https://conceptodefinicion.de/autenticacion/

Formas de autenticación de una persona:

- **Algo que soy:** Tiene que ver con autenticación Biométrica. Ejemplo:
  - *escáner de retina.*
  - *huella digital.*
- **Algo que sé:** Tiene que ver con alguna información que yo conozco. Ejemplo:
  - *usuario y contraseña.*
- **Algo que tengo:** Tiene que ver con alguna información sincrónica en el tiempo. Ejemplo:
  - *Token (el que entregan los bancos*).

Formas de autenticación de un dispositivo

Algo que tiene: Alguna información que posee el dispositivo. Ejemplo:

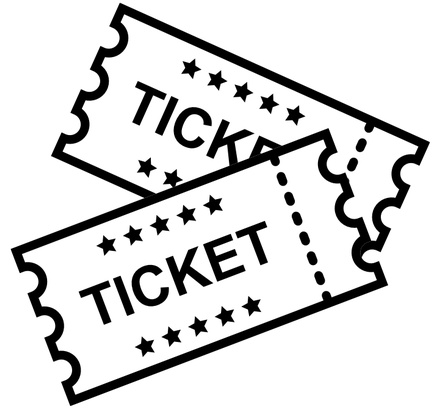
- *IP.*
- *MAC.*
- *Nombre del dispositivo.*
- *Certificado Digital.*

Reflexionemos

¿Cuál cree usted que sería una buena política de autenticación de una persona?

¿Les ha tocado autenticarse de alguna de las formas expuestas? ¿Dónde?

Ticket de salida



01

De manera individual responde, ¿qué algoritmo MD5 o SHA utilizaría para verificar la integridad de un archivo?

02

¿Por qué si AES es el algoritmo más robusto para el cifrado de datos se continúa integrando en los sistemas algoritmos como DES O 3DES?

03

En pares, describan lo que a su parecer sería una política de seguridad robusta a nivel de autentificación.

REFERENCIAS DE CONTENIDO:

- https://www.ciscopress.com/store/ccna-cyber-ops-secfnd-210-250-official-cert-guide-9781587147029
- https://latam.kaspersky.com/resource-center/definitions/encryption