Ministerio de Educación
Gobierno de Chile

UNIVERSIDAD CATÓLICA DE TEMUCO

Protocolos de cifrado, integridad y autenticación

Módulo 5: Configuración de la seguridad en redes de área local

Conectividad y Redes

Perfil de Egreso – Conectividad y redes

Módulo 1	**OA1** Leer y utilizar técnicamente proyectos de conectividad y redes, considerando planos o diagramas de una red de área local (red LAN), basándose en los modelos TCP/IP y OSI. **OA3** Instalar y mantener cableados estructurados, incluyendo fibra óptica, utilizados en la construcción de redes, basándose en las especificaciones técnicas correspondientes. **OA7** Instalar y configurar una red inalámbrica según tecnologías y protocolos establecidos.
Módulo 2	**OA2** Instalar y configurar sistemas operativos en computadores personales con el fin de incorporarlos a una red LAN, cumpliendo con los estándares de calidad y seguridad establecidos. **OA11** Armar y configurar un equipo personal, basándose en manuales de instalación, utilizando las herramientas apropiadas y respetando las normas de seguridad establecidos.
Módulo 3	**OA8** Aplicar herramientas de software que permitan obtener servicios de intranet e internet de manera eficiente.
Módulo 4	**OA4** Realizar pruebas de conexión y señales en equipos y redes, optimizando el rendimiento de la red y utilizando instrumentos de medición y certificación de calidad de la señal, considerando las especificaciones técnicas.
Módulo 5	**OA5** Aplicar métodos de seguridad informática para mitigar amenazas en una red LAN, aplicando técnicas como filtrado de tráfico, listas de control de acceso u otras.
Módulo 6	**OA9** Mantener y actualizar el hardware de los computadores personales y de comunicación, basándose en un cronograma de trabajo, de acuerdo a las especificaciones técnicas del equipo.
Módulo 7	**OA10** Mantener actualizado el software de productividad y programas utilitarios en un equipo personal, de acuerdo a los requerimientos de los usuarios.
Módulo 8	**OA6** Aplicar procedimientos de recuperación de fallas y realizar copias de respaldo de los servidores, manteniendo la integridad de la información.
Módulo 9	No esta asociado a Objetivos de Aprendizaje de la Especialidad (OAE), 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 ocupacionales, 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

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 específicos de su área y de las tendencias de desarrollo para el desempeño de sus actividades y funciones.

Metodología seleccionada

Demostración guiada

- Esta presentación te servirá para avanzar paso a paso en el desarrollo de la actividad propuesta.

Aprendizaje Esperado

- **5.4.** 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. Algunos ejemplos

- DES
- 3DES
- AES

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

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:**

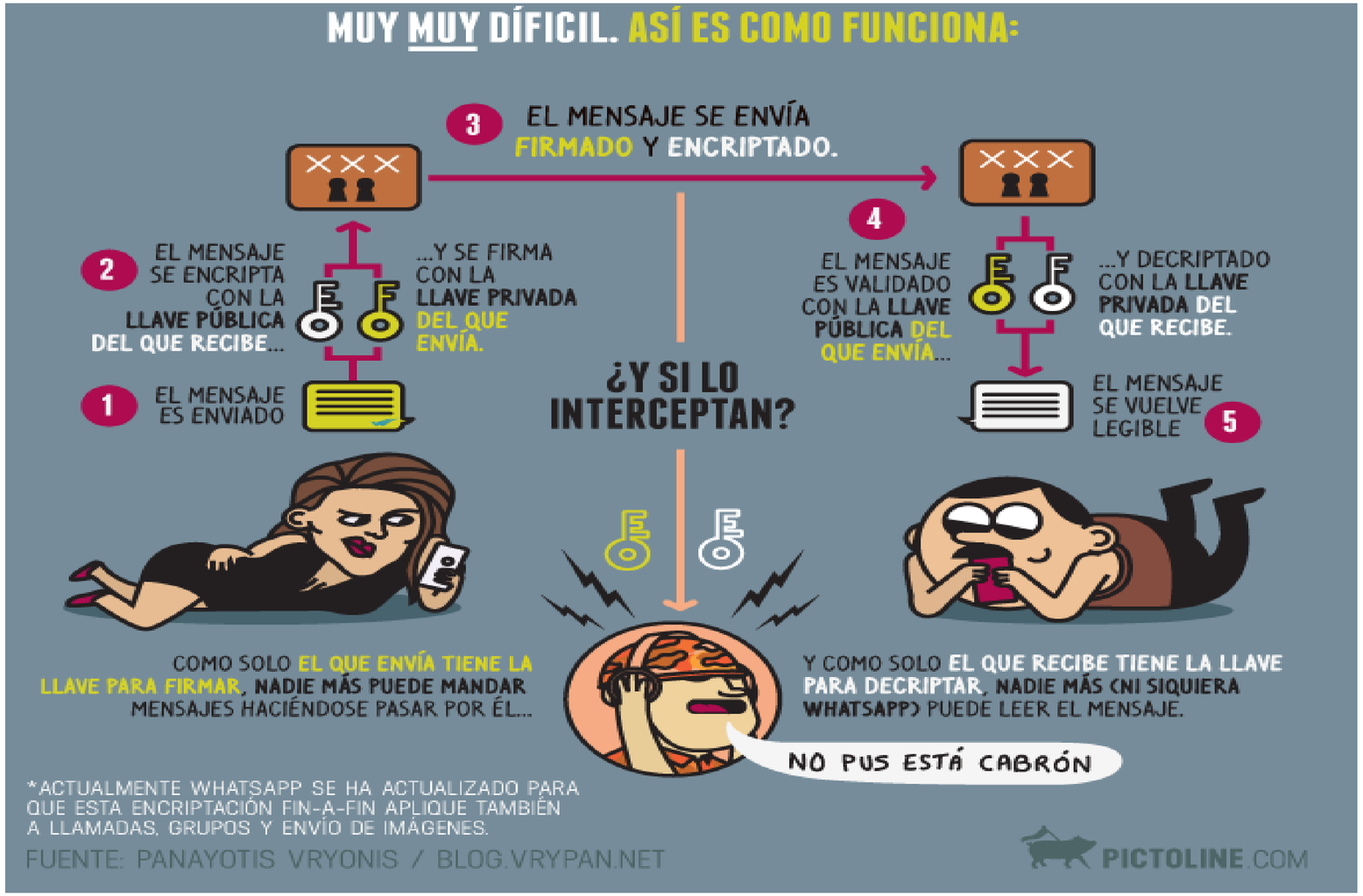
  Algoritmo RSA.

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?

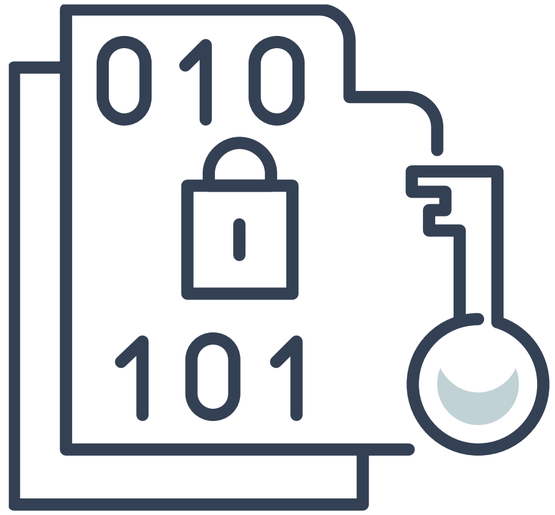
- Cuando hablamos de integridad de un archivo, se refiere a que éste no pueda modificarse **dado el riesgo que conlleva.**

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.*

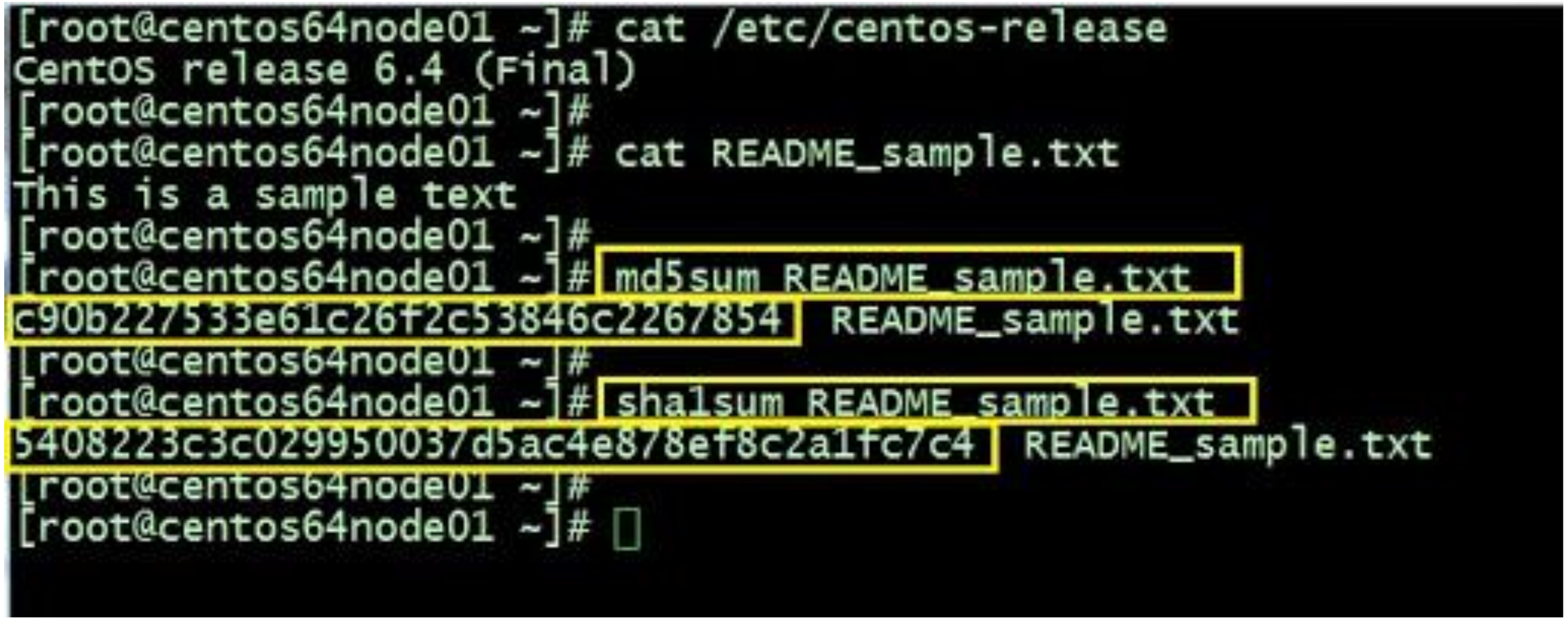
¿Cuáles son los algoritmos que proporcionan integridad a un archivo?

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

- **MD5.**
- **SHA.**



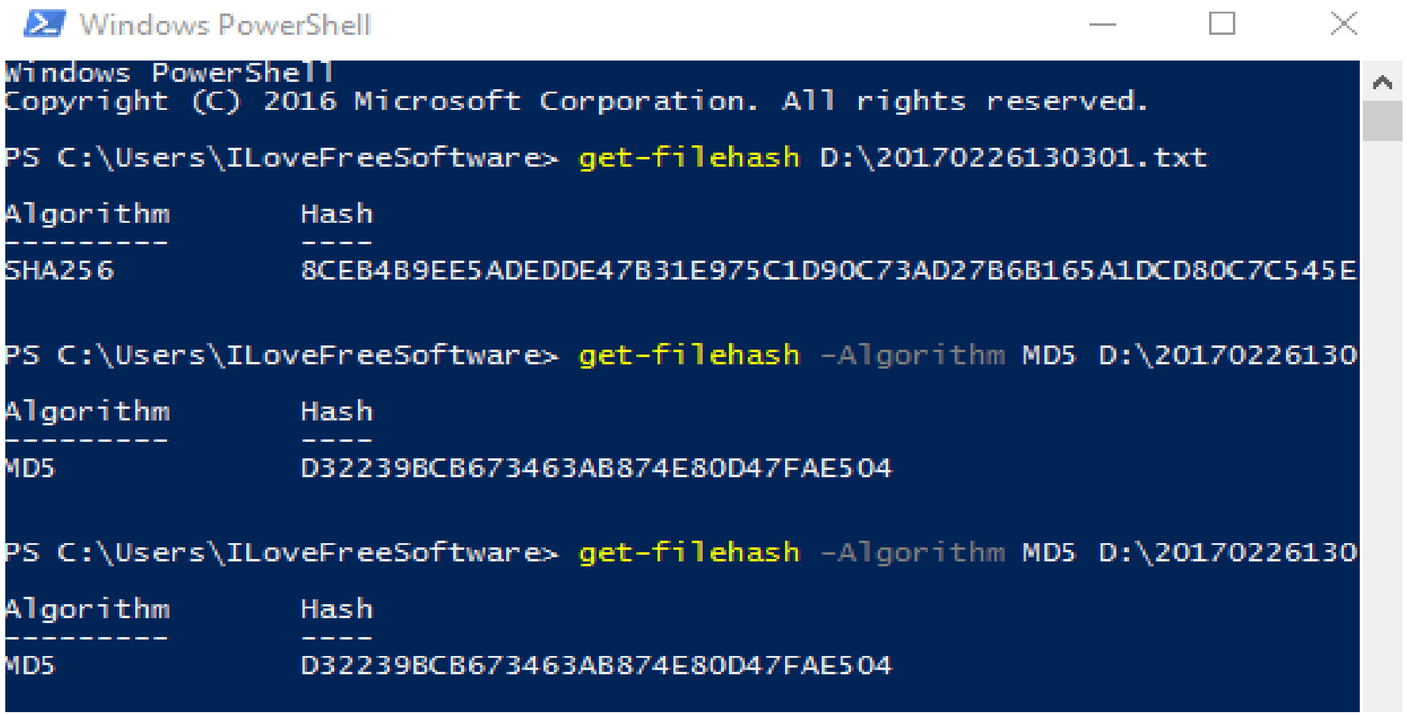
Ejemplos de MD5 Y SHA en Linux



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.

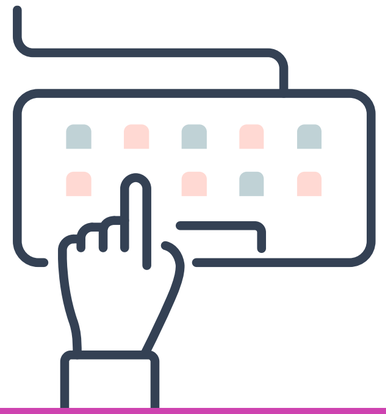
Ejemplo:

- **Escáner de retina.**
- **Huella digital.**

Algo que se: 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.**

Preguntas de Reflexión

¿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

¿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 sigue integrando algoritmos como DES O 3DES en los sistemas?

03

Describe la que, a tú parecer, sería una política de seguridad robusta a nivel de autenticación.

Referencias

https://www.ciscopress.com/store/ccna-cyber-ops-secfnd-210-250-official-cert-guide-9781587147029

https://latam.kaspersky.com/resource-center/definitions/encryption