Ciberseguridad con Inteligencia Artificial

Sesión 1

Dr. Vitali Herrera Semenets (vherrera@cenatav.co.cu)

MSc. Felipe Antonio Trujillo Fernández (felipe.trujillo@ibero.mx)

MSc. Joshua Ismael Haase Hernández (joshua.Haase@ibero.mx)

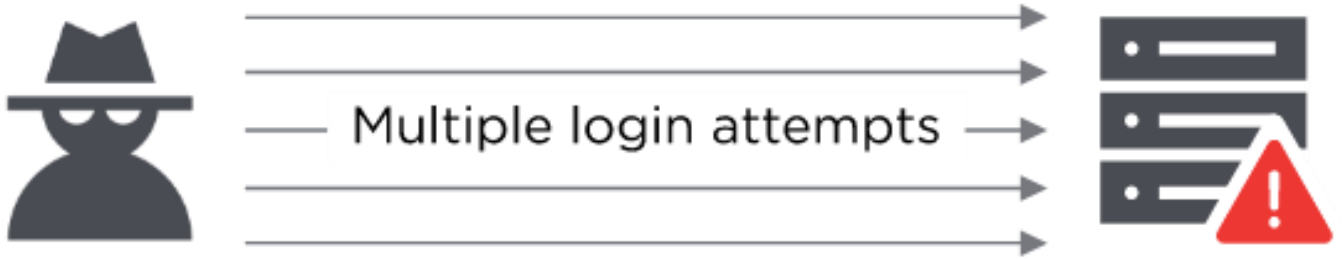
Dr. Lázaro Bustio Martínez (lazaro.bustio@ibero.mx)

Introducción

¿Por qué son importantes las contraseñas?

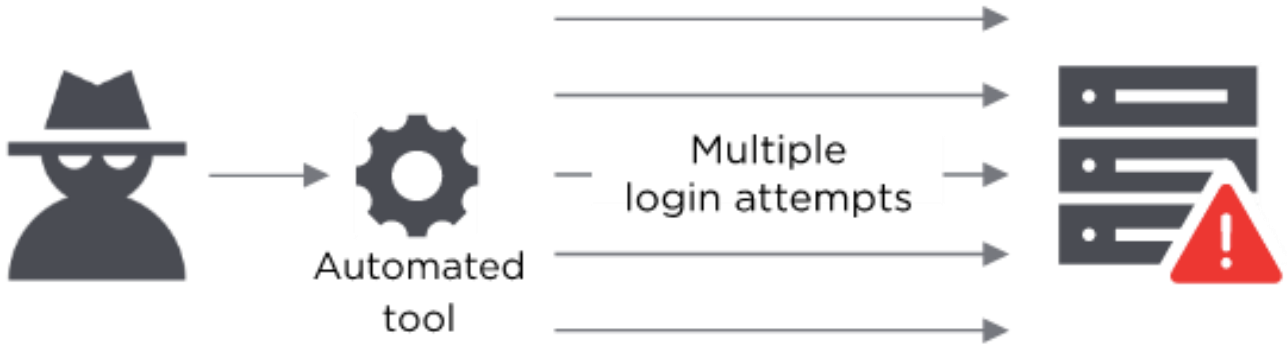
- Defensa inicial: Las contraseñas actúan como la primera línea de defensa contra ataques cibernéticos.
- Protección de datos: Ayudan a salvaguardar la integridad de nuestra información confidencial.

Ataques de contraseña



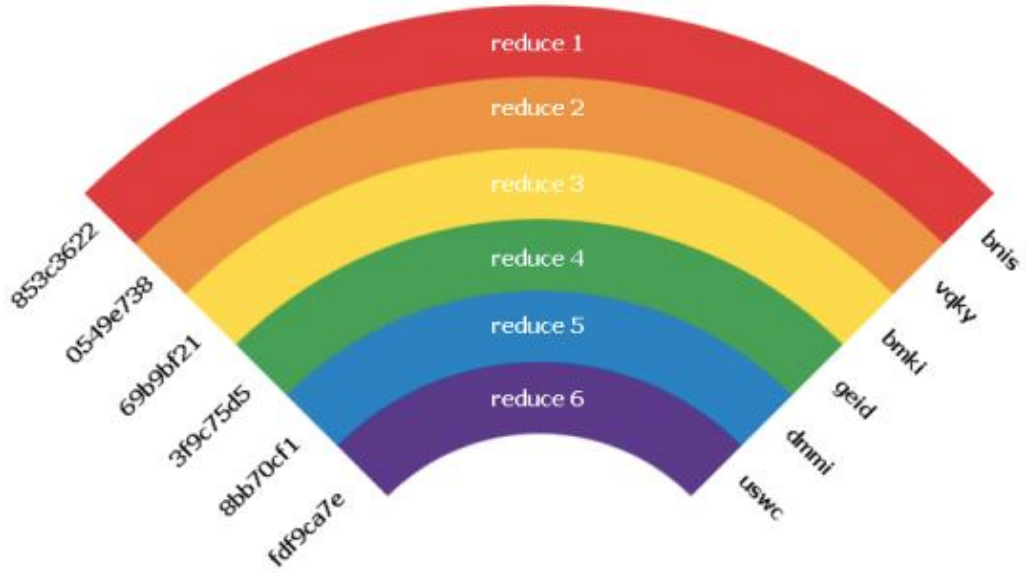
Ataque de diccionario	Se aprovecha de que los usuarios tienden a utilizar palabras comunes y contraseñas cortas.
	Se utiliza una lista de palabras comunes (**el diccionario)**, y se evalúan, a menudo con números antes y/o después de las palabras.
	Suele ser común su aplicación en escenarios empresariales.

Ataques de contraseña



Fuerza bruta	Se usan programas para generar contraseñas probables o incluso conjuntos de caracteres aleatorios.
	Comienzan con contraseñas débiles de uso común, como Contraseña123 y continúan desde allí.
	Suelen también evaluar variaciones de caracteres en mayúsculas y minúsculas.

Ataques de contraseña

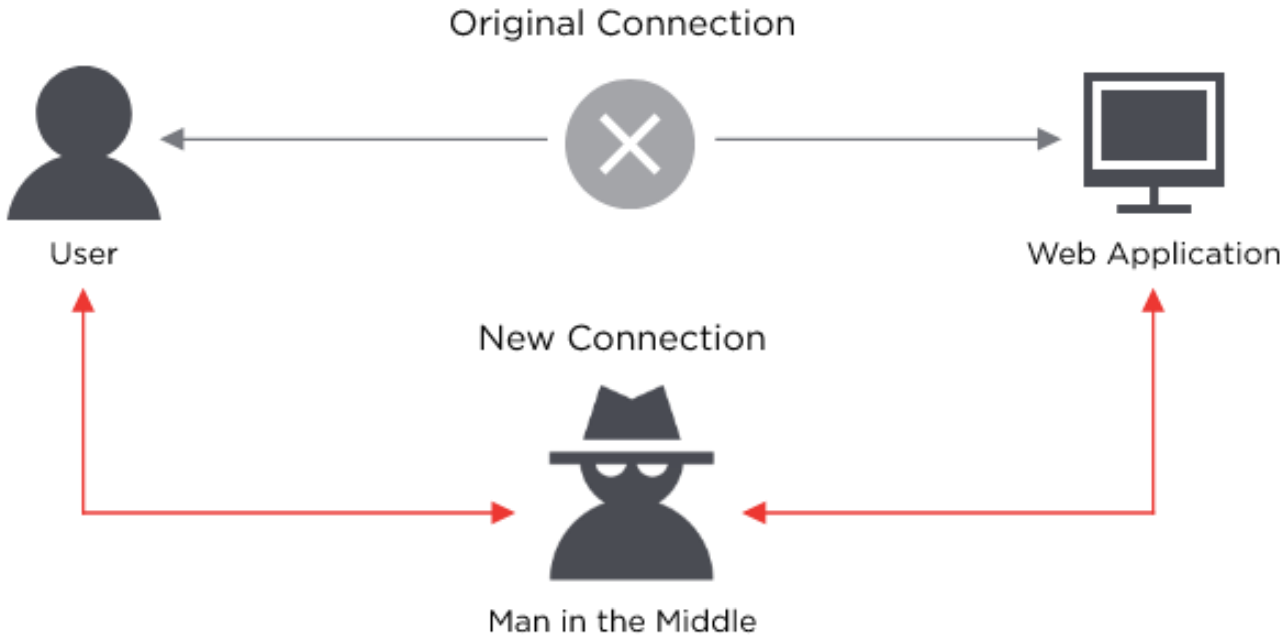


Tablas arco iris

Las tablas arco iris contienen hashes de contraseñas que se han calculado previamente

Estos hashes se utilizan como recurso para ejecutar ataques de diccionario y encontrar la contraseña de un usuario a partir de términos localizados en datos filtrados.

Ataques de contraseña

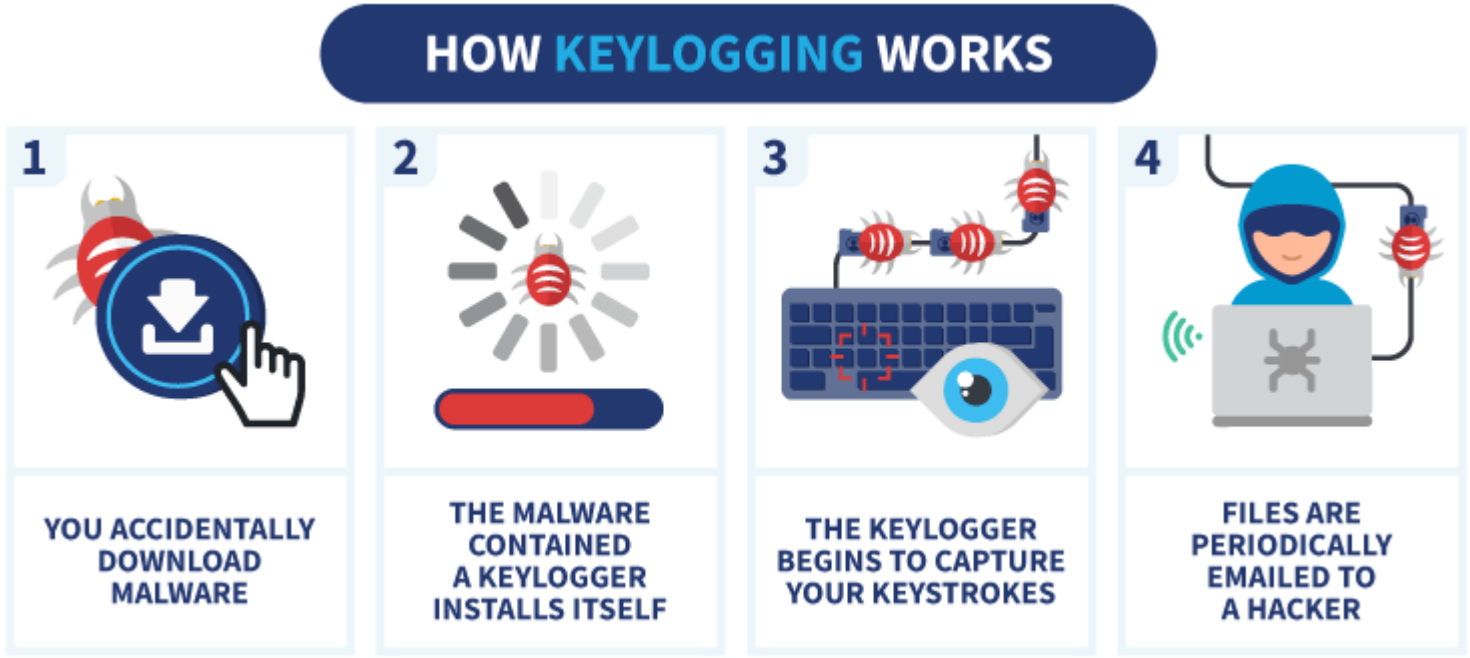


Hombre en el medio	Permite a un tercero malintencionado interponerse entre dos dispositivos o usuarios que están comunicándose.
	Permite interceptar los datos que se envían entre dispositivos así como el robo de información confidencial.

Ataques de contraseña

Intercepción de tráfico	Se utiliza un software, como rastreadores de paquetes, para monitorear el tráfico de la red y capturar contraseñas a medida que se pasan.
	Dependiendo de la solidez del método de cifrado utilizado, incluso la información cifrada puede ser descifrable.

Ataques de contraseña



Keylogger	Un actor malintencionado obtiene acceso a una computadora e instala software o hardware que registra cada pulsación de tecla realizada por el usuario.
	Registrar contraseñas, mensajes, correos electrónicos y cualquier otro texto ingresado.
	Funciona en el sistema durante mucho tiempo sin ser detectado.

Contraseñas más comunes

Recolectaron conjuntos de datos (públicos) asociados a contraseñas filtradas

Anonimizaron los usuarios para solo centrarse en la contraseña

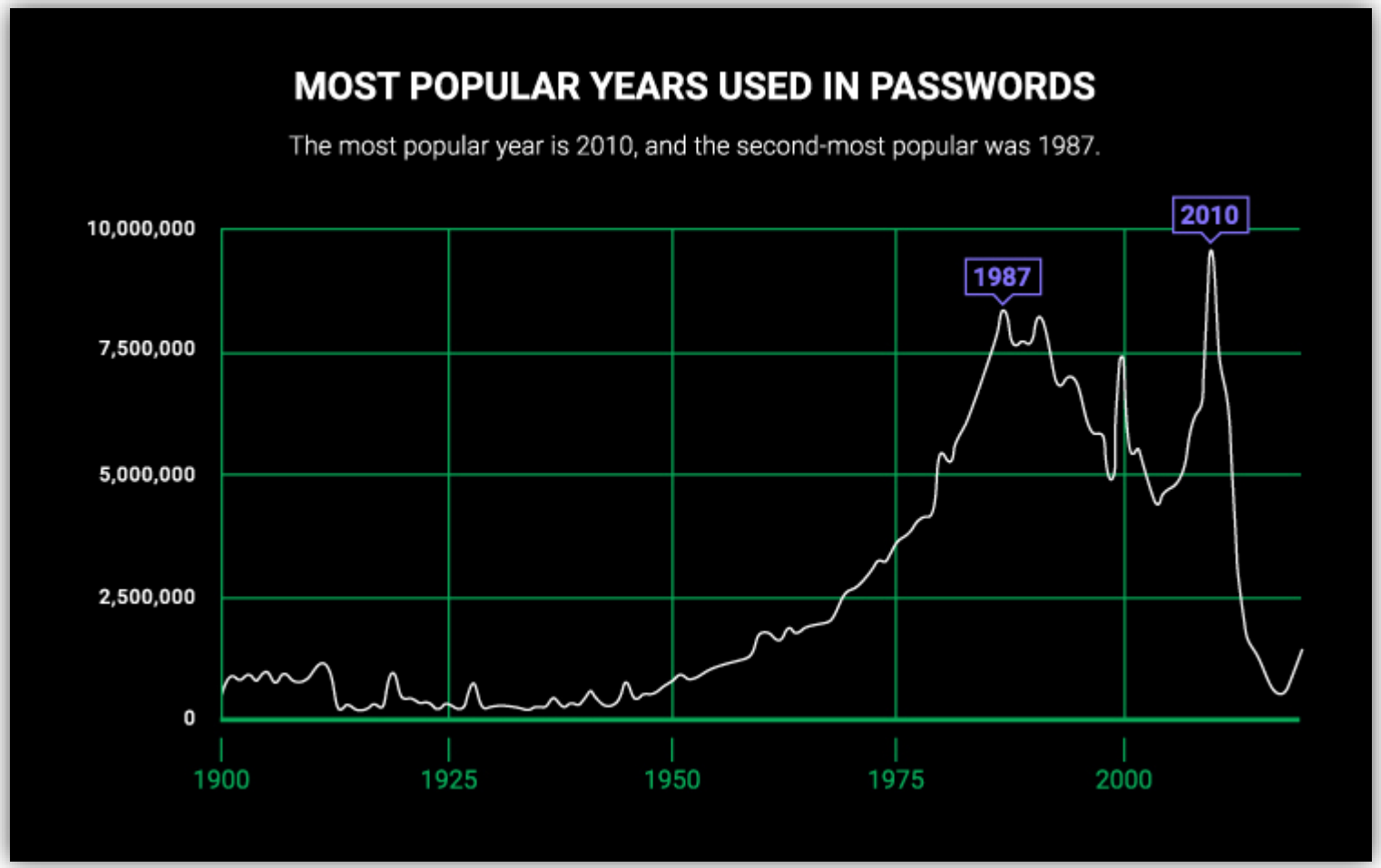
Analizaron un total de **15 212 645 925** de las cuales 2 217 015 490 (**14%**) eran únicas

Top 10 en 2024

1. 123456
2. 123456789
3. qwerty
4. password
5. 12345
6. qwerty123
7. 1q2w3e
8. 12345678
9. 111111
10. 1234567890

https://cybernews.com/best-password-managers/most-common-passwords/

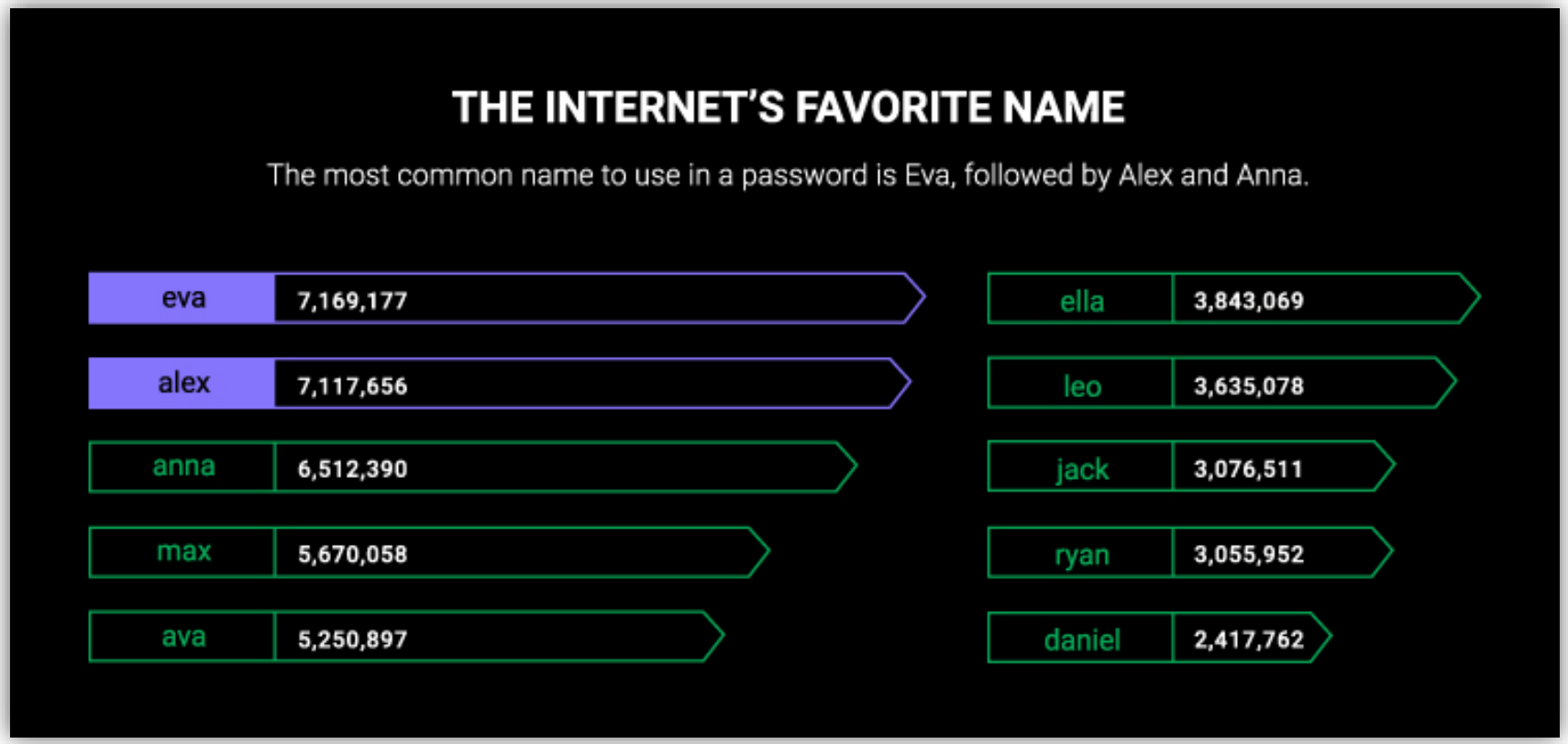
Características comunes en las contraseñas



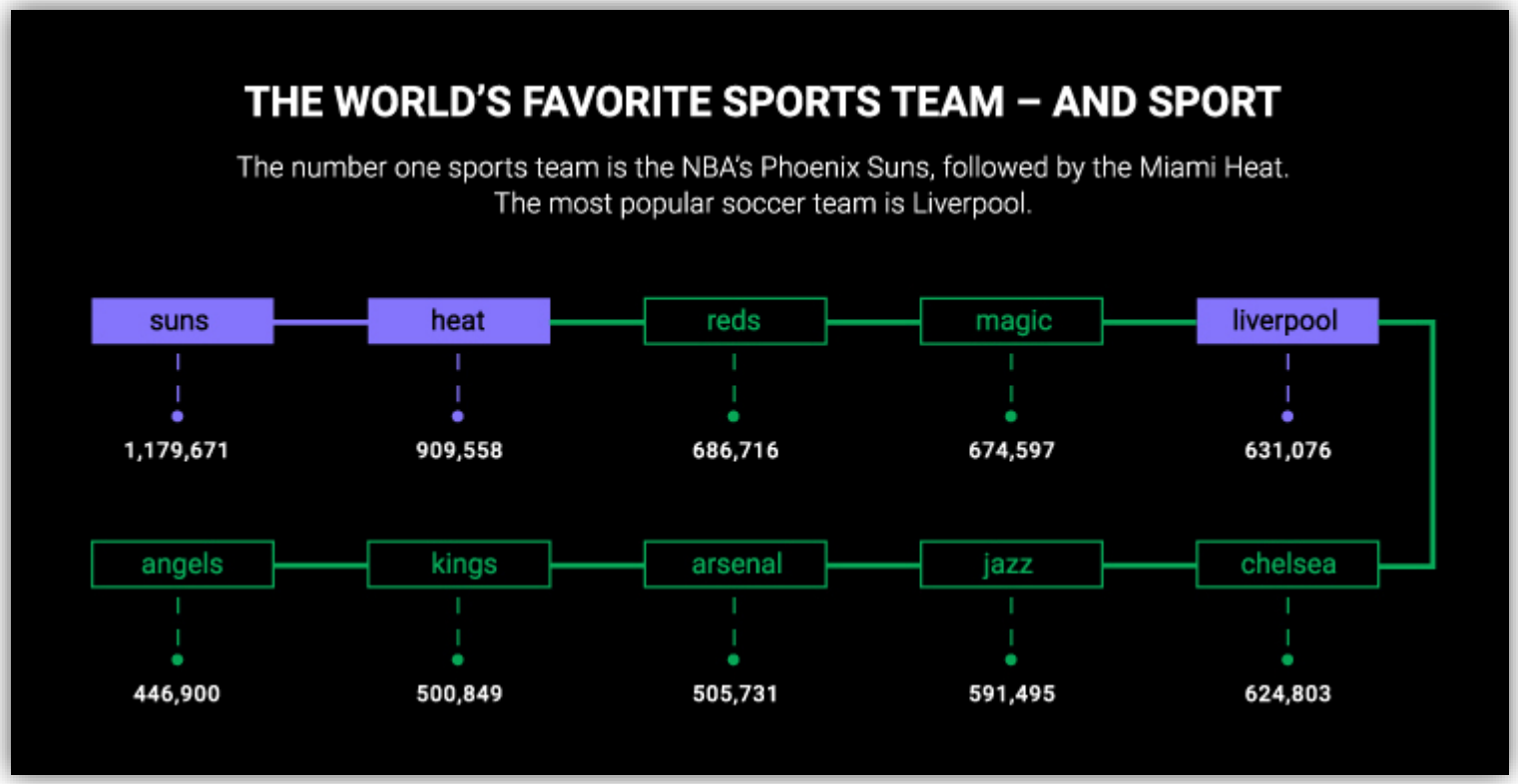
Posibles razones

- Fecha de nacimiento
- Fecha en que se creó la contraseña
- Año de un acontecimiento especial

Características comunes en las contraseñas



Características comunes en las contraseñas



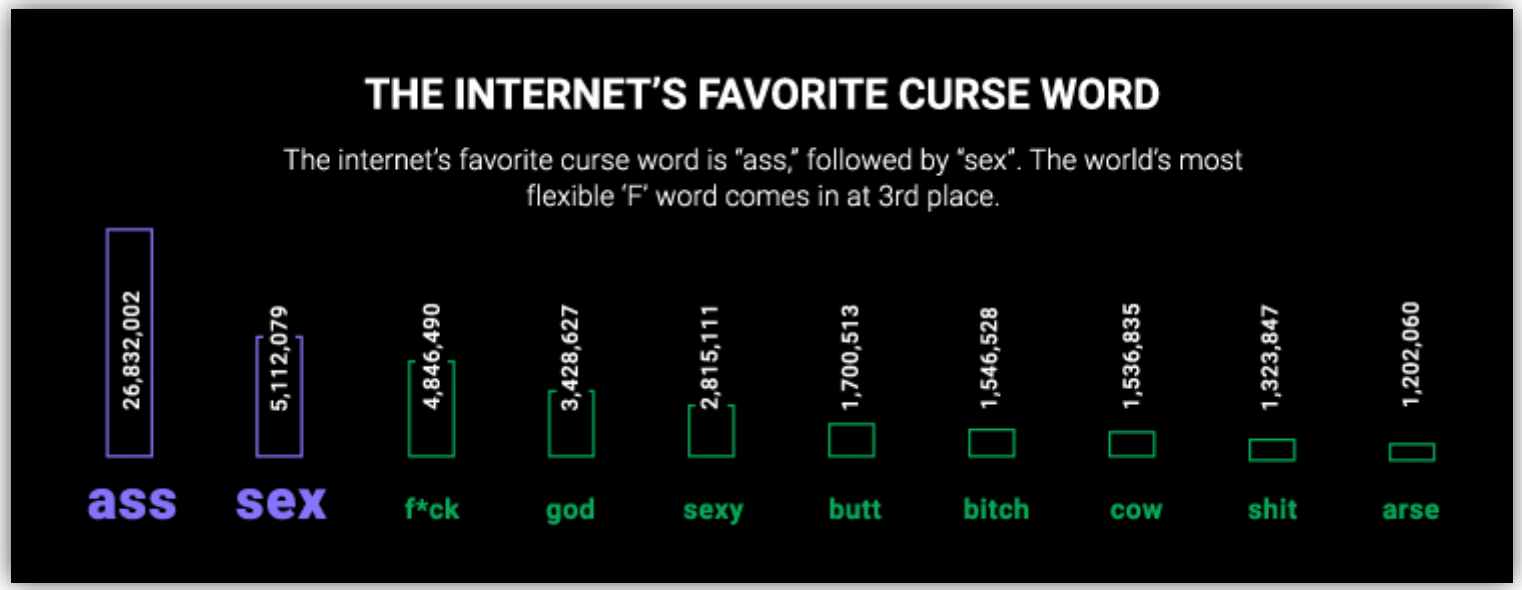
Equipo menos popular

- wolverhamptonwanderers (club de fútbol inglés, utilizado 3 veces)

Deportes más comunes

- NBA (5 equipos)
- Fútbol (3 equipos)
- MLB (2 equipos)

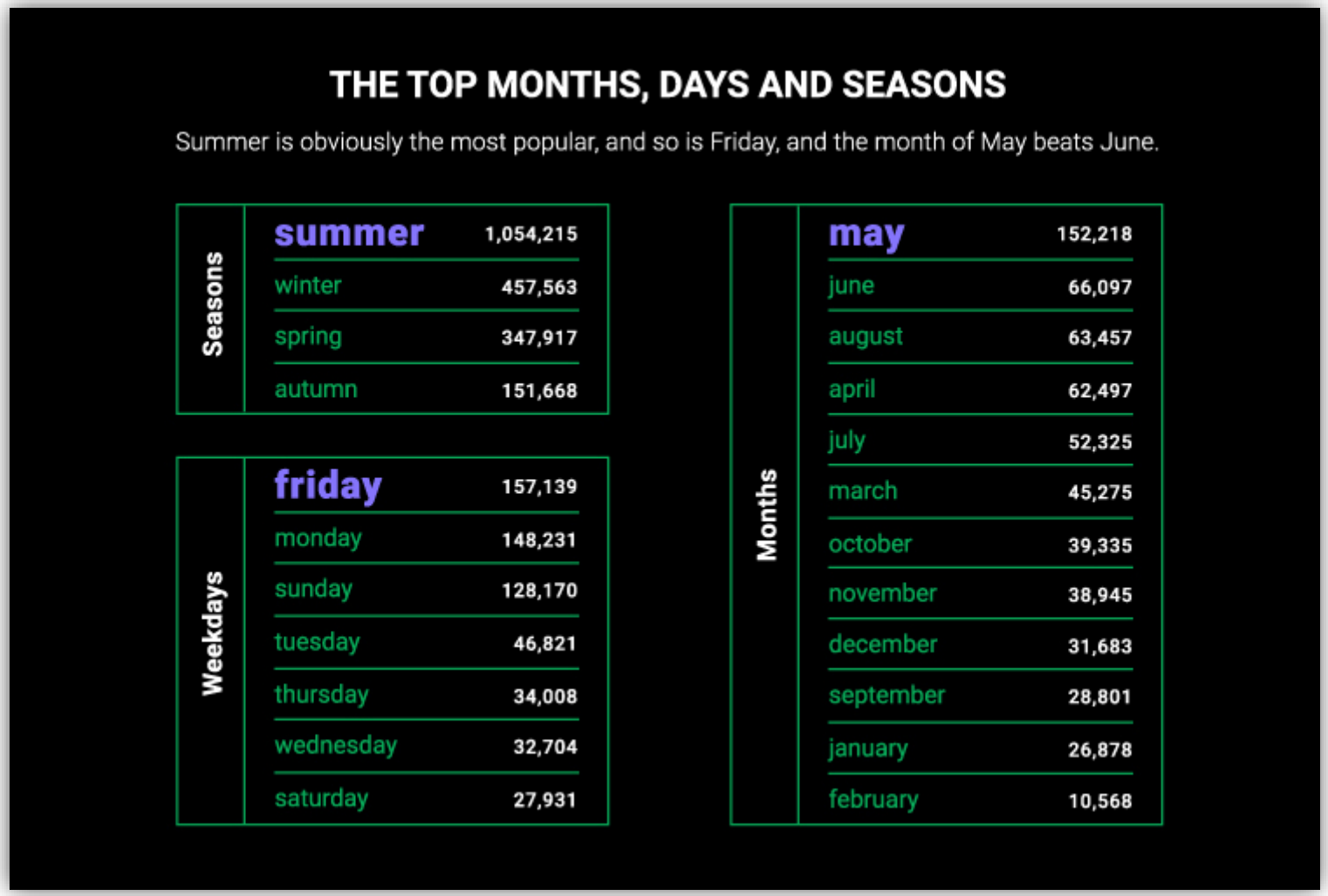
Características comunes en las contraseñas



Contraseñas que contienen palabras para maldecir

- Total: 152 933 335

Características comunes en las contraseñas

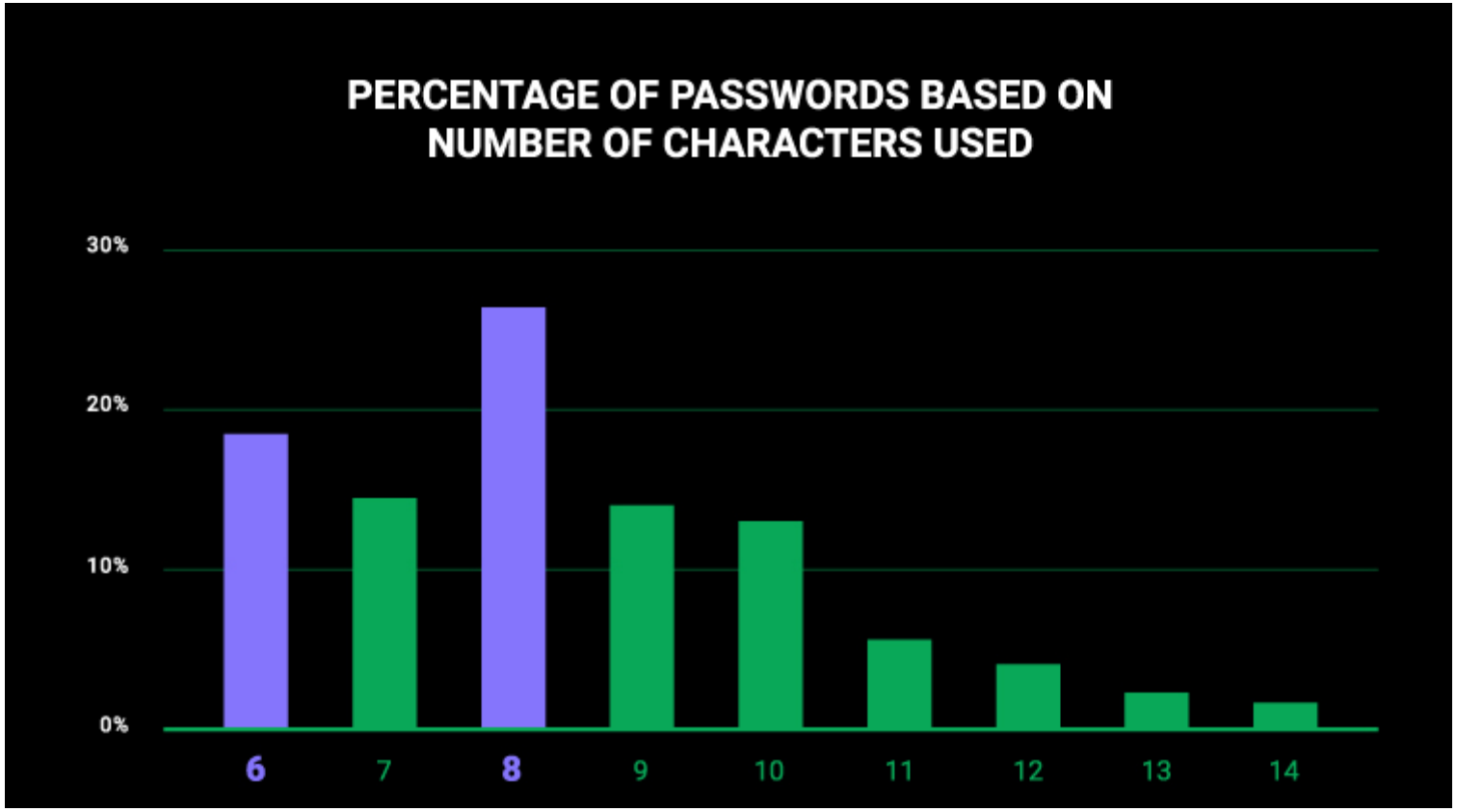


Características comunes en las contraseñas

Contraseñas que contienen palabras relacionadas con alimentos

- Aproximadamente 42 millones (1.9% del total)

Características comunes en las contraseñas



Generando Contraseñas Robustas

Complejidad

- Las contraseñas deben ser complejas, utilizando combinaciones de letras mayúsculas, minúsculas, números y caracteres especiales.

Longitud

- Cuanto más larga sea la contraseña, más segura será.

Evitar patrones predecibles

- Evita secuencias como “123456” o “password”.

Confidencialidad de las Contraseñas

Formas seguras de compartir contraseñas

Gestor de Contraseñas

- Estas herramientas utilizan cifrado conocimiento cero, lo que garantiza que las contraseñas compartidas permanezcan cifradas en todo momento.

Autenticación de Dos Factores (2FA)

- Proporciona una capa adicional de seguridad.

Actualizaciones

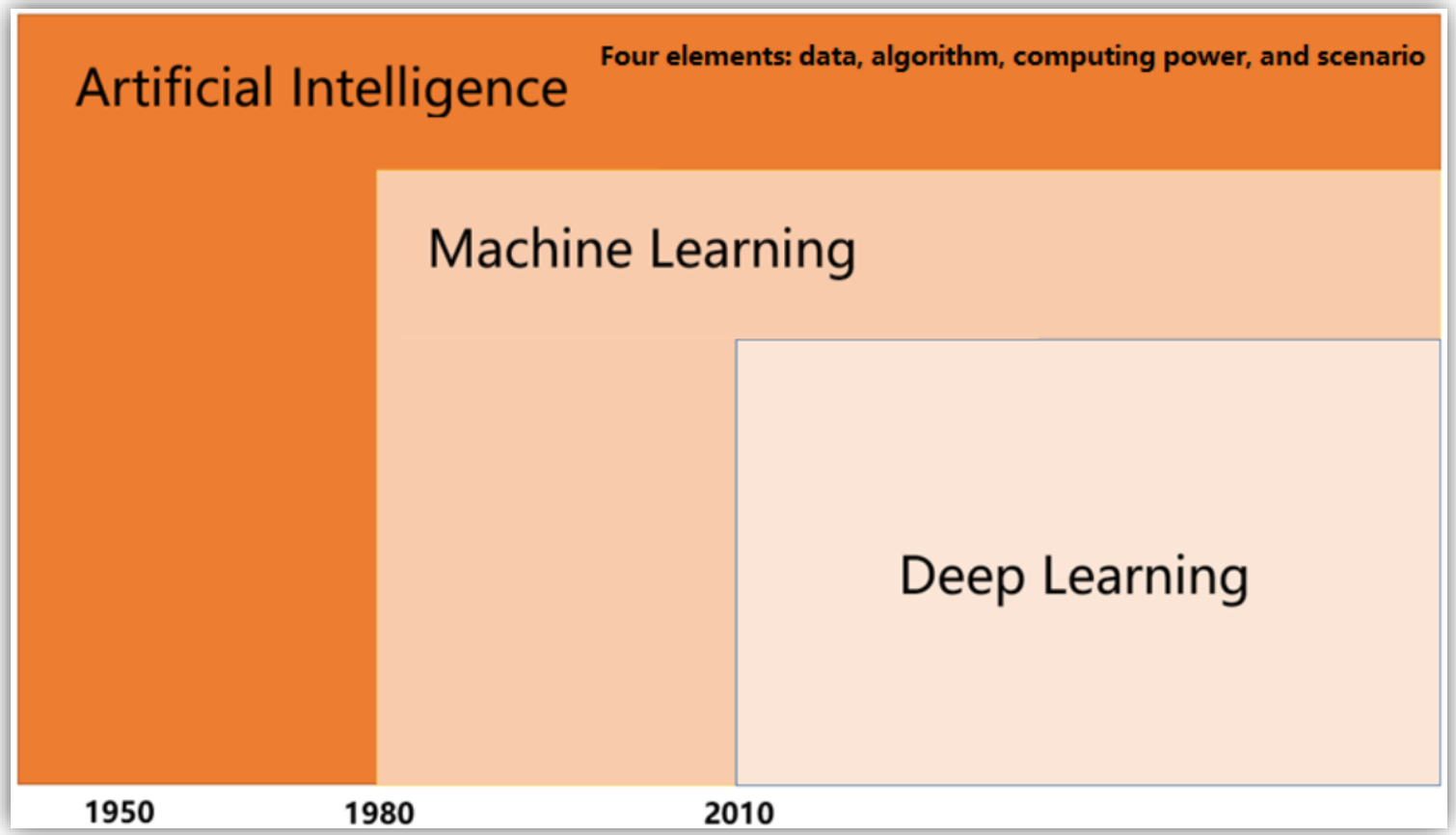
- Cambia las contraseñas periódicamente.
- Si tienes disputas o relaciones rotas con alguien con quien compartiste contraseñas, cámbialas.

Evita Métodos No Seguros

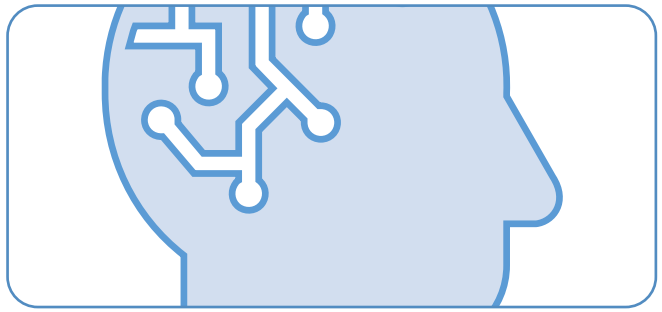
- No reutilices contraseñas.
- No las compartas a través de mensajes de texto, correos electrónicos o aplicaciones no cifradas.
- No las almacenes en lugares visibles físicamente.

Empleo de IA para el análisis de contraseñas

Conceptos más populares de las ciencias de la información en la actualidad.

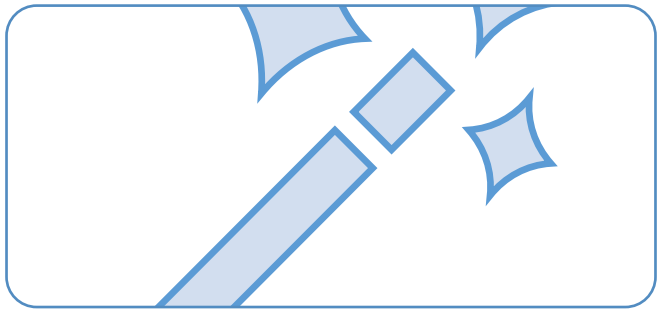


Conceptos más populares de las ciencias de la información en la actualidad.



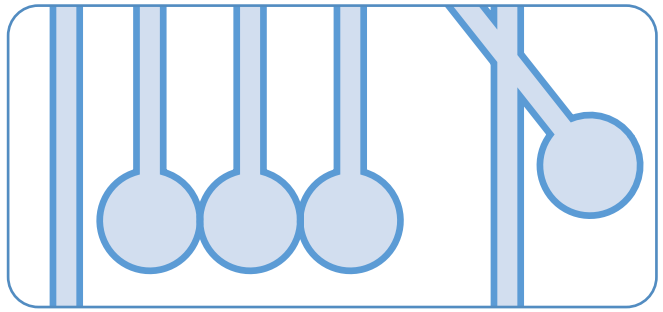
IA

- Una nueva ciencia técnica que se centra en la investigación y el desarrollo de teorías, métodos, técnicas y sistemas de aplicación para simular y ampliar la inteligencia humana.



Aprendizaje automático

- Campo de investigación central de la IA. Se centra en el estudio de cómo los ordenadores pueden obtener nuevos conocimientos o habilidades simulando o realizando el comportamiento de aprendizaje de los seres humanos y reorganizar la arquitectura de conocimiento existente para mejorar su rendimiento. Es uno de los principales campos de investigación de la IA.



Aprendizaje profundo

- Un nuevo campo del aprendizaje automático. El concepto de aprendizaje profundo tiene su origen en la investigación de las redes neuronales artificiales. El perceptrón multicapa (MLP) es un tipo de arquitectura de aprendizaje profundo. El aprendizaje profundo pretende simular el cerebro humano para interpretar datos como imágenes, sonidos y textos.

Cross Industry Standard Process for Data Mining (CRISP-DM)

Compresión del negocio

- Fase inicial enfocada en la comprensión de los objetivos y exigencias del proyecto desde una perspectiva de negocio.

Comprensión de los datos

- Se encarga de la recolección de datos inicial y continúa con las actividades que permiten familiarizarse primero con los datos.

Preparación de los datos

- Cubre todas las actividades necesarias para construir el conjunto de datos final.

Modelado

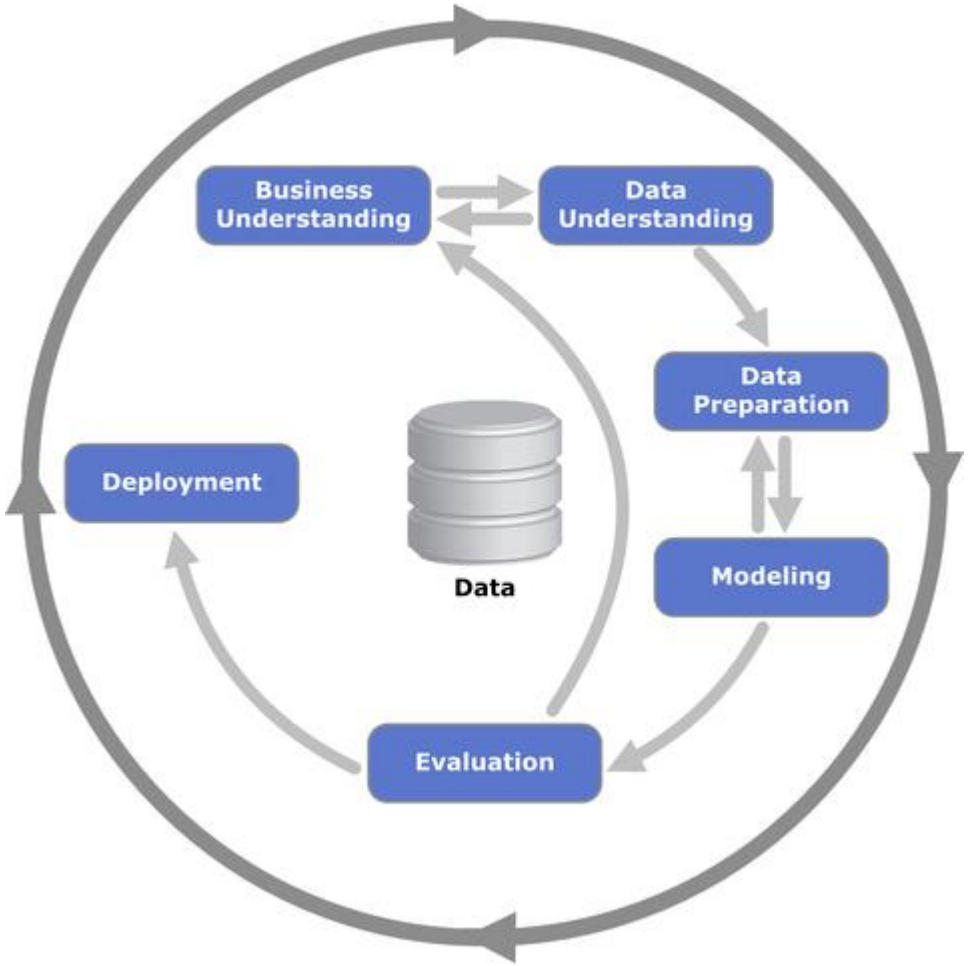
- Aplicación de técnicas de modelado y los parámetros de uso de las mismas se afinan hasta alcanzar los valores óptimos.

Evaluación

- Se evalúan los modelos anteriores para determinar si son útiles a las necesidades de negocio.

Despliegue

- Implica la explotación de los modelos dentro de un entorno de producción.



Caso de estudio

Rockyou

Fue fundada en 2005 en San Francisco, California y declarada en bancarrota en el 2019.

Fue una compañía que desarrolló widgets para MySpace e implementó aplicaciones para varias redes sociales, incluida Facebook. En sus últimos años se dedicó principalmente a la compra de derechos de videojuegos clásicos.

En diciembre de 2009, la compañía experimentó una violación de datos que resultó en la exposición de más de 32 millones de cuentas de usuario.

La compañía utilizó una base de datos sin cifrar para almacenar los datos de la cuenta de usuario.

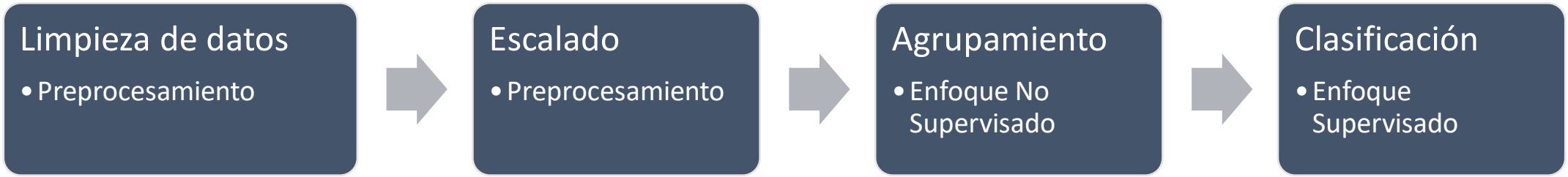
Características del conjunto de datos Rockyou

- Comprende 14 millones de contraseñas filtradas de la brecha de seguridad de RockYou Inc. en 2009.
- Las contraseñas son variadas en complejidad y longitud.
- Reflejan patrones comunes de elección de contraseñas por parte de los usuarios.
- Se incluyen contraseñas simples y predecibles, como palabras comunes, secuencias numéricas, combinaciones alfanuméricas, y variaciones de nombres, fechas y palabras relacionadas con la cultura Pop.

Importante

- El uso y análisis de este conjunto de datos plantea preocupaciones éticas y de privacidad, ya que contiene información confidencial de usuarios que fue obtenida de manera ilegal. Por lo tanto, su uso debe realizarse con precaución y siguiendo las pautas éticas y legales establecidas en la investigación en ciberseguridad.

Procesos a realizar sobre el caso de estudio



Limpieza de datos

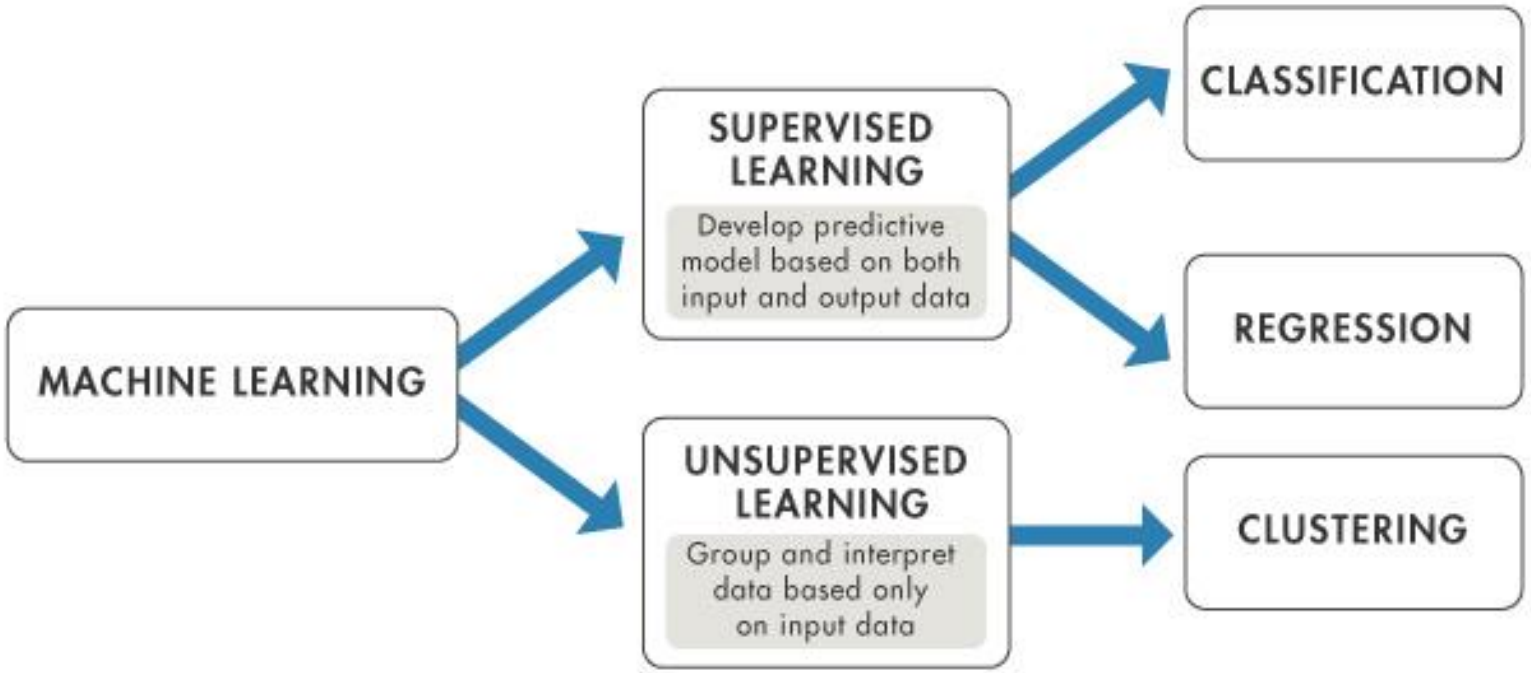
Incompletos:	Carecen de valores o contienen solo datos agregados. Por ejemplo, ocupación = “”.
Ruido	Contienen errores o valores atípicos. Por ejemplo, Salario = “-10”.
Inconsistencia	Contiene discrepancias en códigos o nombres. Por ejemplo, Edad = “42” y Cumpleaños = “07/03/1997”.

Escalado de datos

El escalado transforma los valores de las características para que estén confinados en un rango específico, típicamente **[0, 1]** o **[-1, 1]**.

Por ejemplo, si tenemos características con diferentes escalas (ingresos y edad), el escalado los ajusta para que tengan una magnitud similar.

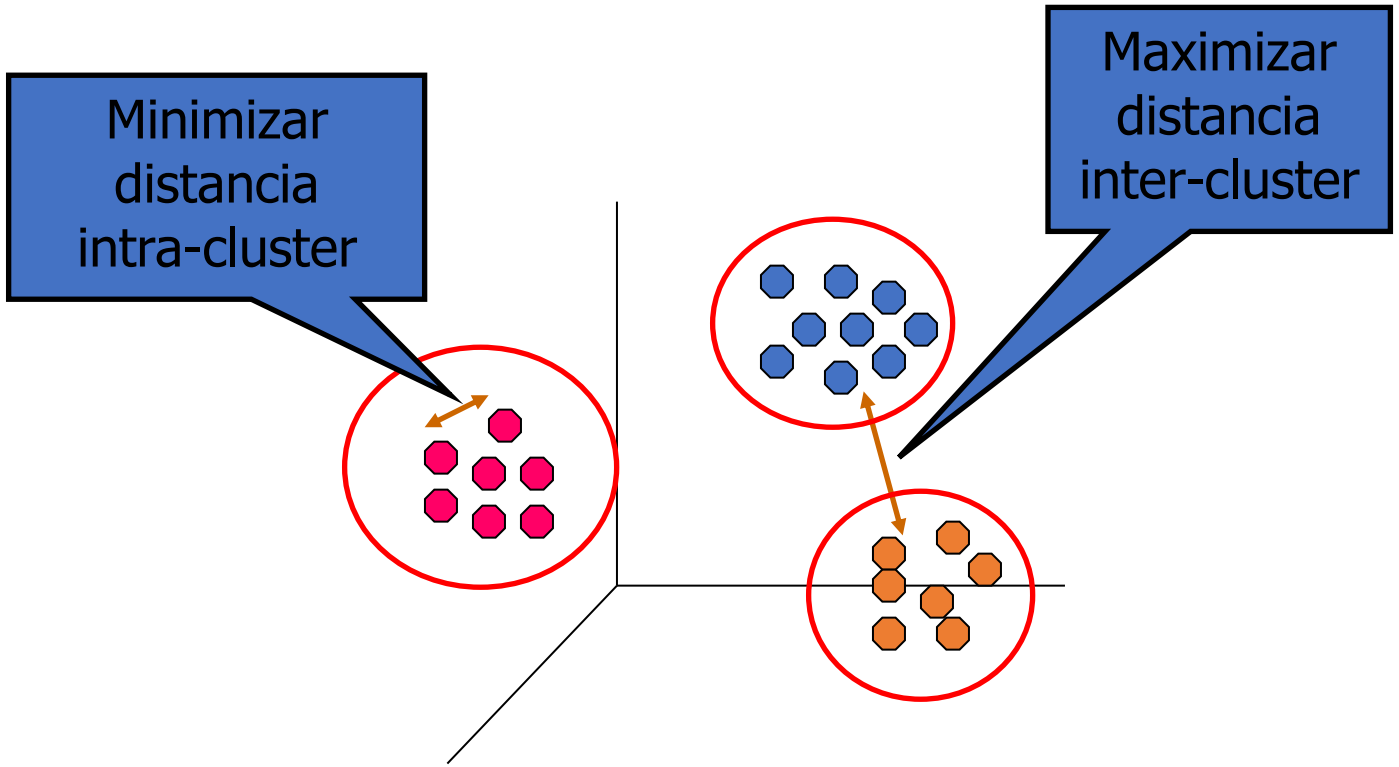
Aprendizaje automático



Agrupamiento

- Objetivo:
  - Agrupar objetos similares entre sí que sean distintos a los objetos de otros agrupamientos [clusters].
- Aprendizaje no supervisado
  - No existen clases predefinidas
- Los resultados obtenidos dependerán de:
  - El algoritmo de agrupamiento seleccionado.
  - El conjunto de datos disponible
  - La medida de similitud utilizada para comparar objetos.

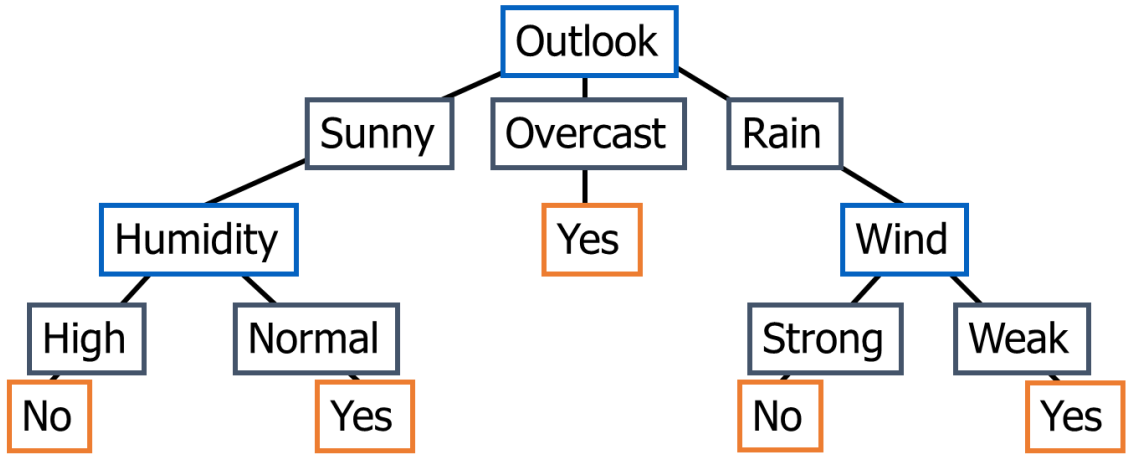
- Encontrar agrupamientos de tal forma que los objetos de un grupo sean similares entre sí y diferentes de los objetos de otros grupos:



Clasificación

La clasificación es la tarea de aprender una función objetivo *f* que asigna el conjunto de atributos *x* a una de las etiquetas de clase predefinidas *y*.

Day	Outlook	Temp.	Humidity	Wind	Play Tennis
D1	Sunny	Hot	High	Weak	No
D2	Sunny	Hot	High	Strong	No
D3	Overcast	Hot	High	Weak	Yes
D4	Rain	Mild	High	Weak	Yes
D5	Rain	Cool	Normal	Weak	Yes
D6	Rain	Cool	Normal	Strong	No
D7	Overcast	Cool	Normal	Weak	Yes
D8	Sunny	Mild	High	Weak	No
D9	Sunny	Cold	Normal	Weak	Yes
D10	Rain	Mild	Normal	Strong	Yes
D11	Sunny	Mild	Normal	Strong	Yes
D12	Overcast	Mild	High	Strong	Yes
D13	Overcast	Hot	Normal	Weak	Yes
D14	Rain	Mild	High	Strong	No



Actividad práctica

Objetivo

- Aplicar técnicas de Aprendizaje Automatizado para evaluar la fortaleza de las contraseñas.

Tareas

- Obtener los agrupamientos de contraseñas.
- Obtener un resumen estadístico de las contraseñas en el dataset.
- Aplicar un algoritmo de sobre las contraseñas.
- Entrenar un modelo de clasificación.
- Evaluar la fortaleza de una contraseña.
- Conclusiones