



# SEGURIDAD Y CONTRASEÑAS

Luis Joel Donato Jiménez  
LabCAD- UPRRP

# BOSQUEJO

- El problema
- ¿Qué es un manejador de contraseñas?
- ¿Qué hace un manejador de contraseñas?
- ¿Qué hacer una vez lo tengamos funcionando?
- Ejemplos de manejadores
- Demostración

# EL PROBLEMA CONTRASEÑA

- Protegen nuestros datos
- Las necesitamos - pero es un esquema de protección no muy eficiente en estos momentos
- No se deben (pueden) repetir (excepto “single sign-in”). No deben ser fáciles de recordar o asociadas directamente a mi persona.
- No nos recordamos de tantas
- Queremos entrar rápido
- Queremos entrar desde cualquier sitio y dispositivo
- Los lugares donde las usamos pueden ser jaqueados



<https://pixabay.com/illustrations/password-keyword-code-word-solution-866977/>

# ¿POR QUÉ ESTAN TAN DIFÍCIL CREAR CONTRASEÑAS HOY?

- **POR NUESTRA CULPA**

- Por la costumbre de crear contraseñas tan sencillas de averiguar y repetirlas
  - 123456, qwerty, password, letmein, mismo username
  - palabras del diccionario, al derecho o al revés
  - frases famosas, títulos de libros o películas, versículos (Juan3 | 6)

- **PORQUE LAS COMPUTADORAS SON MEJORES**

- Una contraseña de 8 caracteres, mayúsculas y minúsculas, números y símbolos, puede ser descubierta con un ataque de “fuerza-bruta” en menos de 4 horas.

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols	Hardware
8	Instantly	6 secs	24 mins	2 hours	4 hours	RTX 2080
8	Instantly	6 secs	13 mins	52 mins	2 hours	RTX 3090
8	Instantly	1 sec	5 mins	22 mins	59 mins	RTX 4090
8	Instantly	Instantly	2 mins	7 mins	19 mins	A100 x8
8	Instantly	Instantly	1 min	5 mins	12 mins	A100 x12
8	Instantly	Instantly	Instantly	Instantly	1 sec	A100 x10,000 (ChatGPT)

*Max time required to crack randomly generated 8-character MD5 password hashes of various complexity on different hardware.*

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols	Hardware
8	2 hours	4 months	92 years	375 years	989 years	RTX 2080
8	17 mins	4 weeks	18 years	72 years	189 years	RTX 3090
8	9 mins	2 weeks	9 years	38 years	99 years	RTX 4090
8	2 mins	2 days	2 years	7 years	17 years	A100 x8
8	1 min	2 days	1 year	4 years	12 years	A100 x12
8	Instantly	3 mins	11 hours	2 days	5 days	A100 x10,000 (ChatGPT)

*Max time required to crack randomly generated 8-character bcrypt password hashes set to 32 iterations of various complexity on different hardware.*

# ESTRATEGIAS PARA CREAR CONTRASEÑAS

- **Número de caracteres**
  - Mientras más caracteres mejor
    - Recomendación de NIST (National Institute of Standards and Technology) vs. complejidad
- **Azar**
  - Mientras más azarosa, mejor
- **Combinación de palabras no relacionadas**
  - jugoautorecaomaravilla2olaquífuncional (32 o más caracteres)
- **Aún así, y para todo lo demás, recomendamos un manejador de contraseñas**

# ¿Y LA AUTENTICACIÓN SIN CONTRASEÑAS?

- **Passkeys**

- Usan dos codificaciones auto-generadas, una pública y una privada. Lo encriptado con el código público solamente puede ser descifrado con el código privado, y esto solamente luego de corroborarse que es usted quien genera el proceso.

- **Biométricos**

- Huella dactilar; Facciones (cara)

- **Físicos**

- FIDO2-compatible USB key

- **Tradicionales**

- contraseña de la computadora

- Ventajas- eliminan las contraseñas, eliminan phishing, eliminan los códigos multi-factor. Desventajas- está comenzando. Necesita equipos modernos.

# ¿QUÉ ES Y QUE HACE UN MANEJADOR DE CONTRASEÑAS?

- Es un programa / app / webapp que permite guardar todas nuestras contraseñas, incluso de forma interactiva
- Genera, automáticamente, contraseñas más fuertes y seguras, dependiendo de los parámetros que escojamos
  - mayúsculas, minúsculas, números, símbolos, largo
- Entra los datos por nosotros
- NOTA: SIEMPRE tendremos que recordar alguna contraseña, p. ej. la que abre el manejador, la que abre la computadora o teléfono...



# ¿QUÉ ES Y QUE HACE UN MANEJADOR DE CONTRASEÑAS (OPCIONAL)?

- Tiene mecanismos de anti-phishing
- Tiene auditoría de contraseñas flojas, repetidas, comprometidas
- Provee monitoreo de fisuras (breach) y filtrado de datos y nos alerta
- Provee para entrar info personal- no más llenar tanto dato en los sites
- Provee para datos de tarjeta de crédito
- Provee notas seguras
- Provee para guardar información de números de licencia de apps
- Provee para generación de passkeys y contraseñas de un solo uso (TOTP)
- Multi-plataforma (Mac, Windows, iOS, iPadOS, Android, Linux, Chrome)

# ¿Y EL MANEJADOR DE MI NAVEGADOR?

- Sirve solo con el navegador (excepto iCloud Keychain)
- Algunos no son tan seguros
- Fueron explotados por esquemas de recoger información.

# ¿QUÉ HACER UNA VEZ TENGAMOS NUESTRO MANEJADOR FUNCIONANDO?

- Cambiar las contraseñas débiles y repetidas. Chequear la auditoría y cambiar todas las comprometidas.
- Eliminar toda instancia de “Remember me” y auto-entrada
- Eliminar toda instancia de recuerdo, pista u orejita (hint)
- Siempre hacer logout cuando terminamos de usar los servicios
- Pensar seriamente si continuará utilizando el “auto-fill” de sus navegadores, que puede ser menos seguro y solo funciona por navegador
- Botar, quemar o guardar bajo bóveda la libretita...

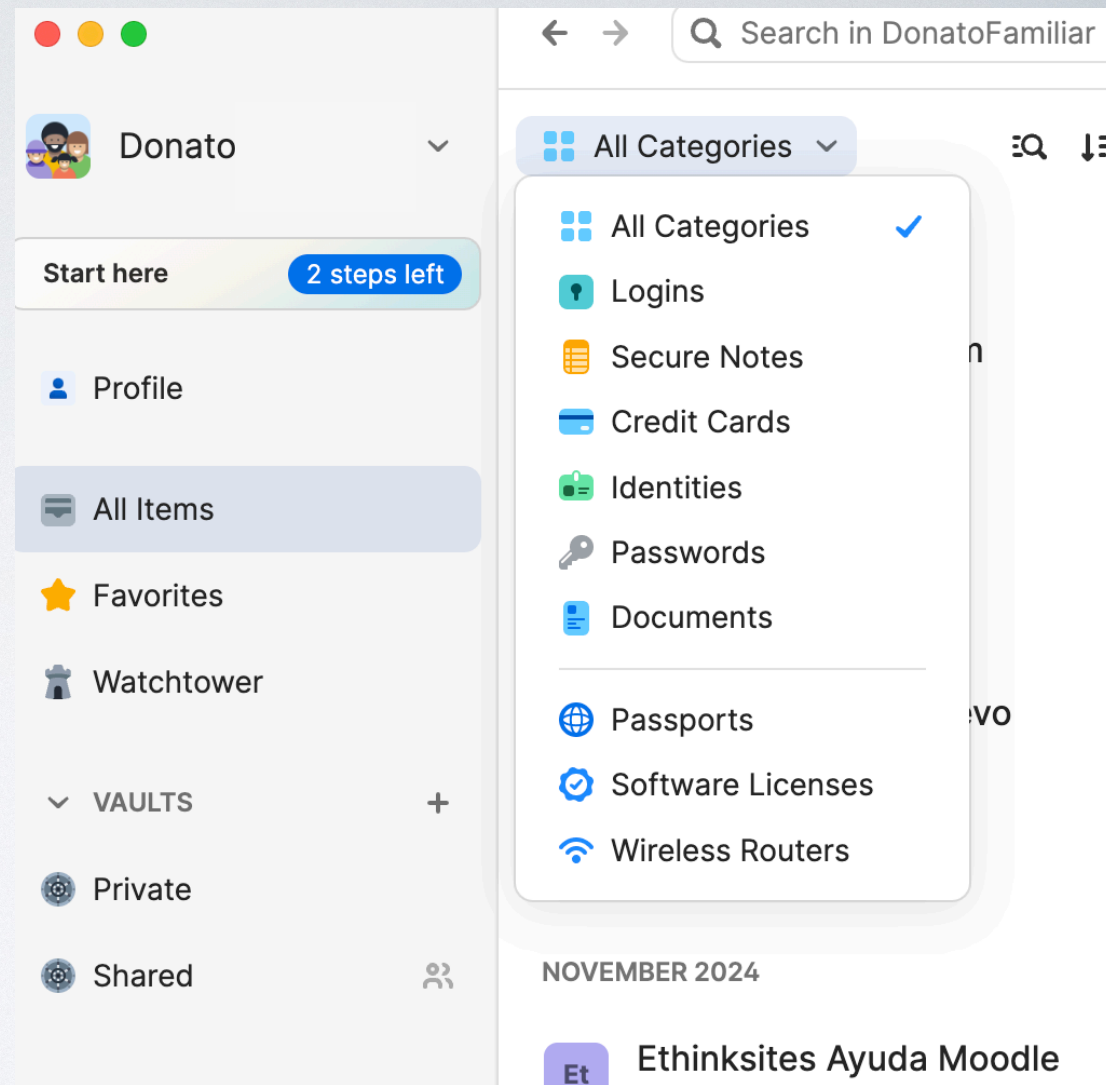
# ALGUNOS MANEJADORES

- 1Password (\$2.99/m)
- Bitwarden (open source, 0, \$10/año)
- Dashlane (\$4.99/m)
- Keeper (\$34.99/a)
- NordPass- (0, \$1.99/m)
- Proton Pass (0, \$4.99/m o \$1.99 x 12/a)








DEMOSTRACIÓN

# VISION DEL PANEL



# VISION DEL PANEL

WATCHTOWER		▼
	Compromised Websites	25
	Vulnerable Passwords	
	Reused Passwords	193
	Weak Passwords	118
	Unsecured Websites	169
	Two-Factor Authenticat...	23
	Expiring	2

# OTROS AVISOS

## Expired

This item has expired. If you've renewed it, enter your updated information.



## Compromised Website



This website was affected by a security breach since you last changed your password. Change your password to keep your account safe. [Learn more about this security breach.](#)

## Reused Password



This password is used in more than one of your items. Change your password to something unique.

1 other item ▾

## Weak Password



This password is too easy to guess. Change your password to something stronger.

## Unsecured Website



This item can be filled on an http:// page, which is not secure. Use https:// if the website supports it.

Use HTTPS

Ignore Warning

## Two-Factor Authentication Available



You can save your two-factor authentication codes for this account in 1Password. [Learn how to enable two-factor authentication.](#)


Scan QR Code




Don't Save in 1Password



# EJEMPLO DE LOGIN


Cancel Save

 **SuperWebsite**


 >  Personal 

---

username  
ljd@email.com

password  
8goPm\*B!7BvDdF 



---

website  
https://www.superwebsite.com 

website 2  
https://example.com

---

**SECTION**



label  
new field  

---


notes  
apellido materno de tu madre- Salchicha  
donde vivías en tercer grado- Marte  
primer auto- Schwinn

pin de seguridad- 4567

---

tags  
 

---

display  
Suggest in browser 

View Saved Form Details



**Muchas gracias**

Sesión de preguntas y comentarios

[luis.donato3@upr.edu](mailto:luis.donato3@upr.edu)

**LabCAD**  
LABORATORIO COMPUTACIONAL DE APOYO A LA DOCENCIA