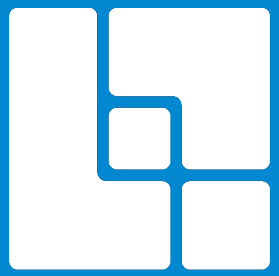


experts
coding

WebAuthn: No más passwords por favor!

Quienes somos

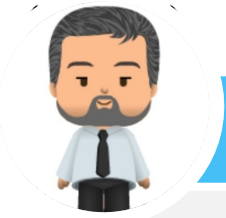
Manu Vilachán

Más de 15 vueltas al sol diseñando cohetes.

Arquitecto de Software, muy experto en tecnologías Microsoft y diseño de soluciones técnicas.

Desarrollo software complicado a veces, simple otras y si me queda un rato libre hago pan.

manuel.vilachan@expertscoding.es
@manuvilachan



Antonio Marín Alberdi

20 años dando caña

Especializado en Arquitectura de Soluciones, diseño de frameworks e implementación de soluciones técnicas.

Destaca en la creación de proyectos locos y pruebas de concepto arriesgadas pero absurdas.

antonio.marin@expertscoding.es
@realcodeprophet

Objetivos

Qué es y para que vale WebAuthn

Como se usa lo que sea que quiera ser WebAuthn

WebAuthn en el mundo real

¿Qué es WebAuthn?

Web Authentication API

Es la especificación de un API en navegadores web para crear y almacenar credenciales de forma segura

Estándar para dispositivos de seguridad capaces de interactuar con el API WebAuthn

¿Para que sirve?

Mejorar la seguridad evitando contraseñas y añadiendo dispositivos TUP.

Evitar el phishing mediante el uso de criptografía asimétrica (PKI) y comprobación de orígenes de sitios web.

¿Qué soporte tiene?

WebAuthn: W3C Recommendation – Marzo de 2019

En navegadores

18+ 67+ 60+ 13+ 54+

En SO's

10+ 7+

Demo


}(n||(delete s[u].data
(e){return e=e.nodeType
!==e.nodeType)return
for(r=o.attr
(){b.data(this,e,n)}).
"false"===r?!1:"
e?(n=(n||"fx")+"queue"
i&&(i=n.shift(),r--)
e,n)})})}),b.fn.
dequeue:function(e){return
r,i=1,o=b.Deferr
textarea|button|object
this,b.attr,e,t,argument
this.each(function(){try
r=1===n.node

Demo

¿Qué ha pasado en el registro?

Eh App, quiero registrarme!

Claro! Junto con estos datos que te doy, mándame tu clave pública

Voy, estoy creando un nuevo par de claves...

Allá van!

Gracias! Ya he creado tu registro. Desde ahora puedes iniciar sesión.

¿Y cuando he hecho login?

Hola! quiero logarme

Está bien, firma estos datos para saber que tú eres tú

Voy, los estoy firmando con mi clave privada...

Te envío la firma!

Verificando ...

Bien! Todo correcto. Let's rock&roll

Behind The Scenes

Registro

```
// attestationType: possible values: none, direct, indirect
// authenticatorAttachment: possible values: <empty>, platform, cross-platform
// userVerification: possible values: preferred, required, discouraged
// requireResidentKey: possible values: true,false
let options = await Register.client.makeCredentialOptions(username, displayName, "none", "", false, "preferred");
                                    ...
let newCredential = await navigator.credentials.create(options);
                                    ...
let response = await Register.client.makeCredential(rawResponse);
```

Login

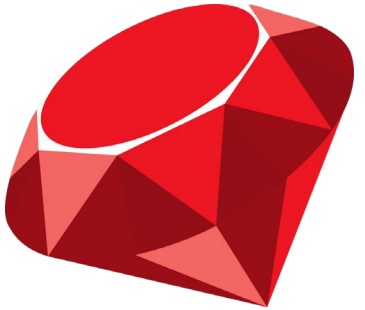
```
let makeAssertionOptions = await Login.client.assertionOptionsPost(username, "");
                                    ...
let credential = await navigator.credentials.get(makeAssertionOptions);
                                    ...
let response = await Login.client.makeAssertion(rawResponse);
```

Y en el servidor ¿que uso?

Duo Labs
Yubico
Google

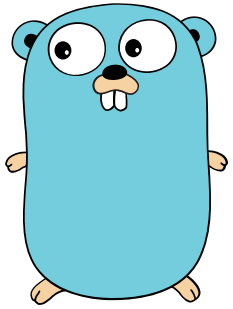
Fido Alliance

Duo Labs
Yubico

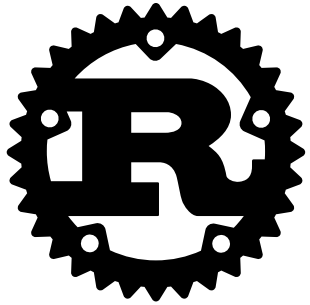


Cedarcode

Anders Åberg
Bryce Foster



Duo Labs
Koen Vlaswinkel



William Brown
Tiziano Santoro

Yubico

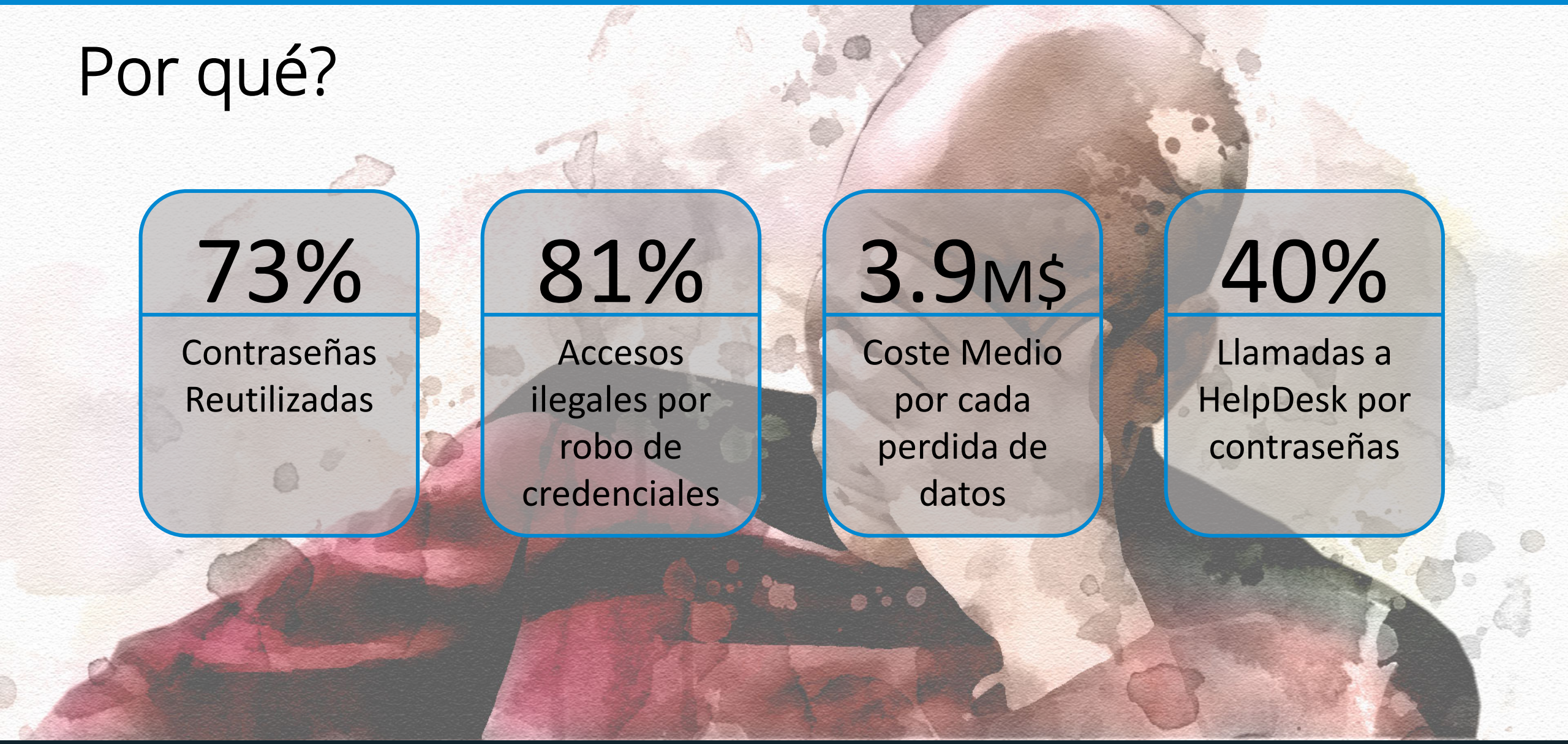
Consideraciones

Por qué?

porque mola

WebAuthn y el mundo empresarial

Por qué?

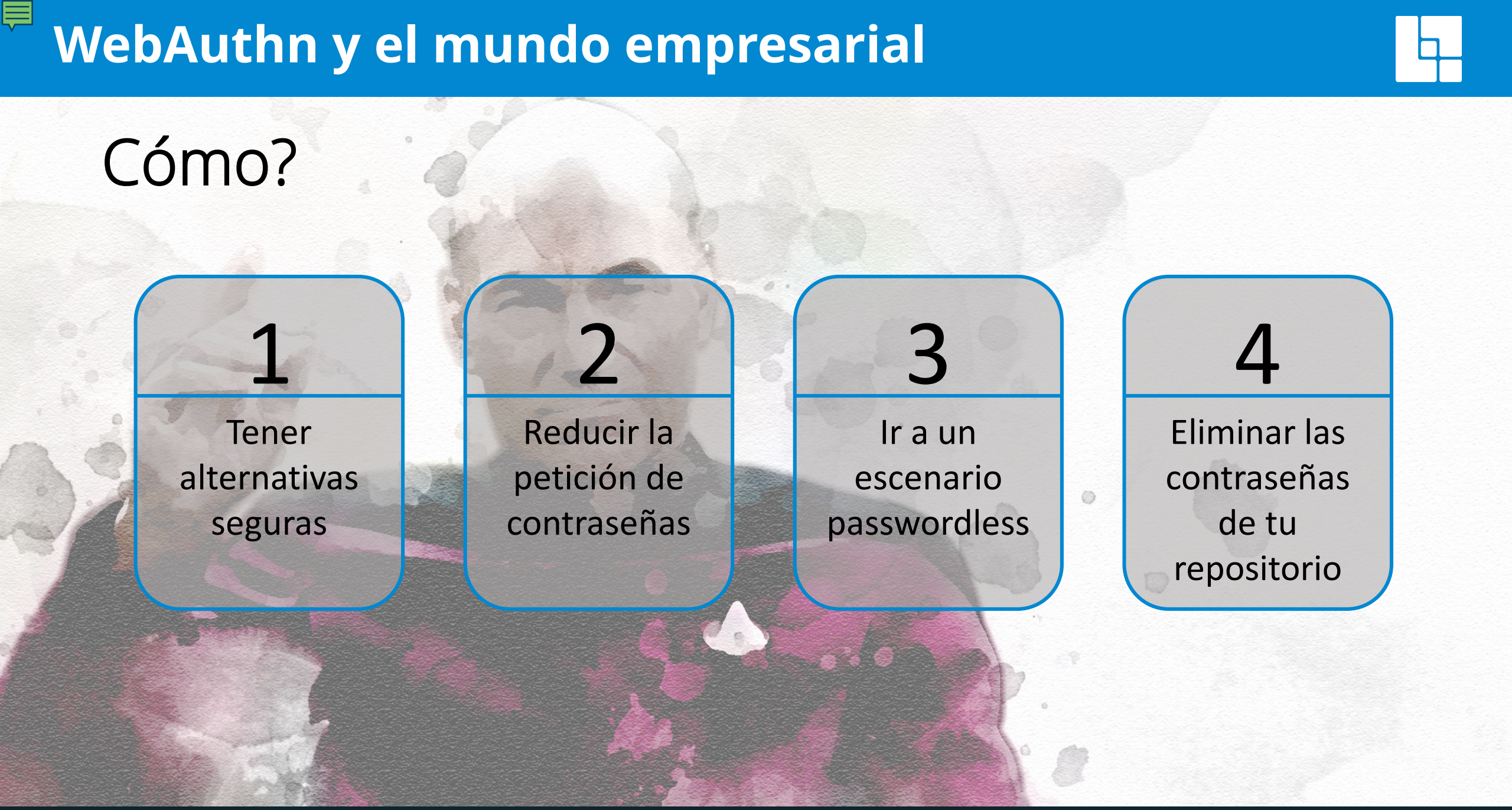


73%	81%	3.9M$	40%
Contraseñas Reutilizadas	Accesos ilegales por robo de credenciales	Coste Medio por cada perdida de datos	Llamadas a HelpDesk por contraseñas

Cómo?

Llaves para todos

WebAuthn y el mundo empresarial



Cómo?

1. Tener alternativas seguras
2. Reducir la petición de contraseñas
3. Ir a un escenario passwordless
4. Eliminar las contraseñas de tu repositorio

Llaves disponibles

Yubico

Feitian

SoloKeys

Referencias

Documentación Oficial
https://fidoalliance.org/fido2/
https://fidoalliance.org/specs/fido-v2.0-ps-20190130/fido-client-to-authenticator-protocol-v2.0-ps-20190130.html
https://fidoalliance.org/specs/fido-u2f-v1.2-ps-20170411/fido-u2f-hid-protocol-v1.2-ps-20170411.html
https://www.w3.org/TR/webauthn
https://w3c.github.io/webauthn

Info No Oficial
https://webauthn.guide/
https://github.com/herrjemand/WebauthnAwesome
https://blog.mozilla.org/security/2019/03/19/passwordless-web-authentication-support-via-windows-hello/
https://www.cio.com/article/3019536/what-fido-credentials-mean-in-windows-10.html
https://slides.com/fidoalliance/webauthn-overview#/
https://www.yubico.com/2019/11/yubico-reveals-first-biometric-yubikey-at-microsoft-ignite/
https://hackernoon.com/why-choosing-a-fido2-security-key-8cb0e5a1a71e
https://www.zdnet.com/article/apple-killing-off-web-passwords-safari-trials-webauthn-logins-on-macos/
https://www.brianmadden.com/opinion/How-does-FIDO-work-on-Apple

Llaves Fido2
Llave Fido2 Open Source (disponible kit de desarrollo): https://solokeys.com/
https://www.ftsafe.com/Products/FIDO
https://www.yubico.com/products/yubikey-hardware/

Linux Howdy (Autenticación integrada en el sistema): https://github.com/Boltgolt/howdy
Azure AD: https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-authentication-passwordless-security-key

Referencias

Librerías e Implementaciones
Java: https://github.com/duo-labs/android-webauthn-authenticator
Java: https://github.com/Yubico/java-webauthn-server
Java: https://github.com/google/webauthndemo
Node: https://github.com/fido-alliance/webauthn-demo
Python: https://github.com/duo-labs/py_webauthn
Python: https://developers.yubico.com/python-fido2/
Ruby: https://github.com/cedarcode/webauthn-ruby
.Net: https://github.com/abergs/fido2-net-lib
.Net: https://github.com/brucedog/U2F_Core
Go: https://github.com/duo-labs/webauthn
Go: https://github.com/koesie10/webauthn
Rust: https://docs.rs/crate/webauthn-rs/0.1.4
Rust: https://docs.rs/crate/webauthn/0.1.2
C++: https://developers.yubico.com/libfido2/

Development
https://github.com/MicrosoftEdge/webauthnsample
https://www.passwordless.dev/
https://webauthn.io/
https://fidoalliance.org/developers/resources/
https://docs.microsoft.com/en-us/microsoft-edge/dev-guide/windows-integration/web-authentication

Q & A

github sources

Gracias por tu atención

Credits

Photo by Casey Horner on Unsplash
Photo by NeONBRAND on Unsplash
Photo by Markus Spiske on Unsplash
Photo by Thought Catalog on Unsplash
Photo by naomi tamar on Unsplash
Wikimedia commons for the OS logos
Jean-Luc Picard – The Captain
Vincent Vega – The Hitman