


CHARLA

¿Podemos hacer que la seguridad sea Usable?

Josmell Chavarri

josmell.chavarri@guayoyo.io

@j0sm3ll

 Guayoyo

Victoria Perez

perezmvictoria@gmail.com

@perezmvictoria

pyxis 



TestingUy

13 y 14 de mayo, 2019

testinguy.org

@testinguy | #testinguy

A close-up photograph of a hand holding two wooden blocks. The block on the left has a large, dark, engraved letter 'U' on its face. The block on the right has a large, dark, engraved letter 'X' on its face. The background is a plain, light-colored surface.

User Experience

Experiencia de Usuario



A shiny metal padlock is the central focus, set against a vibrant background of a circuit board. The circuit board features a gradient from green on the left to orange on the right, with intricate patterns of lines and dots representing electronic components. The padlock is positioned in the lower right quadrant, casting a soft shadow on the surface below it.

SEGURIDAD

Informática





SEGURIDAD

- informática -

INTEGRIDAD

CONFIDENCIALIDAD

DISPONIBILIDAD





TODOS QUEREMOS USAR SISTEMAS

FIABLES Y SEGUROS

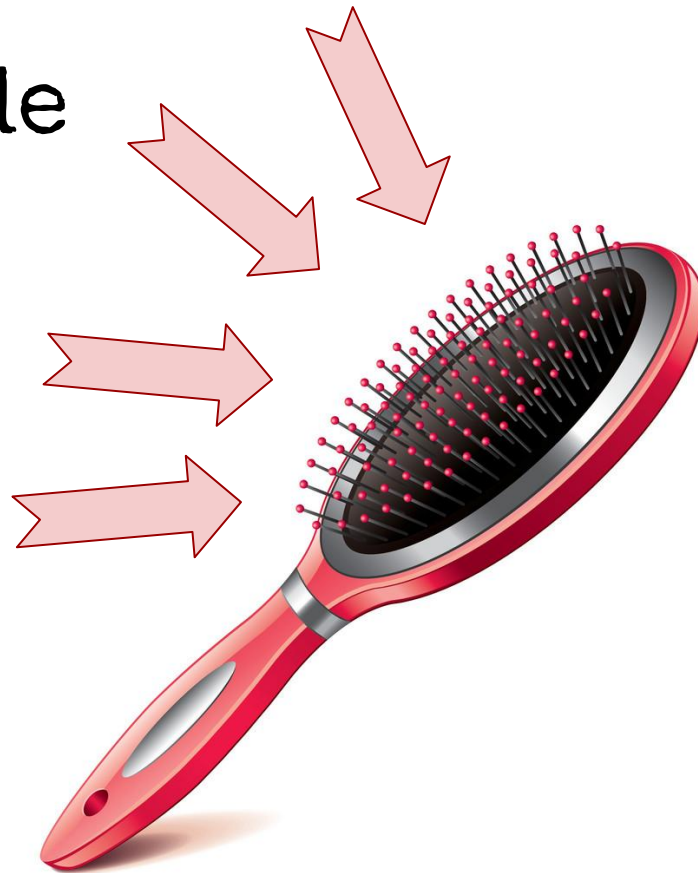




@perezmvictoria | @j0sm3ll | #testinguy



Puntas de
metal
afiladas



ser ex
human inte
Usability
ite dev

Qué tan sencillo de usar nos
resulta un producto/servicio



USABILIDAD

Quieren que
todo sea
más fácil



SEGURIDAD

Quieren que
todo sea
más difícil



Origen Común

Met-Ed / GPU
**THREE MILE ISLAND
NUCLEAR
GENERATING STATION**

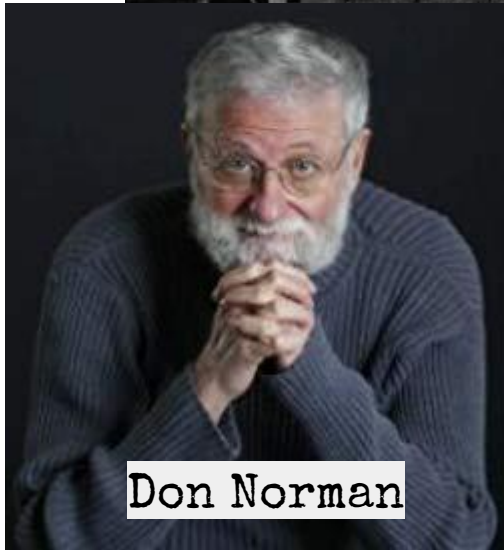
Authorized Personnel Only

**OBSERVATION CENTER
3/4 Mile Ahead**

Pennsylvania, US - 1979



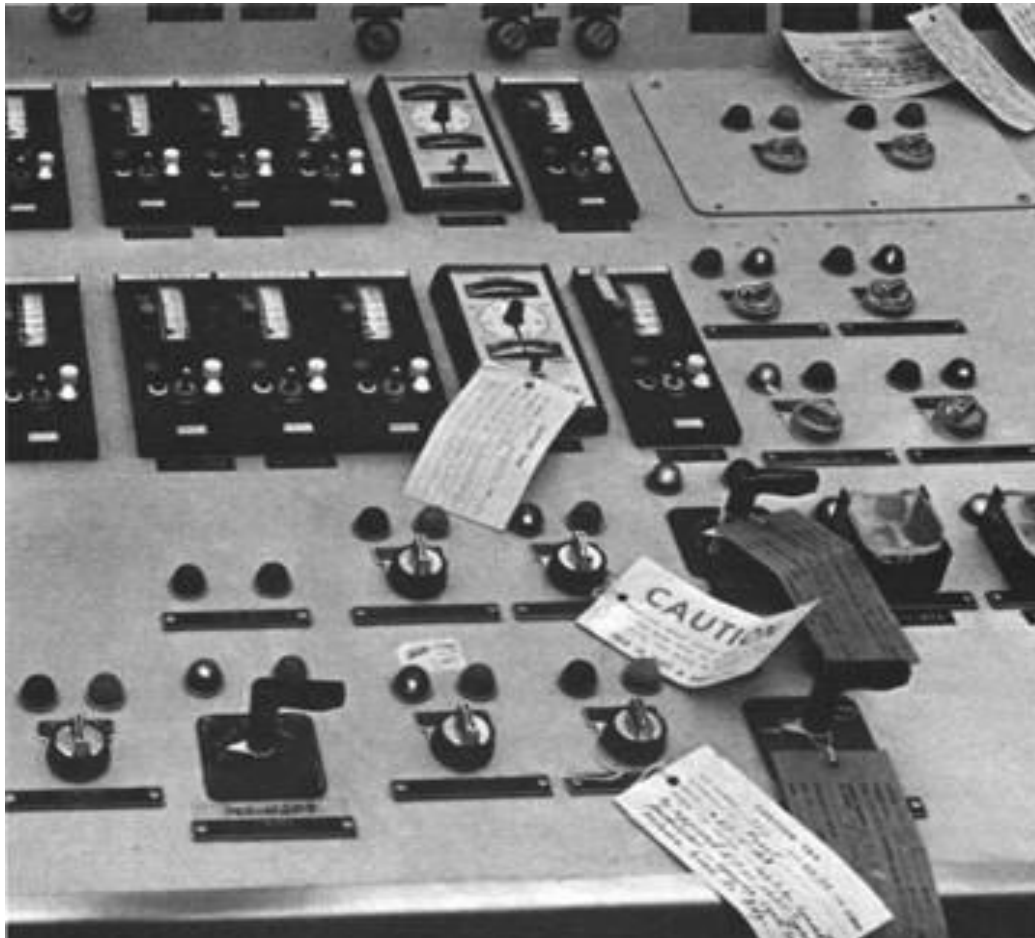
Sala de Máquinas de
la Planta Nuclear



Don Norman

@perezmvictoria | @j0sm311 | #testinguy





“Si hubieran querido diseñar los controles de una forma más confusa no hubieran podido”

Don Norman





PASSWORD



Estándares de seguridad

No palabras del diccionario

+ 14 caracteres

+ Mayúscula

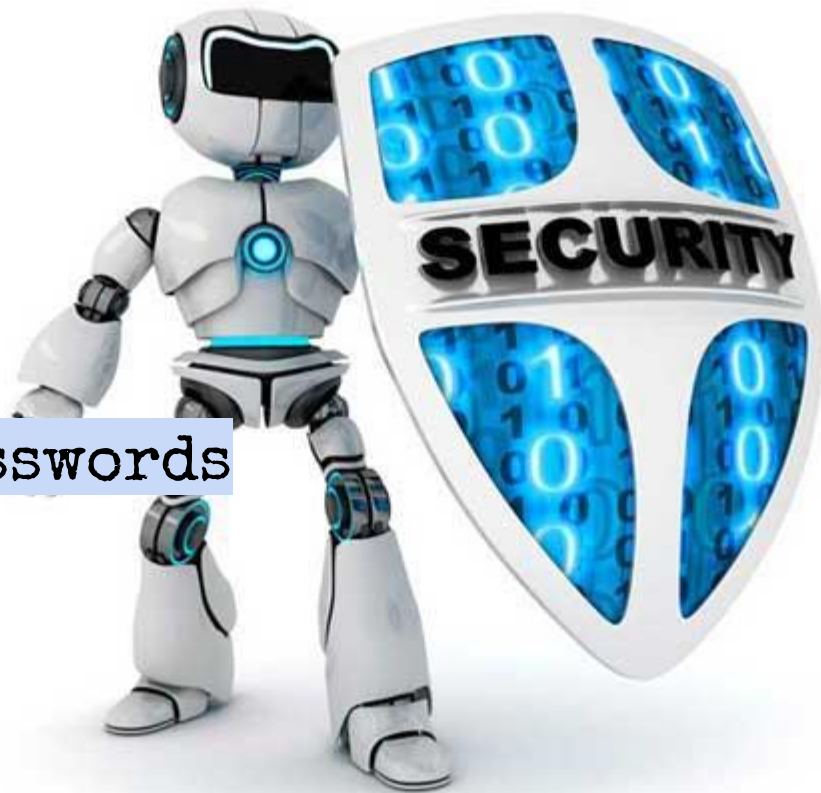
+ Minúsculas

+ Número

+ Símbolo

NO caracteres iguales consecutivos





No últimas 5 passwords





No últimas 5 passwords

Cambiarla cada 90 días





No últimas 5 passwords

Cambiarla cada 90 días


No repetir passwords entre sistemas





@perezmvictoria | @j0sm311 | #testinguy



A person in a dark suit and green tie is holding a large fan of US dollar bills, with the bills fanned out in front of them. The background is a plain, light-colored wall.

En el 2018

Ganancias del cibercrimen

1,5 billones de dólares



Fortaleza de las Contraseñas

TIPO	EJEMPLO	TIEMPO (MÉTODO)	NIVEL DE SEGURIDAD
10 Random CHAR	jskervergs	59 minutos	RIESGOSO
10 Random CHAR+NUM	jskerver43	1 día	RIESGOSO
10 Random CHAR + NUM + MAY + MIN + SYM	?jPk3rv3r0	800 años	SEGURO
Palabra Diccionario	naranja	200 milisegundos	NO SIRVE
Palabra Inventada	gulofunch	2 minutos	NO SIRVE

<https://howsecureismypassword.net/>



Fortaleza de las Contraseñas

TIPO	EJEMPLO	TIEMPO (MÉTODO)	NIVEL DE SEGURIDAD
10 Random CHAR	jskervergs	59 minutos	RIESGOSO
10 Random CHAR+NUM	jskerver43	1 día	RIESGOSO
10 Random CHAR + NUM + MAY + MIN + SYM	?jPk3rv3r0	800 años	SEGURO
Palabra Diccionario	naranja	200 milisegundos	NO SIRVE
Palabra Inventada	gulofunch	2 minutos	NO SIRVE

<https://howsecureismypassword.net/>



Fortaleza de las Contraseñas

TIPO	EJEMPLO	TIEMPO (MÉTODO)	NIVEL DE SEGURIDAD
10 Random CHAR	jskervergs	59 minutos	RIESGOSO
10 Random CHAR+NUM	jskerver43	1 día	RIESGOSO
10 Random CHAR + NUM + MAY + MIN + SYM	?jPk3rv3r0	800 años	SEGURO
Palabra Diccionario	naranja	200 milisegundos	NO SIRVE
Palabra Inventada	gulofunch	2 minutos	NO SIRVE

<https://howsecureismypassword.net/>



Forbes

Billionaires

Innovation

Leadership

Money

Consumer

187,650 views | Dec 14, 2018, 11:45am

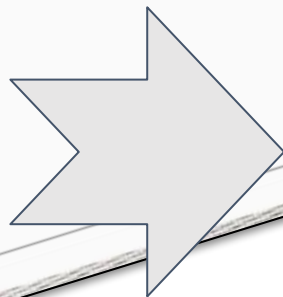
The Worst Passwords Of 2018 Show The Need For Better Practices

Kate O'Flaherty Contributor @
Cybersecurity

I'm a freelance cyber security journalist.



TOP 10



123456

password

123456789

12345678

12345

111111

1234567

sunshine

qwerty

iloveyou



El eslabón más débil de la cadena es el usuario



Kate O'Flaherty Contributor
Cybersecurity
I'm a freelance cyber security journalist.

- 123456
- password
- 12345
- 1111
- 1234567
- sunshine
- qwerty
- iloveyou



Los usuario somos
VAGOS



nunca subestimes
nuestra vagancia



SISTEMA 1

SISTEMA 2



Intuición

Respuesta rápida

Emoción

Aprendizaje

Respuesta lenta

Lógica y deducción





@perezmvictoria | @j0sm3ll | #testinguy





¡Propongamos soluciones para hacer Seguridad Usable!

@perezmvictoria | @j0sm3ll | #testinguy



Fortaleza de las Contraseñas

TIPO	EJEMPLO	TIEMPO	NIVEL DE SEGURIDAD
2 palabras comunes	Buen día	5 meses	BAJO RIESGO
3 palabras comunes	Esto es divertido	10 billones de años	SEGURO

<https://howsecureismypassword.net/>



Fortaleza de las Contraseñas

TIPO	EJEMPLO	TIEMPO	NIVEL DE SEGURIDAD
2 palabras comunes	Buen día	5 meses	BAJO RIESGO
3 palabras comunes	Esto es divertido	10 billones de años	SEGURO
10 Random CHAR + NUM + MAY + MIN + SYM	?jPk3rv3r0	800 años	SEGURO



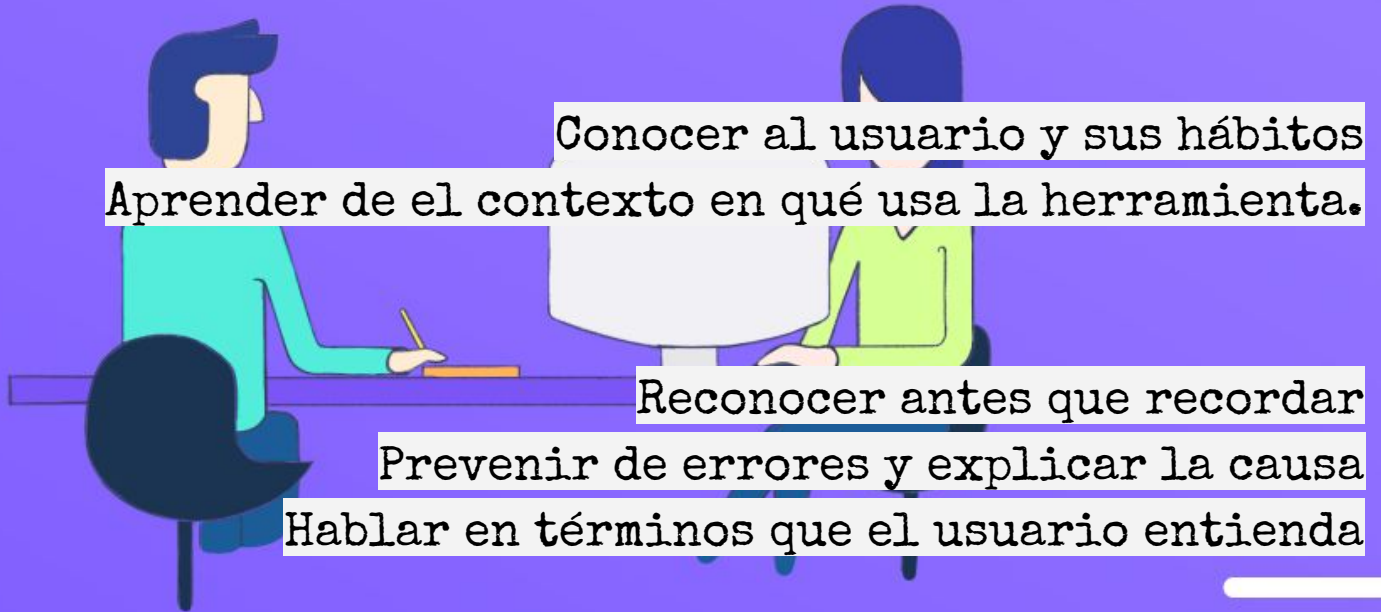
TIPS



Seguridad Usable debe estar desde la concepción del producto y en los planes de pruebas.



TIPS



TIPS



www.shutterstock.com • 131861585

-> El usuario no puede ser responsable de toda la seguridad

-> Las medidas de seguridad deben ser transparentes al usuario

-> Pongamos las medidas de seguridad solo cuando son necesarias



CONCLUSION



Complejidad no
garantiza seguridad






«TestingUy»

¿PREGUNTAS?

¡MUCHAS GRACIAS!

Josmell Chavarri

josmell.chavarri@guayoyo.io
@j0sm3ll

 Guayoyo

Victoria Perez

perezmvictoria@gmail.com
@perezmvictoria

pyxis 


13 y 14 de mayo, 2019
testinguy.org | @testinguy | #testinguy



<TestingUy>

Josmell Chavarri

josmell.chavarri@guayoyo.io
@j0sm3ll

 Guayoyo

Victoria Perez

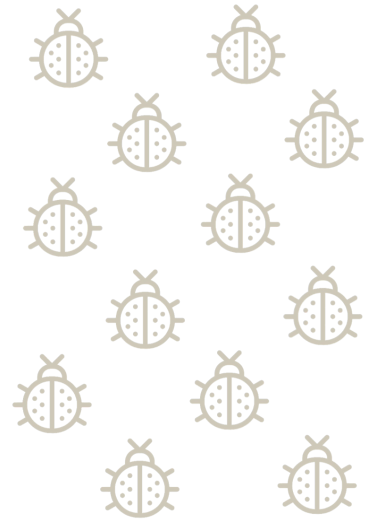
perezmvictoria@gmail.com
@perezmvictoria

pyxis 

13 y 14 de mayo, 2019
testinguy.org | @testinguy | #testinguy

Fuentes

- [5 Razones porque eres malo eligiendo pswd](#)
- [Introducción a la seguridad para la experiencia de usuario](#)
- [Cuanta más seguridad es igual a más inseguro](#)
- [Diseñando para usuarios](#)
- <https://www.sachinuppal.com/blog/ux-design/3-button-designs-that-changed-history/>
- <https://www.mindflowdesign.com/insights/user-centric-design-the-lessons-of-3-mile-island/>
- <https://psnet.ahrq.gov/perspectives/perspective/33/In-Conversation-With-Donald-A-Norman-PhD>
- <https://www.baekdal.com/trends/password-security-usability>
- <https://www.baekdal.com/thoughts/the-usability-of-passwords-faq/>
- <http://sid.toolness.org/ch13yee.pdf>
- <https://www.coursera.org/learn/usable-security/lecture/KOjBU/usable-authentication-and-passwords>
- <https://latam.kaspersky.com/blog/cybercrime-inc-how-profitable-is-the-business/8098/>
- <https://www.forbes.com/sites/kateoflahertyuk/2018/12/14/these-are-the-top-20-worst-passwords-of-2018/#69692aa04541>
- <https://www.baekdal.com/thoughts/the-usability-of-passwords-faq/>
- <https://www.itdigitalsecurity.es/actualidad/2018/04/las-ganancias-del-ciber crimen-alcanzan-los-15-billones-de-dolares>
- <https://www.welivesecurity.com/la-es/2016/11/03/modelo-de-negocio-del-ciber crimen/>



Gracias a: Edgar y Jorge Salazar, Rodrigo Gomez, Federico Reale y Virginia Abreu

