



# ¿POR QUÉ JHONNY NO PUEDE ENCRIPtar? GUIAS DE DISEÑO PARA SEGURIDAD USABLE

PhD. Paulo C. Realpe M.  
[pcrealpe@admon.uniajc.edu.co](mailto:pcrealpe@admon.uniajc.edu.co)



# Motivación/Introducción

El mundo está cada vez mas conectado

- El riesgo de ataque se incrementa.
- El cibercrimen se incrementa.
- Muchos (la mayoría?) de los ataques se enfocan en el elemento humano.

Necesitamos limitar el ataque al elemento humano y usar soluciones de seguridad.

La comunidad académica está de acuerdo en que la usabilidad es imprescindible para las soluciones de seguridad que van a utilizar los usuarios finales.

# Motivación/Introducción

3

## Seguridad usable para los usuarios finales?

Una característica de seguridad con que un usuario tiene que interactuar debería ser...

Invisible cuando no se necesita,  
Útil cuando si lo es.

# Motivación/Introducción

4



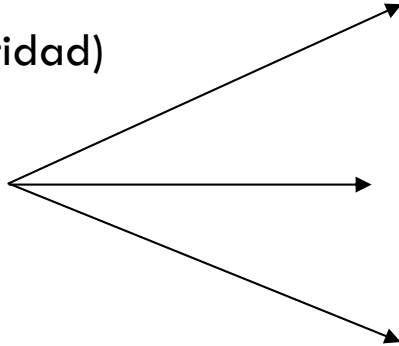
invisible



# Motivación/Introducción

5

Autenticación  
(Confirmar la identidad)



facebook.



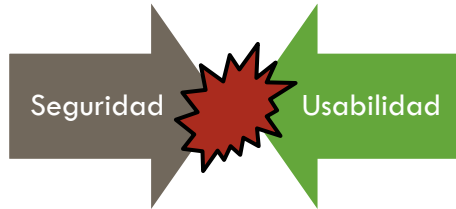
Gmail



BBVA



Usable?



# Motivación/Introducción

6



Fecha y hora actual: Miércoles 28 de Octubre de 2020 2:08:35 PM

## Inicio de sesión

### Imagen y frase de seguridad seleccionadas

Verifica que tu imagen y frase de seguridad sean correctas, de esta manera te asegurarás de estar ingresando a la Sucursal Virtual Personas de Bancolombia.

**Clave**

Si la imagen y frase no son las que has definido, por seguridad no ingreses la clave.

Ingresar tu clave

Ingresar mediante el teclado virtual la clave que usas en el cajero automático.

Genera una clave personal



Usable?

# Motivación/Introducción

“Los mecanismos de seguridad solo son efectivos cuando se usan correctamente”

*Jeremy Hyland*

Si Usable entonces

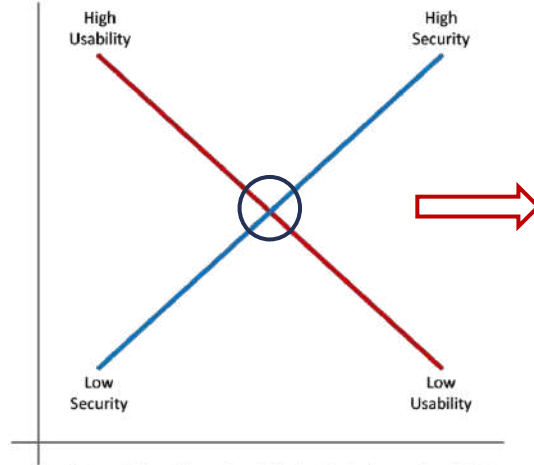
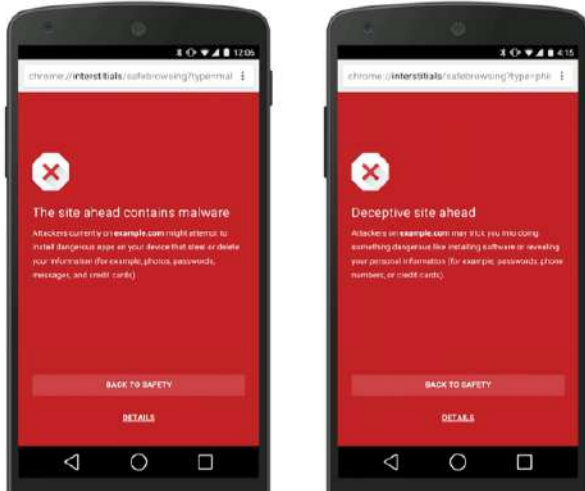


sino



# Motivación/Introducción

El error humano es la causa mas común para los problemas de seguridad.



Guías USec  
(Whitten & Tygar, 1999)

Figure 1: Security and usability tend to be inversely related





# Motivación/Introducción

9

La seguridad usable es una ciencia,  
pero poca gente lo trata como una ciencia.

**Interdisciplinario**

# ¿Por qué Johnny no puede encritpar?

Whitten and Tygar, (1999). Why Johnny Can't Encrypt: A Usability Evaluation of PGP.

[http://www.usenix.org/publications/library/proceedings/sec99/full\\_papers/whitten/whitten.html/index.html](http://www.usenix.org/publications/library/proceedings/sec99/full_papers/whitten/whitten.html/index.html)

<p><b>Why Johnny Can't Encrypt: A Usability Evaluation of PGP</b></p> <p>Technical University of Brno Erasmus Summer Seminar jan.sousedek@seznam.cz</p>	<p><b>Why Johnny Still Can't Encrypt: Evaluating the Usability of Email Encryption</b></p> <p>Steve Sheng Engineering and Public Policy Carnegie Mellon University shengx@cmu.edu</p> <p>Levi Broderick Electrical and Computer Engineering Carnegie Mellon University lpb@ece.cmu.edu</p> <p>Jeremy Heinz School of Man Carnegie M jhyland@ar</p>		
<p><b>Why Johnny Can't Encrypt: Evaluating the Usability of PGP</b></p> <p>Scott Ruoti, Jeff Andersen {ruoti, andersen}@</p>	<p>Why Johnny Can't Encrypt: A Usability Evaluation of PGP</p> <p>Whitten, J. S. Tygar, D. M.</p> <p>University of California, Berkeley</p> <p>whitten@cs.berkeley.edu tygar@cs.berkeley.edu</p>		

# ¿Por qué Johnny no puede encritpar?

Para Whitten y Tygar (1999), las características de seguridad es usable si las personas que lo utilicen:

- Están informados de manera confiable sobre las tareas de seguridad que deben realizar.
- Son capaces de descubrir cómo realizar con éxito esas tareas.
- No cometen errores “peligrosos”.
- Están lo suficientemente cómodos con la interfaz para seguir usándola.

# ¿Por qué Johnny no puede encritpar?

## ¿Por qué es difícil la seguridad usable?

1. Los usuarios desmotivados. La seguridad suele ser un objetivo secundario.
2. Abstracción de políticas. Los programadores entienden la representación, pero los usuarios normales no tienen conocimientos previos.
3. La falta de retroalimentación. Necesidad de evitar errores “peligrosos”.
4. Necesita centrarse en la prevención de errores.
5. El eslabón más débil. El atacante solo necesita encontrar una vulnerabilidad.

# ¿Por qué Johnny no puede encritpar?

Los errores de usuario causan o contribuyen a la mayoría de las fallas de seguridad de las computadoras, sin embargo, las interfaces de usuario para la seguridad tienden a ser torpes, confusas o casi inexistentes. *¿Se debe simplemente a una falla en la aplicación de técnicas de diseño de interfaz de usuario estándar a la seguridad?*

# ¿Por qué Johnny no puede encriptar?

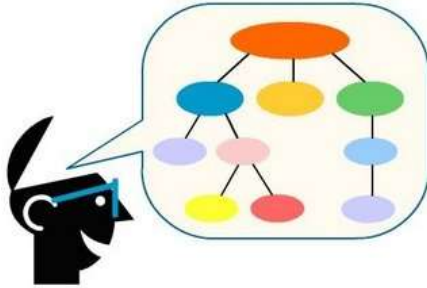


Se realiza un estudio de caso de un programa de seguridad que tiene una “buena” interfaz de usuario según los diseñadores: PGP 5.0 (Pretty Good Privacy). El análisis encontró una serie de fallas en el diseño de la interfaz de usuario que pueden contribuir a fallas de seguridad.

Demostró que cuando los participantes de la prueba se les dio un tiempo para firmar y encriptar un mensaje usando PGP, la mayoría de ellos no pudieron hacerlo con éxito.

# Guías de Diseño – Seguridad Usable

## Modelo Mental



## Diseño iterativo



## Fuente de conflicto



## Permiso y autoridad



# Guías de Diseño – Seguridad Usable

## 1. Realizar la tarea mas fácil con la menor concesión de autoridad.

### INICIAR SESIÓN

Completa tus datos. Si ya tienes una cuenta en nuestros portales Informativos, inicia sesión con tu correo electrónico y contraseña registrada.

Mostrar

¿Olvidaste tu contraseña?

INICIAR SESIÓN

[O crea una cuenta](#)

---

O conéctate desde

f FACEBOOK

Nunca publicaremos en tu muro sin tu permiso

---

[TÉRMINOS Y CONDICIONES](#) • [POLÍTICA DE PRIVACIDAD](#)

### REGISTRO

**OPCIÓN 1**  
COMPLETA TUS DATOS

Mostrar

He leído, entendido y autorizo los [Términos y Condiciones](#), la [Política de Tratamiento de Datos de CASA EDITORIAL EL TIEMPO S.A.](#) y su [Política de datos de Navegación/cookies](#).

No soy un robot

CREA UNA CUENTA

[Si ya tienes cuenta ingresa aquí](#)

Facebook - Google Chrome

facebook.com/login.php?skip\_apl\_login=1&api\_key=6218097478

f Facebook

Log in to use your Facebook account with EL TIEMPO Casa Editorial.

Email or Phone:

Password:

Log In

[Forgot account?](#)

Create New Account



# Guías de Diseño – Seguridad Usable

## 2. Otorgar autoridad a otros de acuerdo con las acciones del usuario que indiquen su consentimiento.



**Washington Post Social Reader**

Share what you read with friends!

Okay, Read Article

Cancel

---

**ABOUT THIS APP**

This app shares articles with your friends as you read them. Click Okay, Read Article to start.

Who can see posts this app makes for you on your Facebook timeline: [?]

Friends ▼

**THIS APP WILL RECEIVE:**

- Your basic info [?]
- About You
- Your likes

This app may post on your behalf, including articles you read, people you liked and more.

By proceeding, you agree to Washington Post Social Reader's [Terms of Service](#) and [Privacy Policy](#) · Report App

# Guías de Diseño – Seguridad Usable

## 3. Ofrecer al usuario formas de reducir la autoridad de otros para acceder a los recursos del usuario.

### Revocar autoridad

The screenshot shows the Facebook 'Configuración y herramientas de privacidad' page. On the left, a navigation menu lists various settings, with 'Privacidad' selected. The main content area is divided into sections: 'Accesos directos de privacidad' (links to important privacy options), 'Administrar tu perfil' (manage who can see your profile), 'Consultar aspectos básicos de la privacidad' (interactive guide), 'Tu actividad' (activity log), and '¿Quieres limitar los destinatarios de las publicaciones que compartiste con los amigos o que hiciste públicas?' (limit public posts). Each section includes a brief description and an 'Editar' (Edit) link.

# Guías de Diseño – Seguridad Usable

19

## 3. Ofrecer al usuario formas de reducir la autoridad de otros para acceder a los recursos del usuario.

The screenshot shows the Facebook settings page for 'Apps and sites web'. A red arrow points to the 'Apps and sites web' option in the left-hand navigation menu. The main content area is titled 'Apps y sitios web' and includes a description: 'Estas son apps y sitios web en los que iniciaste sesión con Facebook. Pueden recibir información que decidiste compartir con ellos. Las apps ceducadas y eliminadas podrán seguir accediendo a la información que se haya compartido con ellas previamente, pero no podrán recibir información nueva que no sea pública. Más información'. Below this, there are tabs for 'Activos', 'Cadaucados', and 'Eliminados', with 'Activos' selected. A search bar for 'Buscar apps y sitios web' is present. A list of active apps is shown, including 'Encuesta', 'Dell Like', 'edX', and 'Academia edu', each with a 'Ver y editar' link and a trash icon. At the bottom, there are two preference cards: 'Apps, sitios web y juegos' (set to 'Activado') and 'Notificaciones de juegos y apps' (set to 'Activado').

# Guías de Diseño – Seguridad Usable

## 4. Los usuarios deben saber qué autoridad tienen los demás.



**Download Free Games**  
#1 Source for Free Games

✔ No Adware or Spyware  
 • Safe & Easy Downloads  
 • No pirated software, 100% legal games

[Home](#)   [Free PC Games](#)   [Free Mobile Games](#)   [Free Online Games](#)   [Games by Genre](#)   [Jewel Quest](#)      [Search](#)

[Home](#) » [Puzzle Games](#) » [Laruaville 10](#)

Help to recover the Sun from Merlin's Castle in Laruaville 10



**Laruaville 10**

Avg. Rating: ★★★★★ (0 Player Ratings - Avg. Rating 0 out of 5) [Rate](#)

**Download & Play Free**

(Secure Download - NO Adware or Spyware!)

- What's Free - Play game for 100 minutes.
- File Size - 130 MB
- Play It On - Windows 7 or better

Advertisement

# Guías de Diseño – Seguridad Usable

## 5. Los usuarios deben saber qué autoridad tienen ellos mismos.

[Log Out](#) | [Help](#) | [Security and Protection](#)

**PayPal**

[My Account](#) | [Send Money](#) | [Request Money](#) | [Merchant Services](#) | [Products & Services](#)

[Overview](#) | [Add Money](#) | [Withdraw](#) | [History](#) | [Statements](#) | [Resolution Center](#) | [Profile](#)

### Transaction details

Payment Received (Unique Transaction ID # 8DG84457VDI [redacted])

Sent by: CafePress.com, Inc (The sender of this payment is Verified)

Payment sent from: [redacted]

Payment sent to: golbeck@ [redacted]

---

**Business Contact Information**

Customer Service URL: [redacted]

Customer Service Email: [redacted]

---

Amount received: \$51.92 USD  
 Fee amount: \$0.00 USD  
 Net amount: \$51.92 USD

[Issue a refund](#) ?

You have up to 60 days to refund the payment.

---

Date: Aug 12, 2014  
 Time: 11:39:14 PDT  
 Status: Completed

# Guías de Diseño – Seguridad Usable

22

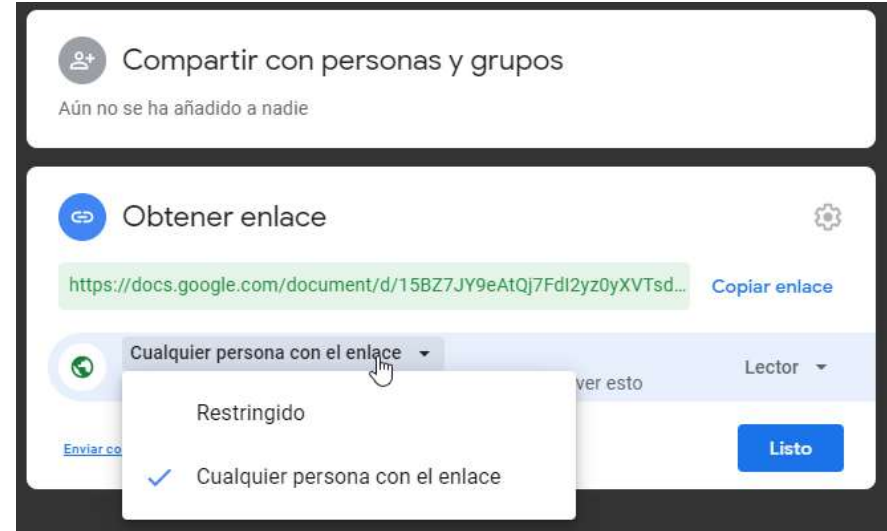
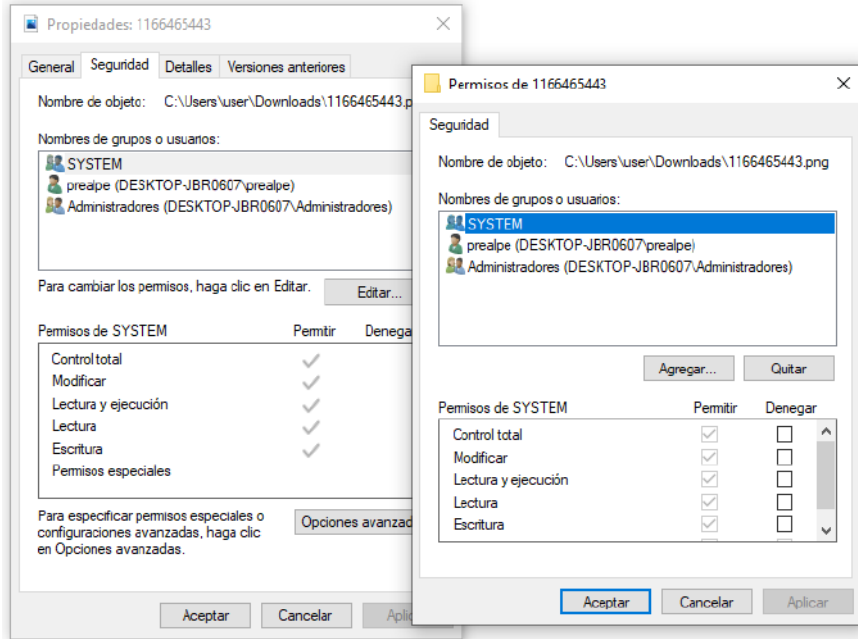
## 6. Hacer que los usuarios confíen en el software.



# Guías de Diseño – Seguridad Usable

23

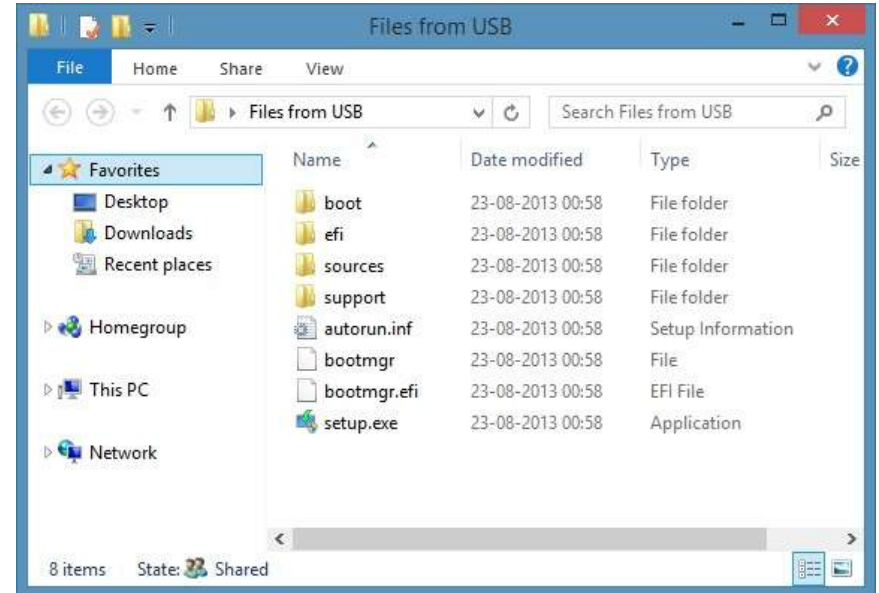
## 7. Permitir que el usuario exprese políticas de seguridad que se adapte a la tarea del usuario.



# Guías de Diseño – Seguridad Usable

24

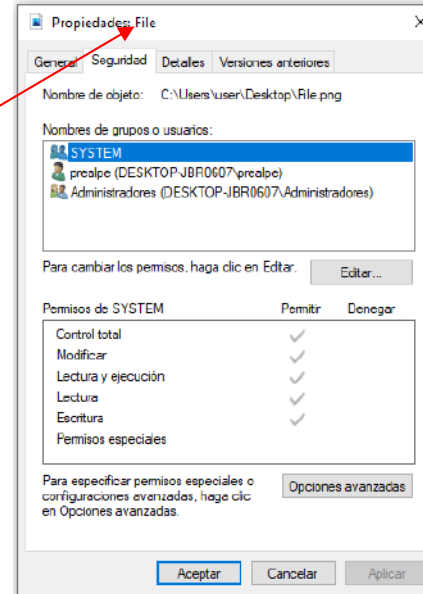
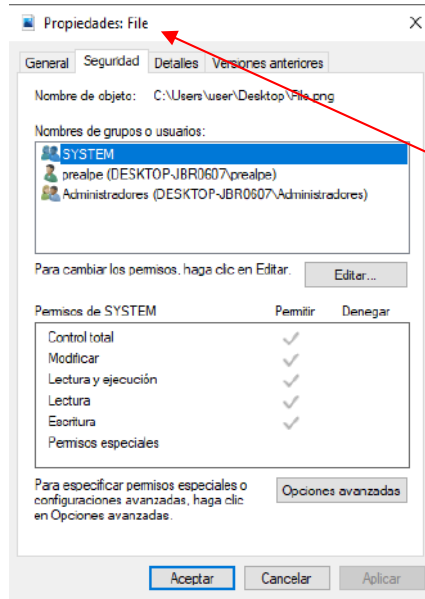
8. Dibujar distinciones entre objetos y acciones a lo largo de los límites relevantes para la tarea.





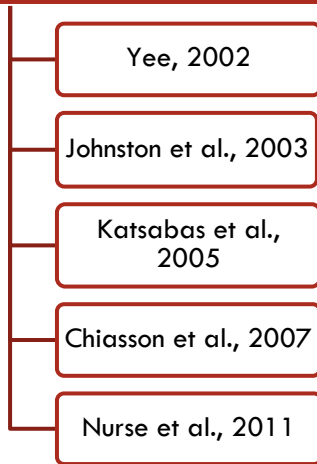
# Guías de Diseño – Seguridad Usable

## 9. Presentar objetos y acciones utilizando apariencias veraces y distinguibles.

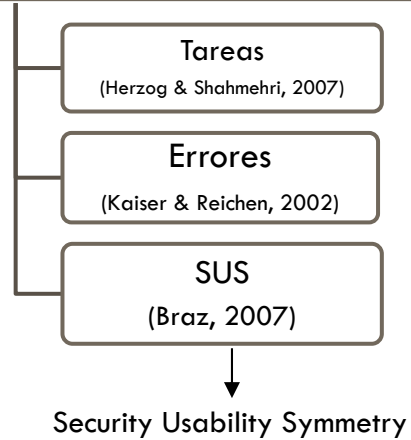


# Guías de Diseño – Seguridad Usable

## Guías de diseño USec



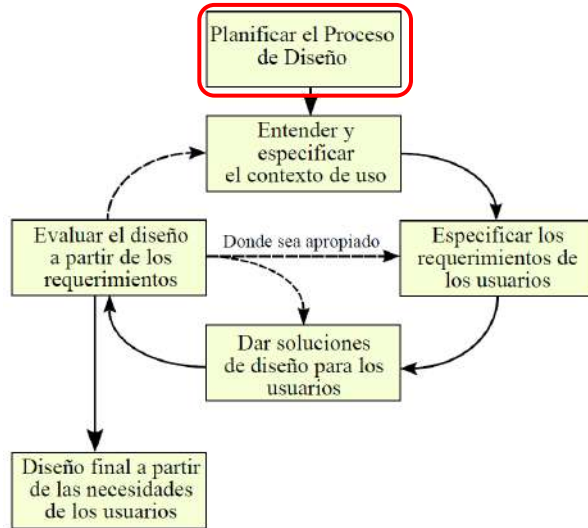
## Evaluación USec



# Desarrollo Heurístico USec

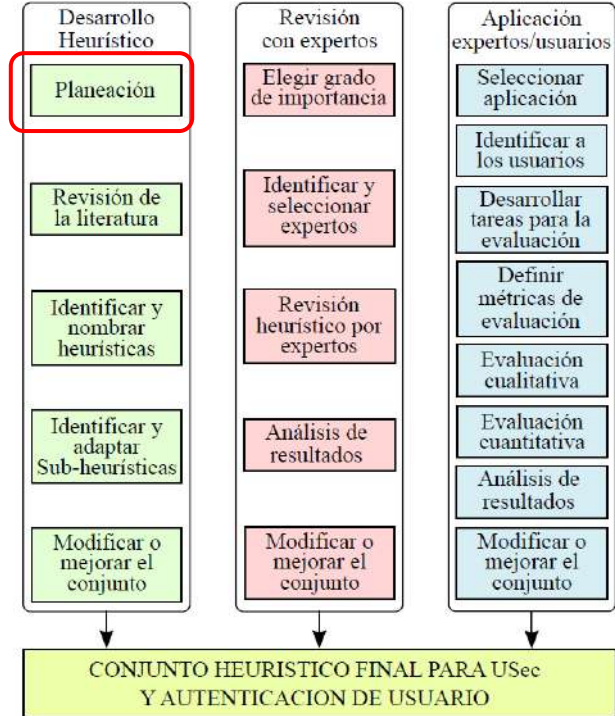
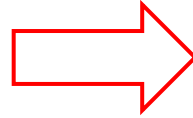
27

## ISO 9241-210



Diseño centrado en el humano para sistemas interactivos

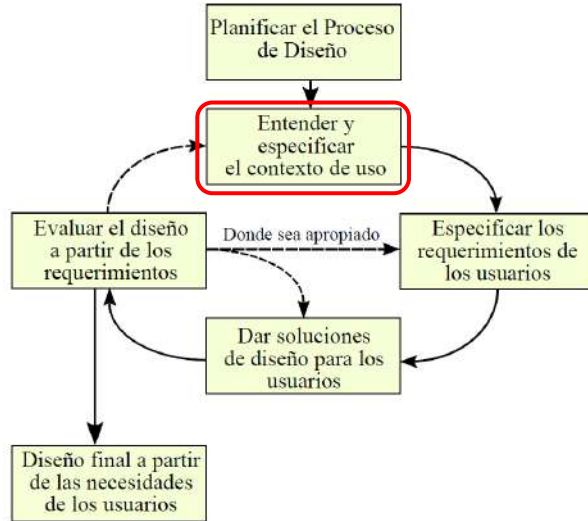
Integración



# Desarrollo Heurístico USec

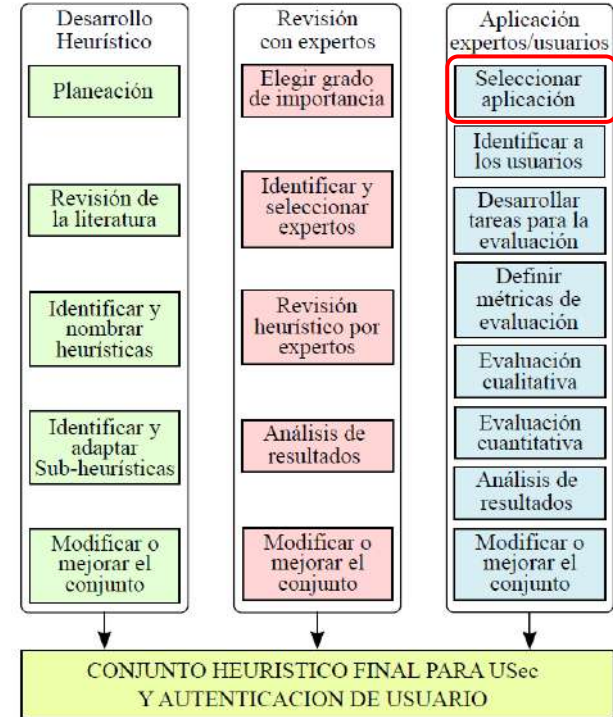
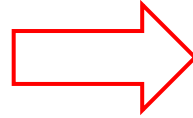
28

## ISO 9241-210



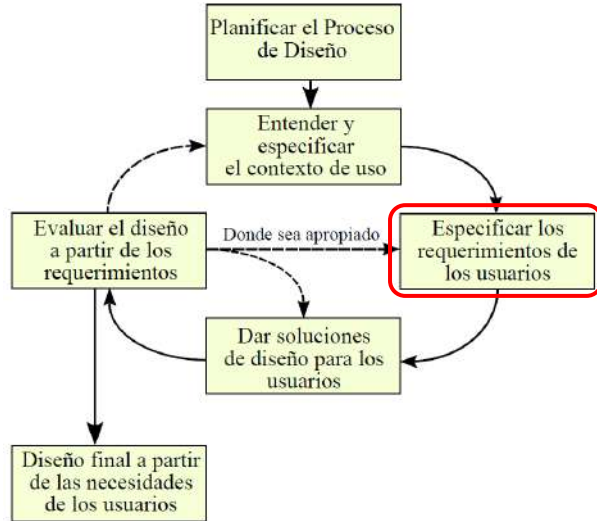
Diseño centrado en el humano para sistemas interactivos

Integración



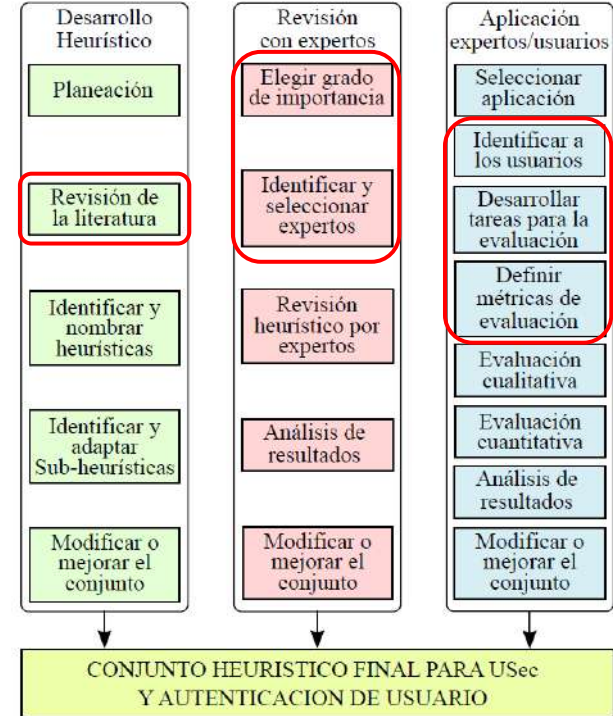
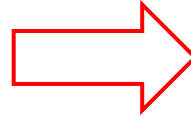
# Desarrollo Heurístico USec

## ISO 9241-210



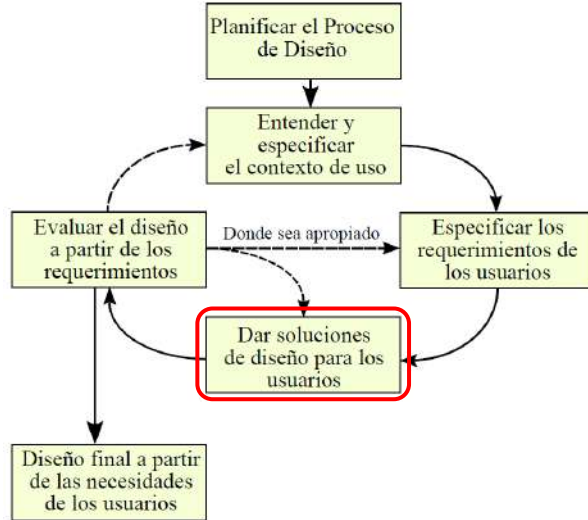
Diseño centrado en el humano para sistemas interactivos

Integración



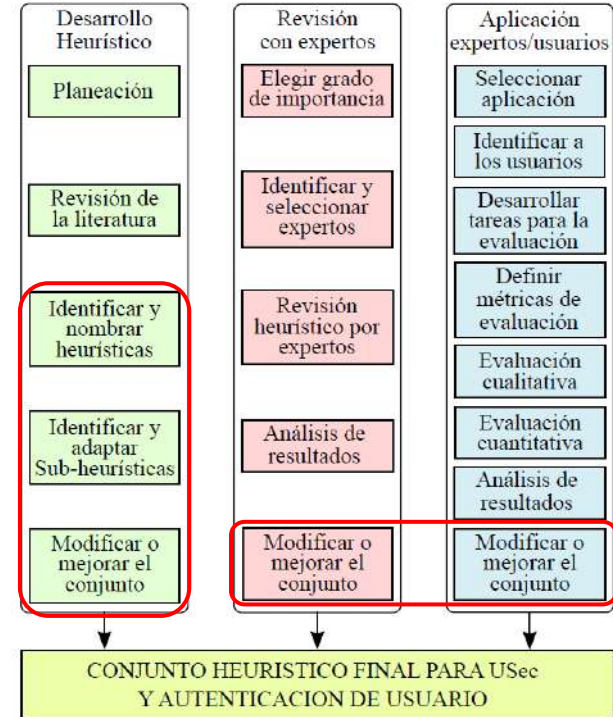
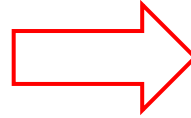
# Desarrollo Heurístico USec

## ISO 9241-210



Diseño centrado en el humano para sistemas interactivos

Integración

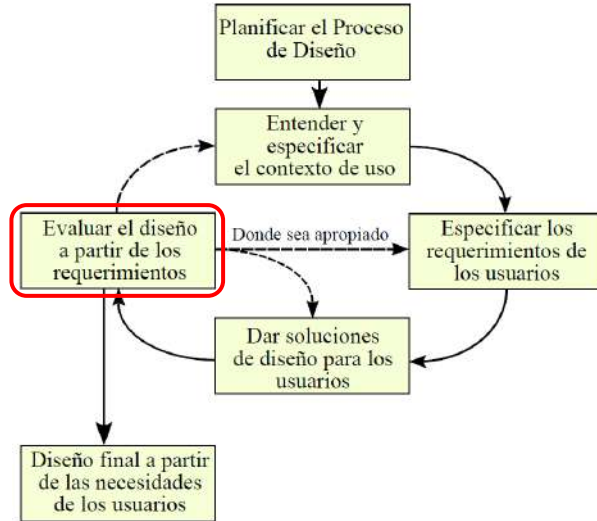




# Desarrollo Heurístico USec

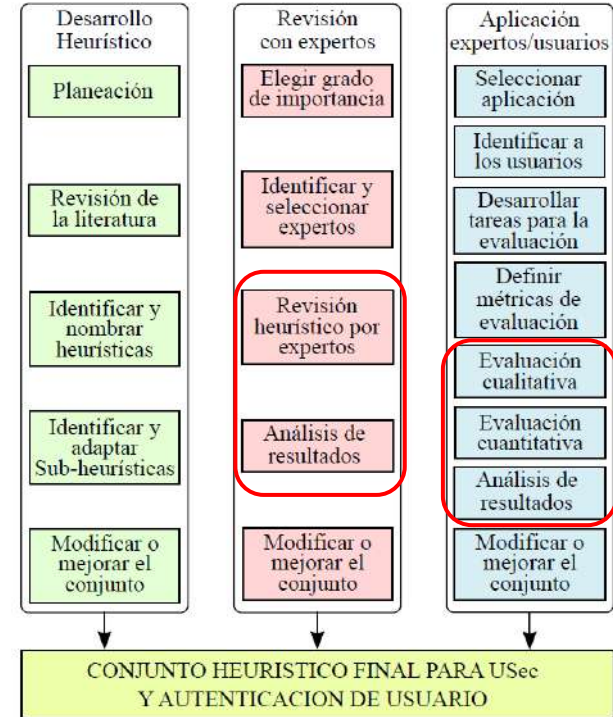
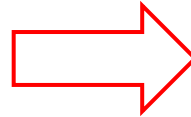
31

## ISO 9241-210



Diseño centrado en el humano para sistemas interactivos

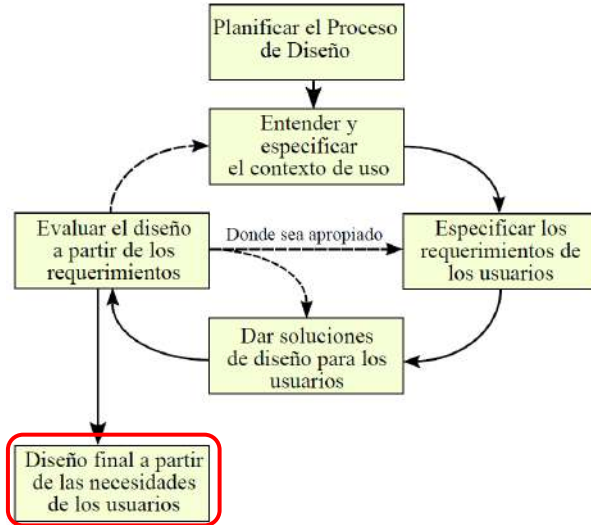
Integración



# Desarrollo Heurístico USec

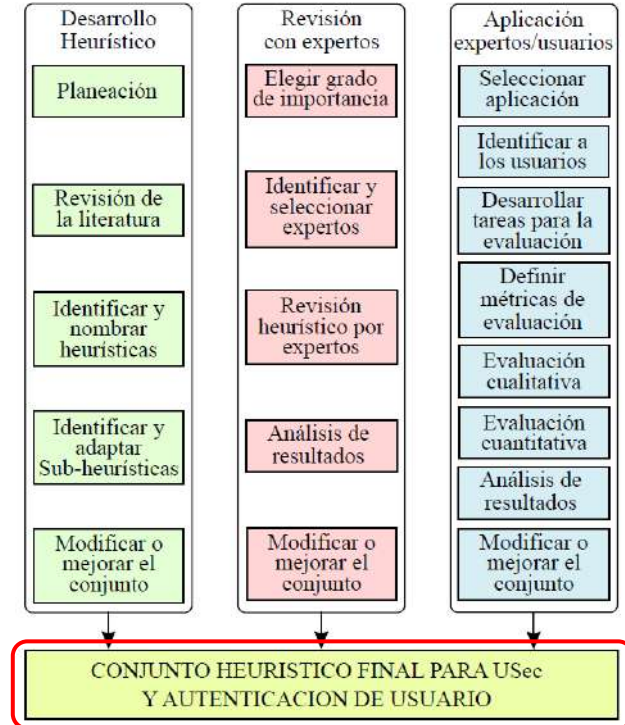
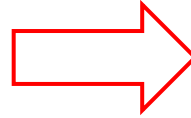
32

## ISO 9241-210



Diseño centrado en el humano para sistemas interactivos

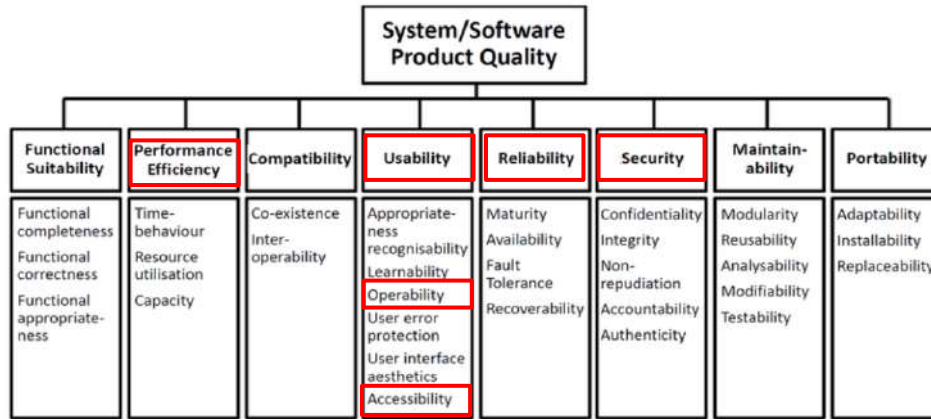
Integración



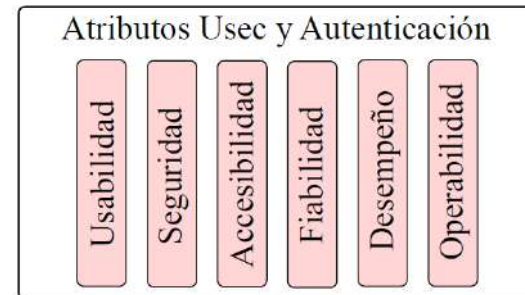


# Desarrollo Heurístico USec

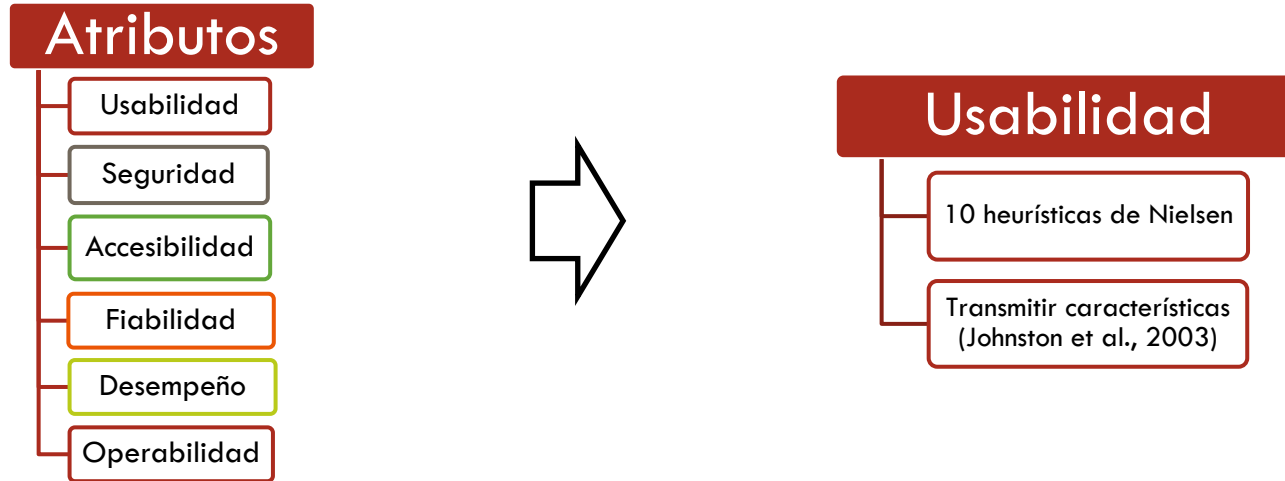
## ISO/IEC 25010:2011



Requisitos de calidad y evaluación de sistemas y software.



# Desarrollo Heurístico USec



# Desarrollo Heurístico USec

## Usabilidad

Heurística	Número de sub-heurísticas
Visibilidad del estado del sistema	11
Estética y mínimo diseño	5
Control y libertad de usuario	7
Utilización del lenguaje del usuario	5
Minimizar carga de memoria	9
Reconocer, diagnosticar y recuperarse de los errores	7
Flexibilidad y eficiencia de uso	7
Prevención de errores	5
Consistencia y estándares	6
Ayuda y documentación	6
Transmitir características	7
<b>TOTAL</b>	<b>75</b>

## USec y Autenticación

Atributo	Número de sub-heurísticas
Usabilidad	75
Seguridad	34
Accesibilidad	8
Desempeño	11
Operabilidad	9
Fiabilidad	15
<b>TOTAL</b>	<b>152</b>

# Desarrollo Heurístico USec

36

## Niveles de Importancia

Nivel	Descripción
S	Las sub-heurísticas de grado <b>S</b> son <b>vitales</b> para que el sistema evite violaciones de seguridad y usabilidad, y asegurarse que el usuario alcance una experiencia adecuada.
SS	Las sub-heurísticas de grado <b>SS</b> son <b>importantes</b> para que el sistema evite violaciones de seguridad y usabilidad, y asegurarse que el usuario alcance una experiencia adecuada.
SSS	Es <b>recomendable</b> considerar las sub-heurísticas de grado <b>SSS</b> para que el sistema evite violaciones de seguridad y usabilidad, y asegurarse que el usuario alcance una experiencia adecuada.

**Evaluación heurística de Seguridad Usable y Autenticación  
cualitativa y cuantitativa**

Gracias!

