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

PhD. Paulo C. Realpe M.
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

Seguridad usable para los usuarios finales?

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

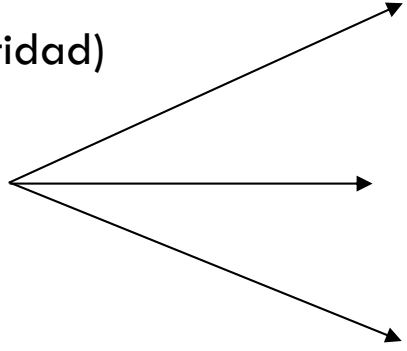
Invisible cuando no se necesita,
Útil cuando si lo es.

Motivación/Introducción

invisible

Motivación/Introducción

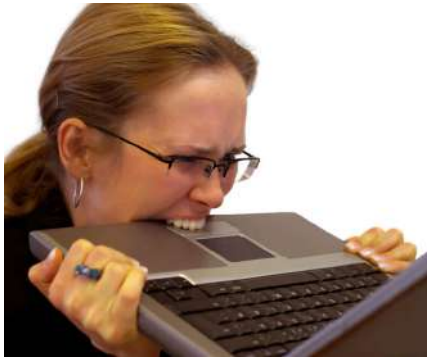
Autenticación
(Confirmar la identidad)



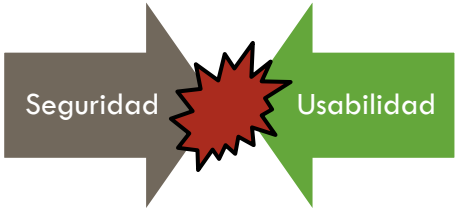
facebook

Gmail

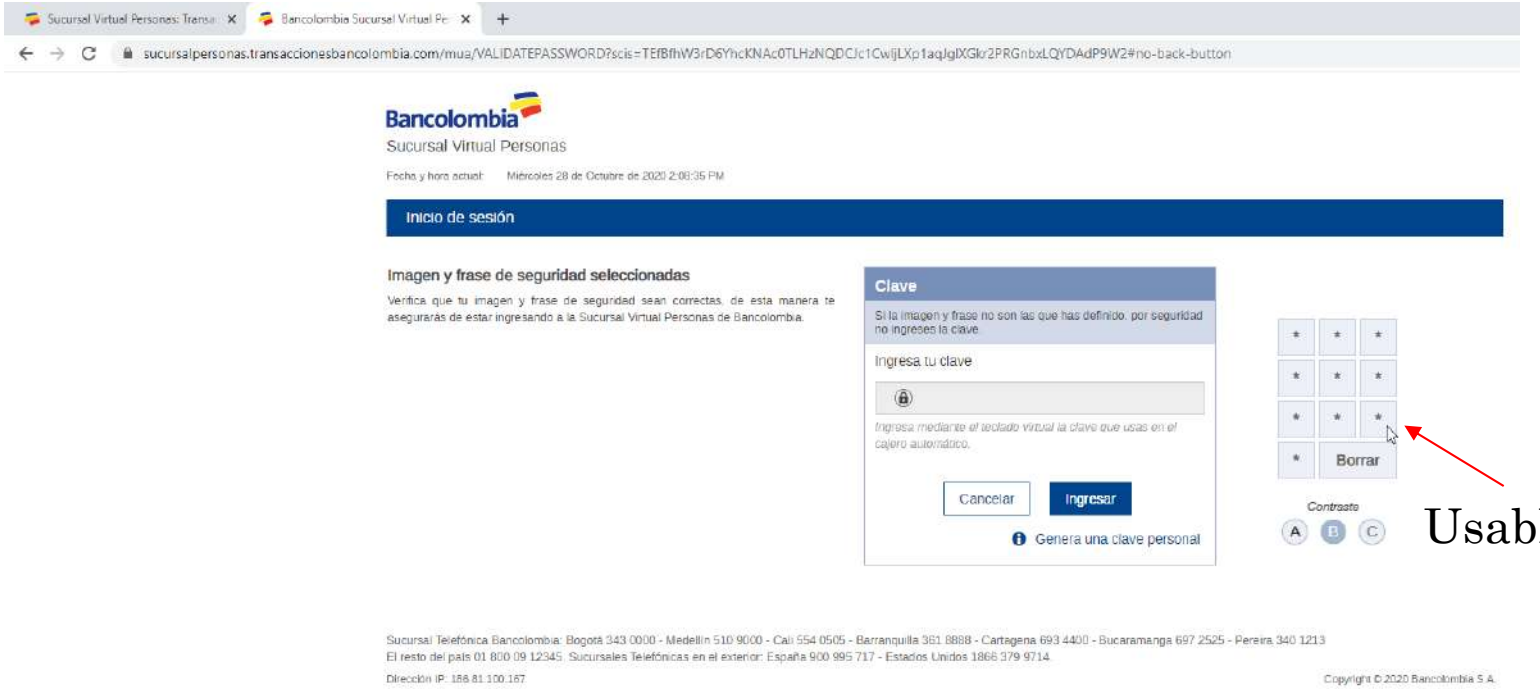
BBVA



Usable?



Motivación/Introducción



Motivación/Introducción

"Los mecanismos de seguridad solo son efectivos cuando se usan correctamente"

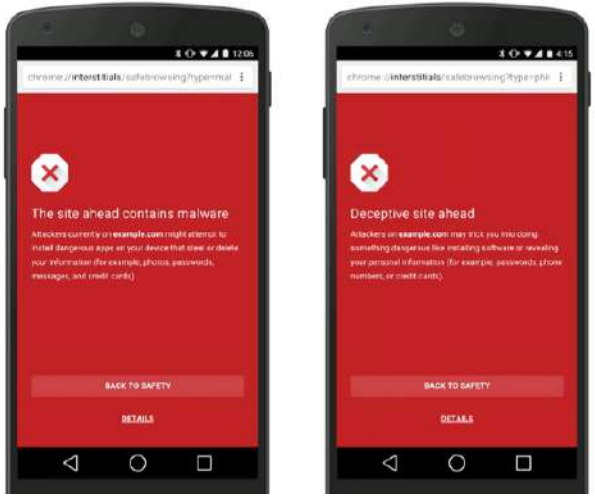
Jeremy Hyland

Si Usable entonces

sino

Motivación/Introducción

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



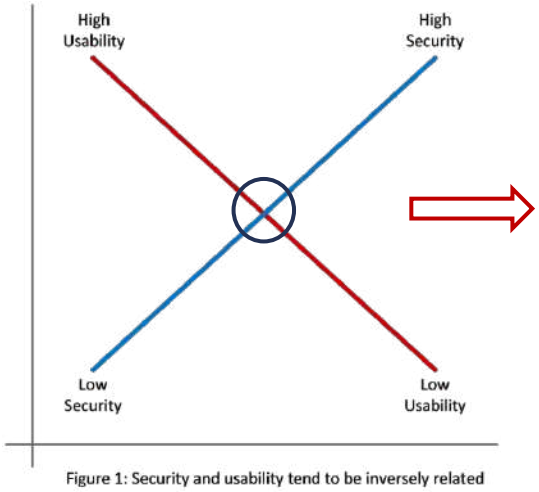


Figure 1: Security and usability tend to be inversely related

Guías USec

(Whitten & Tygar,1999)

Motivación/Introducción

La seguridad usable es una ciencia,

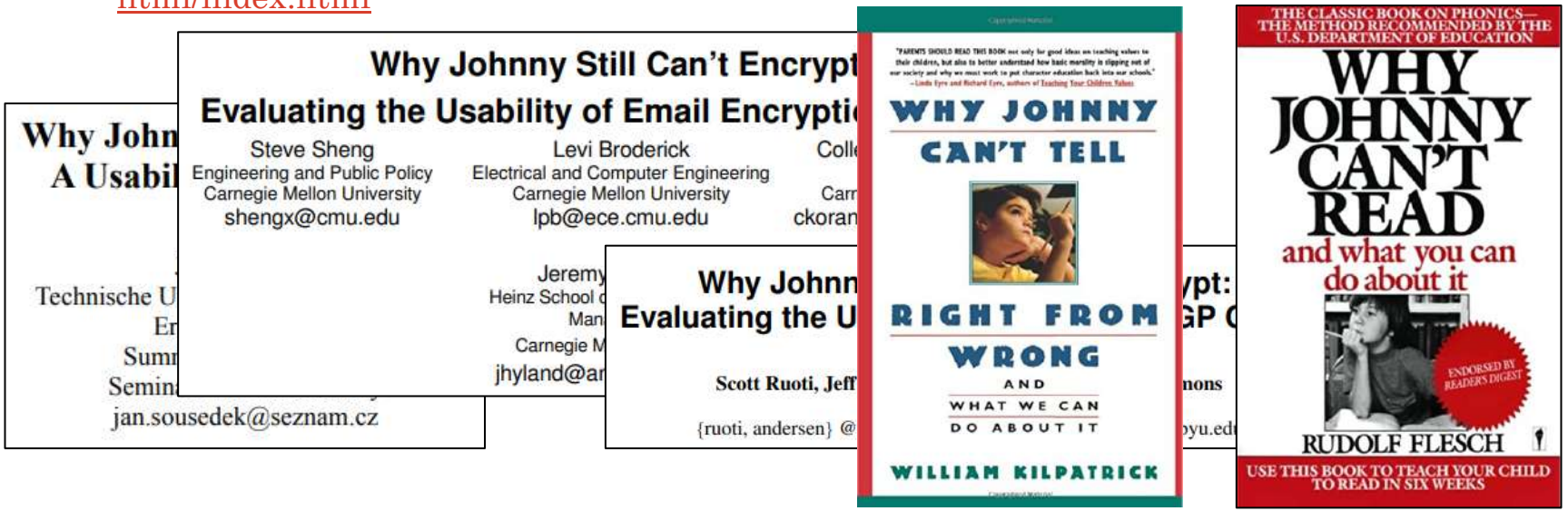
pero poca gente lo trata como una ciencia.

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



¿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”.

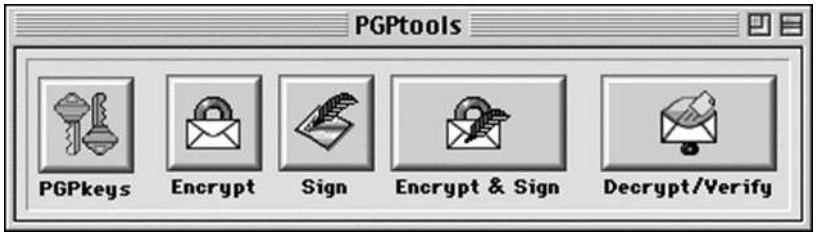
4. Necesita centrarse en la prevención de errores.

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 encritpar?



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.

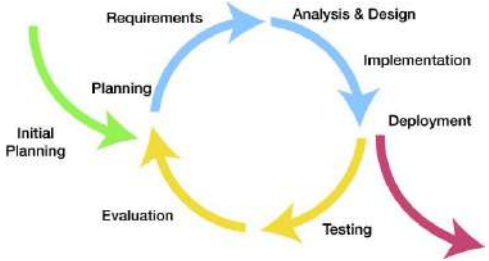
Demostró que cuando los participantes de la prueba se les dio un tiempo para firmar y encriptar un mensaje usando PGP, la mayoría de ellos no pudieron hacerlo con éxito.

Guías de Diseño – Seguridad Usable

Modelo Mental

Fuente de conflicto

Diseño iterativo



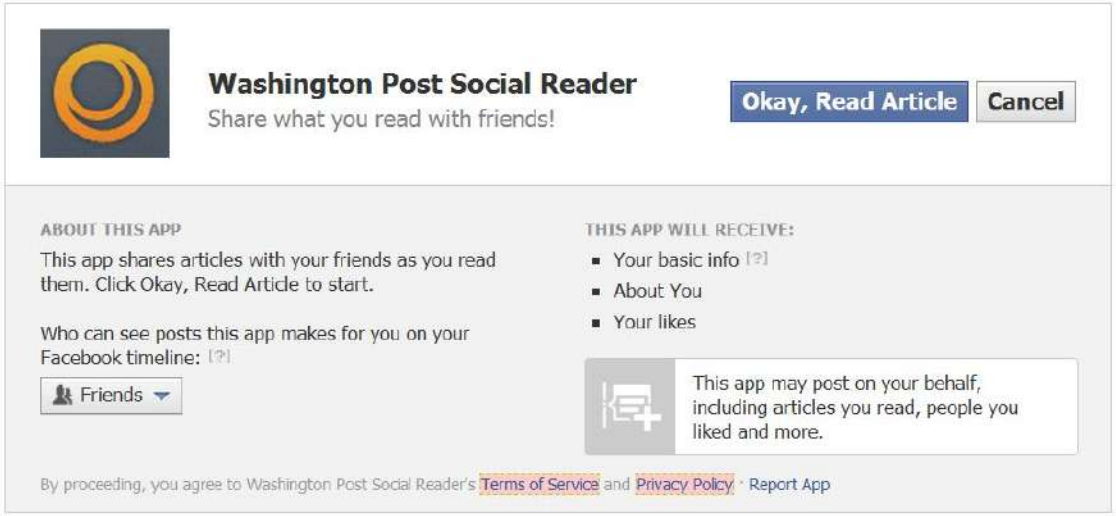
Permiso y autoridad

Guías de Diseño – Seguridad Usable

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

Guías de Diseño – Seguridad Usable

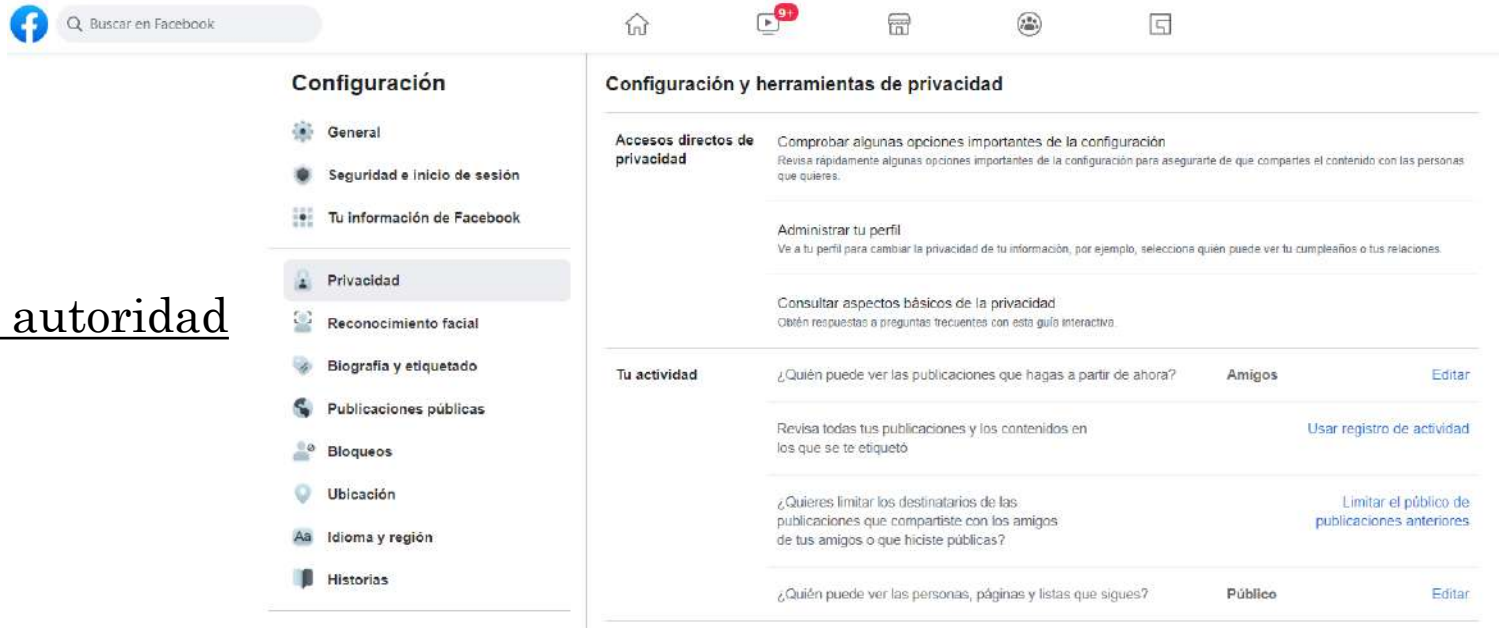
2. Otorgar autoridad a otros de acuerdo con las acciones del usuario que indiquen su consentimiento.



Guías de Diseño – Seguridad Usable

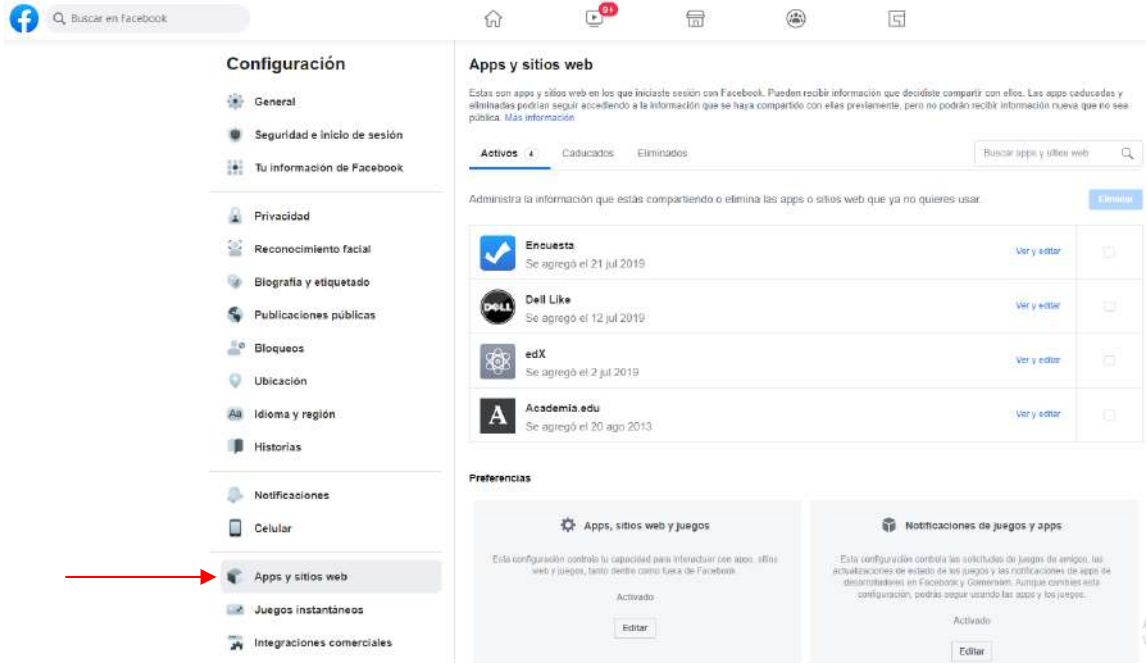
3. Ofrecer al usuario formas de reducir la autoridad de otros para acceder a los recursos del usuario.

Revocar autoridad



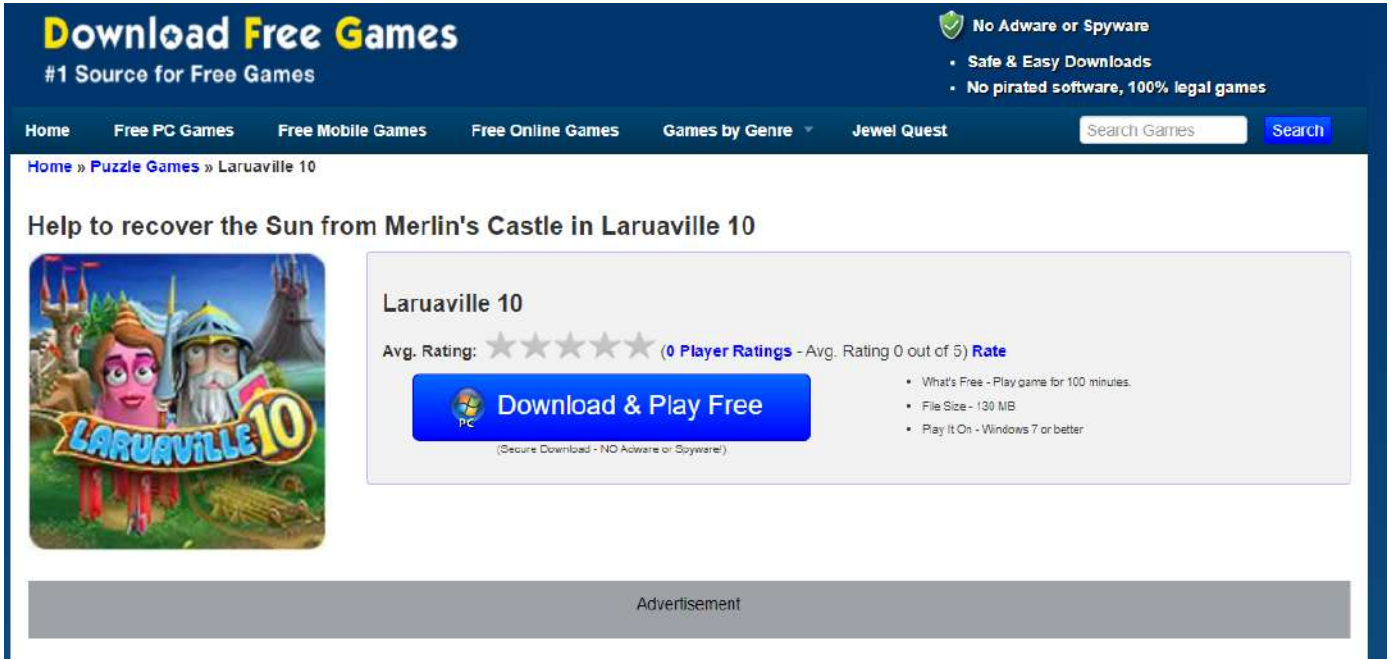
Guías de Diseño – Seguridad Usable

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



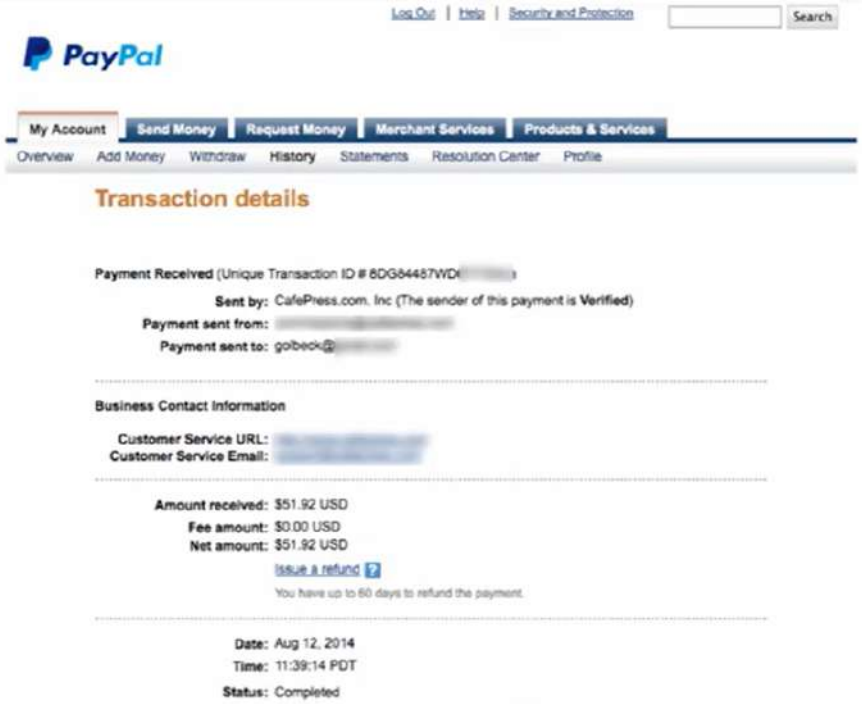
Guías de Diseño – Seguridad Usable

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



Guías de Diseño – Seguridad Usable

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

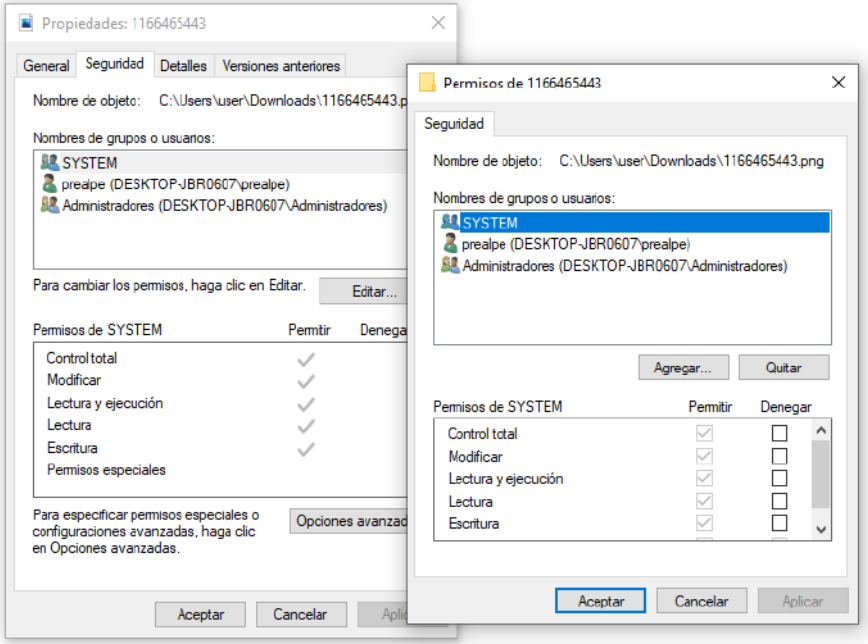


Guías de Diseño – Seguridad Usable

6. Hacer que los usuarios confíen en el software.

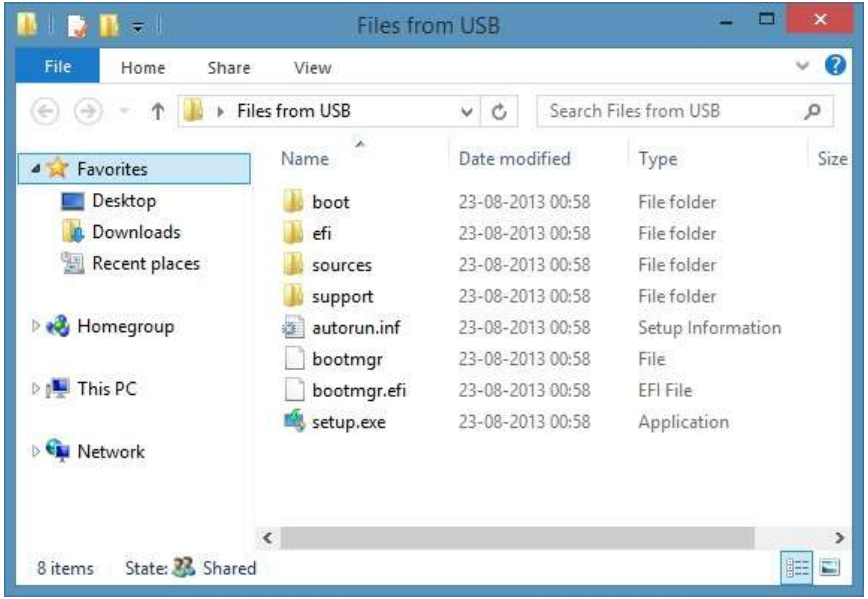
Guías de Diseño – Seguridad Usable

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



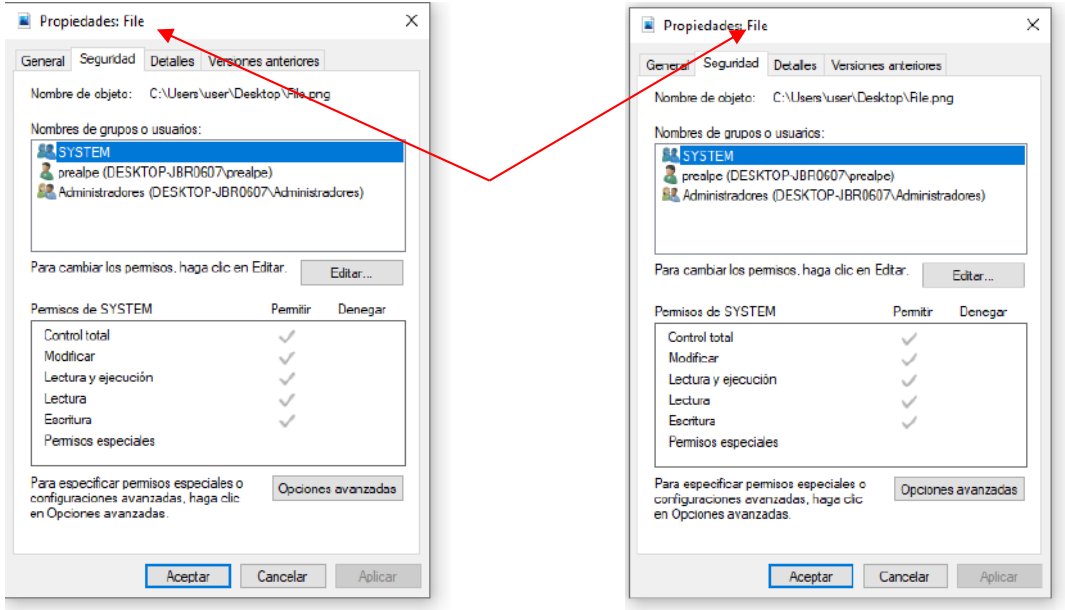
Guías de Diseño – Seguridad Usable

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

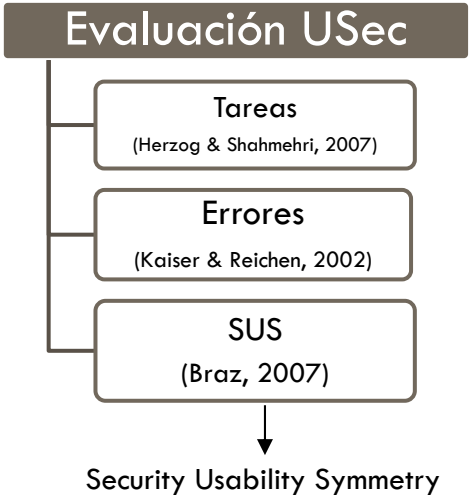


Guías de Diseño – Seguridad Usable

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

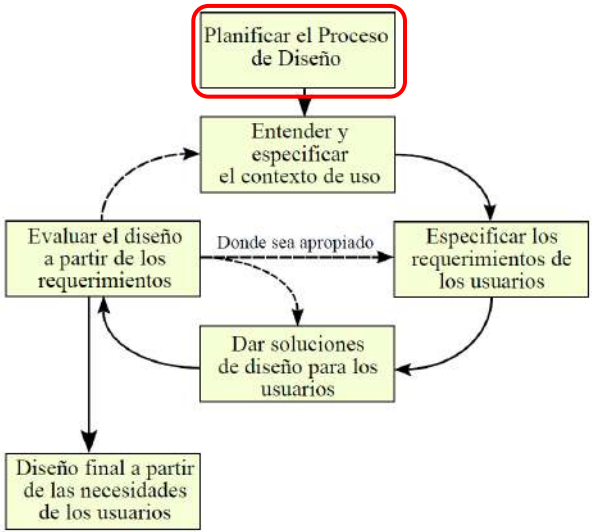


Guías de Diseño – Seguridad Usable



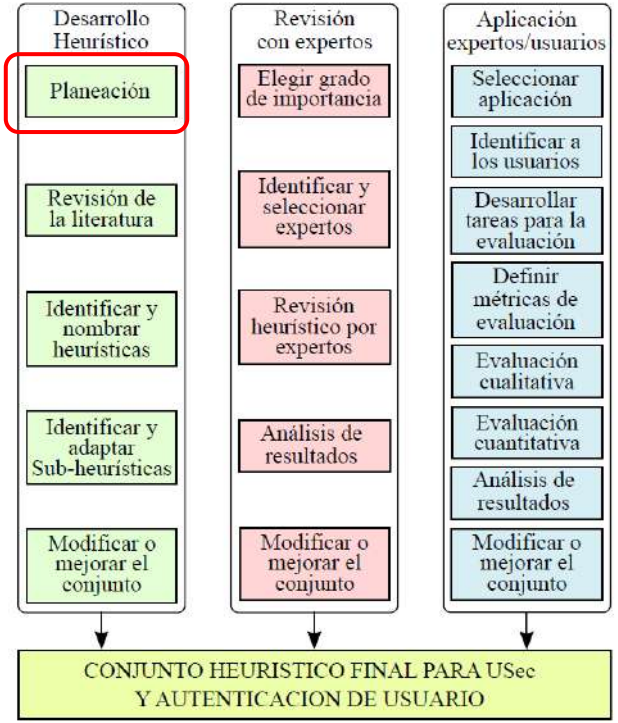
Desarrollo Heurístico USec

ISO 9241-210



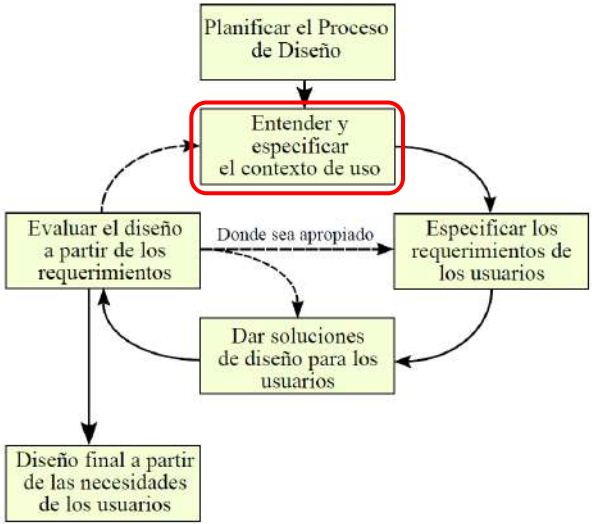
Diseño centrado en el humano para sistemas interactivos

Integración



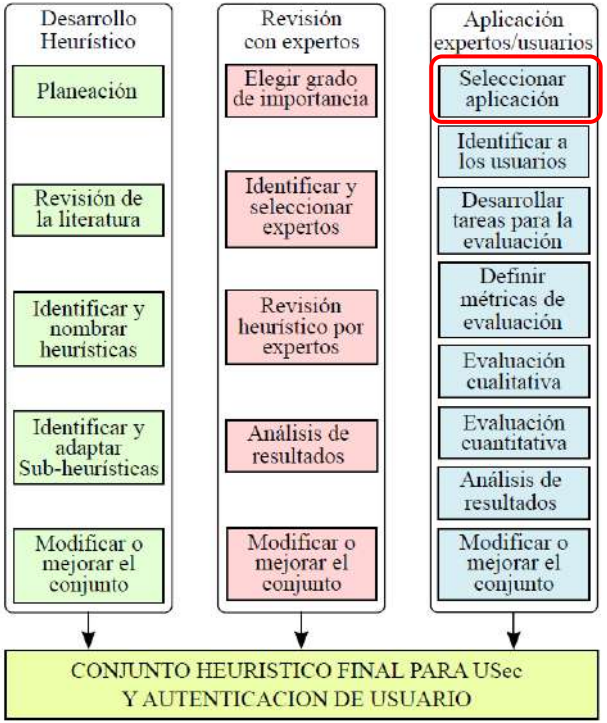
Desarrollo Heurístico USec

ISO 9241-210



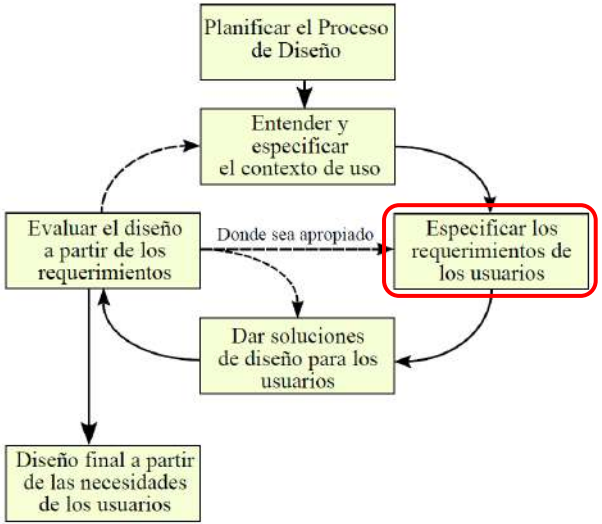
Diseño centrado en el humano para sistemas interactivos

Integración



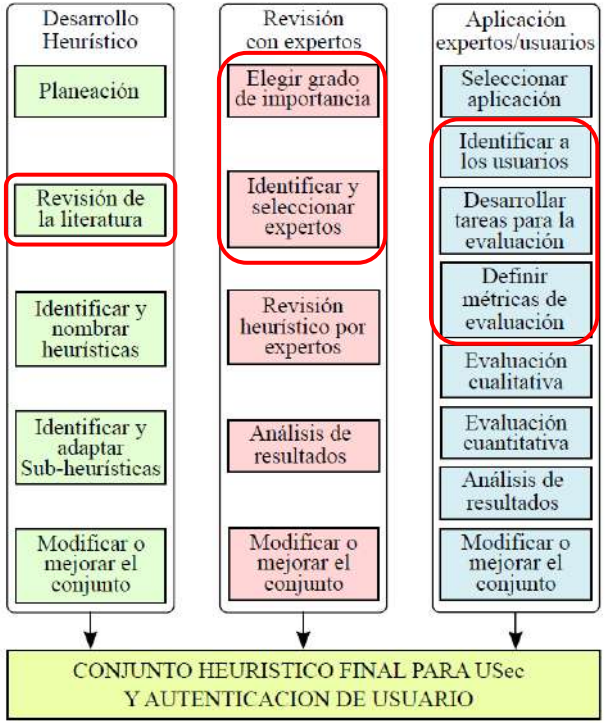
Desarrollo Heurístico USec

ISO 9241-210



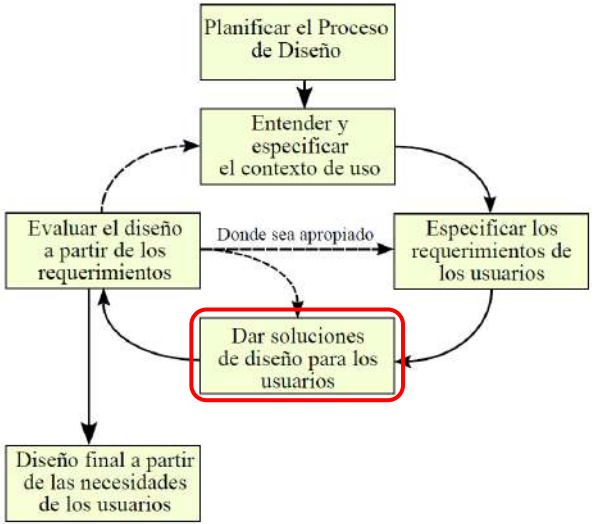
Diseño centrado en el humano para sistemas interactivos

Integración



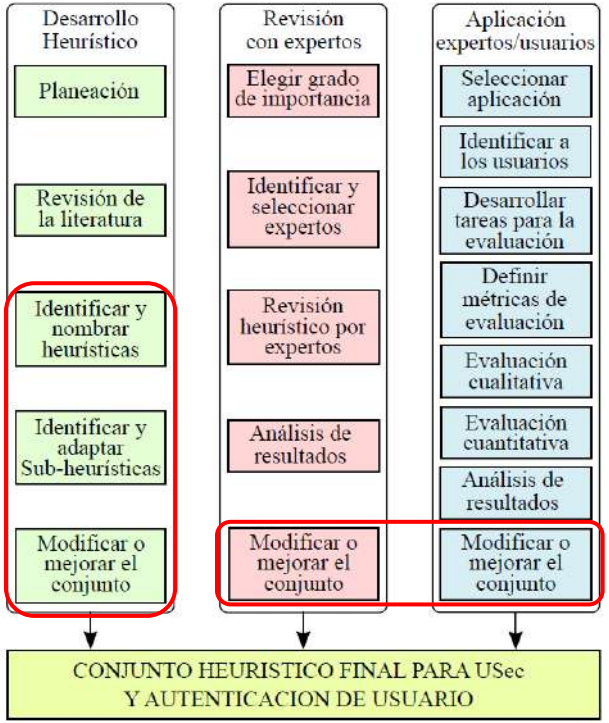
Desarrollo Heurístico USec

ISO 9241-210



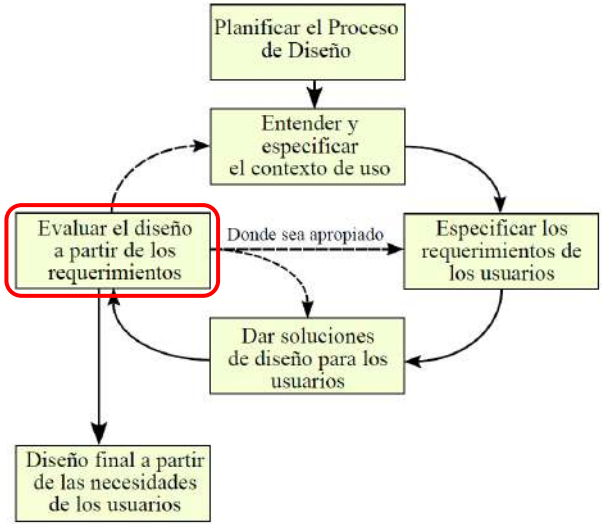
Diseño centrado en el humano para sistemas interactivos

Integración



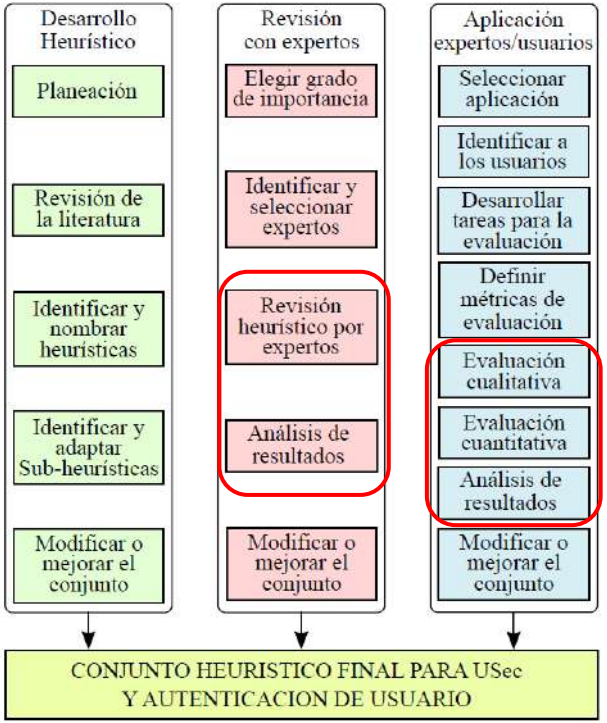
Desarrollo Heurístico USec

ISO 9241-210



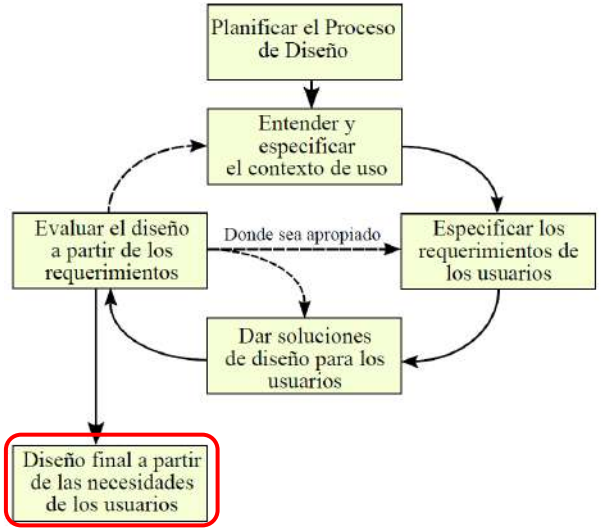
Diseño centrado en el humano para sistemas interactivos

Integración



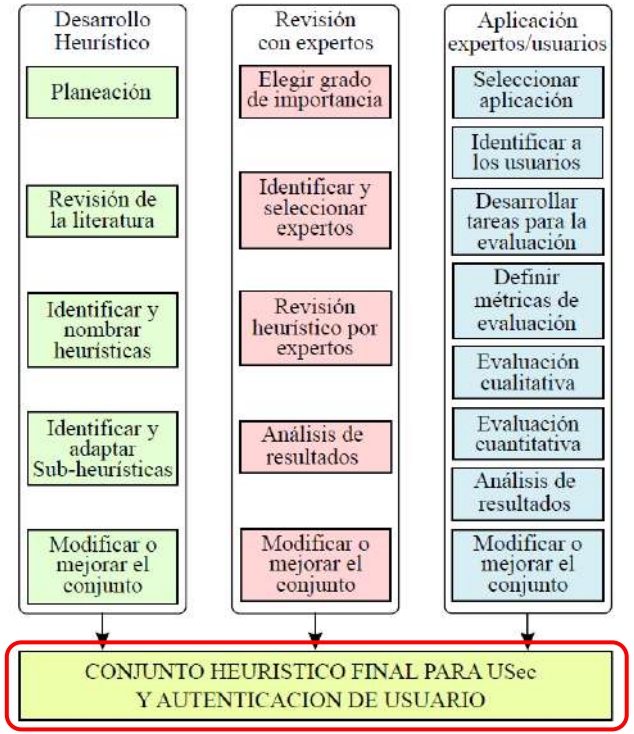
Desarrollo Heurístico USec

ISO 9241-210



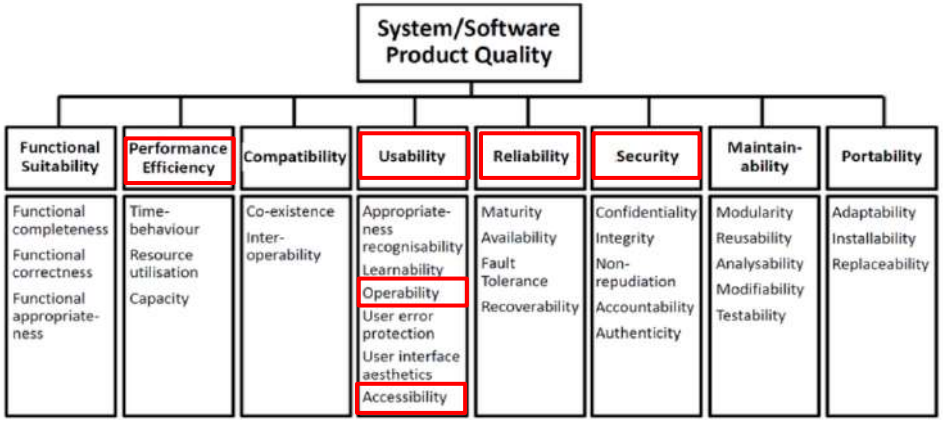
Diseño centrado en el humano para sistemas interactivos

Integración

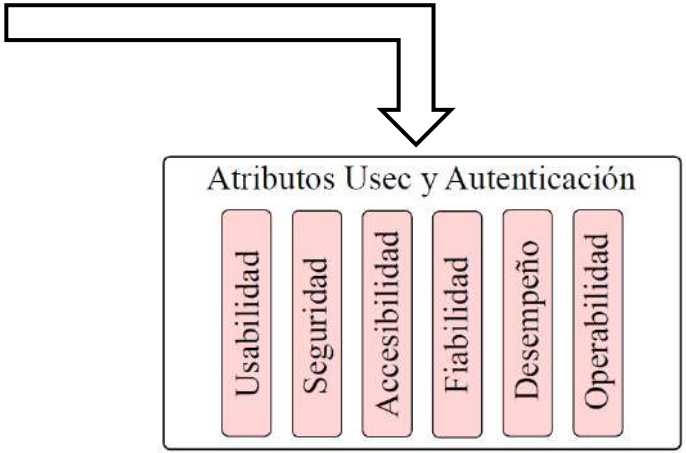


Desarrollo Heurístico USec

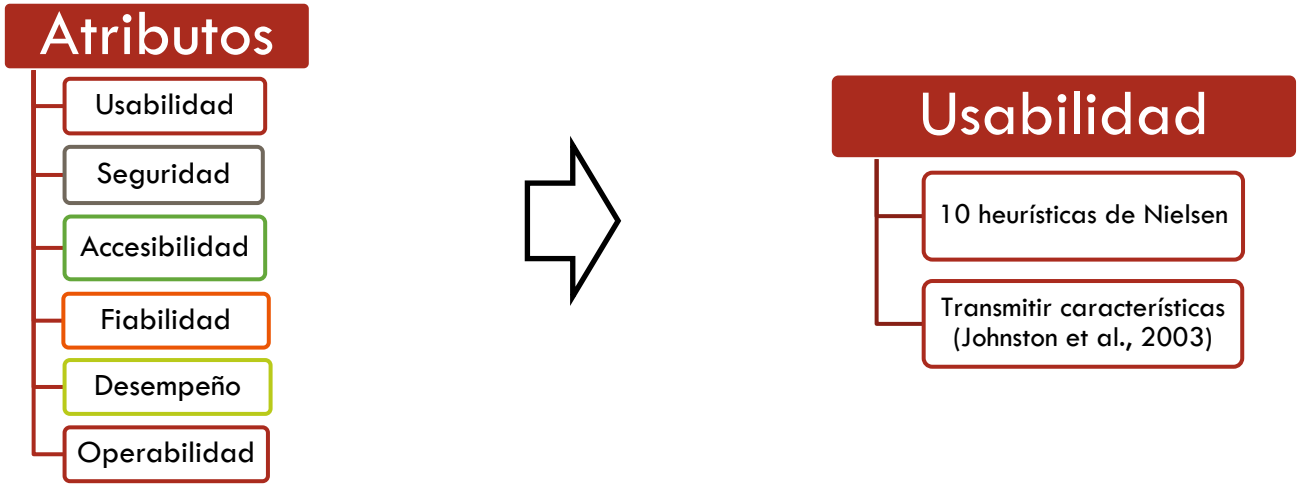
ISO/IEC 25010:2011



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
TOTAL	**75**

USec y Autenticación

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

Desarrollo Heurístico USec

Niveles de Importancia

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