

A large, semi-transparent watermark of Tux the penguin is centered in the background. Tux is a cartoon penguin wearing a blue and red cape with a white star on the chest. The text 'tux_01' is faintly visible in the background behind the penguin.

Seguridad y fuentes abiertas

Juan Carlos Inostroza O.

jci@tux.cl

<http://www.tux.cl>

Congreso Nacional de Software Libre (CONASOL)

<http://conasol.otalca.cl>

11 de Noviembre, 2003

¿Seguridad?

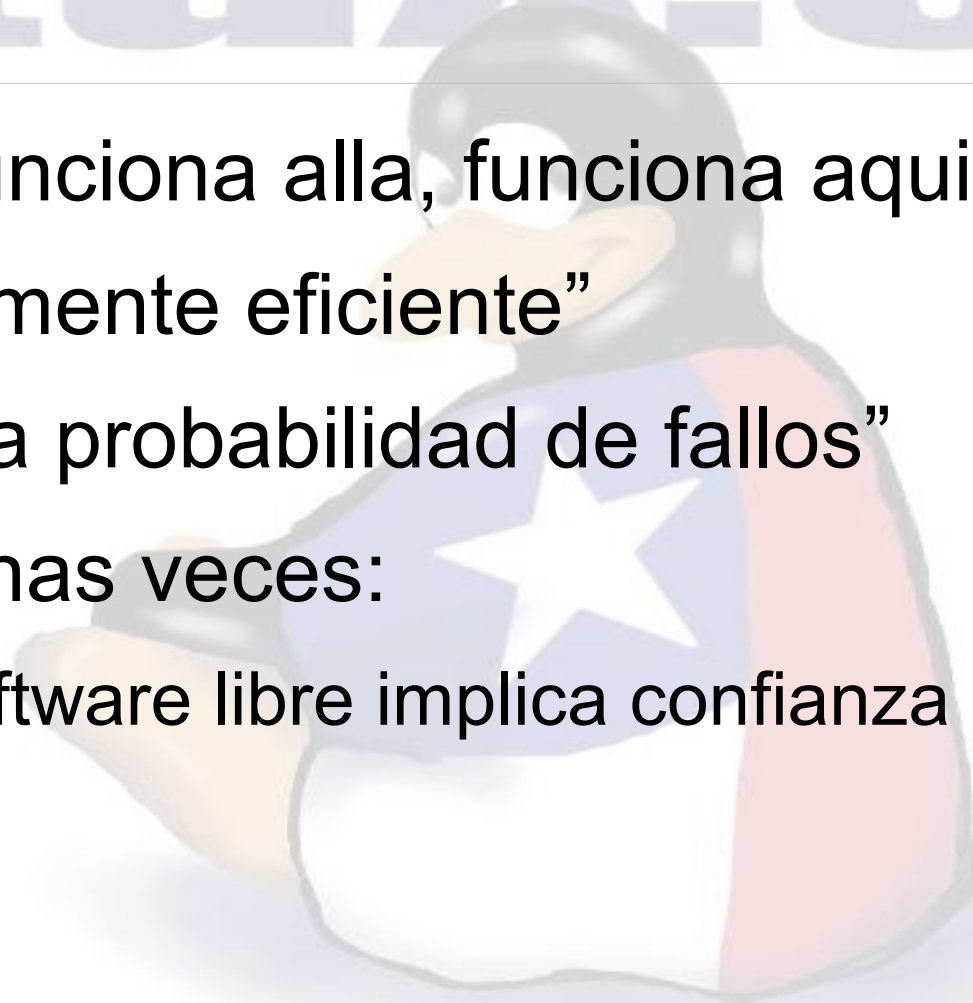
- Mitos de la Seguridad Informática
 - Seguridad por Oscuridad
 - Confiabilidad Extrema
 - Errores de Codificación
 - Dispositivos de “Alta Eficiencia”
 - Codigos Fuentes
 - etc...

Seguridad por Oscuridad

- ¿Entrego o no entrego el código fuente?
- Modelo Clásico
 - Microsoft
 - Sun
 - Entre otros...
- Poca documentación/mala documentación/documentación controlada
- APIs con funcionalidades ocultas

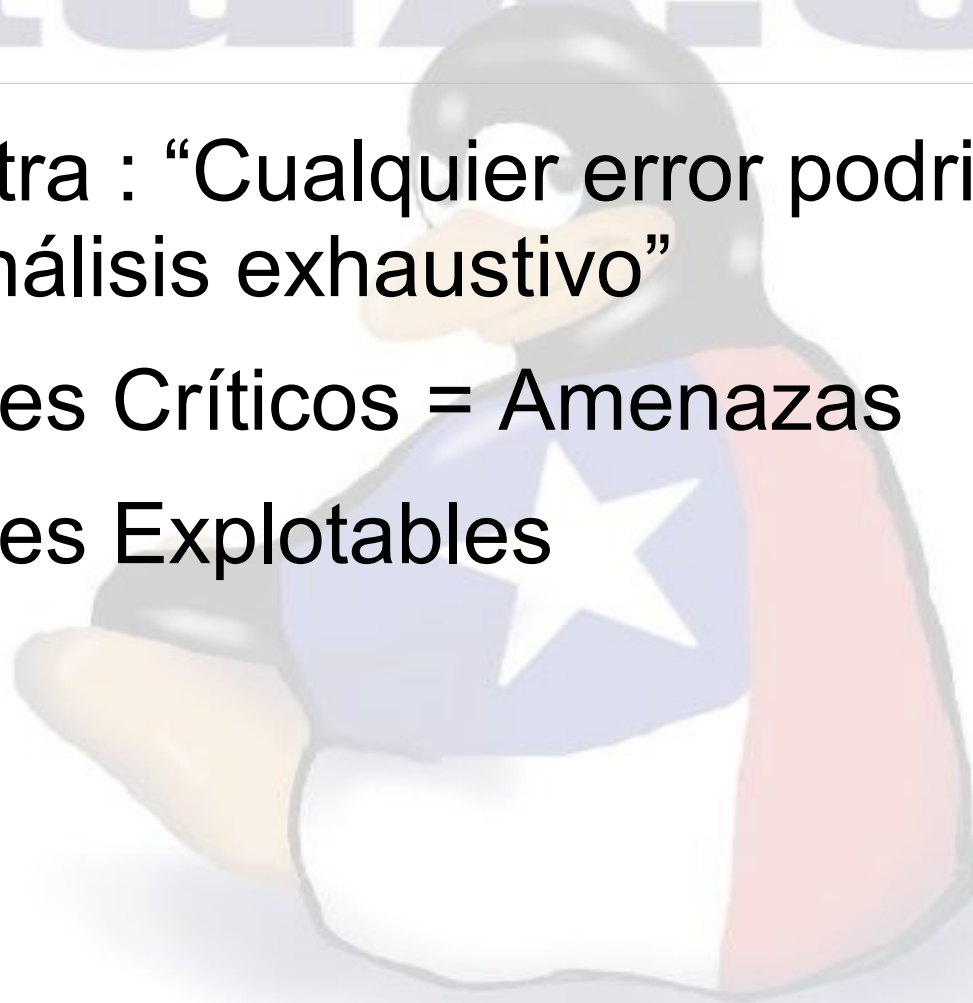
Confiabilidad Extrema

- “Si funciona alla, funciona aqui”
- “Altamente eficiente”
- “Poca probabilidad de fallos”
- Algunas veces:
 - Software libre implica confianza extrema



Errores de Codificación

- Dijkstra : “Cualquier error podría escapar de un análisis exhaustivo”
- Errores Críticos = Amenazas
- Errores Explotables



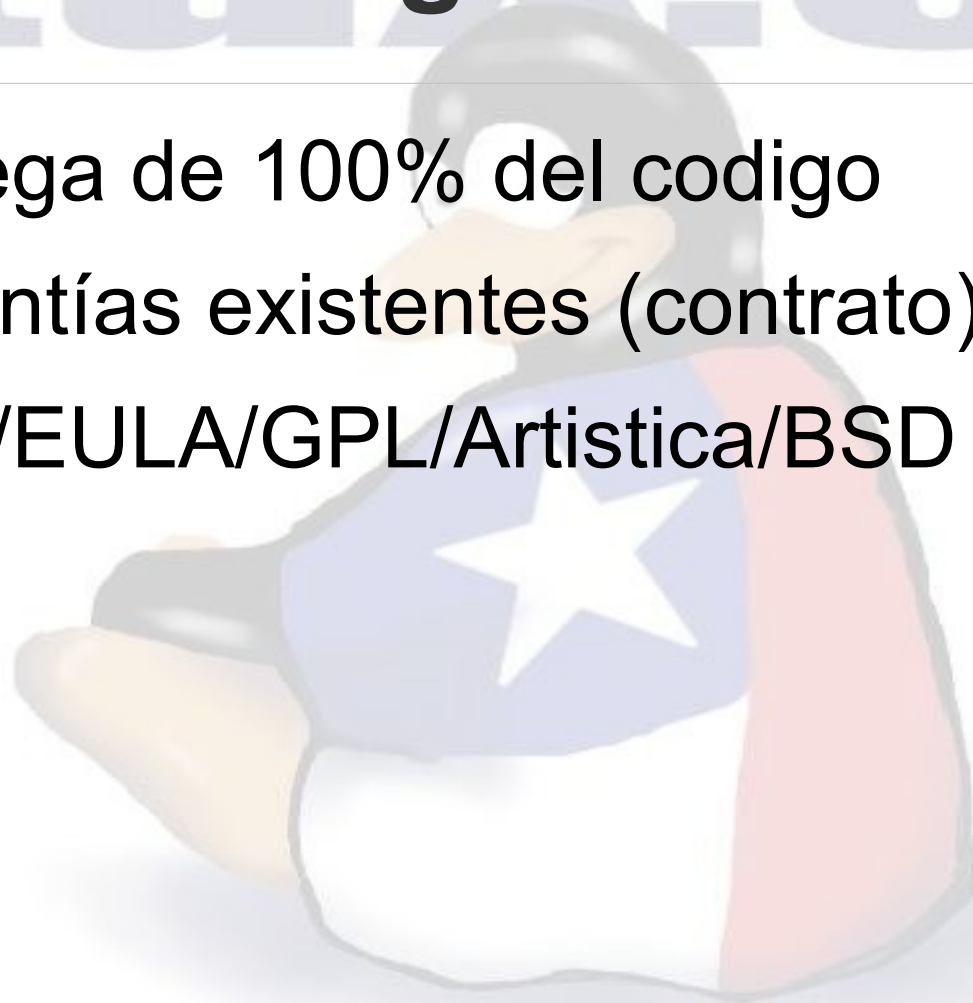
Dispositivos de “Alta Eficiencia”

- Firewalls
- UPS's
- Independientes del código



Códigos Fuentes

- Entrega de 100% del código
- Garantías existentes (contrato)
- NDA/EULA/GPL/Artística/BSD (Licencias)



A large, semi-transparent watermark of Tux the penguin is centered in the background. Tux is a black penguin wearing a red, white, and blue cape with a white star on the blue section. The word "tux" is written in a large, light blue, lowercase font behind the penguin.

Ejemplos Prácticos

- Fallos de Seguridad : ejemplos
 - Sendmail (Unices)
 - Kernel 2.4.X (Linuces)
 - RPC (WinXP)
 - UPnP (WinXP)
- Paradigma : en qué y cómo confiar?
- Poder de Decisión

Ejemplos de Índice de Correctividad

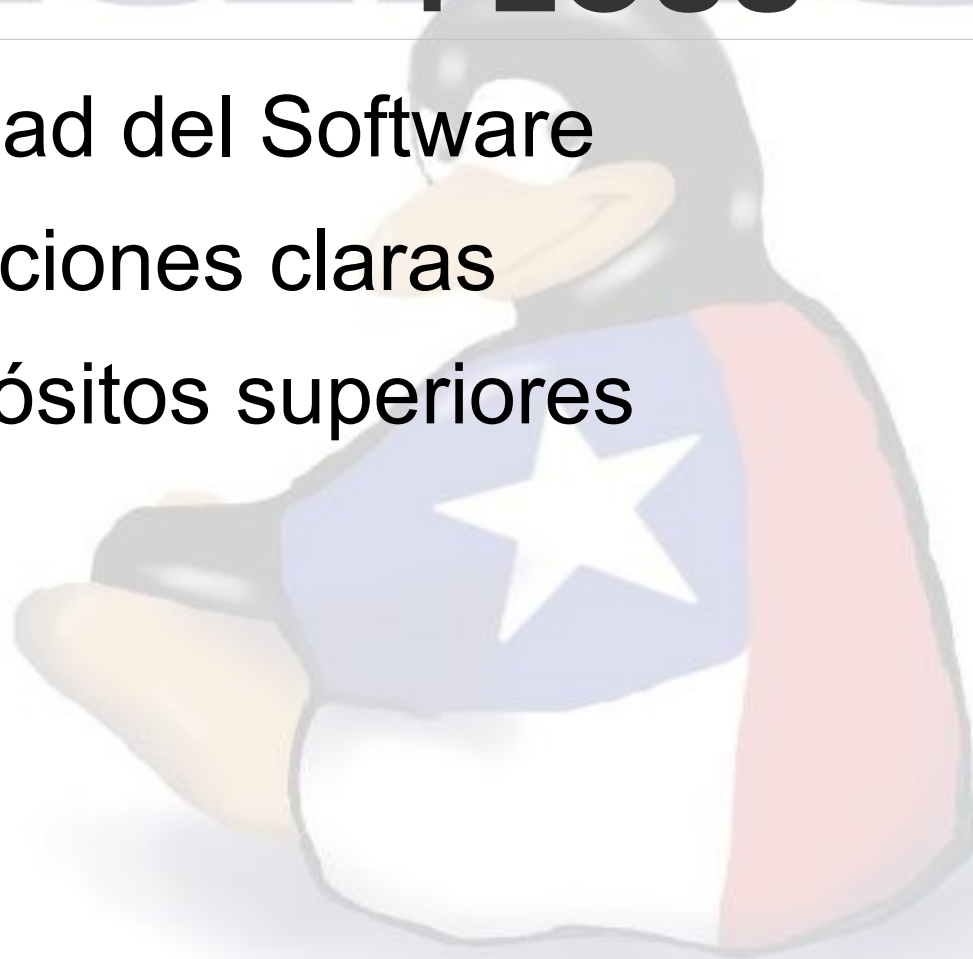
- Ptrace() bug : solucionado en horas (Alan Cox)
- Troyanización SSH : dentro de 24 horas
- Troyanización Kernel 2.6 : horas
- Troyanización Sendmail

...mientras que la “competencia”...

- IIS (Blue/Red Code + Nimda) : aun suelto
- UpnP : 1 semana
- RPC (Blaster) : 1 semana completa
(windowsupdate.com bajo DDOS)
- MS SQL Server...

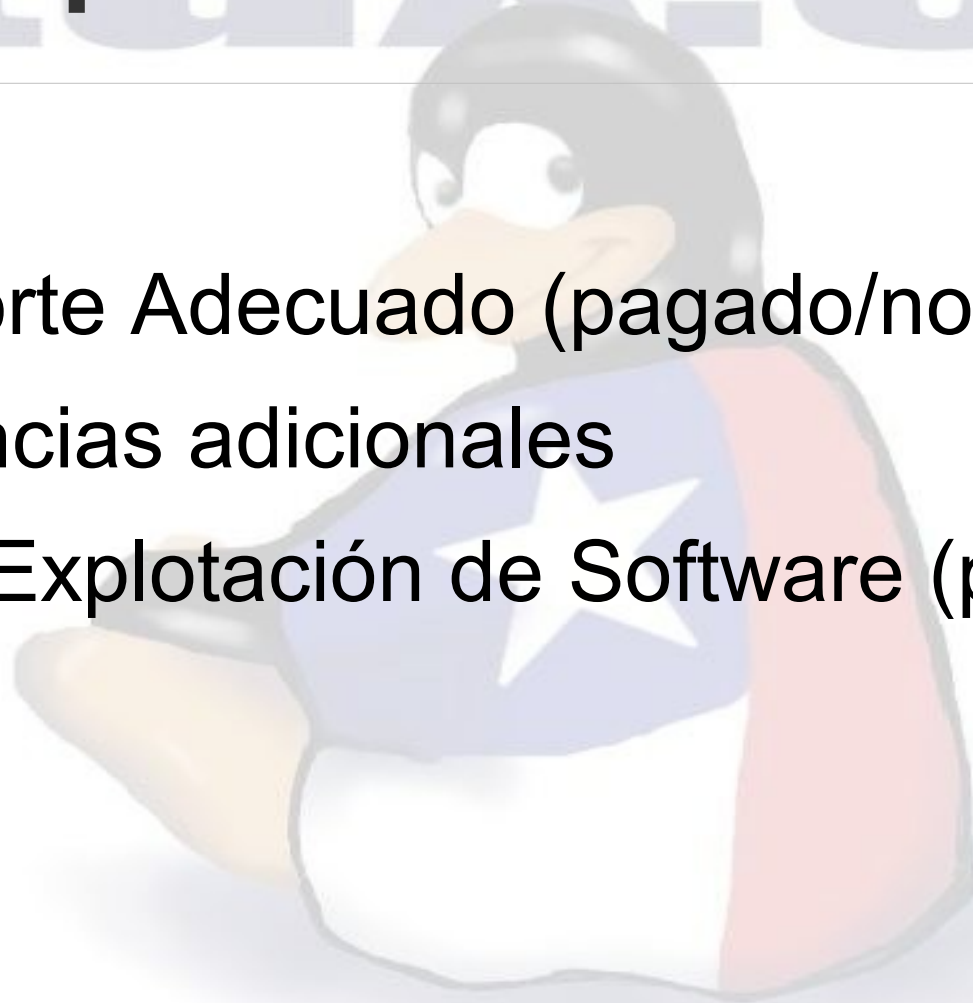
Porqués de la correctividad en FLOSS

- Calidad del Software
- Intenciones claras
- Propósitos superiores



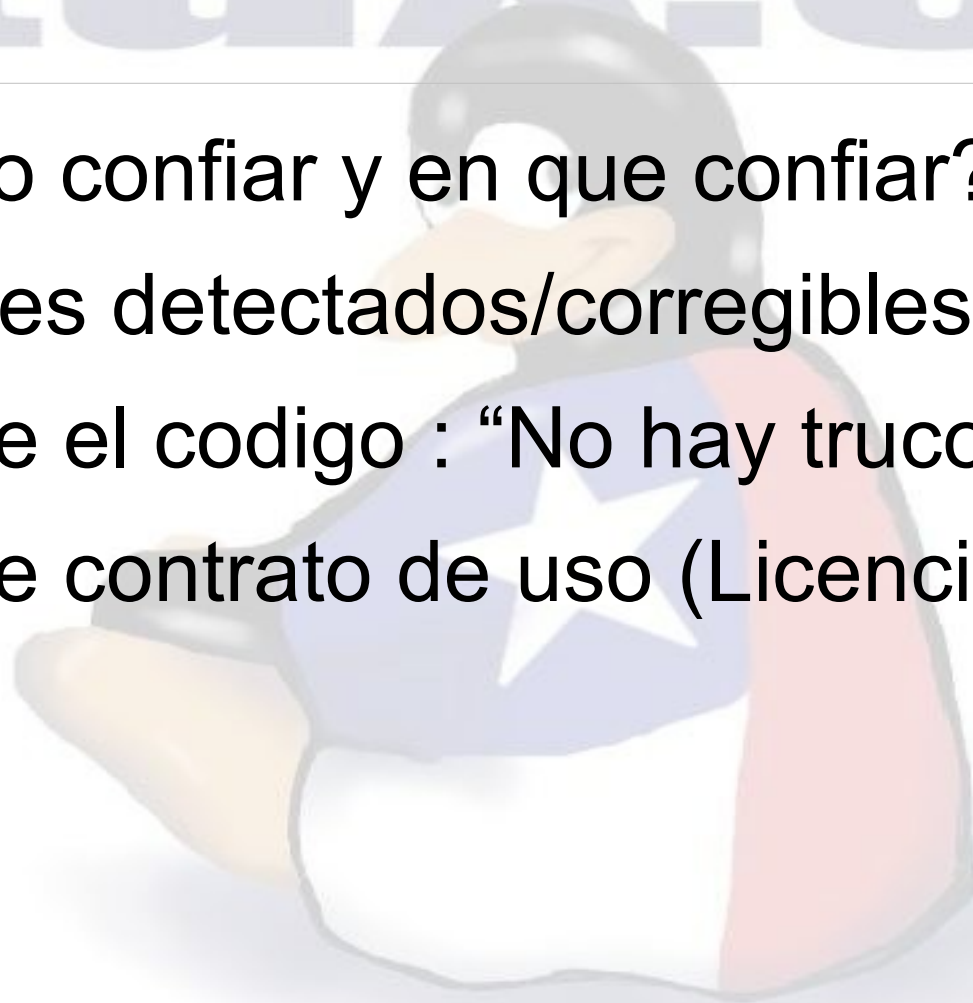
Esquema de Confiabilidad

- Soporte Adecuado (pagado/no pagado)
- Licencias adicionales
- Uso/Explotación de Software (propósito)



Software Libre : Seguro?

- Como confiar y en que confiar?
- Errores detectados/corregibles
- Existe el código : “No hay trucos”
- Existe contrato de uso (Licencias)



A large, semi-transparent watermark of Tux the penguin is centered in the background. Tux is wearing his signature blue turtleneck with a white star and a red cape. The text "tux_01" is faintly visible behind him.

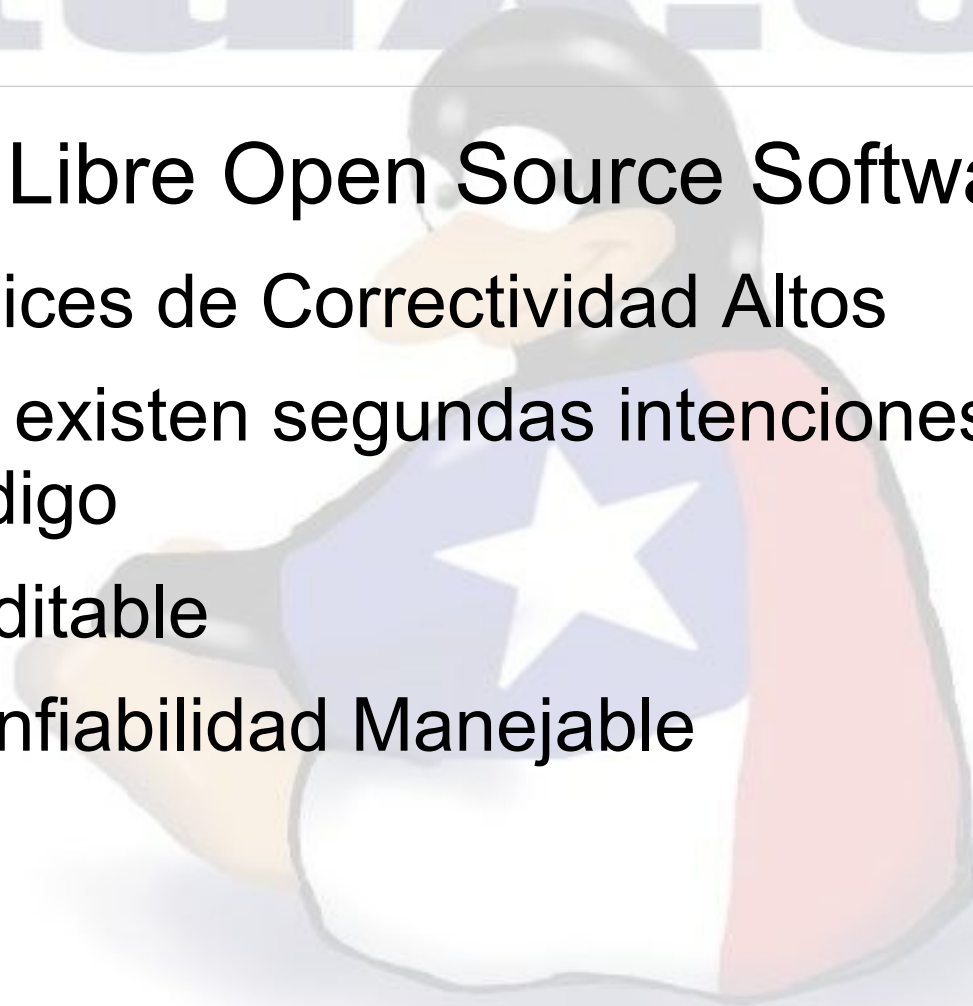
“Show me the code!”

- ¿Shared Source?
- ¿Codigo fuente de Win?
- NDAs (SCO, MS)
- Código se convierte en “Eyes Only”
- Correctividad Oculta
 - “Podríamos ahora limpiar esto...”

tux-01

FLOSS

- Free Libre Open Source Software
 - Indices de Correctividad Altos
 - No existen segundas intenciones dentro del código
 - Auditable
 - Confiabilidad Manejable



Resumen

- Seguridad del Código
- Códigos fuentes : ¿Seguros o corregibles?
- Resumen General

