VERIFICACION FORMAL DEL SISTEMA DE CONTROL DE ACCESO A APLICACIONES CORPORATIVAS DE LA F.L.C.

Pablo Javier Tuya González
Esther Suárez Calvo
Junio de 2001

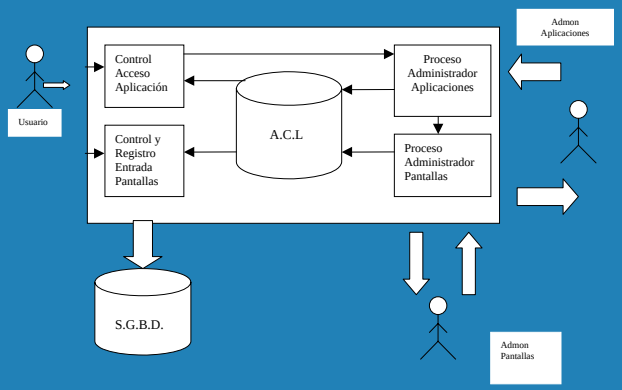
1

Seguridad

- Ley orgánica 15/99, de 13 de Diciembre
- Preocupación por controlar la seguridad
- Manual de Seguridad de la Información
- Responsable de Ficheros

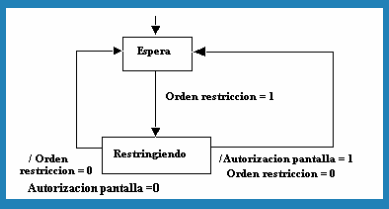
2

Marco tecnológico del Sistema

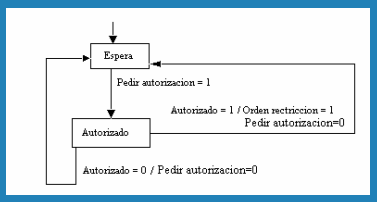


3

Primer Modelo



Estados del Administrador de las Pantallas



Estados del Administrador de la Aplicación.

Sistema respecto a las autorizaciones y entradas de usuarios en la aplicación

Estados del Sistema de Control respecto a las peticiones del Usuario

4

Especificaciones

- Un usuario no autorizado no podrá entrar nunca en la Aplicación
- Un usuario no autorizado para entrar en una pantalla, no podrá entrar nunca en la misma

5

Salida del Sistema

- AG (!autorizado -> !control_acceso_aplicacion.estado=dentro... is true
- AG (!autorizacion_pantalla -> !control_acceso_aplicacion.estado=dentro_pantalla... is false:
  - Un usuario no autorizado pide autorización para entrar en la Aplicación.
  - El administrador de la aplicación se la concede y envía un correo al administrador de pantallas para que le restrinja la entrada en las mismas.
  - El usuario inmediatamente entra en la aplicación y en la pantalla.
  - El administrador de Aplicaciones le restringe la entrada en esa pantalla, pero el usuario ya está dentro.

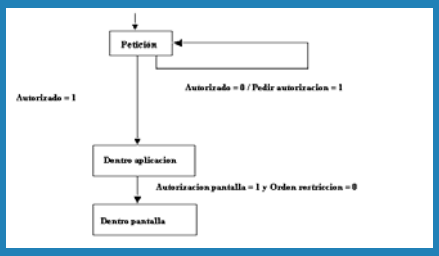
6

Posibles Soluciones

- Al crear un usuario, por defecto no tendrá acceso a ninguna pantalla de la aplicación. DESCARTADA POR EL USUARIO
- Bloquear la entrada del usuario hasta que el administrador de pantallas realice las restricciones sobre las mismas

7

Implementación de la Solución

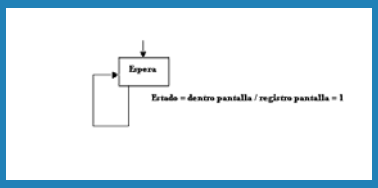


AG (!autorizacion_pantalla -> !control_acceso_aplicacion.estado=Dentro Pantalla... is true

PROBLEMA: ¿Desbloquear la cuenta del usuario?

8

Segundo Modelo



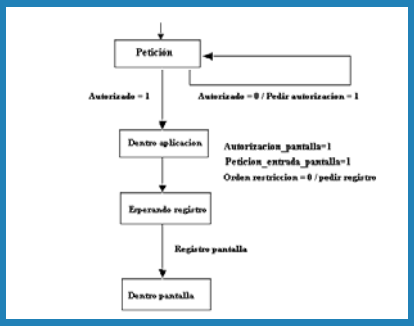
Sistema respecto a los registros de acceso a pantallas

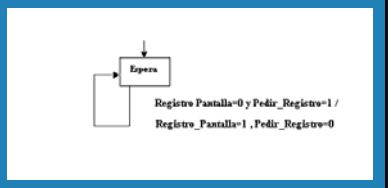
AG (estado = dentro_pantalla -> registro... is false

Registro una vez dentro de la Pantalla, ¿ Si falla el proceso de registro?

9

Implementación de la Solución



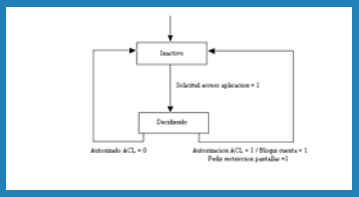


AG (estado = dentro_pantalla -> registro... is true

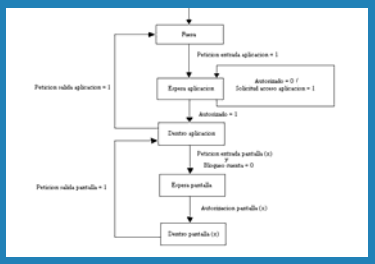
Condicionamos la entrada a una pantalla al registro previo de esta acción

10

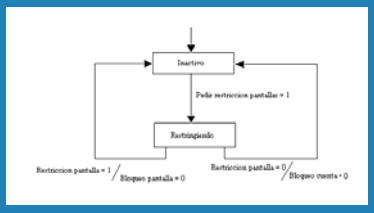
Modelo Completo Entidades Externas



Un administrador de Aplicaciones



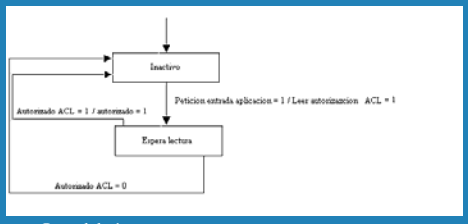
El usuario



El Administrador de Pantallas

Un S.G.B.D

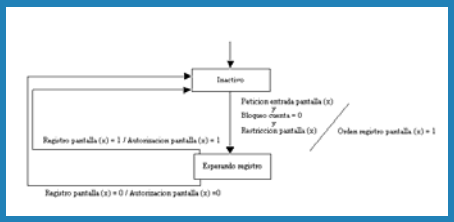
Modelo Completo Entidades Internas



Control de Acceso

Lista de Control de Acceso

Interface con Administrador de Pantallas



Registro y accesos a Pantalla

Interface con Administrador de la Aplicación

Especificaciones Finales

- SPEC AG (estado = Dentro_Aplicacion -> autorizado)
- SPEC AG (estado = Dentro_Pantalla1 -> autorizacion_pantalla1)
- SPEC AG (estado = Dentro_Pantalla1 -> registro_pantalla1)
- SPEC AG (estado = Dentro_Pantalla1 -> autorizado)
- SPEC AG (estado = Dentro_Pantalla1 -> !bloqueo_cuenta)
- SPEC AG (estado = Dentro_Pantalla2 -> autorizacion_pantalla2)
- SPEC AG (estado = Dentro_Pantalla2 -> registro_pantalla2)
- SPEC AG (estado = Dentro_Pantalla2 -> autorizado)
- SPEC AG (estado = Dentro_Pantalla2 -> !bloqueo_cuenta)
- SPEC AG (!autorizacion_pantalla2 -> !estado=Dentro_Pantalla2)
- SPEC AG (bloqueo_cuenta -> !estado=Dentro_Pantalla2)

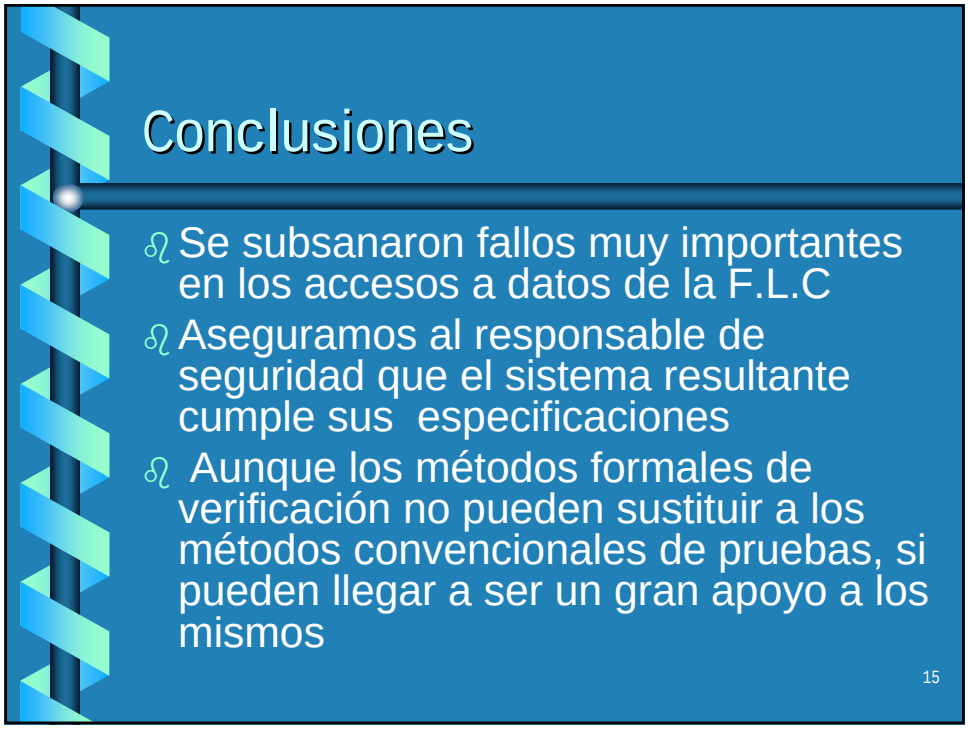
- -- specification AG (estado = Dentro_Aplicacion -> autori... is true
- -- specification AG (estado = Dentro_Pantalla1 -> autoriz... is true
- -- specification AG (estado = Dentro_Pantalla1 -> registr... is true
- -- specification AG (estado = Dentro_Pantalla1 -> autoriz... is true
- -- specification AG (estado = Dentro_Pantalla1 -> !bloque... is true
- -- specification AG (estado = Dentro_Pantalla2 -> autoriz... is true
- -- specification AG (estado = Dentro_Pantalla2 -> registr... is true
- -- specification AG (estado = Dentro_Pantalla2 -> autoriz... is true
- -- specification AG (estado = Dentro_Pantalla2 -> !bloque... is true
- -- specification AG (!autorizacion_pantalla2 -> !estado =... is true
- -- specification AG (bloqueo_cuenta -> !estado = Dentro_P... is true

13

¿ Por Qué ?

- El sistema había sido probado de manera exhaustiva por los usuarios, sin detectar fallo alguno en la seguridad.
  - Desconocimiento del ENTORNO.
  - Alta involucración en Pruebas de los Administradores
- No se tuvieron en cuenta fallos físicos de los sistemas

14


Conclusiones
Se subsanaron fallos muy importantes en los accesos a datos de la F.L.C
Aseguramos al responsable de seguridad que el sistema resultante cumple sus especificaciones
Aunque los métodos formales de verificación no pueden sustituir a los métodos convencionales de pruebas, si pueden llegar a ser un gran apoyo a los mismos
15