

Seguridad en entornos financieros

Pedro Sánchez
Responsable de seguridad de ATCA

password psanchez@atca.es

Agradecimientos



Vicente Aguilera Díaz

ASP Spain Local Chapter

Agenda

INTRO: Estado actual de la seguridad en entornos financieras

1.- Que es ATCA

2.- CMMI en seguridad web

2.1.- Ciclo de vida

3.- 'Tiger team' de ATCA

4.- Seguridad en Banca Electrónica

4.1.- Componentes de seguridad

- Desarrollos propios**
- Sistema gestión de alertas**
- Sistema anti fraude**
- ATCA Labs Security**

5.- Futuro

- CERT Security ATCA**

6.- Conclusiones

Estado actual

- A) Partimos de que el nivel de seguridad del entorno financiero es alto, debido especialmente a la protección de datos y del dinero digital**
- B) Desde hace años y sin ninguna regulación, las entidades financieras (en España) se han protegido con políticas internas de seguridad de la información e incluso creando comités de trabajo.**
- C) Banco de España, se perfila como 'líder' aunque no crea ninguna recomendación al respecto**

Estado actual

D) Los problemas de fraude (duplicaciones de tarjetas) vienen dados especialmente fuera de España, ya que se trabaja en OFF-LINE, las soluciones vienen dadas por un estándar como EMV.

E) Los malos sistemas de autenticación de las BE y la baja seguridad de los usuarios hacen que las mafias se centren en este 'negocio' llegando a superar al negocio de la droga.

F) Según el INTECO, el 80% de los ordenadores españoles tienen algún tipo de Malware, sin que el usuario lo sepa (España a la cabeza del SPAM) Según VERISIGN en el mundo, las infecciones superan el 90%

G) Se ha demostrado, que cuando se audita una entidad financiera, este mejora en su continuidad y credibilidad de clientes y usuarios

H) Muchas entidades subcontratan actualmente la seguridad ¿?

1.- Que es ATCA

1.- Que es ATCA

ATCA A.I.E., es una agrupación de interés económico con un Capital Social de 6.923.520 Euros distribuido entre sus socios de la forma siguiente:



1.- Que es ATCA

ATCA desarrolla, mantiene y explota las aplicaciones del núcleo bancario de las Cajas, el Terminal Financiero, la Banca por Internet y aplicaciones departamentales.

Durante toda su trayectoria se ha destacado por su apuesta firme por la innovación, las últimas tecnologías y la inversión en proyectos de I+D+i, siendo una compañía pionera en el uso de Software Libre.

La seguridad es una de sus máximas prioridades, lo que le ha llevado a convertirse en la primera entidad del sector financiero español en obtener la máxima certificación para su sistema de gestión de seguridad de la información, conforme a la norma ISO/IEC 27001.

También en este año se ha conseguido la certificación CMMI Nivel 5, siendo la única empresa con capital Español con esta categoría

1.- Que es ATCA

En ellas trabajan más de 6.400 empleados. En cuanto a la red de atención al público, la cifra global es de 1.233 sucursales, 2.358 cajeros automáticos y 25.013 TPV's

Misión: Minimizar los incidentes de seguridad



1.- Que es ATCA

PARAMETRIZACIÓN:

- Las aplicaciones son comunes para las cuatro Cajas.
- Las diferencias existentes en productos, tarifas o criterios de gestión se manejan en base a parámetros.
- Las bases de datos son iguales y se manejan juegos de tablas por Caja.
- Los procesos son similares, pero se ejecutan una vez por cada Caja.
- Las Aplicaciones son *multi-divisa*, *multi-entidad* y *multi-idioma*, y se explotan con dos usos horarios (Península y Canarias).

1.- Que es ATCA

- Herramientas de código abierto
- Desarrollo del terminal financiero con autenticación robusta
- Certificación en CMMI Nivel 5 (Solo dos empresas en España)
- Certificación de Seguridad SGSI en ISO 27001 (Única en España cuyo alcance es toda la empresa)
- Certificaciones: CISCO ⁽³⁾, MCSA⁽³⁾, MCSE ⁽⁶⁾, CISM ⁽¹⁾, OCP ⁽³⁾
- Primera empresa en España en pasar la auditoria PCI de VISA y MASTERCAD sin ningún incumplimiento
- Unica empresa (del sector financiero) cuyo centro de respaldo está a más de 350 Kilometros

1.- Que es ATCA

The logo for ABACO features the lowercase letters 'abaco' in a grey, sans-serif font. The letter 'a' is partially overlaid by a solid blue square.

abaco

El proyecto ABACO tiene por objetivo desarrollar todas las aplicaciones básicas de lo que se denomina un "nucleo bancario", es decir, aquellas aplicaciones que soportan el servicio a los clientes de una entidad financiera, los canales de distribución y las principales herramientas de gestión.

Estas aplicaciones se escriben en Java y corren sobre plataformas de hardware estándar y productos de software libre (Linux, etc...).

Sus componentes técnicos de arquitectura, herramientas y metodologías han sido certificados por la [Agencia de Acreditación en Investigación, Desarrollo e Innovación Tecnológica \(AIDIT\)](#) como un proyecto de I+D.

1.- Que es ATCA

The logo for atux, featuring the lowercase letters 'atux' in a grey serif font. The letter 'a' is partially covered by a blue square.

Workstation

The logo for atux, featuring the lowercase letters 'atux' in a grey serif font. The letter 'a' is partially covered by a blue square.

Server

The logo for atux, featuring the lowercase letters 'atux' in a grey serif font. The letter 'a' is partially covered by a blue square.

Live

The logo for atux, featuring the lowercase letters 'atux' in a grey serif font. The letter 'a' is partially covered by a blue square.

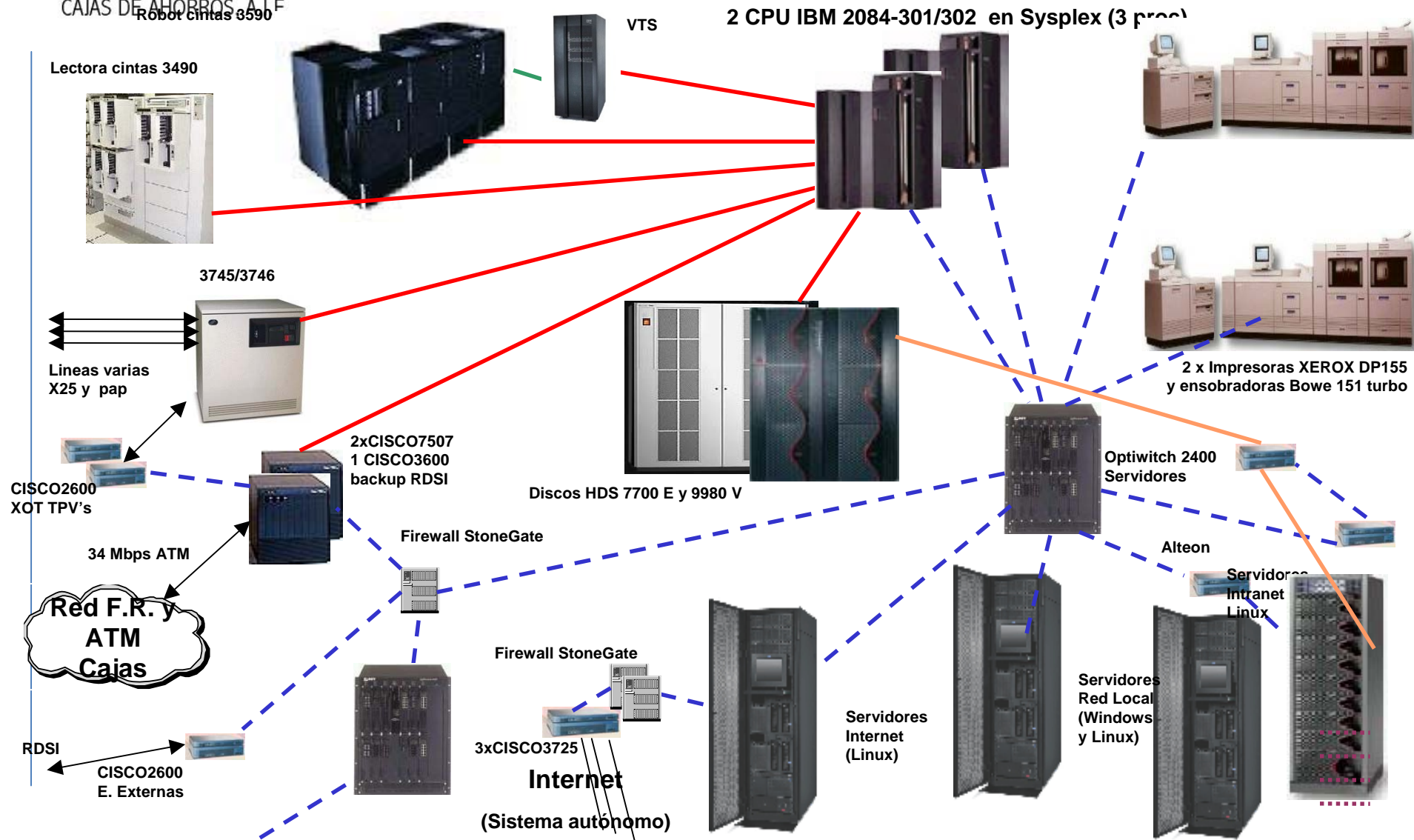
Security

Atux (De ATca y tUX), consiste en una distribución GNU/Linux construída específicamente para atender las necesidades de un puesto de trabajo de ATCA y las Cajas de Ahorros asociadas.

En la actualidad está instalado en la mayoría de los puestos de ATCA y se está probando exhaustivamente con vistas a su implantación en las oficinas de las Cajas de Ahorros a lo largo de 2007.

Atux Security está pensado para equipos de alta criticidad basado en OpenBSD

1.- Que es ATCA



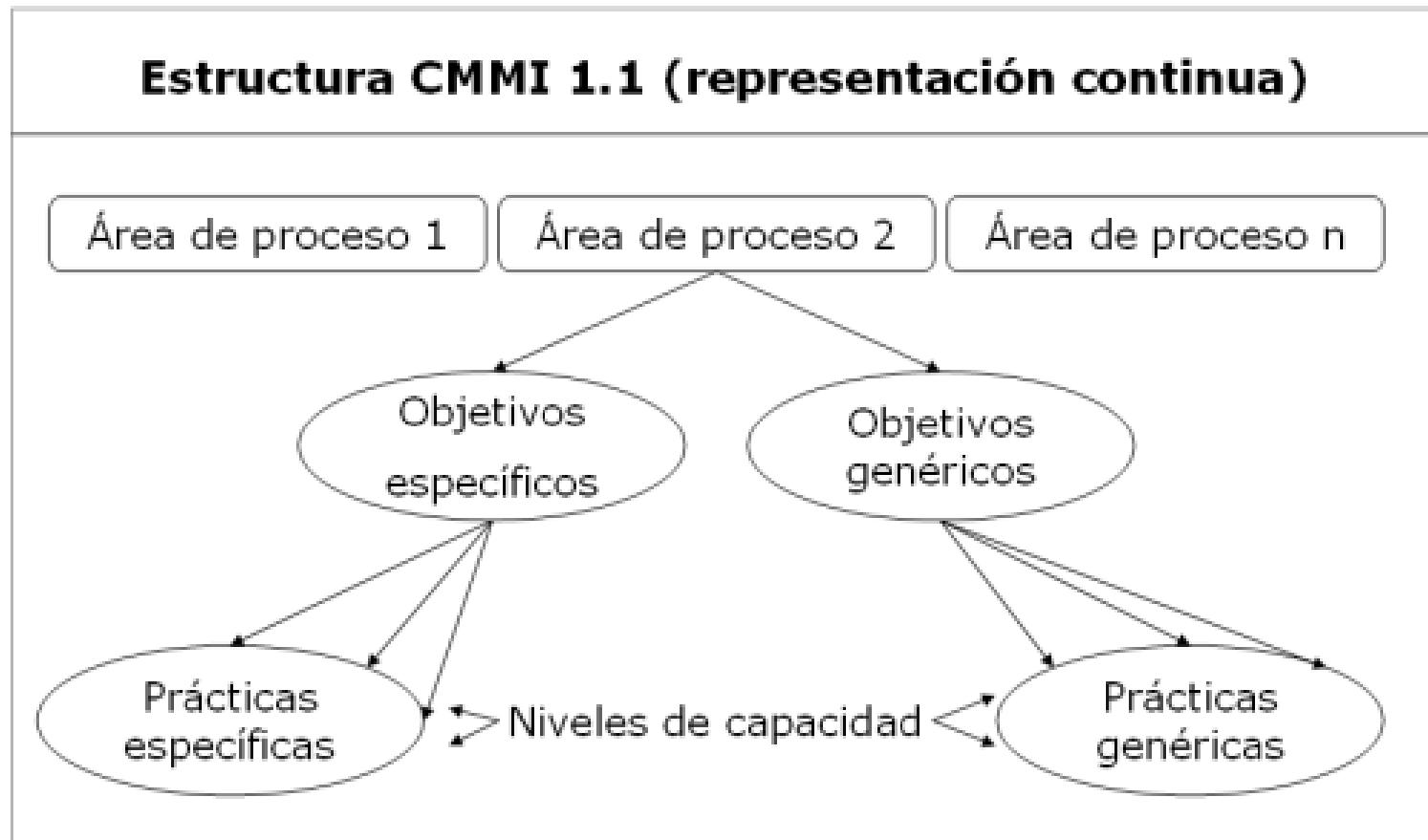
2.- CMMI -Seguridad

2.- CMMI -Seguridad

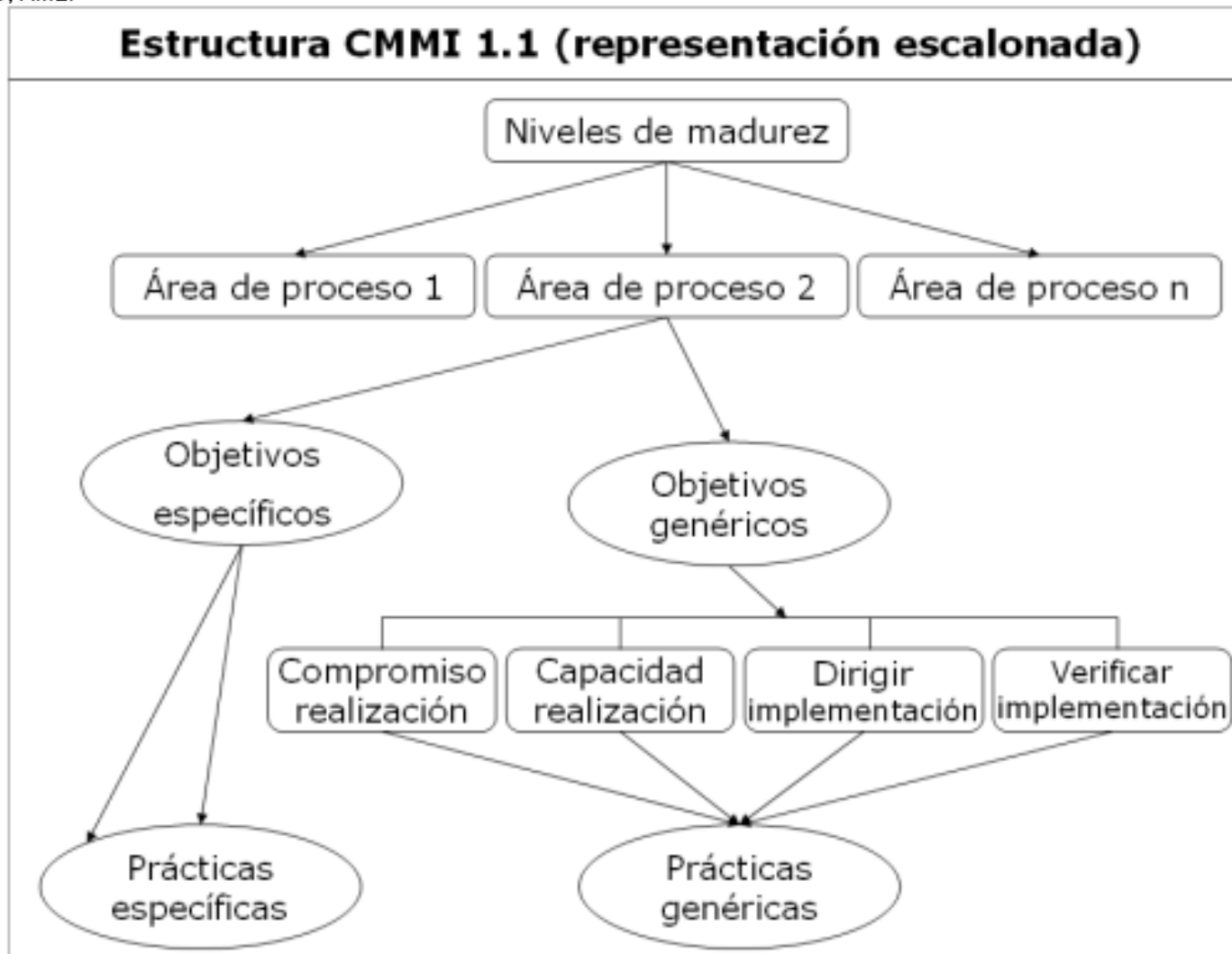
Capability Maturity Model Integration. Modelo para la mejora o evaluación de los procesos de desarrollo y mantenimiento de sistemas y productos de software. Fue desarrollado por el Instituto de Ingeniería del Software de la Universidad Carnegie Mellon ([SEI](#)), y publicado en su primera versión en enero de [2002](#).

2.- CMMI - Seguridad

Estructura CMMI 1.1 (representación continua)



2.- CMMI - Seguridad



2.- CMMI – Seguridad

Como se integra la seguridad en el desarrollo

- 1.- Todos los desarrollos de software, deben de pasar por el visto bueno del departamento de seguridad (Estudio, definición, desarrollo, test, formación y producción)
- 2.- En todos los entornos , se realizan documentos que deben de aprobarse por los responsables de la petición de desarrollo
- 3.- Cuando una aplicación viene dada por terceros, deben de cumplir las normas de seguridad de ATCA (ej. Los proveedores externos nunca se conectan de forma remota)
- 4.- En todos los proyectos debe de haber un responsable de código seguro, designado por el departamento de desarrollo o seguridad.

¡¡La media de un proyecto es de seis meses!!

2.- CMMI - Seguridad

Más de 150 Procedimientos de seguridad
60 de ellos dedicados al desarrollo de software seguro
10 de los 60 dedicados a el ciclo de vida del software
264 Metricas (117 de seguridad)

Objeto:

Durante la fase de planificación todos los proyectos deben de identificarse, justificarse, acordarse y documentar.

Alcance:

Los proyectos de nuevos productos, gestión interna y optimización
Las peticiones de trabajo cursadas por las Cajas con causas mtto evolutivo o normativo.
Los proyectos y trabajos llevados a cabo por Sistemas que afectan a las plataformas Hw/Sw que prestan servicio de producción

2.- CMMI - Seguridad

Algunos criterios útiles podrían ser:

Se realiza tratamiento de datos nivel alto LOPD (salud, religión,...)

Se envía información al exterior física o electrónicamente. En concreto siempre deberá ser objeto de revisión la primera vez que se envíen a una entidad externa datos de carácter personal (DNI's, nombres,...).

Se realiza o modifica una conexión on-line de entrada desde el exterior (Servicios Web, CICS to CICS, MQ-series,...) incluidas las propias Cajas ATCA.

Se va a utilizar una nueva plataforma de desarrollo y/o explotación.

Se accede a datos a través de interfases no estandarizadas (diferentes del Terminal Financiero, Banca Electrónica, Cajeros, 3270, etc..).

Se requiere la integración de un paquete externo o en general la instalación de un software de terceros (incluido el nuevo software base).

Se requiere la instalación de servidores con acceso a / de Internet.

En general cualquier petición que requiera un tratamiento no estándar en cuestiones como:

- El tratamiento de back-up de datos
- El tratamiento en el centro de respaldo
- Los controles de autenticación y acceso de usuarios y el registro de log.
- Las reglas de firewall.

http://www.portal.atca/?q=502060-toma-de-decisiones-sistemica

Google

Go

Bookmarks

90 blocked

Check

AutoLink

AutoFill

Send to

50.20.60 - Toma de decisiones sistemática | Portal...

Página

Herram

- Propuestas Mejora
- Métricas
- Producción
- Sistemas
 - Drupal en ATCA
- SAO
- Presentaciones
- Programación ABACO

Aplicaciones Cajas

- SGA Cajas
- Web Transaccional
- Producción
 - Caja Inmaculada
 - Caixa Sabadell
 - Caja Rioja
 - Caja Insular
- Test
 - Caja Inmaculada
 - Caixa Sabadell
 - Caja Rioja
 - Caja Insular
- Gema Visual
- Estados Financieros
- Paladín
- EIS de Caja Rioja
- SACOM
- SIAC

PROCESO DE TOMA DE DECISIONES SISTEMÁTICAS

Este proceso implica establecer pautas para determinar qué situaciones se deben sujetar a un proceso formal de evaluación para después aplicar dichos procesos, reduciendo así la naturaleza subjetiva de la decisión.

Un proceso formal de evaluación es un acercamiento estructurado a evaluar soluciones alternativas en determinadas situaciones que, en ATCA corresponderán a las siguientes:

Incidencias graves en producción.

Ante una incidencia grave en producción que pueda implicar alguna de las consecuencias siguientes en un grado importante:

- Pérdida de servicio.
- Repercusiones económicas a las Cajas y/o clientes.
- Pérdida de imagen de las Cajas.

el responsable de equipo/grupo, junto con el Director de Área y los responsables del resto de equipos afectados, evaluarán las posibles soluciones alternativas, en base a los siguientes criterios:

- Rapidez de recuperación del servicio.
- Impacto en clientes.
- Implicación requerida a las Cajas.

Según la naturaleza de la incidencia, se presentará a las Cajas las posibles alternativas para aplicar la solución que consideren más adecuada.

http://www.portal.atca/?q=502020-gestin-y-desarrollo-de-requerimientos

Google

Archivo Edición Ver Favoritos Herramientas Ayuda

Google G Go Bookmarks 90 blocked Check Look for Map AutoFill Send to

50.20.20 - Gestión y desarrollo de requerimientos ...

Página Herram

1. GESTION DE REQUISITOS.

1.1 Recepción, almacenamiento y acceso a los requerimientos

Debe existir siempre para cualquier proyecto o petición un documento en el que se incluyen todos los requerimientos asociados a los mismos. Este documento deberá estar actualizado y a disposición de todas las partes que intervienen en el proyecto o petición.

Como punto de partida, se trabajará sobre los requerimientos remitidos por el solicitante:

- Para aquellos trabajos considerados como proyectos, el responsable del proyecto deberá redactar los requerimientos según la plantilla estándar del Documento de Requerimientos partiendo de los documentos, notas, correos, actas, etc.. que reciba del solicitante (Cajas, Grupos ATCA, Producción, Normativa, etc..). Este documento incluirá con el resto de información del proyecto y será accesible a través del portal del conocimiento en el apartado de documentación.
- Para el resto de trabajos, los requerimientos se recogerán en la aplicación SGA Web según el procedimiento 10.20.70 de gestión de la cartera de peticiones.

1.2 Revisión de requisitos

Una vez que se dispone de los requerimientos del usuario, el responsable del proyecto procederá a revisarlos y a completarlos realizando las siguientes acciones:

- Comprobar si son asumibles, completos, consistentes y suficientemente claros.
- Revisar con el solicitante los requerimientos que puedan ser más problemáticos o confusos.
- Completar aquellos requerimientos no especificados por el solicitante, tanto a nivel funcional, como en temas de seguridad, plataforma,...
- Comunicar y revisar con todos los equipos afectados los requerimientos y negociar con ellos los compromisos que

60.90.22 - Pruebas y mantenimiento del Plan | Portal de atca - Windows Internet Explorer

http://www.portal.atca/?q=node/849

Google

ArchivoEdiciónVerFavoritosHerramientasAyuda

Google

Go

Bookmarks

90 blocked

Check

Look for Map

AutoFill

Send to

60.90.22 - Pruebas y mantenimiento del Plan | Po...

Página

Herram

Aplicaciones Cajas

SGA Cajas

Web Transaccional

Producción

Caja Inmaculada

Caixa Sabadell

Caja Rioja

Caja Insular

Test

Caja Inmaculada

Caixa Sabadell

Caja Rioja

Caja Insular

Gema Visual

Estados Financieros

Paladín

EIS de Caja Rioja

SACOM

SIAC

Comisiones Bonificadas

Log unificado

Ver Comunicados

Mapa ATCA

Mapa de ATCA en vigor

Mapa de ATCA (revisión)

Mapa de ATCA (redacción)

1.- PLAN DE PRUEBAS PERIODICO

Para la realización de las pruebas:

Determinar la fecha y hora en que será realizada cada una de las pruebas. Ha de evitarse cualquier interferencia operativa habitual de ATCA y las Cajas Asociadas.

Comunicar a todo el personal que deba participar en las pruebas la fecha y hora en que serán realizadas.

Comprobar que todas las personas involucradas disponen de una copia del Plan de Continuidad del servicio

Ejecutar las pruebas previstas.

Las pruebas y resultados obtenidos deben ser convenientemente documentados. Cada uno de los integrantes de los equipos que participen en el desarrollo de las mismas debe mantener un registro detallado de las acciones realizadas, los resultados obtenidos, tiempo empleado e incidencias que hayan podido surgir, con el fin de evaluar los resultados obtenidos.

El responsable de cada uno de los equipos entregará al Responsable del Plan de Continuidad del servicio un informe en el que figuren:

Objetivo de la prueba efectuada.

Resultados obtenidos y tiempo empleado para la recuperación.

Incidencias que hayan podido surgir.

Posibles recomendaciones de corrección y seguimiento.

Evaluación de los resultados

Antes de la realización de cualquier prueba han de especificarse los criterios de evaluación de los resultados obtenidos tras su realización.

Una vez finalizadas las pruebas se mantendrá una reunión de evaluación de los resultados obtenidos, con el fin de evaluar la eficacia de los procedimientos establecidos en el Plan de Continuidad del servicio e introducir todas aquellas

60.90.22 - Pruebas y mantenimiento del Plan | Portal de atca - Windows Internet Explorer

http://www.portal.atca/?q=node/849

Google

ArchivoEdiciónVerFavoritosHerramientasAyuda

Google

Go

Bookmarks

90 blocked

Check

Look for Map

AutoFill

Send to

60.90.22 - Pruebas y mantenimiento del Plan | Po...

Página

Herram

Aplicaciones Cajas

SGA Cajas

Web Transaccional

Producción

Caja Inmaculada

Caixa Sabadell

Caja Rioja

Caja Insular

Test

Caja Inmaculada

Caixa Sabadell

Caja Rioja

Caja Insular

Gema Visual

Estados Financieros

Paladín

EIS de Caja Rioja

SACOM

SIAC

Comisiones Bonificadas

Log unificado

Ver Comunicados

Mapa ATCA

Mapa de ATCA en vigor

Mapa de ATCA (revisión)

Mapa de ATCA (redacción)

1.- PLAN DE PRUEBAS PERIODICO

Para la realización de las pruebas:

Determinar la fecha y hora en que será realizada cada una de las pruebas. Ha de evitarse cualquier interferencia operativa habitual de ATCA y las Cajas Asociadas.

Comunicar a todo el personal que deba participar en las pruebas la fecha y hora en que serán realizadas.

Comprobar que todas las personas involucradas disponen de una copia del Plan de Continuidad del servicio

Ejecutar las pruebas previstas.

Las pruebas y resultados obtenidos deben ser convenientemente documentados. Cada uno de los integrantes de los equipos que participen en el desarrollo de las mismas debe mantener un registro detallado de las acciones realizadas, los resultados obtenidos, tiempo empleado e incidencias que hayan podido surgir, con el fin de evaluar los resultados obtenidos.

El responsable de cada uno de los equipos entregará al Responsable del Plan de Continuidad del servicio un informe en el que figuren:

Objetivo de la prueba efectuada.

Resultados obtenidos y tiempo empleado para la recuperación.

Incidencias que hayan podido surgir.

Posibles recomendaciones de corrección y seguimiento.

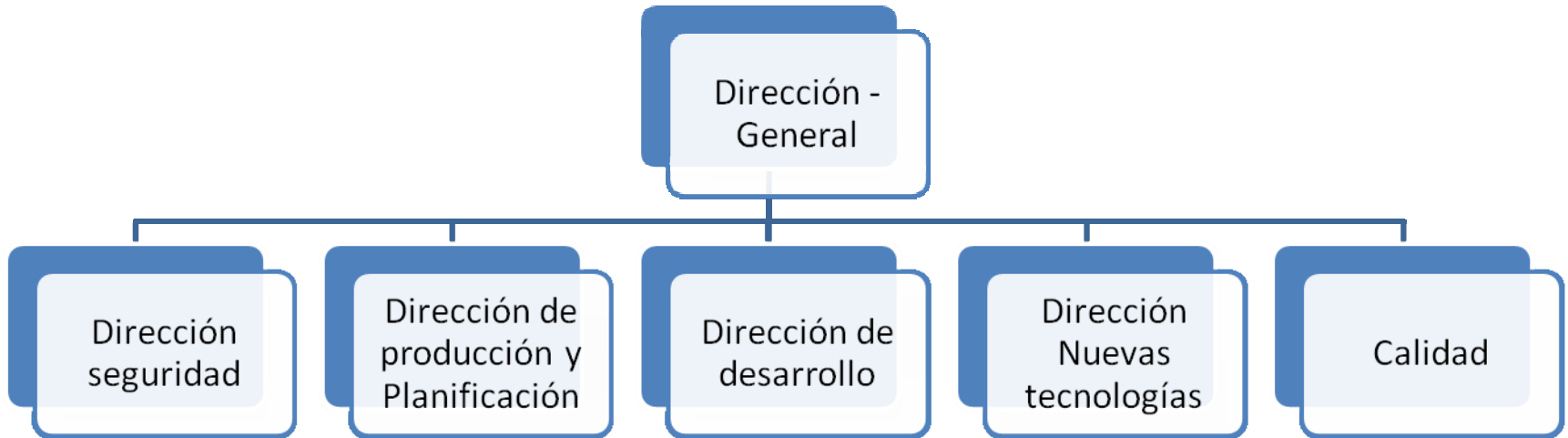
Evaluación de los resultados

Antes de la realización de cualquier prueba han de especificarse los criterios de evaluación de los resultados obtenidos tras su realización.

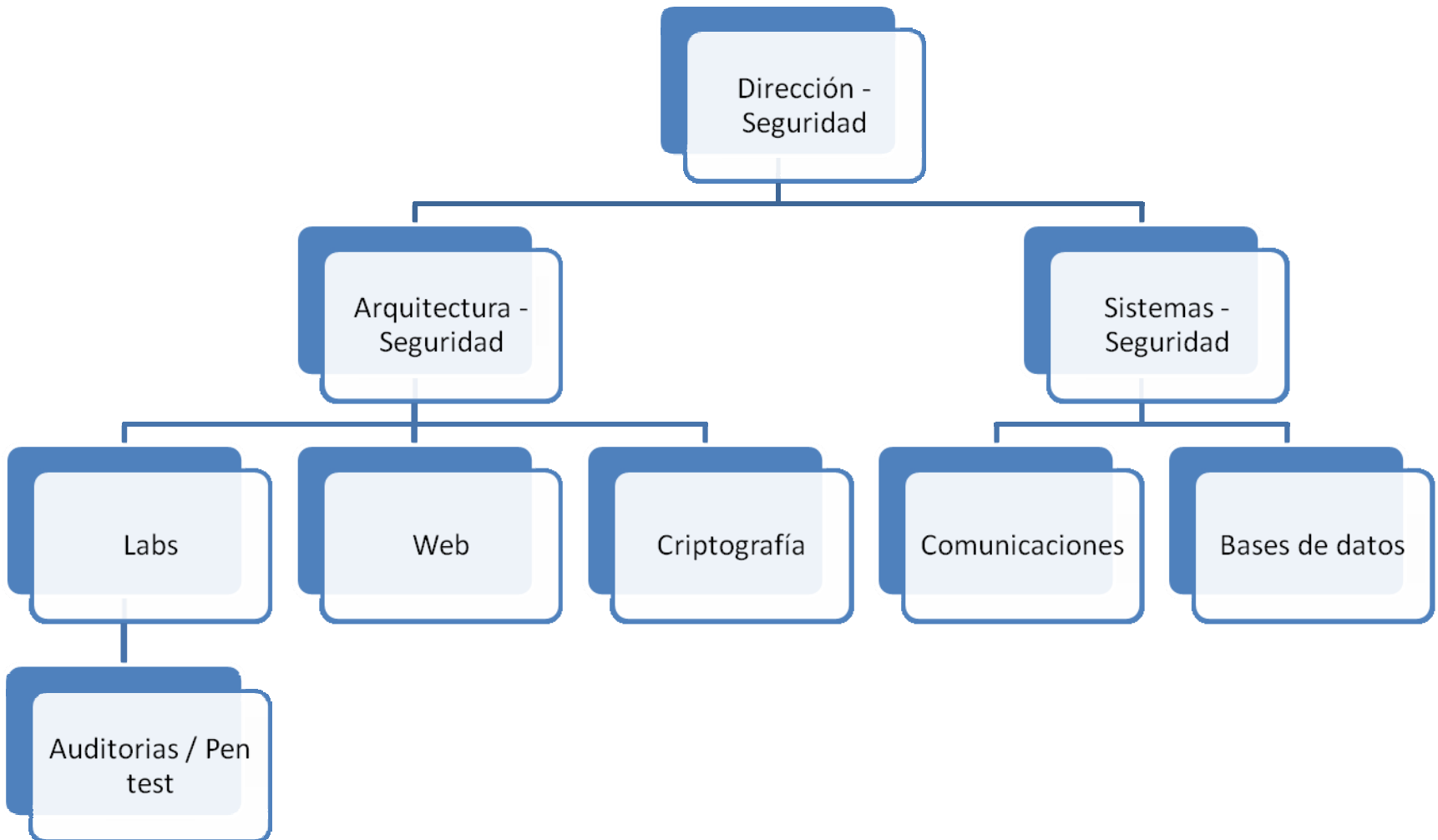
Una vez finalizadas las pruebas se mantendrá una reunión de evaluación de los resultados obtenidos, con el fin de evaluar la eficacia de los procedimientos establecidos en el Plan de Continuidad del servicio e introducir todas aquellas

3.- Equipo de seguridad

3.- Equipo - Seguridad



3.- Equipo - Seguridad



3.- Equipo - Seguridad



4.- Seguridad en Banca Electrónica

4.- Seguridad en Banca Electrónica

Activa:

Seguridad en el Sistema operativo
Seguridad en el perímetro
IPS/IDS a nivel de red
Firewall capa 7

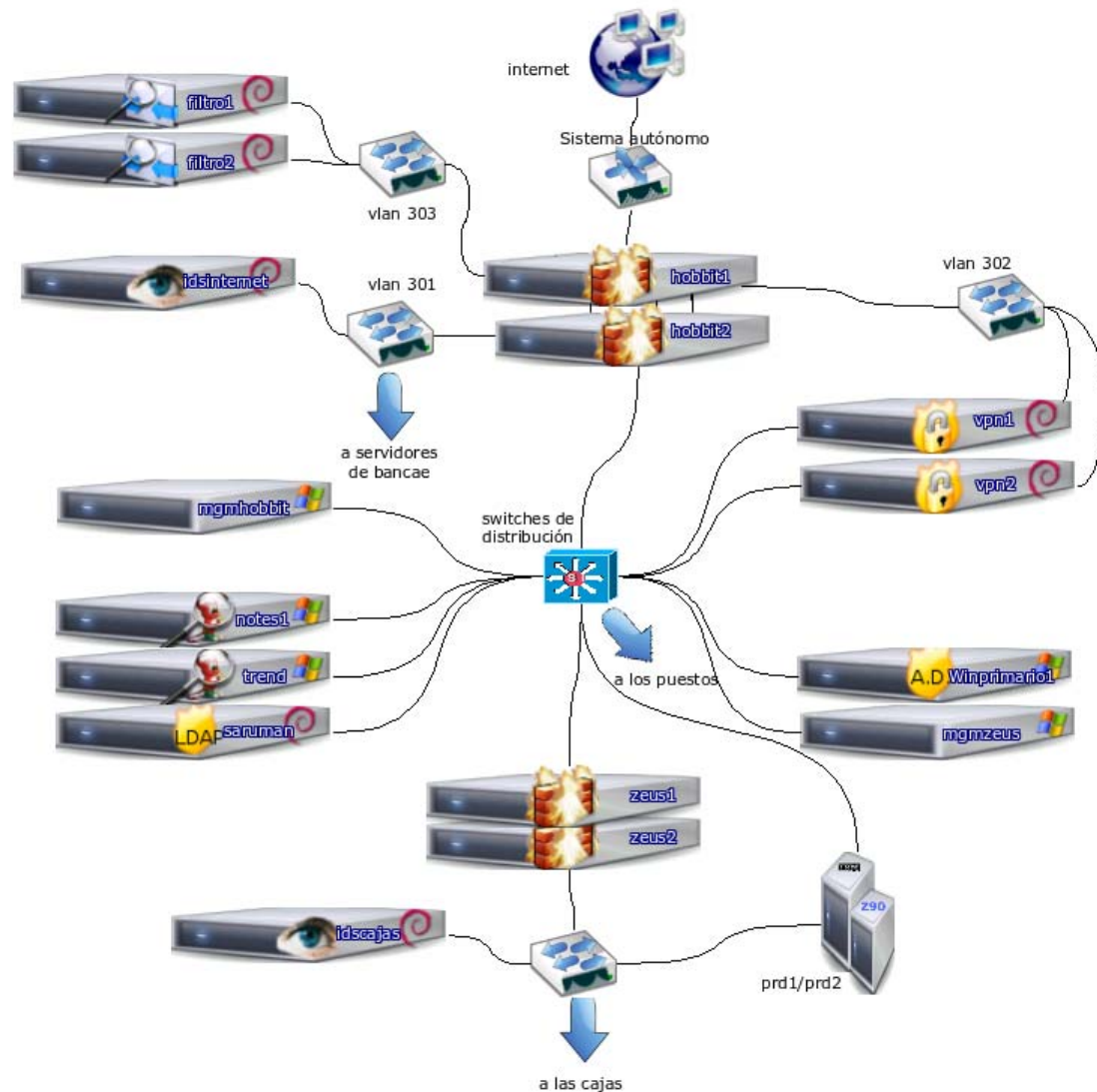
Reactiva:

Sistemas de alertas
Anti fraude
HoneyNet

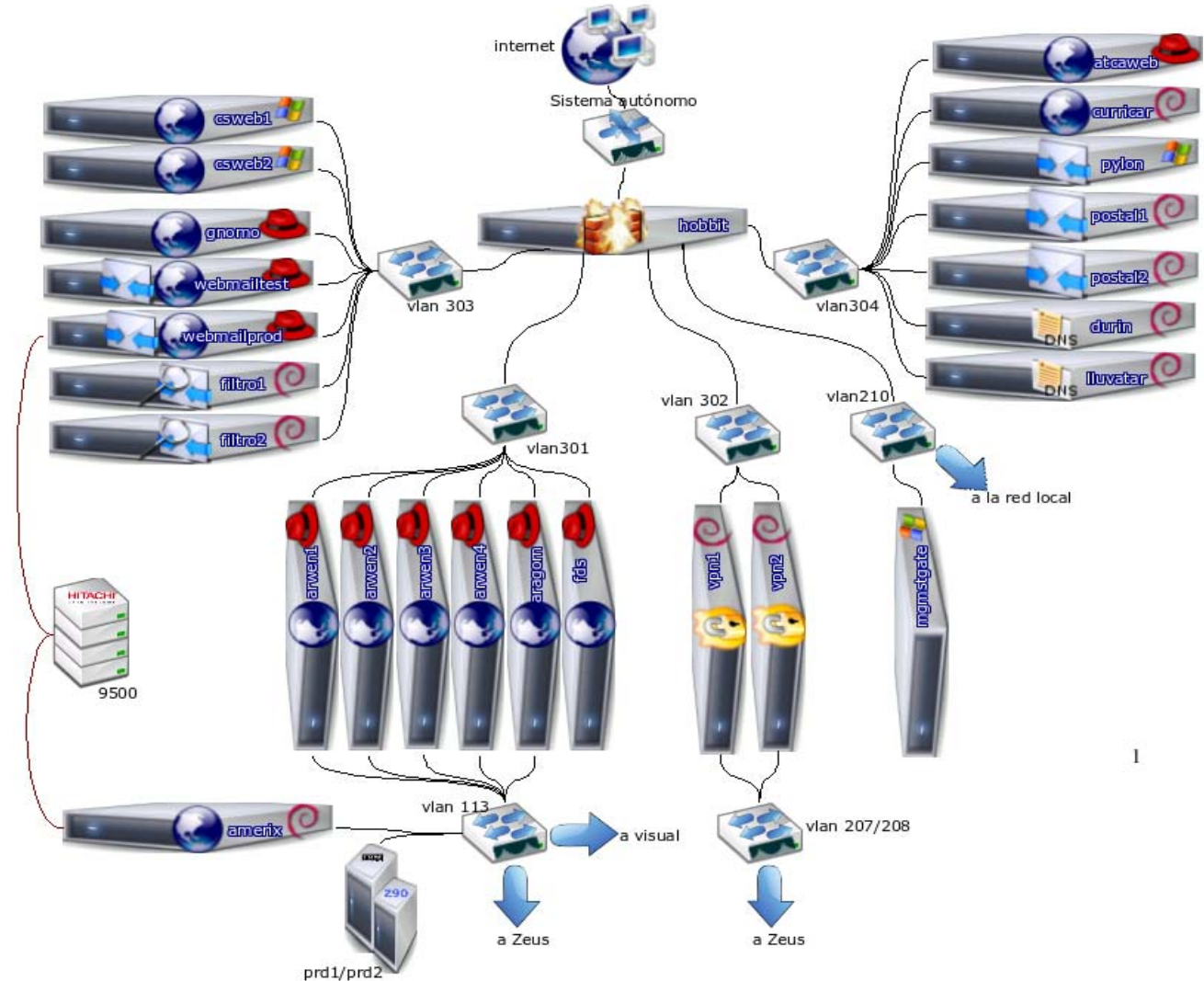
Usuarios:

Login / Teclado virtual
Token
eDNI
SMS con clave única

4.- Seguridad BE



4.- Seguridad BE



4.- BE - Seguridad



Sistema operativo:

<http://www.openbsd.org/es/security.html>

- Objetivos de seguridad del proyecto.
- Política de transparencia absoluta.
- Proceso de auditoría del código fuente.
- «Seguridad predeterminada».
- Uso de criptografía.
- Monitorización de cambios.
- Informes sobre asuntos de seguridad.



<http://www.engardelinux.org/>

SELinux

4.- BE - Seguridad

Firewall CAPA 7: ATUXid



Cuando se inicia apache:

- Carga de firmas de Mod_security

- Carga de controles propios desarrollados en JAVA

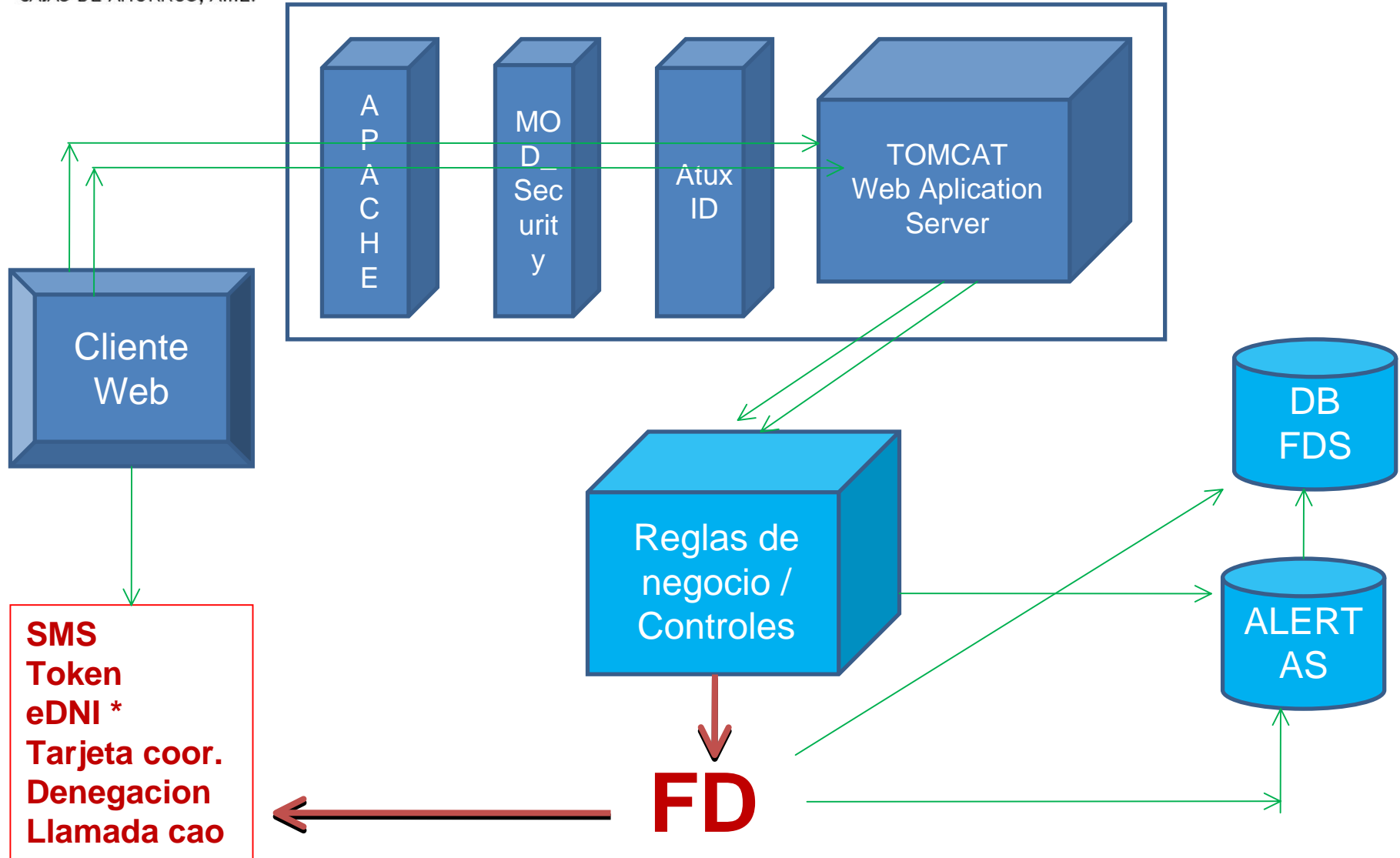
Cuando se entra en la aplicación:

- Seguimiento y monitorización de la sesión del usuario

- Carga de controles específicos dependiendo de la
criticidad

- Firmas específicas según la validación

4.- BE - Seguridad



4.- BE - Seguridad

Setting and rule				
General tab				
Maximum headers length	32768	32768	32768	32768
Maximum payload length	10485760	10485760	65536	Any
Maximum URL length	16384	319	1024	16384
Maximum query length	4096	13	512	4096
Verify normalization	Yes	Yes	Yes	Yes
Block high bit characters	No	Yes	Yes	Yes
Block responses containing Windows executable content	Yes (Note 1)	Yes	Yes	Yes
Methods tab				
Allow only specified methods	BCOPY BDELETE BMOVE BPROPPATCH DELETE GET MKCOL MOVE POLL POST PROPFIND PROPPATCH SEARCH SUBSCRIBE	GET HEAD POST	OPTIONS POST	RPC_IN_DATA RPC_OUT_DATA

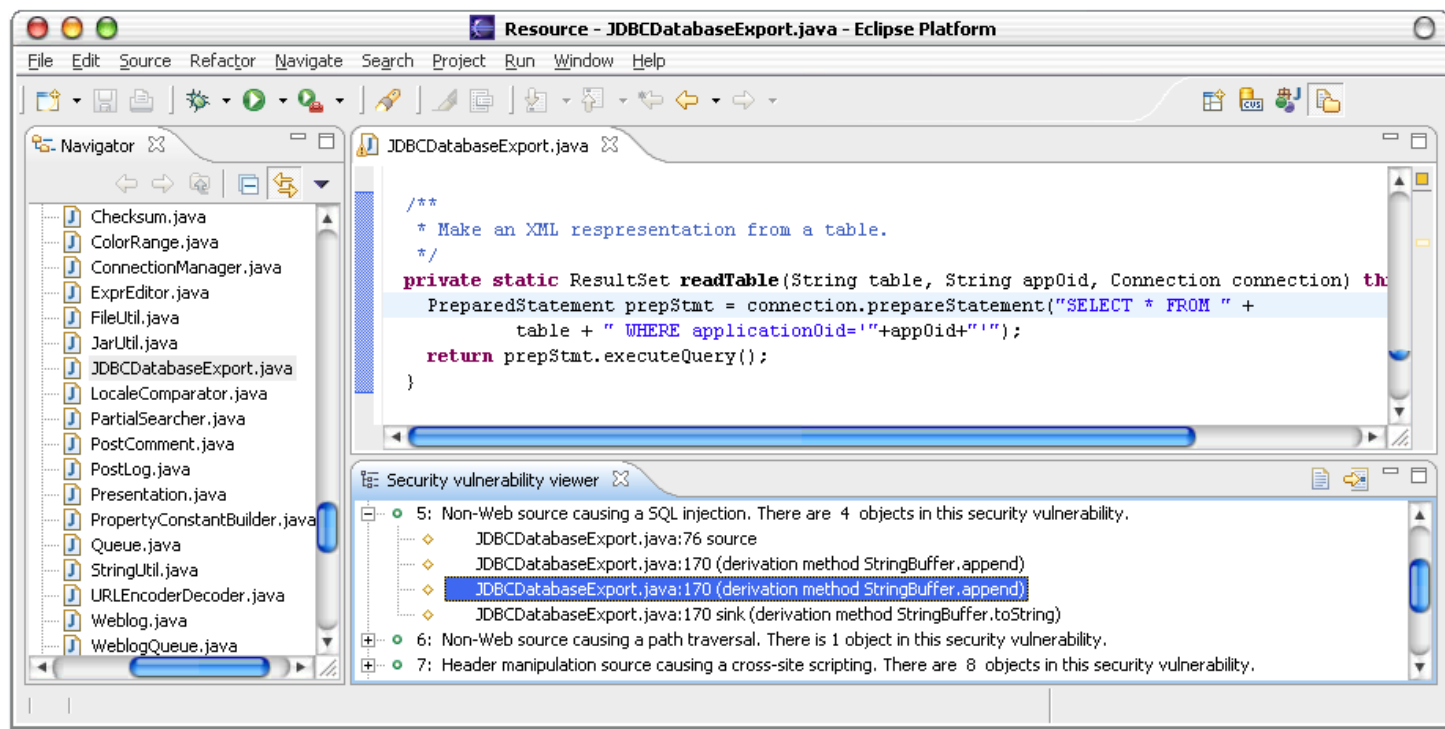
4.- BE - Seguridad

Seguridad en el código:

Formación continua

Auditoria del código fuente (2 veces al año, externalizado)

Auditoria de nuevos módulos (Peer – review)



ACCEDA A SUS CUENTAS**Acceso con Código de Usuario**Código de usuario: Pulse sobre el teclado para
introducir su Clave de Acceso:**Acceso con DNI Electrónico**

Pulse sobre la imagen del DNI:

[Darse de alta en CAI On Line](#) | [Demostración](#)**RECOMENDACIONES DE SEGURIDAD:**

Caja Inmaculada nunca solicitará mediante teléfono, correo electrónico o fax, información que revele sus claves personales de CAI OnLine.

- Acceder a CAI On Line
- Correo electrónico: enlaces y virus
- Seguridad en micorreo.cai.es
- Antivirus
- Navegar por Internet

RENTA 2006

Presenta tu declaración desde
CAI On Line

Recibirás respuesta inmediata de la AEAT
Sin certificados adicionales

**HOY DESTACAMOS**

- En CAI On Line también puede securizar su tarjeta CAI para realizar compras seguras por Internet: billetes de RENFE, etc.
- Ahora también puede tramitar Ordenes de Librado: pago de efectos, devoluciones, envío otras entidades...
- Presente su Declaración de la Renta sin certificados electrónicos
- Ahora también puede acceder a CAI On Line con DNI electrónico
- Aviso mediante mensajes SMS gratis a su móvil: abono de nómina, movimientos de sus cuentas, saldos, cargos, etc.
- Disponible el traspaso global o parcial entre Fondos de Inversión CAI



Caja de Ahorros de la Inmaculada de Aragón - NIF. G-50000819.
Entidad de Crédito inscrita en el Registro Especial del B.E.; Código B.E.:2086.
Domicilio Social: Paseo de la Independencia, nº 10. 50004 - Zaragoza.

4.- BE - Seguridad

Herramientas:

Imperva (Scan)

Acunetix

CANVAS ([Gleg, Ltd's VulnDisco](#) and the [Argeniss Ultimate 0day Exploits Pack](#))

Auditorias:

Cuatro de seguridad en Internet al año

5 in situ al año:

- PCI – VISA y MASTERCAD

- Banco España

- Controles Generales

- LOPD

- Seguridad redes

4.- Seguridad BE

ATCA Labs Security:

Departamento para el análisis de troyanos y otros programas malware, que nos remiten los clientes

Desarrollo de software de protección a clientes, como USB's Live, o 'SandBox' para explorer

¿Qué hacemos mal?

Seguimos dependiendo de las personas (No me fio)

Malas configuraciones

Malas intenciones

Seguimos dependiendo (cada vez menos) de aplicaciones desarrolladas por terceros

Retrasos por nuestra política

Productividad contra seguridad

5.- Futuro

5.- Futuro

ATCA CERT

Pretende ser el centro de seguridad gestionado de las Cajas Asociadas

Todos los eventos de monitorizados (Servidores, puestos, circuitería, etc)

Queda pendiente definir roles administrativos y servicio de atención a usuarios

6.- Conclusiones

6.- Conclusiones

1. – Todas las entidades bancarias tienen altos niveles de seguridad, basados en la tecnología, pero no todas lo gestionan correctamente
- 2.- El fraude a día de hoy sigue siendo en los Cajeros, siendo mínimo en internet.
- 3.- El auge del phishing, pharming y ataques a entidades financieras, hacen que ‘nos espabilemos’ si queremos ganar la confianza de los clientes de canales como BE
- 4.- Difícilmente un ataque puede llegar a tener éxito (económico) (y a excepción , el problema radica en el fraude interno y la mala imagen reputacional
- 5.- Es mas sencillo el robo de tarjetas e información en ‘intermediarios’
- 6.-Nuestro problema: Las denegaciones de servicio



ASOCIACION TECNICA
CAJAS DE AHORROS, A.I.E.

¿Preguntas?