Generando confianza en el correo electrónico

Miguel Macías Enguídanos
miguel.macias@upv.es

RedIRIS

UNIVERSITAT POLITÈCNICA DE VALÈNCIA

Jornadas Técnicas
Valladolid, 01/12/2011

Índice

- Scams
  - fraudes a través del e-mail
- Una solución: el procedimiento CFD
- S/MIME
- Aspectos a tener en cuenta
- Conclusiones

La gota que colma el vaso

- Mensaje de correo recibido en la UPV (agosto 2008)

Estimado Universidad Politécnica de Valencia los usuarios de correo web,

Este mensaje es de la Universidad Politécnica de Valencia, centro de mensajería para todos Universidad Politécnica de Valencia webmail **users**. **We son** actualmente la mejora de nuestra base de datos y e-mail centro. Estamos suprimiendo todos los no utilizados **upf.edu** correo electrónico, Usted está obligado a verificar y actualizar su mensaje de correo electrónico confirmando su identidad. Esto evitará que su dirección de correo electrónico de concluidos durante este ejercicio. Con el fin de confirmar la identidad de correo electrónico que usted, usted es para proporcionar los siguientes datos;

Confirmar su identidad por debajo de correo electrónico

Nombre :.....
Apellido :.....
Email Nombre de usuario: .....
E-mail Contraseña: .....

¡Advertencia! Universidad Politécnica de Valencia
Email usuario que se niega a verificar y, posteriormente, actualizar su correo electrónico dentro de los siete días de haber recibido esta advertencia **perderá su correo electrónico permanentemente**.

Thank you for using Universidad Politécnica de correo electrónico!
Advertencia Código: VX2G99AAJ

Gracias,
Universidad Politécnica de Valencia Centro de Mensajes…

La gota que colma el vaso

- Mensaje de correo recibido en la UPV (agosto 2008)

Estimado Universidad Politécnica de Valencia los usuarios de correo web,

Este mensaje es de la Universidad Politécnica de Valencia, centro de mensajería para todos Universidad Politécnica de Valencia webmail **users**. **We son** actualmente la mejora de nuestra base de datos y e-mail centro. Estamos suprimiendo
todos
elect
ejerc
datos

Conf

Nom
Apell
Ema
E-ma

¡Adv
Ema
recib

Thar
Advertencia Código: VX2G99AAJ

Gracias,
Universidad Politécnica de Valencia Centro de Mensajes...

Durante el verano de 2008 varias Universidades Españolas sufrieron una ataque de Phishing dirigido cuyo objetivo era el de recopilar credenciales webmail para realizar, a partir de dichas cuentas, diversos ataques de envío de SPAM indiscriminado, suplantación de identidad, etc..

Fueron 12 las instituciones de RedIRIS afectadas por este ataque, y aunque el número de cuentas de webmail comprometidas no fue muy elevado, el uso de las mismas por los atacantes para enviar SPAM fue extensivo.

RedIRIS: Informe de incidentes de seguridad año 2008
http://www.rediris.es/cert/doc/informes/2008/

La evolución de los ataques

- Mensaje recibido en la UJI en julio de 2009

From: UJI LEQUIP DE SUPORT

Benvolgut Propietari Email UJI,
Aquest missatge és UJI del centre de missatges de correu electrònic a tots els propietaris UJI. Ara som la millora de la nostra base de dades i de correu electrònic està esborrant tots els **center.We UJI correu** no utilitzats per crear més espai per a un nou
.==========
Per **evitar el tancament del seu compte** vostè haurà d'actualitzar que a continuació per que sabrà que es tracta d'un compte utilitzen actualment
.==========
CONFIRMAR SU EMAIL AVALL
EMAIL nom d'usuari:
EMAIL CONTRASENYA:
CONFIRM EMAIL CONTRASENYA:
DATA DE NAIXEMENT:
De correu electrònic alternativa:
==========
Advertència! En cas contrari, fer immediatament la seva compte desactivada del nostre database.We disculpes per les molèsties que això causa que durant aquest període, però la confiança que entén que la nostra principal preocupació és per als nostres clients i per a la seguretat dels seus clients data. our són totalment segurs

Gràcies,
UJI L'EQUIP DE SUPORT

- http://blogsi.uji.es/correu/2009/07/

La evolución de los ataques

- Primer *phishing* al correo de la UPV (enero 2010)

UNIVERSIDAD POLITECNICA DE VALENCIA

Hola,

Debido a la actualización de nuestro SECURTY nuevos y la eliminación de todas las cuentas no utilizadas tendrá que confirmar su dirección de e-mail con la firma en su cuenta. También sería cerrar todas las cuentas no utilizadas.

Lo que hay que hacer:
1. Inicie sesión en su cuenta en https://webmail.upv.es, haciendo clic en la URL.
2. Introduzca su ID de usuario y contraseña.
3. Una vez que inicie sesión en un nuevo perfil de seguridad se actualizará para su cuenta.

Después de seguir las instrucciones de la carta, su cuenta no será interrumpido y continuará como normal. Gracias por su atención a esta solicitud. Nos disculpamos por cualquier inconveniente.

Por favor, acceda a su cuenta inmediatamente y seguir utilizando la cuenta de forma habitual mientras disfruta de nuestras nuevas actualizaciones de seguridad.

https://webmail.upv.es
Webmaster.
https://webmail.upv.es

© 2009 **Universidad Politécnica de Valencia**

- http://asic.blogs.upv.es/correo-electronico/¡no-te-dejes-enganar/

La evolución de los ataques

- Primer *phishing* al correo de la UPV (enero 2010)

UNIVERSIDAD POLITECNICA DE VALENCIA

Hola,

Debido a la actualización de nuestro SECURTY nuevos y la eliminación
no utilizadas tendrá que confirmar su dirección de e-mail con la firma er
sería cerrar todas las cuentas no utilizadas.

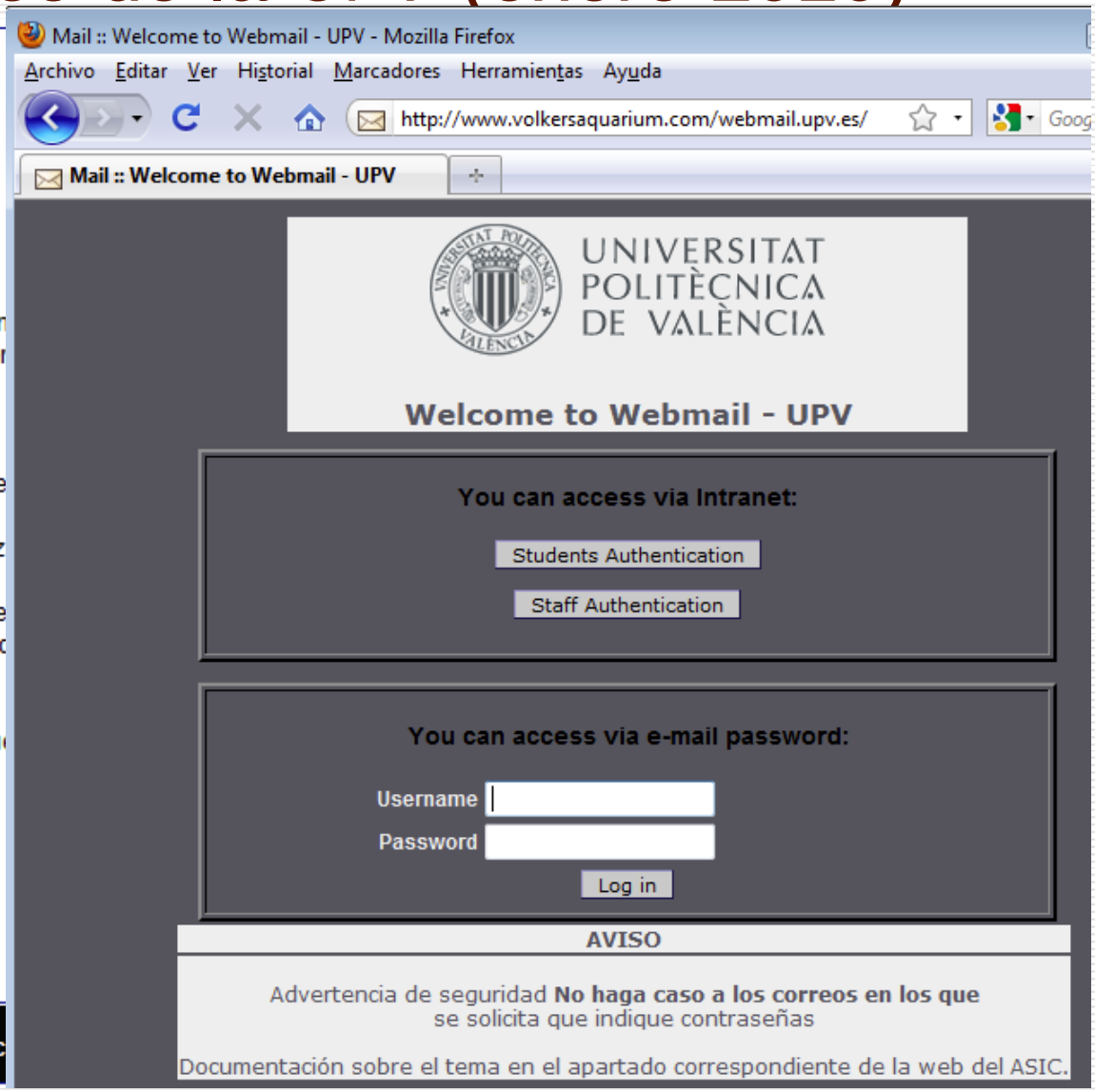
Lo que hay que hacer:
1. Inicie sesión en su cuenta en https://webmail.upv.es, haciendo clic e
2. Introduzca su ID de usuario y contraseña.
3. Una vez que inicie sesión en un nuevo perfil de seguridad se actualiz

Después de seguir las instrucciones de la carta, su cuenta no será inte
como normal. Gracias por su atención a esta solicitud. Nos disculpamc
inconveniente.

Por favor, acceda a su cuenta inmediatamente y seguir utilizando la cu
mientras disfruta de nuestras nuevas actualizaciones de seguridad.

https://webmail.upv.es
Webmaster.
https://webmail.upv.es

© 2009 Universidad Politécnica de Valenc



- http://asic.blogs.upv.es/correo-electronico/¡no-te-dejes-enganar/

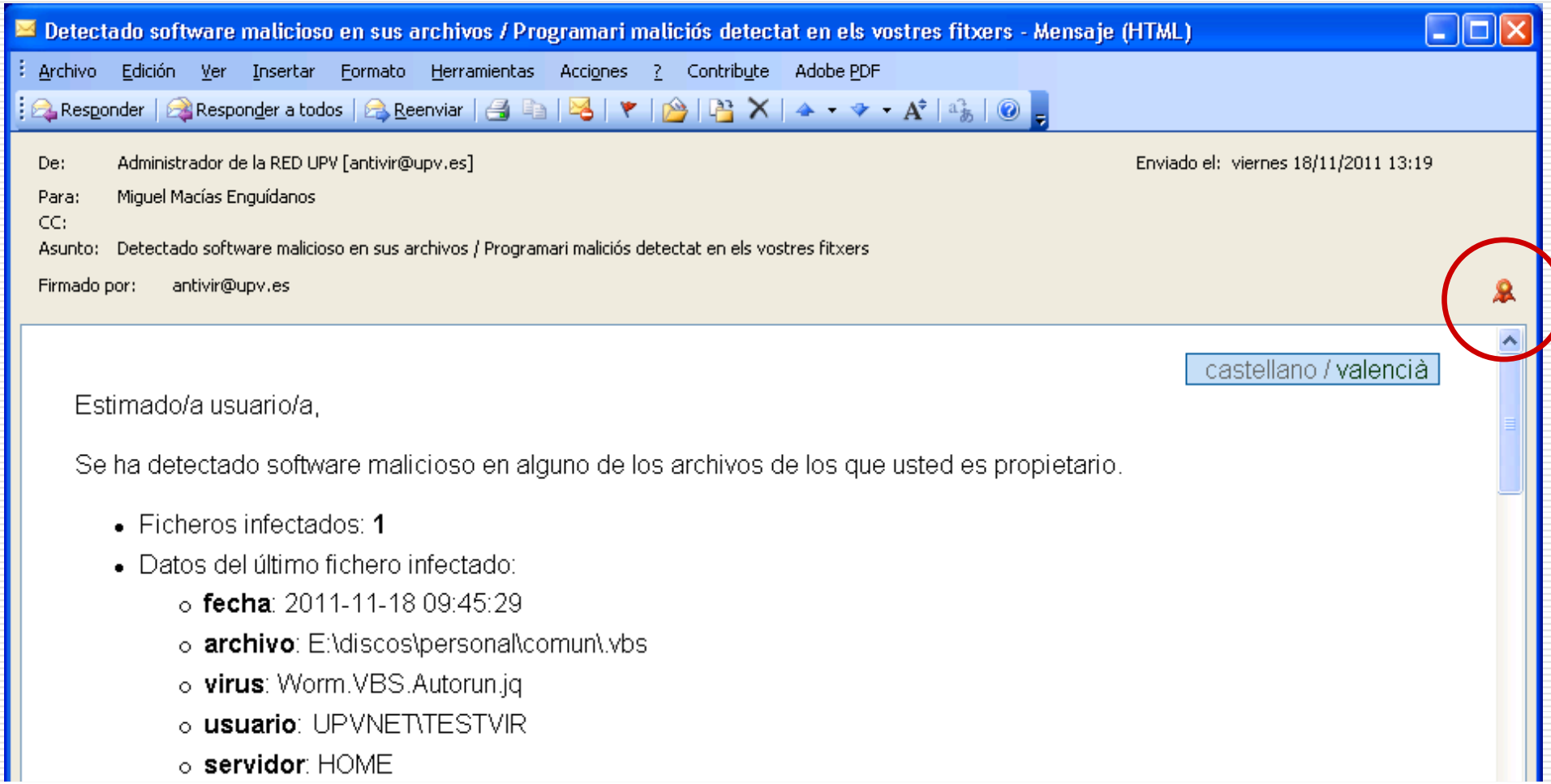
Posibles contramedidas

- Se necesita un sistema que permita al usuario determinar, fácilmente y por su cuenta, si un mensaje de correo es legítimo o no
- Añadir mensajes y advertencias a los propios mensajes y a las páginas web ¡no es efectivo!
  - los usuarios no solemos leer todo el contenido
  - las advertencias se pueden copiar en los fraudes
- S/MIME es el mecanismo ideal...
  - garantiza la integridad del mensaje y la cuenta remitente
- ... si no fuera porque:
  - algunos clientes de correo no dan soporte a S/MIME
  - la mayoría de los usuarios no tiene la cultura necesaria

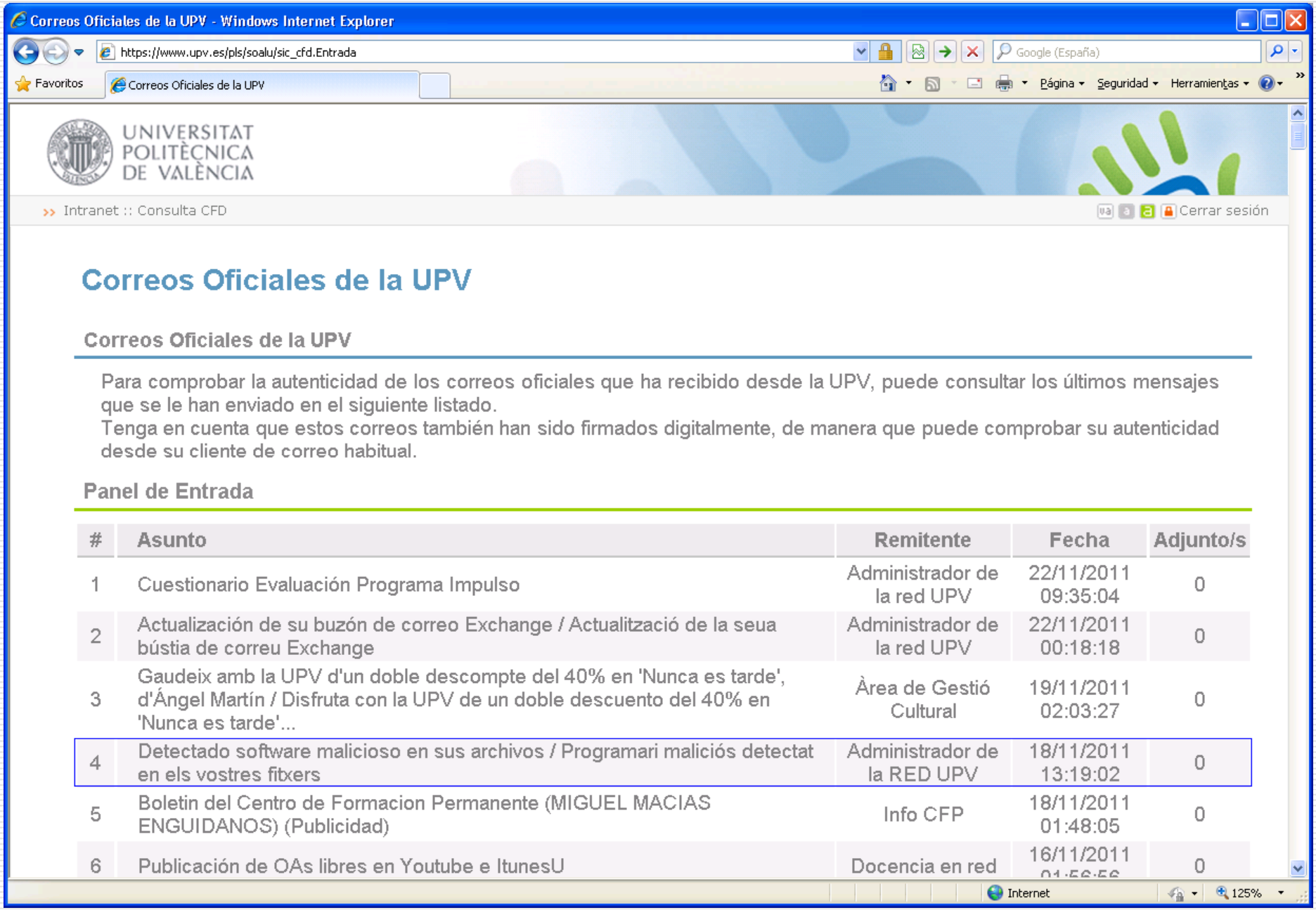
El procedimiento CFD en la UPV

- La UPV puso en marcha el **procedimiento CFD** (Correos Firmados Digitalmente) en noviembre/2009
- Todos los correos oficiales (correos cuyo remitente es un servicio de la Universidad):
  - se firman digitalmente
  - pueden consultarse desde la Intranet de la UPV
- Así pues, cuando un usuario tiene dudas sobre la autenticidad de un mensaje:
  - puede comprobar si está firmado digitalmente y verificar que la firma es correcta
  - puede entrar en la Intranet y comprobar que el mensaje (con todo el contenido) se ha enviado oficialmente

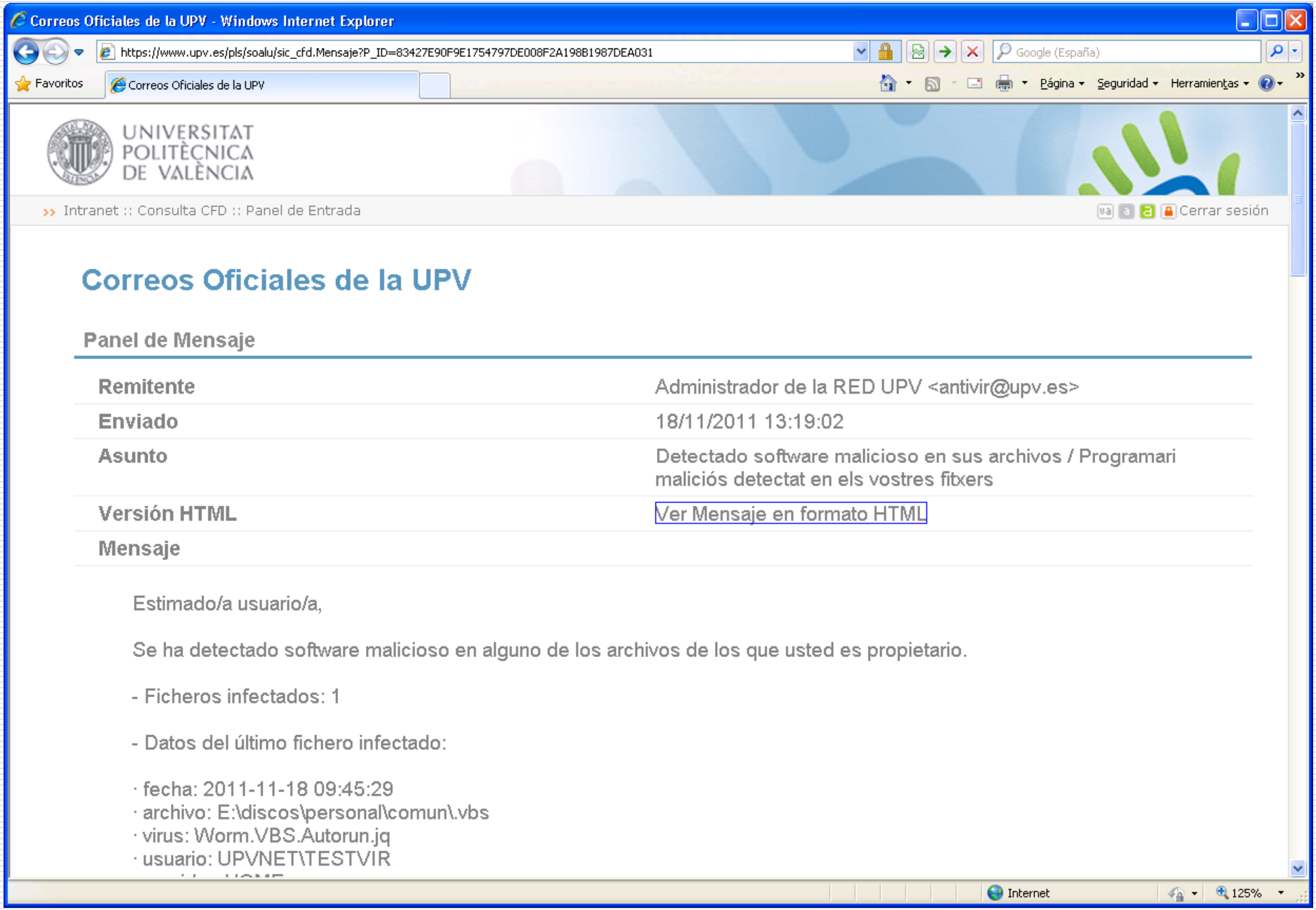
Mensaje firmado digitalmente



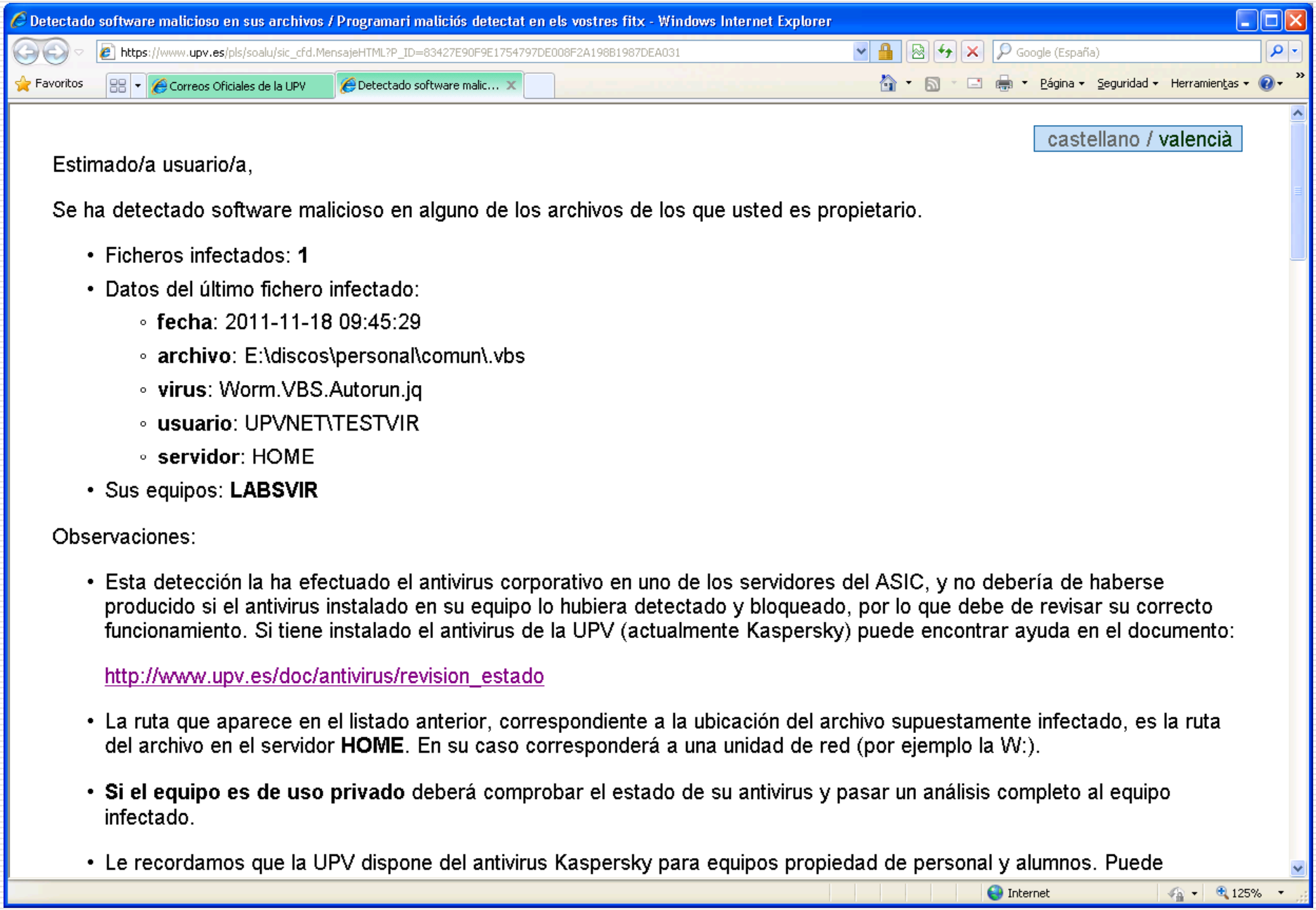
Lista de mensajes oficiales



Mensaje consultado en la Intranet



Mensaje consultado en la Intranet



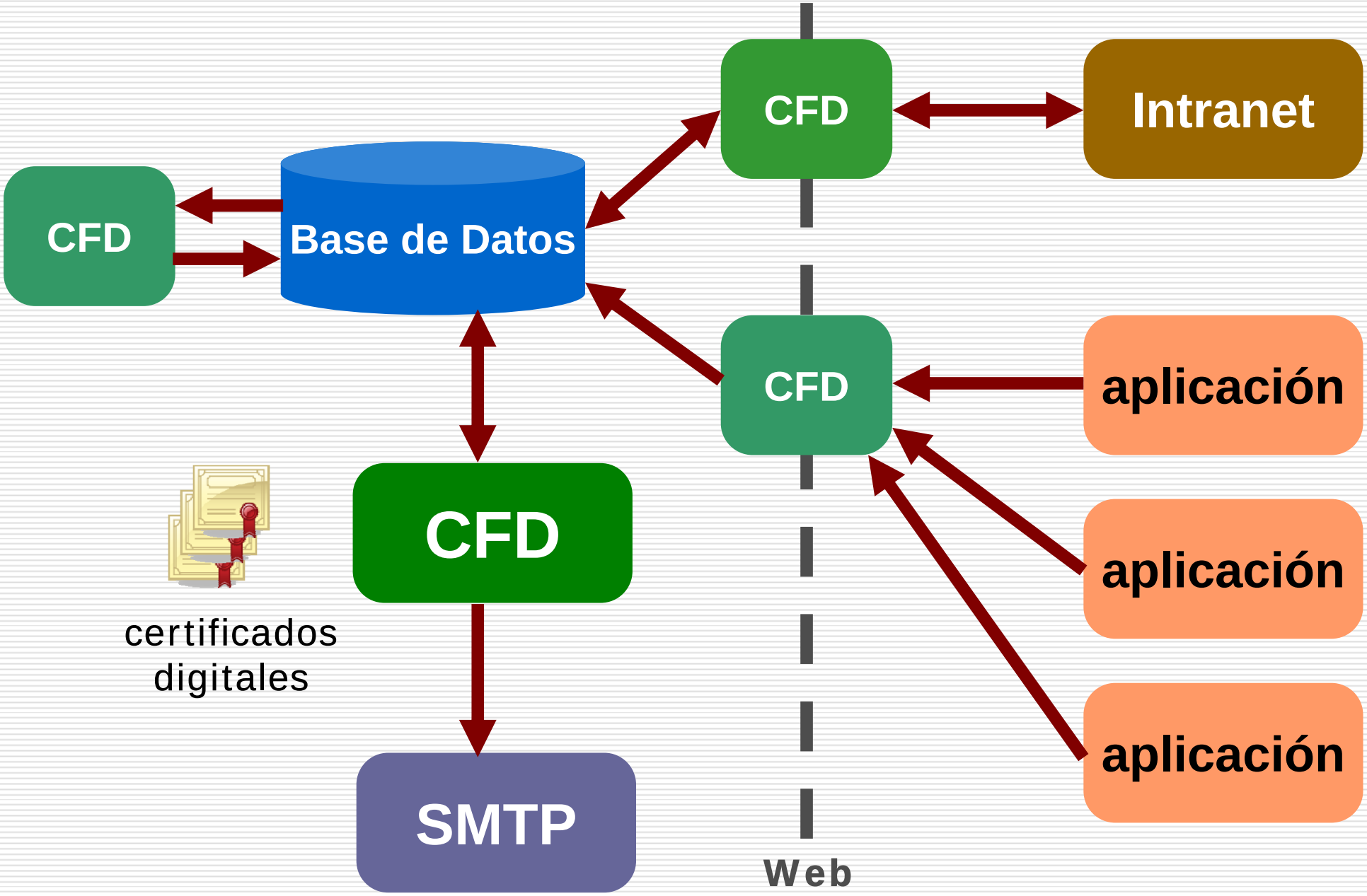
Certificados digitales

- S/MIME implica la utilización de certificados digitales para todas las direcciones oficiales de la UPV
  - los certificados tienen que ser válidos y reconocidos por la mayoría de clientes
- Utilizamos los certificados gratuitos de Comodo:
  - Free Secure Email Certificates https://www.instantssl.com/
- Tienen una validez de 1 año
- Pueden renovarse tantas veces como se quiera
- Centralizamos la gestión de los certificados

Consulta de correos en la Intranet

- La decisión de mostrar los mensajes oficiales en la Intranet ha contribuido al éxito de la iniciativa:
  - los usuarios conocen y confían en la Intranet
- Pero ha 'complicado' la solución necesaria para aportar confianza al correo electrónico
- Todos los mensajes han de conservarse en Base de Datos durante un tiempo mínimo
  - actualmente conservamos los mensajes durante 2 meses
- La escalabilidad de la solución es un factor determinante para el éxito de la misma
  - en estos momentos se están enviando una media de 23000 mensajes de correo, por semana, a través de CFD

Arquitectura de CFD



Las interfaces de CFD

- Para que la solución fuese efectiva, teníamos que permitir que cualquier tipo de aplicación fuese capaz de generar envíos
- Hay aplicaciones corporativas basadas en paquetes de la Base de Datos, así pues, CFD tiene un interfaz de envío en la propia Base de Datos
  - PL/SQL sobre Oracle
- Para el resto de aplicaciones se optó por implementar un servicio Web, con autenticación básica sobre SSL y filtrado de IPs
  - se utiliza XML como formato de intercambio de datos

Plantillas de mensajes

- Para optimizar recursos, CFD gestiona los mensajes a través de plantillas
- Cada plantilla define:
  - el remitente (nombre y dirección de correo)
  - el asunto
  - el cuerpo del mensaje (formatos TEXTO y HTML)
  - adjuntos (si los tiene)
- Para cada envío el asunto y el cuerpo del mensaje pueden personalizarse (con variables de reemplazo)
- También se admite cambiar el remitente (dentro de los admitidos para una plantilla) y añadir adjuntos distintos para cada envío

Destinatarios

- Se admiten destinatarios internos y externos
  - utilizando los campos Para, Copia y Copia oculta
- Para los internos (miembros de la UPV), CFD busca el nombre y dirección de correo oficiales
  - y mantiene los mensajes para que pueden consultarse, posteriormente, desde la Intranet
- Las listas de correo son eficientes para el envío, pero ¡sus miembros cambian con el tiempo!
  - se utiliza la lista para el envío
  - se 'despliega' la lista en Base de Datos, almacenando los miembros de la misma en el momento del envío
- CFD permite detectar direcciones de correo erróneas

Equidad en el reparto de recursos

- Algunas plantillas de correo, en CFD, se utilizan para envíos masivos
  - ej.: boletines a suscriptores
- Otras plantillas tienen un uso mucho menor, pero requieren la inmediatez del envío
  - ej.: códigos de comprobación de direcciones de correo
- Actualmente se está ‘penalizando’ a los envíos masivos para dar salida inmediata al resto de envíos
- En cada invocación del procedimiento se comprueba el total de envíos pendientes para cada plantilla
- Se envían mensajes pendientes de todas las plantillas, pero con un límite de envíos

Añadiendo un servicio al CFD

- Los pasos que seguimos para añadir un nuevo servicio al procedimiento CFD son:
  - solicitar certificados digitales para todas las cuentas (no personales) que se utilizan desde el servicio
  - generar plantillas de mensajes (normalmente se empieza con una plantilla genérica)
  - dar de alta al usuario y las IP que invocarán a CFD
  - proporcionar código de ejemplo, según la tecnología que se utilice en el servicio, de acceso a CFD
- Se hace una integración gradual, empezando con una cuenta de correo y un tipo de mensajes y se va ampliando, rápidamente, a la totalidad del servicio

A tener en cuenta: certificados

- Para la emisión/renovación de los certificados digitales que utilizamos se comprueba que la dirección de correo pertenece al solicitante
  - se envía un código por correo, necesario para el proceso
- La práctica nos enseña que esta comprobación del correo puede no ser tan sencilla
  - el mensaje de Comodo se trata como spam...
  - los gestores del correo oficial lo tratan como spam...
- Interesa renovar los certificados digitales lo antes posible, antes de que caduquen los actuales
  - para evitar que un mensaje que se ha enviado recientemente aparezca, a los pocos días, como *problemático* por haber caducado el certificado

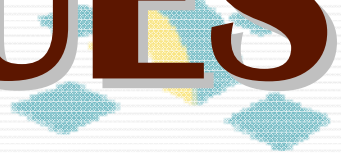
Conclusiones

- ¿Evita el procedimiento CFD que los usuarios sean víctimas de ataques por correo electrónico?
  - No (o no del todo). Pero este procedimiento va generando una conciencia y un modo de actuar ante mensajes fraudulentos
- ¿Hay constancia de la efectividad del CFD?
  - Sí, hemos tenido comentarios del tipo: ‘este mensaje deber ser falso, porque no aparece en la Intranet’
- ¿Proporciona algún valor añadido el CFD?
  - Sí. El hecho de utilizar consistentemente S/MIME hace que los usuarios vayan aprendiendo el funcionamiento del correo firmado/cifrado y que quieran integrarlo en su trabajo cotidiano

Generando confianza en el correo electrónico

GRACIAS POR VUESTRA ATENCIÓN

Miguel Macías Enguídanos
miguel.macias@upv.es



Jornadas Técnicas
Valladolid, 01/12/2011