tecnimap 2002
www.tecnimap.com
VII JORNADAS SOBRE TECNOLOGÍAS DE LA INFORMACIÓN PARA LA MODERNIZACIÓN DE LAS ADMINISTRACIONES PÚBLICAS
A CORUÑA
15, 16, 17 y 18 de octubre de 2002
Palacio de Congresos y de la Ópera
Ponencias

Experiencias de Comercio Electrónico en las AAPP: La Tienda Virtual del BOE

David Guerrero
Dolores Martín
José Manuel Ruiz
Dpto. Tecnologías de la Información

1. Introducción

El Boletín Oficial del Estado, a través de su Librería tiene como misión poner a disposición de todos los ciudadanos los títulos que publica así como los del resto de Administraciones Públicas a través de acuerdos de distribución. El auge del acceso a Internet por parte del ciudadano ha hecho que la vía del comercio electrónico se convierta en uno de los canales más importantes para la distribución de este tipo de material, y el BOE no podía quedarse al margen de este hecho.

A mediados del año 2000 se planteó el proyecto de creación de una plataforma que permitiese la venta de dichas ediciones a través de Internet, de forma que se integrase con los procesos internos de mantenimiento de la Librería y de facturación común a toda la organización. Por otra parte, dicha plataforma, inicialmente diseñada para la venta de

libros, debería ser compatible, al menos en cuanto a la parte de pago electrónico se refiere, con otros procesos de venta, como la de bonos de consulta a la base de datos, o la de suscripción a servicios de información personalizados.

Desde un primer momento, el análisis y desarrollo fue asumido por el personal del Departamento de Tecnologías de la Información, y se optó por el uso de tecnologías de software libre hasta donde pudiera tener sentido. La plataforma de desarrollo elegida, después de diversas pruebas fue Apache + Mod_SSL + PHP + Oracle.

En la situación de partida se contaba ya con un sistema de gestión de la propia Librería , Kriter Empresarial, en la cual se mantenía el control de stock, y con el cuál se debía hacer interface tanto en entrada como en salida. La idea era extraer la información de stock y datos comerciales de dicho sistema, y retornar la información de ventas a dicho sistema para mantener su información de stock actualizada. Por otra parte se desarrollo sobre Oracle el aplicativo necesario para la gestión de la información que no se disponía en la propia aplicación de gestión de la Librería como era, por ejemplo, la imagen de la portada del libro en cuestión, o un resumen de sus contenidos.

Como es lógico también se debió hacer hincapié en las cuestiones de seguridad del sistema, dado que implica transacciones económicas y manipulación de datos sensibles como el número de la tarjeta de crédito del cliente.

2. Arquitectura del sistema

Se opta por una arquitectura en varios niveles, en las que claramente se diferencian tres elementos:

- El front-end de ventas o tienda, que es el interfaz contra el cuál trabaja el usuario a la hora de comprar en la tienda.

- El back-end de ventas o trastienda, que es el interfaz contra el cuál trabaja el personal de la Librería que se encarga de cumplimentar (realización del paquete, cobro y envío) los pedidos. Es en este nivel donde se integra el TPV-Virtual, un elemento clave para el proceso de cobro.

- La aplicación de gestión del catálogo es el aplicativo que permite al Departamento Editorial mantener actualizada la base de datos de los libros a vender, así como determinar distintos aspectos comerciales de los mismo, como por ejemplo, qué libros desean que aparezcan como publicitados en la página de entrada a la tienda.

Tanto el front-end como el back-end de ventas, al ser nuevos desarrollos, se han realizado en PHP, un potente lenguaje de programación para web, altamente integrado tanto con Apache, el servidor web utilizado de forma habitual por la organización, como con Oracle, el motor de bases de datos corporativo. Tanto Apache como PHP son dos buenos ejemplos de software libre con alto nivel de penetración en el mercado y que gozan de un cuidado soporte por parte de sus desarrolladores, hasta el punto de haber contactado varias veces con ellos para perfeccionar y corregir algunos aspectos de los mismos, y haberse obtenido respuesta satisfactoria en pocas horas. El uso de PHP como herramienta de programación para las páginas web ha permitido que la generación de dichas páginas sea 100% dinámica, orientada a objetos, y todas ellas sean dirigidas por la base de datos.

La aplicación de gestión del catálogo, al ser únicamente un interfaz de mantenimiento de una serie de tablas Oracle y con un ámbito de utilización muy restringido (menos de 5 usuarios), se decidió desarrollar con herramientas cliente-servidor proporcionadas por el propio fabricante, en este caso, Developer 2000.

El TPV-Virtual es el elemento clave para la transacción económica. Es un programa suministrado por el proveedor de servicios de pago, BBVA en el caso del BOE, a través del cuál y gracias al API en C proporcionado, es posible ordenar el cobro de un importe asociado a una tarjeta de crédito desde la aplicación de trastienda.

3. Consideraciones de seguridad

Debido a las restricciones de seguridad, se decidió ubicar únicamente el front-end de ventas en los servidores externos del BOE, junto al resto de webs públicos del organismo. Tanto el back-end de ventas, como la aplicación de gestión del catálogo se sitúan físicamente detrás del cortafuegos, en la zona segura. Es en esta zona segura donde se mantiene el histórico de pedidos y se realizan las operaciones de cobro.

Esta separación física de los distintos papeles también llevó a la separación física de los dos entornos de base de datos. En el entorno del front-end únicamente es necesaria una copia actualizada de la base de datos de publicaciones, a nivel de referencias y stock. El que la base de datos de publicaciones del exterior sea únicamente una copia y que la base de datos real y su mantenimiento se ubiquen en el interior, no es más que una forma de garantizar que ante cualquier modificación no autorizada realizada en el exterior por algún hipotético incidente de seguridad, la integridad de los datos se vea asegurada. La simple copia periódica interior-exterior, refrescaría con datos auténticos la base de datos exterior.

Para poder garantizar esta estanqueidad de los datos interiores es preciso forzar en la política de seguridad de los cortafuegos que solo sea posible establecer conexiones de dentro hacia fuera y nunca al revés.

Este condicionante de la imposibilidad de establecer conexiones hacia el interior es el que fuerza a que todo las inserciones de información de pedidos en la base de datos interna haya de ser por polling periódico de esta última. Es decir, los pedidos se introducen en una tabla externa, y cada 5 minutos, un proceso interno, se conecta al exterior y si existe algún pedido en dicha tabla, se lo trae a una tabla interna y lo elimina, de forma que cualquier ataque al servidor exterior solo pueda tener acceso a una cantidad mínima de información de pedidos.

Aunque este procedimiento de recogida de los pedidos desde el interior de forma periódica minimiza el tiempo que la información de un pedido está presente en los servidores externos, es preciso dotar a estos pedidos de medidas de seguridad adicionales dado que contienen el dato sensible del número de tarjeta de crédito del cliente. Para evitar cual-

quier fuga de información a este respecto, en cuanto el usuario introduce dicho número en el sistema, éste es cifrado con la ayuda de GnuPG, la versión libre del popular PGP, y es insertado en esta forma en la base de datos de pedidos, desde donde en poco tiempo, normalmente poco minutos, es transferido al interior.

Para garantizar la seguridad del sistema, es preciso que en los servidores exteriores solo se encuentre la clave pública utilizada para cifrar el número de la tarjeta de crédito. En los servidores internos es suficiente con disponer de la clave privada correspondiente, para descifrar el número en el momento del pago, y si éste es satisfactorio, se vacía dicho campo para evitar mantener almacenado este dato sensible más tiempo del estrictamente necesario.

Otro importante aspecto de la seguridad del sistema de comercio electrónico es el referente al cifrado de las comunicaciones. Dada la heterogeneidad de los clientes potenciales de un servicio universal como éste, se opto por utilizar el estándar de facto de cifrado en Internet: SSL. Para ello, se le instaló a los servidores Apache del front-end de ventas el complemento Mod_SSL, y se gestionó la emisión de un certificado de servidor firmado por Verisign Inc., reconocido de forma automática por la inmensa mayoría de los navegadores web. De esta forma se asegura la integridad y la confidencialidad de la información sensible transmitida por los clientes hacia el BOE, así como se garantiza al usuario que está introduciendo dicha información en el servidor correcto.

En el caso de las comunicaciones entre el software de TPV-Virtual y la central de pagos de la entidad BBVA, estas se realizan también a través de Internet y con SSL, esta vez iniciándose la conexión desde el interior del cortafuegos, en la máquina en la que reside el back-end o trastienda, utilizándose en este caso unas librerías y certificados propios de la entidad colaboradora.

4. El proceso de compra

Cuando un usuario se conecta a la página http://tienda.boe.es, lo primero que se encuentra es con una serie de libros en promoción, así como una serie de pestañas laterales que le permiten profundizar en el catálogo en función de las

categorías definidas. También tiene la posibilidad de realizar búsquedas en la totalidad del catálogo, ya sea por campos o por texto libre. Cuando selecciona un libro de sus interés se le muestra, además de la foto de la portada, el resto de datos del mismo, y un botón que le ofrece la posibilidad de echar el articulo en la cesta de la compra.

Una vez el artículo está en la cesta, se le ofrece al usuario la posibilidad de seguir comprando más artículos o finalizar la compra realizada. Si elige esta última opción se le redirige automáticamente al servidor con SSL donde a través de dos formularios podrá rellenar sus datos personales y de pago de forma completamente cifrada. Para superar estos formularios se realizan una serie de chequeos sobre los datos introducidos, con objetivo de disuadir potenciales pedidos falsos, en los que se verifican, entre otros, la validez de la dirección de correo electrónico y que la tarjeta introducida cumple la algoritmo MOD 10.

Una vez superados estos chequeos, se le asigna un identificador al pedido, y se introduce en el sistema. Se le envía al usuario un mensaje por correo electrónico comunicándole este hecho y un recordatorio de los artículos y precios solicitados. También se envía una notificación por correo electrónico al grupo de operadores de la trastienda.

Un aspecto importante de la finalización del pedido son las cuestiones fiscales relativas al pedido, que son bien diferentes en función del país o comunidad en que resida el cliente, y que fuerzan a calcular el importe total en función de los datos introducidos.

Una vez introducido el pedido, un proceso que reside en los servidores de trastienda, se conecta periódicamente a los servidores externos y traspasa dicho pedido a los servidores internos, donde será posteriormente procesado por los operadores.

Los operadores de la trastienda varias veces al día se conectan a la aplicación de gestión de pedidos, y una vez cumplimentado cada pedido pendiente pulsan el botón de cobrar a través de la pasarela de pagos. Si la transacción se verifica como correcta, se envía automáticamente un mensaje por correo electrónico al comprador, notificándole el cargo a su tarjeta y que el pedido pasa a la empresa de transporte para su entrega.

Si la transacción no es certificada como válida por parte de la entidad colaboradora, el pedido se anula y se le comunica al cliente este hecho por correo electrónico, quien tiene la oportunidad de repetir el mismo, una vez solucionados los problemas de la tarjeta de crédito con su entidad bancaria.

Uno de los elementos más complejos a la hora de implementar el sistema front-end de la tienda, es la denominada cesta de la compra. Uno de los problemas a la hora de desarrollar aplicaciones web es la atomicidad de las transacciones HTTP, o lo que es lo mismo, para el servidor web cada petición es independiente y no sabe absolutamente nada de lo que pudiera haber hecho anteriormente el usuario. La solución viene dada por el uso de sesiones de PHP, que permiten crear un fichero en el servidor donde ir almacenando los valores modificados por el usuario, tales como la lista de artículos seleccionados por el cliente. Dicho fichero tiene un nombre asociado o identificador, que es devuelto al usuario en forma de cookie o parámetro en el URL en el caso de que el usuario no soporte el uso de cookies, y con el que transparentemente para la aplicación estarán disponibles dichas variables. Este sistema de almacenamiento de sesiones puede generar problemas en el caso de tener distribuido el servicio front-end en varios servidores, detrás de un repartidor de carga web. Es necesaria en este caso, la utilización de algún sistema de persistencia que garantice que un usuario siempre accede al mismo servidor donde mantiene su cesta de la compra.

5. Unas cuantas cifras

A través del sistema de estadísticas del servicio de la Tienda Virtual, se han registrado algunos datos que pueden ser significativos:

- Más de 1.000 pedidos desde su inauguración el 12 de diciembre de 2000
- Más de 6.000 referencias en stock
- Aproximadamente 900 visitas diarias

6. Conclusiones

El disponer de una herramienta como la tienda en Internet ha permitido el acceso a multitud de clientes desde puntos donde antes no llegaba la Librería física del BOE, y ha servido al Departamento Editorial como un servicio de valor añadido que ofrecer a otros organismos de la Administración a la hora de negociar la integración de sus catálogos entre los libros que se ofrecen.

La implantación de un sistema de comercio electrónico en una organización es un proyecto complejo que implica prácticamente a todos y cada uno de los departamentos de la misma, en el cual no se ha de establecer una cadena de toma de decisiones a la hora de procesar pedidos y mantener consistente el catálogo y la información comercial del mismo y cuyo componente logístico nunca debe ser despreciado.

Otra consideración digna de mención es la importancia de la publicidad y el marketing de un sistema de este tipo para que genere negocio, haciendo especial hincapié en la publicidad on-line. En el BOE se realizaron distintas campañas en medios convencionales como encartes en la propia edición del Boletín Oficial del Estado, o anuncios a página completa en la revista de MUFACE, pero las campañas que realmente han tenido más éxito han sido las de inclusión de banners (anuncios gráficos) y pop-ups, (anuncios emergentes) en la página web del organismo, http://www.boe.es, de forma que en el último diseño de esta página ya se han dejado espacios especiales reservados para este menester.

Es importante reseñar aquí el papel que han ejercido las tecnologías abiertas y el uso de software libre, en el hecho del control total por parte de la organización del proceso de desarrollo y del producto final, así como la reducción drástica de costes, que permiten considerar el proyecto como un éxito absoluto. Siguiendo esta filosofía, en estos momento se esta estudiando la posibilidad de poner a disposición del resto de la comunidad el software generado utilizando la licencia GPL de GNU.