

## i-bankeXpress

Un producto desarrollado y registrado por

**SOFICANA**

Internet Consulting

**i-bankeXpress** es una plataforma de aplicaciones bancarias basadas en Internet e Intranet, conformando una base de soluciones de software Web tanto para clientes como para uso interno del banco. En el caso de clientes el acceso se realiza a través de Internet, mientras que para el uso interno se aprovecha tanto Internet como la infraestructura de sucursales y filiales que componen la Intranet del banco.

**i-bankeXpress** -desarrollado desde cero con tecnología de punta, con la concepción de cumplir con requerimientos de aplicaciones de misión crítica- agrega nueva funcionalidad para el usuario, donde Internet e Intranet no sólo conforma una nueva interfaz para los sistemas existentes, sino también se provee de procesos *back-end* que le otorgan valor agregado - minimizando además el costo de modificar sistemas centrales.

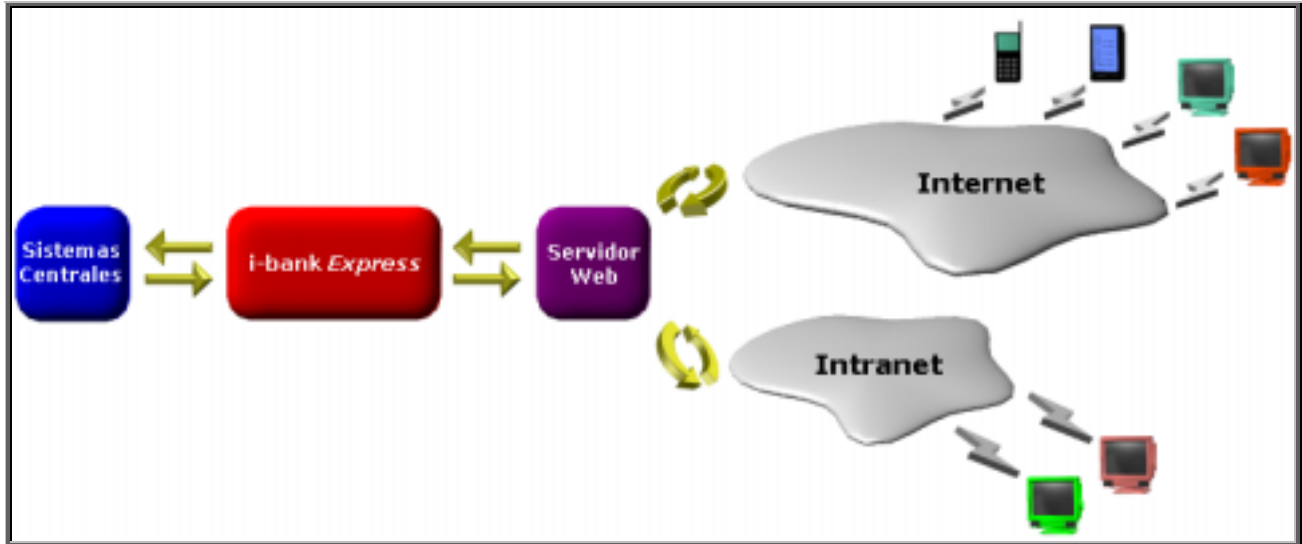
Con respecto a clientes, **i-bankeXpress** no sólo abarca todos los productos que un banco puede ofrecer utilizando la red, sino también genera valor agregado al potenciar nuevos servicios basados en esta tecnología. Internet no significa únicamente un canal de acceso adicional, enfocado en facilitar la operatoria actual. Nuevos productos y servicios pueden disponerse permitiendo agilizar, automatizar y programar consultas y transacciones, como así también la posibilidad de asesorar, motivar y concretar la inversión en nuevos productos.

Por otro lado, la implementación de sistemas en una Intranet compuesta por sucursales y filiales del banco, es un proceso que día a día traza con mayor nitidez la tendencia en el desarrollo de software del nuevo milenio. Internet, junto a las ventajas que ofrece el uso de esta tecnología, no sólo proporciona la posibilidad de crear nuevos servicios para clientes, sino también para agilizar y simplificar la operatoria bancaria.

Con respecto a la tecnología utilizada, se provee de un amplio abanico de alternativas, adecuándose a los estándares establecidos en cada banco, además de proporcionar así mayor migrabilidad.

Finalmente, todas las soluciones de software son presentadas dentro de un proyecto estándar listo para ser implementado. Tanto la funcionalidad como la tecnología se encuentran resueltas, como así también su planificación. Al estar divididas en capas bien definidas, las aplicaciones se encuentran preparadas para adecuarse distintos sistemas centrales –con varias alternativas en cada caso- previendo de esta forma una rápida puesta en marcha.

Esquema General de i-bankExpress

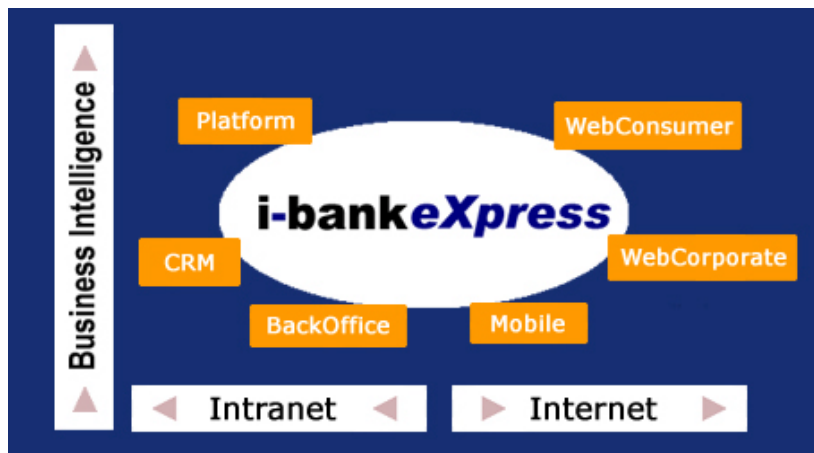


**Distintos accesos**

Además de acceder desde navegadores Web, el sistema provee la posibilidad de interactuar con dispositivos móviles a través de tecnología WAP y SMS, por ejemplo teléfonos celulares y palmtops. Utilizando una única lógica para todas las formas de acceso, la información se encuentra integrada, reflejando en línea las transacciones realizadas.

## Aplicaciones Web

**i-bankeXpress** se compone de las siguientes Aplicaciones Web.



### Clientes

**i-bankeXpress WebConsumer** Consultas y transacciones bancarias a través de Internet para Consumidores

**i-bankeXpress WebCorporate** Consultas y transacciones bancarias a través de Internet para Empresas

**i-bankeXpress Mobile** Consultas y transacciones bancarias a través de dispositivos móviles

### Banco

**i-bankeXpress CRM** Gestión de clientes y *Business Intelligence* a través de Internet

**i-bankeXpress Platform** Plataforma comercial integral basada en Intranet de sucursales

**i-bankeXpress BackOffice** Gestión de información operativa basada en Intranet de sucursales

## Tecnología

### Alternativas de Implementación

Existe un gran abanico de alternativas para la implementación de la aplicación. Siguiendo los estándares del mercado, el sistema **i-bankeXpress** ha sido desarrollado en su totalidad con tecnología Orientada a Objetos, disponible en dos versiones: Java y C++, tanto en plataformas UNIX como Windows NT/2000 y AS/400. Se utiliza JDBC en el acceso a la base de datos en el caso de clases Java, mientras que en C++ el acceso se realiza en forma nativa, a través de las APIs propias de la base de datos a utilizar. Las opciones de bases de datos son: Oracle, Sybase, SQLServer y acceso ODBC en C++, acceso JDBC en Java.

Dependiendo de los estándares, estrategias y requerimientos del sistema, el banco podrá elegir por una u otra opción.

También es importante señalar que al seguir un único criterio, el mismo servidor Web puede ser utilizado para todos los módulos de **i-bankeXpress**, incluyendo la funcionalidad WAP.

### Interacción con los Sistemas Centrales del Banco

#### *Acceso a Sistemas Centralizados*

Una forma común de implementación es la adecuación de **i-bankeXpress** a sistemas centralizados ya preparados para atender distintos tipos de acceso a los sistemas bancarios: un único módulo interactúa con cajeros automáticos, terminales de autoservicio, banca telefónica. En este caso, la aplicación se encuentra lista para adecuarse a las solicitudes y respuestas de distintos sistemas transaccionales, donde la capa de acceso a datos es resuelta internamente por una función de bajo nivel. Bajo este esquema, **i-bankeXpress** no hace uso de una base de datos propia para almacenar información operativa (salvo la necesaria para implementar funcionalidad de *Business Intelligence*, resuelta por la misma aplicación).

La capa de acceso a datos en general se adapta a los sistemas centrales a través de esquemas de mensajería como MQSeries y JMS, o a través de interfaces de programa provistas por el banco.

#### *Integración orientada a Bases de Datos*

La aplicación se encuentra lista para funcionar con una estructura de base de datos propia. Por lo tanto, configurando la replicación de información desde los sistemas centrales con una herramienta de software de base (en general provista por la misma base de datos), las consultas de **i-bankeXpress** ya se encuentran listas, logrando además buena performance a través de replications basadas en comunicaciones asincrónicas. El camino inverso, o sea las transacciones generadas desde la aplicación hacia los sistemas centrales se implementan dependiendo de la forma en que los sistemas del banco se encuentran preparados para interactuar con sistemas departamentales, tanto en línea como fuera de línea.

## Arquitecturas

A continuación se enumeran las opciones de la arquitectura para la implementación del sistema:

### *Sistemas Operativos*

- Sun Solaris
- HP-UX
- Linux
- Windows NT/2000
- IBM AIX
- IBM AS/400

### *Bases de Datos*

- Oracle
- Sybase
- Microsoft SQLServer
- IBM DB/2
- ODBC
- JDBC

### *Servidores Web*

- Microsoft Internet Information Server
- Sun/Netscape iPlanet
- Apache Web Server
- IBM Websphere

## Capas de Software

Tanto nuestros productos como servicios siguen una metodología de desarrollo estructurada -basada en clases de objetos- que nos permite, por un lado, agilizar el proceso de desarrollo mediante la reutilización de componentes, y por el otro obtener productos de calidad. En el caso de **i-bankeXpress**, el desarrollo en capas delimita en forma bien definida los subsistemas a implementar, principalmente la diferenciación entre contenido y presentación. De esta manera, la aplicación se encuentra preparada tanto para browsers tradicionales como para dispositivos móviles (teléfonos celulares y *handheld*), habiendo desarrollado una sola capa de contenido común para todas las capas de presentación.



### Dispositivos Móviles

**i-bankeXpress** cuenta con un módulo **i-bankeXpress Mobile** que utiliza tecnología WAP (Wireless Application Protocol) junto con WML (Wireless Markup Language) para atender requerimientos iniciados desde teléfonos celulares y palmtops. El mismo servidor Web atiende todos los tipos de acceso, sin ser necesaria la instalación o implementación de software de base o hardware adicional.

## Seguridad

Al tratarse de una aplicación financiera, se ha hecho énfasis en resolver aspectos de seguridad en forma exhaustiva. Estos aspectos se encuentran ligados a la arquitectura del sistema, siendo implementados a nivel sistema operativo, red y aplicación. La estructura de seguridad se compone por una serie de barreras que funcionan en forma independiente, cada una de las cuales agrega una limitación adicional restringiendo la vulnerabilidad del sistema.

Los objetivos propuestos para cumplir con el esquema de seguridad son los siguientes:

1. Tener un entorno seguro entre el servidor y el *browser*, preservando así la confidencialidad de su información.
2. Identificar al usuario en su ingreso al sistema, transmitiendo el par usuario/contraseña en forma encriptada.
3. Evitar, dentro de lo posible, que el usuario de la aplicación analice el contenido de las páginas HTML, WML y las direcciones URL, minimizando así el riesgo que implica ingresar al sistema con un cliente para operar con otro.
4. Eliminar la posibilidad del ingreso de requerimientos a través del armado de páginas HTML o direcciones URL externas a la aplicación.

### Seguridad a nivel Sistema Operativo

#### Validación de Contraseña del usuario

Al ingresar a la página del sistema, la aplicación solicita del su identificación, junto con la contraseña. Ya fue iniciada una sesión SSL, por lo tanto la contraseña viaja encriptada.

#### Inhabilitación de acceso a otros recursos del servidor Web

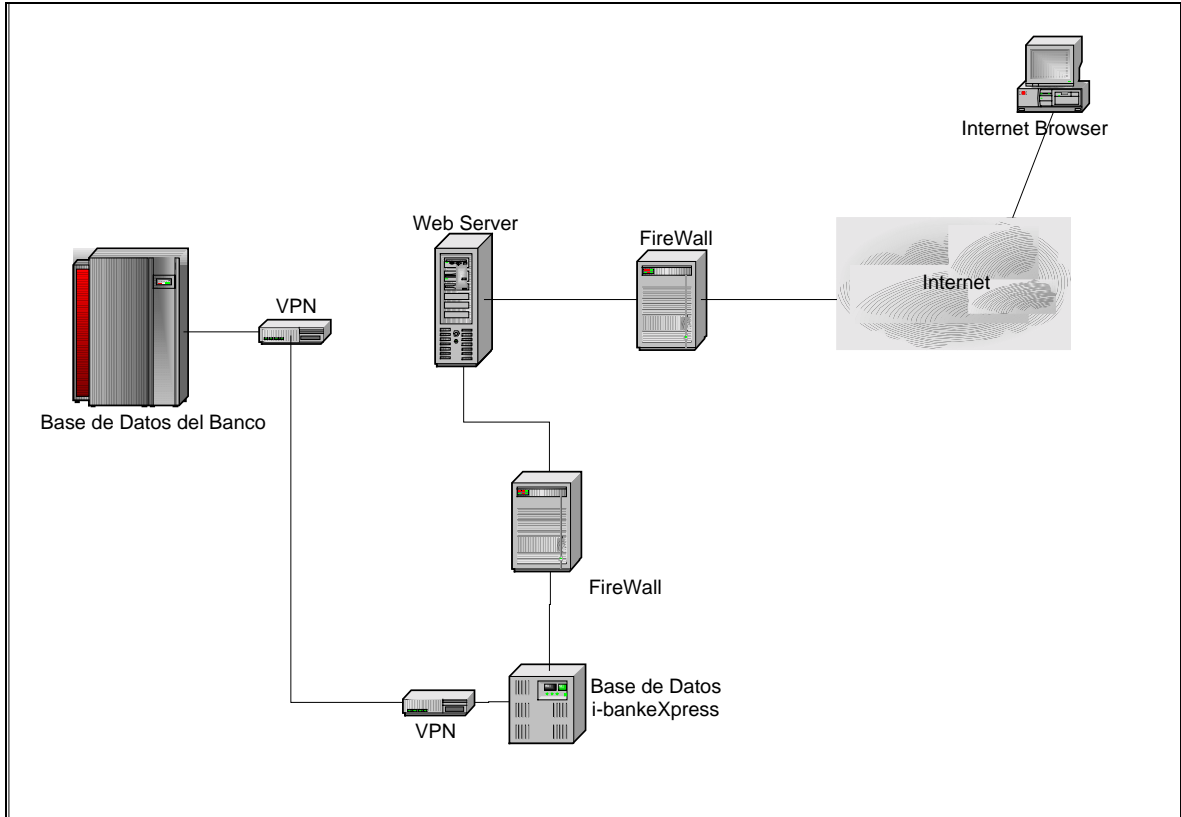
A través de la configuración del sistema operativo, se restringe el acceso a todos los recursos que no deben estar habilitados a usuarios de la aplicación.

### Seguridad a nivel Red

Existe una gran variedad de alternativas con respecto a la implementación de esquemas de seguridad de red. Estas alternativas dependen principalmente de los estándares definidos por el banco con respecto a arquitecturas de sistemas y de la estrategia que optó con respecto al acceso de aplicaciones Web por parte de los clientes. Si el banco aún no adoptó una estrategia en este sentido, ésta puede ser definida en conjunto con el esquema de seguridad de **i-bankeXpress**.

Es importante destacar que las aplicaciones **i-bankeXpress** e **i-bankeXpress Mobile** en particular son independientes al esquema de seguridad de red con el que cuenta o contará el banco.

Una opción estándar con respecto a la implementación de seguridad es la que se describe en la siguiente figura:



En este caso, se cuenta con una configuración de dos firewalls y un VPN para acceder a la base de datos del banco. Los firewalls filtran el acceso a la aplicación y a la base de datos respectivamente. Entre la base de datos de la aplicación y los sistemas centrales del banco es utiliza un VPN (Virtual Private Network) creando una relación de confianza entre las mismas con una conexión virtual punto a punto implementando encriptación y autenticación según los estándares IPSEC/IKE.

SSL

Permite resolver la identificación del usuario, la autenticidad de la información y el encriptado del vínculo entre el browser y la aplicación. Si la certificación la realiza el mismo banco, se implementa con Netscape Enterprise Server o Microsoft Certificate Server, según el servidor Web utilizado. De todas formas, se recomienda que la certificación la realice una entidad externa autorizada.

## Seguridad a nivel aplicación

### Encriptado de datos sensitivos en POST, GET y direcciones URL

Los datos sensitivos, por ejemplo números de cuenta, pueden encontrarse dentro de variables de memoria en páginas con código HTML, WML, Javascript o WMLScript. Si bien el usuario de la aplicación visualiza en pantalla la información con la que opera, las variables de POST y GET, como así también el Query List del URL se encuentra encriptado.

### Volver a leer/validar con cada requerimiento

Si bien existe en la aplicación un flujo de pantallas y se utilizan cookies para mantener la información propia de la sesión, con cada requerimiento de página el servidor web vuelve a realizar nuevamente todas las lecturas y validaciones realizadas en pasos anteriores.

### No permitir saltar la página de inicio de sesión

Si el usuario aun no fue identificado en su ingreso, al no haber iniciado una sesión todo requerimiento de URL es rechazado.

### Rechazar ingresos de usuarios en forma simultánea

Si un usuario intenta ingresar al sistema desde más de un acceso, el requerimiento de inicio de sesión no es aceptado, indicándole que ya se encuentra dentro del sistema.

### Timeout de sesión

Al pasar n minutos sin operar (esto es, sin realizar ningún requerimiento al servidor), el usuario no puede continuar operando, obligándolo a volver a ingresar al sistema.

### Mensajes vagos

Tanto en el ingreso de usuario/contraseña como en el intento de acceder a una dirección IP con un URL por fuera de la aplicación, los mensajes retornados por la aplicación no declaran en ningún momento el motivo del error.

### Control de seguridad biométrica - reconocimiento de la huella dactilar (opcional)

En el ingreso al sistema, el usuario debe tocar con su dedo un dispositivo conectado a la PC donde corre el Browser.

### Dispositivo físico para puerto USB (opcional)

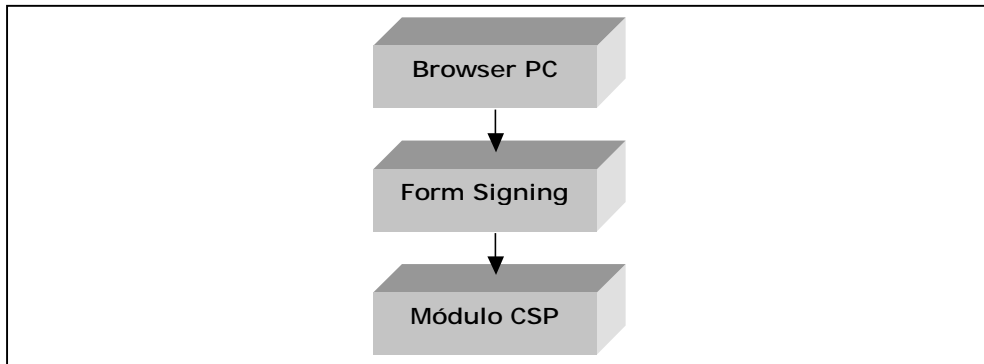
Para poder ingresar al sistema, el usuario debe insertar un dispositivo físico en el puerto USB de la PC donde corre el Browser.

### Secure-ID (opcional)

Además del ingreso de usuario/contraseña, el cliente debe ingresar un número que aparece en un dispositivo físico en forma de tarjeta de crédito. Este número número varía cada n minutos y sólo es conocido por el servidor Web.

Form Signing

Form Signing es una tecnología que implica que el usuario firme digitalmente cada transacción que realiza, asegurando el banco legalmente su autenticidad. Esto se logra a través del desarrollo de un módulo CSP (Cryptographic Service Provider) bajo Microsoft Windows (donde reside el *browser*), tomando la contraseña privada del cliente para firmar digitalmente los datos de la transacción. Estos datos son tomados en el servidor, por un lado para comprobar la autenticidad del requerimiento, mientras que por otro lado esta firma se almacena en el log de base de datos para posteriores verificaciones.



## Más Información

Acceda a [www.sofiana.com/pdfs/sofianaibewebconsumer.pdf](http://www.sofiana.com/pdfs/sofianaibewebconsumer.pdf) para obtener información sobre **i-bankeXpress** WebConsumer

Acceda a [www.sofiana.com/pdfs/sofianaibewebcorporate.pdf](http://www.sofiana.com/pdfs/sofianaibewebcorporate.pdf) para obtener información sobre **i-bankeXpress** WebCorporate

Acceda a [www.sofiana.com/pdfs/sofianaibemobile.pdf](http://www.sofiana.com/pdfs/sofianaibemobile.pdf) para obtener información sobre **i-bankeXpress** Mobile

Para obtener información adicional sobre otros productos y servicios, envíe un e-mail a [info@sofiana.com](mailto:info@sofiana.com), visítenos en [www.sofiana.com](http://www.sofiana.com) o póngase en contacto con nuestra área comercial llamando telefónicamente al ( 54-11 ) 4827-4333 en Buenos Aires, Argentina.