

INFORME TÉCNICO PREVIO DE EVALUACIÓN DE SOFTWARE

“ADQUISICIÓN E IMPLEMENTACIÓN DEL SISTEMA DE ATENCIÓN DE TRNSACCIONES POR INTERNET”

1. NOMBRE DEL ÁREA

Departamento de Informática

2. RESPONSABLES DE LA EVALUACION

Oscar López López Jefe de la Sección de Soporte en TI
Henry Paredes Ojeda, Jefe de la División de Desarrollo de TI

3. FECHA

San Isidro, 13 de Junio del 2006

4. JUSTIFICACIÓN

El actual sistema que utiliza el Banco para atender las transacciones de sus Clientes por Internet solo tiene un limitado conjunto de transacciones, las que operan en forma restringida ya que operan mediante una “Agencia Virtual” entre las 9:00 am y las 6:00 pm no estando disponibles para operar en 7x24.

Nuestro nivel de atención por este medio ha crecido y requiere ser fortalecido, además de reestructurado para aprovechar la infraestructura que el convenio con el proveedor de acceso a Internet ahora nos proporciona la capacidad de operar en un esquema de alta disponibilidad con elementos para el balanceo de carga y tener doble acceso a esa red. Por otro lado, la solución deberá cumplir estándares SOA (Service Oriented Architecture) y los de J2EE.

Este Ssistema forma parte del Proyecto del Sistema de Atención a Clientes (SAC) el cual se orienta hacia conseguir el objetivo estratégico que es el de: “Mejorar la atención de nuestros Clientes brindándoles Servicios de Calidad”, el cual permitirá mejorar la Atención del Cliente y mejorar la Competitividad del Banco, ambos con el propósito de mejorar la imagen Institucional por lo siguiente:

- Contar con herramientas modernas, flexibles y parametrizables que nos permitan mejorar el tiempo de respuesta a las necesidades del negocio por nuevos productos y/o servicios para este canal de atención.
- Incrementar el número de transacciones que se ejecutan por este medio.
- Se espera darle a los clientes una mayor agilidad en la atención de los servicios por medios electrónicos de autoservicio con una mayor disponibilidad 7x24.
- Ofrecerles medios de atención con soluciones tecnológicas de vanguardia.
- Reducir las colas en las Agencias al ampliar la cobertura de servicios incluyendo más transacciones.

Por otro lado, se mejorará la competitividad del banco al:

- Atender operaciones por Internet las 24 horas del día, los 7 días de la semana, ampliando las opciones que tiene el cliente para acceder al Banco.
- Ofrecer medios de atención nuevos y renovados con uso de tecnología de punta.

Requerimiento:

Se requiere adquirir una solución basada en tecnología Web que cumpla las exigencias definidas en el **Anexo A**, que permita la atención de transacciones a través de Internet definidas en el **Anexo B** operando en un esquema de alta disponibilidad y que cumpla los Controles de Seguridad señalados en el **Anexo C**

La solución debe considerar las licencias de software, así como, el servicio de personalización e implantación de la misma.

5. ALTERNATIVAS

Existen muchas soluciones tecnológicas capaces de atender lo solicitado entre ellas podemos mencionar:

- Excelsys producto chileno de gran difusión en entidades financieras de la región
- eBanking de Fidelity National Information Services, Inc.
- Sun One solución de SUN Microsystems con Open Net Environment
- Bea Systems con su solución BEA WebLogic
- IBM con la línea de productos Websphere
- Macosa con su producto COBIS Internet/Kiosk de fabricación ecuatoriana con alguna difusión regional

Todas ellas satisfacen las Especificaciones Técnicas Mínimas preparadas para este proceso.

6. ANÁLISIS COMPARATIVO DE COSTOS

Durante el proceso de determinación del precio referencial se hizo convocatoria para cotización a diferentes empresas, respondiendo las compañías J Evans y Asociados S. A. C. y Solucerv Perú S. A. C con las soluciones COBIS y Excelsys.

De este análisis se pudo determinar como precio referencial S/. 918,075.00 (Novecientos dieciocho mil, setenta y cinco y 00/100 nuevos soles) incluido IGV.

7. CONCLUSIONES

Las áreas operativas del Banco requieren ser atendidas con la celeridad que la globalización y la modernidad exige; que serán resueltas con los entregables de la solución requerida.

Nuestra limitada presencia recortada a un horario de lunes a viernes y el reducido número de alternativas que se le ofrece al cliente será mejorado y ampliado; por lo que se espera se incremente el número de transacciones que los clientes ejecutan por este medio.

El banco requiere ampliar su cobertura transaccional por el canal de Internet; no solo en cuanto al número de transacciones, si no también en cuanto a la disponibilidad en el esquema de altamente disponible que se exige. Además de operar en modo 7x24.

Por otro lado, en concordancia con los objetivos institucionales se espera darle a los clientes una mayor agilidad en la atención de los servicios por medios de atención modernos, seguros y disponibles con soluciones tecnológicas de vanguardia

Otro beneficio esperado es la reducción de las colas en las Agencias, mejorando la competitividad del banco

8. FIRMAS

Responsables de la Evaluación	Firmas
Oscar López López	
Henry Paredes Ojeda	

ANEXO A

EXIGENCIAS TECNICAS MINIMAS

Requerimiento / Funcionalidad
REQUERIMIENTOS GENERALES
La solución propuesta deberá considerar todas las licencias de software que ésta involucre para los ambientes de desarrollo, certificación y producción, así como el servicio de personalización e implementación de la solución en dichos ambientes.
El postor deberá considerar en su propuesta la entrega de todos los programas fuentes que se hayan personalizados para el Banco de la Nación, asimismo pondrá a disposición del Banco todos los programas fuentes de la solución propuesta, para que en el caso de que la empresa desaparezca, esto se regularice mediante un Contrato de Plica, que consiste en nombrar a una entidad financiera, que ejecute el traslado de los productos a favor del Banco.
La solución deberá incluir una herramienta de alta productividad para el desarrollo y mantenimiento de las transacciones, minimizando la codificación de lenguajes de programación mediante una estructura simple, modular y debidamente documentada.
El Personal Técnico del Banco responsable del actual Sistema de Transacciones por Internet, prestarán su colaboración al ganador de la buena pro, sin que esto implique de ninguna manera participación directa en las fases de programación.
El ganador de la buena pro deberá transmitir los conocimientos necesarios al personal del Banco para el posterior mantenimiento y soporte de la solución.
REQUERIMIENTOS DE ARQUITECTURA
La solución debe estar basada en tecnología Web, cumpliendo estándares J2EE y cumplir los criterios de la Arquitectura Orientada al Servicio (SOA).
La solución deberá permitir la construcción de transacciones a partir de un generador de código de alto nivel ¹ , que permita reducir las labores de programación (paramétrico).
El postor deberá garantizar que la solución propuesta no degrade su rendimiento (tiempo de respuesta) ² ante un incremento del número de operaciones en el plazo que se mantenga vigente la garantía.
La solución ofertada debe cumplir con la arquitectura que se muestra en la Ilustración 2 “Arquitectura del Canal Internet”
Por exigencias de la arquitectura, las necesidades del esquema de alta disponibilidad y por el hardware disponible, se tendrá las siguientes consideraciones: <ul style="list-style-type: none">• El acceso redundante a Internet estará disponible en nuestro local de contingencia.• Los equipos de Load Balancing y Reverse Proxy serán proporcionados por el Banco• Los equipos para la residencia de los servidores Web y Servidor de Aplicaciones serán proporcionados por el Banco³

¹ Un generador de código de alto nivel se refiere a la funcionalidad de la solución propuesta o producto adicional para construir las interfases de usuario de las transacciones reduciendo las labores de programación.

² Se estima que este Canal se iniciará con un promedio aproximado de 2 millones de operaciones en el primer año, considerándose un incremento estimado de 12% anual.

<ul style="list-style-type: none"> • La solución debe tener la capacidad de ejecutarse en un servidor virtualizado con administración de recursos que ofrece nuestra consolidación de servidores el cual dispone de licenciamiento VMWare SX para tal fin.
<p>El postor deberá considerar en su propuesta todos los elementos necesarios (hardware y software) que aseguren la correcta implementación y operación de la solución, por lo que se sugiere se tenga muy en cuenta los equipos y software que el Banco dispone, así como los estándares que soporta cada producto, su versión, la versión del estándar y el protocolo.</p>
<p>Sobre el Gateway, debe ser definido por el proveedor y considerar que entre el mainframe y éste se establecerá una sesión HTTP transportando mensajes SOAP, tanto para Inbound como Outbound. Para este fin puede incluirse productos que dispone el Banco</p>
<p>Sobre el Gateway, debe interactuar contra el servidor de aplicaciones a través del HUB de integración. El postor, de considerarlo conveniente, puede prescindir del uso del Gateway</p>
<p>El servidor Web debe ser de alta disponibilidad operando en los equipos destinados por el Banco para implementar la solución.</p>
<p>El Banco viene usando a la fecha un certificado digital de Verisign para ofrecer seguridad en las transacciones realizadas a través de su pagina Web, si la solución exige la inclusión de certificados adicionales estos deben incluirse en la propuesta, los mismos que deberán ser emitidos por entidad certificadora internacional a nombre del Banco de la Nación.</p>
<p>El Banco dispone de Windows 2003 Enterprise Server como Sistema Operativo, de requerirse otro Sistema Operativo el postor debe proveer el licenciamiento respectivo.</p>
<p>La solución debe estar basada en arquitectura Internet.</p>
<p>Debe permitir a los clientes la utilización de un browser estándar como medio de navegación, tales como: Internet Explorer, Mozilla, Netscape, FireFox, etc.</p>
<p>La solución debe ser capaz de generar estadísticas de consumo, frecuencias, tiempo de respuesta, etc., que permitan tener una visión clara del comportamiento de los servicios a través del tiempo.</p>
<p>Debe poder trabajar con los servidores Web mas conocidos, como: Apache Web Server, Microsoft Internet Information Server, SunOne (iPlanet) Web Server entre otros.</p>
<p>Debe poder ser configurado en cluster de software (independiente del sistema operativo utilizado) para balanceo de carga y alta disponibilidad. Es necesario se ejecute en cluster de Sistema Operativo.</p>
<p>Debe ser capaz de proveer un failover automático (mantener sesión) y operación continua en caso de falla de algún componente de hardware o software.</p>
<p>Debe contar con facilidades para poder definir reglas y pesos a los diferentes nodos dentro del cluster logrando así crear un esquema de balanceo que esté de acuerdo con la capacidad real de cada servidor.</p>
<p>Debe permitir realizar de forma secuencial actualizaciones de una aplicación en un cluster de manera tal de que se vaya actualizando en los nodos uno por uno sin detener la aplicación en el cluster y sin afectar el servicio a los usuarios</p>
<p>Debe incluir herramientas para el respaldo y restauración de la configuración del servidor de tal manera de poder restaurar toda la configuración del servidor en caso de que el</p>

³ El servidor Web: Maquinas IBM Blade Intel Xeon EMT 64 de 2 procesadores 3.6 Ghz, 8 Gb RAM, 2 discos de 73 Gb. El Servidor de Aplicaciones: IBM Intel Xeon de 4 procesadores de 3 Ghz, 10 Gb en RAM, 300 GB en Disco

hardware falle.
SERVIDOR DE APLICACIONES
Cumplir estándares de seguridad LDAP e incluir el soporte necesario para integrarse con el Sistema de Seguridad Corporativa que el Banco adopte para el manejo de identidades y control de accesos.
Ser escalable y que tenga la capacidad de crecer migrando de plataforma tecnológica o sobre la misma tecnología.
Operar en un esquema de alta disponibilidad a través del uso de servidores montados en dos locales y conectados por enlaces de fibra óptica, con transporte Gb Ethernet y Fiber Channel para la nube SAN que le dará acceso de ambos extremos al disco externo que es un IBM ESS 800 (Shark), haciendo uso de los Switch IBM 2109.
Tener la capacidad de interactuar a través de interfaces con otros canales financieros, ejemplo: SWIFT, VISA, etc.
Tener en cuenta que el Banco dispone de software para la creación y despliegue de aplicaciones orientadas al servicio a través del middleware.
La administración del motor de aplicaciones debe estar basada en roles y perfiles de usuarios.
Debe permitir realizar actualizaciones parciales de las aplicaciones. De tal manera de poder realizar una actualización de un archivo o grupo de archivos desde una la consola de administración y que se distribuyan automáticamente a todos los nodos de un cluster sin necesidad de detener la aplicación.
Debe incluir herramientas para el respaldo y restauración de la configuración del servidor de tal manera de poder restaurar toda la configuración del servidor en caso de que el hardware falle.
Debe permitir que las aplicaciones se auto instalen al ser copiadas a un directorio del sistema de archivos.
Debe permitir la programación de ejecución de tareas en batch.
Permitir el desarrollo único para los distintos canales de distribución existentes en el mercado Internet y dispositivos Móviles.
Detectar el tipo de dispositivo solicitante de un requerimiento al Servidor de tal forma que el envío de la información resultante se ajuste a las características de dicho dispositivo.
Ser parametrizable.
Interactuar en Web Services contra el Servidor Web, haciendo uso de WSDL, XML y otros propios del estándar.
Ser concebida bajo criterios modernos haciendo uso de patrones, de negocio, runtime, comunicaciones, esquemas y otros, cuya concepción será elaborada en la etapa de diseño y aprobada por el equipo técnico del banco.
REQUERIMIENTOS DE COMUNICACIÓN CON EL COMPUTADOR CENTRAL
Las transacciones de interfaz de usuario especificadas en el Anexo A que desarrolle el ganador de la buena pro, debe enlazarse con su correspondiente transacción existente en el motor transaccional TOLD II, el cual recibirá un mensaje de comunicación (trama) y retornará otro como respuesta de acuerdo a los diseños establecidos, de tal manera que asegure la integridad de procesamiento de la transacción.
El ganador de la buena pro, deberá incluir en su propuesta el desarrollo de una Interfase

CICS que será invocada por las Aplicaciones Legacy, la cual interactuará contra el Gateway o el HUB vía mensajes SOAP en HTTP.
REQUERIMIENTOS DE SEGURIDAD
Considerar todos los controles de seguridad del actual Sistema de Atención de Transacciones por Internet, debiendo interactuar con el modelo de seguridad del CORE. (Anexo C)
Considerar la transacción que permita la generación de la clave por Internet de los tarjeta habientes, según procedimientos descritos en el Anexo C.
La autenticación del tarjeta habiente, de la tarjeta, de la operación, así como los procedimientos y mecanismos de seguridad de la solución, deberá realizarse de acuerdo a lo señalado en el Anexo C, por razones de confidencialidad, de requerirse mayor información, ésta será proporcionado al ganador de la buena pro.
Permitir el uso de certificados digitales a través del protocolo de seguridad Secure Socket Layer (SSL de 128 bits) entre el servidor y el cliente (browser). Estos certificados digitales deben cumplir con el estándar X.509v3 y del tipo VeriSign Inc., Identidata Holding and Alagraf, ID Certify, etc.
Tener soporte para servidores LDAP que le permita integrarse a nuestra solución de acceso corporativo. Integrándose a los productos: Tivoli Identity Manager y Tivoli Access Manager.
La solución ofrecerá dos niveles de seguridad: <ul style="list-style-type: none"> ○ El primer nivel relacionado al acceso a Banca por Internet únicamente para operaciones de consulta, hará uso de la asociación Número de Tarjeta y Pin de la Tarjeta (cuatro dígitos). El ingreso del Pin debe ser por teclado virtual. ○ El segundo nivel guarda relación con la autorización para efectuar operaciones con cargo en cuentas, para lo cual el sistema deberá validar la asociación Número de Tarjeta y Pin de la Tarjeta (seis dígitos). El ingreso del Pin debe ser por teclado virtual.
REQUERIMIENTOS DE FUNCIONALIDAD
Tener total compatibilidad con cualquier dispositivo con acceso a Internet.
Tener la interfase intuitiva y permitir una fácil navegación.
Contemplar un Módulo para un Usuario Administrador que permita la definición, personalización y modificación de parámetros de prevalidación y diseño relacionados al canal Internet. Ejemplo: horarios de atención, interrupción de un determinado servicio, montos máximos y mínimos por transacciones, inhabilitación de un determinado tipo de transacción, tipos de moneda aceptadas, tipos de cuentas disponibles para el procesamiento de una determinada transacción, etc.
Soportar operaciones multi-moneda y multi-idioma ⁴ .
Estar alineada de conformidad a las normas Unicode.
Tener diferentes plantillas de presentación por fecha, las que deben ser administradas con

⁴ Se deben considerar dos criterios para el concepto de multi-idioma. El primero, se refiere a la capacidad de reconocer el origen del usuario remoto y dar el soporte necesario para que vea la página Web sin problemas relacionados con el idioma. El segundo criterio se refiere a la capacidad de que el contenido de la página pueda leerse en uno de los siguientes idiomas: español e inglés, con relación al criterio multimonedado, se refiere a la capacidad de poder efectuar operaciones en otras monedas diferentes al sol peruano.

las promociones correspondientes.
Tener presentaciones personalizadas por tipo de cliente.
Permitir establecer límites por tipo de operaciones, montos, según lo establezca el Banco (por ejemplo: transferencias y telegiros)
La solución deberá permitir realizar operaciones con cargo en las cuentas que el cliente elija y se encuentren relacionadas al número de la tarjeta ⁵ con la cual opera con el Banco.
Contemplar los requerimientos de registro y control de operaciones comprendidas dentro de las normas de Lavado de Dinero.
Ser capaz de generar reportes estadísticos y manejar información histórica que permitan tener control de las transacciones que se procesan por este canal.
Permitir hacer consultas y generar reportes estadísticos diarios y mensuales respecto del número de operaciones por servicio, por tipo de transacción, por hora, por fecha, por rangos de importe, estado de las transacciones (fallidas, culminadas satisfactoriamente, sospechosas, etc.), usabilidad (frecuencia de uso de una determinada transacción), etc.
Permitir hacer consultas de afiliaciones de servicios, generación de clave, cambio de clave y desafiliación de clave y servicios.
Considerar que los trabajos de diseño y presentación del Sitio Web por parte del ganador de la buena pro, debe realizarse en coordinación con el personal designado por el Banco, siguiendo los estándares de diseño.
REQUERIMIENTOS DE INTERFAZ DE DESARROLLO
Utilizar tecnologías actuales como SOA (Service Oriented Architecture), Web Services, XML (Extended Markup Language), etc.
Poder desarrollar componentes basados sobre una arquitectura de capas, independizando de esta forma la capa de lógica de presentación, de lógica del negocio y de las fuentes de datos.
Controlar a través de un registro la solicitud de un programa para su revisión o modificación (check-out) de manera que ningún otro desarrollador pueda modificarlo hasta que libere el primero (check-in).
Tener características de ayuda como: verificación de errores de tipeo, intellisense, acceso instantáneo local y on line.
Permitir búsquedas en el código en la página actual o en todo el proyecto.
Visualizar el proyecto de acuerdo al perfil del desarrollador, lenguaje específico o aplicación.
Tener herramienta(s) de depuración de código.
PERSONALIZACIÓN E IMPLEMENTACIÓN DE LA SOLUCIÓN
La solución propuesta deberá considerar la personalización de las transacciones descritas en el <i>Anexo A</i> Asimismo, el postor debe considerar en su propuesta el desarrollo de 10 transacciones adicionales, debiendo el Banco definir dichas transacciones y comunicar al postor ganador de la buena pro, hasta un (01) mes antes del término del proyecto.
Durante la ejecución del proyecto, previo al inicio del desarrollo de una determinada transacción, de requerirlo el Banco, podrá solicitar su cambio o reemplazo. Si durante la ejecución del proyecto surgieran modificaciones por necesidades del negocio en cualquier transacción ya personalizada, el postor deberá realizar su correspondiente modificación

⁵ Deberá tenerse en cuenta que una tarjeta podrá estar relacionada a más de una cuenta, y a su vez, una cuenta podrá estar relacionada con más de una tarjeta (tarjetas adicionales).

hasta un (01) mes antes del término del proyecto.
La solución propuesta deberá contemplar la necesidad de poder seguir operando con la solución actual y paralelamente se pueda implementar la nueva solución. Por otro lado, el postor deberá indicar los niveles o puntos de riesgos que se requiere cubrir para el éxito del proyecto, como también definir todas las actividades necesarias para asegurar la calidad de la solución.
Para el proceso de implementación de la solución definitiva, el postor deberá considerar la realización de un piloto controlado cuya ejecución deberá ser coordinado entre ambas partes y cuyo resultado condicionará el pase a producción de la solución, Previo a dicha actividad la solución deberá pasar por el ambiente de certificación.
El postor deberá presentar el plan de implementación, el mismo que deberá ser revisado y aprobado por el Banco. La implementación no deberá afectar la operatividad de la actual solución.

ANEXO B

Tabla 11 Transacciones Canal de Internet

CANAL INTERNET	
N°	TRANSACCIONES POR SERVICIOS 1/
SERVICIOS : AHORROS	
XXXX TARJETAS MULTIRED Y MULTIRED GLOBAL DEBITO	
1	Bloqueo de Tarjeta
XXXX CONSULTAS Y MOVIMIENTOS	
2	Consulta Código CCI MN
3	Consulta Código CCI ME
4	Consulta de Saldo MN
5	Consulta de Saldo ME
6	Consulta Ultimos Movimientos MN
7	Consulta Ultimos Movimientos ME
8	Consulta Anual ITF MN
9	Consulta Anual ITF ME
SERVICIO : CUENTAS CORRIENTES	
XXXX CONSULTAS Y MOVIMIENTOS	
10	Consulta Código CCI MN
11	Consulta Código CCI ME
12	Consulta de Saldo MN
13	Consulta de Movimientos MN
14	Consulta de Saldo ME
15	Consulta de Movimientos ME
16	Consulta Anual ITF MN
17	Consulta Anual ITF ME
SERVICIO : TRANSFERENCIAS 2/	
XXXX TRANSFERENCIAS MISMO BANCO	
18	De Cta. Ahorros MN A Cta. Ahorros MN
19	De Cta. Ahorros MN A Cta. Ahorros ME
20	De Cta. Ahorros MN A Cta. Cte. MN
21	De Cta. Ahorros MN A Cta. Cte. ME
22	De Cta. Ahorros ME A Cta. Ahorros ME
23	De Cta. Ahorros ME A Cta. Ahorros MN
24	De Cta. Ahorros ME A Cta. Cte. MN
25	De Cta. Ahorros ME A Cta. Cte. ME
26	De Cta. Cte. MN A Cta. Cte. MN
27	De Cta. Cte. MN A Cta. Cte. ME
28	De Cta. Cte. MN A Cta. Ahorros MN
29	De Cta. Cte. MN A Cta. Ahorros ME
30	De Cta. Cte. ME A Cta. Cte. ME
31	De Cta. Cte. ME A Cta. Cte. MN

32	De Cta. Cte. ME A Cta. Ahorros MN
33	De Cta. Cte. ME A Cta. Ahorros ME
34	De Cta. CTS MN A Cta. Ahorros. MN
35	De Cta. CTS ME A Cta. Ahorros. MN
	XXXX TRANSFERENCIAS INTERBANCARIAS
36	De Cta. Ahorros MN A O/B en MN
37	De Cta. Ahorros MN A O/B en ME
38	De Cta. Ahorros ME A O/B en MN
39	De Cta. Ahorros ME A O/B en ME
40	De Cta. Cte. MN A O/B en MN
41	De Cta. Cte. MN A O/B en ME
42	De Cta. Cte. ME A O/B en MN
43	De Cta. Cte. ME A O/B en ME
	SERVICIO : PAGO A CUENTA DE TARJETAS DE CREDITO
	XXXX TRANSFERENCIA POR PAGO A CUENTA DE TARJETAS DE CREDITO
44	Pago a Cta Tarjetas de Crédito O/B MN con Cargo Cta Ahorros MN
45	Pago a Cta Tarjetas de Crédito O/B MN con Cargo Cta Ahorros ME
46	Pago a Cta Tarjetas de Crédito O/B ME con Cargo Cta Ahorros MN
47	Pago a Cta Tarjetas de Crédito O/B ME con Cargo Cta Ahorros ME
	SERVICIO : COMPENSACION POR TIEMPO DE SERVICIO - CTS
	XXXX CONSULTAS Y MOVIMIENTOS
48	Consulta de Saldos MN Y ME
49	Consulta de Movimientos MN y ME
	SERVICIO : PRÉSTAMOS MULTIRED
	XXXX CONSULTAS
50	Consulta de Préstamos
51	Consulta Calendario de Pagos
	XXXX PAGO DE PRESTAMOS
52	Pago de Cuotas Vencidas y una cuota adelantada o Totalidad del Préstamo Con Cargo en Cuenta de Ahorros MN
	SERVICIO : TELEGIROS
	XXXX EMISION
53	Con Cargo en Cuenta Ahorros MN
54	Con Cargo en Cuenta Ahorros ME
	SERVICIO : CORRESPONSALÍA
	XXXX PAGO DE SERVICIOS
	CONSULTA Y PAGO DE AGUA
55	Agua con Cargo en Cuenta Ahorros MN
	CONSULTA Y PAGO DE TELEFONIA EN MN Y ME 3/
56	Servicios de Telefonía Con Cargo en Cuenta de Ahorros MN
57	Servicios de Telefonía Con Cargo en Cuenta de Ahorros ME
58	Servicios de Telefonía Con Cargo en Cuenta Corriente MN
59	Servicios de Telefonía Con Cargo en Cuenta Corriente ME
60	Pago de Telefonía – Claro Con Cargo en Cuenta Ahorros MN y ME
	CONSULTA Y PAGO DE CUPONES
61	Pago de Cupones MN y ME Con Cargo en Cuenta Ahorros MN y ME

SERVICIO : RECAUDACIÓN TRIBUTOS	
	XXXX PAGOS SUNAT
62	PDT con Cargo en Cuenta Corriente MN
63	PDT con Cargo en Cuenta Corriente ME
64	PDT con Cargo en Cuenta Corriente MN – Deduciones
	XXXX PAGOS ENTIDADES PUBLICAS 4/
65	Pago de Tasas con Cargo en Cuenta Ahorros MN
66	Pago de Tasas con Cargo en Cuenta Ahorros ME
	1/ Al finalizar alguna transacción el cliente debe de tener la facilidad de poder imprimir una constancia de conformidad de la operación, guardarla en disco o enviarla por correo electrónico.
	2/ Los montos máximos por transferencias a cuentas propias y a terceros y los horarios de acreditación serán fijados de acuerdo a las políticas internas que establezca el BN. Las transacciones deben poder fijar este tipo de restricciones.
	3/ Los servicios de telefonía deben de cubrir todos los servicios de cobranza que actualmente realiza el Banco de acuerdo a los convenios que maneja (celular, cable, Internet, teléfono fijo, líneas control, etc.)
	4/ El Postor deberá considerar el desarrollo e implementación de las actuales transacciones por Internet con las que cuenta el Banco. Asimismo, deberá considerar que para el pago de tasas se tienen 10 tipos de formatos diferentes, los cuales guardan relación con diferentes grupos de tributos.

Servicios Complementarios del Canal Internet	
1	Generación de Clave de Internet (6 dígitos)
2	Cambio de Clave
3	Desafiliación de Internet
4	Afiliación de Servicios
5	Desafiliación de Servicios

ANEXO C

CONTROLES DE SEGURIDAD DE INFORMACIÓN PARA LAS OPERACIONES POR EI CANAL DE INTERNET

Para brindar confianza y garantizar el no-repudio de las operaciones realizadas por Internet, los tarjeta habientes que deseen usar este medio, deben afiliarse al sistema (paso 1) y contar con una segunda clave de uso exclusivo para Internet (paso 2) y el sistema debe incluir controles de seguridad de información en todo el proceso de operación (paso 3).

Paso 1. Afiliación para realizar operaciones por Internet

Para realizar operaciones por Internet, el tarjeta habiente titular deberá acercarse a las Agencias del Banco y firmar un Contrato de Afiliación para realizar operaciones por Internet, presentando su tarjeta del Banco de la Nación, DNI y su clave de 4 dígitos (clave 1) usada en agencias, cajeros automáticos y POS. Firmado el contrato, el sistema habilitará la tarjeta para que el tarjeta habiente pueda generar su clave de Internet (clave 2).

El tarjeta habiente podrá generar su clave de Internet (clave 2) en un periodo máximo de 3 días después de la firma del contrato. Pasado este periodo el sistema deshabilitará la generación de la clave de Internet (clave 2). En este caso, el tarjeta habiente deberá apersonarse nuevamente a la Agencia, para solicitar la rehabilitación de la generación de la clave 2.

Paso 2. Generación de la clave de Internet (clave 2)

Para que el tarjeta habiente pueda generar su clave de Internet (clave 2), deberá seguir los siguientes pasos:

- Estar habilitado para generar la clave de Internet (clave 2), descrito en el paso 1.
- Generar la clave de Internet (clave 2), ingresando a la página Web del banco (www.bn.com.pe) y/o en la Intranet (<http://intranet>).
- El sistema debe solicitar al tarjeta habiente el ingreso de:
 - o El tipo de tarjeta afiliada (Multired Global Débito).
 - o Número de tarjeta afiliada (16 dígitos).
 - o Clave de 4 dígitos (clave 1) usada en Agencias, Cajeros Automáticos y POS.
 - o Nueva clave de Internet (clave 2) de 6 dígitos.
 - o Confirmación de la nueva clave de Internet.
 - o Cuenta de correo electrónico.
 - o Confirmación de la cuenta de correo electrónico.

El sistema deberá enviar la constancia de generación de la clave de Internet (clave 2) y la autorización para realizar operaciones por Internet, a través del correo electrónico.

Paso 3. Operación por Internet

Una vez que los usuarios cuenten con una clave de Internet (clave 2), podrán realizar operaciones por Internet, para lo cual el sistema debe contar con los siguientes controles de seguridad de información:

- **Autenticación de la página Web del Banco de la Nación:** el tarjeta habiente debe asegurar la identidad del banco visualizando los controles de seguridad establecidos en la página Web, por lo que el sistema debe permitir el uso de Certificados Digitales a través del protocolo de seguridad Secure Socket Layer (SSL de 128 bits) entre el servidor y el tarjeta habiente (browser), que cumplan con el estándar X.509v3 y que sean emitidos por autoridades certificadoras. A la fecha se tiene un Certificado Digital de Verisign que cumple este requisito.
- **Autenticación del tarjeta habiente:** Este concepto está asociado a proveer la seguridad de que la persona que está iniciando la transacción es la persona autorizada para esto. El sistema debe asegurar la identidad del tarjeta habiente para minimizar el no repudio de las operaciones, validando los siguientes datos:
 - Tipo de tarjeta (Multired Global Débito).
 - Número de tarjeta (16 dígitos).
 - Clave de Internet (clave 2) de 6 dígitos.
 - CVV2 (Card Verification Value 2), de 3 dígitos

La clave de Internet (clave 2) de 6 dígitos denominado PIN (Número de Identificación Personal), de conocimiento exclusivo del Tarjeta-Habiente debe ser diferente al que use en Ventanillas, Cajeros Automáticos y POS; y debe ser configurable de **6 a 8** dígitos

El sistema debe permitir que el tarjeta habiente pueda cambiar su PIN en forma periódica y a voluntad.

El PIN del tarjeta habiente tiene una contraparte, la cual se calcula utilizando el método de cifrado Algoritmo DES. Cuando el tarjeta habiente ingresa su PIN, el sistema recalcula la contraparte y si ésta concuerda con lo registrado, entonces el PIN se asume válido.

El número de intentos fallidos para el ingreso de la clave de Internet (clave 2) será de 3 veces como máximo, luego de lo cual la tarjeta quedará bloqueada para su uso en este canal hasta el día siguiente.

- **Autenticación de la tarjeta:** Este concepto está asociado a proveer la seguridad de que la tarjeta que se está usando para iniciar la transacción es una tarjeta válidamente emitida por el Banco. Para esto el método utilizado es el **CVV 2** basado en el algoritmo DES, el cual consiste en utilizar datos propios de la misma banda magnética, los cuales al combinarse con una clave secreta que sólo el Banco conoce, dan como resultado dicho valor.

Este valor está grabado en la tarjeta y viaja con la transacción, el sistema lo recalcula y compara con el recibido, si son iguales, entonces la tarjeta se asume válida.

- **Autenticación de operación:** Este concepto está asociado a proveer la seguridad de que las operaciones realizadas en este canal son auténticas, ya que los recibos se utilizan como comprobantes de pago.

El método a usar para este tipo de autenticación se denomina MAC (Message Authentication Code), el cual consiste en imprimir al final del recibo electrónico un valor de verificación calculado en base a datos del recibo y una llave de MAC específica asociada con la tasa materia del pago.

- **Seguridad del PIN:** para el ingreso de la clave del tarjeta habiente en Internet se deberá usar teclado virtual aleatorio, de manera que la clave no sea capturado a través del teclado.
- **Seguridad en el Host** Para garantizar la integridad y confidencialidad de la clave 2 de los tarjeta habientes en la base de datos que reside en el Host IBM, se debe mantener protegida bajo algoritmos de encriptamiento DES y con claves criptográficas de uso exclusivo para este canal. La validación del PIN y de la tarjeta se debe realizar en el Host IBM.

El sistema deberá brindar seguridad de las transacciones realizadas en Internet, La solución debe incluir mecanismos de seguridad, que permita el encriptamiento de las tramas para el transporte de datos entre la aplicación que reside en el Servidor WEB y el Motor Transaccional que reside en el Host IBM, utilizando algoritmos y llaves de encriptamiento DES, permitiendo la migración al algoritmo Triple DES

Log de Auditoría registrado en el servidor WEB por cada transacción.

- **Validación de la operación:** para la validación de la operación, el sistema debe solicitar el ingreso de la clave de Internet (clave 2) por cada operación realizada, luego de lo cual deberá mostrar la confirmación de la transacción, que podrá ser impresa o enviada por correo electrónico.

Además, se debe implementar un tiempo máximo de 3 minutos para la ejecución de la transacción, pasado los cuales el sistema cerrará la sesión, debiendo el tarjeta habiente reingresar nuevamente la clave de Internet para continuar con las operaciones.

Paso 4. Manejo de la clave de Internet (clave 2)

El sistema debe facilitar al tarjeta habiente el manejo de su clave de Internet, a través de las siguientes opciones:

- **Olvido de la clave de Internet:** en este caso el tarjeta habiente debe acercarse a una agencia del banco para solicitar se habilite la generación de la clave de Internet que le permita generar una nueva clave.
- **Cambio de clave de Internet:** el sistema debe permitir el cambio de la clave de Internet a voluntad del tarjeta habiente y en forma periódica cada 6 meses.
- **Desafiliación:** el sistema debe contar con la opción de desafiliación para realizar transacciones por Internet cuando el tarjeta habiente considere necesario.

Paso 5. Transacciones por Internet

Con la finalidad de proteger la clave de los tarjeta habientes de 4 dígitos (clave 1), creada para el uso en Agencias, Cajeros Automáticos y POS, se crea la clave de Internet de 6 dígitos (Clave 2), por lo cual **toda operación en Internet que** afecten el saldo de una cuenta, debe realizarse **usando la clave de Internet** (clave 2).