



INFORME TÉCNICO PREVIO DE EVALUACIÓN DE SOFTWARE

NÚMERO: P660 – DGTI

“PROYECTO GESTION DE IDENTIDADES Y ACCESOS”

1. NOMBRE DEL ÁREA

División Seguridad de Información

2. RESPONSABLE DE LA EVALUACIÓN

- a) Sr. Martin Figueroa Revilla
- b) Sr. Segundo Loloy Lopez
- c) Sr. Luis Palacios Quichiz
- d) Sr. Marco Mena Miranda

3. CARGO

- a) Profesional IV
- b) Apoderado general
- c) Profesional III
- d) Técnico IV

4. FECHA

30 de octubre de 2006

5. JUSTIFICACIÓN

En la actualidad, el Banco de la Nación afronta un crecimiento exponencial en las demandas de servicios que involucran la administración de los permisos de acceso a la información y la autenticación de la identidad del usuario autorizado. La organización precisa administrar cómo acceden los usuarios a las aplicaciones sobre una variedad de plataformas y, además, extender su infraestructura de TI para proporcionarles a los socios, proveedores, clientes y empleados remotos acceso a un creciente número de aplicaciones.

Al mismo tiempo, se espera ocasionar un impacto positivo en la imagen, mejorando la retención y fidelidad de los clientes, reduciendo los gastos operativos y respondiendo con prontitud y eficiencia a los cambios.

La administración de muchas aplicaciones sobre múltiples plataformas para un número creciente de usuarios internos y externos presenta los siguientes desafíos de seguridad y administración:



- Proporcionarles a los socios de negocios acceso a aplicaciones y herramientas de colaboración sin sacrificar la seguridad de las aplicaciones o de la red interna.
- Limitar el número de contraseñas que los usuarios precisan para obtener acceso seguro a las aplicaciones. Tener demasiadas contraseñas, a menudo, conduce a que los usuarios empleen prácticas de seguridad muy pobres, como escribir contraseñas en hojas adhesivas.
- Administrar la carga administrativa de mantener datos duplicados de usuarios en múltiples directorios de aplicaciones y, a su vez, no sobrecargar un directorio centralizado con datos específicos de aplicaciones.
- Sacar provecho de las herramientas administrativas existentes en un conjunto más grande de entornos de aplicaciones.

Suele decirse que una cadena es tan fuerte como lo sea el más débil de sus eslabones. Y en muchas empresas, cuando se trata de seguridad TI, el eslabón más vulnerable es la gestión de accesos e identidades.

6. ALTERNATIVAS

eTrust:

- eTrust Admin. Administración del ciclo de vida de la identidad.
- eTrust Access Control. Control de acceso a los servidores, archivos y aplicaciones, basado en identidad.
- eTrust Audit. Verificación basada en identidad.
- eTrust Directory. Repositorio de seguridad escalable y seguro.
- eTrust Single Sign-On. Acceso simplificado a múltiples aplicaciones.
- eTrust Web Access Control. Control de acceso a sitios en Internet, portales, servicios Web y otros recursos extranet, basado en identidad.

BMC:

- BMC Directory Management: Repositorio de Seguridad
- BMC Access Management: Control de accesos a aplicaciones y datos
- BMC User Administration and Provisioning: Administración del ciclo de vida de la identidad
- BMC Password Management: Administración de contraseñas
- BMC Audit and Compliance Management: registro de auditoria, reportes y monitoreo de cumplimiento de políticas

Novell:

- Novell Identity Manager: Administración del Ciclo de vida de la identidad
- Novell Secure Login: Logon Unico (Single Sign On)
- Novell eDirectory: Repositorio de Identidades
- Novell iChain: Control de acceso a aplicaciones y recursos Web
- Novell Nsure Audit: registro de auditoria

Tivoli :



- Tivoli Identity Manager: Administración de Identidades
- Tivoli Directory : Repositorio de Identidades
- Tivoli Access Manager for eBusiness: Control de acceso a aplicaciones Web
- Tivoli Access Manager for Enterprise SSO: Logon Unico (Single Sign On)
- Tivoli Access Manager for Operating Systems: Control de acceso a sistemas operativos Unix
- Tivoli Enterprise Console: administración de eventos de seguridad en Identidades y Control de Accesos.

7. ANÁLISIS COMPARATIVO TÉCNICO

En la matriz siguiente se muestra los algunos fabricantes de productos, disponibles en el mercado, especializados en la implementaciones de soluciones de gestión de identidades y accesos, versus en área funcional requerida por el Banco.

Area Funcional	CA	IBM	Oracle	Sun	HP	BMC	Novell
Aprovisionamiento de Usuarios	Si	Si	Si	Si	Si	Si	Si
Logon Unico SSO	Si	Si	No	No	Partner	Si	Si
Control de Accesos a Aplicaciones Web	Si	Si	No	No	No	Si	Si
Contención del Usuario Root (Unix/Linux)	Si	Si	No	No	No	No	No
Administración de Contraseñas	Si	Si	Si	Si	No	Si	Si
Aprovisionamiento basado en Roles y Políticas	Si	Si	Si	Si	No	Si	Si
Workflow para la Administración de Identidad	Si	Si	Si	Si	No	Si	Si

a) Aprovisionamiento de Usuarios.

Control de Ciclo de Vida del Usuario, manejo del concepto de Usuario corporativo, manejo de altas, bajas. Administración de Identidad basada en Roles (RBAC) y debe soportar todas las plataformas instaladas actualmente en el Banco incluyendo Mainframe (z/890).

b) Login Único de Conexión (Single Sign-On).

La Solución debe permitir la implementación de un login único para la autenticación de todos los usuarios en las diferentes plataformas. Debe estar integrado directamente con el Control de Accesos y el Aprovisionamiento de Usuarios.

c) Control de Acceso a aplicaciones Web

De manera externa a las aplicaciones se requiere poder definir y controlar quien tiene acceso, a que aplicativos y recursos disponibles vía Web y cuando puede hacerlo. Los controles deben basarse en las políticas y reglas de operación que el Banco defina.



d) Contención de Privilegios de la Cuenta ROOT (Unix/Linux)

La Solución debe permitir controlar el acceso a Servidores Unix, y a las aplicaciones y recursos que en ellos residen, a través de Políticas de Acceso robustas y de fácil administración.

e) Administración de Contraseñas.

Integrado con el Aprovisionamiento de Usuarios y el Logon Único de conexión debe permitir la sincronización de contraseñas y auto-reset de contraseñas por parte del usuario final a través de una interfaz web.

f) Aprovisionamiento Basados en Roles y Políticas.

La solución debe permitir el uso de roles y políticas para la asignación de permisos de acceso a los recursos (Ejemplo: sistemas, aplicaciones, bases de datos).

g) Workflow para la Administración de Identidad.

Automatizar el proceso de aprovisionamiento y administración de las identidades a lo largo de su ciclo de vida mediante el uso de un Workflow.

8. ANÁLISIS COMPARATIVO DE COSTO – BENEFICIO:

a) Licenciamiento

Se requiere adquirir licencias de software necesarias para cumplir con los siguientes requerimientos:

COMPONENTE	CANTIDAD
Aprovisionamiento de Usuarios	Licencias necesarias para el aprovisionamiento de 4,000 usuarios
Single Sign On	Licencias necesarias para soportar 4,000 usuarios
Control de Acceso Web	Licencias necesarias para el control de acceso Web para 4,000 usuarios
Contención del Usuario Root (Unix/Linux)	Licencias necesarias para el control de acceso a servidores Unix con un total de 30 procesadores.

b) Hardware necesario para su funcionamiento

La solución tecnológica solicitada, deberá de considerar todos los gastos que sean necesarios para el servicio de Instalación, Configuración e Implementación. (Hardware y Software), sin costo adicional para el Banco.



c) Soporte y Mantenimiento Externo

La garantía, mantenimiento y soporte técnico será por un periodo de dos (02) años para el hardware, el software y los servicios que conforman la solución .

Durante este periodo, se requiere un mantenimiento preventivo sin costo para el Banco.

El tiempo máximo de respuesta a fallas deberá ser de dos (02) horas.

d) Personal y Mantenimiento Interno

El Banco cuenta con personal que tiene conocimiento conceptual técnico, más no de detalle debido a que es una solución que se desconoce la marca del producto a adquirir.

e) Capacitación

El Plan de Capacitación debe considerar los siguientes perfiles:

- Perfil Seguridad: Orientado a instruir en la correcta administración de las aplicaciones que comprenden la solución. Mínimo cinco (05) personas, cincuenta (50) horas por persona.
- Perfil Soporte Técnico: Orientado a instruir en la instalación, configuración, mecanismos de recuperación y funcionalidades de alta disponibilidad de la solución. Mínimo cinco (05) personas, cincuenta (50) horas por persona.
- Perfil de Procesos: Orientado a instruir en la correcta Administración de los flujos de Procesos de Seguridad, producto de la implementación que comprende la solución. Mínimo dos (02) personas, cuarenta (40) horas por persona.
- Perfil de Usuario Final: Orientado a capacitar a los usuarios finales en el manejo de la herramienta de Single Sign On y de Autoservicio. Esta capacitación debe dictarse para 200 usuarios en Lima y para 20 instructores quienes replicaran esta capacitación para los usuarios de Lima y Provincias.

f) Tiempo en que se va a entregar la solución con las condiciones exigidas por el BN (time to market)

El plazo de implementación (incluida la consultoría) estimada para la entrega de la solución esta dentro de un rango de 180 y 240 días calendario.

La evaluación formal del análisis de costos se realizará durante el proceso de compras según la Ley de Contrataciones y Adquisiciones del Estado – N° 28267.



9. CONCLUSIONES:

De lo expresado podemos concluir que, se requiere de la implementación de una Solución coherente, consistente e integrada, que permita una adecuada administración de las políticas, los usuarios los procesos y las aplicaciones, necesaria para poder cumplir con los requerimientos de seguridad del Banco.

El dejar de adquirir esta solución implicaría no contar con un usuario único siendo el eslabón más vulnerable la gestión de accesos e identidades.

En una situación ideal, se debería contar con un proceso automatizado para otorgar acceso a sus aplicaciones, así como para anular los permisos de acceso pertinentes cuando cualquier empleado abandona la compañía. Las identidades de empleados deberían estar sincronizadas a través de todos los sistemas, y determinadas tecnologías habrían de permitir a la organización contrastar las identidades de suministradores, socios de negocio y otros usuarios externos vinculados al negocio que requieren acceso seguro a sus sistemas.

En el Banco la realidad es otra. Los empleados que dejan de serlo continúan a menudo disponiendo de acceso a sistemas sensibles durante semanas quizá sencillamente porque el administrador TI nunca llegó a prestar atención al correo electrónico notificando un despido emitido por el departamento de recursos humanos. Y el resto de empleados, deben en cualquier caso soportar la carga de tener que recordar múltiples contraseñas o escribirlas en papeles que después son pegados sobre sus teclados.

10. FIRMAS:

Responsables de la Evaluación	Firmas
Sr. Martin Figueroa Revilla	
Sr. Segundo Loloy Lopez	
Sr. Luis Palacios Quichiz	
Sr. Marco Mena Miranda	