Universidad de San Martin de Porres
Facultad de Ingeniería y Arquitectura
Escuela de Ingeniería de Computación y Sistemas

Implantación del sistema de administración de accesos e identidades en el proceso de control de accesos en el Banco de la Nación

Tesis para optar el Título Profesional de Ingeniero de Computación y Sistemas

AUTOR
Karla Evita Castro Velarde
Jannet del Rosario Guzmán Salgado

Lima - Perú 2010

RESUMEN

Actualmente el Banco de la Nación a través de su División Seguridad de Información, otorga accesos en forma independiente utilizando los módulos de seguridad de cada una de las aplicaciones y/o plataformas tecnológicas. Además, el registro de nuevos usuarios se realiza a través de una comunicación formal desde el Departamento de Personal a la División Seguridad de Información, esta forma de trabajo ocasiona que no se lleve un control estricto del ciclo de vida de la gestión de identidad, las cuentas de los usuarios y la normativa actual vigente, tal como la circular SBS G-140; todo esto trae como consecuencia un incremento en el riesgo sobre la confidencialidad, disponibilidad e integridad de la información del Banco.

El Banco de la Nación cuenta en la actualidad con 5,500 usuarios a nivel nacional y con 250 aplicaciones implementadas. El presente proyecto tiene como objetivo principal administrar eficientemente los accesos a las aplicaciones del Banco de la Nación mediante la implementación de un Sistema de Administración de Accesos e Identidades, puesto que a través de una eficiente gestión de los accesos a las aplicaciones, se espera obtener un mayor control sobre los activos de información.

ABSTRACT

Nowadays the National Bank through its Information Security Division provides an independent access by using security modules of each application and / or technology platforms. Furthermore, registration of new users is done through a formal communication from Personnel Department to Information Security Division, this kind of work made difficult a strict control about the life cycle of identity management, the user accounts and the laws currently in force, such as regulation SBS G-140; all of this increases risk of confidentiality, availability and integrity of the Bank.

Currently, the National Bank has 5,500 nationwide users and 250 implemented applications. The main objective of this project is to manage efficiently the access to applications belong to the National Bank, which is made through the implementation of an Access and Identity Management System, as through an efficient management of access to applications, it is expected to obtain a greater control over information assets.

INTRODUCCIÓN

La falta de políticas y procedimientos en seguridad es uno de los problemas más graves que afrontan las empresas hoy en día en lo que se refiere a la protección de sus activos de información frente a peligros externos e internos. Las políticas de seguridad son esencialmente orientaciones e instrucciones que indican cómo manejar los asuntos de seguridad y forman la base de un plan maestro para la implantación de medidas de protección tales como: identificación y control de accesos, respaldo de datos, planes de contingencia y detección de intrusos.

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.

La situación actual del Banco se refiere a la gestión del ciclo de vida de la identidad, representa una actividad crítica para el Banco debido a que cuenta con un alto requerimiento de administración de cuentas de los recursos informáticos debido a:

- La gran cantidad de cuentas administradas por acceso a los sistemas de información, servicios informáticos y plataformas tecnológicas.
- Un constante requerimiento en la red de agencias en la asignación de roles y perfiles.
- Un alto uso de personal externo temporal.

- Alta rotación y/o temporalidad de los empleados.
- Administración de contraseñas - número excesivo de contraseñas que los usuarios tienen para diferentes aplicaciones.
- Cumplimiento del marco normativo - incapacidad de evaluar el cumplimiento de regulaciones debido a no identificar la población de usuarios y su asociación con los recursos.

El problema planteado es la dificultad que se presenta para desarrollar estrategias eficientes relacionadas a la administración de control de accesos internos y externos de usuarios a los recursos informáticos, al acceso personalizado de los mismos, el manejo de información confidencial, así como al cumplimiento adecuado de las normas regulatorias requieren de un estricto control interno y de un alto nivel de seguridad por lo que no existe un control eficiente de la identidad.

La propuesta de solución del proyecto tiene como objetivo implantar un sistema donde los usuarios realicen por única vez el procedimiento de identificación y autenticación para el acceso a los diferentes servicios brindados dentro de la infraestructura informática. El mecanismo habitual para lograr esta funcionalidad es que el procedimiento de identificación y autenticación dé como resultado un conjunto de credenciales que pueden ser posteriormente utilizadas para demostrar la identidad de los usuarios en el acceso a los diferentes servicios, sin necesidad de volver a proporcionar la información de autenticación.

Previamente al proceso de implantación del sistema es necesario realizar un levantamiento de información respecto a las necesidades de accesos según las funciones de cada área de la organización. A esta actividad se le denomina Ingeniería de Roles, que es el insumo para aplicar la metodología RBAC. Las características de la propuesta de solución son:

- Se realizará la Administración de Accesos basada en Roles (RBAC) para el otorgamiento de accesos a todas las plataformas tecnológicas.
- Se habilitará los controles necesarios para tener una eficiente administración de las identidades, aprovisionamiento de usuarios y el acceso: la auditoría, monitoreo y seguimiento de la seguridad.
- Los componentes de la solución estarán integrados en forma nativa, con la finalidad de prevenir sobre costos en la administración de la seguridad, además de prevenir brechas de seguridad provenientes de la implantación de soluciones de seguridad aisladas.
- Para la implantación de la solución integrada de Administración de Seguridad y la Gestión de Accesos e Identidades y Accesos (IAM), contará con la infraestructura tecnológica necesaria y con las características técnicas mínimas especificadas, las cuales soporten adecuadamente y brinden un eficiente servicio para la solución a implementar.

El objetivo general es integrar el sistema de administración de accesos e identidades al proceso de control de accesos en el Banco de la Nación. Mientras que los objetivos

específicos son:

- Contar con políticas de control de accesos.
- Controlar los accesos a la red.
- Controlar los accesos a las aplicaciones informáticas del Banco y prevenir el acceso de usuarios no autorizados.

La justificación del proyecto está en que mejorará en un 25% la seguridad de la información respecto al control de accesos y mayor productividad de los trabajadores, dado que actualmente el otorgamiento de accesos en promedio se demora un día por requerimiento y con la implantación de este sistema se pretende reducir en un 90% el tiempo de demora en la atención de solicitudes. De acuerdo a las recomendaciones de auditoría externa referente a las amenazas y vulnerabilidades en las entidades financieras en lo que respecta a la seguridad de información, el Banco de la Nación debe realizar la implantación del Sistema de Administración de Accesos e Identidades tomando como referencia la norma ISO 27001 en el dominio de Control de Accesos.

El alcance del Sistema de Gestión de Identidad y Accesos abarca desde la definición del problema y describe cómo debe gestionarse la identidad de las personas y los equipos y cómo proteger los datos de identificación (sincronización, gestión de password y aprovisionamiento de usuarios). El Sistema de Administración de Accesos e Identidades nos permiten mejorar la relación entre los usuarios, gerentes y directivos. En cuanto a las limitaciones, podría centrarse principalmente en la cultura organizacional de los usuarios ante los nuevos cambios, el no contar con personal especializado que cuente con una amplia visión de seguridad de la información en el Banco de la Nación respecto a las nuevas metodologías a implementarse.

El módulo de seguridad que controla los accesos a las distintas aplicaciones del Core del negocio no cuentan con los mínimos estándares de seguridad en las entidades financieras en lo que respecta a la seguridad de información, el Banco de la Nación desea realizar la implantación del Sistema de Administración de Accesos e Identidades tomando como referencia la norma ISO 27001

CAPÍTULO I MARCO TEÓRICO

1.1.Sistema de gestión de accesos e identidades

Poner en marcha el Sistema de Gestión de Accesos e Identidades (IAM, Identity Access Management) es uno de los retos a los que se enfrentan en estos momentos los responsables de TI de las grandes organizaciones y empresas de nuestro país. Antes de abordar uno de estos proyectos hay una serie de elementos estratégicos prioritarios, como conocer cómo afecta el cumplimiento normativo a la hora de iniciarlos o quién debe liderarlo.

El Banco debe establecer la mejor forma de trabajar teniendo en cuenta los requerimientos del negocio y sobre todo la forma en la que nuevos retos y proyectos como la Gestión de Accesos e Identidades puede ayudar a controlar de manera fiable y eficaz los accesos y las identidades respetando las políticas de seguridad implementadas en el Banco,

El primer aspecto a la hora de hablar de Gestión de Accesos e Identidades (IAM) es saber que no sólo estamos hablando de sincronización de passwords y acceso a los sistemas sino que va más allá, cuando hablamos de IAM estamos definiendo quién tiene acceso a qué, saber quién ha accedido a qué o cuáles son las personas que tienen el nivel adecuado de acceso a las aplicaciones correctas, es decir, nos referimos a la

combinación de personas, procesos y tecnología que proporciona acceso a los usuarios a los activos de la organización, protegiendo toda la información confidencial del sistema.

1. Principales condicionantes de IAM

2.

i. a.1) Tan importante como definir los usuarios que tienen acceso a la información es conocer cuáles son los motivos que llevan a una organización a implantar este tipo de sistemas de seguridad. Actualmente existen tres elementos estratégicos, el cumplimiento regulatorio, las mejoras en la seguridad y la reducción de costos y riesgos.

ii. a.2) Actualmente dentro de las organizaciones encontramos una gran variedad de usuarios y diversas aplicaciones, lo que supone multitud de identidades. La Gestión de Accesos e Identidades permite resolver estos problemas a través de la administración y auditoría, como de la autenticación y la autorización de la gestión de accesos.

iii. a.3) Para poder hacer frente a estos requerimientos hay dos tipos de respuestas: táctica y estratégica. La primera de ellas pretende identificar los problemas de seguridad más urgentes; evaluar, definir y comunicar las funciones de cada uno de los integrantes de la organización, definiendo e implantando los procesos de ciclo de vida y explotar la tecnología ya existente para soportar las personas y los procesos. Frente a esto, la respuesta estratégica define claramente la política IAM que soportará la definición del negocio, y que por supuesto, debe estar alineada con él. Realiza una administración centralizada involucrando a todas las áreas de negocio. También prevé la automatización de los procesos clave y utiliza tecnologías que soporten la automatización de los procesos.

iv. a.4) En una correcta gestión de identidades, son evidentes los beneficios y el valor que ésta apuesta por una respuesta estratégica, como cumplimiento más efectivo de la regulación, la reducción de los costos de operación, una mejora en la calidad del servicio y sobre todo, permitir a la organización adquirir ventaja competitiva. Existen una serie de retos comunes que deben evitarse cuando se pone en marcha un proyecto de gestión de accesos e identidades, como por ejemplo, la ausencia de patrocinio de la dirección, una definición pobre de los requisitos o la ausencia de la implicación por parte de los usuarios, entre otros. Conseguir resolverlos es sin duda el camino para conseguir el éxito en estos proyectos.

Figura Nº 1.1 Componentes del IAM

[1]

1.2. Administración de Roles de la Organización

La ingeniería de roles para RBAC es el proceso de definición de roles, permisos y asignación de permisos para cada rol. La ingeniería de roles es el primer paso hacia la implementación de un sistema RBAC. La ingeniería de roles pude ser descompuesta en tres etapas:

La primera consiste en el análisis de los permisos y roles que se requiere implementar. El nombre de esta etapa en ingles ROLE-PERMISSION ANALYSIS (RAP). A esta etapa ingresan los objetivos de las aplicaciones, información del contexto y un análisis de escenario. Como resultado de esta etapa se obtienen roles y permisos iníciales.

La segunda etapa, llamada ROLE-PERMISSION REFINEMENT (RPR), tiene como objetivo el concretar el análisis para producir los roles y permisos definitivos. A esta etapa ingresan los roles, escenarios y permisos iniciales para su refinamiento. El resultado de

[1] Fuente:http://www.in.kpmg.com/services/ras/it_advisory/ita_IAM.asp

esta etapa son roles y permisos definitivos, lo que podemos llamar el modelo RBAC.

La última etapa, llamada ROLE-PERMISSION MAINTENANCE (RPM), tiene como objetivo fijar las políticas adecuadas para que el modelo RBAC se mantenga vigente en el tiempo. Las actividades de la última etapa son: mantenimiento de roles, mantenimiento de permisos, permisos de aplicaciones y mantenimiento de la relación roles y permisos.

Ciclo de vida de identidad 1.

2.

a.1) Administración de identidades y accesos (IAM) i.

Es una solución coherente, consistente e integrada, que permite una adecuada administración de las políticas, los usuarios, los procesos y las aplicaciones; de acuerdo a sus roles en los procesos de negocio del Banco. La solución será altamente disponible e integrada al entorno de seguridad de los diferentes ambientes y plataformas del Banco de la Nación. ii.

Se espera habilitar los controles necesarios para tener una eficiente administración de las identidades, aprovisionamiento de usuarios y el acceso, la auditoría, monitoreo y seguimiento de la seguridad. iii. iv.

a.2) Aprovisionamiento de usuarios. 1.

Este concepto está asociado al control del Ciclo de Vida del Usuario, manejo del concepto de usuario corporativo que permite a una persona ser identificada en el sistema a través de una sola cuenta, manejo de altas u otorgamiento de accesos, bajas o eliminación de accesos. Administración de Identidad basada en Roles (RBAC – Role Base Access Control) y debe soportar todas las plataformas instaladas actualmente en el Banco incluyendo Mainframe (z/890). 2.

a.3) Login único de conexión (Single Sign-On) 1.

Este concepto está asociado al uso de un login único para la autenticación de todos los usuarios en las diferentes plataformas, lo que permitirá que un usuario acceda a sus aplicaciones a través del ingreso de una única contraseña. 2.

a.4) Control de acceso a aplicaciones web 1.

Este concepto está asociado a dos aspectos: uso de la misma contraseña utilizada para aplicaciones tales como emulación, para el acceso a aplicaciones web. El otro aspecto es el control de los usuarios en los aplicativos y recursos disponibles vía Web. 2.

a.5) Administración de contraseñas 1.

Este concepto está asociado a mejorar la administración de las contraseñas, verificando que éstas sean seguras y permitiendo al usuario final el autoservicio, es decir el reseteo de su contraseña de manera personal a través de su computadora, sin necesidad de llamar a un tercero y reduciendo el riesgo que otra persona tenga 2.

conocimiento de la misma. Esto se realizará respondiendo a ciertas preguntas configuradas en el sistema.

a.6) Aprovisionamiento basado en roles y políticas 1.

Este concepto está asociado al uso de roles y políticas para la asignación de 2.
permisos de acceso a los recursos (ejemplo: sistemas, aplicaciones, bases de datos). El rol está relacionado con el puesto y función de una persona dentro del Banco, a partir de los cuales se generan los accesos respectivos a los sistemas de información.

a.7) Workflow para la administración de identidad 1.

Este concepto está asociado a la automatización del proceso de aprovisionamiento y 2.
administración de las identidades a lo largo de su ciclo de vida mediante el uso de un Workflow. Una aplicación de Flujos de Trabajo (workflow) automatiza la secuencia de acciones, actividades o tareas utilizadas para la ejecución del proceso, incluyendo el seguimiento del estado de cada una de sus etapas y la aportación de las herramientas necesarias para gestionarlo.

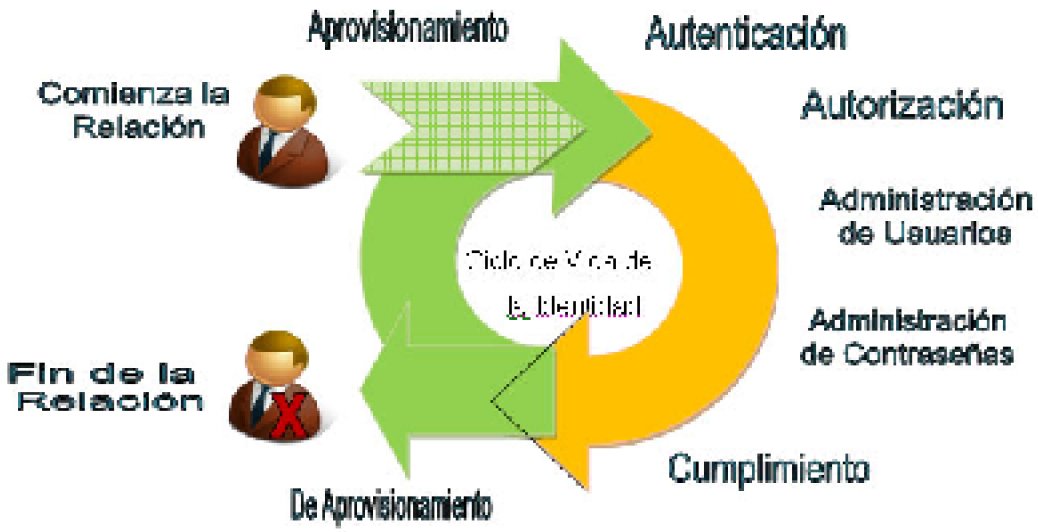

Figura Nº 1.2: Ciclo de vida de identidad

[2]

a.8) Gestión de accesos e identidades 1.

Todos los accesos a los sistemas de información, servicios informáticos y 2.
plataformas tecnológicas deben ser otorgados mediante roles funcionales.

[2] Fuente: http://www.sap.com/chile/about/events/solutions- tour/pdf/Track%203-%20CIO/Presentaci_n_IAM_SAP.pdf

Las solicitudes de accesos que dependan de las acciones de personal formalizadas a[3]4: través del Departamento de Personal serán atendidas una vez que éstas hayan sido autorizadas y registradas en el módulo de recursos humanos Oracle Financial (SAI).

La información de los usuarios externos y de proveedores, debe ser proporcionada 5. por los Jefes de la unidad orgánica que solicita los accesos.

Figura Nº 1.3: Gestión de accesos e identidades

[3]

En el siguiente cuadro se observan los problemas que se tienen en la administración de usuarios.

[3] Fuente: http://www.microsoft.com/australia/business/business-and-industry/ products/microsoft-identity-lifecycle-manager

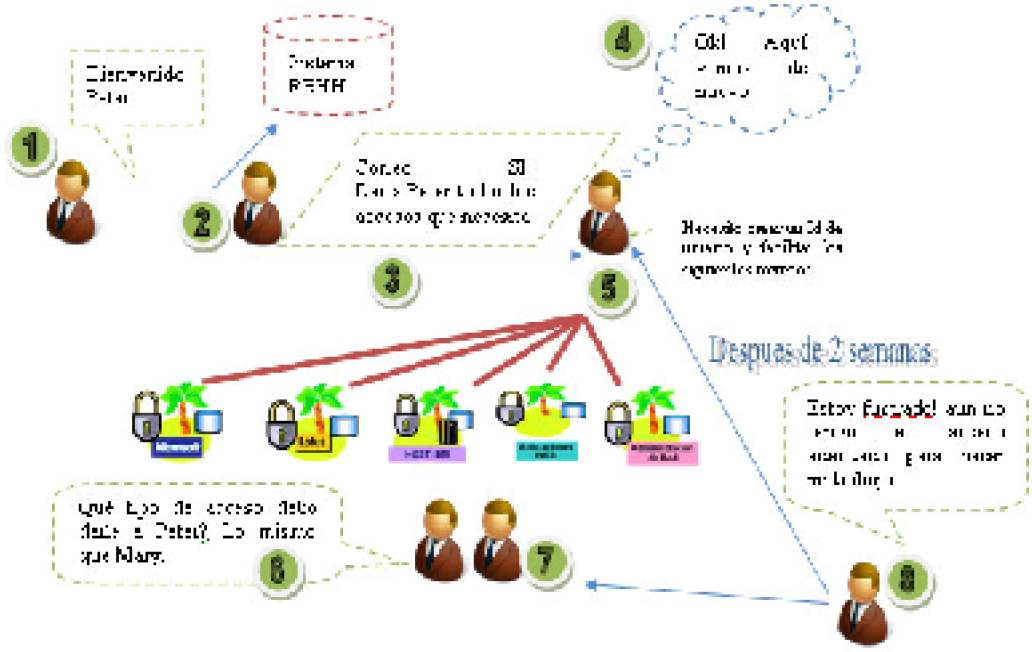

Figura Nº 1.4: Problemas de administración de usuarios

[4]

Las razones para que se realice la gestión de accesos e identidades son las siguientes:

[4] Elaboración: Los autores

METAS DE NEGOCIO	VALOR DE IAM
Aumentar Valor de Negocio	Seguridad consistente.
	Integración más rápida de nuevos usuarios.
	Reducción de Costos.
	Reducción de la pérdida de productividad.
Mejorar el Cumplimiento	Automatización de cumplimiento.
	Mejor capacidad de auditoria y monitoreo.
	Flexibilidad para adaptarse a la nueva normativa
Reducir Riesgo	Mejor capacidad de informes.
	Reducir/prevenir el fraude.
	Mejor ejecución de las políticas.
Reducir Costos	Seguridad consistente.
	Reducción de costos, recursos.

Figura Nº 1.5: Razones para la Gestión de Accesos e Identidades (IAM)

[5]

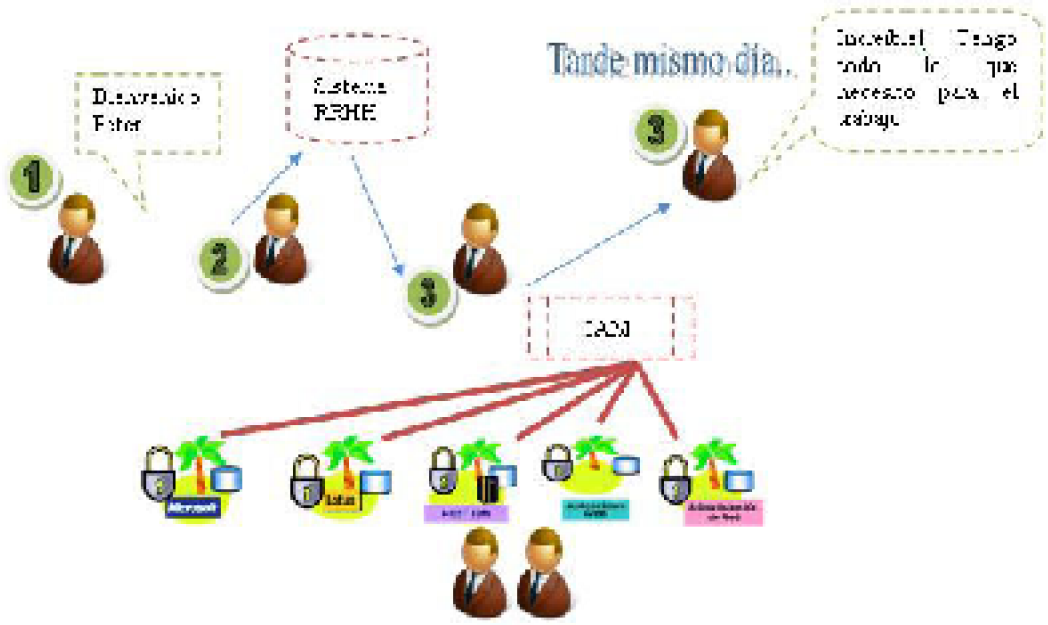

Figura Nº 1.6: Solución con la gestión de identidades

[6]

[5] Elaboración: Los autores

[6] Elaboración: Los autores

1.3. Situación actual

Actualmente en el Banco de la Nación la administración de accesos se realiza utilizando la metodología discrecional, la cual consiste en el modelo de control de acceso discrecional (DAC, Acceso de Control Discrecional), también llamado modelo de seguridad limitada, es un modelo no orientado al control del flujo de información, el propietario del recurso (es decir, un usuario bien identificado) decide cómo protegerlo, estableciendo cómo compartirlo, mediante controles de acceso impuestos por el sistema, y esto ayuda a que el administrador del sistema no tenga que hacer este tipo de tareas, este riesgo puede ser extendido a todo el sistema violando un conjunto de objetos de seguridad.

Sin embargo, es difícil para DAC (Acceso de Control Discrecional) garantizar las reglas de integridad que son necesarias en los ambientes con procesos colaborativos, es poco efectivo para solucionar grandes problemas al enfrentarse a los recursos de información de forma efectiva, además de que el sistema no está protegido frente a los abusos o errores que puedan llegar a tener los usuarios.

Existe un área encargada de la gestión de accesos, la cual utiliza los módulos de seguridad de las distintas plataformas con las que cuenta el Banco para cumplir dicha función; sin embargo esta forma de otorgamiento de accesos es vulnerable en el cumplimiento de los estándares de seguridad generando un alto riesgo para el Banco. Por otro lado, no existe un eficiente control de la identidad de los empleados lo cual conlleva a que en el Banco existan cuentas sin un usuario responsable de la misma.

El Banco de la Nación cuenta con una aplicación (Sistema de Claves) desarrollada en Cobol CICS y Batch, para que se integre a nuestro RACF (Resource Access Control Facility) el cual forma parte del Security Server del Mainframe, desarrollada internamente para administrar permisos y accesos; pero por su antigüedad, no cumple estándares de seguridad acordes a las políticas de seguridad habituales y que tiene uso tanto en aplicaciones del Core Bancario (mainframe) como en aplicaciones de nuestra Intranet.

Los usuarios tienen varias cuentas de acceso a diferentes servicios y aplicaciones Web, estas cuentas requieren de un nombre de usuario y contraseña, para autenticarse y poder usar estos servicios, la utilización de diversas cuentas, puede ocasionar pérdida u olvido de las contraseñas. Al no recordar la contraseña adecuada de cada aplicación es un trabajo que puede reducir la productividad, mucho más cuando existen fallos que producen tiempos muertos y llamadas de soporte.

Para esto es necesario implementar procesos y herramientas que permitan el cumplimiento de estándares para garantizar la seguridad de la información en el Banco. Las áreas que participan son:

a) Seguridad de información 1.

- Recibe solicitudes de usuario para otorgar los accesos.
- Verifica si existe perfil definido para otorgar los accesos.
- Otorgar accesos según los perfiles definidos o autorizados por los propietarios de las aplicaciones.
- Notifica al usuario la atención de la solicitud.

b) Informática 1.

- Recibe solicitud derivada por la División Seguridad de la Información.
- Atiende requerimientos.
- Notifica atención a la División Seguridad de la Información.

c) Usuarios 1.

- Solicita accesos para los diferentes aplicativos.
- Da conformidad de los accesos otorgados.

d) Propietarios del aplicativo 1.

- Recibe solicitud derivada por la División Seguridad de la Información para evaluar el requerimiento.
- Notifica conformidad a la División Seguridad de la Información.

1.4.Identificación de los procesos de negocio

El enfoque de procesos es una manera de visualizar a las organizaciones como un conjunto de procesos cuyo objetivo es la satisfacción del cliente. Cabe resaltar que cada uno de los procesos del Banco de la Nación con la finalidad de conseguir el objetivo que el proceso persigue, y a nivel de actividades y tareas cada persona que interviene lo hace teniendo como referencia el resultado final del proceso.

CAPÍTULO II METODOLOGÍA

2.1.Material y métodos para HW

A continuación se presentan las herramientas de hardware y software empleados en el presente trabajo; asimismo, se cita a los participantes del proyecto, con sus diferentes roles y responsabilidades.

a) Herramientas de hardware y software 1.

HERRAMIENTA DESOFTWARE	
Plataformas	Windows XP Correo Lotus 8.5 Java 1.5.7
Aplicaciones	Aplicativos de la intranet del BN (Anexo 1) Oracle Service Center Registro de Incidencias Host On Demand (java web start) Tivoli Access Manager Tivoli Access Manager for Enterprice Single Sign – on Tivoli Enterprise Console
Browser	Internet Explore 7.0
Microsoft Office 2003	Word Project

Software necesario para la instalación del producto (IAM)

[7]

b) Participantes en el proyecto 1.

Jefes del Proyecto. Labor de Karla Evita Castro Velarde y Jannet del Rosario Guzmán Salgado, Bachilleres de la carrera de Ingeniería de Computación y Sistemas en la Facultad de Ingeniería y Arquitectura de la Universidad de San Martín de Porres.

Profesional	Cantidad Solicitada
Líder del proyecto	02
Gestor de proyecto	01
Analista de calidad de soluciones	02
Analista de soporte plataformas	01
Implementadores	05
Usuarios del negocio	10

[8]

Los participantes antes mencionados deben de trabajar según un orden jerárquico, para un mejor desempeño. En este proyecto se ha establecido un Organigrama Funcional para la Implantación del Sistema de Administración de Accesos e Identidades en el Banco de la Nación

fig006.jpg

[9]

c) Roles y responsabilidades 1.

A continuación se describen las principales responsabilidades de cada uno de los puestos en el equipo del desarrollo para la Implantación del Sistema de Administración de Accesos e Identidades en el Banco de la Nación.

[7] Elaboración: Los autores

[8] Elaboración: Los autores

[9] Elaboración: Los autores

Cargo	Responsabilidad
Líder de Proyecto	Implantación de la Administración de la solución de contraseña única (Tamesso) y la Gestión de Identidades.
Analista Calidad de Soluciones	Revisión y Aprobación de la funcionalidad de la Administración de la solución de contraseña única (Tamesso) y la Gestión de Identidades.
Analista Soporte de Plataforma	Proporcionar una plataforma estándar según el requerimiento de la solución.
Usuario de Negocio	Revisión de la funcionalidad del Agente Tamesso en todos los ámbitos que corresponda.
Implementadores	Instalar el aplicativo Tamesso dejando operativos los servicios de los usuarios para que el producto funcione eficientemente.
Gestor de Proyecto	Gestiona los recursos necesarios para el proyecto, revisa periódicamente los tiempos y avances del proyecto.

[10]

2.2. Desarrollo del proyecto

El proyecto lo hemos desarrollado con una metodología realizada por nosotras. A continuación mostramos la metodología y mejoras prácticas para la ejecución del proyecto de gestión de identidades:

a) Metodología 1.

[10] Elaboración: Los autores

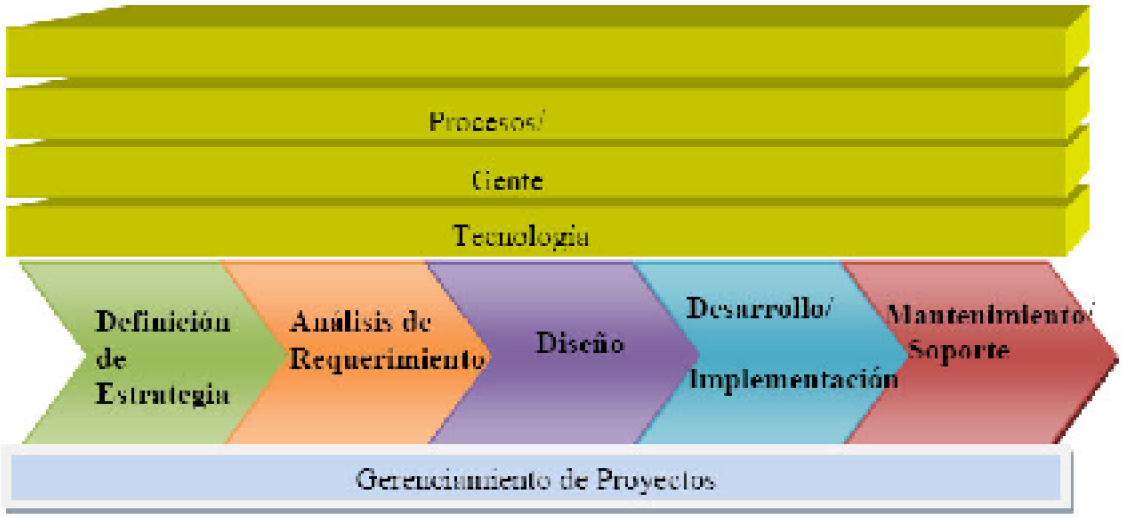

Figura 2.5: Metodología

[11]

En el grafico tenemos Estrategia, Procesos/ Organización, Gente y Tecnología que son los procesos de actividades de soporte para aplicar la Metodología que se inicia con la definición de Estrategia. 1.

a.1) Definición de estrategia 1.

- Se define el alcance general y prioriza los problemas de negocio a resolver. Proporciona claridad sobre la justificación del proyecto.
- Se mide el cambio organizacional dentro del Banco de la Nación.
- El alcance del proceso cubre a todos los usuarios de los activos de la información del Banco de la Nación que residen en las plataformas, Lotus Dominio, Oracle Financial, Intranet, Unix/ Linux y Host On – Demand , en lo que respecta a los sistemas que se conectan directa o indirectamente al sistema de gestión de accesos e identidades y procedimentalmente para el resto de Plataformas/ Sistemas del Banco de la Nación.
- Administrar la seguridad de los activos de información de forma tal que garantice la integridad, disponibilidad y confidencialidad de la información, otorgando los accesos a los mismos de acuerdo a las responsabilidades de los usuarios.

a.2) Análisis de requerimiento 1.

- Se identifica los usuarios y sus roles.
- Se identifica las operaciones del sistema que se va a realizar.
- Levantamiento de información para el diseño de la solución según las necesidades y priorización del negocio.

[11] Elaboración: Los autores

- Evalúa la problemática del negocio para obtener los requerimientos de la solución.
- Construye el caso del negocio y el de implementación.
- Provee una base para la estimación de costos y el tiempo para desarrollar la implantación.
- Desarrolla una arquitectura robusta para el sistema (Anexo 2)

a.3) Diseño (Anexo 3) 1.

- Diseña los componentes técnicos y de negocio de la solución.
- Planifica la etapa de implementación.

a.4) Desarrollo/ implementación (Anexo 4) 1.

- Desarrollo de los componentes.
- Pruebas unitarias de los componentes.
- Puesta en producción.
- Conectores estándares y enlatados.

a.5) Mantenimiento/ soporte 1.

- Evolución y soporte de la solución.
- Actualización de los roles.
- Mantenimiento preventivo y correctivo.

CAPÍTULO III PRUEBAS Y RESULTADOS

En este capítulo se describirán las pruebas y resultados que se realizaron en la Implantación del Sistema de Accesos e Identidades, se realizó también el análisis Costo/Beneficio para saber si al Banco le convenía invertir en este proyecto o no.

3.1.Análisis costo/beneficio

El análisis de costo beneficio determina si el proyecto es económicamente “rentable” para el Banco. Para ello, se aplicará diferentes métodos de análisis o criterios, para comprobar la rentabilidad económica del proyecto, utilizando diversos indicadores económicos.

Antes de detallar el análisis costo/ beneficio presentamos a continuación algunos factores que se consideran para la evaluación:

- El desarrollo de todo el sistema de Información Gerencial se realizara con un mínimo de personal los cuales a su vez forman parte de la organización.
- Algunos de los software a utilizar ya fueron adquiridos por la organización por lo que no se realizó ningún gasto en la compra de estos. (Symantec Antivirus, Windows XP Professional)

3.1.1.Costos

a) Costos incurridos 1.

La inversión del proyecto será la siguiente.

a.1) Recursos humanos 1.

Cant.	Cargo	Total X Mes(S/.)
1	Líder de Proyecto	5500.00
1	Analista Calidad de Soluciones	3800.00
1	Analista Soporte de Plataforma	3200.00
1	Usuario de Negocio	3500.00
2	Implementadores	3000.00
1	Gestor de Proyecto	5200.00
Total mensual		24,200.00
Total periodo Proyecto		S/. 193,600.00

[12]

El horario del personal es a tiempo completo a excepción del Analista de Calidad de Soluciones. 1.

a.2) Equipos 2.

Cant.	Equipos	Costo (S/) X Unidad	Costo Total (S/)
8	Servidores + mantenimiento X mes	6,000.00	48,000.00
1	Impresora	160.00	160.00
Total soles		S/. 48,160.00	

Elaboración: Los autores

Los Servidores se van adquirir para la implantación de este proyecto. Las instalaciones de la Corporación cuentan con cableado tipo UTP categoría 5 para la conexión de red, en caso contrario se estima US $ 70 por cada punto de red adicional. 1.

[12] Elaboración: Los autores

a.3) Software 1.

Licencia de Software	Costo Total (S/)
Windows XP Professional	0.00
MS-Office 2003 Professional	100.00
Symantec Antivirus	0.00
MySql	0.00
Windows Server 2003	0.00
WebSphere Network Deployment	130.00
WebSphere Application Server	150.00
DB2	100.00
Suse Linux	0.00
IBM Tivoli Identity Manager – ITIM	0.00
TAMESSO	0.00
IBM Tivoli Access Manager for e-business -TAMeB	0.00
Total	S/. 480.00

[13]

a.4) Gastos administrativos 1.

Los gastos administrativos presentados son: 2.

Cuadro Nº 3.4: Gastos administrativos

Útiles de oficina mensual	Costo Total (S/)x mes
Hojas	S/. 11
Toner	S/. 80
Cd	S/. 15
Lapiceros y lápices	S/. 10
Sellos	S/. 25
Perforadores	S/. 12
Potapapeles	S/. 30
Grapador y grapas	S/. 10
Servicios básicos (Luz, agua, teléfono)	S/. 100
Otros	S/. 60
Total	S/. 353.00
Total Tiempo proyecto	S/. 2,824.00

[14]

[13] Elaboración: Los autores

[14] Elaboración: Los autores

Cuadro Nº 3.5: Costos incurridos por año

COSTO	MONTO
RECURSO HUMANO	S/. 193,600.00
EQUIPOS	S/. 48,160.00
SOFTWARE	S/. 480.00
MATERIAL DE OFICINA	S/. 28,24.00
Total	S/. 242,240.00

15

Costos de Operación

(Costo Fijo + Costo Variable)

Costo fijo

b.1) Personal para mantenimiento

Cuadro Nº 3.6: Costo de Personal para mantenimiento

Cant.	Cargo	Total (S/.)
1	Jefe Área Sistema Informático	900
1	Analista de sistema	450
1	Técnico informático	420
Total		S/. 1,770.00
Total Tiempo proyecto		S/. 14,160.00

16

b.2) Personal responsable

Cuadro Nº 3.7: Costo de personal responsable

15 Elaboración: Los autores

16 Elaboración: Los autores

Cant.	Cargo	Total (S/.)
1	Gerente de Riesgos	12000
1	Gerente de Informática	12000
Total		S/. 24,000.00
Total Tiempo proyecto		S/. 192,000.00

[17]

b.3) Costo por uso de servicios 1.

Cuadro Nº 3.8: Costo por uso de servicios

+Item	Suministros	Costo Total (S/)
1	Energía eléctrica – Servidor	200
2	Energía eléctrica – Cliente	100
3	Conexión a Internet	95
4	Material de oficina	380
5	Otros gastos	300
Total		S/. 1,075.00
Total en soles		S/. 8,600.00

[18]

Costo variable

Costos Variables ⟶ S/ 2,240.00

Cuadro Nº 3.9: Costos variables

Item	Suministros	Cant.	Unidad de Medida	Costo (S/)	Costo Total (S/)
1	Discos Duros Extraibles	1	Unidad	150	150
2	Cds	50	Unidad	1	50
3	Otros			80	80
Total					S/. 280.00
Total en soles					S/. 2,240.00

[19]

[17] Elaboración: Los autores

[18] Elaboración: Los autores

3.2.Beneficios

Los beneficios tangibles e intangibles obtenidos en este proyecto son los que se muestran a continuación.

- Reducción de los costos de operación debido a la optimización del proceso gracias a la implantación del sistema.
- Mejora la calidad del servicio debido a la reducción de los tiempos de atención y errores en el proceso.
- Reducción de los costos del área de TI debido a la menor cantidad de las llamadas al servicio de la Sección de Soporte Usuario acerca de las contraseñas.
- Seguridad en todos los niveles de entrada, salida, acceso sin que el usuario vuelva autenticarse.
- Mayor rapidez de atención al cliente.
- Mejora en la imagen institucional.

Beneficios tangibles

Cuadro Nº 3.10: Beneficios

Descripción	Total (S/.)
Personal Administrativo	26,448.00
Gastos de Gestión (Movilidad, Llamadas)	261,552.00
Total	S/. 288,000.00

[20]

a) Personal administrativo 1.

Cuadro Nº 3.11: Beneficio tangible – Personal administrativo

[19] Elaboración: Los autores

[20] Elaboración: Los autores

Función	Horas X Mes	Horas perdidas X mes	Pago X Hora X Mes	Total (S/.)
Personal de Soporte Usuario	160	80	107.75	8,620.00
Personal de Seguridad	160	60	111.70	11,170.00
Personal de informática	160	30	78.60	10,220.00
Usuario	160	10	17.89	2,684.00
Total	2	3	4	S/. 32,694.00
Total en soles	2	3	4	S/. 261,552.00

[21]

b) Gastos de gestión 1.

Cuadro Nº 3.12: Beneficio tangible – Gastos de gestión

Función	Cantidad X Mes	Unidad Med	Costo (S/.)	Total en Minutos	Monto (S/.)
Movilidad	33	Soles	2.00	- - - - - -	66.00
Llamadas Telefónicas	18	Minutos	1.00	180	3,240.00
Total					S/. 3,306.00
Total en soles					S/. 26,448.00

[22]

c) Resumen del análisis costo/beneficio 1.

Cuadro Nº 3.13: Datos del proyecto

[21] Elaboración: Los autores

[22] Elaboración: Los autores

	Mes1	Mes2	Mes3	Mes4	……	Mes8
Inversión inicial	S/. – 242240					
Ingresos (Beneficios)		S/. 288,000	S/. 288,000	S/. 288,000	……	S/. 288,000
Egresos (Costos de Ope. y Mantenimiento)		S/.217,000	S/.217,000	S/.217,000	……	S/.217,000
Flujo de Beneficios		S/. 71,000	S/. 71,000	S/. 71,000		S/. 71,000

[23]

3.2.1.Indicadores económicos

a) Valor Actual Neto (VAN)

El VAN del proyecto tomando como rentabilidad un 22 %, con una duración de 8 meses.

$$\text{Formula: } VAN = -I_o + \frac{F}{(1+i)^n}$$

Valor actual neto

Dónde: VAN = Valor actual neto

Io = Inversión inicial

F = Flujo de beneficios

I = Rentabilidad en porcentaje

VAN = 12,072.13

Entonces el VAN > 0 es decir que se puede realizar el proyecto, con beneficios.

b) Tasa Interna de Retorno (TIR)

Tasa que se espera recuperar de una inversión

VAN=0

[23] Elaboración: Los autores

TIR= 24% 5.

6.

La tasa interna de retorno de inversión es mayor que el costo de oportunidad de capital del 22%(i), siendo el resultado muy óptimo para la inversión. 7:

3.3.Pruebas y resultados

a) Control de Acceso Web (IBM Tivoli Access Manager for e-business -TAMeB) 1.

Servirá para proteger los servidores corporativos, para mejorar los niveles de seguridad de autenticación para aplicaciones web. 2.

Prueba	Resultado
Control de Acceso a Aplicaciones Web	
Mostrar la instalación de los Proxy reversos para Internet e Intranet.	Controlar el acceso de los usuarios a las aplicaciones Web del Banco tanto desde Internet como desde la red interna
Mostrar las políticas de control de acceso que rigen para los servicios de proxy: interno y externo.	Sistema de control de acceso basado en políticas que filtre quién desde Internet/intranet puede acceder a que aplicaciones Web específicas, y cuándo puede hacerlo.
Mostrar que se puede realizar control de acceso a los recursos web a través de los mecanismos: Lista de Control de Acceso (ACL). Objetos protegidos (POP) Reglas	Control de acceso a un recursos Web debe basarse en los tres siguientes mecanismos: el uso de listas de control de acceso (ACL), el uso de políticas de protección a nivel del recurso y en reglas de operación del Banco.
Mostrar que se puede brindar acceso a través de HTTPS a los recursos protegidos por el proxy reverso.	Autenticación segura a los diferentes recursos Web, así como brindar un acceso basado en la administración de contenidos.
Mostrar el LDAP donde se almacena la información de cuentas.	La información de usuarios y sus credenciales de acceso se almacenan en el Directorio LDAP de Identidades utilizado por la herramienta de aprovisionamiento
Mostrar la integración de TAMeB con TIM para el aprovisionamiento de usuarios.	Las cuentas de usuario y contraseñas de la herramienta de control de accesos Web pueden aprovisionarse y removerse desde la herramienta de aprovisionamiento.
Mostrar el SSO con las aplicaciones protegidas.	El SSO protege (SSO Web) las aplicaciones Web.
Mostrar que la comunicación entre los componentes se realiza a través de SSL.	La comunicación entre los componentes de la solución ofrecida maneja niveles de encriptación.
Mostrar que para la implementación del módulo para control de acceso Web no se requirió de la instalación de ningún agente en los servidores de aplicaciones.	El control de accesos no requerirá obligatoriamente la modificación de las aplicaciones Web y tampoco la instalación o uso de agentes o código cliente en los servidores de las aplicaciones.
Verificar que sólo el administrador de la solución puede realizar cambios en la configuración.	Solo el administrador puede realizar cambios en la configuración.
Mostrar la documentación del producto que hace referencia al soporte a IIS, WebSphere, WebLogic y Apache.	Soporta los siguientes servidores de aplicaciones: IIS, Websphere, Weblogic, Apache
Hacer referencia a la documentación del producto que muestra el almacenamiento de políticas de control	Los controles de acceso (ACLs, políticas, reglas) se almacena en un servidor de políticas el cual por seguridad está en la red

Prueba	Resultado
de acceso en el Policy Server.	interna del Banco.
Realizar las pruebas de acceso deteniendo el servicio de Políticas de TAMeB.	Por razones de rendimiento debe ser posible habilitar en los Proxys reversos la validación de accesos sin necesidad de consultar siempre al servidor de Políticas.
Requerimientos de Disponibilidad del Servicio	
Mostrar que una vez que se pierde la conexión en un proxy reverso, el otro toma las conexiones en menos de 1 minuto.	Alta disponibilidad del Control de Acceso Web.

b) Módulo de Single Sign-On (TAMESSO) 1.

Permitirá una Identificación y Clave Única, de manera que los usuarios solo tengan la2. necesidad de conocer una única identificación y una única clave de accesos para múltiples sistemas, eliminando las vulnerabilidades asociadas con el manejo de múltiples identidades.

Prueba	Resultado
Autenticación única. Después de que el usuario se autentica en el AD, tiene acceso al resto de aplicaciones.	Verificar que la funcionalidad de autenticación única se realice a través de Active Directory.
Configuración de SSO con aplicaciones. Después de que el usuario se autentica en el AD, tiene acceso directo (sin ingresar su usuario y contraseña) a Lotus Domino, Oracle Financial, aplicaciones legacy (emuladores de Terminal 3270 vía Host OnDemand), consolas Unix (Telnet) e Intranet del Banco.	Verificar la configuración de SSO con los siguientes servicios: a. Correo electrónico Lotus Domino b. Oracle Financial c. Emuladores de Terminal 3270 d. Emuladores de Terminales Unix (Telnet) e. Intranet del Banco
Almacenamiento de contraseñas de usuarios. Haciendo uso de la consola de administración del TAM-ESSO, se mostrará los registros de credenciales de los usuarios en el AD del Banco. Verificar que la información de contraseñas se almacene en un repositorio centralizado y no distribuidos en cada estación. Alta disponibilidad del servicio de SSO. Haciendo uso del mecanismo de replicación del AD del Banco, el administrador de red podrá bajar alguno de los controladores de dominio y los usuarios podrán seguir utilizando la funcionalidad de SSO.	Verificar que la arquitectura de la solución de SSO soporte el uso de réplicas de su repositorio, de tal manera que la pérdida de una de las réplicas no afecte al servicio.
Encriptación de credenciales. Esta prueba se resuelve revisando la documentación publicada por el fabricante del producto (IBM). Utilizando la consola de administración del TAM-ESSO, se puede observar el tipo de encriptación habilitado.	Verificar la utilización del mecanismo de encriptación triple DES o AES para: a. Los passwords almacenados en el Directorio de SSO. b. La información de credenciales enviadas del Directorio SSO hacia el cliente. c. Los passwords almacenados en el Cache Local en el disco del Cliente (en caso de que se utilice) d. La información de Usuario y Password almacenada en la memoria del Cliente
SSO no intrusivo. Los administradores de cada aplicación pueden validar la integridad de sus aplicaciones.	Verificar que la implementación de la solución SSO sea no Intrusiva, es decir NO requiere de cambios en el código fuente de las aplicaciones a soportar.
Servicio de restablecimiento de contraseñas. El usuario, haciendo uso	Verificar que solución de SSO permita a los usuarios poder restablecer su contraseña de

Prueba	Resultado
de la barra que aparece arriba de la ventana de login o bloqueo (locked), podrá ingresar a un servicio Web el cual le permitirá restablecer su contraseña por medio de un mecanismo de preguntas y respuestas.	Windows desde una estación de trabajo bloqueada (locked), en caso de que olvidaran dicha contraseña. Es decir, que el usuario no necesite de una estación ya logueada para restablecer su clave de acceso.
Integración con otros módulos de la solución. Haciendo uso de la interfaz administrativa de TIM, crear y remover cuentas SSO.	Verificar que las cuentas de usuario de la herramienta de SSO se pueden crear y remover desde la herramienta de aprovisionamiento.
Haciendo uso de la interfaz administrativa de TIM, enviar cuentas SSO	Verificar que es posible la distribución de credenciales de las aplicaciones desde la herramienta de aprovisionamiento hacia la herramienta de SSO.
Haciendo uso de la interfaz administrativa de TIM, cambiar contraseñas y verificar el cambio en la aplicación de SSO.	Verificar que el reseteo de password de alguna aplicación desde la herramienta de aprovisionamiento actualiza a la herramienta de SSO.
Requerimientos de Disponibilidad del Servicio	
Mostrar que se puede acceder al servicio cumpliendo los requerimientos de menos de 1 minuto para recuperación del servicio.	Alta disponibilidad

c) Aprovisionamiento de Cuentas de Usuarios (IBM TivoliIdentity Manager - ITIM) 1.

Permitirá la administración de las cuentas de usuarios de los empleados del Banco. 2. Incluye la alta y baja modificación, validación de cumplimiento de políticas, remediación y todas las funciones asociadas a la administración de la identidad para las plataformas del Banco incluyendo el Mainframe.

Prueba	Resultados
Aprovisionamiento de Usuarios	
Creación de una persona en ITIM. A esta persona se le asociará de manera automática los permisos (cuentas) para el rol que se le asignará de manera automática (de acuerdo a la información de la persona).	Soportar el aprovisionamiento y des 1 aprovisionamiento automático basado en Roles y en Políticas.
a) Cuentas Corrientes b) Ahorros c) Préstamos d) TAND e) INCA f) Correo Lotus g) Exchange h) Active Directory i) RACF Se realizarán las operaciones de: • Creación • Modificación: Cambio de atributos, cambio de clave. • Borrado	La solución debe permitir la creación, 1 modificación y borrado de las cuentas de usuario, contraseñas y privilegios en las siguientes aplicaciones: j) Cuentas Corrientes k) Ahorros l) Préstamos m) TAND n) INCA o) Correo Lotus, Exchange, Active Directory, z/890 (RACF)
Probar la interfaz proporcionada para la creación de personas.	Permitir la interacción de la solución con 1 diferentes fuentes autoritativas. Por ejemplo, la aplicación de recursos humanos.
Para cada una de las aplicaciones: a) Cuentas Corrientes b) Ahorros c) Préstamos d) TAND e) INCA f) Correo Lotus g) Exchange h) Active Directory i) RACF Se realizarán las operaciones de: • Creación • Modificación: Cambio de atributos, cambio de clave. • Borrado	Realizar todas las funciones de 1 aprovisionamiento de Usuarios sin importar en que plataforma se encuentren definidos estos usuarios. 1
Validar en la interfaz administrativa de ITIM el uso de la entidad Persona como la entidad que centraliza el uso de múltiples cuentas y que permite el concepto de “usuario corporativo” que requiere el Banco.	Para efectos de la administración de 1 Identidades de los Usuarios internos y externos de la organización, debe existir un único usuario corporativo de tal forma que todas las funciones asociadas al ciclo de vida de la identidad sean realizadas bajo el concepto de usuario corporativo.
Validar en la interfaz administrativa de ITIM el uso de la entidad Persona como la entidad que centraliza el uso de múltiples cuentas y que permite el concepto de “usuario corporativo” que requiere el Banco.	Debe asegurar la implementación de la 1 Identidad Única. Una vez instalada la herramienta, para cada usuario corporativo deberá corresponderle una y solamente una identidad.
Probar el bloqueo de cuentas para una Persona.	Debe asegurar que si un Usuario es 1 dado de baja en la corporación, éste pueda ser eliminado o bloqueado de

Prueba	Resultados	
	todas las plataformas (Sistemas Operativos, Bases de Datos, Aplicaciones, Correo) desde la consola de administración de la solución.	
Probar el bloqueo de una persona a través de la interfaz proporcionada por VisionTech para el manejo de personas.	La baja también debe poderse hacer de manera automática al retirar el registro del usuario de una fuente autoritativa. Por ejemplo, al eliminarlo del registro de empleados del Banco o al eliminar su cuenta en el Active Directory	1
Listar las cuentas huérfanas en la interfaz de administrador de ITIM, para una plataforma: a) Cuentas Corrientes b) Ahorros c) Préstamos d) TAND e) INCA f) Correo Lotus g) Exchange h) Active Directory i) RACF	Debe presentar facilidades para la identificación automática de “cuentas huérfanas.”	1 1
Verificar que se asociaron de manera automática las cuentas de las plataformas: a) Cuentas Corrientes b) Ahorros c) Préstamos d) TAND e) INCA f) Correo Lotus g) Exchange h) Active Directory i) RACF Asociándose éstas de acuerdo a las reglas automáticas por default (userid).	La solución debe permitir la asociación automática basada en reglas, de las cuentas huérfanas con la identidad corporativa de cada usuario.	1 1
TAMESSO	Permitir configurar políticas de expiración de contraseñas y forzar su cumplimiento global en los sistemas y aplicaciones solicitado en las bases. Este debe ser un mecanismo de control diferente e independiente al que cada sistema operativo o aplicativo utilice para la caducidad de passwords.	1
Realizar el proceso de recertificación para Active Directory.	Debe contarse con mecanismos de control que permitan configurar y automatizar políticas de recertificación de cuentas.	1
TAMESSO	Brindarle al usuario final facilidades de auto-servicio que le permita el reseteo de sus contraseñas y así no necesitar hacer llamadas de soporte.	1
TAMESSO	Debe ofrecer una administración de contraseñas tal que permita controles	1

Prueba	Resultados	
	de envejecimiento, histórico, y de sintaxis.	
Mostrar en la interfaz de administración de ITIM la opción de Vista Previa en la edición de Políticas de Aprovisionamiento.	Debe permitir la aplicación de un conjunto de políticas de seguridad en modo advertencia, basado en mejores prácticas que permitan monitorear el estado actual de accesos en el servidor protegido para luego poder activarlas en producción.	1
Desde la intefaz de ITIM crear, borrar y manejar la cuentas de los sistemas: a) Cuentas Corrientes b) Ahorros c) Préstamos d) TAND e) INCA f) Correo Lotus g) Exchange h) Active Directory i) RACF	El Administrador de Seguridad debe poder crear, borrar y manejar cuentas desde la consola de administración de la herramienta sin necesidad de conocer detalles técnicos de las plataformas.	1
Mostrar en la interfaz de administración de ITIM la creación de nuevas cuentas directamente en las plataformas: a) Cuentas Corrientes b) Ahorros c) Préstamos d) TAND e) INCA f) Correo Lotus g) Exchange h) Active Directory i) RACF Y verificar que se envía la notificación vía correo electrónico.	En el caso de realizarse creaciones de cuentas directamente en las plataformas destino, la solución debe ser capaz de registrar y notificar estos hechos al Administrador de Seguridad.	1 1 1
Verificar que al crear una nueva persona, si el rol se le asocia, éste le da los permisos definidos para el rol.	Toda la administración de Privilegios y accesos debe ser realizada bajo el concepto de Roles. Los Roles deben definir los accesos y privilegios de acuerdo a las responsabilidades de trabajo de cada empleado.	1
Verificar en la interfaz de administración de ITIM que son los roles lo cuales se asocian a los privilegios que se otorgan (Políticas de aprovisionamiento).	Debe permitir la definición de roles de Usuarios por diferentes categorías de tal forma que la asignación de privilegios y accesos sean otorgados directamente a los roles simplificando así la administración.	1
Verificar en la interfaz de administración de ITIM la asignación dinámica de roles de acuerdo a atributos de la persona.Mostrar que se puede realizar la asociación manual de roles.	Soportar la asignación dinámica de roles como respuesta a cualquier cambio detectado en los atributos de la identidad (Ejemplo: ubicación). Así mismo debe permitir la posibilidad de una asignación manual de roles y permisos de accesos.	1

Prueba	Resultados
Mostrar los reportes de: Roles y políticas de aprovisionamiento 1 Usuarios por rol 1	La solución debe proporcionar reportes detallados sobre los roles y sus permisos asociados y los usuarios por cada rol. 1
Mostrar en la interfaz de ITIM la suspensión de personas para el caso de vacaciones.	La solución debe proveer la función de “asignación y suspensión temporal de roles”. Esta función está orientada a evitar brechas de seguridad durante períodos de vacaciones, licencias o reasignación temporal de un usuario. 1
Mostrar con un LDAP browser la información de identidades almacenada en el Tivoli LDAP.	La solución debe almacenar la información de identidades en un LDAP Server (Directorio de identidades) 1
Mostrar que los cambios que se realizaron en ITIM se vean reflejados en las plataformas: a) Cuentas Corrientes b) Ahorros c) Préstamos d) TAND e) INCA f) Correo Lotus g) Exchange h) Active Directory i) RACF	Se requiere sincronización en tiempo real de datos críticos de identidades entre los sistemas y aplicaciones a soportar y el Directorio de Identidades de la herramienta propuesta. 1
Mostrar el directorio Tivoli LDAP réplica implementada para el proyecto.	Se requiere contar con un mecanismo de distribución, sincronización y replicación automática de la información del Directorio de identidades de tal forma que permita tener Réplicas de la información del Directorio de identidades en diferentes ubicaciones geográficas. 1
Mostrar que todos los cambios realizados por el directorio a través de la interfaz de administración de ITIM se procesan de manera inmediata.	Se requiere tener la capacidad de detectar y responder a cambios en el Directorio de identidades en tiempo real.
Mostrar la documentación del producto que menciona las plataformas y sistemas operativos en los cuales se puede montar el producto.	El repositorio de las identidades no deberá depender de una plataforma específica para su funcionamiento. Debe poder montarse en más de un sistema operativo, 1
Mostrar la interfaz para realización de Workflows en ITIM.	La solución debe proveer un Workflow flexible y configurable que permita definir y ordenar todos los pasos necesarios para la administración de las identidades de acuerdo al proceso definido como parte de la licitación. 1

Prueba	Resultados
Mostrar en la Interfaz de Administración de ITIM el estado de un Workflow en progreso	Este Workflow debe ofrecer mecanismos de control y monitoreo que permitan identificar en qué estado esta cada solicitud. Por ejemplo, en que paso del proceso se encuentra una solicitud en particular, que aprobaciones están pendientes, quien es el aprobador, entre otros. 1
Mostrar en la Interfaz de Administración de ITIM la funcionalidad que permite el enrutamiento dinámico de aprobaciones.	Enrutamiento dinámico de aprobaciones y flujos de trabajo con base en la información de las identidades. 1
Mostrar en la Interfaz de Administración de ITIM la funcionalidad de delegación	El Workflow debe contar con la funcionalidad de delegación de la autoridad de aprobación, para el caso de ausencias programadas del aprobador titular como vacaciones y licencias.
Mostrar en la Interfaz de Administración de ITIM la opción que permite realizar el escalamiento en ITIM.	Escalamiento automático del aprobador para el caso de aquellas solicitudes que no hayan sido atendidas en un lapso determinado.
Mostrar en la Interfaz de Administración de ITIM que se puede realizar la aprobación en paralelo y en serie.	El Workflow debe permitir definir niveles de aprobación tanto en paralelo como en serie. 1
Mostrar en la Interfaz de Administración de ITIM que se puede realizar la administración delegada en cualquiera de las unidades del Árbol Organizacional.	Administración delegada a cualquier nivel de dentro de la organización. 1 1
Mostrar en la Interfaz de Administración de ITIM las cuentas que no cumplen con las políticas que se ingresaron a ITIM.	Debe contar con mecanismos que ayuden a detectar rápida y fácilmente que cuentas de usuario no cumplen con las políticas de acceso definidas. 1
Mostrar que se tiene la opción en ITIM para realizar el forzamiento de las políticas de aprovisionamiento.	Se requiere contar con ayudas que reduzcan el tiempo de solución de los problemas de No Cumplimiento (cuentas de usuario que no cumplen con las políticas de acceso) 1
Mostrar que la Interfaz de Administración de ITIM se puede acceder vía navegador de Internet.	Interfaz gráfica de administración independiente de la plataforma para su funcionamiento y debe poder accederse desde cualquier punto de la red del Banco de la Nación. 1
Mostrar en la Interfaz de Administración	Permitir la configuración de políticas 1

Prueba	Resultados
de ITIM la configuración de políticas de contraseña para todas las plataformas y verificar que ITIM fuerza al cumplimiento de las mismas al momento de realizar el cambio de clave.	corporativas de contraseñas y supervisar su cumplimiento en los sistemas y aplicaciones cubiertas en la licitación.
Mostrar que se puede realizar la detección de eventos en las plataformas, pero que no se implementará, sino que se mantendrán reconciliaciones programadas de manera diaria que proporcionen la funcionalidad solicitada.	Detección de eventos en tiempo real en cada uno de los sistemas conectados y/o integrados. Eventos son adiciones o cambios en la información del perfil de usuario- 1
Según la realidad del Banco y la licitación, se desarrollarán agentes para: • Sistema de Claves • Cajeros Automáticos (Stratus versión FT5600) • Intranet • Cuentas Corrientes • Ahorros • Préstamos • TAND • INCA	En caso que se requiera desarrollar agentes según la realidad del Banco de la Nación, éstos deberán ofrecer la funcionalidad de Altas, Bajas, Sincronización, entre otros. 1
Los sistemas que requieran la instalación en el sistema a integrar se realizarán de manera nativa: RACF 1 Sistema de Claves 1	Los elementos de software de la solución deberán tener la capacidad de instalarse de manera nativa según el sistema a integrar / conectar. 1
Se mostrará en la documentación de ITIM que existe soporte para las plataformas mencionadas.	Soporte a nivel de servidor y cliente de las siguientes plataformas: UNIX, NT, Windows 2000/XP/2003, Oracle, DB2, Microsoft SQL Server, Websphere, Lotus Domino, Mainframe-
Se mostrará que se encuentran en español los servicios de: a. Interface Web de Autoservicio b. La orientación al usuario en tareas de autoservicio como el reseteo de contraseñas c. Preguntas y respuestas (Challenge y Response) d. Notificaciones vía Email e. Log de errores y mensajes	Debe estar en español los siguientes servicios: 1 f. Interface Web de Autoservicio g. La orientación al usuario en tareas de autoservicio como el reseteo de contraseñas h. Preguntas y respuestas (Challenge y Response) i. Notificaciones vía Email j. Log de errores y mensajes-
Se mostrará que se puede realizar la opción de notificaciones consolidadas de correos electrónicos.	Notificaciones vía e-mail consolidadas que ayuden a reducir significativamente la cantidad de correos relacionados con la administración de identidades que a diario recibe un aprobador. 1
Realizar la creación de una persona que le permita realizar Single Sign-On con las aplicaciones que tiene acceso.	La herramienta de aprovisionamiento debe poder crear y manejar cuentas de 1

Prueba	Resultados
	usuario en el sistema de Single SignOn, distribuyendo además las credenciales de las aplicaciones a las que el nuevo usuario tiene acceso.
Se mostrarán los reportes: a. Lista de todas la cuentas que pertenecen a una persona especifica b. Lista de todas las cuentas de las personas que pertenecen a un rol determinado c. Detalle de las cuentas que existen en un sistema dado d. Mostrar todas las políticas (y sus recursos relacionados) que pertenecen a un rol en particular. e. Listado de las autorizaciones dadas a un individuo en particular f. Listado de todas las acciones de aprovisionamiento que cumplen con un criterio en específico, por ejemplo: listar todas las Adiciones o relación de todas las Suspensiones temporales de cuenta. g. Listado de todas las acciones de aprovisionamiento realizadas por determinado administrador. h. Listado de las solicitudes aprobadas y las rechazadas i. Relación de todas las aprobaciones pendientes j. Listado de todas las cuentas que han sido suspendidas 3.1 Listado de todos los sistemas y aplicaciones que se están aprovisionando 3.2 Listado de todas las políticas definidas 3.3 Numero de cuentas procesadas, de cuentas huérfanas, de cuentas que violan alguna política, cuentas que han sido des aprovisionadas, numero de cuentas suspendidas, etc. 3.4 Listado de todas las cuentas que no están en cumplimiento y la razón :	a. La solución propuesta debe llevar un registro de auditoria seguro y brindar reportes de gestión predefinidos. Entrega de reportes- b. Lista de todas la cuentas que pertenecen a una persona especifica c. d. Lista de todas las cuentas de las personas que pertenecen a un rol determinado e. Detalle de las cuentas que existen en un sistema dado f. Mostrar todas las políticas (y sus recursos relacionados) que pertenecen a un rol en particular. g. Listado de las autorizaciones dadas a un individuo en particular h. Listado de todas las acciones de aprovisionamiento que cumplen con un criterio en específico, por ejemplo: listar todas las Adiciones o relación de todas las Suspensiones temporales de cuenta. i. Listado de todas las acciones de aprovisionamiento realizadas por determinado administrador. j. Listado de las solicitudes aprobadas y las rechazadas k. Relación de todas las aprobaciones pendientes l. Listado de todas las cuentas que han sido suspendidas m. Listado de todos los sistemas y aplicaciones que se están aprovisionando n. Listado de todas las políticas definidas o. Numero de cuentas procesadas, de cuentas huérfanas, de cuentas que violan alguna política, cuentas que han sido des aprovisionadas, numero de cuentas suspendidas, etc. p. Listado de todas las cuentas que no están en cumplimiento y la razón. q.
Requerimientos de Disponibilidad de Servicio	
Mostrar que una vez se ha detenido el servidor principal de aprovisionamiento (ITIM) se restaura el servicio en menos de 30 minutos.	Alta disponibilidad del Servicio de Aprovisionamiento de Usuarios. 1

CAPÍTULO IV DISCUSIÓN Y APLICACIONES

Actualmente nos hemos visto en la necesidad de proteger los activos de la información frente a peligros externos e internos asegurando así la información del Banco de la Nación.

La implantación del Sistema de Administración de Accesos e identidades en el proceso de control de accesos llevará a una mejor administración de los accesos en las aplicaciones del Banco y especialmente en el proceso de la gestión de accesos garantizando mayor control de la Seguridad de la Información. Las pruebas realizadas en la implantación del Sistema de Administración de Accesos e identidades fueron totalmente favorables para el Banco en:

- Aprovisionamiento de Cuentas de Usuarios (IBM TivoliIdentity Manager - ITIM)
- Control de Acceso Web (IBM Tivoli Access Manager for e-business -TAMeB)
- Módulo de Single Sign-On (TAMESSO)

CAPÍTULO V CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones

1. De lo expresado se concluye que se requiere 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.

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

3. 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 permitirían a la organización contrastar las identidades de suministradores, socios de negocio y otros usuarios externos vinculados al negocio que requiere acceso seguro a sus sistemas.

4. El contar con el Registro Automático de Contraseñas asociadas a la cuenta de red permite eliminar el riesgo de utilizar canales poco confiables (teléfono o correo electrónico) para otorgar credenciales a los usuarios.

5.2. Recomendaciones

1. Realizar la transferencia de conocimiento a personal de la institución para la administración de la solución y principalmente para el desarrollo de nuevos adaptadores.

2. Definir un plan de mejoramiento continuo que permita garantizar la continuidad del proyecto

3. Implementar controles administrativos para continuar mejorando los niveles de seguridad de información en la institución.

FUENTES DE INFORMACIÓN

- ISO 27001:2005
- ISO 17799
- ISO 7498-2
- http://www.marblestation.com/?p=660
- http://www.alegsa.com.ar/Dic/emulacion.php
- Referencia del SSO: http://es.wikipedia.org/wiki/Single_Sign-On
- http://www.internet2.edu/pubs/200703-IS-MW.pdf
- http://www-01.ibm.com/software/tivoli/products/identity-mgr/

ANEXOS

ANEXO 1. APLICATIVOS DIVERSOS – INTRANET

ADMINISTRACIÓN DE CONTRATOS Y CONVENIOS 1.
ACCI 2.

- Mantenimiento de Documentos
- Consulta de Documentos

ADMINISTRACIÓN DE PAGARÉS 1.
PRCA 2.

- Mantenimiento
- Consulta General
- Administración de Red (Dpto. informática)
- Administración de Placas de rodaje (Dpto. informática)
- Administración de Riesgos (División Riesgos TI)

SARO 1.

ADMINISTRACIÓN DE RED 1.

ADMINISTRACIÓN DE ACCESOS E IDENTIDADES 2.

ADMINISTRACIÓN DE PLACAS DE RODAJE 3.

4.

5.

ATENCIÓN DE RECLAMOS 1.

AISR 2.

- Ingreso del Reclamo
- Resultado sin visto final
- Resultado con visto final
- Modificación de reclamos
- Derivación a otra oficina
- Consulta a la misma oficina
- Consulta a cualquier oficina
- Estadística sin detalles
- Estadística con detalles
- Mantenimiento de tablas
- Diversas opciones generales
- Reconsideración
- Generación contra cargos VISA

CAJEROS MONEDEROS 1.

RESI 2.

- Consulta Movimientos
- Consulta por Agencia

COBRANZA COACTIVA 1.

RECC 2.

- Registro de Expediente de Cobranza
- Eliminación de Expediente de Cobranza
- Consulta por número de expediente
- Consulta por fecha de pago
- Registro de documentos y pagos

CONSTANCIA DE PAGOS EN LÍNEA 1.
INTR 2.

- Consulta de Pagos de servicios
- Consulta de Pagos de Tasas
- Estadísticos

CONSULTA DE REGISTRO DE FIRMAS SARASIGN 1.
AISG 2.

- Consulta de Judiciales
- Consulta por Cuenta todos los Servicios
- Consulta Alfabética todos los Servicios
- Consulta por Institución
- Consulta por RUC
- Consulta por Documento de Identidad – Firmante
- Consulta de Notarios
- Consulta de Funcionarios
- Consulta Tabla de Facultades.

CONSULTA RENIEC 1.
RECA 2.

- Consulta por Nombre
- Consulta por Documento
- Consulta por Foto
- Consulta por Firma
- Consulta Consolidada
- DEPOSITOS JUDICIALES (Informativo)

DETRACCIONES SUNAT 1.
CTEN 2.

- Ingreso / Consulta de Detracciones masivas Intranet
- Borra Transmisión Intranet

ESTADÍSTICAS RECAUDACIÓN 1.

ESFI 2.
ESTADO DE CUENTAS DE AHORRO 3.
ECAI 4.

- Impresión estado con comisión
- Impresión estado sin comisión
- Consulta de Transacciones
- Consulta alfabética de Ahorros

EVALUACION DE CRÉDITOS (Dpto. de Créditos) 1.

EXPEDIENTES ELECTRÓNICOS LABORALES 1.
EXJU 2.

- Consulta Expedientes regulares
- Consulta Expedientes sensibles
- Modificación Expedientes propios
- Modificación Expedientes todos
- Eliminación Expedientes propios
- Eliminación Expedientes todos
- Modificación Información Abogados

GENERACIÓN DE CONVENIOS 1.
AHCO 2.

- Creación de Convenios
- Modificación de Convenios
- Consulta de Convenios

JOURNAL ELECTRÓNICO (Dpto. Informática) 1.

HERMES Y PROSEGUR 1.
AISC 2.

- Red Digital de Firmas – Hermes
- Red Digital de Firmas – Prosegur

HORAS EXTRAS 1.

RHHE 2.

- Adicionar Empleado HE
- Actualizar HE de Empleado
- Eliminar HE de Empleado
- Consulta HE de Empleado
- Confirmar HE.

INFORMACION SBS 1.
COBD 2.

- Reporte Deudores SBS Intranet
- Cta. Cte. / tarjeta Crédito Intranet

LAVADO DE DINERO 1.
LADI 2.

- Mantenimiento. Cuentas propuestas a Exonerar
- Consulta general de Exoneración

LOGISTICA-BIENES CORRIENTES (obsoleto) 1.

MEPECOS – BANCOS 1.
SUTE 2.

- Envió de Archivos
- Consulta Totales

NOTAS DE CARGO/ABONO 1.
SIMA 2.

- Impresión de Notas / Municipalidades

ORACLE FINANCIALS (SAI) 1.

PAGO ELECTRÓNICO DE FACTURAS 1.
POCC 2.

- Movimiento de Entidades

- Mantenimiento de Proveedores
- Consulta de factura
- Reportes

PEDIDOS DE DIRECTORIO (Directorio) 1.
PERMISOS Y MOVILIDADES (Dpto. Informática) 2.
PREFACTURACIÓN DE ATMs (Dpto. Informática) 3.
4.
5.

PRICOS-SUNAT 1.

- Envío de Archivos
- Consulta Total de Acumulados

QUEJAS Y CONSULTAS 1.
AISR 2.

- Quejas
- Consultas

REPORTES BALANCE COGT 1.
GOGT 2.

REPORTES NUEVA TARJETA MULTIRED 1.
ATCA 2.

ROL VACACIONAL 1.
RHRV 2.

- Ingreso de Rol Vacacional
- Modificación de Rol Vacacional
- Eliminación de Rol Vacacional
- Impresión de Rol Vacacional
- Consulta

SALDO DE CAJEROS AUTOMATICOS 1.
AISC 2.

- Consulta por Agencia (Local)

· Consulta General

SISTEMA DE OPERACIONES A NIVEL NACIONAL 1.
SION 2.
Reportes 3. i.

SISTEMA CARTA FIANZA 1.
SISTEMA COLD (División de Producción) 2. 3:
SISTEMA DE ADMINISTRACIONES MASIVAS 4. 5:
SISTEMA DE TRAMITE DOCUMENTARIO (STD) 6. 7:

SISTEMA DE RECAUDACION – CARATULA DE LOTES 1.
READ 2.

SISTEMA UNICO DE CLIENTES (Nuevo) 1.
SIUC 2.

SUMATORIA ATM´s DIEBOLD) 1.
AISC 2.

TRANSFERENCIA RT-SUNAT 1.
SUTE 2.

VACACIONES (Sección Registro Personal) 1.

OTROS

SISTEMA DE EVALUACION DE DESEMPEÑO

SEDL 1.

· Realizar Evaluaciones
· Configurar Periodos de Evaluación
· Consulta de Evaluaciones Propias.

ANEXO 2. ARQUITECTURA

Modelo de administración

El modelo de administración de identidades permite focalizar los recursos humanos en áreas que ofrezcan mayor estrategia para la institución. Asimismo introducir nuevos roles y responsabilidades que vigilen el buen funcionamiento del manejo de identidades. Se necesita entonces considerar recursos que manejen la infraestructura central del manejo de identidades y acotar la interacción de las áreas involucradas (HelpDesk, Seguridad de la Información, etc) con esta infraestructura central dadas las actividades de mantenimiento que ella misma realiza de manera automática. Asimismo, puesto que la arquitectura considera elementos que se interrelacionan con los roles de la organización, ofrecerá un punto central para el monitoreo y auditoria de la operación y los intereses del Banco de la Nación.

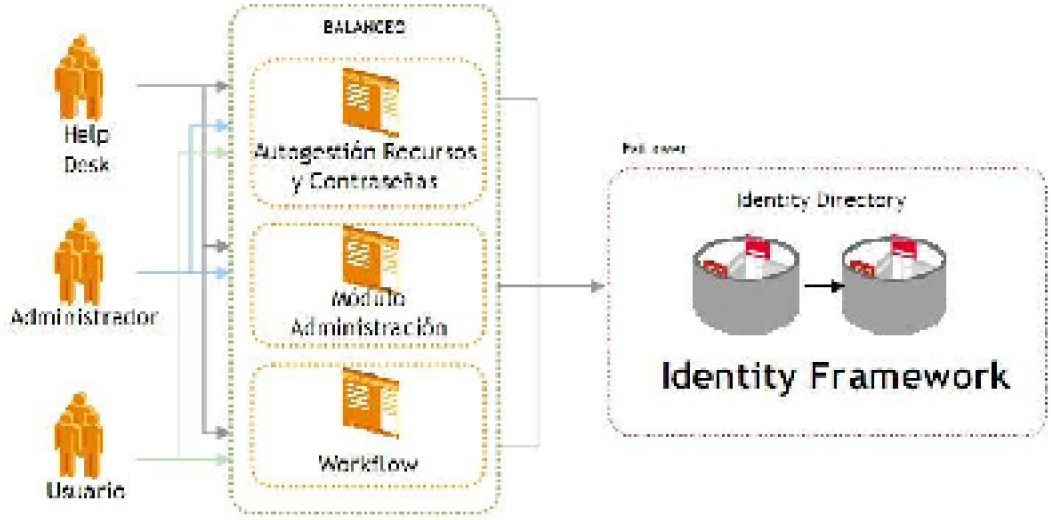

Figura. Modelo de Administración de Identidades.

Arquitectura de identidades y seguridad

La arquitectura de seguridad del Banco de la Nación consistirá en un modelo de arquitectura multi – hilos basada en un sistema central de manejo de identidades. En el siguiente diagrama se muestra el modelo de seguridad definido.

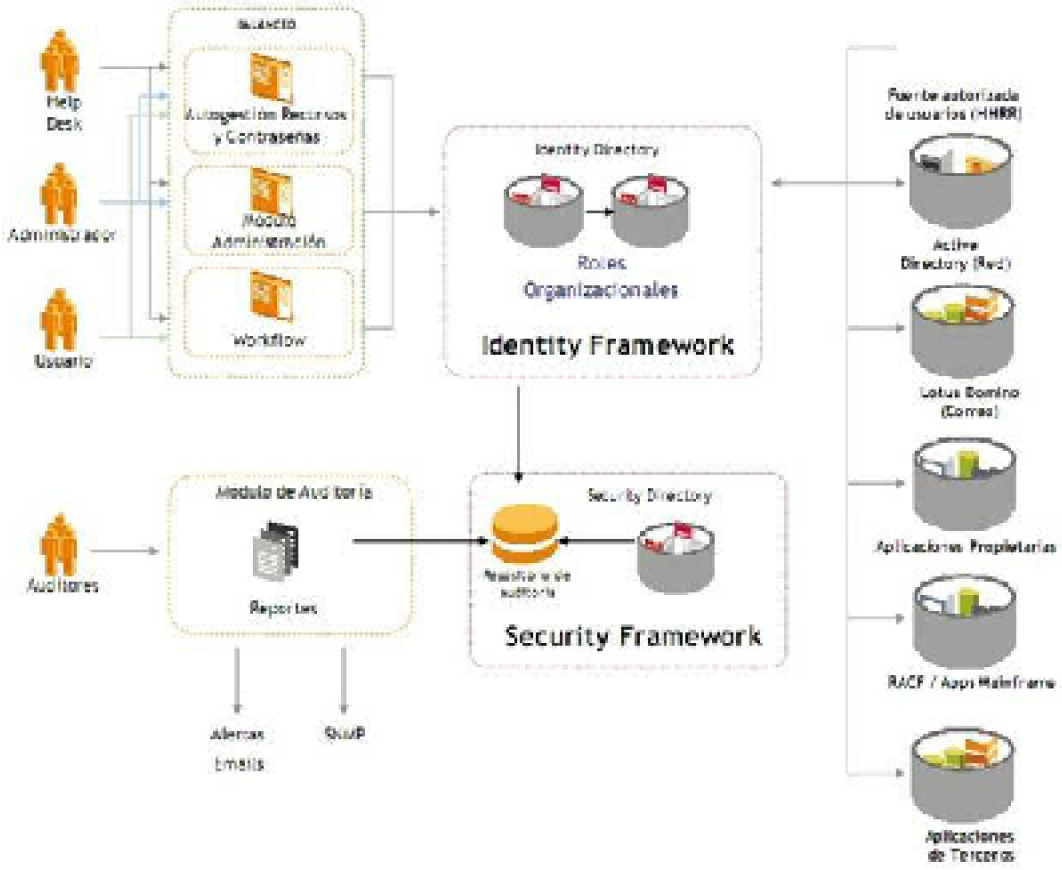

Figura. Modelo de Seguridad

En el centro de la arquitectura se encuentra un directorio basado en LDAP que almacena la mayoría de las identidades de usuarios que se conectan con los sistemas del BN. El directorio servirá como hub de la infraestructura de seguridad de integración, el cual habilitará un punto central para el aprovisionamiento y administración de usuarios. Dentro del contexto de esta solución, el nuevo Repositorio Central de Identidades es referido como “MID” (Master IdentityDirectory) o “Meta directorio”

El MID será conectado con las aplicaciones y sistemas del BN, por medio de un motor de administración de identidades. Los eventos generados en el Meta directorio tales como la adición de una nueva cuenta o modificación de la información de un usuario ya existente será replicada automáticamente a cualquiera de los sistemas conectados en los cuales el usuario tenga una asociación.

Otras de las funciones primarias de la arquitectura es el manejo seguro de identidades del BN es la implementación de un módulo de auditoría que permita registrar

todos los eventos de seguridad para luego poder ser consultados y generar reportes relacionados con la administración de identidades y accesos.

Arquitectura lógica

La arquitectura del manejo de Identidades para el BN se deriva de principios y características que permiten definir módulos con funciones específicas. Para este fin, se utiliza una arquitectura por capas, donde cada capa tiene su propio propósito y funcionalidades y que pueden ser implementados utilizando distintas tecnologías y técnicas. La arquitectura por capas tiene el principio de “Separación de Intereses” Esto hace que la implementación de esta arquitectura sea más manejable y más flexible, también permite una entrega efectiva de los servicios de directorios y una rápida actualización o reemplazo, según sea necesario.

Los componentes que incluyen la Arquitectura del Manejo de Identidades para el BN son:

- Capa de interfaces de accesos.
- Capa de aplicación.
- Capa de servicios.
- Capa de directorio.
- Capa de base de datos.
- Capa de conectividad con recursos.

A continuación se detalla la representación lógica de la arquitectura de manejo de identidades del BN incluyendo las seis capas de mayor relevancia de la arquitectura que soportará la solución.

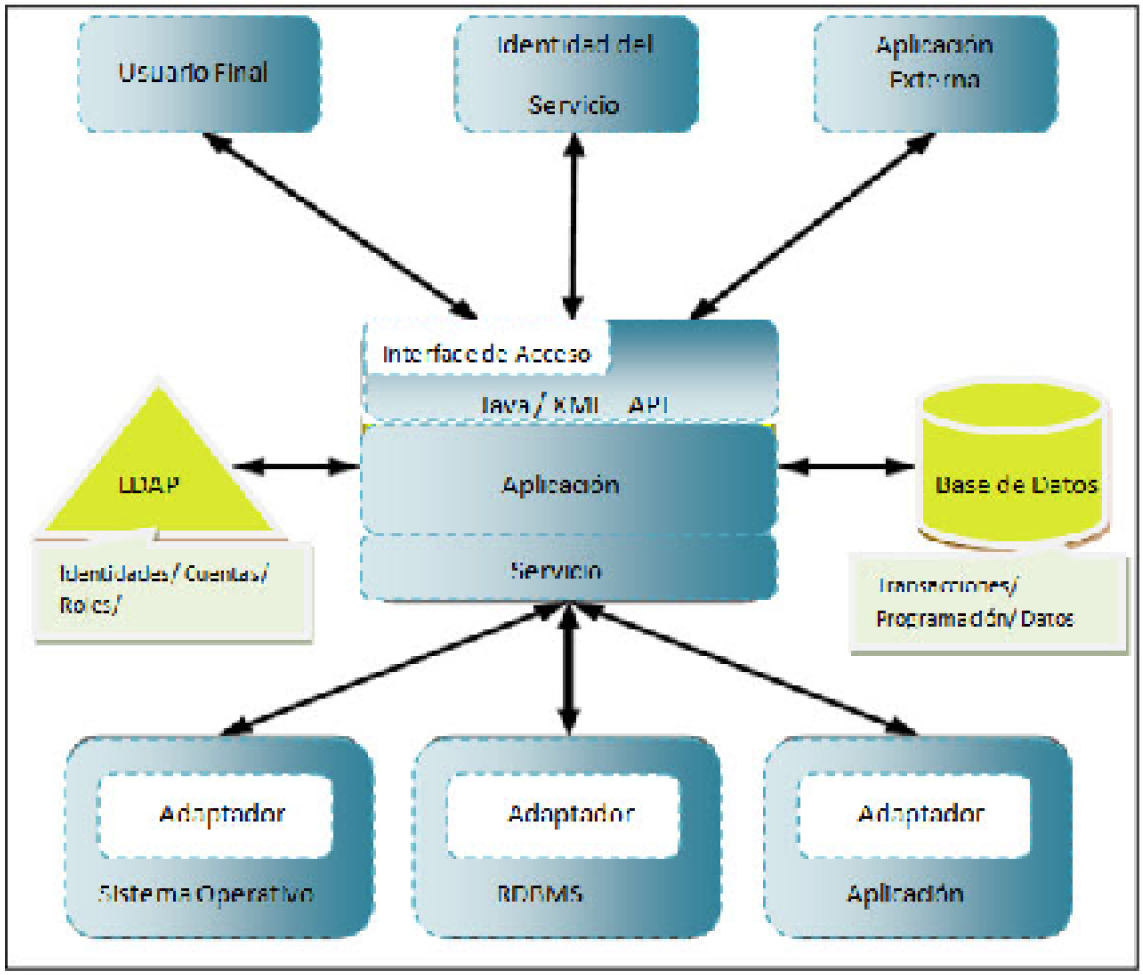

Figura. Arquitectura Lógica.

Capa de interfaces de accesos

La interfaz Web de usuarios es un conjunto de sub procesos que proporcionan todas las aplicaciones disponibles en esta capa al navegador del usuario

Capa de aplicación

Esta capa es la interfaz externa remota utilizada para acceder a todas las funciones de aprovisionamiento disponible públicamente. Este sub sistema de aplicaciones contiene todos los módulos que proporcionan las capacidades específicas de aprovisionamiento, como la administración de identidades, cuentas y políticas. Cada aplicación utiliza los servicios base en la capa de servicios para lograr su funcionalidad.

Este módulo de aplicaciones es quien proporciona la interfaz externa para aprovisionar las diversas plataformas a integrar.

Capa de servicios

El sub sistema de servicios base contiene todos los módulos que proporcionan los servicios generales que se utiliza para el aprovisionamiento, como la autenticación, autorización, workflow y forzamiento de políticas.

Capa de directorio

La solución utiliza un directorio LDAP versión 3 como su principal repositorio para almacenar el estado actual de la empresa que está administrando. Esta información del estado incluye las identidades, cuentas, roles, árbol de la organización, políticas y workflows.

Capa de base de datos

La solución utiliza una base de datos relacional para almacenar información de todas las transacciones, reportes y horarios de tareas. Normalmente esta información es temporal y es utilizada por las transacciones en ejecución, pero también contiene información histórica que es almacenada indefinidamente para efectos de auditoría de todas las transacciones ejecutadas en la solución.

Capa de conectividad con recursos

La solución proporciona una capa extensa para adaptarse a estas diferencias con la finalidad de comunicarse directamente con el recurso. Para proporcionar una mejor alternativa computacional distribuida

Arquitectura física

El siguiente cuadro muestra la arquitectura física de la solución.

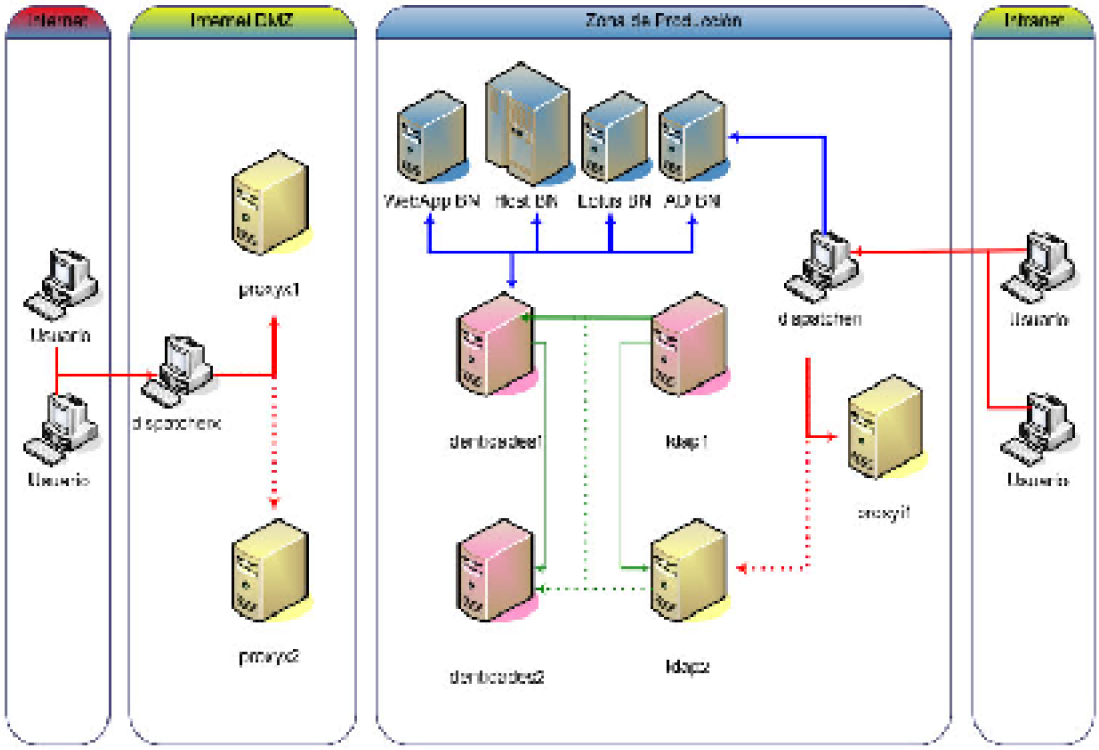

Figura. Arquitectura Física.

La función de cada uno de los elementos se describe en el siguiente cuadro.

Nombre de máquina	Sistema operativo	Productos Tivoli	Función
dispatcher	Windows XP Pro	Dispatcher, TAMESSO Console	Provee los mecanismos de conexión HTTP y HTTPS a alguno de los proxies reversos que se encuentran en la red de servidores. Alberga la consola de administración de TAMESSO
dispatcher2	Windows XP Pro	Dispatcher	Provee los mecanismos de conexión HTTP y HTTPS a alguno de los proxies reversos que se encuentran en la DMZ
identidad1	SUSE 9	TIM, TAM - Policy Server, TEC	Servidor que mantiene las políticas de seguridad Web y de identidades. También mantiene el motor de correlación de eventos.
identidad2	SUSE 9	TIM, TAM - Policy Server, TEC	Servidor que mantiene las políticas de seguridad Web y de identidades. También mantiene el motor de correlación de eventos.
ldap1	Windows 2003	LDAP Master, TIM Adapters, IIS	Mantiene el repositorio de usuarios y las identidades para el aprovisionamiento de cuentas y alberga la consola de Password Reset de TAMESSO
ldap2	Windows 2003	LDAP Replica, TIM Adapters, TAM - WebSEAL	Mantiene el repositorio de usuarios y las identidades para el aprovisionamiento de cuentas. Además realiza la función de proxy reverso de backup para los usuarios de Internet
proxy1	SUSE 9	TAM - WebSEAL	Proxy Reverso para los los servicios HTTP y HTTPS. Punto de acceso y autorización para los servicios Web que ofrece el banco.
proxy1	SUSE 9	TAM - WebSEAL	Proxy Reverso para los los servicios HTTP y HTTPS. Punto de acceso y autorización para los servicios Web que ofrece el Banco.
proxy2	SUSE 9	TAM - WebSEAL	Proxy Reverso para los los servicios HTTP y HTTPS. Punto de acceso y autorización para los servicios Web que ofrece el Banco.

Figura. Detalle de los elementos de la Arquitectura Física.

Arquitectura y alta disponibilidad de la solución

La alta disponibilidad la definimos como la combinación de elementos de software y hardware para minimizar caídas del servicio, a través de la rápida restauración de los servicios esenciales, cuando un sistema o aplicación falla.

Requerimientos de Disponibilidad de Servicios

Los requerimientos de alta disponibilidad exigidos por cada uno de los servicios críticos que conforman la solución. En cada caso se indica el tiempo de interrupción máximo aceptable por el Banco.

SERVICIO	TIEMPO MÁXIMO
Aprovisionamiento de Identidades	30 minutos
Single SignOn	2 minutos
Control de Acceso Web	1 minuto
Contención de Privilegios de Usuarios	1 minuto

Figura. Cuadro del tiempo máximo de interrupción.

Arquitectura para alta disponibilidad

El objetivo es reducir al mínimo el tiempo de caída de los servicios de la solución, utilizando para ello los componentes de software disponibles con la familia de productos IBM Tivoli y evitando en lo posible la dependencia de componentes de alta disponibilidad de sistemas operativos o de hardware. El diseño está orientado a cumplir con los requerimientos de alta disponibilidad señalados en los “Requerimientos de Disponibilidad de Servicios”

ANEXO 3. DISEÑO

Gestión de usuarios centralizada

La Gestión de Accesos e Identidades es el proceso de gestionar la información de la interacción de un usuario con una organización. Es una elemento importante en la seguridad y vital para mantener el ambiente e-business. Sin una solución de Gestión de Accesos e Identidades puede ocurrir problemas cuando los usuarios (empleados, clientes, proveedores…) requieren acceso a los recursos IT. Los beneficios de centralizar el control de la gestión de usuarios, permitiendo también la administración descentralizada, afecta dos áreas de negocio importantes: los costos de gestión de usuarios pueden ser reducidos y las políticas de seguridad pueden ser forzadas a cumplirse.

Las capacidades de la solución de Gestión de Accesos e Identidades pueden ser clasificadas en ocho niveles. Estos niveles pueden ser agrupados en una pirámide como en la figura mostrada, la base de la cual es la funcionalidad básica en la solución de aprovisionamiento. Después de cumplir los niveles más bajos en la pirámide, se toman los siguientes niveles que proveen mayores funcionalidades. La solución de Gestión de Accesos e Identidades propuesta hace posible el cumplimiento de los primeros 7 niveles, y facilita la integración del nivel de relacionado a identidades federadas (Nivel 8).

Figura. Niveles de la Gestión de Accesos e Identidades

- Adaptadores para acceder a los sistemas controlados
- Realiza la integración entre ITIM y los sistemas mencionados en las bases de la licitación con la finalidad de poder aprovisionar, modificar, eliminar y auditar usuarios.
- Gestión de claves
- Permite manejar las claves de acceso de forma centralizada, aplicando políticas de seguridad a las mismas para evitar el uso de claves débiles.
- Manejo de los derechos de acceso
- Permite tener control de los derechos de acceso que poseen los usuarios. De forma centralizada se puede controlar el acceso de los usuarios de la organización.
- Aprobación de requerimientos de acceso y automatización de procesos
- La Gestión de Accesos e Identidades y Control de Acceso, al ser un componente vital

de seguridad, requiere el uso de flujos de trabajo que permitan la asignación o revocación de permisos.

- Auditoria de accesos
- Permite controlar de manera centralizada los accesos concedidos a todas las cuentas que forman parte de los sistemas controlados por la herramienta de gestión de identidades.
- Administración delegada
- Para facilitar la administración de todos los usuarios del banco, se proporciona la facilidad de delegar la administración de los mismos. Esto permite disminuir la carga de trabajo del administrador de ITIM y acelerar los procesos administrativos.
- Automatización de políticas
- Las políticas de identidades se realizarán de manera automática, pudiendo forzarse el cumplimiento de las mismas o realizar reportes de incumplimiento.
- La automatización también se lleva a cabo mediante la asignación automática de roles, mediante los cuales se concede a la persona derechos de acceso a los sistemas controlados por ITIM o la revocación de los mismos según sea la definición del rol.
- Control de identidades federadas
- El control de identidades federadas permite la Gestión de Accesos e Identidades a través de diferentes instituciones.
- Esta etapa no está contemplada, sin embargo se dejan los cimientos para la implementación futura por parte del banco.
- Adaptadores para acceder a los recursos administrados
- Para lograr el aprovisionamiento de usuarios, la solución debe comunicarse de manera segura con cada uno de los sistemas destino que serán integrados a la solución. Si el adaptador no existe, entonces un administrador debe realizar los cambios de manera manual. Los adaptadores son los componentes clave que traducen los comandos de aprovisionamiento de la solución al lenguaje que maneja el recurso administrado. El adaptador debe soportar las necesidades de los recursos administrados y las necesidades de la organización para la creación y modificación de cuentas.
- La comunicación entre la Solución de Aprovisionamiento y el Recurso Administrado es bidireccional, segura y eficiente en el uso de ancho de banda. La bidireccionalidad es crítica para capturar los cambios realizados directamente en el Recurso Administrado y reportar los cambios a la solución de aprovisionamiento para su evaluación y acción. El enlace es encriptado para mantener la confidencialidad de la información de autenticación y evitar el robo de claves. Se utilizan enlaces SSL para mantener la confidencialidad de los datos. Este enlace además permite la autenticación para evitar la inyección de comandos por un impostor para crear cuentas no deseadas.

· El esquema general de arquitectura para los adaptadores es el siguiente:

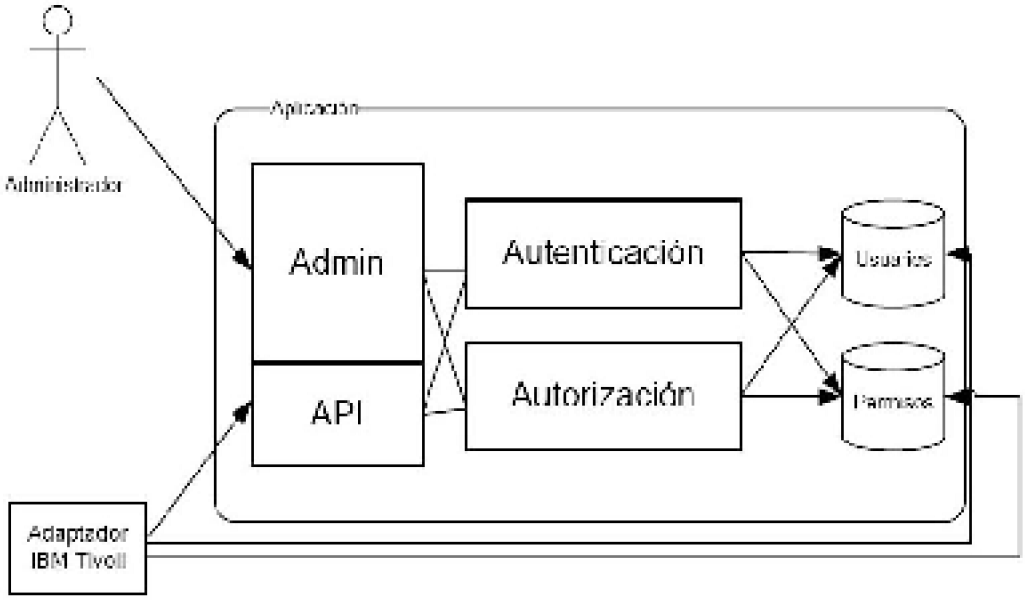

Figura. Arquitectura general de integración con aplicaciones para aprovisionamiento

.

· La administración sin una solución para la Gestión de Accesos e Identidades es realizada por el administrador de la aplicación. En cuanto a operaciones relacionadas a la gestión de identidades, las operaciones son:

· Crear

· Modificar: Cambios de atributos, clave y bloqueo

· Eliminar

· Auditar (reconciliar).

· Estas operaciones son realizadas por el administrador de la aplicación, con la solución de Gestión de Accesos e Identidades estas operaciones son realizadas por

el Adaptador el cuál realiza las mismas funciones como un Administrador Virtual.

- Cuando hablamos de recursos administrados, se hace referencia a dos tipos de repositorios:
- Repositorio de Personas: El repositorio de personas mantiene información acerca de la gente que tiene relación con la organización. En nuestro caso el Repositorio de Personas será la base de datos de Recursos Humanos, la cuál será accedida a través de JDBC.
- Repositorio de cuentas: Los repositorios de cuentas mantienen información de cuentas y privilegios. Para el proyecto de Gestión de Accesos e Identidades y Control de Acceso se tendrán en cuenta los Repositorios de Cuenta mencionados:
- Cuentas Corrientes
- Ahorros
- Préstamos
- TAND
- INCA
- Correo Lotus
- Exchange
- Active Directory
- RACF

- Considerándose los tres primeros dentro de la aplicación SaraWeb.
- Gestión de claves
- La Gestión de Claves es la habilidad de controlas la calidad de la clave y el cambio de la misma a través de los Recursos Administrados. Con el crecimiento en la cantidad de aplicaciones, cada vez es mayor el número de claves que el usuario tienen que gestionar lo cual incrementa el riesgo de robo de claves ya que los usuarios tienden a escribir sus claves. Otro riesgo es el olvido de claves lo cual según investigaciones genera aproximadamente el 30% de llamadas a Mesa de Ayuda.
- Una clave fuerte es otro de los problemas comunes. Los hackers poseen herramientas para averiguar claves poco complejas. Con la implementación de la Gestión de Accesos e Identidades se abre la posibilidad de controlar la complejidad de las claves en los múltiples recursos administrados.
- La Gestión de Claves habilita a los usuarios a realizar un autoservicio de sus claves. Para ello se implementará un sistema basado en Web. Los usuarios de deben ingresar a través de navegador Web, autenticarse y luego pueden cambiar su clave en todas sus cuentas. La clave que manejan es forzada a cumplir las políticas de Clave establecidas, la cuales son:
- Longitud mínima de 6
- Longitud máxima de 8

- Al menos 2 dígitos
- No podrá ser igual al userid
- No podrá ser igual a las últimas 5 claves utilizadas.
- Se forzará al cambio cada 60 días a través de la interfaz de ITIM.

- Dado que el uso de AD es extendido en todo el Banco, el forzamiento de cambio de clave se realizará en AD y un componente de sincronización de claves del sistema de Gestión de Accesos e Identidades realizará la validación de esa clave con las políticas generales y la sincronizará con las cuentas que pertenecen al usuario.
- Puntos clave en la Gestión de Claves que se implementarán:

- Autoservicio para cambio de clave a través de interfaz Web.
- Reto-respuesta para autenticar al usuario en caso de olvido de clave.
- Implementación de reglas para claves para forzar el uso de claves fuertes.
- Sincronización de claves para los recursos administrados.
- Responsabilidad de derechos de acceso

Llevar el seguimiento de quién tiene acceso a qué información a través de la organización es un función crítica en la solución de aprovisionamiento. No sólo permite el control de sistemas críticos sino que expone todas las cuentas que no tienen permisos no autorizados o autorizaciones que ya no son necesarias. Estas cuentas representan un serio problema para la seguridad de la organización porque son cuentas válidas y activas que no pueden ser detectadas como un ataque tradicional.

Las cuentas huérfanas son aquellas cuentas encontradas en los Recursos Administrados que no han podido ser asociadas a una persona válida. Estas cuentas pueden aparecer en cualquier momento debido al uso de las consolas de los Recursos Administrados. La clave para evitar la cuentas huérfanas es realizar continuamente la asociación de cuentas con personas, ya que la asociación automática que realiza el sistema de Gestión de Accesos e Identidades puede no asociar algunas de ellas debido a que son procesadas satisfactoriamente por los scripts que realizan la asociación.

Las cuentas configuradas incorrectamente son aquellas asociadas con la persona correcta pero que tienen autorizaciones inapropiadas. La gestión manual de cuentas configuradas incorrectamente es difícil, ya que requiere la comparación de lo que debe ser con lo que hay.

La cuentas huérfanas y las configuradas incorrectamente sin un sistema de Gestión de Accesos e Identidades pueden ser reportadas como correctas. El sistema de Gestión de Accesos e Identidades identificará aquellas cuentas de manera automática, facilitando las tareas de auditoria relacionadas a la gestión de identidades.

La Responsabilidad de Derechos de Acceso incluye:

Mecanismos de conexión a los Repositorios de Cuentas mencionados:

- Cuentas Corrientes
- Ahorros
- Préstamos
- TAND
- INCA
- Correo Lotus
- Exchange
- Active Directory
- RACF

Considerándose los tres primeros dentro de la aplicación SaraWeb, TAND e INCA están considerados como parte de Sistema de Claves. En adelante la referencia a Repositorios de Cuenta o Recursos Administrados considera las aplicaciones y sistemas mencionados.

Programación del mecanismo para cargar la información de los Repositorios de Cuentas de manera diaria.

Detección de cambios en los Repositorios de Cuentas y respuesta en tiempo real a los cambios detectados.

Comparación de la información de los Repositorios de Cuentas con las políticas de aprovisionamiento que deben cumplir.

Detección de las cuentas que no están asociadas a una persona, es decir detección de cuentas huérfanas. Las cuentas huérfanas serán consideradas aquellas que no pueden asociarse de manera automática a una persona. La asociación automática se realizará mediante el userid de la cuenta.

Facilidad para la eliminación de cuentas huérfanas.

La posibilidad de forzar al cumplimiento de las políticas de aprovisionamiento. Esta opción puede realizarse una vez se hayan cargado todas las políticas de aprovisionamiento y se haya realizado la verificación que realmente se necesita realizar el forzamiento de políticas de aprovisionamiento sin que estas afecten el funcionamiento normal de la empresa (dado que se pueden eliminar grupos o cuentas para cumplir con las políticas de aprovisionamiento)

Reportes de las cuentas huérfanas.

Capacidad para ver los recursos y cuentas asociadas a una persona.

Capacidad para asignar cuentas huérfanas a una persona válida.

- Automatización de procesos y aprobación de requerimientos de acceso

La Automatización de Procesos y Aprobación de Requerimientos de Acceso es un componente clave en el cambio de derechos de acceso de forma rápida y precisa. Los procesos de aprobación son una forma especializada de workflows que determinan,

basados en las políticas organizacionales, la necesidad de aprobar un requerimiento de derechos de acceso antes de su ejecución. Algunas organizaciones todavía dependen de autorizaciones en papel y correo electrónico que deben recorrer diferentes rutas para su aprobación.

Estos enfoques de aprobación son bastante lentos. Los requerimientos pueden incluso rechazarse por falta de información, lo cual implica el nuevo inicio del proceso. La solución de Gestión de Accesos e Identidades provee de workflows que automáticamente enlutan los requerimientos a los aprobadores y realizan el escalamiento en caso no se hayan tomado acciones específicas en un tiempo determinado. Estos workflows automatizados pueden convertir un proceso que tarda típicamente semanas en uno que tarde sólo minutos.

Usualmente se requiere información adicional en los requerimientos, esta información puede ser ingresada durante la ejecución del workflows mediante el uso de los RequestforInformation (RFI) que proporciona la solución de Gestión de Identidades.

La Automatización de Procesos y Aprobación de Requerimientos de Acceso incluye las siguientes características:

Enrutamiento automático de aprobaciones para acceso a los recursos.

Capacidad para delegar la aprobación a otras personas.

Capacidad para escalamiento de aprobaciones a otro aprobador si ha pasado un tiempo mayor a 4 horas.

Capacidad para establecer que información puede ver cada persona.

Facilidad de creación, diseño y modificación de workflows vía interfaz gráfica

Facilidad para la solicitud de información adicional durante el desarrollo del workflows mediante el uso del componente de requestforinformation.

Los workflows serán definidos en la etapa de procesos

- Acceso a registros de auditoria

Tradicionalmente muchas organizaciones utilizan los registros de auditoría para ver la causa de las brechas de seguridad descubiertas. Esta forma de uso es inadecuada, ya que el uso de la información debe realizarse en todo momento, monitoreando y reaccionando de acuerdo a la información para evitar las brechas de seguridad.

La solución de Gestión de Accesos e Identidades brinda un registro de auditoria en formato XML que puede ser utilizado por la herramientas de monitoreo que tenga en uso la empresa para evitar posibles brechas de seguridad.

La información proporcionada será registros con fecha y hora de:

Requerimientos de cambios de acceso, aprobaciones y rechazos.

Cambios administrativos a derechos de acceso.

Acceso a la interfaz Web.

- Administración distribuida

La Administración Distribuida permite que las tareas administrativas relacionadas con el aprovisionamiento, sean manuales o automáticas, ser distribuidas de manera segura entre las unidades organizaciones de la empresa. Esta característica es importante por dos razones: precisión y escala. Es recomendable mover los procesos de requerimientos y aprobación cerca de las personas que realmente conocen la necesidad de un individuo de tener acceso a los recursos.

La distribución también permite balancear la carga de trabajo a lo largo de varios administradores en lugar de un único administrador con toda la carga de trabajo.

Un aspecto fundamental en la delegación de administración es filtrar la información presentada al administrador, sólo se le presentará la información pertinente.

La Administración Distribuida incluirá:

La posibilidad de asignar a un administrador a cada una de las unidades organizacionales definidas en el Árbol Organizacional que proporcionará RR.HH.

Posibilidad para definir un control granular (por ejemplo aprobación, creación de usuarios, definición de workflows).

- Automatización de políticas

La Automatización de Políticas es la forma de evaluar y forzar las reglas del negocio para conceder accesos. El método de conceder accesos a los usuarios es Role Based Access Control (RBAC), el cuál define los accesos de las personas de acuerdo a su pertenencia a roles.

La automatización es la clave para la gestión de una gran cantidad de usuarios a través de la empresa, ya que estos a la vez tienen acceso a gran cantidad de recursos lo que dificulta la gestión manual. La solución permitirá la asignación de roles. Los derechos de acceso para los usuarios pertenecientes a un rol serán definidos en las políticas de aprovisionamiento.

Los siguientes elementos serán considerados en la implementación:

Se crearán 50 roles organizacionales.

- Los roles organizacionales creados permitirán conceder acceso a los recursos que define el rol.
- El cambio de rol sólo hará efectivo cambios en los accesos cuando se realice el forzamiento de cumplimiento de políticas en los recursos.
- Mientas no se realice esta acción, los roles sólo realizarán la concesión de accesos cuando se asignen por primera vez.
- Los roles organizacionales creados se asignarán de manera automática a las personas. La asignación de los roles se realizará de acuerdo a los atributos de la persona, estos serán: área, código de puesto y ubicación, capacidad para asociar los derechos de acceso con un rol organizacional.

- Capacidad para asignar a uno o más usuarios a uno o más roles.
- Capacidad para asignar recursos que no estén disponibles a determinados roles.
- Capacidad para automáticamente realizar cambios en los derechos de acceso una vez realizado el cambio de roles, siempre que los recursos se encuentren en modo de forzar cumplimiento de políticas.
- Capacidad para realizar reportes de roles, los derechos asociados con ellos y los usuarios asociados a un rol.
- Capacidad para crear usuarios consistentes con las políticas de la empresa y que no se encuentren en uso.
- Capacidad para extender o limitar los derechos de acceso de acuerdo a la pertenencia a roles, siempre que los recursos se encuentren en modo de forzar cumplimiento de políticas.
- Capacidad para considerar atributos de cuenta como opcionales y mandatarios.
- Capacidad para crear el usuario de acuerdo a un algoritmo definido por la organización.

- Procesos del negocio y gestión de identidades

La solución de Gestión de Accesos e Identidades compromete funcionalidades de negocio (procedimientos) y técnicos. La implementación abarca la instalación de una herramienta para la gestión de identidades, que incluye la integración con procesos del negocio y quizá la reingeniería de algunos procesos de negocio (BPR) con los Recursos Administrados.

La lista de procesos incluye:

- Ingreso de una nueva persona al banco.
- Otorgamiento de cuentas para acceder a los Recursos Administrados.
- Entrega de claves para autenticación de cuentas.
- Cambio de la persona en la estructura organizacional
- Cambio de la pertenencia a rol
- Cambio de claves
- Vacaciones de una persona
- Reseteo de clave por un administrador
- Desbloqueo de cuentas
- Bloqueo de cuentas
- Eliminación de cuentas para una persona.
- Cambios en las políticas de aprovisionamiento.
- El diseño e implementación de los procesos involucra:
- El departamento de seguridad.

- Administradores de sistemas. Incluye a los administradores de seguridad, mesa de ayuda y soporte técnico.
- Usuarios. Incluye a todos los que tienen o pueden tener acceso a los Recursos Administrados por el sistema de Gestión de Identidades.

La Gestión de Accesos e Identidades con el uso de IBM TivoliIdentity Manager consolidará, aprovisionará y gestionará las identidades a lo largo de todos los Recursos Administrados. Con la implementación de la solución se logrará:

- Facilidad para cumplir con los requerimientos de auditoría.
- Consolidar el control de los procesos de control de usuarios.
- Eliminar inconsistencias por error humano con el uso de workflows automatizados.
- Reducir el costo de entrenamientos para administrar plataformas diversas.
- Reducir llamadas a mesa de ayuda por olvido de claves.
- Reducir la cantidad de personas en la administración de identidades de los recursos administrados.
- Delegar administración a unidades organizacionales.
- Mejorar el tiempo de respuesta a cambios.

- Autenticación única en estaciones de Trabajo

Tivoli Access Manager for Enterprise Single Sign-On provee autenticación única a nivel de estaciones de trabajo, introduce una capa de autenticación la cual se encarga de detectar automáticamente cualquier subsiguiente requerimiento de credenciales. TAMESSO utiliza un agente que responde a los requerimientos de credenciales de usuario para las aplicaciones Windows, Web y de host.

TAMESSO utiliza una base de datos encriptada utilizando el algoritmo Triple-DES. Los usuarios pueden utilizar sus credenciales en cualquier estación de trabajo ya que éstas se encuentran en el Active Directory del dominio.

Además, se extenderá las funciones de TAMESSO con los adaptadores:

- Desktop PasswordResetAdapter: Permite el reinicio de password por los mismos usuarios en caso de olvido de su password.
- ProvisioningAdapter: Permite la integración con la plataforma de aprovisionamiento de usuarios.
- Adicionalmente está la consola administrativa para todas aquellas tareas de administración de TAMESSO.

Los agentes para Single SignOn serán instalados en las estaciones de trabajo y el alcance del despliegue está definido en la sección Estrategia de Despliegue del Servicio de Single Sign-On

Los módulos de la arquitectura:

1) Autenticación 1.

La autenticación es como el sistema valida a los usuarios de TAMESSO. Para la implementación se considerará sólo la autenticación mediante usuario y clave.

2) Encriptación 1.

La encriptación de credenciales de usuario se realiza mediante el uso de una llave de encriptación simétrica para cada usuario. El algoritmo de encriptación utilizado será Tiple-DES.

Las credenciales son almacenadas encriptadas en el cliente, cuando están en tránsito entre el repositorio de Active Directory y la PC, en memoria y en Active Directory. El diseño modular de TAMESSO permite el uso de otras librerías de encriptación si después de la implementación fuera necesario cambiar el módulo de encriptación:

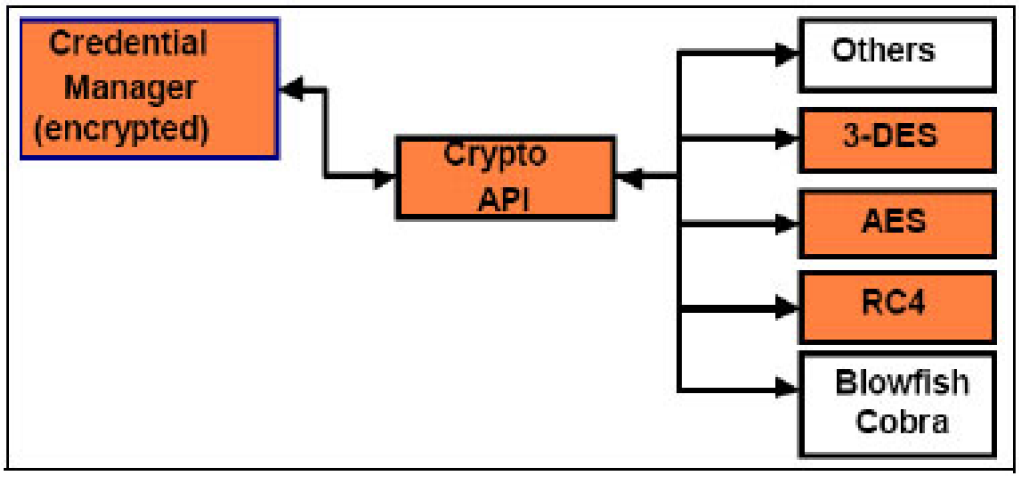

Figura. Módulo de encriptación.

3) Respuesta Inteligente del Agente 1.

Cuando una aplicación presente un requerimiento de credenciales, el agente detectará el evento, determinará la acción apropiada y entregará las credenciales correspondientes. Las aplicaciones que se entregarán configuradas para SSO son:

a. Correo electrónico Lotus Domino 1.

b. Oracle Financial 2.

c. Emuladores de Terminal 3270 3.

d. Emuladores de Terminales Unix (Telnet) 4.

e. Intranet del Banco 5.

4) Núcleo (Core) 6.

TAMESSO almacena la información de credenciales encriptadas en el almacenamiento local de credenciales. Nunca se mantiene la credencial sin encriptar, ni en disco ni en memoria. Las credenciales son almacenadas localmente en un archivo de base de datos

en cada estación de trabajo. El almacenamiento local de las credenciales permite no depender de un servidor central para poder utilizar las credenciales y adicionalmente acelera el acceso a las credenciales, ya que no hay un acceso remoto a las credenciales.

La información de credenciales es almacenada en %UserProfile%, el cuál apunta por defecto a c:\Documents and Settings\%UserName%. El archivo es almacenado como %UserName%\AML.mdb en %UserProfile%\Application Data\IBM, así por ejemplo para el usuario user1 sería: C:\Documents and Settings\user1\Application Data\IBM\user1\AML.mdb

5) Sincronización de Credenciales 1.

La sincronización de credenciales permite mantener actualizada la base de datos de credenciales de TAMESSO. Para tal efecto se utilizará la integración con la solución de Aprovisionamiento de Usuarios.

6) Registro de Eventos 1.

TAMESSO permite reportar eventos locales y remotos.

7) Componentes adicionales 1.

a) InstallerPackage 2.

Permite el despliegue de la solución con instaladores msi

b) Backup/restore 1.

Permite el respaldo y restauración del archivo de credenciales.

8) Desktop PasswordResetAdapter 1.

El Desktop PasswordResetAdapter permite a los usuarios realizar un cambio de clave desde la estación de trabajo aunque se encuentre bloqueada. Esta funcionalidad permite la reducción de llamadas a Mesa de Ayuda debido a olvido de clave.

La arquitectura del adaptador es:

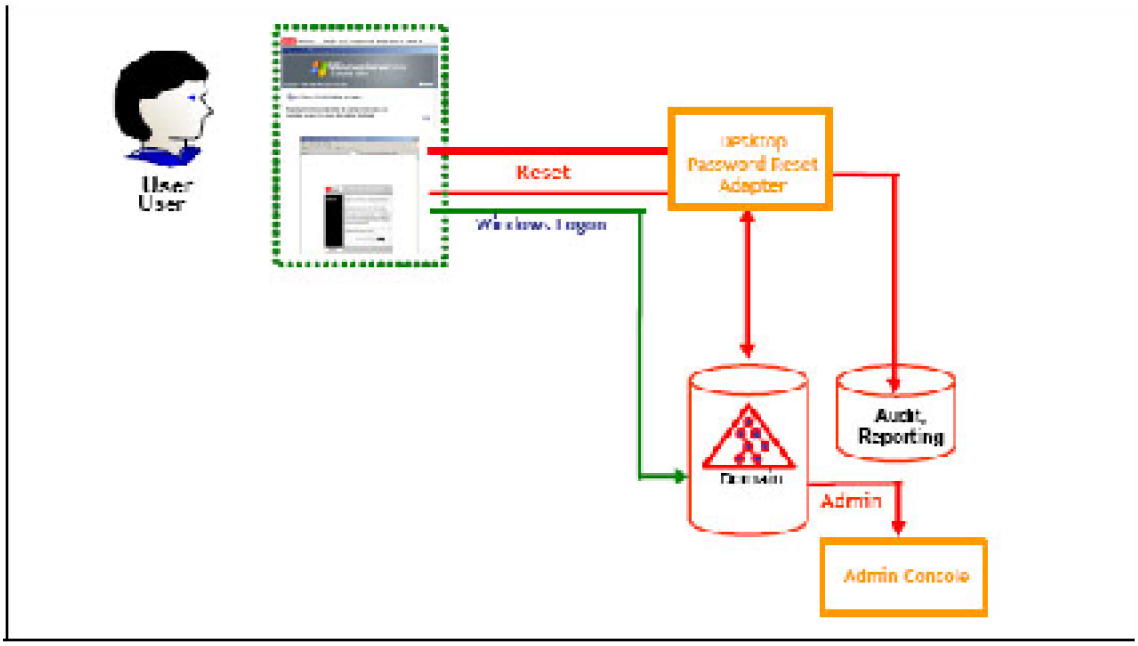

Figura. Arquitectura del adaptador.

La interfaz de ingreso a PasswordReset será la misma pantalla de autenticación de Windows:

Figura. Interfaz de ingreso.

9) ProvisioningAdapter 1.

El componente de ProvisioningAdapter automatiza el proceso de distribución de credenciales a través de la herramienta para aprovisionamiento de usuarios: TivoliIdentity Manager.

La arquitectura para del ProvisioningAdapter es la siguiente:

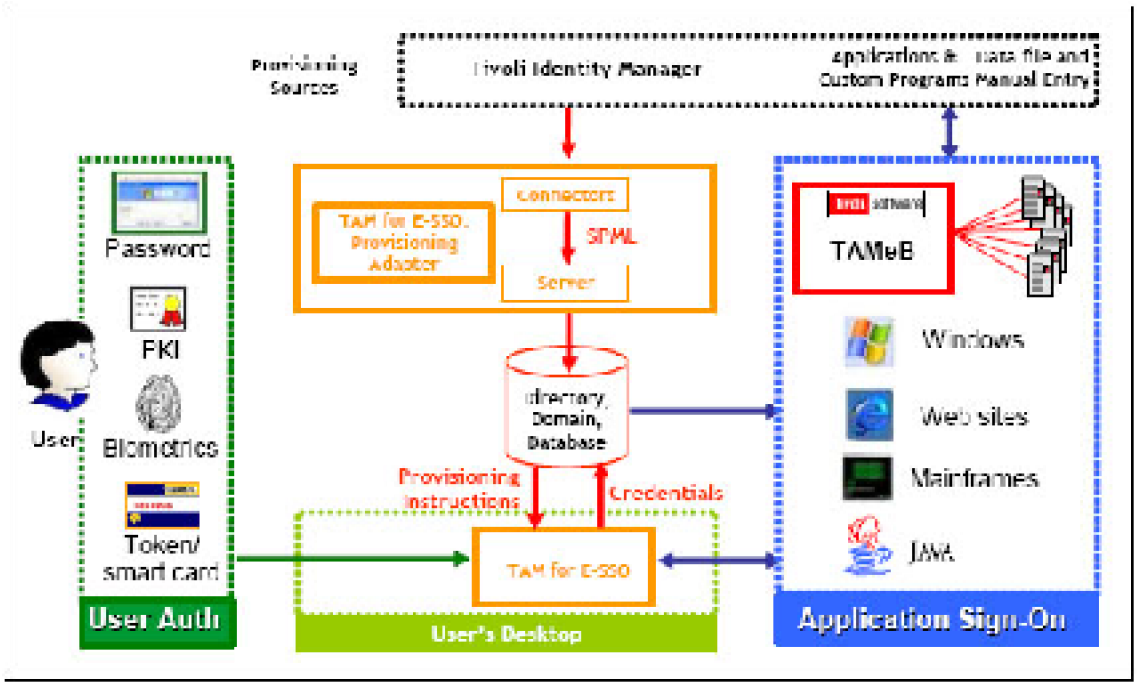

Figura. Arquitectura del ProvisioningAdapter

· Control de Acceso

En este capítulo se tratarán los módulos correspondientes al Control de Acceso para acceso a aplicaciones Web y Contención de privilegios de la cuenta root (Linux/unix). La herramienta utilizada para la solución de Control de Acceso es IBM Tivoli Access Manager, los componentes son:

1) Componentes Base, los cuales son comunes a los productos Access Manager 1.

2) Resource Manager, los cuales proporcionan la autorización para las aplicaciones Web o Sistemas Operativos. 2.

3) Componentes de Interfaz, los cuales permiten a las aplicaciones interactuar con las funciones de Access Manager. 3.

· Familia Tivoli Access Manager

IBM Tivoli Access Manager es una solución para autenticación y autorización de aplicaciones Web y Sistemas Operativos (Linux y Unix). TivoliAcess Manager realiza el control de acceso a información y recursos protegidos. Provee la solución para el control de de acceso centralizado, flexible y escalable.

Tivoli Access Manager provee:

· Framework de Autenticación

· Tivoli Access Manager provee un rango amplio de módulos de autenticación y brinda soporte a métodos de autenticación externos.

- Framework de Autorización
- El servicio de autorización en conjunto con los resource managers provee mecanismos estándares de autorización.
- Los Resource Managers para el proyecto de Gestión de Accesos e Identidades y Control de Acceso son:
- IBM Tivoli Access Manager WebSEAL
- WebSEAL maneja y protege información y recursos basados en Web. WebSEALestáincluído con Tivoli Access Manager for e-business. (TAMeB)
- IBM Tivoli Access Manager for Operating Systems
- Access Manager forOperatingSystems (TAMOS) provee una capa de para forzar políticas de autorización en sistemas Linux y UNIX en adición a los proveidos por los sistemas operativos nativos. Las aplicaciones existentes pueden tomar ventaja del servicio de autorización de Tivoli Access Manager para proveer de un servicio común políticas de seguridad para toda la empresa.

- Tivoli Access Manager for e-Business (TAMeB)

La presencia Web se ha convertido en una consideración muy importante en la mayoría de empresas. Casi todas las organizaciones utilizan la Web como una herramienta esencial para la difusión de información y como una extensión de la organización misma, la cual se integra directamente con procesos operativos. Mientas toman lugar estos cambios, la importancia en la seguridad aumenta.

En esta sección se detallan los aportes de la solución de Control de Accesos en una arquitectura que utiliza componentes Web.

- Características de Seguridad Web

Son comunes en las organizaciones colocal los servidores Web que dan cara a Internet en una zona protegida (demilitarizedzone o DMZ), la cual es generalmente separada por un firewall de Internet. La DMZ provee de una barrera entre Internet y la red interna de la corporación. Para mayor seguridad de los servidores back-end, estos son colocados en una zona de mayor protección, la red interna. Esta red a su vez está protegida por otro firewall de la DMZ

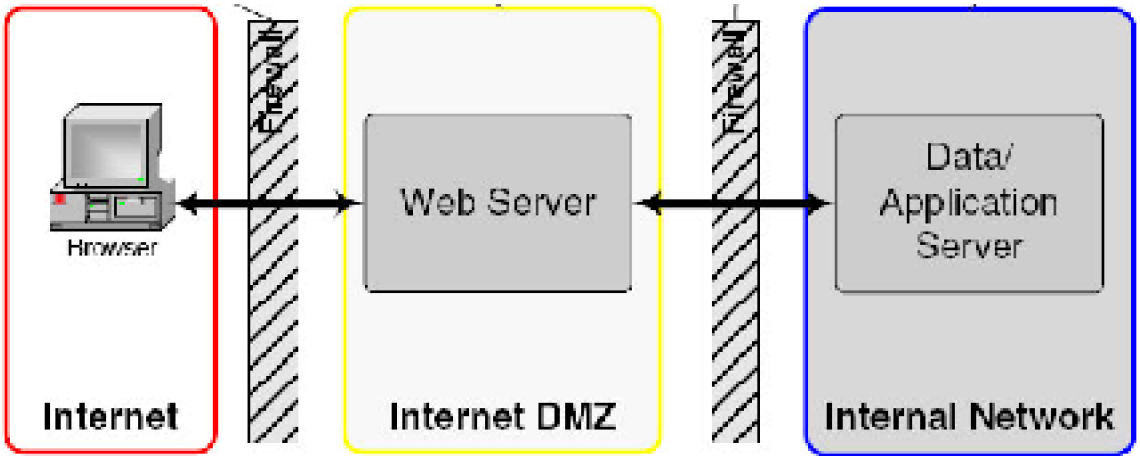

Figura. Típica arquitectura de seguridad Web.

· La típica arquitectura de seguridad Web tiene ciertas desventajas:

Los mecanismos de autenticación y autorización son manejados por cada una de las plataformas Web de la empresa.

La autenticación, autorización y auditoría no son centralizadas.

Las políticas de seguridad pueden ser inconsistentes entre los servidores Web (las políticas de control de acceso son controladas por diferentes administradores).

· Con Tivoli Access Manager for e-business se cumplen con los requerimientos que la arquitectura típica no logra:

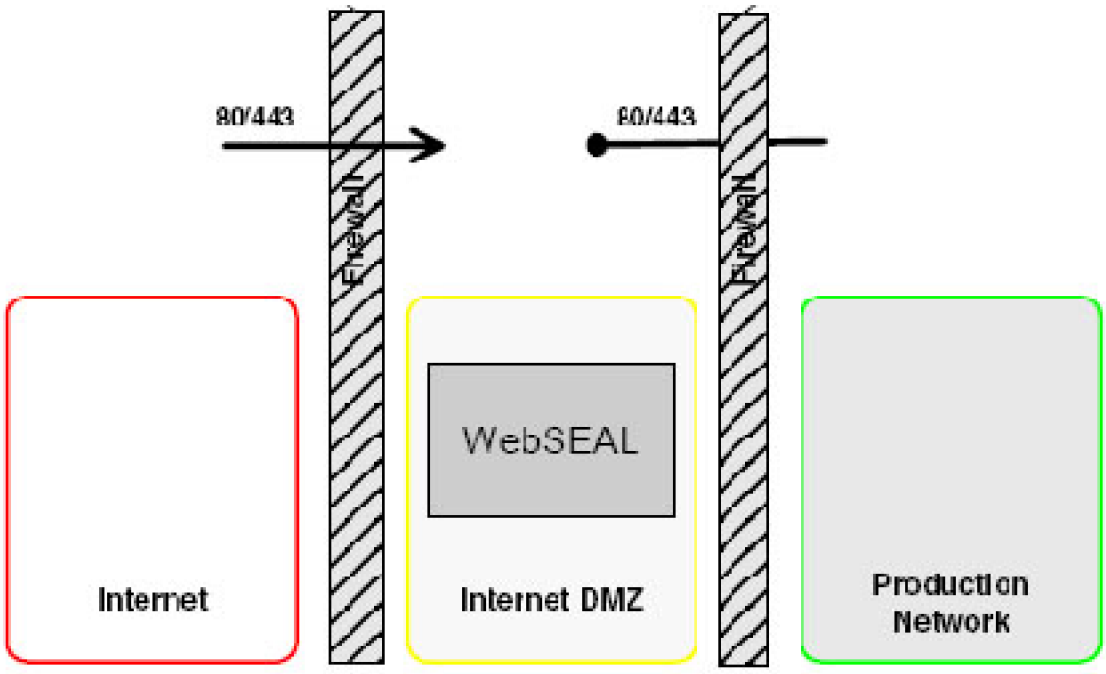

Figura. Zonas de seguridad considerando TAMeB.

· Consideraciones de diseño

La implementación de control de acceso Web tendrá la siguiente arquitectura lógica:

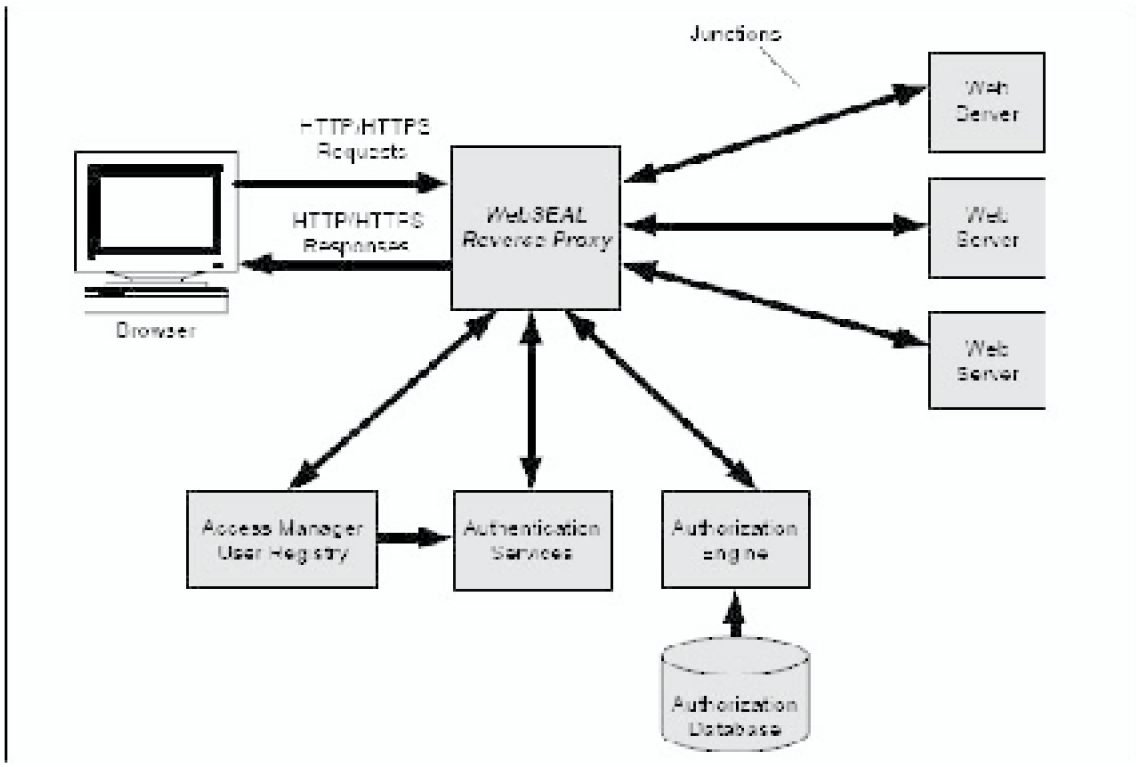

Figura. Arquitectura lógica del diseño

- El proxy reverso WebSEAL será el punto único de ingreso a los servicios Web. Éste se comunicará con los navegadores Web y enviará los requerimientos a los servidores Web o servidores de aplicaciones considerados para la implementación.
- Antes de pasar cualquier requerimiento, WebSEAL utiliza el motor de autorización para validar el acceso a los recursos Web. Si la URL no está protegida, simplemente se realiza el acceso al recurso Web. Si la URL está protegida, se realiza un control de acceso al recurso. Si el usuario no está autorizado se fuerza al proceso de autenticación para validar al usuario y verificar si tiene permiso para acceder al recurso.
- Los servidores protegidos considerados para la implementación son:
- Servicio de Intranet
- Servicio de correo Web
- Ambos recursos se considerarán recursos protegidos, para los cuales será necesario realizar la autenticación antes de poder acceder a los mismos. Una vez autenticado el usuario, éste podrá acceder a ambos recursos sin necesidad de realizar nuevamente la autenticación (SSO a nivel Web).
- La solución de control de acceso permitirá al administrador del banco realizar un control más granular sobre las URLs a las que tienen acceso determinado grupo de usuarios, correspondiendo esta tarea al banco.

ANEXO 4. IMPLEMENTACIÓN

Una vez realizada la implementación de los productos de la solución, es necesario el desarrollo de procedimientos que garanticen el correcto uso de las herramientas de Gestión de Accesos e Identidades y Control de Accesos. Asimismo se detallan algunas observaciones para tener en cuenta.

Gestión de Identidades

La herramienta IBM TivoliIdentity Manager realizará la gestión centralizada de cuentas para todas las personas que se encuentren registradas en el repositorio de RR.HH.

· Asociación de cuentas a personas: adopción

De manera automática se asignará a cada persona del Banco las cuentas que le correspondan de acuerdo a un criterio establecido. Para realizar esta asociación automática se tendrá en consideración uno o más atributos de cuenta que correspondan a uno o más atributos de persona.

Los atributos de cuenta utilizados por servicios son:

· Lotus Notes: userid
· Active Directory: código de empleado
· STCL: Código de empleado
· RACF: userid
· Saraweb: Código de empleado

Todas aquellas cuentas que no cumplan los criterios por servicio no serán asociadas a ninguna persona, denominándose éstas huérfanas.

Corresponde al Banco realizar validar que las cuentas asociadas de manera automática reflejen la realidad del Banco. Las cuentas que sean adoptadas de manera automática deben ser validadas por el banco.

· Verificación de políticas

Las políticas de aprovisionamiento de usuarios deben ser cargadas en su totalidad en ITIM. Una vez realizada esta carga, ITIM validará por cada persona que las cuentas que posee cumplan las políticas del Banco y mostrará cuáles no cumplen las políticas de aprovisionamiento del Banco.

Para todas aquellas cuentas que no cumplan las políticas, el Banco tendrá que realizar el proceso de estandarización de las mismas para adecuarlas a las políticas del Banco. Esto proceso puede realizarse:

- Cambiando la cuenta para que cumpla las políticas.
- Cambiando los roles a los cuales pertenece la persona para que pueda cumplir las políticas.

Es responsabilidad del Banco verificar la validez de las cuentas huérfanas, quedando a su criterio el mantenerlas o eliminarlas. En el caso de mantenerlas, debe realizarse la asociación de cuenta a una persona, denominándose este proceso adopción.

El proceso de adopción debe realizarse para todas las cuentas de las aplicaciones/plataformas integradas a ITIM, debiendo el Banco completar el proceso en un tiempo que considere pertinente.

Control de Accesos

- Control de Acceso Web

El Control de Acceso Web es una capa de seguridad adicional a la que proveen las aplicaciones Web. Esta capa adicional debe integrarse a la seguridad del Banco, debiendo modificarse la manera de acceso a los aplicativos Web que se maneja actualmente.

El escenario actual permite el ingreso directo desde la estación de trabajo del usuario al servidor Web.

Figura. Escenario actual de ingreso desde una estación de trabajo de la red del Banco a un servidor Web.

- Para el uso adecuado de Tivoli Access Manager for e-business es necesario se modifique la arquitectura actual, limitando el acceso directo hacia los Servidores de Aplicaciones Web. El esquema de ingreso al servidor debería ser:

Esquema de ingreso al servidor

Esto es tanto para el acceso desde Internet como desde la Intranet.