UNIVERSIDAD DE CHILE
FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS
DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

MIDDLEWARE PARA UN SISTEMA DE GESTIÓN DE IDENTIDAD EN TELEFÓNICA CHILE

TESIS PARA OPTAR AL GRADO DE MAGISTER EN TECNOLOGÍAS DE LA INFORMACIÓN

CHRISTIAN ALONSO ALVARADO SÁNCHEZ

PROFESORA GUIA:
ERIC TANTER

MIEMBROS DE LA COMISION:
ALEJANDRO HEVIA ANGULO
RAFAEL HERNANDEZ CONTRERAS
PATRICIO GALDAMES SEPULVEDA

SANTIAGO DE CHILE

2015

Resumen

La administración de cuentas de acceso en los sistemas y recursos TI (Tecnologías de Información) es una actividad compleja y costosa que actualmente preocupan a las grandes empresas. El problema radica principalmente en la coexistencia de múltiples fuentes de registros de usuario, cada uno de estos con diferentes formatos, estándares y objetivos, enfocados a responder a las necesidades de negocio particulares. Por otra parte, la presencia de numerosos sistemas heterogéneos demanda un sobreesfuerzo por parte del equipo de soporte, con lo que no se pudo garantizar que las cuentas de acceso fueran creadas o eliminadas en el momento adecuado. Todo esto, tiene como consecuencia un incremento en los costos de administración, disminuyendo la productividad de los equipo de soporte encargados de esta actividad.

La empresa Telefónica se hace cargo de esta realidad, adquiriendo un Sistema de Gestión de Identidad (IDM) de llamado Oracle Identity Manager (OIM). Lamentablemente, al integrar OIM a la compañía, se provocaron problemas de interoperabilidad, dado a que módulos de conexión de esta plataforma fueron ineficientes y poco amigables para manejar las inconsistencias de las fuentes autoritativas de identidad (repositorios de registros de usuario) y en la reutilización de componentes al conectarse con los diferentes recursos TI de la empresa. A razón de esto, la presente tesis de grado, tiene por objetivo construir un Middleware que estandarice y agilice la integración de OIM tanto con los servicios de usuarios como con las aplicaciones de la empresa.

Como resultado de este trabajo, se obtiene una aplicación web en donde se presenta información tanto de usuarios como recursos en cuanto a aspectos de seguridad y auditoría. Para esto, también se dispone una Fuente Única Autoritativa de Identidad donde se concentraron todos los registros de usuarios. Finalmente, se provee un medio único de autentificación para todos los sistemas que se integren a esta Plataforma de Gestión de Identidad.

Abstract

Management of access accounts to systems or IT resources is a complex and expensive activity which concerns companies nowaday. This problem lies mainly in the co-existence of multiple sources of user records, each one of them with different formats, standards and targets, focused on answering to needs of private bussines projects. The presence of heterogeneous systems also demands an extra effort from the support team which can not assure that all access accounts were created or deleted at the appropriate time. As a result, there was an increase in administration costs, decreasing productivity among the support team responsible for this activity.

Telefónica takes on responsibility regarding this problem acquiring a Identity Management System (IDM) called Oracle Identity Manager (OIM). Unfortunately, when this system was implemented, there were problems of interoperability, given that this platform's connection modules were inefficient and unfriendly when handling inconsistencies in authoritative sources of identity (user records repositories) and in the reuse of components to connect with IT resources (systems) of the company. Because of this, the present thesis aims to build a Middleware to standardize the OIM integration of both users and services with enterprise applications.

As a result of this work, we have a web application where the user and resource information is presented in terms of security and audit aspects. In order to do this, we also have a Single Identity Authoritative Source where all user records are concentrated. Finally, efforts are made to provide a unique authentication mechanism for systems integrated into the identity management platform.

Dedicado a la memoria de mi Madre,

Mi Esposa Susy y toda mi Familia.

Las Piedras Angulares de mi Vida.

Tabla de Contenido

INDICE DE TABLAS

INDICE DE FIGURAS

1 Introducción

La necesidad de ser cada vez más productivos y enfrentar los desafíos que imponen los mercados globales, impulsa a las empresas a mejorar sus procesos de negocio de manera que sean más eficientes y rentables. En este sentido, una actividad bastante compleja ha sido la administración eficiente de una enorme cantidad de cuentas de acceso para usuarios en las aplicaciones o recursos TI. Así, los equipos de soporte comúnmente deben lidiar con la gestión de cuentas de accesos, tomando como referencia diversas fuentes autoritativas de identidad (FAI), es decir repositorios de identidades, las que por lo general operan en forma independiente. Por cada una de éstas FAIs, se pueden encontrar diferentes tipos de usuario, tales como:

- ✓ Empleados internos de la compañía.
- ✓ Profesionales de empresas proveedoras de servicios externos.
- ✓ Clientes y otros tipos de entidades externas.

Por otro lado, la incorporación de múltiples sistemas o recursos TI en la organización incrementa el número de credenciales de acceso que se deben controlar, lo que provoca un aumento en los costos de administración de cuentas de usuario. Entre los tipos de recursos se pueden encontrar:

- ✓ Plataformas empresariales de los grandes fabricantes TI del mercado: IBM, Oracle, Microsoft.
- ✓ Aplicaciones opensource.
- ✓ Sistemas propietarios construidos a medida según los requerimientos de las empresas.
- ✓ Recursos TI en conectividad de redes: acceso remoto, FTP, VPN, SSH, TELNET.
- ✓ Herramientas de ofimática: correo electrónico.

1.1 Antecedentes: Gestión de Identidad en Telefónica Chile

La empresa Telefónica, desde el año 2008 se ha encargado de los problemas de gestión de identidad (IDM) invirtiendo por una herramienta especializada en este tema llamada Oracle Identity Manager (OIM). Esta aplicación empresarial tiene por objetivo optimizar los procesos de negocio referente al aprovisionamiento de cuentas de acceso en los recursos TI. Así mismo, tiene por función controlar de forma centralizada el ciclo completo de vida de todas las identidades presentes en la organización.

Para esto, OIM cuenta con módulos de integración llamados conectores, los cuales son los encargados de enlazar las FAIs y Recursos TI (Sistemas de información) con la plataforma OIM. Los conectores se pueden clasificar en dos tipos:

- ✓ Conectores de Reconciliación: Módulo de integración para FAI.
- ✓ Conectores de Administración de Cuentas de Accesos: Módulo de integración para la ejecución de operaciones de aprovisionamiento de cuentas de accesos en los sistemas.

En la Figura 1, se presenta el esquema de funcionamiento de conectores OIM. En la sección 1.2 se describe con mayor profundidad cada uno de estos módulos de integración.

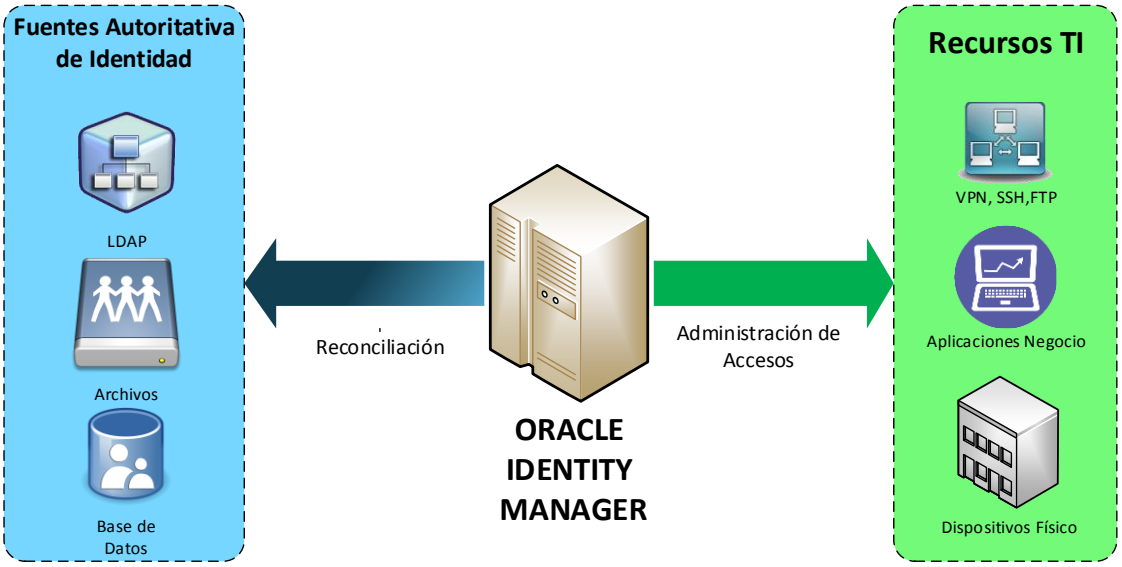


Figura 1. Esquema Funcionamiento OIM

1.2 El Problema

En el año 2008, se realizó la primera instalación de OIM en su versión 9 en cada uno de los países en los cuales Telefónica tiene presencia en Latinoamérica. Este proyecto de implantación se ejecutó simultáneamente en todas las divisiones de Telefónica con equipos de proyecto independientes, los cuales apenas tuvieron interacción. Pese a que los profesionales involucrados en la instalación adquirieron el conocimiento funcional y técnico de la herramienta, lamentablemente se sobrepasó el presupuesto de instalación y los costos de mantenimiento de esta plataforma. Esta situación, se debió principalmente a problemas de interoperabilidad, lo que se tradujo en complicadas y heterogéneas integraciones tecnológicas entre OIM y los recursos TI de la organización. Como producto de la instalación de OIM, se obtuvo una solución altamente acoplada, de difícil mantenimiento y escasamente reutilizable entre los países. Con todo esto, los equipos de soporte realizaron un sobresfuerzo considerable en atención de incidencias y desarrollo de nuevas mejoras en los módulos de integración de esta plataforma de gestión de identidad.

Los problemas de los 2 módulos de integración de la primera instalación de OIM 9 se detallan a continuación.

1.2.1 Módulo de Reconciliación

En el ámbito de gestión de identidad, la reconciliación se puede definir como un servicio automático y periódico de integración, encargado de la obtención de registros de usuario desde las FAIs con el fin de poder importarlas y administrarlas en la plataforma OIM.

Para este servicio de sincronización, se presentaron los siguientes problemas:

1. La primera dificultad presentada, fue la heterogeneidad de los diferentes repositorios de identidad considerados, los cuales hasta hoy operan de forma independientes con diferentes formatos y nomenclatura. Esto provocó un incremento en los costos de mantenimiento, dado a que se debían gestionar tantos grupos de usuario como FAIs estuvieran integradas a la plataforma de gestión de identidad. También se generaron brechas de seguridad por existencia de un usuario activo en más de una FAI, produciéndose así colisiones de identidades, las que no fueron controladas ni tratadas adecuadamente por OIM. Adicionalmente, las inconsistencias de formato en las identidades de OIM trajeron como consecuencia una sobrecarga de trabajo analítico por parte de las entidades auditoras del sistema.
2. La segunda dificultad fue la confiabilidad de los datos obtenidos, debido a que muchos registros de usuarios presentaban errores de sintaxis o simplemente estaban incompletos. Prueba de ello, es que se podían encontrar registros de usuarios desactualizados, RUT incorrectos o nombres con cargos inexistentes.
3. La tercera complicación presentada, fue la disponibilidad de los servicios que proveen las FAIs. Por un lado, una de las FAI sólo se encuentra disponible en un entorno pre-productivo, sin supervisión ni mantenimiento que velen la continuidad de su servicio. Ante este escenario, solucionar un problema o incidente podría tardar días o incluso semanas en solucionarlo, debido a que no se tiene oficialmente un área de soporte. Por otra parte, la existencia de trabajos programados no notificados producía intermitencias o problemas de conectividad entre OIM y las FAIs, corrompiendo el proceso de reconciliación. En la Figura 2, se presenta el esquema del proceso de reconciliación que consiste en la importación de los registros en la plataforma OIM 9.

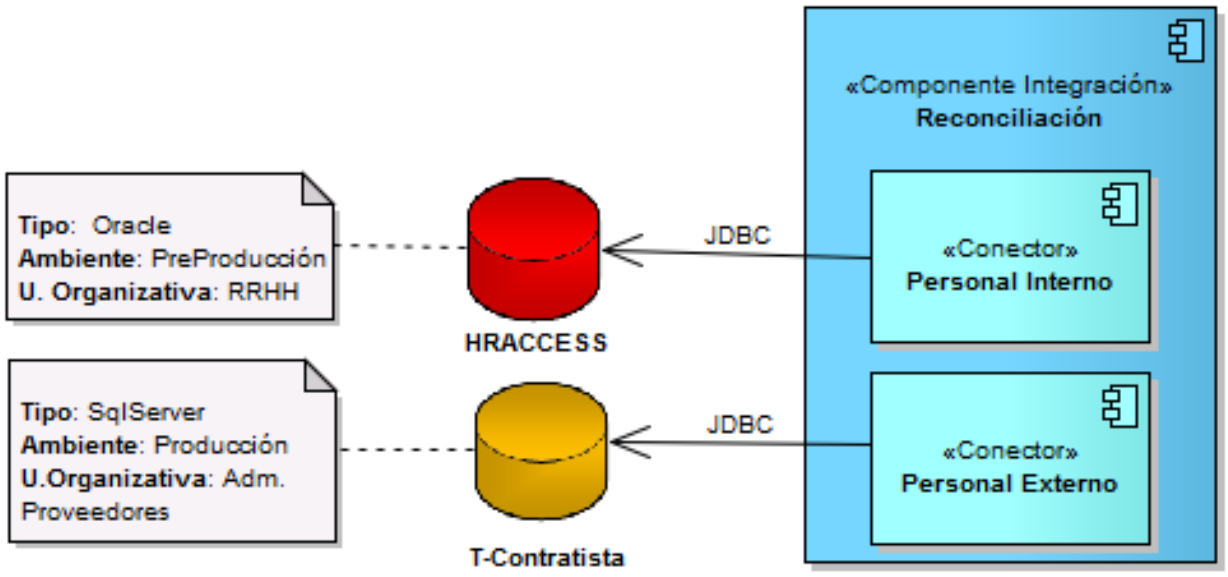


Figura 2. Proceso de Reconciliación en OIM 9

1.2.2 Módulo de Administración de Cuentas de Accesos

Este módulo es el encargado de la generación y gestión de las cuentas de acceso para un usuario en un recurso TI. Adicionalmente de indicar un nombre de usuario y contraseña, es responsable de configurar las características de la cuenta. Por ejemplo: para una cuenta de correo electrónico se podría indicar su capacidad o si se considera una cuenta de acceso VPN opcionalmente puede tener un período de Vigencia.

Para que OIM pueda comunicarse con el Recurso y crear una cuenta de acceso, se utiliza un componente llamado conector. Este es el encargado de realizar las operaciones de gestión de cuentas de acceso directamente en el recurso TI. En la actualidad, OIM ofrece un conjunto de conectores los cuales se integran a un grupo acotado de sistemas corporativos del mercado.

En Telefónica Chile existen centenas de sistemas de información heterogéneos, desde sistemas legados, aplicaciones propietarias hasta software empresariales de los grandes proveedores de software del mercado. Tomando en consideración este escenario y al no contar con conectores pre-fabricados necesarios para las aplicaciones que se deseaba integrar, se optó por utilizar la API (Application Programming Interface) de integración que posee OIM. La justificación de esto, es que el proceso de aprovisionamiento de cuentas de acceso debía ser adaptado a la realidad existente en la compañía, por lo que la utilización de un conector pre-fabricado no cumpliría los requerimientos establecidos por la empresa.

Sin embargo, cuando el equipo de desarrollo implementó sus propios conectores, se presentaron los siguientes inconvenientes:

- ✓ Se tuvo que rehacer el trabajo en la construcción de cada conector, debido a que la lógica común tales como las validaciones e implementaciones comunes, se replicaban para cada conector. Lo que significó que el desarrollador debía repetir bloques completos de código fuente para la programación de cada conector, los cuales no siempre quedaban homogéneos. Esta redundancia provocó un sobre esfuerzo a la hora de realizar mantenimiento o reparación en cada conector tal como es ilustrada la Figura 3.

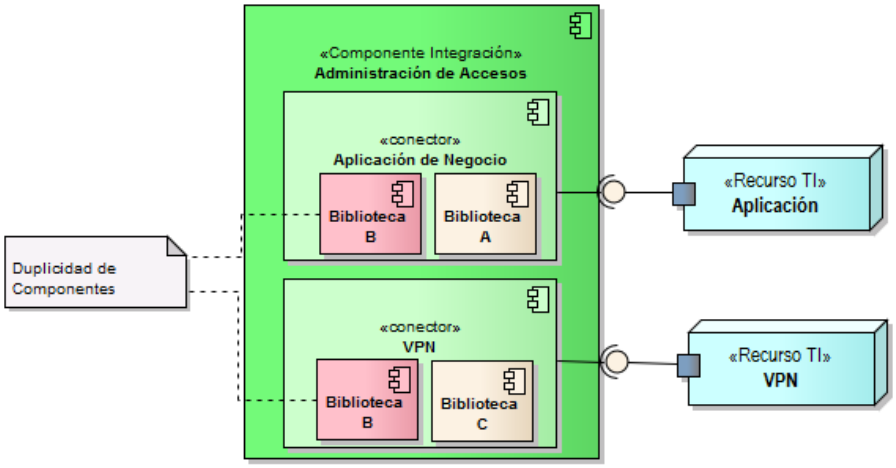


Figura 3. Duplicidad de Componentes

- ✓ Para incorporar una mejora o una reparación al servicio de administración de cuentas de acceso, se tenía que reiniciar completamente la plataforma de gestión de identidad. Esto debido a que los componentes importados por OIM debían recompilarse y cargarse en este módulo. Esto perjudicó los indicadores de operatividad y disponibilidad del sistema completo. Durante este proceso, incluso no se podía utilizar el módulo de reconciliación, el cual no sufrió ningún cambio. En la Figura 4, se ilustra esta situación.

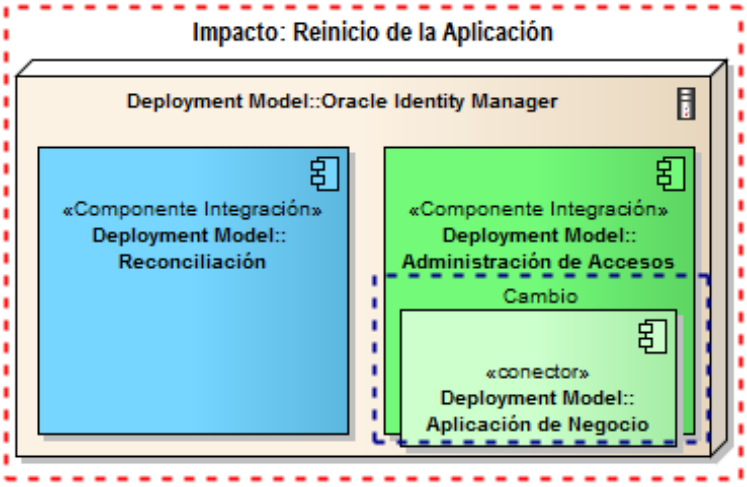


Figura 4. Disponibilidad de la Plataforma OIM

- ✓ No existió una uniformidad por aspectos transversales en la implementación de cada conector en OIM. Temas tales como Monitorización y Auditoría implicaron sobrecarga de trabajo, esto debido a que se trataron de forma independiente, inconsistente, descentralizada y comúnmente no documentado. En Figura 5 se puede apreciar la implementación de dos aspectos transversales en los conectores con diferentes bibliotecas tecnológicas Java.

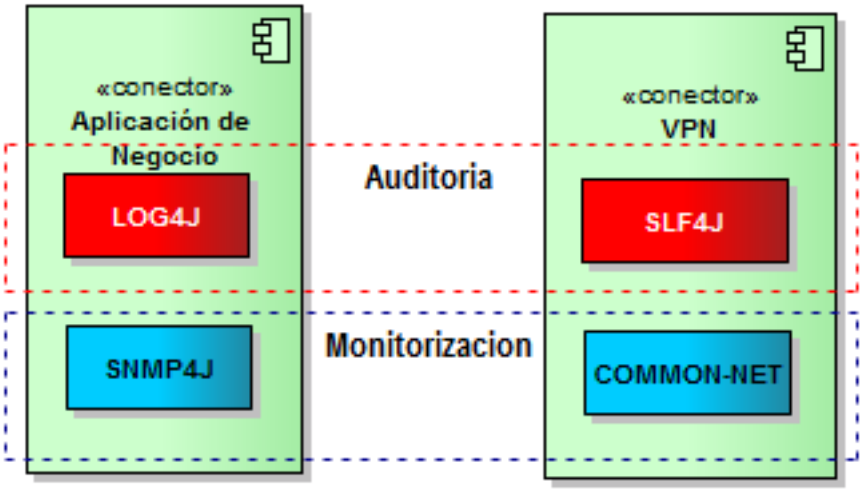


Figura 5. Heterogeneidad de Aspectos Transversales

1.3 Solución Propuesta

En esta tesis de grado, se buscará mejorar y superar las dificultades de integración que tiene la plataforma OIM mediante la construcción de middleware de integración que introduzcan mejoras en los aspectos de interoperabilidad, mantenimiento y auditoría. En este sentido, el primer middleware resolverá los problemas y requerimientos del módulo de reconciliación. Mientras que el segundo middleware se encargará de gestionar de forma centralizada todas las solicitudes de cuentas de acceso para los recursos TI de la organización que estén integrados a la plataforma de gestión de identidad.

Además, con la finalidad de extrapolar el funcionamiento de estos middleware a otras divisiones de Telefónica en Latinoamérica, los elementos que los componen son diseñados e implementados mediante el Patrón de Diseño Inyección de Dependencia (DI) [15, p. 118-119], promoviendo así las características de mantenimiento y portabilidad de estos componentes, para poder adaptarla a la realidad de cada país.

Con la estandarización de los mecanismos de la integración tanto de la reconciliación como de la administración de cuentas de acceso en la plataforma de gestión de identidad, se pretende lograr una simplificación en las tareas de construcción y mantenimiento, aumentando así la productividad de los equipos de mantenimiento de OIM.

Adicionalmente a los temas de interoperabilidad y mantenimiento, en este proyecto se busca cumplir con las normativas de auditoría y políticas de seguridad de la compañía, las que actualmente protegen la comunicación e información de todos los empleados que trabajan en Telefónica. En este sentido, el middleware contará con funciones que detecten y reporten las principales brechas de seguridad que se produzcan en el módulo de reconciliación.

Finalmente, se construirá un mecanismo uniforme y centralizado de autentificación implementado a través de un servicio Web, lo que permitirá integrarse a cualquier sistema que soporte el protocolo SOAP[1]. La razón de su utilización viene dada a que es estándar soportado por los principales fabricantes de software del mercado, tales como Microsoft, IBM y Oracle entre otros.

El desarrollo de estas importantes mejoras se enmarca en un proceso de migración global de la plataforma OIM. Esto dada la declaración de Oracle de finalizar el contrato de soporte extendido para la actual versión instalada, es decir, el proveedor no proporcionará más actualizaciones ni servicio de mantenimiento a esta versión del producto.

Ante el riesgo de una obsolescencia tecnológica producto de esta situación, la Dirección de Seguridad de Telefónica LATAM ha dado la directriz de migrar a la versión 11 de OIM, lo que garantizará su vigencia operativa hasta diciembre del año 2021. [1, p. 34]. En la Tabla 1, se muestra los períodos de los distintos tipos de soporte.

[1] SOAP: es un protocolo estándar que define cómo dos objetos en diferentes procesos pueden comunicarse por medio de intercambio de datos XML.

Tabla 1. Período de Soporte de las versiones de OIM

Lanzamiento de versiones de Oracle Identity Management				
Versión	Fecha de Lanzamiento	Fin de Soporte Premier	Fin de Soporte Extendido	Fin de Soporte Sostenido
9.1.x	Marzo 2008	Diciembre 2012	Diciembre 2013	Indefinido
11.1.2.x	Agosto 2012	Diciembre 2018	Diciembre 2021	Indefinido

1.4 Metodología y Desarrollo de la Solución

Para llevar a cabo esta solución, se utilizó el modelo de desarrollo iterativo-incremental [19, p. 32-35], en donde en el primer incremento se consideraron las necesidades del módulo de reconciliación, mientras que en el segundo incremento se enfocó a la resolución de problemas del módulo de administración en la provisión de cuentas de acceso.

Así, en la primera fase de este trabajo se identificaron todas las FAI relevantes a considerar, luego se determinaron cuáles son los atributos representativos de la identidad digital con los que se integrará el sistema OIM. Las siguientes actividades en esta etapa se enfocaron en el diseño de un motor de formateo y validación de identidad. Esto para poder estandarizar y normalizar los registros de usuarios que provenían desde distintas fuentes de datos. El producto final de este incremento correspondió a una aplicación Web llamada Normalizador de Datos de Usuarios (NDU) que nutrirá la FUAI la que fue implementada mediante un Active Directory[2] (AD).

En el segundo incremento, los esfuerzos se centraron en analizar los problemas de integración entre OIM y los recursos TI. Para esto, se determinó cuáles son los tipos de recurso TI involucrados (sistemas de la infraestructura de la Dirección de Red) junto con los operaciones de administración de acceso para estos dispositivos (alta , baja y actualización de una cuenta de acceso). Luego, se diseñó y desarrolló un Middleware de Integración el cual expone una interfaz genérica de aprovisionamiento, la que es responsable de procesar todas las operaciones de administración de cuentas de acceso sobre los recursos TI. Junto con esto, como un trabajo adicional se diseñó e implementó un mecanismo de autentificación para los sistemas propietarios de Telefónica que deseen integrarse a esta plataforma de gestión de identidad.

Como productos finales se obtuvo aplicaciones Web interoperable e integrable con otras plataformas de gestión de identidad. Esto es importante, dado que en un futuro si se desea migrar de plataforma (incluso para otros fabricantes de este tipo de plataformas), los esfuerzos se centraran en la configuración interna del producto y en menos medida en aspectos técnicos de integración tanto con las FAIs como recursos TI ya existentes en la compañía.

[2] Active Directory: Es el término que utiliza Microsoft para referirse a su implementación de Servicios de Directorio, permite almacenar información de usuarios y recursos en una red distribuida utilizando principalmente el protocolo LDAP.

2 Objetivos

2.1 Objetivo General

Esta tesis tiene por objetivo general proporcionar a Telefónica Chile Middleware de Integración que provean un mecanismo estándar de generación de cuentas de acceso y de unificación de todas las Fuentes Autoritativas de Identidad que tenga la organización. Con estos artefactos, se espera reducir los tiempos y costos de operatividad que actualmente se tienen con esta plataforma implantada en Telefónica.

2.2 Objetivos Específicos

- ✓ Presentar el estado del arte de los sistemas IDM en el mercado global y en la empresa Telefónica Chile.
- ✓ Diseñar y construir una aplicación Web que estandarice los registros de identidad desde los diferentes repositorios de datos en una Fuente Única Autoritativa de Identidad.
- ✓ Diseñar y construir un servicio Web que procese de forma estandarizada y centralizada las peticiones de aprovisionamiento de cuentas de accesos en los recursos TI que provengan desde OIM.
- ✓ Diseñar y construir un servicio Web de autentificación para los recursos TI que se deseen integrar a la plataforma de gestión de identidad.
- ✓ Responder eficientemente a las necesidades normativas de auditoria que tiene Telefónica Chile.
- ✓ Extender alguna de las funcionalidades implementadas en estos middleware a otros recursos TI en la organización.

2.3 Alcances y Limitaciones

En el desarrollo de esta tesis el alumno sólo abarcó los módulos de integración en la plataforma de gestión de identidad de OIM. Estos componentes de software son los que se conectan tanto con las FAI (Componente de Reconciliación) como con las aplicaciones corporativas o recursos TI existentes en una organización (Administración de Cuentas Acceso). Así, los temas de configuración y administración de perfiles, flujos de aprobación y autorizaciones de acceso son elementos autónomos dentro del producto OIM, por lo que no se consideraron en el trabajo en esta tesis. Estos temas fueron tomados por el resto del equipo del proyecto, así este trabajo sólo se enfocó en los temas de integración de la plataforma de gestión de identidad tanto con fuentes autoritativas de identidad como con recursos TI.

Dentro de las fuentes autoritativas de identidad que se consideraron en la integración con el servicio de reconciliación son:

- ✓ Información de Recursos Humanos.
- ✓ Información sobre las cuentas de dominio.
- ✓ Información de personas desde administración de proveedores.
- ✓ Usuarios Excepcionales que puedan ingresar a la plataforma.

Por otro lado, los recursos TI críticos que se abordaron en esta tesis fueron los relacionados con la infraestructura de red de la compañía. Estos recursos son importantes dado a que conforman la columna vertebral de los servicios entregados a los clientes de Telefónica. En este sentido, es primordial controlar los accesos de forma centralizada a esta infraestructura, mantener registros de otorgamientos de accesos restringidos y prevención de cualquier brecha de seguridad. Los servicios de red que abarcaron fueron:

- ✓ Servicio VPN de diferentes redes.
- ✓ Acceso a diferentes dispositivos de la infraestructura de red.
- ✓ Acceso a Sistemas de Negocio Web.

Por otra parte, los diferentes servicios de red tratados como recurso TI en el contexto de los sistemas IDM, debieron suscribirse al procedimiento de autentificación llamado Single Sign-ON[3] (SSO) implementado mediante un AD, que viene a ser la misma fuente autoritativa de usuarios con la que se integra la plataforma de gestión de identidad. Asimismo, la arquitectura de este segundo middleware debe ser capaz de soportar la integración de aplicaciones a las cuales no es posible aplicar esta forma de autentificación (aplicaciones legadas autónomas sin interfaces de integración con un AD).

[3] SSO: Es un procedimiento de autenticación que habilita al usuario para acceder a varios sistemas con una sola cuenta de acceso.

3 Introducción a la Plataforma Oracle Identity Manager

La finalidad de este capítulo es describir brevemente, los conceptos básicos de la Gestión de Identidad desde la perspectiva de OIM en el ámbito empresarial. Para esto, se tomó como referencia la primera instalación OIM en el año 2009 en Telefónica con la versión 9 hasta su última versión instalada 11GR2 el año 2014.

3.1 Antecedentes

La empresa Oracle presentó su primer producto ligado a la gestión de identidad al mercado en el año 1999, con el lanzamiento del sistema llamado Oracle Identity Directory (OID). Desde entonces esta herramienta ha ido avanzado y evolucionado de manera sostenida hasta su actual versión llamada Oracle Identity Manager 11GR2 en el año 2014 [2, p. 2].

Esta plataforma desde un inicio se concibió con el objetivo de administrar todo el ciclo de vida de las identidades y controlar el acceso a los diferentes recursos corporativos TI. Así, su funcionamiento se enfoca principalmente en la protección en el otorgamiento de accesos a sistemas, reducción del trabajo operativo del personal soporte y a la automatización de procesos de negocio mediante reglas de aprobación y políticas de otorgamiento de acceso [3]. Un ejemplo de esto, es cuando una persona es desvinculada de la organización, este sistema lo detecta desde las bases de datos de recursos humanos y elimina automáticamente todos sus accesos. De la misma manera ocurre cuando una persona es contratada, la plataforma OIM detecta la incorporación y según su cargo, unidad organizacional, lugar de trabajo que pertenece le otorga las cuentas de accesos a los sistemas que le corresponde según su perfil. Así, uno de sus objetivos es centralizar los mecanismos de acceso y disminuir el trabajo operativo de los profesionales que mantienen la plataforma.

3.2 Definición de Identidad

Una identidad, en el contexto de los sistemas IDM, es un conjunto de atributos que identifican de manera única a un usuario. Este grupo de atributos, también determina la relación que existe entre usuario y la organización. Por ejemplo:

- ✓ Unidad organizativa a la que pertenece el usuario.
- ✓ Cargo que desempeña el usuario.
- ✓ Lugar de trabajo.

Adicionalmente, la identidad de un usuario puede contener atributos propios del sistema IDM que definen las acciones permitidas sobre él por ejemplo: username, password, tipo de usuario [4, p. 29]. En la Figura 6 se presenta como se estructura los atributos que componen la identidad de un usuario.

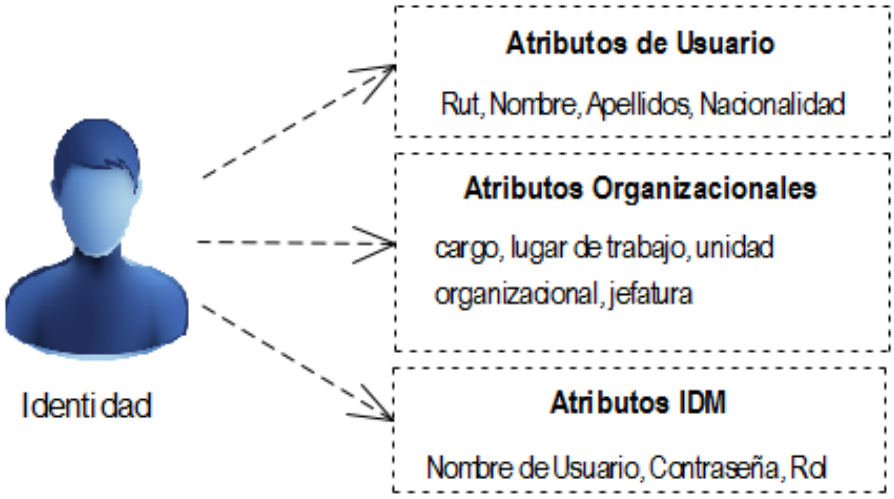


Figura 6. Definición de Identidad

Es importante destacar que la identidad de usuario sólo debe considerar los atributos relevantes enfocados a responder eficientemente a los requerimientos estratégicos de negocio de la organización tal como lo indica la siguiente referencia:

> *"Mantener un control de los accesos a la infraestructura a los sistemas de TI y/o aplicaciones con una jerarquización de los usuarios para las aplicaciones o funcionalidades específicas de la corporación"* [5, p. 5].

Otro punto importante es verificar la confiabilidad de los datos, dado que con estos la plataforma de gestión de identidad opera para construir sus reglas de negocio para el otorgamiento de cuentas de acceso a los recursos TI. La confiabilidad de los datos se determina por la frecuencia en que los datos son actualizados en la FAI cuando un evento que afecte a los atributos de usuario haya ocurrido. Por ejemplo: ascensos laborales, cambios de unidad organizativa o desvinculación del empleado.

Respecto a la Contraseña de la cuenta de acceso, esta debe regirse por las políticas que establece la "Normativa Corporativa de Seguridad de la Información" de la compaña:

- ✓ Es intransferible.
- ✓ Vigencia de 3 meses.
- ✓ Debe contener al menos 8 caracteres considerando mayúsculas, minúsculas y números.
- ✓ No debe ser igual a las 6 últimas contraseñas anteriormente utilizadas.
- ✓ Bloqueo automático cuando no se utilice en un período de 2 semanas.

3.3 Áreas Funcionales de Gestión de Identidad

En el ámbito de gestión de identidad, la empresa que desee implementar este tipo de soluciones desde la perspectiva de OIM, se debe abarcar al menos tres áreas funcionales para plantear su diseño y arquitectura:

- ✓ Reconciliación.
- ✓ Gestor de identidad.
- ✓ Administración de acceso.

3.3.1 Reconciliación

La reconciliación es un proceso de integración automático y periódico encargado de sincronizar los registros de usuarios desde las FAI al sistema de persistencia de OIM. En esta actividad, se determina las diferencias existentes entre la FAI y OIM, luego aplica operaciones de creación, modificación y eliminación de registros de usuario para actualizar las identidades [6, p. 226]. Ejemplos de FAI pueden ser:

- ✓ Un Active Directory en Windows o LDAP [4]en Unix.
- ✓ Una Base de Datos.
- ✓ Un archivo plano.
- ✓ Cualquier sistema persistente que contenga registros de usuario.

3.3.2 Administración de Control de Cuentas de Accesos

La Administración de Control de Cuentas de Accesos es el proceso encargado de controlar las operaciones de creación, eliminación y actualización de cuentas de acceso en los recursos TI de la organización originadas desde la plataforma de gestión de identidad. En otras palabras, este módulo es el responsable de habilitar a un usuario para utilizar un recurso mediante una cuenta de acceso con ciertos privilegios. Por ejemplo: una cuenta VPN, una cuenta de acceso a un sistema SAP.

Este proceso consta de las cuatro siguientes actividades:

- ✓ Especificación de Cuenta de Acceso: Corresponde a la definición del usuario que hará uso de la cuenta de acceso. Opcionalmente en esta tarea se puede especificar manualmente su credencial (dupla nombre de usuario y contraseña), aunque en la mayoría de las veces esta credencial es calculada automáticamente según las definiciones de seguridad de la organización. El segundo paso de esta actividad es la especificación de las características que va a tener la cuenta de acceso. Por ejemplo: privilegio de acceso (lectura/escritura), período de vigencia y capacidad de una cuenta de correo electrónico.

[4] LDAP: Referencia a un protocolo a nivel de aplicación que permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red.

- ✓ Validación de Negocio: Son procedimientos que garantizan las condiciones para que se lleve a cabo el aprovisionamiento de una cuenta de acceso. Por ejemplo: interacciones con sistemas externos. Si la validación es incorrecta el sistema avisa automáticamente al usuario que la cuenta no fue creada.
- ✓ Creación de Cuenta de Acceso: Corresponde al aprovisionamiento de las credenciales y configuraciones de acceso en el recurso TI. Si el aprovisionamiento fue correcto, se le notifica al usuario que la credencial fue generada.
- ✓ Notificación de Cuenta de Acceso: Es la tarea de informarle al usuario por algún medio tecnológico la generación de una cuenta de acceso TI para un recurso en particular. Por ejemplo, un correo electrónico o un mensaje de texto a un celular.

3.3.3 Gestión de Identidad

Este módulo representa una amplia área funcional que encapsula varias actividades para su correcto funcionamiento, tales como:

- ✓ Administración de grupos, perfiles y usuarios: Los usuarios se pueden organizar de forma jerárquica mediante una estructura jerárquica. Los roles determinan las capacidades de los usuarios sobre la plataforma de gestión de identidad, por ejemplo: beneficiario solicitante y aprobador. Finalmente actualizar los datos de los usuarios que corresponden a la administración propia de la plataforma.
- ✓ Autoservicio de restablecimiento de contraseñas: Con esta característica ya no es necesario levantar una solicitud a la mesa de atención de cuentas para ejecutar un cambio de contraseña, solamente el mismo usuario podrá solicitarlo a OIM.
- ✓ Administración delegada y flujo de aprobaciones: La administración delegada corresponde a una derivación automática de responsabilidad si un usuario no es capaz de atenderlo (usuario aprobador inactivo o desvinculado). El flujo de aprobaciones, por otro lado, corresponde un conjunto lógico y finito de instancias de autorización de solicitudes con el objetivo de otorgar una cuenta de acceso para usuario en un recurso TI.

Estas tareas de gestión roles empresariales y reglas de negocio son contenidas y personalizable mediantes componentes propietarios del sistema de gestión de identidad OIM. Esto permite automatizar el trabajo operativo de provisión de cuentas de acceso, otorgar a las personas la capacidad de auto-administrar sus propias cuentas y delegar algunas de sus responsabilidades a otros usuarios dentro de su organización [2, p. 4].

Las actividades de este módulo no serán abordado en este trabajo de tesis, debido a que OIM es la herramienta del mercado que tiene el mayor nivel la madurez y su configuración es responsabilidad del resto del equipo de proyecto.

3.4 Ciclo de Vida de las Identidades

Las identidades dentro de la plataforma de gestión de identidad siguen un ciclo de vida asociado a la relación existente entre los usuarios y la organización. Este ciclo se compone por las etapas que presenta en la Figura 7.

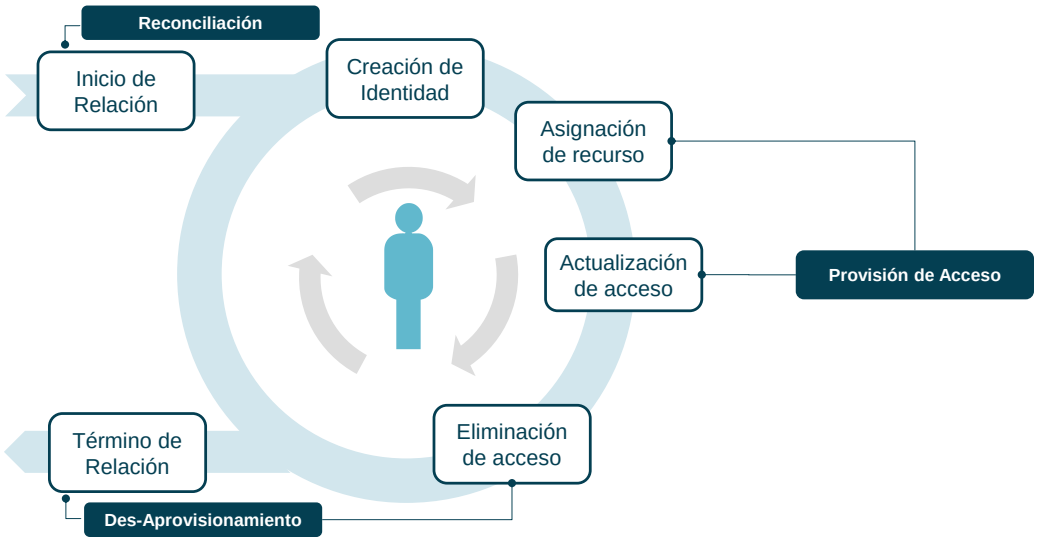


Figura 7. Ciclo de Vida de una Identidad

- ✓ Creación: Esta etapa se realiza la creación de la identidad del usuario de forma automática por medio del proceso de reconciliación con las FAIs.
- ✓ Asignación de recurso: Por medio de la operación aprovisionamiento de acceso se le asignan una serie de recurso al usuario.
- ✓ Aprovisionamiento y Actualización de Acceso: Corresponde a las operaciones de mantenimiento que se realizan sobre las cuentas de acceso del usuario, mientras éste tenga relación con la organización. Esto significa que un acceso puede cambiar de configuración en el tiempo. Esta actividad es una de las más tediosas que realiza el equipo de soporte debido a que entre más actividades realice el usuario más son los accesos que deben gestionarse.
- ✓ Desaprovisionamiento: Esto se puede dar en dos situaciones:
  - Las funciones de un usuario no ameritan el uso de un determinado recurso.
  - Termino de la relación entre usuario y organización.

3.5 Políticas y Roles

En la plataforma de OIM, las políticas y los roles definen las relaciones que tienen los usuarios sobre los recursos TI de una organización. Mientras los roles definen agrupaciones de usuario, las políticas establecen las reglas, derechos y autoridades de acceso de estos grupos sobre los recursos organizacionales. Las políticas se pueden dividir en dos tipos [7, pp. 3-1]:

- ✓ Política de Acceso: Determina que grupos de usuarios puede tener acceso a que recurso.
- ✓ Políticas de Aprobación: Define que usuarios será el administrador de los recursos.

De esta forma, los accesos a recursos puede ser auto-aprovisionado (para el caso de los administradores sobre los recursos que gestiona) o a través de solicitudes de acceso (esto para los grupos de usuarios finales). Así, este usuario es el único que puede aprobar, rechazar o modificar una solicitud de cuenta de acceso.

De acuerdo a lo anterior, se pueden distinguir 3 categorías de usuarios según las políticas con las que se encuentren relacionados.

- ✓ Usuarios Finales: Son los usuarios a los que se le generaran las cuentas de acceso sobre los recursos.
- ✓ Usuarios Solicitantes: Son los usuarios que realizan la petición de accesos para ellos o para usuarios finales.
- ✓ Usuarios Administradores o aprobadores: Son los usuarios que aprueban o rechazan una petición de acceso.

En la Figura 8 se ilustra la relación existentes entre roles y políticas.

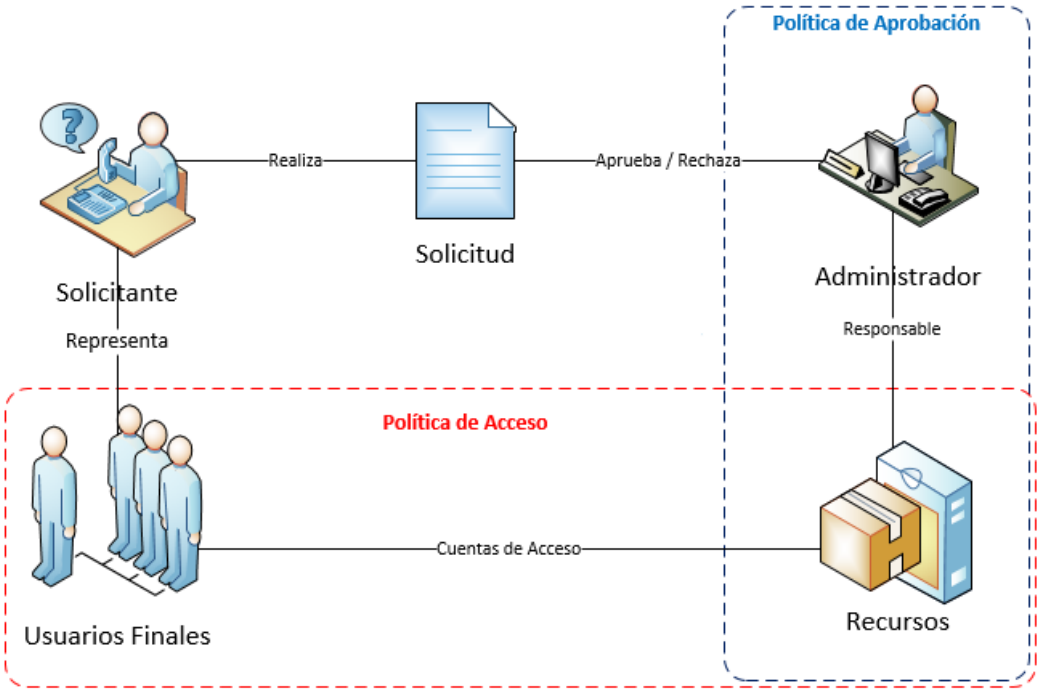


Figura 8. Relación entre Tipos de Usuarios y Políticas

3.6 Mercado de la Gestión de la Identidad

En la actualidad, para las grandes empresas el tema de gestión de identidad cobra vital relevancia, debido a que se están produciendo perdidas de billones de dólares cada año por este concepto principalmente debido a la deficiente administración que se tiene sobre las cuentas de usuario. Para afrontar este problema, las compañías han estado invirtiendo cada vez más en soluciones TI basadas en la gestión de identidad, esperando disminuir los costos de esta actividad y garantizar la seguridad de acceso sobre los activos TI en toda la organización.

Reflejo de la preocupación que conlleva esta labor, es el aumento sostenido de la inversión en el mercado global de la gestión de identidad, empezando el año 2006 con USD 2,6 billones hasta USD 5,13 millones el 2013 y pronosticado para año 2018 en USD 10.39 billones [8, p. 6]. Esto según el estudio de la empresa Forrest Research la cual se enfoca en la investigación del impacto de Tecnologías de Información en el Mercado. La Figura 9 grafica la evolución en la inversión en gestión de identidad.

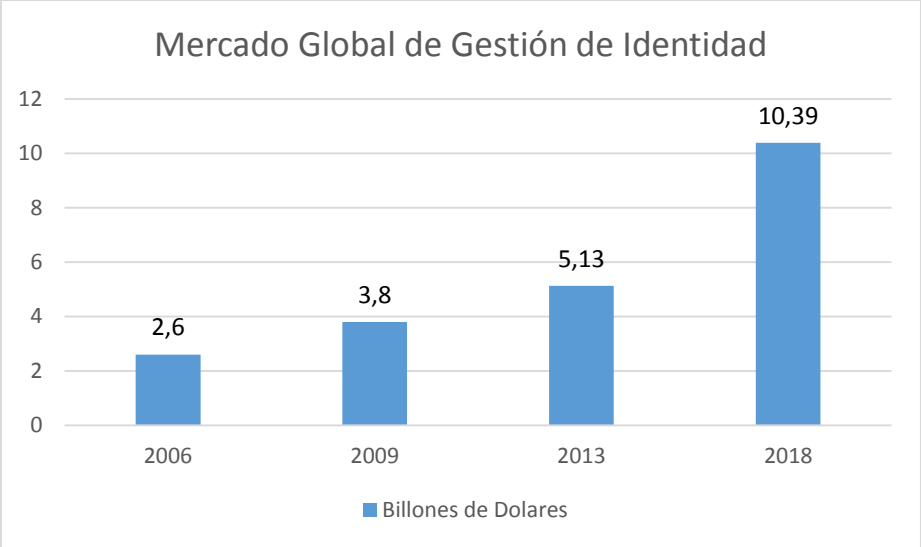


Figura 9. Gráfico del Mercado Global de Gestión de Identidad

Debido a este incremento de la inversión en el mercado de gestión de identidad, es que en el año 2012, una de las principales compañías de investigación y asesoramiento de TI, Gartner Inc. realizó un estudio de madurez referente a los beneficios que estos proveedores de sistemas IDM, dentro de los cuales se destacan los siguientes:

- ✓ Reducción de costo.
- ✓ Rápida implementación de soluciones.
- ✓ Compatibilidad de conexión con los distintos sistemas de información.
- ✓ Simplificación de la gestión e Integración de fuentes autoritativas de usuarios repartidas en toda la organización.
- ✓ Alto grado de mantenimiento.

El resultado de este estudio fue un diagrama que refleja el posicionamiento alcanzado por cada una de estas empresas, referido al nivel de madurez obtenido en la administración y aprovisionamiento de gestión de identidad tal como se ve en la Figura 10[9, p. 6].

Figura 10. Cuadrante Mágico de Fabricantes de Soluciones de Gestión de Identidad

Tabla 2. Principales Fabricantes de Soluciones IDM

Empresa Proveedora	Sistema de Gestión de Identidad
Oracle	Oracle Identity Manager(OIM)
Microsoft	Forefront Identity Manager (FIM)
IBM	Security Identity Manager
Dell	Quest One Identity Manager
CA Tecnologies	Identity Manager & Governance
Novell	NetIQ Identity Manager
Hitachi	Hitachi ID
COURION	Cuorion Access Risk Management for Government
SailPoint	Identity Access Manager

3.7 Implementación de OIM en Telefónica LATAM

La Dirección de Seguridad de la Información es la encargada de velar por la seguridad tecnológica integral de todas las empresas del Grupo Telefónica. Esta unidad organizacional nace en el año 1984 y desde hace más de 20 años se encuentra proveyendo soluciones innovadoras y servicios especializados en TI. Actualmente, tiene presencia directa en Chile, Perú, España, Argentina, Brasil y México y tiene planes de crecimiento en otros países de Latino América.

En el año 2008, el departamento de seguridad de la información inicia su participación en la iniciativa global de Gestión de Identidades dentro del Holding Telefónica. En este sentido, en Chile, Perú, México y Colombia han sido pioneros en implementar localmente la solución OIM. Los antecedentes en cuanto a cantidad de usuarios y sistemas integrados en cada país se presenta en la Tabla 3.

Tabla 3. OIM 9 implantado en Telefónica LATAM

Nro.	País	División	Cantidad de Usuarios	Cantidad de Recursos TI
1	Chile	Telefónica Chile	60.000	6
2	Perú	Telefónica del Perú	12.000	2
3	México	Telefónica México	11.000	5
4	Colombia	Movistar Colombia	18.000	37

Como se puede apreciar en la Tabla 3, Chile lidera en cuanto a la cantidad de usuarios que se encuentran registrados en sus fuentes autoritativas de datos seguidos por Colombia y Perú. Por otro lado, en cuanto a la integración de aplicaciones o recursos TI, la división de Telefónica que tiene la mayor experiencia es Colombia, seguido por Chile y México.

4 Construyendo una Fuente Única Autoritativa de Identidad

En este capítulo, primeramente se describen y detallan las principales Fuentes Autoritativas de Identidad de la compañía Telefónica Chile, junto con considerar sus restricciones, características de acceso y mecanismo de funcionamiento. Así mismo, se determinaron los atributos críticos de los usuarios extraídos de cada FAI para conformar la Identidad Digital de la plataforma OIM. También se explica el diseño e implementación del Middleware de Integración NDU, cuya función es consolidar las distintas FAI en un sólo repositorio para reducir los problemas con el módulo de reconciliación.

4.1 Definición de Fuente Autoritativa de Identidad

Una Fuente Autoritativa de Identidad es un repositorio de registros de usuario que es controlado por un Sistema de Gestión de Identidad. Generalmente estas fuentes de datos suelen ser bases de datos, LDAP, archivos planos o cualquier sistema persistente en donde se almacene información de los empleados de una compañía, tales como: id, nombre, fecha de contratación, departamento, cargo, etc. En algunos casos, estos repositorios además de almacenar información, poseen funciones adicionales, como por ejemplo el AD, debido a que es capaz de administrar roles, unidades organizativas, políticas de seguridad, etc.

4.2 Identificación de Fuentes Autoritativas de Identidad

En Telefónica, existen múltiples almacenes de información de usuario, que podrían ser considerados como Fuentes Autoritativas de Identidad. Estos repositorios se caracterizan por ser heterogéneos, se encuentran controlados por distintos departamento y están enfocados en responder las necesidades específicas de negocio de unidades organizativas a las que pertenecen. Así se atribuyen distintas responsabilidades a las fuentes de identidad según la unidad organizacional que lo controle. Por ejemplo, el departamento de TI indicó que su LDAP es la FAI de los usuarios, mientras el departamento de RRHH indicó que su base de datos es la fuente autoritativa en cuanto a ingresos y desvinculaciones de la compañía.

Así, la actividad de identificación de las FAIs se centró en determinar cuáles son los repositorios de identidad desde donde se extraerán los datos de los usuarios que conformarán el universo de identidades relevantes para ser almacenados en la FUAI. Para esto, resultó esencial tener claro cuáles son los recursos TI a los que se les proveerán cuentas de acceso.

Después del análisis, se determinó que el universo de usuarios relevantes para la plataforma de gestión de identidad son todos los profesionales que utilizan los principales recursos de la infraestructura de Red de Telefónica, específicamente VPN y Acceso Remoto a Equipos. Por lo tanto, las FAIs que tienen los usuarios potenciales de estos recursos son los siguientes:

- ✓ HRACCESS: Empleados internos de Telefónica Chile.

- ✓ T-Contratista: Personal subcontratado.
- ✓ CallCenter: Personal subcontratado.
- ✓ Excepciones: Nominación para profesionales que trabajan ocasionalmente y por un período acotado por un periodo fijo. Ellos no se encuentran registrados en ninguna de las FAIs anteriormente mencionadas.

En la Figura 11, se presenta la categorización jerárquica de los principales tipos de usuario y FAIs consideradas en la conformación de la FUAI.

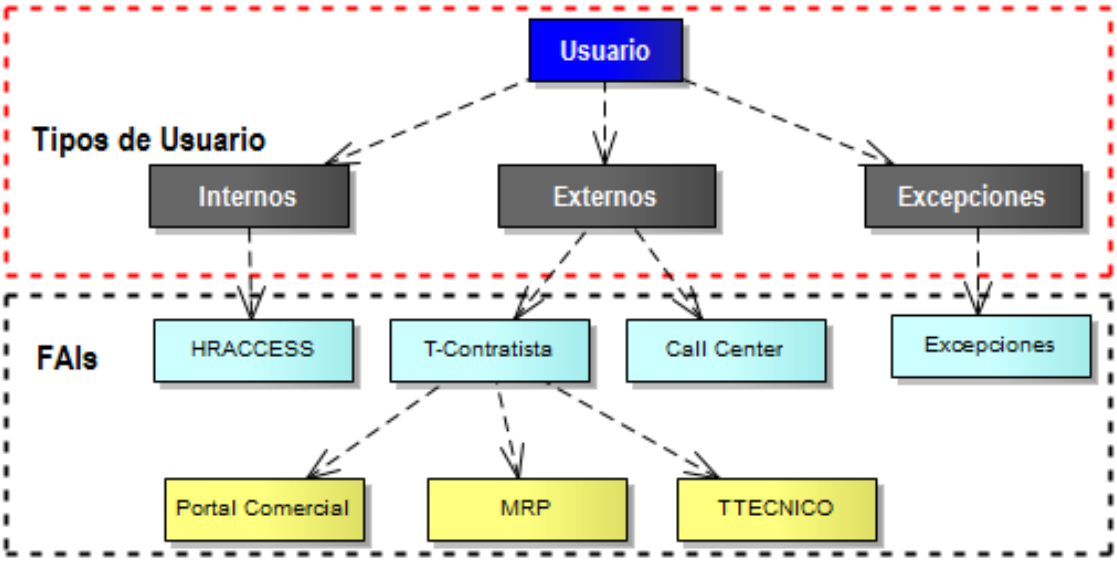


Figura 11. Jerarquía de Tipos de Usuarios

Como se puede ver distinguir la Figura 11, existen 3 tipos de usuarios (internos, externos y excepciones), los cuales son determinados por la FAI a la cual pertenecen. Esta clasificación dentro de la FUAI es importante ya que dependiendo del tipo de usuario se pueden establecer responsabilidades, restricciones y configuraciones para las identidades dentro de la plataforma OIM.

4.2.1 Empleados Internos de Telefónica Chile

En la actualidad, la información de los trabajadores internos de Telefónica se encuentra disponible en una plataforma empresarial orientada a la gestión de personas llamada HRACCESS. Este sistema hoy es administrado y controlado directamente por la Dirección de Recursos Humanos de la organización.

Por otro lado, la persistencia de esta aplicación de gestión de usuario, esta implementada en una Base de datos Oracle en un entorno de producción. Esta base de datos cuenta con servicios de

monitoreo y respaldo, aspectos esenciales para garantizar la operatividad y continuidad del proceso de normalización implementado.

Como es comprensible, el acceso a la información de este tipo de usuario es estrictamente confidencial, ya que se pueden encontrar datos privados, tales como remuneraciones y bonos asignados. En este aspecto, se encuentra prohibido el acceso directo a las tablas de usuarios de esta aplicación, dada la normativa vigente de seguridad de la información que dicta la compañía. Sin embargo, como respuesta a la necesidad de contar al menos con parte de la información de este grupo de personas para la plataforma OIM, la dirección de RRHH dispuso una "Vista de Base de Datos"[5], la cual puede ser consultada mediante una cuenta de lectura sin acceso a cualquier otra información que maneje la plataforma de RRHH.

4.2.2 Profesionales de Empresas Colaboradoras Externas

Hoy en día existen dos FAIs que administran la información del personal de empresas colaboradoras externas de la compañía, las cuales son:

- ✓ T-Contratista.
- ✓ CallCenter.

4.2.2.1 T- Contratista

La FAI T-Contratista es un conjunto de sistemas que administra y controla la información del personal externo de Telefónica Chile. Actualmente, en este repositorio persisten los registros de usuarios para 3 líneas de negocios, las cuales son utilizadas por los siguientes sistemas:

- ✓ T-Tecnico: Administra la información del personal técnico de empresas colaboradoras externas. Estas personas son especialistas en algún tipo de tecnología o servicio, por Ejemplo: fibra óptica, VoIP[6], Internet.
- ✓ MRP: Dirige la información de todos los profesionales externos contratados en las sucursales de telefónica en todo Chile.
- ✓ Portal Comercial: Controla la información del personal contratado que cumplen las funciones de pre-venta y post-venta de la Compañía.

En cuanto a su implementación, el sistema de persistencia de T-Contratista es una base de datos SQLServer 2012 en diferentes esquemas para cada línea de negocio, pero en una misma instancia de base de datos. Para la nueva plataforma de gestión de identidad, la Dirección de Tecnologías

[5] Vista de Base de Datos: consulta accesible como una tabla virtual en una base de datos. La única diferencia con una tabla es que en ella se almacena su definición y no los datos.
[6] VOiP: conocido también como Voz IP, es una tecnología que concentra un grupo de recursos que hacen posible que la señal de audio análoga viaje digitalmente a través de Internet empleando el protocolo IP.

de Información (responsable de este sistema) ha generado una vista de base de datos que integra los registros de usuarios de estos tres sistemas tal como se muestra en la Figura 12.

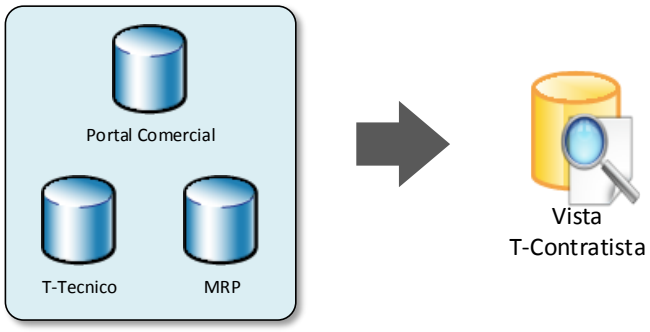


Figura 12. Vista T-Contratista

Para acceder a estos registros de usuario, el área responsable sólo otorgó una cuenta de acceso con permiso de lectura a la vista generada. Una ventaja posee esta base de datos es que se encuentra instalada en alta disponibilidad en la modalidad Activo-Activo. Esto permite por que se pueda asegurar la operatividad del servicio si alguna de los servidores que lo soporta tiene algún problema o se le realizan trabajos programados. Por otro lado, gracias a esta modalidad tiene la capacidad de atender una alta demanda de consultas mediante el balanceo de carga que provee esta tecnología.

4.2.2.2 CallCenter

La FAI CallCenter es el sistema que administra la información del personal de empresas que prestan servicio de atención post-venta de los clientes de Telefónica. Hoy en día, este sistema también es controlado por la Gerencia TI de Telefónica. La persistencia de este sistema esta implementada en una base de datos Oracle, y se ha dispuesto una cuenta de acceso con permisos de lectura para que se puedan extraer los registros desde la tabla de usuario. Cabe señalar que pueden existir coincidencias de registros de usuario almacenados tanto en T-Contratista como en CallCenter, lo que provoca un problema para determinar cuál es la FAI que posee el registro válido.

4.2.3 Active Directory

El Active Directory es un repositorio esencial para la plataforma de gestión de identidad, dado que solamente en ella se almacena “la cuenta de dominio” tanto para empleados internos como para el personal subcontratado de la compañía. En otras palabras, este sistema tiene username vigente para cualquier persona contenida en FAIs descritas anteriormente. Este atributo es importante debido a que es el identificador utilizado para la generación de cuentas de acceso a cualquier recurso de la infraestructura de red.

Hoy en día, esta fuente de datos de usuario se encuentra disponible en un ambiente de producción y es administrada por la Dirección de TI. La organización de este servicio de directorios es una estructura jerárquica donde un objeto se identifica mediante su Distinguished Name (DN)[7]. A través de la Figura 13 se puede ver la estructura principal de organización.

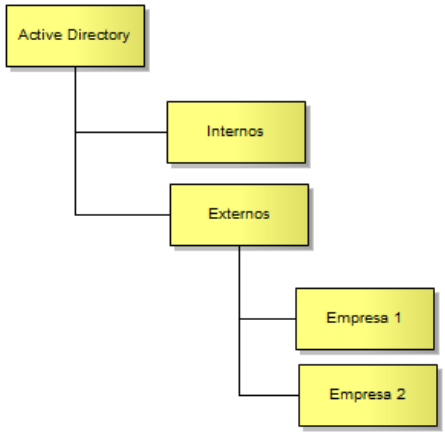


Figura 13. Estructura del Active Directory TChile

En esta estructura, los usuarios internos están en una sola rama independiente de la gerencia a la cual corresponden. En cambio para el personal externo, los usuarios se ordenan segmentadamente según la empresa a la cual pertenecen.

A pesar de que este sistema naturalmente puede ser un candidato perfecto para ser la FUAI, lamentablemente tiene algunas desventajas que impiden que sea el sistema de persistencia para la plataforma de gestión de identidad.

- ✓ La información de usuarios que se encuentra en esta FAI esta desactualizada, por lo que se pueden encontrar cuentas vigentes de usuarios desvinculados en la organización, lo que puede producir una brecha de seguridad.
- ✓ No es una fuente de datos controlada por la dirección de red, por lo que cualquier incidente en el AD provocaría una indisponibilidad de la plataforma de gestión de identidad, no pudiendo realizar acciones de contingencia cuando surja algún incidente.
- ✓ La infraestructura de los servicios de red y este Active Directory se encuentran en Centros de Procesamiento de Datos (CPD) distintos. Esto implicó la comunicación entre OIM y el Active Directory tuviera un rendimiento deficiente, debido a que la configuración de las redes no se encontraba implementada para soportar grandes cantidad de transmisión de información
- ✓ Existen otros tipos de usuarios que el Active Directory, no tiene contemplado administrar, como lo son las excepciones (usuarios clientes, visitas y auditores).

[7] DN: identificador único de un objeto en el sistema LDAP.

4.3 Provisión de Cuentas de Accesos en la Infraestructura de Red

La dirección de TI es la responsable de la creación de las cuentas de usuario de funcionarios internos y externos en su Active Directory mediante el proceso de enrolamiento. Producto de ello, se les generan algunas herramientas básicas de gestión, como lo son: correo electrónico, cuenta MyPass[8] y otros recursos ofimáticos.

Pese a esta facilidad, lamentablemente no es posible generar automáticamente las cuentas de acceso en los recursos de la infraestructura de red. La razón de ello, es que existe una diversidad y complejidad en los sistemas e infraestructura de la Dirección de red que exige un alto grado de conocimiento técnico en la administración de acceso a este equipamiento. Ante el escenario expuesto, se hace imposible la derivación del otorgamiento de accesos hacia los elementos de red a otras unidades funcionales de la organización, como la Dirección de TI.

Hasta antes de la implementación de este proyecto, el otorgamiento de acceso para los usuarios se realizaba mediante una solicitud vía mail a la Dirección de Red. Comúnmente era el envío de un formulario, donde se especificaba el servicio de comunicaciones al cual se requería acceso. El administrador de la red tomaba manualmente la solicitud y buscaba el nombre de usuario en el AD de la Dirección de TI, y generaba una nueva credencial de acceso para el usuario en su propio sistema. A continuación en la Figura 14 se grafica el proceso descrito anteriormente.

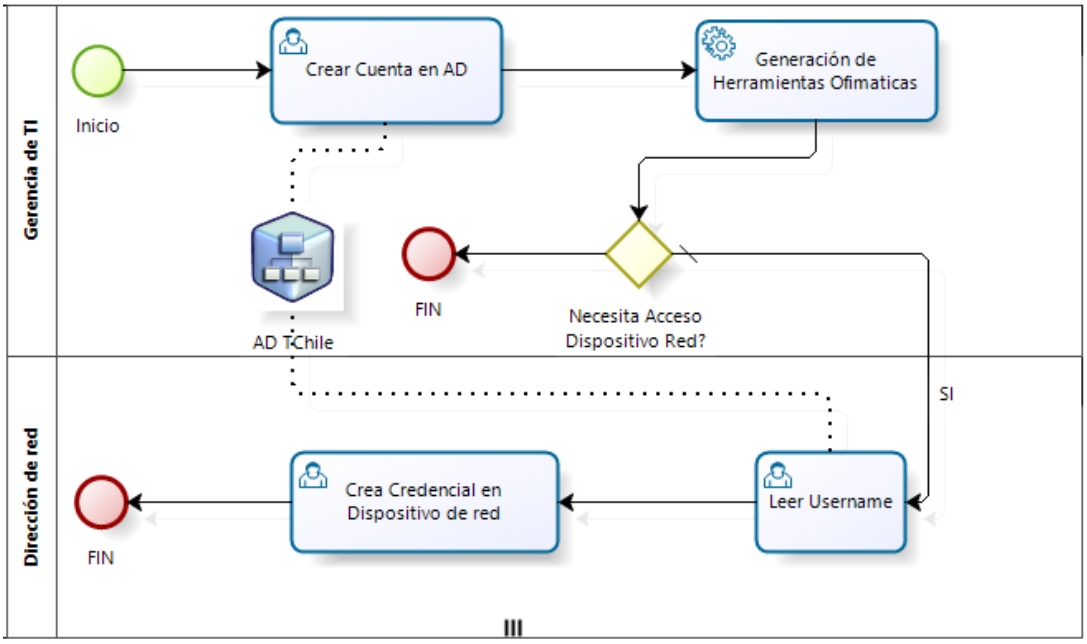


Figura 14. Proceso de Generación de Cuenta en AD

En este sentido, el contar con una FUAI autónoma en la Dirección de Red cobra valor, debido a que es controlado y supervisado por esta unidad organizacional. Esta característica, permite que tenga las siguientes ventajas:

[8] MyPass: Sistema propietario de Telefónica para el restablecimiento de la contraseña del Active Directory.

- ✓ Se mejora el rendimiento de la plataforma, dado a que se configuró e implementó una red LAN dedicada exclusivamente a las necesidades de rendimiento y comunicación que tienen las aplicaciones que conforman el Sistema IDM.
- ✓ Se mejora el control y auditoría al segmentar el Tráfico de red mediante 2 VLAN[9], una dedicada a los Servicios que provee la plataforma a los usuarios y la otra enfocada a la administración de los sistemas que lo conforman para el equipo de soporte de OIM.
- ✓ Mediante el Proceso de Normalización (que se verá en el punto 4.5) se automatiza la obtención de cuenta de dominio.
- ✓ Las identidades que nutrirán esta FUAI, estarán normalizadas y estandarizadas para que respondan las necesidades de negocio de la Dirección de Red. Esto implica que ya no es necesario que OIM haga adaptaciones y transformaciones con sus precarias y rígidas herramientas.

4.4 Diseño de la Fuente Única Autoritativa de Identidad

Como es comprensible, la construcción de una fuente autoritativa de identidad suficientemente flexible para responder las necesidades de todas las unidades organizativas y aplicaciones de negocio de Telefónica resultaría altamente costosa, compleja y tardaría demasiado tiempo para su implementación.

Ante esta situación, se determinó que se construyera una FUAI en la cual se unifiquen los registros de usuario de todos los repositorios de datos relevantes anteriormente mencionados. De esta forma, la FUAI fue diseñada e implementada con el fin de responder eficientemente a las necesidades particulares de la gestión de Identidad para la Dirección de Red.

Para el diseño de la FUAI, sólo se contemplaron los atributos de usuario relevantes para la plataforma de gestión de identidad. Estos campos fueron extraídos desde las fuentes de identidad detalladas en el punto 4.2. Se debe considerar que algunos de los valores de estos atributos serán calculados o extraídos de otras fuentes de datos persistentes (Ej: AD TChile) para completar el registro de la identidad digital de la Dirección de Red. A continuación, se indican cuáles son los atributos de identidad considerados para la nueva plataforma OIM.

- ✓ **Rut**: Atributo que identifica de manera única a una identidad.
- ✓ **Username y Password**: Es la cuenta de dominio existente en el AD. Esto es para que un usuario no tenga que recordar más de una credencial para que pueda acceder a los sistemas de Telefónica de forma transversal.
- ✓ **Nombre Completo**: Nombres y apellidos.
- ✓ **Estado**: Indica si el usuario se encuentra vigente o desvinculado a la empresa.
- ✓ **Estado OIM**: Señala si el registro es válido para ser utilizado en la plataforma de gestión de identidad.
- ✓ **Rut Empresa**: Para los usuarios externos indica la empresa proveedora de servicios de Telefónica. Para los usuarios internos es la misma empresa Telefónica.

[9] VLAN: es un método para crear redes lógicas independientes dentro de una misma red física.

- ✓ **Fecha Inicio Contrato**: Es la fecha en la cual la persona comienza a prestar servicio a Telefónica.
- ✓ **Fecha Fin Contrato**: Es la fecha en la que la persona deja de prestar servicios para Telefónica.
- ✓ **Unidad de Negocio**: Es la división funcional que tiene telefónica para sus procesos de negocio.
- ✓ **Teléfono**: Indica el número del celular o fijo de contacto del usuario.
- ✓ **Correo Electrónico**: indica el email corporativo del trabajador.
- ✓ **Cargo**: Es el puesto de trabajo que tiene el empleado.
- ✓ **Comuna**: Ciudad donde se encuentra trabajando actualmente el usuario.
- ✓ **Lugar de Trabajo**: lugar físico donde el usuario cumple comúnmente sus funciones.

4.5 Proceso de Normalización

El proceso de normalización corresponde a la extracción, estandarización, validación y unificación de registros de usuarios desde las FAIs en una FUAI con identidades limpias, sin errores y enfocadas a responder las necesidades de integración del proceso de reconciliación. A continuación en la Figura 15 se detallan las actividades del proceso.

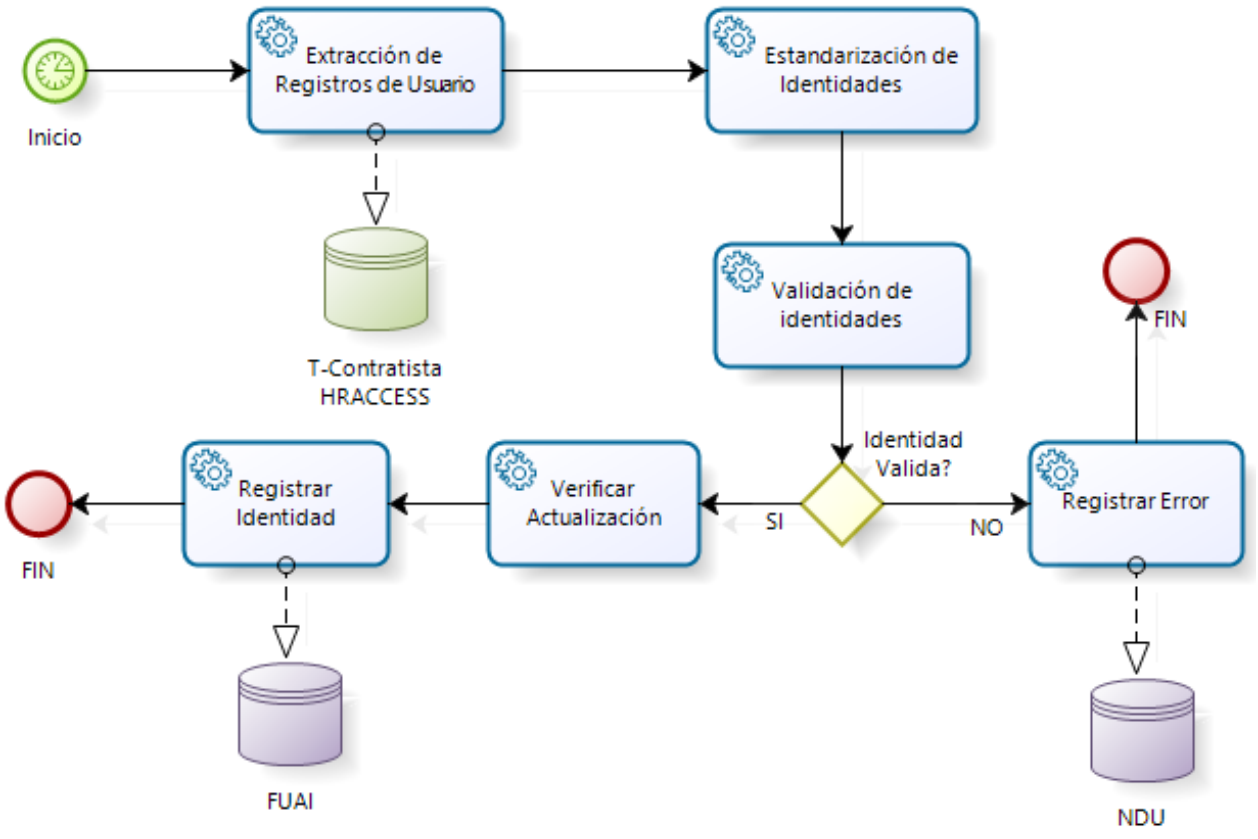


Figura 15. Modelo del Proceso de Normalización

4.5.1 Extracción de Registros de Usuarios

Esta actividad corresponde a la obtención de registros de usuarios desde las distintas FAIs disponibles en la organización. Como es comprensible, los responsables de los distintos repositorios tienen políticas de seguridad de acceso que se deben cumplir y acatar, tales como:

- ✓ Acceso restrictivo sólo de lectura, sin permisos de modificación.
- ✓ Acceso prohibido a información privada de los usuarios. Ejemplo: remuneraciones.

Esta extracción de datos se realizó en distintos tipos de FAI, tales como: heterogéneas bases de Datos y Servicios LDAP. En muchas ocasiones, se descartó información del usuario poco relevante para la plataforma OIM, como por ejemplo: sindicatos, isapres, AFP y mutuales de salud.

4.5.2 Estandarización de Identidades

Esta actividad corresponde a homogeneizar los valores de los atributos de las identidades provenientes de distintas FAIs consiguiendo así identidades consistentes y comparables entre sí. Esta actividad consistió en una serie de transformaciones y adaptaciones a los valores de los atributos de identidades para que los registros posean los mismos formatos y convenciones de forma se puedan comparar los usuarios provenientes desde distintas FAIs.

Esta actividad es una de las más relevantes, dado que de esta forma la información de las identidades se pueden tabular y generar reportes para los requerimientos de auditoría. Otro beneficio de la estandarización, es la mejora en el rendimiento de las consultas a la FUAI por parte de OIM, disminuyendo el tiempo de la reconciliación (En la versión OIM 9 tardaba 4 horas y actualmente demora 50 minutos en la versión OIM 11).

Por otro lado, existen los mismos atributos en diferentes FAIs que mantienen una nomenclatura totalmente heterogénea. En este caso, se debió construir un formateador por cada repositorio de usuario. Si bien es cierto estos casos fueron acotados, exigió un sobreesfuerzo pero permitió que el motor principal de formateo fuera homogéneo.

4.5.3 Validación de Identidades

Esta actividad consiste en realizar una certificación de las identidades estandarizadas. Para esto, se validó la correctitud y completitud de los valores de los atributos de los registros de usuario. Para las validaciones fallidas, los errores son almacenados en la base de datos local del NDU. Estos errores pueden ser consultados en el Front-End (FE) de la aplicación NDU.

La principal característica de los validadores es que son reutilizables independiente de la FAI de procedencia de las identidades. Incluso pueden ser parametrizables para ser utilizadas en más de un atributo de usuario.

4.5.4 Tratamiento de Colisión de Identidades

A diferencia de las tareas anteriores, este proceso solamente se ejecuta bajo una condición:

La existencia de un mismo registro de usuario activo en distintas FAIs

Si se produce este caso, el proceso de tratamiento de colisiones será el encargado de determinar la FAI desde donde se tomará el registro de usuario que se dispondrá en la FUAI. Estas situaciones son registradas y pueden ser consultadas en el FE de la aplicación NDU. Estos casos son claramente una brecha en la seguridad de la información que mantiene Telefónica, por lo que es necesario analizarlo (Se corre el riesgo de otorgar cuentas de acceso a personal desvinculado de la organización). Las reglas de tratamiento de colisiones de identidades son configurables, por lo que pueden cambiar los lineamientos de negocio y solamente se deberá actualizar este componente sin afectar el resto del middleware NDU.

4.5.5 Consolidación de Identidades

Este es el último paso del flujo de normalización y corresponde al registro de las identidades estandarizadas y validadas en la FUAI. Esta fuente de datos pertenece a la Dirección de Red, la cual es autónoma, con servicios de monitoreo y respaldo que asegura el correcto funcionamiento del proceso de reconciliación.

Por otra parte, también se almacenan los registros de usuarios no válidos (registros de usuario que presentan errores).

4.6 Arquitectura de Componentes de la Aplicación NDU

El middleware NDU es una aplicación empresarial JEE[10] responsable de controlar el proceso de normalización de identidades de una manera automática, periódica y configurable. En la Figura 16 se esquematiza la arquitectura que tiene la aplicación empresarial NDU, que soporta este proceso y su relación con el mecanismo de reconciliación de OIM.

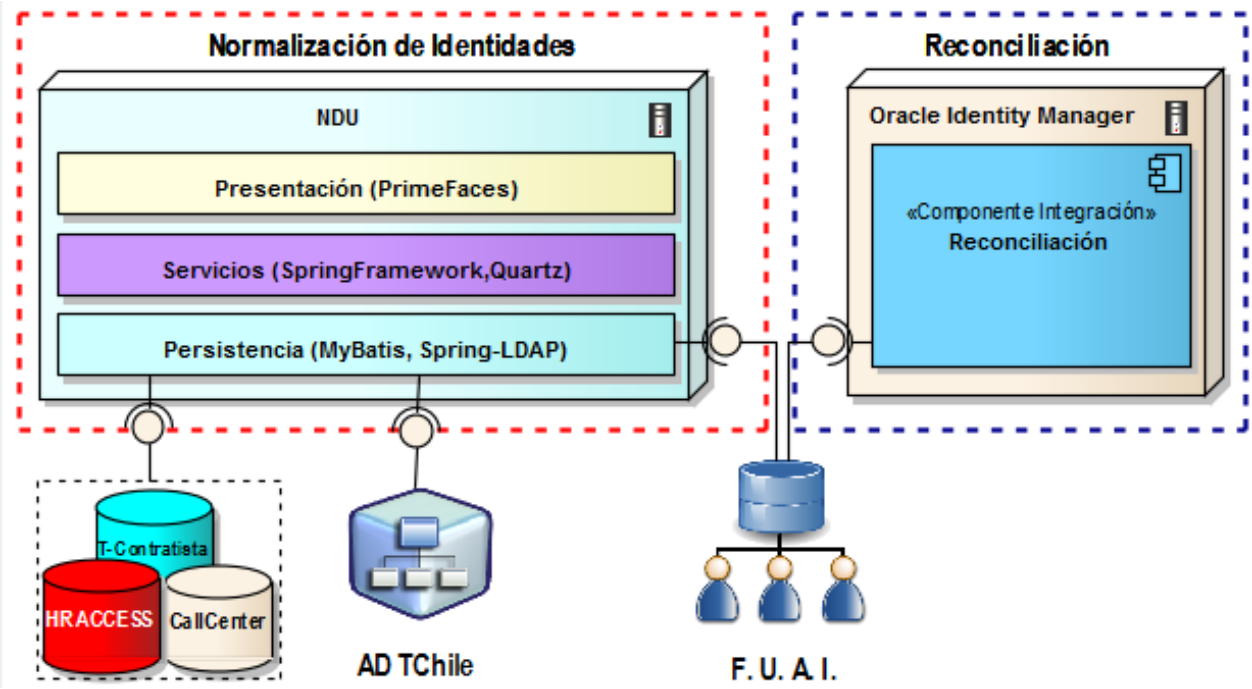


Figura 16. *Esquema Funcional del Middleware NDU*

Tomando en cuenta las preocupaciones de mantenimiento y de interoperabilidad, este middleware fue diseñado en una arquitectura de 3 capas e implementado en la tecnología JEE (acorde las normativas de construcción de software vigente en la compañía). Por otro lado, para abordar los aspectos transversales y comunes del proceso de normalización se utilizó la tecnología AspectJ con Spring AOP (Programación Orientada a Aspectos).

[10] Aplicación JEE: Es una aplicación empresarial desarrollada en el lenguaje de programación Java.

4.6.1 Arquitectura NDU por Capas

En la Figura 17 se presenta el diagrama de componentes de la aplicación NDU integrándose a los diferentes repositorios de registros de usuarios y FUAI.

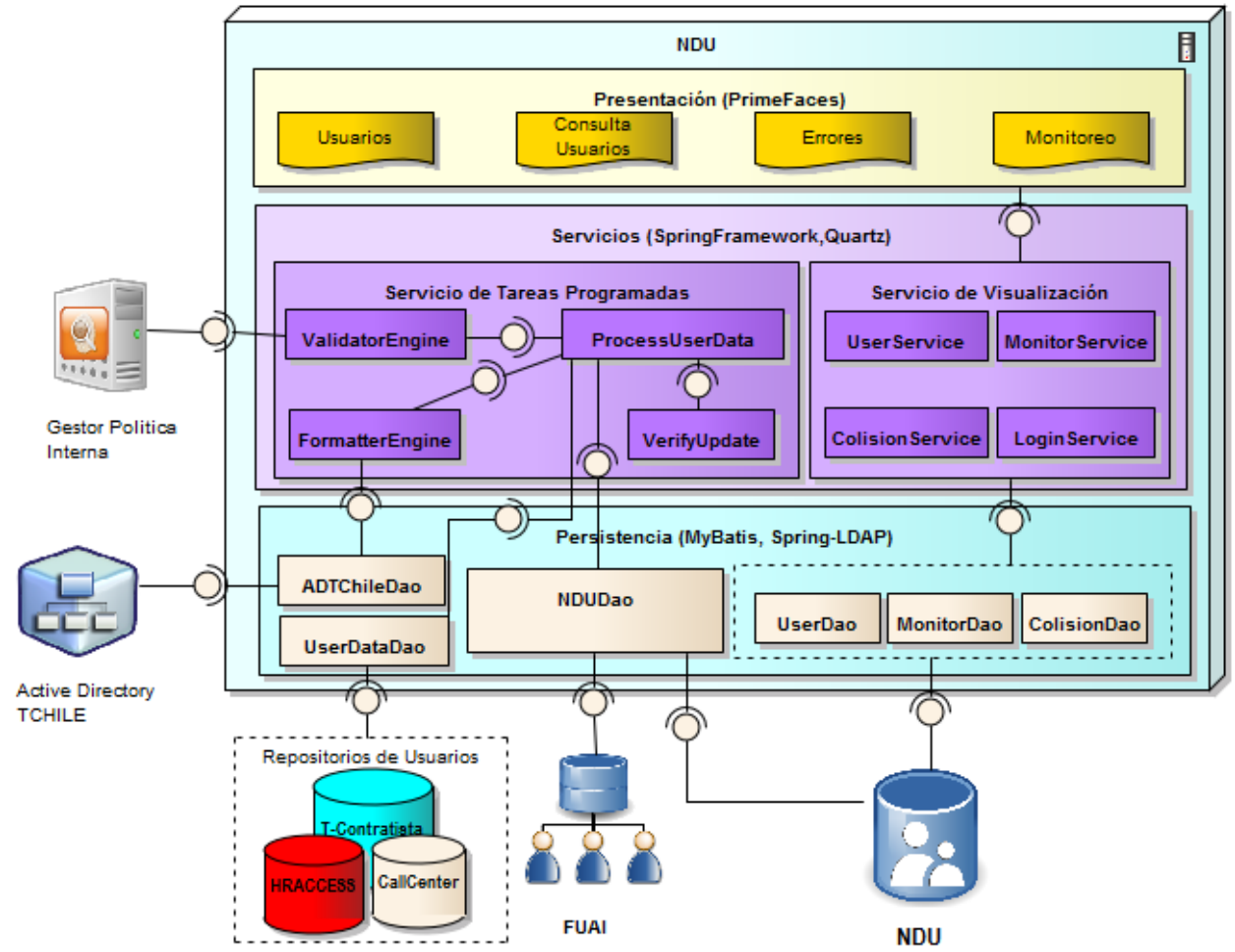


Figura 17. Diagrama de Componentes NDU

A continuación en los siguientes puntos se describirán todos los componentes del middleware NDU agrupados por capas.

4.6.1.1 Diseño de la Capa de Presentación

La capa de presentación corresponde a un módulo Web en el cual principalmente se visualizan los resultados del proceso de normalización, tales como:

- ✓ Consulta de Usuarios: En este módulo se muestran las identidades formateadas y normalizadas desde la FUAI. Junto con esto, se puede ver los registros de usuario que contienen errores encontrados durante la ejecución del proceso de normalización (fila en color naranja) tal como lo muestra la Figura 18.

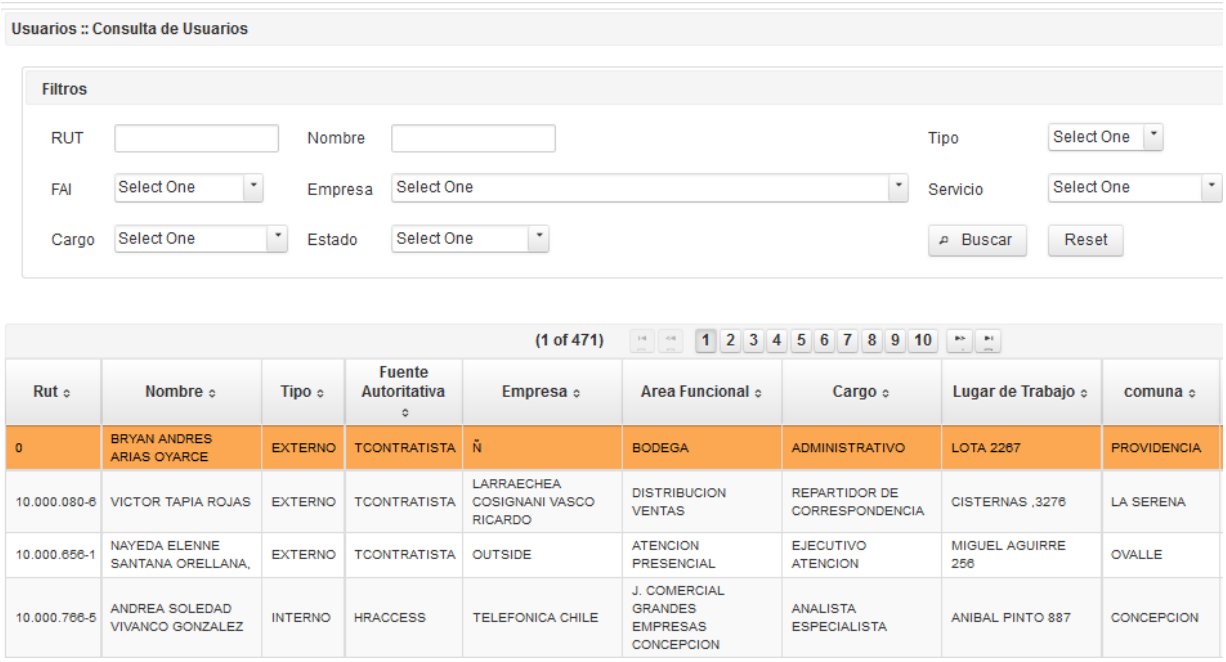


Figura 18. Página Consulta de Usuario

- ✓ Errores: En este módulo se puede apreciar los usuarios que contienen errores categorizados por empresa ó por FAI, como se muestra en la Figura 19 y 20.

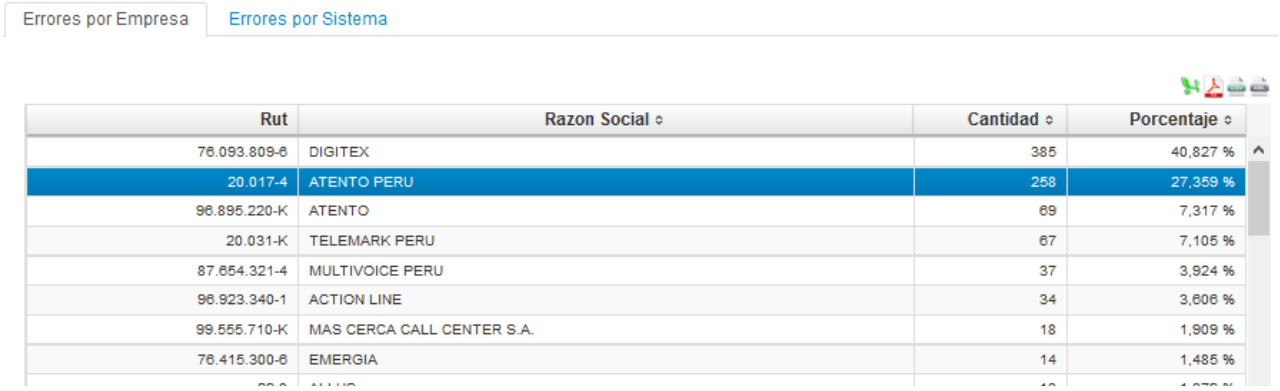


Figura 19. Errores por Empresas

En la Figura 20, se puede apreciar que la FAI que contiene más errores es CallCenter, seguida por T-Contratista y HRACCESS la cual no contiene ninguna identidad con error.

Codigo	Fuente Autoritativa	Cantidad	Porcentaje
3	CALLCENTER	910	96,501
2	TCONTRATISTA	33	3,499

Figura 20. Errores por Sistema

- ✓ Monitoreo: En esta sección de la aplicación web, se presenta el estado del proceso de normalización actual y los que ya se han ejecutados en períodos anteriores. Así mismo, se puede ver el rendimiento en tiempo y cantidad de usuarios considerado en el proceso de normalización para diferentes FAI, como se visualiza en la Figura 21.

Numero	Sistema	Estado	Inicio	Termino	Duracion	Cantidad
756	HRACCESS	OK	01-05-2015 03:02:04	01-05-2015 03:05:15	3 min, 11 sec	4.552
756	TCONTRATISTA	OK	01-05-2015 03:33:42	01-05-2015 04:18:29	44 min, 47 sec	34.263
756	CALLCENTER	OK	01-05-2015 03:05:15	01-05-2015 03:33:34	28 min, 19 sec	31.505
755	HRACCESS	OK	30-04-2015 03:02:04	30-04-2015 03:05:30	3 min, 26 sec	4.557
755	TCONTRATISTA	OK	30-04-2015 03:31:01	30-04-2015 04:17:39	46 min, 38 sec	34.223
755	CALLCENTER	OK	30-04-2015 03:05:31	30-04-2015 03:30:55	25 min, 24 sec	31.505
754	HRACCESS	OK	29-04-2015 03:02:04	29-04-2015 03:05:21	3 min, 17 sec	4.523
754	TCONTRATISTA	OK	29-04-2015 03:31:08	29-04-2015 04:08:30	37 min, 22 sec	34.173
754	CALLCENTER	OK	29-04-2015 03:05:21	29-04-2015 03:31:02	25 min, 41 sec	31.507
753	HRACCESS	OK	28-04-2015 03:02:03	28-04-2015 03:05:57	3 min, 54 sec	4.578

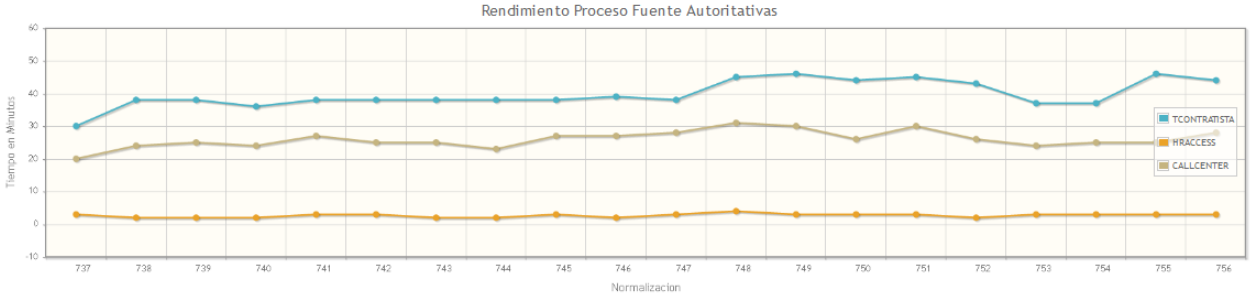
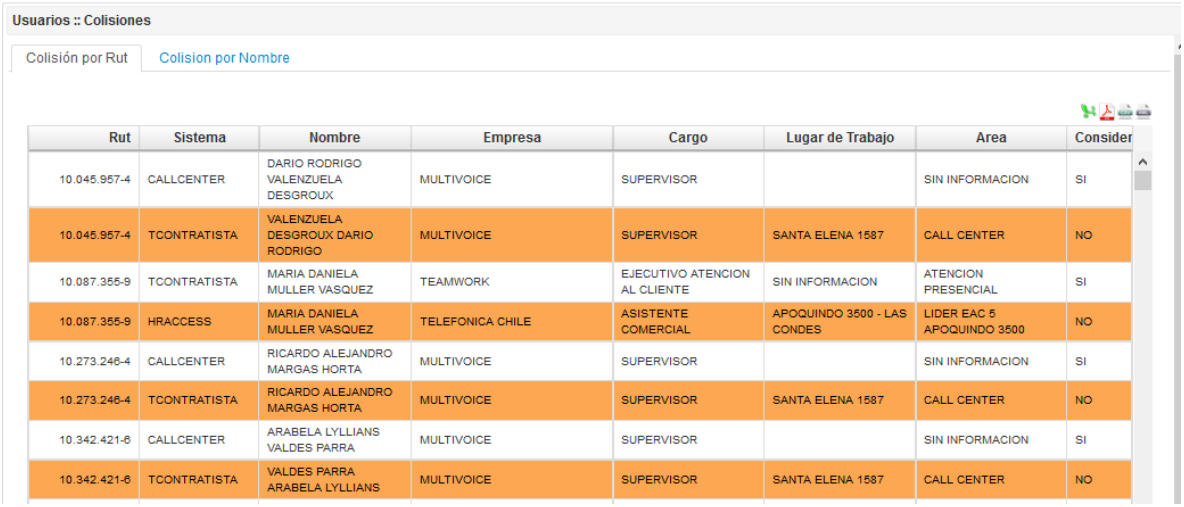


Figura 21. Monitorización del Proceso de Normalización

- ✓ Colisión: la información que se presenta en esta sección de la aplicación NDU es una de las más importantes y corresponden a las colisiones de identidad. Esta situación identifica posible brechas de seguridad dentro de la organización. Al estar duplicado un registro de un usuario, puede tener acceso a sistemas después de ser desvinculado. Las colisiones de identidad, se pueden presentar de dos formas:

    - Mediante el RUT desde distintas FAI, como se ve en la Figura 22.



Usuarios :: Colisiones

Colisión por Rut | Colision por Nombre

Rut	Sistema	Nombre	Empresa	Cargo	Lugar de Trabajo	Area	Consider
10.045.957-4	CALLCENTER	DARIO RODRIGO VALENZUELA DESGROUX	MULTIVOICE	SUPERVISOR		SIN INFORMACION	SI
10.045.957-4	TCONTRATISTA	VALENZUELA DESGROUX DARIO RODRIGO	MULTIVOICE	SUPERVISOR	SANTA ELENA 1587	CALL CENTER	NO
10.087.355-9	TCONTRATISTA	MARIA DANIELA MULLER VASQUEZ	TEAMWORK	EJECUTIVO ATENCION AL CLIENTE	SIN INFORMACION	ATENCION PRESENCIAL	SI
10.087.355-9	HRACCESS	MARIA DANIELA MULLER VASQUEZ	TELEFONICA CHILE	ASISTENTE COMERCIAL	APOQUINDO 3500 - LAS CONDES	LIDER EAC 5 APOQUINDO 3500	NO
10.273.246-4	CALLCENTER	RICARDO ALEJANDRO MARGAS HORTA	MULTIVOICE	SUPERVISOR		SIN INFORMACION	SI
10.273.246-4	TCONTRATISTA	RICARDO ALEJANDRO MARGAS HORTA	MULTIVOICE	SUPERVISOR	SANTA ELENA 1587	CALL CENTER	NO
10.342.421-6	CALLCENTER	ARABELA LYLLIANS VALDES PARRA	MULTIVOICE	SUPERVISOR		SIN INFORMACION	SI
10.342.421-6	TCONTRATISTA	VALDES PARRA ARABELA LYLLIANS	MULTIVOICE	SUPERVISOR	SANTA ELENA 1587	CALL CENTER	NO

Figura 22. Colisiones por Rut

- Por coincidencias de dos registros, que tengan el mismo nombre, el mismo cargo, se desempeñen en la misma unidad funcional, pero que estén registrados con diferente RUT. Si bien esta situación no es considerada como error, es sumamente sospecho por lo que amerita un análisis de mayor profundidad, como se aprecia en la Figura 23.

Usuarios :: Colisiones

Colisión por Rut | Colision por Nombre

Rut	Nombre	Tipo	Fuente Autoritativa	Empresa	Area Funcional	Cargo	Lugar de Trabajo	comuna	Estado	Fecha Ingreso	Fecha Egreso
80.005.383-8	ALDEMAR DIAZ OSORIO	EXTERNO	TCONTRATIST.	DIGITEX INTERNACIONA LTDA	MOVIL	ASESOR	CRA 3 A # 9 30, VILLA DIANA, VILLAMARIA	SIN REFERENCIA	HABILITADO	15-04-2013	31-12-2999
80.002.392-0	ALDEMAR DIAZ OSORIO	EXTERNO	TCONTRATIST.	DIGITEX INTERNACIONA LTDA	MOVIL	ASESOR	CRA 3 A # 9 30, VILLA DIANA, VILLAMARIA	SIN REFERENCIA	HABILITADO	01-01-2013	31-12-2999
80.000.023-8	BIBRIANTH GABRIELA SALAZAR CEBALLOS	EXTERNO	TCONTRATIST.	DIGITEX INTERNACIONA LTDA	SIN INFORMACION	SIN INFORMACION			HABILITADO	20-06-2013	31-12-2999
80.006.444-9	BIBRIANTH GABRIELA SALAZAR CEBALLOS	EXTERNO	TCONTRATIST.	DIGITEX INTERNACIONA LTDA	SIN INFORMACION	SIN INFORMACION			HABILITADO	04-07-2013	31-12-2999

Figura 23. Colisiones por Nombre

4.6.1.2 Implementación de la Capa de Presentación

Para la implementación de la capa de presentación, se utilizó el framework PrimeFaces V 5.0 basada en la especificación JSR 344 [10]. Se optó por utilizar esta tecnología opensource por su característica de alta usabilidad, interacción y mejoramiento de la experiencia del usuario, la que hoy es ampliamente aceptada en la industria según el Ranking del portal DevRates[11] [17]. Otros beneficios que destaca particularmente el fabricante acerca de este producto son: flexibilidad, rendimiento, portabilidad e integración con otros marcos de trabajo, como tomando como referencia la tecnología Java [11]. Cabe señalar que este marco de trabajo utiliza como patrón arquitectónico de la capa de presentación Modelo-Vista-Controlador (MVC):

- ✓ La capa vista está compuesta por páginas XHTML con componentes visuales que embeben comunicación Ajax mediante Jquery. Esta característica favorece el rendimiento de la interfaz web, dado a que solamente se actualizan componentes visuales requeridos y no necesariamente toda la página web.
- ✓ El modelo está compuesto por clases Java llamadas ManageBean. Estas entidades son las encargadas gestionar en envío y recepción de información hacía la Vista. Para realizar el intercambio de información entre la Vista y los ManageBean, se utilizan artefactos especiales llamados Data Tranfer Object[12] (DTO).
- ✓ El controlador de este framework es mediante un XML que especifica los flujos de navegación que tiene la aplicación. También este componente se puede representar mediante anotaciones, las cuales son interpretadas por el componente Servlet Controller Faces.

A continuación en la Figura 24 se muestra el esquema general del funcionamiento de este modelo.

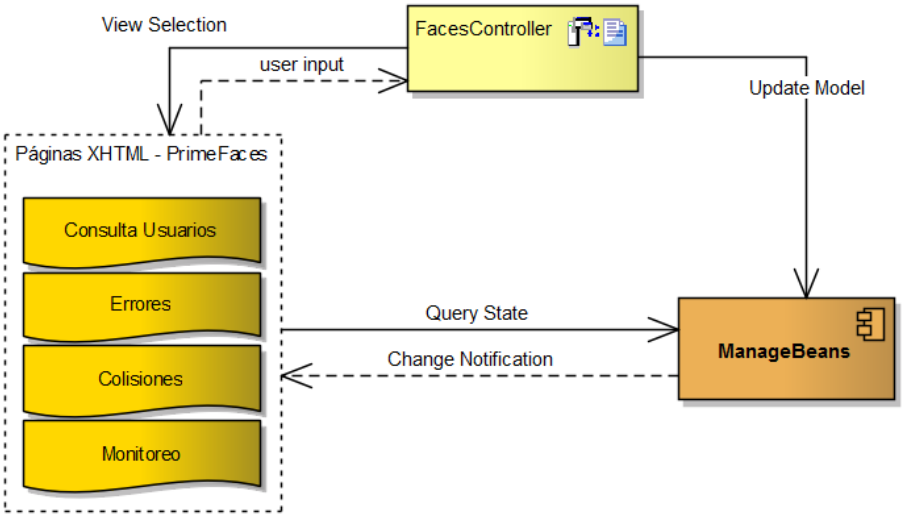


Figura 24. Funcionamiento del Framework Primefaces

[11] DevRates: Sitio Web que valora las tecnologías según las experiencias de los desarrolladores.
[12] DTO: Entidad que encapsula los datos de negocio para optimizar la comunicación entre capas.

4.6.1.3 Diseño de Capa de Servicios

La capa de servicios especifica la lógica y reglas de negocio que contiene las principales funciones de la aplicación. En el caso del middleware NDU es la encargada de ejecutar las siguientes actividades.

- ✓ Controlar y coordinar las tareas del proceso de normalización.
- ✓ Presentar los resultados de proceso de normalización mediante servicios de consultas.

A continuación se describen las responsabilidades de los componentes que forman parte de esta capa.

4.6.1.3.1 SchedulerService

Es el servicio encargado de iniciar periódica y automáticamente el proceso de normalización de identidades. Cabe señalar que la periodicidad y horario de ejecución para las tareas programadas de este módulo son parametrizables mediante un archivo de propiedades.

4.6.1.3.2 ProcessUserDataService

Este servicio se representa mediante la aplicación de una Fachada[13] para el proceso de normalización de identidades. En cuanto a su diseño, se provee una interfaz simple y desacoplada implementación, permitiendo ser actualizada sin impactar otros componentes de la solución (Ejemplo: SchedulerService). Los componentes que forman parte de este servicio cumplen con las siguientes características: independencia, portabilidad y reutilización. En la Figura 25, se presentan todos los elementos en el diseño de este módulo.

[13] Fachada: Patrón de diseño que proporciona una interfaz simplificada para un grupo de servicios o un sistema complejo.

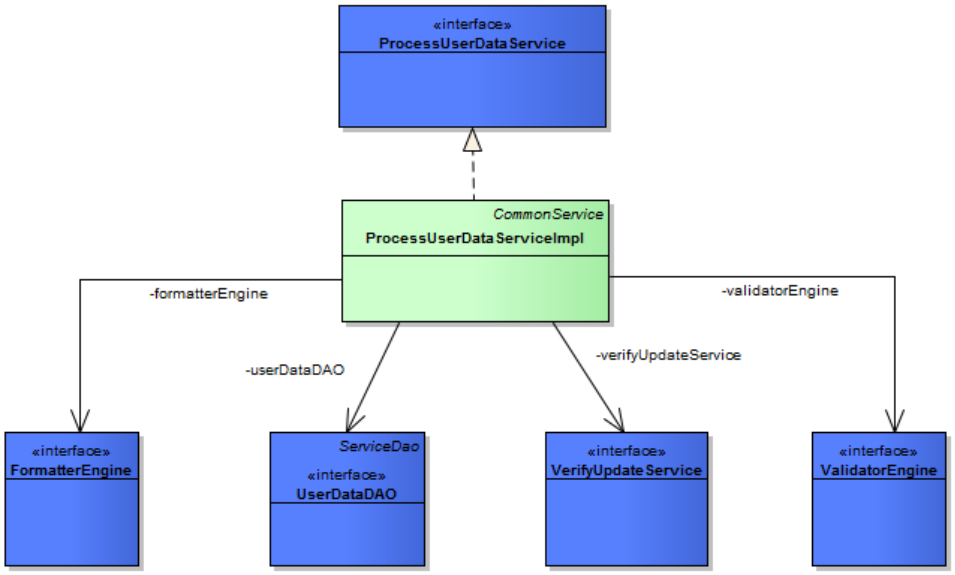


Figura 25. Implementación del Módulo de Procesamiento de Datos de Usuario

A continuación se detallan cada uno de los componentes que conforman este servicio.

4.6.1.3.3 FormatterEngine

Este componente es el encargado de estandarizar los formatos de los atributos de usuario provenientes desde diferentes FAIs. Este motor lo componen un conjunto de formateadores que actúan sobre los atributos de usuario para convertirlos en registros homogéneos. La importancia de este componente es que al estandarizar las identidades, estas se podrán comparar y validar sin importar la FAI de origen.

El diseño de este componente tiene las siguientes características:

- ✓ Su funcionamiento se expone a través de una interfaz, la cual recibe a los usuarios directamente de la FAI de origen para formatearlos.
- ✓ La implementación de esta interfaz contiene un conjunto de ítems formateadores que procesan los atributos de cada uno de los usuarios para estandarizarlos.
- ✓ Todos los ítems formateadores implementan una misma interfaz. De esta manera, el motor realiza una iteración sobre el conjunto de formateadores de forma transparente, sin importar el atributo a formatear.

A continuación en la Figura 26, se presenta el diagrama de clase de este componente.

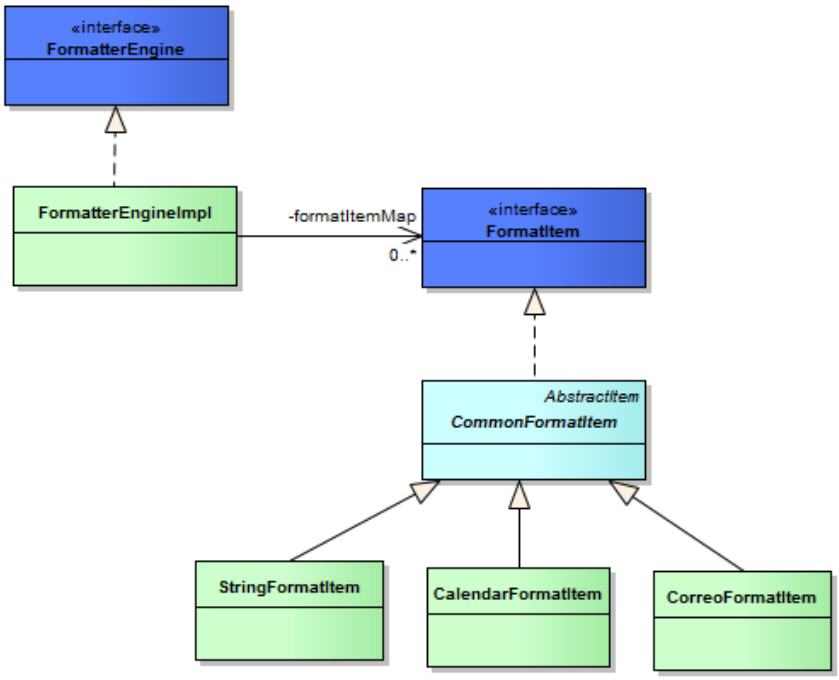


Figura 26. Diagrama de Clases Formateadores

Por otra parte, los atributos de usuarios son obtenidos mediante una clase de apoyo, para posteriormente aplicarle a cada uno de ellos un ítem formateador, como se presenta en el diagrama de secuencia de la Figura 27.

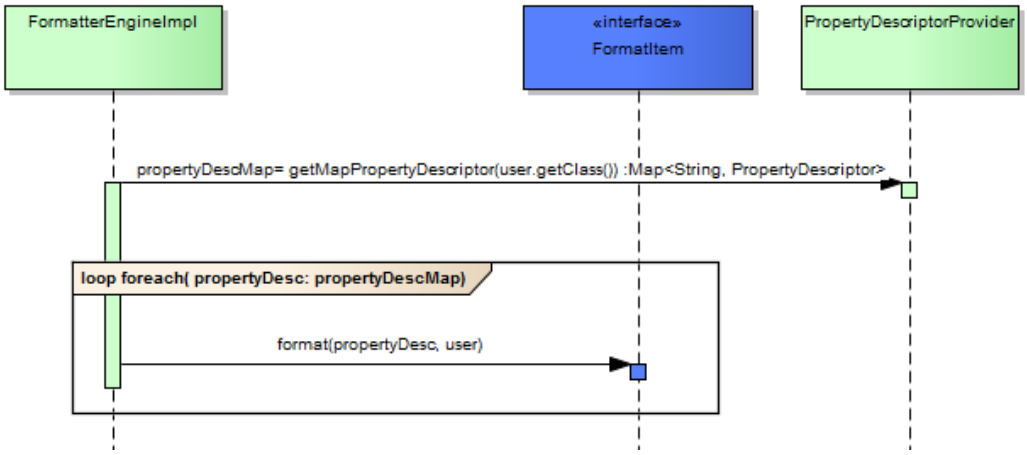


Figura 27. Diagrama de Secuencia del Formateador

4.6.1.3.4 ValidatorEngine

Este componente representa el motor de validación de identidades. Su objetivo es determinar si un registro de usuario cumple con todos los requisitos para poder almacenarse como identidad válida en la FUAI.

El diseño de este módulo es similar al motor formateador. La interfaz de este componente recibe una identidad formateada y entrega el conjunto de errores encontrados por cada ítem de validación. En el caso que no se encuentren errores, la respuesta es nula. Seguidamente en la Figura 28, se presenta el diagrama de clase de este componente.

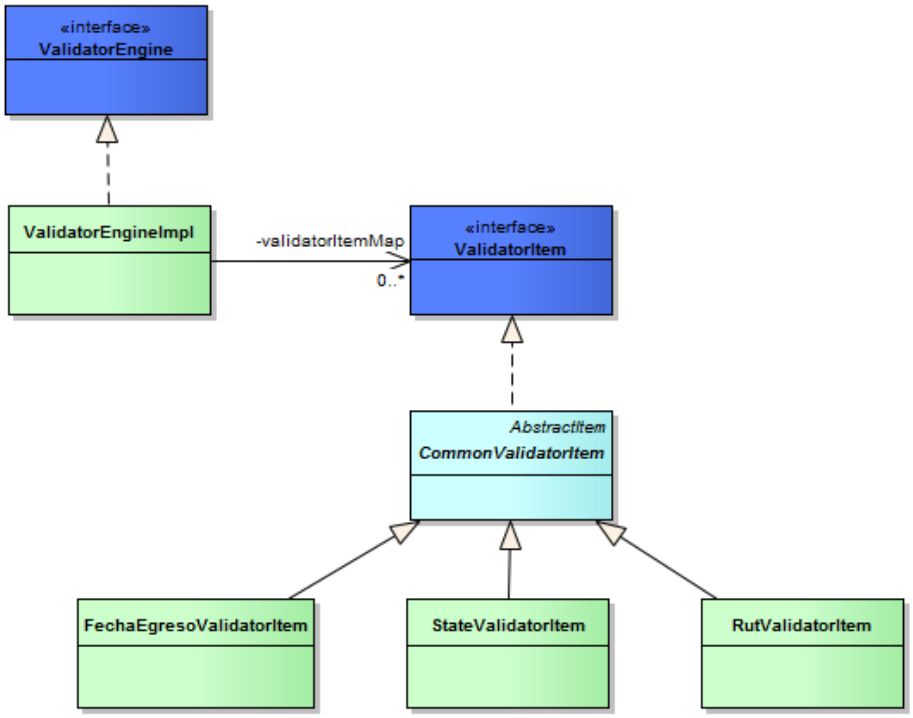


Figura 28. Diagrama de Clases Validadores

Al igual que el funcionamiento de los formateadores, el motor de validación realiza una iteración sobre los atributos críticos a validar a los que les corresponde la aplicación de un validador específico. Los atributos a validar son los siguientes:

- ✓ RUT.
- ✓ Fecha de Egreso.
- ✓ Estado del Usuario.

A continuación, en la Figura 29 se presenta el diagrama de secuencia del funcionamiento de este componente.

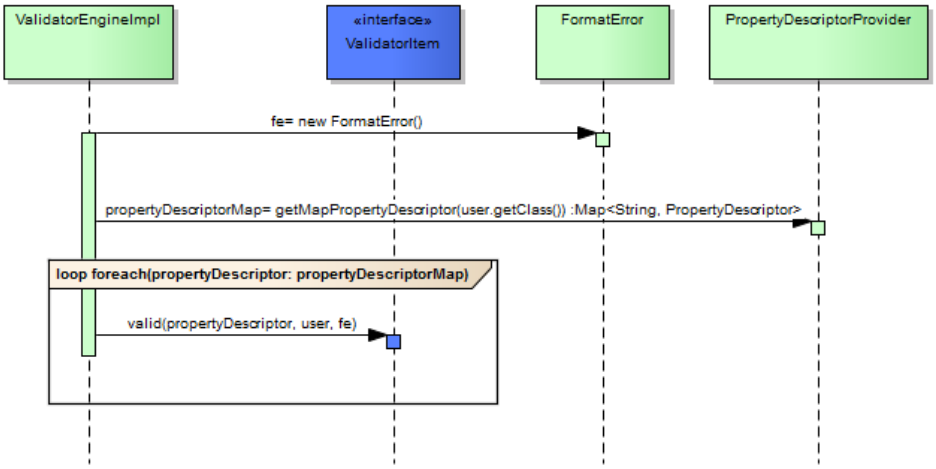


Figura 29. Diagrama de Secuencia del Módulo de Validación

4.6.1.3.5 VerifyUpdate

Este componente de negocio tiene la responsabilidad de determinar si una identidad debe ser o no actualizada. Las condiciones de actualización de la identidad son las siguientes:

- ✓ Los registros válidos desde la FAI HRACCESS siempre son actualizados, debido que es repositorio que cuenta con los mayores niveles de confiabilidad.
- ✓ Los registros válidos que tengan actualización en algunos de sus atributos, siempre son actualizados.
- ✓ Si un registro válido es actualizado y presenta errores, el usuario es modificado quedando en estado inválido.
- ✓ Un caso especial son las colisiones de identidad, o sea, un mismo usuario que se encuentre activo en dos o más FAI. Para resolver esta situación, primero se verifica si la identidad pertenece a HRACCESS la cual tiene prioridad, de lo contrario se evalúan las fechas de ingreso a cada una de las FAIs, siendo el registro válido el que tenga una fecha de ingreso posterior.

4.6.1.4 Implementación de la Capa de Negocio

En cuanto a la implementación de la capa de negocio, cabe señalar que todos los servicios provistos son construidos mediante el Patrón de Diseño llamado “Dependency Inyection” utilizado en el Framework Spring en su versión 3.2.2. La elección de este framework para la construcción de esta capa tiene las siguientes justificaciones:

- ✓ Dada la heterogeneidad existente de las diferentes FAI, el Framework Spring ofrece la flexibilidad de integrarse con tecnologías de diversos fabricantes. Por ejemplo: Hibernate, MyBatis, JPA, LDAP, etc.

- ✓ Es un framework que es constantemente actualizado. En poco tiempo ha integrado un conjunto de nuevas tecnologías y patrones arquitectónicos. Esta característica resulta importante para la construcción del middleware, ya que entrega un soporte sustentable que permite enfrentar de mejor forma las periódicas migraciones o upgrades que se realizan sobre las FAIs.
- ✓ Es mantenible y tiene un bajo nivel de acoplamiento. De esta forma, en la aplicación sólo se utilizan servicios en forma de interfaces, aislando su implementación mediante archivos de configuración XML. Esta característica permite actualizar las implementaciones de los servicios sin afectar el comportamiento general del sistema.
- ✓ El framework Spring ofrece la capacidad de poder desplegarse en distintos servidores de aplicaciones. Esto permite abstraerse del fabricante del servidor de aplicaciones para desplegar el middleware NDU, ejemplo: Websphere (IBM) o WebLogic (Oracle).

En la Figura 30, se presenta el diagrama de clase de la capa de servicio mediante archivos XML de configuración Spring.

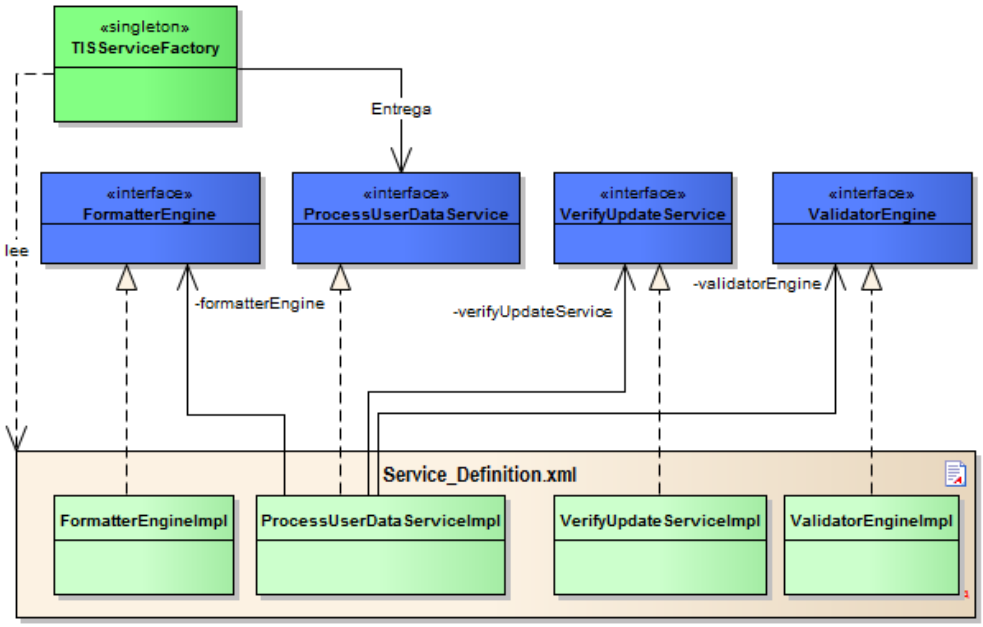


Figura 30. Diagrama de Clase de la Capa de Servicio

En la Figura 31, se presenta el diagrama de secuencia que siguen los elementos utilizados en esta capa.

Figura 31. Diagrama de Secuencia del Proceso de Normalización

4.6.1.5 Diseño de la Capa de Persistencia

La capa de persistencia de este middleware tiene 2 funciones:

- ✓ La primera labor de esta capa, es extraer los registros de usuarios desde las bases de datos que representan todas las FAIs de la organización.
- ✓ La segunda funcionalidad que posee dicha capa es almacenar las identidades certificadas en la FUAI, producto del proceso de normalización.

Para el diseño de la capa de persistencia se escogió el Patrón "Objeto de Acceso a Datos"[14] (DAO) el cual suministra una interfaz común entre la aplicación y el dispositivo de almacenamiento de los datos de los usuarios [15, p. 32]. La mayor ventaja de la utilización de este patrón es que cualquier elemento de la capa de negocio puede ser manejado sin requerir conocer el origen o destino de la información que provee o almacena respectivamente. Esta característica permite aislar la capa de persistencia subyacente en la aplicación, la cual puede ser actualizada sin afectar otros módulos del middleware.

[14] DAO: Patrón de Diseño de Arquitectura que aísla la lógica del negocio con el sistema de persistencia que sustenta la aplicación.

4.6.1.6 Implementación de la Capa de Persistencia

Primeramente en este punto, se indican las características de los repositorios donde se extraerán los registros de usuarios:

- ✓ Son bases de datos legadas donde la dirección de red no posee control.
- ✓ Los registros de usuarios se encuentran desnormalizados y orientados a responder distintas necesidades de negocio.
- ✓ Sufren indisponibilidad de sus servicios, debido principalmente a tareas programadas y migraciones las cuales no son notificadas.

Por estas razones se ha optado por implementar la capa de persistencia del middleware NDU mediante la utilización de una herramienta especializada para estos casos llamada MyBatis [18]. Este framework tiene la característica de mapear sentencias SQL con Objetos Java a través de archivos XML o anotaciones.

Con esto, se permite utilizar todas las funcionalidades de la base de datos, logrado modificar este mapeo cuando se produzcan las siguientes situaciones:

- ✓ Cambios en las estructuras de tablas o vistas.
- ✓ Un upgrade, cambio o migración de versión de base de datos.

En la Figura 32 se puede apreciar la integración del framework MyBatis en la capa de persistencia del middleware NDU.

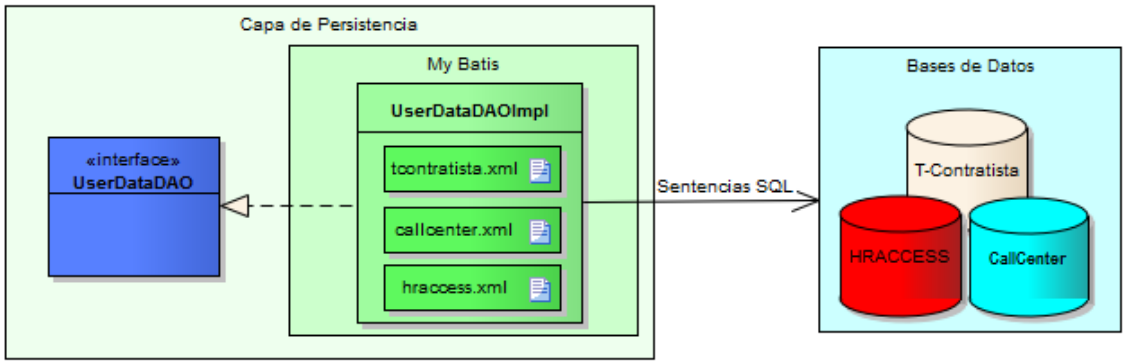


Figura 32. Framework de Persistencia del Middleware NDU

Como se indicó anteriormente, todas las instrucciones SQL de extracción de registros de usuario se encuentran en archivos XML. Estos archivos son interpretados y utilizados por la implementación de la interfaz DAO, la cual puede ser utilizada por cualquier servicio de la capa de negocio.

A continuación se muestra un ejemplo de cómo se obtiene una lista de DTO desde una petición SQL (SELECT). Para esquematizar esto, se toma la funcionalidad de Obtener los usuarios desde

la FAI HRACCESS. Así, en la Figura 33 se muestra el mapeo existente entre las columnas de la Query SQL y Objetos DTO (este caso es un UserDTO y el mapper identificado por userMap).

```
<typeAlias alias="userDTO" type="cl.tis.ndu.dto.UserDTO"/>

<resultMap id="userMap" type="userDTO">
        <result property="nombreCompleto" column="NOMBRE_COMPLETO"/>
        <result property="rut" column="MATCLE"/>
        <result property="primerNombre" column="PRIMERNOM"/>
        <result property="segundoNombre" column="SECNOM"/>
        <result property="primerApellido" column="NOMPAT"/>
        <result property="segundoApellido" column="NOMUSE"/>
        <result property="correoElectronico" column="CORREOELECTRONICO"/>
        <result property="fechaIngreso" column="DATENT"/>
        <result property="areaServicio" column="CODNEG"/>
        <result property="numeroIndice" column="IDSIRI"/>
        <result property="telefonoMovil" column="TELMOVIL"/>
        <result property="rutJefeDirecto" column="JEFEDI"/>
        <result property="cargo" column="CLASSI"/>
        <result property="comuna" column="COMUNA"/>
        <result property="lugarTrabajo" column="LUTRAB"/>
</resultMap>
```

Figura 33. Mapper MyBatis

En la Figura 34, por otro lado, se especificación de la Sentencia SELECT SQL desde donde se proveerán estos datos los cuales los referenciados como respuesta a través del mapper de la Figura 33.

```
<select id="SelectListUsuariosInternos"  resultMap="userMap" parameterType="hashmap">
    select
            UPPER(TRIM(NOMCOM)) as NOMBRE_COMPLETO,
            UPPER(TRIM(MATCLE)) AS MATCLE,
            UPPER(TRIM(NOMBRE)) AS PRIMERNOM,
            UPPER(TRIM(NOMBRE)) AS SECNOM,
            UPPER(TRIM(PATERNO)) AS NOMPAT,
            UPPER(TRIM(MATERNO)) AS NOMUSE,
            UPPER(TRIM(EML)) AS CORREOELECTRONICO,
            UPPER(TRIM(UORG)) AS CODNEG,
            TRIM(NUDOSS) AS IDSIRI,
            TRIM(CEL) AS TELMOVIL,
            TRIM(RUTJEF) AS JEFEDI,
            UPPER(TRIM(HAY_NOMGEN)) AS CLASSI,
            UPPER(TRIM(ZONA)) AS COMUNA,
            UPPER(TRIM(LUTRAB)) AS LUTRAB
    from    (select rownum as fila, b.*  from T_PERSONAS b )
    where   fila >= #{pagInicial} and  #{pagfinal} >= fila order by MATCLE
</select>
```

Figura 34. Sentencia SELECT MyBatis

Las ventajas de utilizar MyBatis con bases de datos existentes son las siguientes:

- ✓ Aislamiento de las sentencias SQL con las implementaciones Java para construir los artefactos DAO. Esto quiere decir que se pueden ocupar un archivo XML para Oracle o SQLServer sin cambiar las clases Java.
- ✓ Disminución del tiempo de desarrollo, gracias a que se reduce la cantidad líneas de código que debe generar el desarrollador. Este mecanismo permite a los programadores abstraerse de generar rutinas redundantes en la aplicación.
- ✓ Al trabajar con archivos XML que contienen sentencias SQL, se pueden aprovechar las particularidades que ofrece cada fabricante de bases de datos.

4.6.2 Aspectos Transversales del Middleware NDU

Una preocupación transversal se puede definir como cualquier funcionalidad que afecta a varios puntos de una aplicación. La utilización de esta tecnología para este proyecto nace por la necesidad de mejorar las antiguas técnicas de reutilización de una funcionalidad común en varias partes de una aplicación mediante una herencia de objetos precaria en donde se utiliza una misma clase básica para todo el sistema.

En relación a esto, la Programación Orientada a Aspectos (AOP)[15] ofrece la alternativa de modularizar las preocupaciones transversales a través de entidades especiales denominadas "aspectos".

Así, la utilización de AOP entrega dos ventajas.

1. La lógica de cada preocupación se encuentra en una única ubicación, en lugar de encontrarse repartida por todo el código de la aplicación.
2. Los módulos de servicios son más claros ya que sólo contienen el código de la funcionalidad principal, mientras que las preocupaciones secundarias se han aislado en los aspectos.

En el middleware de integración NDU, existen aspectos de interés transversales que fueron abordados mediante esta tecnología, las que se verán a continuación.

4.6.2.1 Monitoreo del Proceso de Normalización

Este es aspecto importante, debido a que con esta funcionalidad se proveerá información estadística acerca de la duración del proceso de cada FAI, así como la cantidad de usuarios procesados y la cantidad de usuarios ingresados a la FUAI. Junto con esta información, el monitoreo entrega datos relevantes sobre la estabilidad del proceso cada vez que este se haya ejecutado. En la Figura 35 se presenta como se aplica el aspecto del proceso de normalización en diferentes FAIs.

[15] AOP: paradigma de programación que se centra en modularizar las preocupaciones transversales que tiene una aplicación en entidades llamadas aspectos.

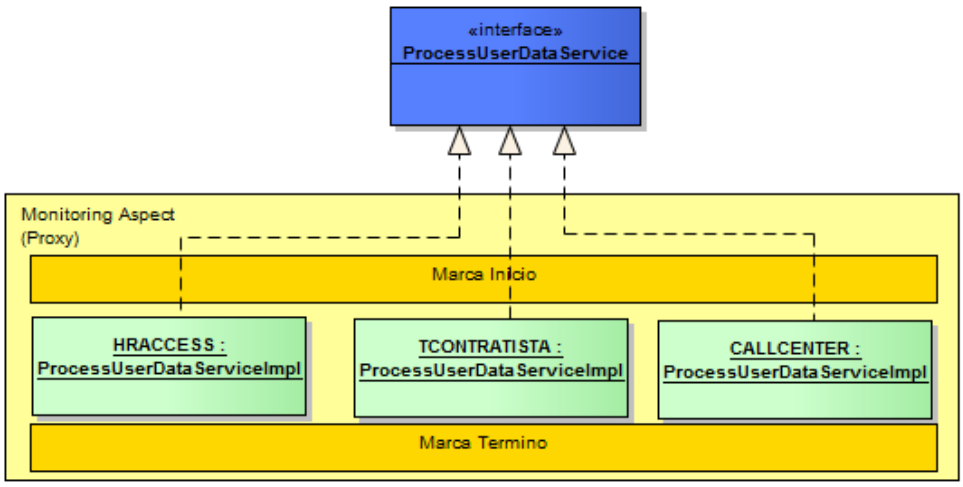


Figura 35. Aspecto de Monitoreo

Una característica de este aspecto, es que se puede habilitar o deshabilitar en tiempo de ejecución mediante la especificación de una propiedad en un archivo de configuración. El beneficio de esta forma de parametrización, radica en que un administrador de sistemas puede gestionar este aspecto sin necesariamente estar familiarizado con los conceptos de AOP ni Spring. Debido a ello, se facilitan las actividades de soporte del middleware como se aprecia en la Figura 36.

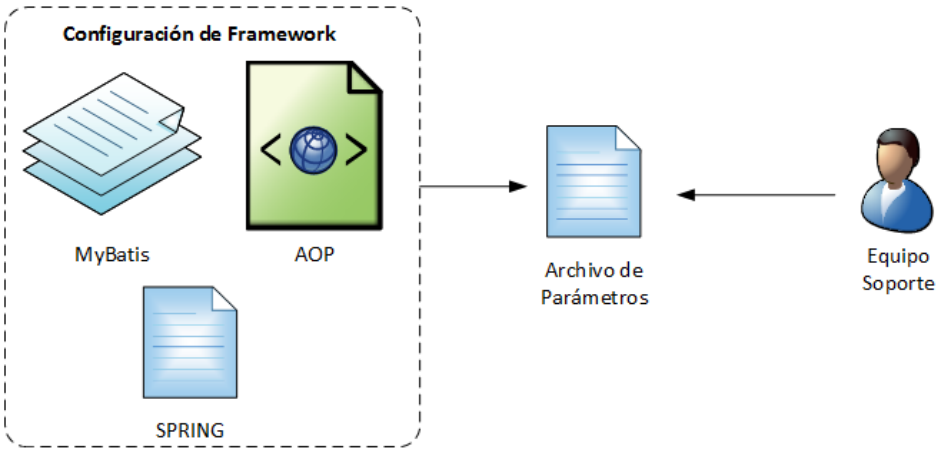


Figura 36. Habilitación del Monitoreo en el Middleware

4.6.2.2 Trazabilidad de Errores

Un segundo tema de preocupación transversal en el middleware NDU, es la trazabilidad de los errores. En este sentido, el registro y seguimiento de errores es un tema primordial cuando se genera alguna incidencia.

La ventaja de ocupar este aspecto es que se puede modificar la implementación de la tecnología de trazabilidad (LOG) de forma centralizada, incluso en período de mantenimiento, sin afectar las

tareas propias del proceso de normalización. En particular para este proyecto, se utilizó la implementación de Log4j[16] con su configuración definida mediante un archivo XML.

4.6.2.3 Rendimiento del Proceso de Normalización

Como un tema relevante en el proceso de normalización es mejorar su rendimiento. El actual diseño del proceso de normalización incluye tratamiento secuencial de las 3 FAIs consideradas. Para efectos prácticos, esto significa que no se puede normalizar más de un registro de usuario a la vez.

Sin embargo, una de las características de las FAIs es que son autónomas, lo que significa que no existe una relación entre ellas. Con esta condición, se puede mejorar este atributo de calidad mediante la aplicación del patrón de diseño orientado a aspecto llamado Worker [12, pp. 320-327], el cual paraleliza los procesos de normalización sobre cada repositorio de usuario disminuyendo el tiempo de procesamiento.

Al igual que el aspecto de monitoreo, esta característica se puede habilitar o deshabilitar de forma parametrizable mediante un archivo de propiedades. Cuando el indicador de optimización se encuentra desactivado, el proceso de normalización se ejecuta de forma secuencial tal como se grafica en la Figura 37.

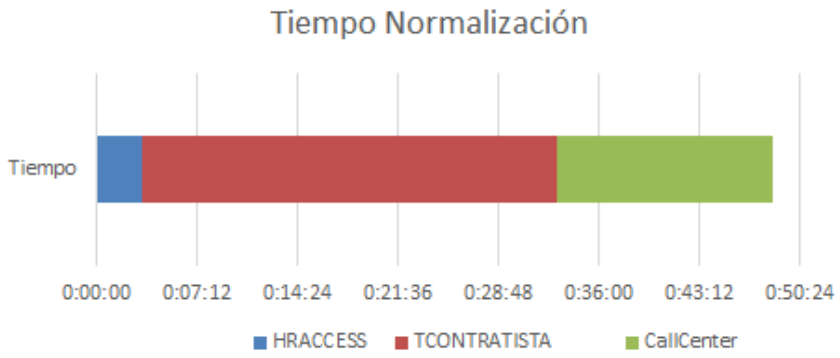


Figura 37. Gráfico de Normalización con Aspecto de Rendimiento Desactivado

En la Tabla 4, se tabularon los tiempos de normalización de cada FAI con el aspecto de rendimiento desactivado.

[16] Log4j: biblioteca opensource desarrollada en Java que permite realizar trazabilidad en niveles de criticidad en sus mensajes de salida.

Tabla 4. Tiempo de Normalización sin Aspecto de Rendimiento Activado

FAI	Inicio	Fin	Tiempo
HRACCESS	0:00:00	0:03:19	0:03:19
T-Contratista	0:03:20	0:33:03	0:29:43
CallCenter	0:33:04	0:48:30	0:15:26
		Tiempo Total	**0:48:28**

Cuando se habilita el aspecto de rendimiento, el tiempo de normalización se reduce aproximadamente en un 30%. Esto se debe a que se normalizan las FAI paralelamente tal como se grafica en la Figura 38.

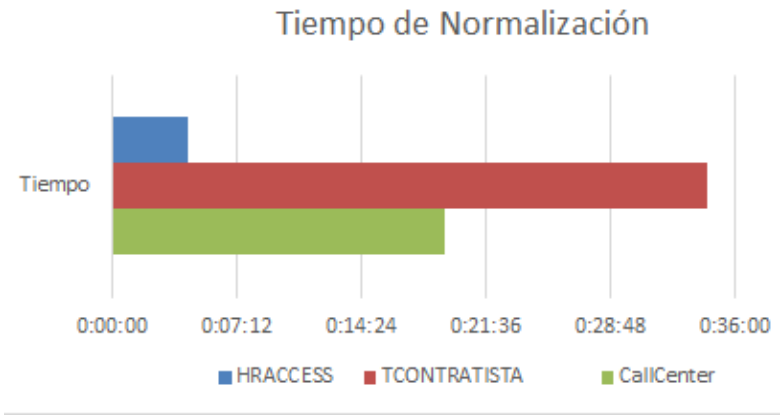


Figura 38. Gráfico de Normalización con Aspecto de Rendimiento Activado

En este caso, la duración del proceso corresponde al tiempo mayor que toma una FAI en el proceso de normalización (T-Contratista) como se tabula en la Tabla 5.

Tabla 5. Tiempo de Normalización con Aspecto de Rendimiento Activado

FAI	Inicio	Fin	Tiempo
HRACCESS	0:00:00	0:04:23	0:04:23
T-Contratista	**0:00:00**	**0:34:26**	**0:34:26**
CallCenter	0:00:00	0:19:17	0:19:17
		Tiempo Total	**0:34:26**

4.6.2.4 Colisiones de identidades

Un tema de seguridad importante para la dirección de red es la confiabilidad de la información de los usuarios que formaran parte de la FUAI. Lamentablemente no todas las FAI dentro de la compañía tienen institucionalizada esta característica, dado que en el antiguo OIM se han

reportado numerosos incidentes referido a “colisiones de identidades”. Estas situaciones generan una brecha de seguridad en la plataforma de gestión de identidad, debido a que se puede encontrar un usuario con cuentas de acceso que no le correspondan.

Para afrontar este tema, se utilizará un aspecto el cual actuará como Proxy[17] sobre el componente de verificación de actualización de identidades (punto 4.6.1.3.5), debido a que este componente determina si una identidad es actualizada o no cuando exista una coincidencia.

4.7 Principales Contribuciones del Middleware NDU

Dentro de los beneficios que entrega el middleware, se pueden indicar los siguientes:

- ✓ Consolidar y estandarizar los registros de usuario en un sólo repositorio autoritativo de identidad.
- ✓ Contar con un repositorio de registros de usuario limpio, libre de errores, con datos confiables y constantemente actualizados.
- ✓ La dirección de red al contar con un repositorio autónomo, mantiene un control y estabilidad del proceso de reconciliación.
- ✓ Se disminuyen las tareas de configuración al momento de integrar OIM, dado a que solamente debe interactuar con una sola fuente autoritativa de identidad.
- ✓ La tarea de reconciliación disminuye su tiempo de procesamiento, debido a que trabaja con datos limpios sin requerir complejas adaptaciones ni transformaciones.
- ✓ El proceso de normalización a cargo del middleware NDU, puede ser extensible a la extracción de identidades en otros tipos de repositorios de usuarios, como archivos de textos, FTP, etc.
- ✓ El middleware al estar construido por capas, se pueden actualizar cada uno de sus componentes sin afectar el resto de la arquitectura de la aplicación. Esta característica lo hace flexible y adaptable al momento de exportar esta herramienta a otras divisiones de Telefónica en Latinoamérica.
- ✓ Gracias a la programación orientada a aspectos, se puede detectar y generar reportes oportunamente sobre brechas de seguridad producidas por colisiones de identidad.
- ✓ Gracias a la programación orientada a aspectos, se puede activar y desactivar funcionalidades tales como la ejecución concurrente del proceso de normalización sobre diferentes FAIs. En este sentido, los administradores de sistema pueden escoger el modo de funcionamiento de este proceso según las prestaciones del hardware que soporta el middleware.

[17] Proxy: Patrón de diseño que proporciona un representante o intermediario de un objeto para controlar su acceso a sus funcionalidades.

5 Administración de Cuentas de Acceso

En este capítulo, se describirá el diseño y la implementación del segundo middleware de integración llamado ACU. Esta aplicación tiene como función brindar servicios de administración de cuentas de acceso en los recursos TI de la organización, de manera a que sea integrable a OIM para que esta pueda hacer uso de sus servicios.

Primeramente se describirán los artefactos con los que cuenta OIM para poder integrarse a los Recursos TI. Luego se identificaran y detallaran la importancia que tienen los recursos TI con los que se conectará la plataforma de gestión de identidad. A continuación se explicará el diseño e implementación del servicio genérico de aprovisionamiento de cuentas de usuario que ofrece este middleware. Para finalizar con el diseño e implementación del servicio de autentificación centralizado.

5.1 Conectores de la Plataforma OIM

Tal como se definió en el punto 3.3.2, la administración de acceso es el servicio de integración que tiene OIM para conectarse con los recursos TI con el objetivo de ejecutar operaciones asociadas con cuentas de acceso, esto quiere decir la creación, eliminación y actualización de cuentas de acceso. Para llevar a cabo estas actividades, la plataforma de gestión de identidad dispone componentes de software llamados conectores**,** cuya función es establecer y construir el canal de comunicación desde OIM hacia recursos TI para poder ejecutar las operaciones de administración de cuentas de usuario.

Como es comprensible, OIM solamente dispone de un conjunto acotado de conectores pre-construidos, principalmente para las marcas comerciales de recursos TI más importantes del mercado. Algunos sistemas con los que se integra OIM mediante estos conectores son los siguientes:

- ✓ Oracle.
- ✓ SAP.
- ✓ IBM.
- ✓ PeopleSoft.
- ✓ Novell.
- ✓ Microsoft entre otros.

Lamentablemente los conectores son artefactos cerrados y construidos con tecnología propietaria, por lo cual no se les puede modificar. Esto es un problema, debido a que no es posible realizar adaptaciones o mantenimiento en su funcionamiento acorde a las necesidades que tiene la compañía.

No obstante a esta situación, OIM responde a la necesidad de personalización de sus componentes mediante una API de integración basada en la tecnología Java. De esta forma, el equipo de desarrollo puede construir sus propios conectores para establecer un canal de

comunicación a los recursos TI. Si bien es cierto, este mecanismo de integración es válido y aceptado por la mayoría de las divisiones de Telefónica, tuvo los problemas descritos en el punto 1.2.2.

5.2 Recursos TI de Infraestructura de Red y su importancia en Telefónica

Se debe recordar que un recurso se puede definir como una aplicación de destino la cual tiene la facilidad de poder administrar sus cuentas de acceso [6, pp. 222-223]. En este sentido, los recursos integrados con la plataforma OIM son los equipos de la infraestructura de red de Telefónica: VPN y Accesos remoto a sistemas (router, switch, firewall, bridge).

Es importante señalar que el equipamiento de la infraestructura de red constituye la columna vertebral de los servicios entregados hacia los clientes y a los propios empleados en Telefónica Chile. En este caso, los equipos de comunicaciones y sistemas computacionales son un complemento que permiten garantizar un servicio de calidad.

Así, los objetivos de la dirección de red son los siguientes [5, p. 5]:

- ✓ Asegurar el cumplimiento de los requisitos normativos.
- ✓ Proteger los elementos más sensibles y la confidencialidad de los datos.
- ✓ Identificar los usuarios que tienen acceso y utilizan los componentes de la red.

Es por esta razón que la dirección de red dentro de su planificación contempló implementar un sistema que permita el control centralizado de los accesos lógicos dentro de la infraestructura de red de la organización. Hasta antes de la implementación de este proyecto, las credenciales de acceso en los dispositivos de red eran genéricas, conocidas por todos los usuarios que operan dispositivos de red e incluso se encuentran publicadas en Internet. Claramente la falta de una política de seguridad y renovación de credenciales, ocasiona riesgos de accesos no autorizados a cualquier elemento en la infraestructura de red.

Ante esta situación, la implementación de la plataforma OIM constituyó la piedra angular para la administración de cuentas de acceso en los dispositivos de la infraestructura de red de la compañía. Así, el middleware ACU cumple un papel fundamental, debido a que con este servicio se pueden generar cuentas de accesos en los dispositivos de red de la compañía.

Referente a los requisitos normativos para la solicitud de cuenta de acceso en los recursos de red, el middleware ACU, debe preocuparse de gestionar los siguientes datos:

- ✓ Identificación del recurso.
- ✓ Tipo de aprovisionamiento (alta, baja y actualización de una cuenta de acceso).
- ✓ Usuario beneficiario del acceso.
- ✓ Usuario solicitante del acceso.
- ✓ Atributos y valores de la configuración del acceso.
- ✓ Identificación del número de operación de aprovisionamiento.
- ✓ Fecha en que se realizó la operación.

5.3 Diseño de la Arquitectura del Módulo de Provisión de Acceso

Ante los problemas de gestión de acceso mencionados en el ítem anterior, el diseño arquitectónico de la solución, se enfocó en la definición de un mecanismo centralizado de provisión de acceso para todo el equipamiento de la infraestructura de red.

Dentro del diseño de esta solución, se contempló la reutilización de la FUAI (AD), como un único mecanismo de autentificación centralizada. Sin embargo, se necesitó segmentar los tipos de usuarios que pueden hacer uso de los dispositivos de red. Para esto, se utilizaron estructuras jerárquicas de contenedores llamados "grupo de usuarios"[18], a los cuales se pueden suscribir las identidades. En otras palabras, las identidades pueden ser miembros de estos "grupos de usuario".

Para poder relacionar estos "grupos de usuarios" con los "grupos de dispositivos de red", se compró una sistema especializado de Cisco llamado "Access Control System" (ACS). Así, esta herramienta tiene como objetivo coordinar las políticas de autenticación y autorización en el uso de los elementos de la infraestructura de red por parte de los usuarios.

En la Figura 39, se puede apreciar el diseño de la arquitectura de sistema para la gestión de accesos y operación sobre los dispositivos de red.

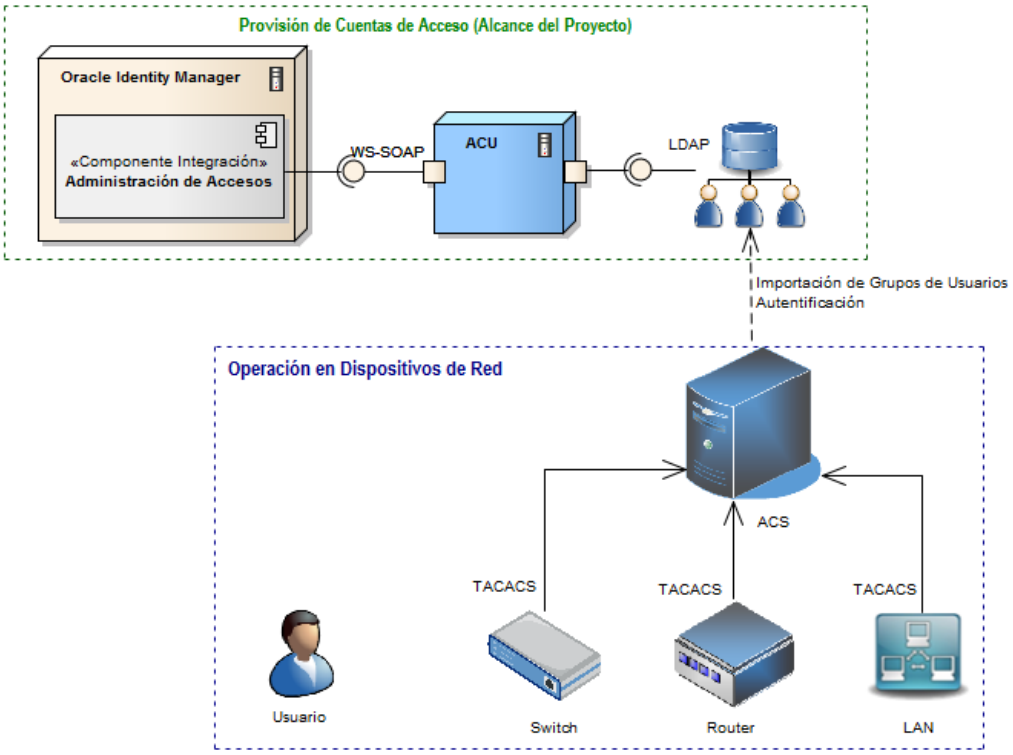


Figura 39. Arquitectura de Sistema Gestión de Acceso de Dispositivos de Red

[18] Grupo de usuario: Un grupo es un conjunto de cuentas de usuario y de equipo, contactos y otros grupos que se pueden administrar como una sola unidad. Los usuarios y los equipos que pertenecen a un grupo determinado se denominan miembros del grupo.

A continuación, se describen los componentes que forman parte de la solución para módulo de administración de cuentas de acceso.

5.3.1 Conector OIM para el Middleware de Control de Acceso

Dentro del módulo de administración de acceso, se encuentran los conectores de OIM, que son los artefactos que tiene la plataforma OIM para comunicarse correctamente con el middleware ACU. Para este proyecto, la función de los conectores se acota sólo al envío de la solicitud de acceso al sistema ACU, siendo este último el responsable de generar la cuenta de acceso en los recursos TI. Cabe señalar que el canal de comunicación entre el conector OIM y el middleware es mediante protocolo SOAP, convirtiéndose así en un cliente de aprovisionamiento dentro de una arquitectura orientada a servicios (SOA)[19].

5.3.2 ACS

El ACS es una plataforma de control de políticas de acceso y autentificación que ayuda a las empresas a cumplir las exigencias regulatorias sobre la gestión de acceso sobre los recursos de la infraestructura de red [13, p. 1].

Para la gestión de usuarios, este sistema tiene la facultad de poder incorporar en su funcionamiento fuentes autoritativas de identidad externas. Así, se pueden reutilizar las credenciales almacenadas en el AD para la autenticación de los usuarios en dispositivos de red. Esto se realiza a través de una configuración en donde el ACS se integra al AD mediante la importación de sus "grupos de usuarios".

En la Figura 40, se puede distinguir la rama del Active Directory que es utilizada por el ACS para el control de acceso en su plataforma.

Figura 40. Importación de Grupos de Usuarios desde AD

[19] SOA: Es un paradigma de arquitectura para diseñar y desarrollar sistemas distribuidos

5.3.3 Dispositivos de Red

Los dispositivos de red son un conjunto de equipamiento de comunicaciones que permiten establecer la conectividad tanto para la infraestructura interna de Telefónica como para los clientes que tengan servicios contratados. Estos dispositivos pueden ser:

- ✓ Router.
- ✓ PE (Provider Edge router) / CPE (Customer-Premises Equipment).
- ✓ VPN.
- ✓ Firewall.
- ✓ Redes WI-FI.

Todos los dispositivos son integrados y configurados en el ACS. Así, dentro de esta herramienta los equipos se pueden segmentar en "grupos de redes" como un conjunto lógico de dispositivos de red. Posteriormente los "grupos de redes" son relacionados con los "grupos de usuarios" mediante entidades propias del ACS llamadas "Políticas de Autorización y Acceso". Estas políticas de acceso determinan 3 aspectos esenciales de seguridad.

- ✓ Autentificación: Proceso en el cual ACS delega su responsabilidad en el AD.
- ✓ Autorización: El ACS verifica si el usuario puede utilizar el dispositivo de red.
- ✓ Trazabilidad: Corresponde al registro de todas las actividades de los usuarios en los dispositivos de red.

Cabe señalar que la comunicación entre el dispositivo de red y el ACS se realiza mediante el protocolo de autentificación TACACS (protocolo propietario de Cisco) especificado en RFC 1492 [14]. A continuación en la Figura 41 se muestra el diagrama de secuencia de este mecanismo.

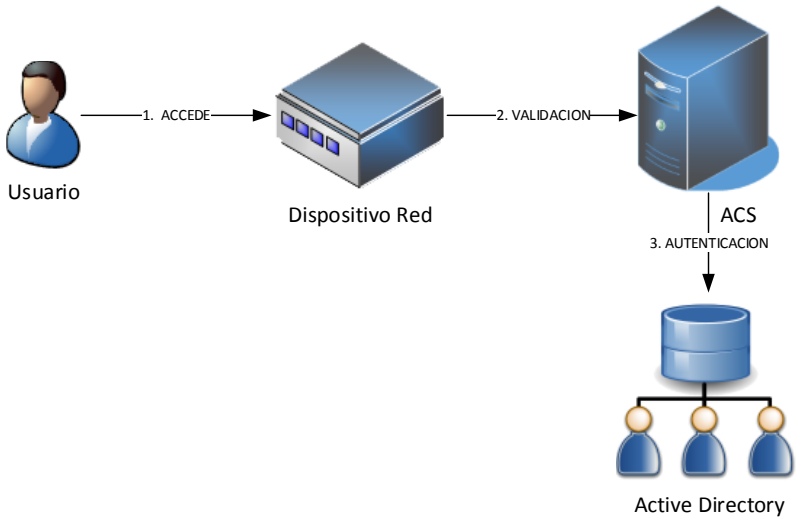


Figura 41. Secuencia de Autentificación con Protocolo TACACS

Los detalles de los pasos señalados en la figura anterior son:

1. El usuario accede a un dispositivo de red, por ejemplo: un router.
2. El dispositivo de red que se encuentra previamente configurado con una autentificación centralizada, procede a validar el acceso en el ACS mediante el protocolo TACACS.
3. Esta validación se divide en los siguientes pasos:
    a. El ACS verifica si existe alguna política de acceso que permita al usuario ingresar al dispositivo de red. Esto significa que la persona se encuentre en un "grupo de usuario" que está relacionado con el "grupo de redes" al que pertenece el dispositivo.
    b. Se realiza la autentificación mediante el AD.
    c. Posterior al ingreso del usuario, las acciones ejecutadas son supervisadas por las políticas de autorización definida para la relación "grupo de usuario" – "grupo de redes".

5.3.4 Middleware: Control de Cuentas de Acceso

La principal labor de este sistema es procesar todas las solicitudes de acceso enviadas desde la plataforma OIM. Esto con el objetivo de aprovisionar cuentas de acceso en los "grupos de usuario" que representan a un recurso en el AD. Se debe recordar que estos "grupos de usuario" están relacionados con los "grupo de redes" mediante una política en el ACS.

Para el middleware ACU, los recursos son representados por estructuras lógicas jerárquicas dentro del AD llamados "contenedores". Estos contenedores a su vez, almacenan los "grupos de usuarios", los que representan los perfiles disponibles que tiene un recurso, como se ve en la Figura 42.

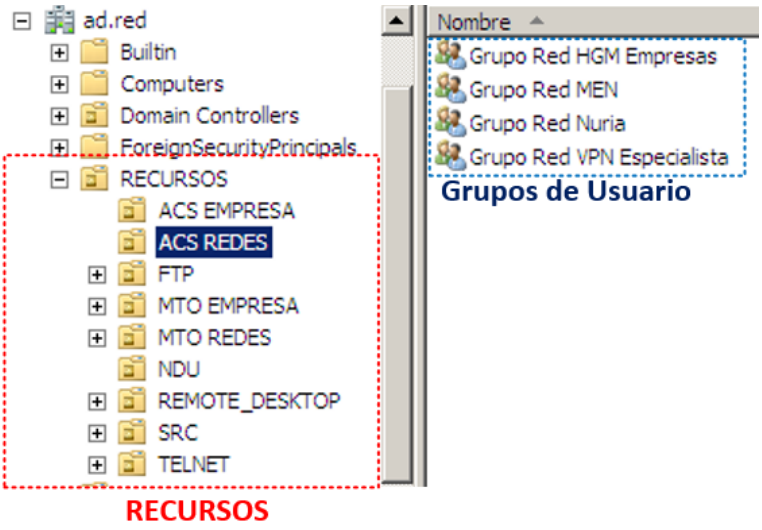


Figura 42. Representación de Recursos en AD

En la imagen anterior, los contenedores son los recursos del cuadro rojo. En el mismo, se aprecia seleccionado el recurso ACS REDES, el cual tiene los siguientes grupos de usuarios: HGM empresas, Nuria, MEN, VPN Especialistas.

En esta estructura, las operaciones de aprovisionamiento se interpretan de la siguiente manera:

- ✓ Creación de cuenta de acceso: Cuando se indica que se genera una nueva cuenta de acceso a un recurso, lo que se realiza efectivamente es que a un "grupo de usuarios" del recurso se le agrega un nuevo miembro.
- ✓ Eliminación de cuenta de acceso: Cuando se da de baja a una cuenta de usuario de un recurso lo que hace ACU es eliminarlo del "grupo de usuario".
- ✓ Actualización de cuenta de acceso: Cuando un usuario actualiza su cuenta, lo que realiza la aplicación es cambiarlo de "grupo de usuario" dentro del mismo contenedor de recurso.

A continuación en la Figura 43 se muestra un ejemplo en el cual los usuarios tienen perfil Red MEN dentro del Recurso ACS.

Figura 43. Usuarios con Cuentas de Acceso en un Recurso de Red

5.4 Proceso de Aprovisionamiento de una cuenta de acceso

El proceso de aprovisionamiento de una cuenta de acceso que realiza el Middleware ACU se puede apreciar en la Figura 44.

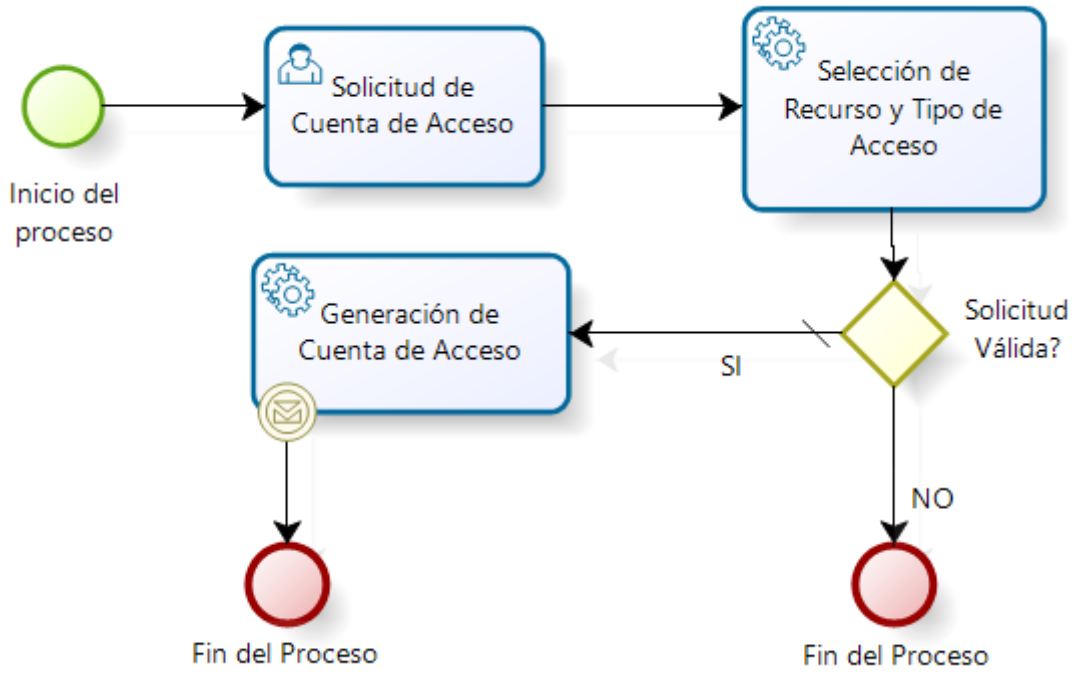


Figura 44. Proceso de Aprovisionamiento de Cuenta de Acceso

A continuación se explica los pasos del procedimiento de aprovisionamiento de cuentas de acceso:

1. El proceso comienza cuando la aplicación ACU recibe las solicitudes de provisión de cuentas de acceso desde OIM.
2. El middleware interpreta los parámetros de la solicitud, con lo cual determina el recurso (una red VPN, Acceso Remoto u otra red) y tipo de operación a ejecutar (alta, baja o actualización de cuenta de acceso).
3. Posteriormente, se valida la identificación del usuario y se interpretan los parámetros configuración de cuenta y se crea el acceso en el recurso.
4. Se entrega el estado de la solicitud procesada.

5.5 Diseño e Implementación del Middleware ACU: Servicio de Aprovisionamiento

La arquitectura de este middleware está definida por 3 capas y tiene como objetivo proveer dos servicios web para la plataforma de gestión de identidad:

- ✓ Provisión de cuentas de acceso.
- ✓ Autentificación centralizada.

Con esta definición, se responde a los requerimientos de mantenimiento e interoperabilidad solicitados al middleware. En la Figura 43, se ilustra el diseño de alto nivel de la aplicación ACU.

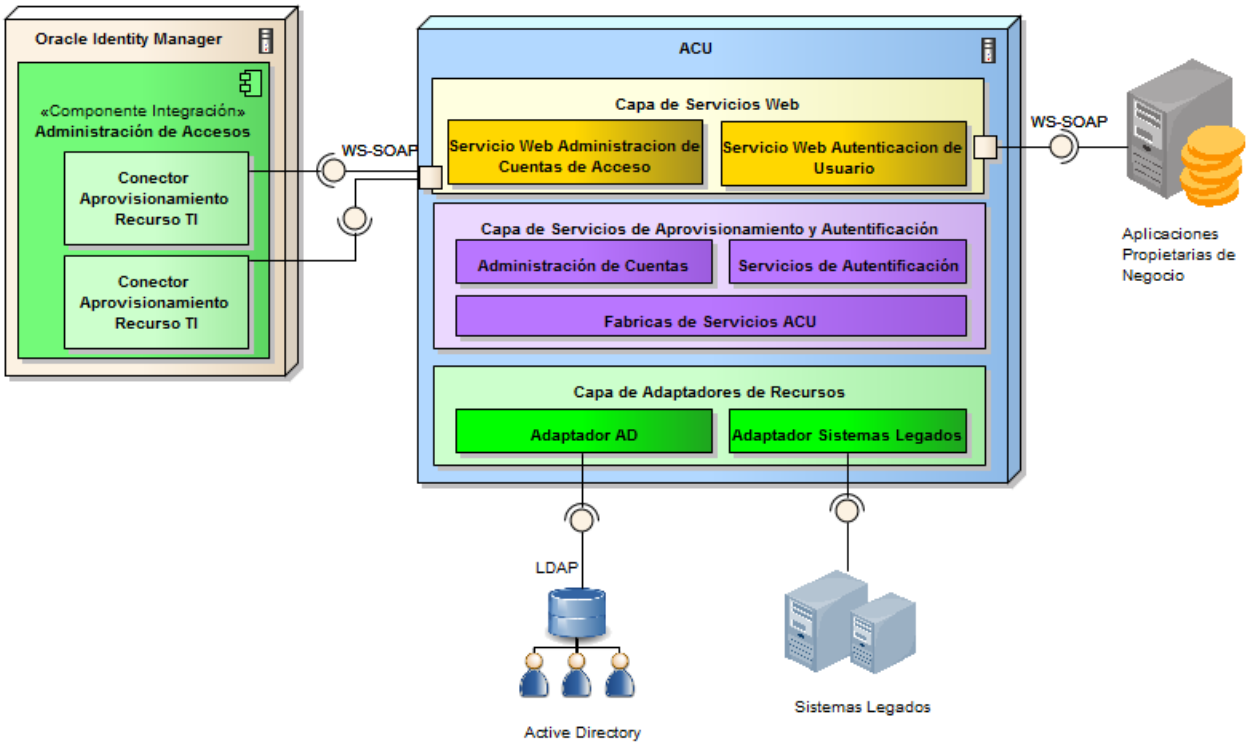


Figura 45. Arquitectura del Middleware ACU

En Figura, la comunicación entre OIM y el Middleware ACU es a través de un cliente WebService (WS). De esta forma, el conector de OIM tiene la responsabilidad de delegar la actividad de administración de cuentas de acceso al middleware ACU.

A continuación se detallan cada uno de estos componentes separados del esquema de solución.

5.5.1 Conectores de Aprovisionamiento de OIM

El diseño del conector de OIM para el aprovisionamiento de cuentas de acceso se enmarca en la definición de una arquitectura orientada a servicios (SOA). Así el conector está definido en 2 capas las que interactúan para la generación de cuentas. La plataforma OIM solo contiene el

cliente de un servicio web genérico de provisión de cuentas de usuarios disponible en el middleware ACU. La decisión de utilizar esta tecnología, responde a la necesidad de interoperabilidad y reutilización carentes en la primera versión implementada de OIM. En este sentido, la interoperabilidad permite que el servicio de aprovisionamiento pueda integrarse con otras tecnologías y plataformas. En cuanto a la reutilización, dispondrá un canal estándar y genérico para las distintas operaciones de acceso.

Para crear una cuenta, el conector debe proveer toda la información de una solicitud de acceso aprobada. La especificación de parámetros se detalla en la Tabla 6.

Tabla 6. Parámetros de Servicio Web Genérico de Aprovisionamiento

Parámetro	**Procedencia**
Identificador del usuario	Corresponde al username del beneficiario de la cuenta de acceso. Con este mismo identificador se puede acceder a la plataforma de gestión de identidad.
Recurso	Es el sistema al cual se le proveerá un acceso. Este dato es una constante dentro de cada conector para distinguir a que recurso se está otorgando la cuenta de acceso.
Tipo de Operación	Determina si la operación de aprovisionamiento corresponde a un alta, baja o actualización de una cuenta de acceso.
Identificador del Proceso	Es el número de solicitud interno de la plataforma OIM.
Identificador de la Tarea	Es el número correspondiente a la cuenta de acceso creada.
Solicitante	Es el usuario que requiere cuentas de acceso para otras personas dentro la plataforma de gestión de identidad. Este tipo de usuario también puede solicitar cuentas de acceso para él mismo.
Aprobador	Es el usuario que tiene la facultad de autorizar el uso de un recurso para otra persona.
Perfil	Corresponde al identificador del grupo de usuarios que otorga permisos de acceso a un conjunto definido de dispositivos dentro de la infraestructura de red.
Parametrización Dinámica	Concierne a las propiedades de la configuración de la cuenta. La cantidad de parámetros depende de las opciones de personalización que tenga el recurso TI.

En la Figura 46 se puede visualizar los componentes que forman parte de la estructura del conector.

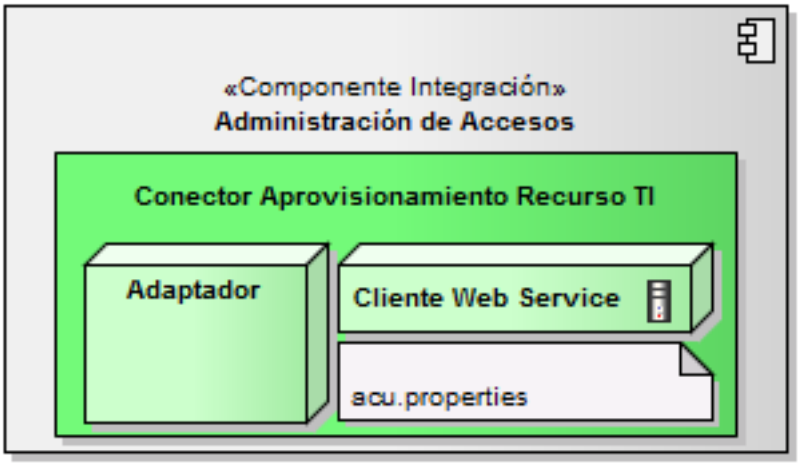


Figura 46. Componentes del Conector Genérico

- ✓ El adaptador es la entidad java que sirve de interfaz de comunicación entre los componentes propietarios de OIM y la lógica del conector.
- ✓ El cliente WebService es un componente implementado mediante la tecnología AXIS, para conectarse con el servicio de aprovisionamiento del middleware ACU.
- ✓ El archivo de parámetros contiene un conjunto de propiedades que especifican los datos de conexión al servicio web de aprovisionamiento de la aplicación ACU.

5.5.2 Capa de Servicios Web: Recepción de Solicitudes de Acceso

Para el diseño de esta capa de servicio se utilizó el Patrón JEE llamado Front Controller [15, p. 31], cuyo objetivo es centralizar el control de todos los tipos operaciones de aprovisionamiento (Alta, baja y actualización de cuenta de acceso) en una sola interfaz, la que es genérica para todos los recursos. En la versión anterior de OIM, se debía lidiar con tantas interfaces como recursos TI integrados a la plataforma de gestión de identidad.

A continuación en la Figura 47 se muestra el diagrama de clases de DTO desde el conector hacia el servicio Web, la explicación de los parámetros se puede encontrar en la Tabla 6.

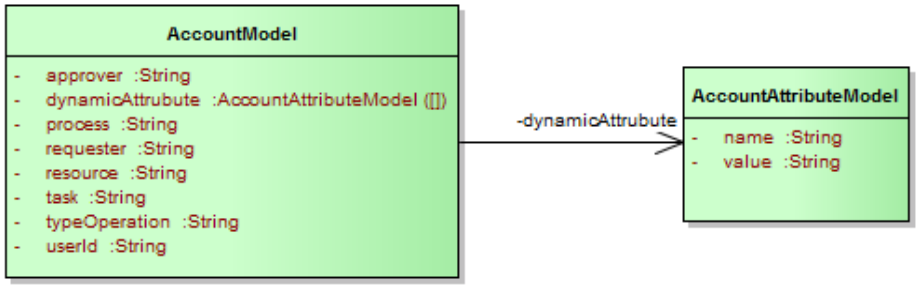


Figura 47. Diagrama de Clase del Modelo de Aprovisionamiento

En este caso, un DTO se puede entender como un objeto que transporta los datos de la solicitud desde el conector OIM hacia el Middleware ACU. Así, en el diagrama anterior, se puede distinguir una sección dinámica correspondiente a un conjunto de atributos cuya responsabilidad es configurar la cuenta de acceso (AccountAttributeModel) y una parte estática que son los datos de gestión de la cuenta de acceso (AccountModel).

A continuación en la Figura 48, se presenta el formato XML del mensaje SOAP que representa una solicitud de acceso al servicio Web de aprovisionamiento del middleware ACU.

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
                  xmlns:web="http://webservice.acu.tis.cl"
                  xmlns:mod="http://model.provisioning.acu.tis.cl">
   <soapenv:Header/>
   <soapenv:Body>
      <web:provisioningAccount>
         <web:accountModel>
            <mod:process>1</mod:process>
            <mod:task>2</mod:task>
            <mod:requester>1111111111</mod:requester>
            <mod:resource>ACS_EMP</mod:resource>
            <mod:typeOperation>ALTA</mod:typeOperation>
            <mod:userId>calvarado</mod:userId>
            <mod:approver>jmcorte</mod:approver>
            <mod:dynamicAttrubute>
               <web:item>
                  <mod:name>PROFILE</mod:name>
                  <mod:value>Grupo Red MEN</mod:value>
               </web:item>
            </mod:dynamicAttrubute>
         </web:accountModel>
      </web:provisioningAccount>
   </soapenv:Body>
</soapenv:Envelope>
```

Figura 48. Mensaje SOAP de Aprovisionamiento

Interpretando el mensaje SOAP anterior, se puede indicar que corresponde a una solicitud de alta de una cuenta para el usuario calvarado en el Recurso ACS teniendo acceso a los dispositivos de red que se encuentren en la Red MEN.

5.5.3 Capa de Negocio: Interpretación de Solicitudes de Acceso

Para el diseño de esta capa se utilizaron los patrones Factory y Double Dispatch. La razón de utilizar estos patrones es para poder interpretar parámetros de la solicitud:

- ✓ Recurso.
- ✓ Tipo de operación.

El objetivo de este diseño es ejecutar todos los tipos operaciones de forma genérica y reutilizable. En la Figura 49, se presenta el diagrama de clase de la capa de negocio del middleware ACU.

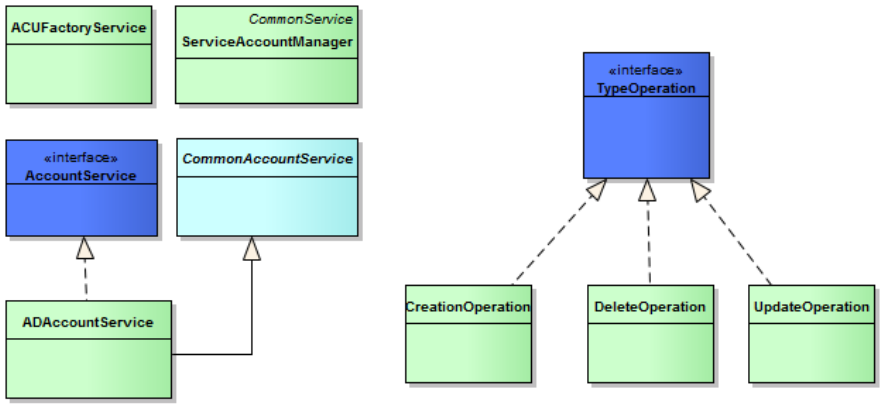


Figura 49. Diagrama de Clase Capa Negocio ACU

1. La capa de negocio es controlada por una clase llamada "Administrador de servicios de cuentas" la cual solicita un "Servicio de Cuenta" apropiado para el recurso indicado la operación. La Factory interpreta este parámetro y proporciona un servicio de cuentas (Interfaz) que provee todas las funcionalidades de administración de accesos sobre el recurso.
2. Para el caso del atributo Tipo de Operación, se utilizó de igual manera el Patrón Factory. La diferencia con los objetos de la interfaz servicio de cuenta, es que efectivamente los objetos que se instancian son del subtipo Tipo Operación, los que son utilizados para ejecutar las acciones sobre los recursos (alta, baja y actualización de cuenta de acceso). Así, la interfaz "Tipo Operación" tiene 3 implementaciones (una para cada acción). LA implementación es determinada por un parámetro de la solicitud, la cual se puede ver en la Figura 50 (Esta es una variante del Patrón de Diseño Double Dispach) [16, pp. 51-53].

```java
public class CreationOperation implements TypeOperation
{
    @Override
    public boolean execute(AccountService accountService,
                           String username,
                           Map<String, AccountAttributeModel> attributeAccountMap)
                          throws ProvisioningException
    {
        return accountService.createAccount(username, attributeAccountMap);
    }
}
```

Figura 50. Implementación de la Clase Tipo de Operacion para la Creación de Acceso

La ventaja de este diseño es que se puede generar un nuevo servicio de administración de cuentas para un recurso que se integre en el futuro. Para esto, solamente se debe construir una nueva implementación de este servicio. El resto del comportamiento está inserto en el funcionamiento de motor de control de acceso que se puede apreciar en el diagrama de secuencia de la Figura 51.

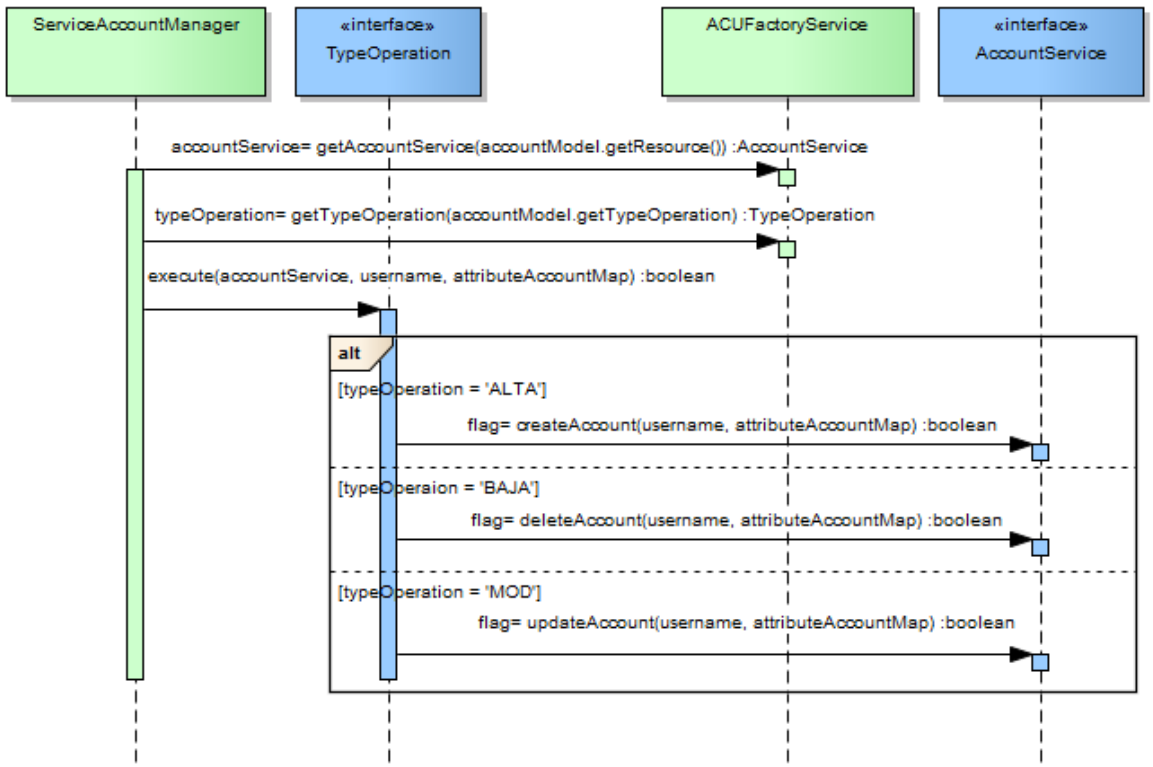


Figura 51. Diagrama de Secuencia del Proceso de Aprovisionamiento

5.5.4 Capa de Adaptadores de Recursos

Esta capa tiene la responsabilidad de comunicarse directamente con los recursos para ejecutar las operaciones de aprovisionamiento. Para diseñar e implementar esta capa, se utilizó el Patrón DAO. La ventaja de este patrón es la autonomía que posee con la capa de negocio, vale decir se puede modificar esta capa sin afectar otras partes del middleware.

Otra ventaja es que solamente se construirá un sólo DAO por tipo de recurso. Por ejemplo, si se desea instalar otro ACS, solamente se deberán cambiar los parámetros de conexión, sin afectar la lógica de aprovisionamiento del DAO.

5.6 Diseño e Implementación del Middleware ACU: Servicio de Autentificación

Esta funcionalidad nace a partir de la necesidad de disponer un mecanismo de autentificación centralizado para los usuarios de la FUAI. Aunque inicialmente fue diseñado así, se puede cambiar esta tecnología, ya que el servicio dispuesto no expone la implementación subyacente a esta funcionalidad. Por ejemplo, si alguna otra división de Telefónica en Latinoamérica desea tener este servicio con una tecnología diferente como una base de datos, solamente se debería actualizar el componente de persistencia de esta funcionalidad. Así, el servicio de autentificación sería trasparente para las aplicaciones clientes que deseen utilizarlo, puesto que no conocen la implementación que lo sustenta.

Actualmente, existen tres aplicaciones propietarias de Telefónica que han integrado este mecanismo de autentificación centralizada mediante el middleware ACU. Para utilizar esta funcionalidad, se debe especificar los siguientes datos:

- ✓ Identificador del recurso.
- ✓ Username de un usuario registrado en el AD.
- ✓ Password del usuario.

En la Figura 52, se presenta el esquema de autentificación de los sistemas con el middleware ACU.

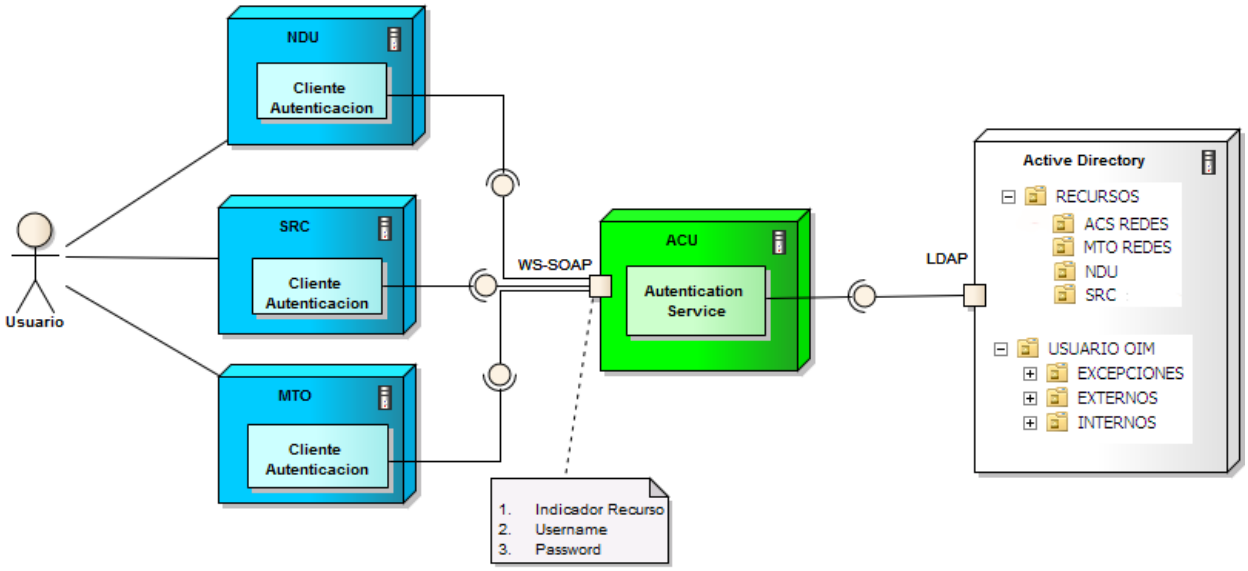


Figura 52. Esquema de Autentificación Centralizada

Por otro lado, es importante indicar que todos los recursos TI que están utilizando este mecanismo de autentificación, también se encuentran integrado a la plataforma de gestión de identidad OIM para la provisión de cuentas de acceso.

Respecto a la contraseña de la clave de acceso, estas son intransferibles según lo indicado en la Normativa de Seguridad Corporativa en la sección “Obligaciones y Responsabilidades del Personal”.

En cuanto al diseño de esta funcionalidad, se tiene una interfaz que define los parámetros requeridos para ejecutar una operación de autentificación, como se mencionó con anterioridad, hoy está definida mediante un AD, pero puede ser actualizada mediante cualquier otra tecnología. A continuación en la Figura 53 se presenta su diagrama de clases.

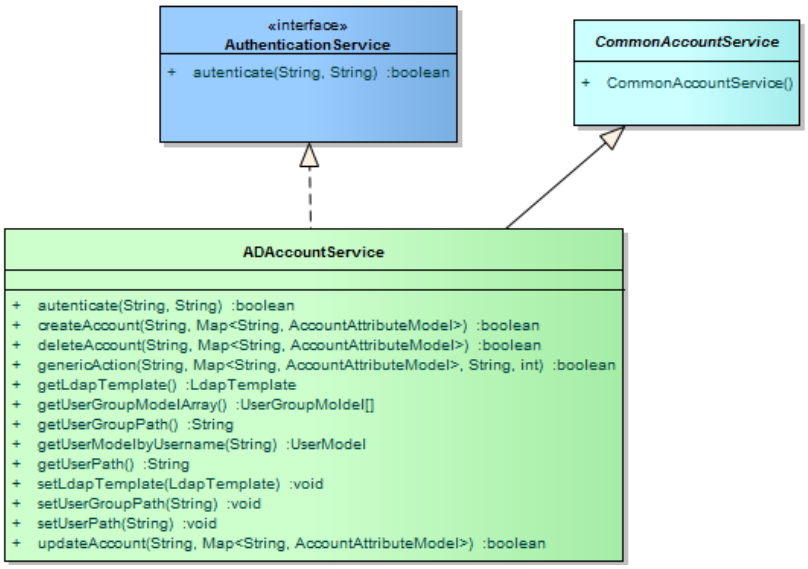


Figura 53. Diagrama de Clase del Servicio de Autentificación

Como se ilustra en la Figura 51, sólo se expone su interfaz para ser utilizada, su implementación se basa en el AD como sistema de almacenamiento. Si en un futuro se desea construir una nueva versión de este servicio, sólo se deberá crear una nueva implementación de esta interfaz.

Como se puede apreciar, la definición del método de autentificación no tiene implícito el parámetro recurso. Esto a razón de que cada recurso puede tener su propio servicio de autentificación independiente. Por este motivo, el identificador de recurso es utilizado por una Factory para instanciar el servicio de autentificación correspondiente a cada recurso, tal como se presenta en la Figura 54.

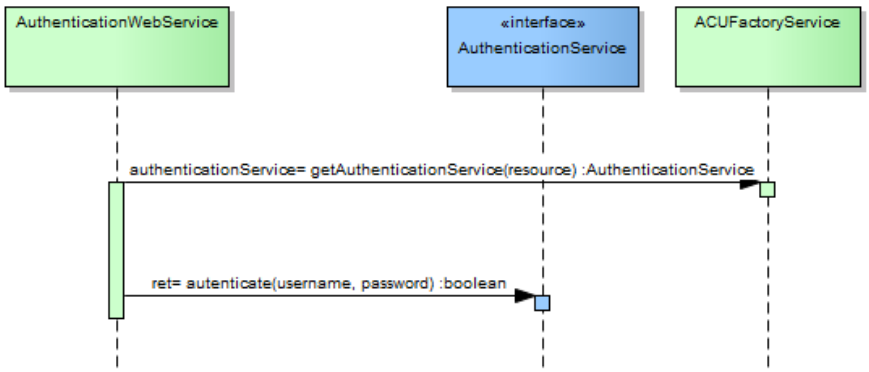


Figura 54. Invocación al Servicio de Autentificación

A continuación los pasos de autentificación para cualquier recurso que esté integrado al AD es el siguiente:

1. Verificación que el usuario se encuentre activo en el AD.
2. Comprobar si el usuario es miembro en alguno de los "grupos de usuario" definidos para el recurso.
3. Se ejecuta la operación de autentificación con el AD.

5.7 Contribuciones del Middleware ACU

Después de la implementación del middleware ACU, este trajo los siguientes beneficios a la plataforma de gestión de identidad.

- ✓ Contar con un único servicio genérico de aprovisionamiento de cuentas de usuarios para los recursos que se encuentren integrados en la plataforma de gestión de identidad.
- ✓ Al aislar o desacoplar la lógica del proceso de aprovisionamiento desde OIM, se puede actualizar el componente ACU, encargado de las operaciones de aprovisionamiento, sin afectar otros procesos, como el de reconciliación.
- ✓ Se deja registro de todas las operaciones de aprovisionamiento sobre los recursos. Así se pueden extraer estadísticas útiles para el departamento de auditoría.
- ✓ La funcionalidad de aprovisionamiento, es extensible para otros recursos que no se puedan integrar al Active Directory. En este caso las credenciales de acceso se almacenaran de forma local en el recurso TI involucrado.
- ✓ Este mecanismo de aprovisionamiento, no solamente utilizó tecnologías que se integren directamente en el Active Directory, como es el caso del ACS. También se integraron aplicaciones propietarias de la Dirección de Red.
- ✓ El mecanismo de aprovisionamiento también puede ser utilizado por otro tipo de sistema IDM que soporte el protocolo SOAP como canal de comunicación.
- ✓ Se provee un mecanismo centralizado de autentificación para los recursos TI que no se integren directamente al Active Directory mediante un servicio web.

6 Conclusiones y Resultados

La metodología iterativo-incremental utilizada permitió entregar middleware completamente funcionales, a razón de uno por cada incremento. Así, el resultado del primer incremento fue totalmente funcional y operativo en un ambiente de producción, mientras se construía el segundo middleware. En este lapso de tiempo los usuarios auditores pudieron notificar a los departamentos dueños de las FAIs las brechas de seguridad encontradas para su revisión. Respecto a la arquitectura general escogida, permitió establecer las piedras angulares para futuras integraciones en cuanto a interoperabilidad, mantenibilidad y portabilidad tanto para el NDU como para el ACU.

Un punto importante a destacar es la naturaleza de los middleware, al ser aplicaciones que se desplieguen en un servidor web, permitió al alumno abstraerse de problemas generales de una aplicación standalone (antiguos conectores de OIM), como son: concurrencia, transaccionalidad, alta disponibilidad y escalabilidad. Esto posibilitó que el desarrollo del trabajo se centrase en los aspectos esenciales de negocio presentes en cada uno de los middleware. El beneficio para equipo de desarrollo de OIM fue una disminución en costos relacionados con las tareas de soporte y administración de credenciales de acceso.

Uno de los problemas que surgieron en el trabajo de esta tesis fue la necesidad de contar con un hardware con mejores prestaciones tanto de procesamiento como de administración de RAM. Esto debido a que el hardware del antiguo OIM no soportó los requerimientos de la nueva plataforma, debiendo invertir en nuevos servidores para desplegar la nueva solución. De todas maneras el antiguo hardware se reutilizó con otras herramientas.

Respecto a contar con una Fuente Única Autoritativa de Identidad, al diseñar e implementar esta solución para la nueva plataforma de gestión de identidad a través de un Active Directory, se obtuvieron los siguientes beneficios para la Dirección de Red:

- ✓ Se cuenta con un repositorio de identidad autónomo. Esto permitió no depender de otras fuentes autoritativas controladas por otros departamentos dentro de la organización. De esta forma, se mitigo el riesgo de sufrir intermitencia en la conectividad, lo que afectaba el proceso de reconciliación.
- ✓ Al unificar todos los registros de usuario en un sólo repositorio, con identidades consistentes y homogéneas, se mejoró el rendimiento operativo de la plataforma de gestión de identidad. Vale decir, se disminuyeron los tiempos de procesamiento de la actividad de reconciliación. Esto debido a que ahora no se contemplan tareas adicionales de transformaciones ni adaptaciones de datos. Por otro lado, se redujo el trabajo de configuración, puesto que todos los usuarios contienen datos estandarizados y comunes, independiente de la fuente autoritativa que provengan.
- ✓ Gracias a la implementación del middleware NDU, actualmente se generan informes de auditoría, con lo que se da cumplimiento a las normativas vigentes del departamento de seguridad de la información. En este punto, las funciones relevantes fueron: conocer los errores de los registros de usuario que no fueron considerados en la FUAI y la detección de brechas de seguridad producto de las colisiones de identidades.

- ✓ Al utilizar el Active Directory como la FUAI, se aprovecharon las funcionalidades de autenticación presentes en esta tecnología, tales como: vigencia de credenciales, estado de los usuarios, restablecimiento y políticas de validación de contraseña.

Una de las desventajas de la implementación del NDU es que para contar con datos confiables, los registros de usuario se deben actualizar constantemente desde las FAI a la FUAI. Esto implica rutinas programadas de actualización de todos los registros de usuario independiente si han sido actualizado o no. En otras palabras, existe un bajo porcentaje de los registros de usuario sufren modificaciones y para detectarlos, se necesita obligatoriamente procesar toda FAI. La frecuencia debe ser al menos diaria, dada la posibilidad de acceso de personas que se encuentren desvinculadas de la compañía.

Respecto al uso de programación orientada a aspectos en esta solución, se pudo implementar y visualizar tareas de monitoreo sobre el proceso de normalización de forma no invasiva. Con los registros entregados por esta función se pudo conocer el estado de salud de la integración desde el aplicativo NDU hacia todas las FAIs consideradas. El beneficio de esto, fue el poder notificar y dejar en evidencia los errores en los servicios de usuario a los departamentos encargados de las FAIs.

En cuanto al ámbito de seguridad, el uso de la programación orientada a aspectos fue esencial, dado que con ella se implementó el registro de colisiones. La información de las colisiones de identidad es vital para auditores, puesto que este tipo de eventos es la principal brecha de seguridad con la que deben lidiar. Así, se garantiza que los usuarios sean obtenidos desde FAI correcta, sean creados y desvinculados en el momento apropiado.

Referente a atributos de calidad, la incorporación de esta tecnología mejoró en un 40% el rendimiento completo del proceso de normalización (Ver evidencias cuantitativas en Figuras 37 y 38, Tablas 4 y 5). En este sentido, se aplicó un aspecto para ejecutar concurrentemente el proceso de estandarización sobre las tres FAIs. Por otro lado, la configuración de esta característica es parametrizable, activándose o no en tiempo de ejecución, dependiendo de las prestaciones del hardware donde se instale el middleware NDU.

Respecto al middleware de administración de cuentas de acceso, se obtuvo un sistema que tiene características de autonomía, interoperabilidad y mantenibilidad. El middleware ACU al ser una aplicación Web implementada en capas, puede actualizarse o mejorarse sin afectar otros servicios del sistema de gestión de identidad, problema que se tenía constantemente en la versión anterior. Esto redujo las de indisponibilidad que tenía OIM con cualquier actualización en sus conectores.

En cuanto al nuevo conector genérico, al ser implementado como un Web Service sobre un protocolo estándar como lo es SOAP, mejoró la interoperabilidad del middleware. Esto significó que no solamente OIM se pueda integrar a este middleware, sino también otros tipos de sistema de gestión de identidad o incluso aplicaciones propietarias que necesiten conectarse al servicio de autentificación que ofrece este middleware.

Respecto a la autentificación centralizada al trabajar con una sola fuente autoritativa de identidad, los usuarios tienen una sola credencial de acceso para los sistemas que se integren directamente con el Active Directory. De esta forma, se simplifica la cantidad de credenciales de acceso que el usuario debe manejar en distintos sistemas, mejorando la experiencia y productividad de las

personas. Sin embargo, esta característica lo vuelve un elemento crítico para esta arquitectura, ya que si el Active Directory falla, los recursos TI integrados a la plataforma de gestión de identidad quedarían inutilizables. En este sentido, para garantizar su funcionamiento, se debió invertir en una solución en alta disponibilidad con 2 Active Directory sincronizados.

Como trabajo futuro, se presenta el desafío de extender ambos middleware a otras divisiones de Telefónica en Latinoamérica, integrando otros tipos de interfaces de comunicación. En el caso del middleware NDU, se necesitaría extender la funcionalidad extracción de los registros de usuario desde nuevos de medios de almacenamiento (archivos de textos, FTPs, sistemas legados). Luego de esto, se deberían reutilizar la mayoría de formateadores y construir sólo los necesarios de acuerdo a los requerimientos de cada división de Telefónica.

Así mismo, durante la elaboración de esta tesis, se identificaron oportunidades de incluir nuevas líneas de negocio de Telefonica a esta plataforma. Las posibles integraciones a esta plataforma son los Sistema de Validación Fraude y Facturación. Esto les permitiría la generación automática de reportes que agilicen el trabajo manual que hoy gestionan estas áreas.

Gracias a los beneficios obtenidos por el desarrollo de este proyecto, ya se ha aprobado el presupuesto y factibilidad técnica para incluir otro tipo de recurso a la plataforma de gestión de identidad, correspondiente al acceso físico mediante tarjetas de ingreso a sitios críticos que posee Telefónica (Edificios Corporativos, Salas de servidores y Monitoreo).

7 Glosario

API	*Application Programming Interface.*
ACS	*Access Control Server.*
ACU	Aprovisionamiento de Cuentas de Usuarios.
AOP	*Aspect-Oriented Programming.*
AD	*Active Directory.*
CPD	Centro de Procesamiento de Datos.
CPE	*Customer-Premises Equipment.*
DAO	*Data Access Object.*
DI	*Dependency Injection.*
DN	*Distinguished Name.*
DTO	*Data Transfer Object.*
FAI	Fuente Autoritativa de Identidad.
FUAI	Fuente Única Autoritativa de Identidad.
FTP	*File Transfer Protocol.*
IDM	*Identity Management.*
IBM	*International Business Machine.*
JEE	*Java Enterprise Edition.*
JPA	*Java Persistence API.*
JSR	*Java Specification Requests.*
LATAM	LatinoAmérica.
LDAP	*Lightweight Directory Access Protocol.*
MVC	*Model View Controller.*
NDU	Normalizador de Datos de Usuario.
OID	*Oracle Identity Directory.*
OIM	*Oracle Identity Manager.*
PE	*Provider Edge.*
RFC	*Request For Comments.*
RRHH	Recursos Humanos.
SOA	*Service-Oriented Architecture.*
SOAP	*Simple Object Access Protocol.*
SQL	*Structured Query Language.*
SSO	*Single Sign On.*
TACACS	*Terminal Access Controller Access Control System.*
VLAN	*Virtual Local Area Network.*
VPN	*Virtual Private Network.*
XHTML	*eXtensible HyperText Markup Language.*
XML	*eXtensible Markup Language.*

8 Bibliografía

[1] Oracle Corporation, (2014, August), *"Oracle Iinformation Driven Support"*. Redwood. CA. U.S. [Online]. Available: http://www.oracle.com/us/support/library/lifetime-support-middleware-069163.pdf. [Accessed: 20/04/2014].

[2] Oracle Corporation, (2008, June) *"Introducción a Oracle Identity Management"*. Redwood. CA. U.S. [Online]. Available: http://www.oracle.com/ocom/groups/public/@ocom/documents/webcontent/345082.pdf. [Accessed: 21/09/2014].

[3] Oracle Corporation, (2013, February) *"Gestion de Identidades | Oracle Identity Manager"* Redwood. CA. U.S. [Online]. Available: http://www.oracle.com/es/products/middleware/identity-management/index.html?ssSourceSiteId=null. [Accessed: 21/09/2014].

[4] J. A. Montoya S. y Z. Restrepo R., "Gestión de Identidades y Control de Acceso desde una Perspectiva Organizacional", *Ingenierías USBMed*, vol. 3, nº 1, pp. 23-34, Junio 2012 [Online]. Available: http://web.usbmed.edu.co/usbmed/fing/v3n1/v3n1a3.pdf [Accessed: 21/09/2014].

[5] Telefónica Chile,(2013, Noviembre) *"Politicas Normativas de Gestion de Identidad"* Santiago, Chile.

[6] A. Kumar, *"Oracle Identity and Access Manager 11g for Administrators"*, 1st ed, Ed, Birmingham: Packt Publishing, 2011.

[7] D. Datta. (2011, August). *"Administrator's Guide for Oracle Identity Manager 11gR2"*, Oracle Corporation. Redwood City. U.S., [Online]. Available: http://docs.oracle.com/cd/E25054_01/doc.1111/e14316.pdf [Accessed 21/09/2014].

[8] Andras Cser and Jonathan Penn, «Identity and Access Management (IAM) Market» Forrester Research, .

[9] Gartner Inc, «Magic Quadrant for User Administration and Provisioning,» Gartner, 2012.

[10] JavaServer Faces 2.0, JSR 344, 2014. [Online]. Available: https://jcp.org/en/jsr/detail?id=314. [Accessed: 21/06/2014].

[11] PrimeFaces, "Prime Faces" [Online]. Available: http://www.primefaces.org/whyprimefaces. [Accessed: 21 6 2014].

[12] R. Laddad, *"AspectJ in Action"*, Second Edition, Greenwich, CT. Manning Publications, 2010.

[13] CISCO, «Cisco Secure Access Control Server 4.2,» 2009. [Online]. Available: http://www.cisco.com/c/en/us/products/collateral/security/secure-access-control-server-

windows/data_sheet_c78-453387.pdf. [Accessed: 23 08 2014].

[14] An Access Control Protocol (TACACS), RFC1492, 1993. [Online]. Available: http://tools.ietf.org/html/rfc1492. [Accessed: 17/08/2014].

[15] D. Roldán Martinez, *"Aplicaciones Web Un Enfoque Práctico"*, Madrid. España, Ed: RA-MA, 2010.

[16] S. Stelting y O. Maassen, *"Patrones de Diseño Aplicados a Java"*, 1ra ed. Madrid. España Publisher: Pearson, 2003.

[17] DevRate, Portal de valoraciones de tecnologia s según experiencias de los desarrolladores[Online] Available: http://devrates.com/stats/index [Accessed: 12/10/2014].

[18] MyBatis, "The MyBatis Blog" [Online]. Available: http://blog.mybatis.org/ [Accessed: 12/10/2014].

[19] Ian Sommerville, "Software_Engineering" 9th Ed. U.S, Publisher: Addison-Wesley, 2010.

ANEXO A: ANTECEDENTES DE LA POLITICA DE GESTION DE IDENTIDAD

A.1 GLOSARIO:

- ✓ Credencial: En el contexto de la Gestión de Identidades la Credencial es el valor de la pareja Identificador de Usuario y su clave o contraseña.
- ✓ Gobierno Central de Identidades: Es un servicio que concentra en un punto central las solicitudes de validación de credenciales.
- ✓ Identificador de Usuario: Es un identificador único que permite diferenciar al "Usuario" del resto. El Identificador es utilizado para acceder a los sistemas y equipos de La Dirección.
- ✓ Clave o Contraseña: Es una forma de autentificación que utiliza información secreta para controlar el acceso hacia algún recurso.
- ✓ Cuenta Genérica, cuenta definida desde fabrica y de conocimiento público, con altos privilegios. En general esta cuenta permite realizar las configuraciones iniciales en los sistemas y equipos.
- ✓ Cuenta de Acceso de Usuario, "En el contexto de la informática, un usuario es aquel que utiliza un sistema informático. Para que los usuarios puedan obtener seguridad, acceso al sistema, administración de recursos, etc, dichos usuarios deberán identificarse. Para que uno pueda identificarse, el usuario necesita una cuenta (una cuenta de usuario) y un usuario, en la mayoría de los casos asociados a una contraseña."

A.2 Objetivos

El objetivo de este documento es complementar las directrices entregadas por la alta administración de la compañía, entregando deberes específicos para la gestión de identidades a los responsables de los activos de la Dirección de Red.

La política de gestión de identidad refuerza a través de estas obligaciones la preocupación e interés de La Dirección de Red en el cuidado de los activos de la Organización y que son parte esencial en la entrega de servicios hacia sus clientes.

Este documento entregará la información necesaria para la correcta administración del ciclo de vida de la Gestión de Identidades poniendo principal énfasis en la creación e identificación de los "Usuarios" que hacen uso de la "Infraestructura de Red", para conseguir este objetivo y con el fin de facilitar el entendimiento y ejecución de lo expuesto el documento se dividió de la siguiente manera:

- ✓ Alcance: Alcance de la política, obligaciones, conocimiento de las personas y sistemas sobre la cual aplica.
- ✓ Vigencia: Duración de la política y caducidad de la misma.
- ✓ Identificación de Roles y Responsabilidades: Identificación de las partes involucradas en la política además de los deberes y responsabilidades de las partes señaladas.

- ✓ Gestión de Identidades: definición de las decisiones de seguridad referidas con la Gestión de Identidades.

A.3 Alcance:

Las definiciones dentro de esta política y que son parte del documento tienen un carácter obligatorio para todos los colaboradores directos e indirectos de la Dirección de Red asimismo para todos los prestadores de servicios relacionados con ella.

Esta política aplica sobre todos los elementos de responsabilidad de la Dirección de Red donde se registren y mantengan cuentas de usuarios.

Por tal razón los elementos considerados en esta política son categorizados de acuerdo a las prestaciones entregadas por ellos; de esta manera se facilita el reconocimiento del elemento referenciado, a continuación los componentes a los cuales se hace mención, mayor detalle ver "Infraestructura de Red" punto 9.1 en el Anexo:

- ✓ Equipos de Comunicación.
- ✓ Equipos de red.
- ✓ Equipos de transporte.
- ✓ Equipos de comunicación móvil.

Tanto los "Equipos de comunicación" y los "Sistemas Computacionales" son considerados de forma general como "Infraestructura de Red" o "Recurso de Red".

Esta política no considera como parte de su aplicación lo relacionado con la gestión de identidad para el control de acceso hacia dependencias de la organización, es decir:

- ✓ Edificios.
- ✓ Oficinas centrales.
- ✓ Oficinas comerciales.
- ✓ Salas técnicas.

A.3 Normativa de Cuentas de Accesos

Como parte de los derechos y obligaciones del Administrador con el ciclo de vida de las Cuentas de Usuario, éste deberá considerar:

- ✓ Las cuentas con capacidad para modificar o borrar archivos de otros usuarios, sólo serán generadas a aquellos usuarios responsables de la Administración de los Sistemas Computacionales y/o Equipos de Comunicación o de la Seguridad de La Dirección.

- ✓ El “Administrador” deberá informar al "Solicitante" la creación de la cuenta, sin embargo la Identificación de la Cuenta y la Clave asociada a ella sólo serán informadas al “Usuario” cuando corresponda.

- ✓ Está prohibido el uso de Cuentas Genéricas para acceder a los Equipos de Comunicación y/o Sistemas Computacionales en la operación normal, esto significa que el “Administrador” no podrá entregar cuentas genéricas o anónimas para dichos accesos.

- ✓ Los datos de creación, modificación y/o eliminación de las cuentas además de sus privilegios y capacidades deben estar en un repositorio maestro que permita el acceso a ellas al Grupo de Seguridad, Responsables de los recursos y/o Administradores.

- ✓ Los valores mínimos recomendados para cada cuenta son los siguientes:
  - Identificador del usuario.
  - Nombre del usuario.
  - Vigencia.
  - Estado (habilitada, deshabilitada).
  - Fecha de creación, modificación o eliminación.
  - Privilegios.
  - Sistemas donde está presenta la cuenta.
  - Unidad de negocio donde pertenece la cuenta.
  - Cargo dentro de la organización.

- ✓ Es responsabilidad del “Administrador” mantener el inventario de las cuentas creadas en los sistemas que estén bajo su cargo considerando las recomendaciones de atributos indicados precedentemente.

A.3.1 Respecto del formato del Identificador del Usuario

El formato de las Cuentas de Usuario entregado por la organización será parte fundamental de las indicaciones de la política con la intención de establecer una conexión natural entre los sistemas corporativos y los Recursos de responsabilidad de La Dirección.

El formato del Identificador de Usuario de la cuenta en los Sistemas Computacionales y/o en Los Equipos de Comunicación para personal interno como externo debe respetar y coincidir con el formato entregado por la organización.

Excepcionalmente, si hay un “Usuario” que requiera de una cuenta y no posea una identificación corporativa, la Dirección de Red proporcionará una a través del “Administrador”, el formato recomendado para el Identificador del Usuario es:

- ✓ Usuario Interno: la primera letra del primer nombre seguido de la primera letra del segundo nombre seguido por el apellido paterno; el largo total de la cuenta no debe sobrepasar los

ocho (8) caracteres. Ejemplo: Si el Usuario se llama Felipe Gabriel Poblete Bustos, el Identificador de Usuario quedaría como: FGPOBLET

- ✓ Usuario Externo: las tres primeras letras como prefijo que identifiquen a la empresa seguido del símbolo "_" guión bajo, luego la primera letra del primer nombre seguida de la primera letra del segundo nombre seguido del apellido paterno; el largo total de la cuenta no debe superar los diez (10) caracteres. Ejemplo: Si el Usuario se llama Felipe Gabriel Poblete Bustos y es empleado de la empresa Tecnocom, el Identificador de Usuario quedaría como: TEC_FGPOBL.
- ✓ La cuenta creada excepcionalmente tendrá una duración que no superará los tres meses, luego que ésta expire deberá ser reemplazada por la cuenta proporcionada por la corporación (si existe).

La Cuenta de Usuario que no pueda cumplir con los formatos especificados debido a restricciones tecnológicas deben ser únicas y deben permitir la fácil identificación del "Usuario" inequívocamente.

A.3.2 Respecto de la creación

El Administrador crea las cuentas en los Recursos de Red con las capacidades solicitadas por el interesado para ello esta política entrega las indicaciones que permiten ejecutar apropiadamente esta actividad.

8.18. El "Administrador" creará la cuenta sí el "Usuario" cumple con las siguientes condiciones: El "Usuario" pertenece a la Dirección de Red y su rol funcional requiere de los atributos y capacidades solicitadas, para esto no será requerido el formulario de solicitud de cuentas de usuario.

Se solicitará el formulario de solicitud de cuentas y las validaciones que corresponda sí:

- ✓ El "Usuario" pertenece a la Dirección de Red y su rol funcional no coinciden con los atributos y capacidades solicitadas.
- ✓ O el "Usuario" no pertenece a la Dirección de Red.

A.3.3 Respecto de la clave o contraseña

Una contraseña o clave es una forma de autentificación que utiliza información secreta para controlar el acceso hacia algún recurso. La contraseña debe mantenerse en secreto ante aquellos a quien no se le permite el acceso.

Debido a la importancia de este instrumento en el acceso a los recursos se establece como recomendación lo indicado en la Normativa Corporativa punto "Obligaciones y Responsabilidades del Personal", además y en este ámbito:

Las claves predefinidas (por defecto) que traen los Sistemas Computacionales y/o Equipos de Comunicación, deben cambiarse inmediatamente al ponerse en servicio el Recurso de Red siempre que no exista un impedimento tecnológico que indique lo contrario (previa validación).

A.3.3 Respecto de la modificación

Los cambios de privilegios en una Cuenta de Usuario queda sometida a la misma definición de una Cuenta nueva, es decir se modifica la cuenta cuando:

- ✓ El "Usuario" pertenece a la Dirección de Red y su rol funcional requiere de los atributos y capacidades solicitadas, para esto no será requerido el formulario de solicitud de cuentas de usuario.
- ✓ Se solicitará el formulario de solicitud de cuentas y las validaciones que corresponda sí:
    - El "Usuario" pertenece a la Dirección de Red y su rol funcional no coinciden con los atributos y capacidades solicitadas.
    - O el "Usuario" no pertenece a la Dirección de Red.

A.3.4 Respecto de la eliminación

La eliminación o bloqueo de la cuenta de usuario para el acceso y uso en los Sistemas Computacionales y/o en Los Equipos de Comunicación se debe realizar cuando el colaborador deje de prestar servicios en el área responsable del recurso, se mantendrán capacidades y privilegios siempre y cuando el "Responsable" del recurso y su nuevo jefe funcional lo establezcan explícitamente formando parte de las excepciones consideradas en la creación de la cuenta.

No deben tener acceso a los Sistemas Computacionales y/o Equipos de Comunicación los "Usuarios" que han sido desvinculados o aquellos que hayan renunciado a la organización, por lo tanto las cuentas asociadas deben ser eliminadas o deshabilitadas de los sistemas donde está presente la cuenta; el cumplimiento de esta tarea se llevara a cabo a través del procedimiento establecido para dicho efecto [2.4].

A.3.5 Respecto de la trazabilidad de la cuenta

Los archivos de bitácora o de logs y los registros de auditoría que graban los eventos relevantes sobre la seguridad de los sistemas informáticos y las comunicaciones, deben ser revisados periódicamente por el Administrador y guardarse durante un tiempo por lo menos doce (12)

meses. Dicho archivos son importantes para la detección de intrusos, brechas en la seguridad, investigaciones, y otras actividades de auditoría. Por tal razón deben protegerse para que nadie los pueda alterar y que sólo los pueden leer las personas autorizadas.

En los sistemas donde se requiera agrupar a los Usuarios (mediante perfiles, grupos u otro mecanismo), esto podrá ser realizado siempre y cuando no se pierda la trazabilidad de las acciones ejecutadas por él en el sistema, si no es posible esta condición se creará un grupo por usuario.

A.3.6 Respecto de las cuentas centralizadas

La gestión de identidades centralizada es un servicio que permite concentrar en un punto todas las cuentas de usuario y eliminar la complejidad de las cuentas distribuidas; con ello se logra disminuir el impacto de la gestión de cuentas al tener todo en un único lugar. El funcionamiento normal es que el "Usuario" intente acceder luego sus credenciales son validadas por el servicio mencionado.

ANEXO B: PATRONES DE DISEÑO

Un patrón de diseño, genéricamente, describe un problema y la solución que se le da al mismo, de modo que si vuelve a suceder el mismo problema se pueda aplicar una solución similar. En el contexto de la ingeniería de software, permiten organizar los objetos según estructuras comunes y probadas, ganando en flexibilidad, reutilización y calidad del software.

Los patrones responden a problemas de diseño de aplicaciones en el marco de la programación orientada a objetos. Se trata de soluciones conocidas y probadas cuyo diseño proviene de la experiencia de los programadores. De esta forma, los patrones de diseño están basado en las buenas prácticas de la programación orientada a objetos.

A continuación se describen los patrones de diseño utilizados en este trabajo de tesis.

B.1 Proxy

Su propósito es proporcionar un representante de otro objeto, por distintas razones como pueden ser el acceso, la velocidad o la seguridad entre otras. Se utiliza cuando se necesite una referencia más elaborada a un objeto que una referencia simple.

Para permitir que el proxy represente al objeto real, el proxy tiene que implementar exactamente la misma interfaz del objeto real. Además, el objeto proxy tiene una referencia del objeto real, esto es necesario para poder llamar a los métodos del objeto real en caso de que sea necesario. De esta manera, los clientes interactúan con el proxy, pero éste puede delegar su ejecución en el objeto real. El proxy implementa la misma interfaz que el objeto real, pero puede ejecutar tareas adicionales que no puede realizar el objeto real, como son la comunicación remota o seguridad.

Se utiliza el patrón proxy en las siguientes situaciones:

1. Cuando se necesite un representante local para un objeto en otro contexto o remoto (otra máquina virtual de java)
2. Cuando se necesite un cache de objetos de costosa instanciación y de frecuente utilización.
3. Cuando se desee establecer políticas de seguridad de creación para el objeto real.

B.2 Factory

Este patrón de diseño también es conocido como “Virtual Builder”, puesto que define un método estándar y abstracto para generar objetos, delegando en las subclases su creación efectiva.

Este patrón se denomina Factory porque crea objetos cuando se necesitan. Cuando se empieza a escribir una aplicación, a menudo está claro qué tipo de componentes se utilizarán. Normalmente se tiene una idea general de las operaciones que deben tener ciertos componentes, pero la

implementación se realiza en otro momento, por lo que pueden surgir situaciones que no se tuvieron en cuenta.

Esta flexibilidad puede ser alcanzada utilizando interfaces para estos componentes. Pero el problema de programar interfaces es que no se puede crear un objeto a partir de la interfaz. Se necesita una clase que las implemente ara obtener el objeto.

Se puede utilizar este patrón en los siguientes casos:

1. Se desee crear un framework extensible. Esto significa proporcionar flexibilidad delegando las decisiones, como el tipo específico del objeto a crear para un momento posterior.
2. Cuando se sabe cuándo crear un objeto, pero no se conoce el tipo de objeto.

B.3 Fachada

Este patrón tiene como objetivo proporcionar una interfaz simplificada para un grupo de subsistemas de compleja gestión. En otras palabras, agrupa las funcionalidades de un conjunto de servicios en una interfaz unificada, siendo fácil de usar por parte de los componentes que lo invoquen.

Normalmente, el patrón fachada delegará la mayoría del trabajo en los subsistemas, aunque muchas veces también puede cumplir con alguna función. Como la de ser coordinador de flujo entre los resultados al invocar de manera ordenada a estos sistemas.

Se debe destacar que la intención del patrón fachada no es esconder los subsistemas. Su misión es proporcionar una interfaz más simple para un conjunto de subsistemas, permitiendo que los clientes más avanzados puedan utilizar las opciones más elaboradas y trabajen directamente con los subsistemas.

Se puede utilizar este patrón para:

1. Simplificar el uso de los sistemas complejos proporcionando una interfaz más sencilla sin eliminar las opciones avanzadas.
2. Reducir el acoplamiento entre los clientes y los subsistemas.
3. Introducir capas para grupos de subsistemas, lo que proporciona un alto grado de mantenibilidad del servicio que proporcionan estos subsistemas.

B.4 Singleton

El patrón singleton tiene como objetivo asegurar que una clase sólo posee una instancia y proporcionar un método de clase único que devuelva esta instancia. A la vez permite que todas clases tengan acceso sólo a esa instancia.

Este patrón se utiliza cuando.

- ✓ Se necesita un objeto global, uno que sea accesible desde cualquier parte del sistema, pero que sólo deba ser creado una vez.

- ✓ Cuando no se quiera pasar la referencia de este tipo de objeto a los otros objetos de la aplicación.
- ✓ Cuando se desee dejar de utilizar las variables globales. Dado que sobre las últimas no se tiene control de quien puede acceder a una instancia estática públicamente disponible.

B.5 Front Controller

Patrón de diseño de la capa vista que centraliza el control de las peticiones de los clientes en un sólo punto. Adicionalmente en este punto, se pueden gestionar la seguridad y control de errores. De esta manera, se reduce la cantidad de código embebido en la vista, puesto que se disminuye la lógica de control generado en las vistas.

Este patrón se utiliza cuando:

1. Se desea evitar lógica de control duplicado.
2. Agrupamiento de lógica de control común a múltiples aplicaciones.
3. Separación total de la lógica de control de las vistas.
4. Centralización del acceso a la aplicación en un único punto.

B.6 Double Dispatch

Es un patrón de diseño también conocido como Visitor, su función es proporcionar una forma fácil y sostenible de ejecutar acciones en una familia de clases. Este patrón centraliza los comportamientos y permite que sean modificados o ampliados sin cambiar las clases donde se actúa.

La forma de trabajar del patrón visitor consiste en extraer unas operaciones relacionadas de un grupo de clases y situarlas juntas en una única clase. El motivo principal es la facilidad de mantenimiento del código. En ciertas situaciones, simplemente resulta complicado mantener todas las operaciones en las propias clases. Este patrón es útil para esas situaciones, ya que proporciona un marco genérico para soportar las operaciones sobre un grupo de clases.

Este patrón se aplica cuando:

1. Un sistema contiene un grupo de clases relacionadas.
2. Se tiene que realizar algunas operaciones no triviales sobre algunas o todas las clases relacionadas.
3. Las operaciones deben ejecutarse diferente para las distintas clases.

B.7 Worker

Es un patrón de diseño cuyo propósito es mejorar la productividad y eficiencia de un proceso que implique la ejecución de tareas repetitivas secuencialmente. De esta manera, es utilizado para separar trabajos automáticos de aplicación mediante el multithreading. El modo de funcionamiento de este patrón es el siguiente: un thread worker toma una tarea de una cola y la ejecuta. Cuando finaliza, pasa a la siguiente tarea de la cola.

Con este patrón es sencillo dividir una aplicación en tareas porque solamente se especifica que hay que hacer algo, pero no se concreta cuando. De esta manera el worker ejecuta muchas tareas independientes una tras otra. En vez de crear un nuevo worker cuando hay que llevar a cabo una tarea, se le asigna la tarea a un worker existente.

Este patrón se utiliza cuando:

1. Se quiera mejorar la productividad.
2. Quiera introducir concurrencia.

B.8 Dependency Injection

La Inyección de Dependencias es un patrón de diseño orientado a objetos, en el que se suministran objetos a una clase en lugar de ser la propia clase quien cree el objeto. En una aplicación típica, suelen existir varias clases que conjuntamente realizan algunas tareas y , por lo tanto, se encuentran interrelacionadas de algún modo. En lugar de definir las relaciones en el código de la aplicación, estas dependencias suelen especificare en archivos XML de configuración para que sea el contenedor el responsable de inyectar las relaciones cuando se creen las entidades llamadas beans.

B.9 DTO

Es un patrón de diseño de la capa lógica cuyo propósito es encapsular y transportar los datos de una entidad por las capas de una aplicación. De este modo, durante el intercambio de información entre los módulos que forman parte del sistema, se evitara el paso de muchos argumentos en los métodos de los objetos. Esto tiene como ventaja que si se produce un cambio en la lista de atributos de dicho objeto, solo cambiamos la definición del DTO y no todas las referencias en los métodos donde participe. Los DTO deben ser objetos serializables para facilitar su transporte entre contextos, deben ser simples y no deben proveer información de la lógica del negocio. Esto quiere decir que su única responsabilidad es almacenar y entregar los datos contenidos en sus atributos.

B.10 DAO

Es un patrón de la capa de persistencia que separa la lógica de la aplicación del acceso a los datos, independizando de esta forma la aplicación de ña fuente de datos utilizada. Para esto, se suministra una interfaz común entre aplicación y uno o más medios de almacenamiento. Las ventajas de este patrón son las siguientes:

1. Los objetos de negocios no requieren conocimiento del destino final de la información que gestiona.
2. Centraliza el acceso a datos, escondiendo a los clientes los detalles completos de las fuentes de datos.
3. Facilita la mantenibilidad, puesto que si se produce un cambio produce un impacto mínimo en el resto de la aplicación.
4. Reduce la complejidad de la implementación del acceso a los datos en la lógica de la aplicación

B.11 MVC

El propósito de este patrón es dividir un componente o un sistema en tres partes lógicas "Modelo, Vista y Controlador", facilitando la modificación o personalización de cada parte. Este patrón responde a la necesidad de controlar la complejidad y prevenir los efectos de los cambios mediante la división de las siguientes tres partes funcionales:

- ✓ Modelo: se trata del núcleo funcional que gestiona los datos manipulados en la aplicación.
- ✓ Vista: se trata de los componentes destinados a representar la información al usuario. Cada vista está vinculada con un modelo. Un modelo puede estar vinculado a varias vistas.
- ✓ Controlador: un componente de tipo controlador recibe los eventos que provienen del usuario y los traduce en consultas para el modelo o para la vista. Cada vista está asociada a un controlador.

En este patrón la información es generada por un modelo y será el controlador el que cambiará el aspecto de la interfaz de usuario o vista en función de las reglas de negocio y la información generada por el modelo.

Este patrón se utiliza en las situaciones que se enumeran a continuación:

1. Cuando hay que crear componentes que sean flexibles y fáciles de mantener. Normalmente se utiliza para los casos en que se esperan cambios en los componentes y también se esperan que sean reutilizados.
2. Para aplicaciones flexibles e interactivas que distribuyen las funcionalidades de dicha aplicación entre los distintos objetos que la componen, de manera que el grado de acoplamiento entre estos objetos sea mínimo.