PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

FACULTAD DE INGENIERÍA

ESCUELA DE SISTEMAS

DISERTACIÓN PREVIA A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS

"ESTUDIO TEÓRICO DE SOLUCIONES A LA GESTIÓN CENTRALIZADA DE ACCESOS A LOS SISTEMAS MEDIANTE LA APLICACIÓN DE UN SISTEMA DE GESTIÓN DE IDENTIDADES"

NOMBRE: CALDERÓN BELTRÁN GALO ANDRÉS

DIRECTOR: ING. JAVIER CÓNDOR

QUITO, 2009

DEDICATORIA

A mis padres:

Con todo el afecto, la presente investigación está dedicada a mis queridos padres, que mediante su colaboración, han permitido la culminación exitosa de esta disertación de grado.

AGRADECIMIENTOS

Me gustaría expresar en estas pocas palabras, mi más sincero agradecimiento a todas aquellas personas, que a través de su gratificante colaboración, me han ayudado en la culminación de la presente disertación de grado.

En primer lugar, quisiera agradecer al director de la presente investigación, el Ing. Javier Cóndor, quien a través de sus concejos y conocimientos, me han guiado para el desarrollo exitoso de esta tesis.

Así mismo, quisiera destacar la gran colaboración recibida por parte del Ing. Hilmar Grijalva (Jefe de Seguridad de la Información – Telefónica Ecuador), Ing. Álvaro Barrera (Ingeniero Senior en Seguridad de la Información – Telefónica Ecuador), Ing. Robert Soto (Jefe de Seguridad Informática – Telefónica Ecuador), Ing. Raúl Gaybor (Ingeniero Senior en Seguridad Informática – Telefónica Ecuador), por las grandes facilidades brindadas para la obtención de información, útil para esta investigación.

Concluyo agradeciendo a mis seres queridos, por su paciencia y comprensión, durante todo el proceso de desarrollo de la presente disertación. Sin su ayuda y su interés, esta tesis difícilmente habría llegado a concluirse en los plazos y forma que hoy tiene.

INTRODUCCIÓN

En la actualidad, la mayoría de las organizaciones de nuestro país mantienen una no muy buena administración correspondiente a los accesos a sus sistemas informáticos, entendiéndose por sistemas informáticos: aplicaciones propias o ajenas al negocio, bases de datos, sistemas operativos, como también los servicios organizacionales. La falta de implementación de una solución que permita gestionar estos accesos, de una manera segura y centralizada, causa un sin número de riesgos o brechas de seguridad, que en la mayoría de los casos, son altamente perjudiciales para las organizaciones. Tal es el caso, de fraudes informáticos o robos de información sensible para la organización, debido a que personas no autorizadas, aprovechando la inexistencia de un control en las cuentas de acceso a los sistemas, acceden a los distintos recursos informáticos a través de la usurpación de identidad.

Una solución disponible en el mercado, que ayuda a contrarrestar este inconveniente, es a través de una herramienta denominada ***Sistema de Gestión de Identidades***, la cual permite administrar adecuadamente, todo el ciclo de vida de las identidades en un sólo repositorio de datos, brindando una alta seguridad en la información almacenada en éste.

Específicamente, administrar el ciclo de vida de las identidades, es tener un control centralizado en los procesos de creación, modificación, como eliminación de las cuentas de acceso a los distintos sistemas; permitiendo de esta manera, verificar como conocer con exactitud los privilegios de acceso que posee un determinado usuario.

Por este motivo, la presente investigación está enfocada al estudio y análisis de esta solución, enfatizando sus beneficios, su arquitectura, como también las funcionalidades técnicas de cada uno de los componentes que lo conforman.

ÍNDICE

1. PROBLEMÁTICA A LA GESTIÓN CENTRALIZADA DE ACCESOS A LOS SISTEMAS

1.1. Introducción

Un porcentaje considerable de organizaciones presentan un gran inconveniente en lo que se refiere a un manejo adecuado y centralizado de los accesos a los sistemas que se manejan dentro de ellas, entendiéndose por accesos, como cuentas de usuario que contienen su respectivos privilegios de acceso; por lo que se vuelve indispensable la implementación de un sistema que controle estos accesos de una forma segura y eficiente. Adicionalmente, se debe tomar en cuenta que cuando se habla de sistemas, se refiere a: aplicaciones propias o ajenas al negocio, bases de datos, sistemas operativos, como también servicios que se manejan dentro de las organizaciones, como es el caso del servicio de acceso a internet.

Con la finalidad de ampliar y entender el problema existente a la gestión centralizada de accesos a los sistemas, se presenta el siguiente cuadro:

PROBLEMAS A NIVEL DE ACCESO A LOS SISTEMAS	
ÁREA O CAMPO FUNCIONAL	**PROBLEMAS EXISTENTES**
Criticidad en los Riesgos de los Procesos	• Accesos no autorizados amenazan a la reputación, imagen y credibilidad de la empresa. • Problemas en los accesos pueden causar interrupciones puntuales y amenazas al cumplimiento de leyes y reglamentaciones (***SOX***[1]), como también posibles fraudes informáticos.

Cuadro 1 - 01 - Problemas a Nivel de Acceso a los Sistemas **[A]**

Cuadro que muestra aquellos problemas existentes en el acceso a los sistemas, tomando como referencia, la criticidad en los riesgos de los procesos implementados en una empresa.

[1] Ley Federal de Estados Unidos que permite monitorear a las empresas, para de esta manera evitar que los procesos llevados en éstas, sean alteradas de manera dudosa.

PROBLEMAS A NIVEL DE ACCESO A LOS SISTEMAS	
ÁREA O CAMPO FUNCIONAL	**PROBLEMAS EXISTENTES**
Herramientas de Soporte	• No existe un mecanismo adecuado para solicitar los accesos a los distintos sistemas empresariales. • Repositorio de personas externas desacoplado, amenazando la integridad y la exposición a riesgos laborales como jurídicos, relacionados a la tercerización de personal. • Diversas herramientas (e-mail, plantillas de Excel, etc.) y procedimientos manuales para soportar el proceso de gestión de usuarios, lo cual dificulta esta tarea.
Procesos	• Difícil manejo de la confidencialidad de accesos otorgados a los usuarios.
Gestión de Accesos	• La administración de los accesos por cada sistema, toma mucho tiempo.
Viabilidad Operacional	• Gran esfuerzo para efectuar o reforzar las políticas de seguridad, en lo referente al acceso a los sistemas.

Cuadro 2 - 01 Problemas a Nivel de Acceso a los Sistemas **[B]**

Cuadro que muestra aquellos problemas existentes en el acceso a los distintos sistemas, tomando como referencia, ciertas áreas funcionales inmersas en la gestión de este proceso.

1.2. Tipos de Usuario Informático

Para continuar con el estudio del presente tema, es necesario identificar los tipos de usuario informático que se manejan dentro de los sistemas, con la finalidad de determinar su rol e importancia.

1.2.1 Usuario de Diálogo

Es el tipo de usuario con el que deben acceder normalmente los usuarios finales que necesitan interactuar con el sistema a través del GUI o interfaz gráfica del sistema.

Todos los parámetros de autenticación definidos son verificados al iniciar sesión, como así también las restricciones de autenticación múltiple. Normalmente la mayoría de los usuarios que forman parte de una organización debieran formar parte de este tipo.

1.2.2 Usuario de Auditoría

Es un tipo de usuario de diálogo, con la diferencia que posee determinados privilegios de acceso, con el objetivo de evaluar la eficacia y la eficiencia del sistema, a fin de evitar riesgos.

1.2.3 Usuario Administrador

Este tipo de usuario puede ser creado en cualquier sistema informático, cumpliendo con operaciones de administración; es decir, cumpliendo las funciones de gestión, mantenimiento y soporte del sistema, o administrando tareas específicas cuando el usuario posee personal a su cargo.

1.2.4 Usuario de Sistema o Genérico

Los usuarios de este tipo son no interactivos, lo que significa que no pueden autenticarse a través del GUI al sistema. Comúnmente son utilizados como usuarios de procesamiento por lotes, flujos de trabajo, procesos propios del sistema, entre otros. Su contraseña solo puede ser cambiada por parte del administrador del sistema.

1.2.5 Usuarios de Comunicación

Utilizados para comunicación ***RFC***[2] entre sistemas. No es posible establecer autenticación por parte de usuarios finales a través del GUI del sistema.

1.2.6 Usuarios de Servicio

Se los usa por parte de usuarios que requieren acceso anónimo. No respetan las normas de expiración de contraseñas y la misma solo puede ser cambiada por el administrador del sistema. Las autorizaciones que se le otorguen al mismo deben ser mínimas y restringidas específicamente a la necesidad por la que se creó el usuario.

1.2.7 Usuarios de Referencia

No admiten *logon* de diálogo y pueden ser utilizados para traspasar sus autorizaciones, al usuario que lo tiene como referente.

1.3. Gestión de Accesos

Con el fin de determinar los distintos inconvenientes que presentan los administradores, en el tema de la administración de accesos a los sistemas, se presenta un estudio clasificado de la siguiente manera:

1.3.1 Administración de Servidores

En lo referente a la gestión de accesos a los servidores, se evidencian los siguientes inconvenientes para su respectiva administración:

- No existe un proceso automático que permita el aprovisionamiento de accesos a los servidores.

[2] Remote Function Call o Llamada a Función Remota es un procedimiento de intercambio de información entre un cliente y el servidor.

- La inexistencia de un sistema que permita administrar tanto la identificación como la autenticación, de todos aquellos usuarios con acceso a los servidores.

- La necesidad de detectar y corregir las inconsistencias entre los accesos que se han otorgado y los privilegios locales definidos para el acceso a los servidores; eliminando de esta manera, posibles cuentas ***huérfanas***[3] como también cuentas con privilegios adicionales que no hayan sido aprobadas en su momento.

- En concordancia con lo mencionado anteriormente, se vuelve indispensable contar con ciertas alarmas que comuniquen acerca de estos sucesos, al respectivo administrador del servidor, para de esta manera, evitar posibles ingresos no autorizados.

- Se hace necesario contar con un proceso automático que permita la identificación de las cuentas de acceso inactivas, presentes en los distintos servidores, por temas de auditoría.

- La necesidad de implementar ***workflows***[4], con la finalidad que el proceso de solicitar requerimientos de acceso a los servidores, sean gestionados por parte de los respectivos aprobadores y jefes de personal; de tal forma, que se minimice los accesos no autorizados como también los errores e inconsistencias en el respectivo proceso de aprobación de estos requerimientos.

- Por temas de auditoría, se vuelve necesario contar con un proceso que permita el registro de ***logs***[5], de toda la actividad o ciclo de vida de una determinada cuenta de usuario creada en un servidor; y a su vez, permitir la presentación de esta información, a través de reportes estándar de auditoría.

[3] Cuentas activas que no corresponden a ningún usuario.
[4] Conjunto de tareas ejecutadas de forma secuencial o en paralelo por distintos miembros, para la consecución de un mismo objetivo.
[5] Término usado para registrar datos o información sobre quién, qué, cuándo, dónde y por qué, un evento ocurre para un dispositivo en particular o aplicación.

- Adicionalmente, los administradores cuentan con un gran problema en lo referente al cifrado de las contraseñas de acceso, de los cuales hacen uso los usuarios para acceder a los respectivos servidores; por lo cual, las contraseñas deben ser codificadas o cifradas con el mayor nivel de restricción de acceso posible, de tal forma que se garantice su confidencialidad e integridad.

1.3.2 Administración de Sistemas Operativos y Bases de Datos

En la gestión de accesos para los diferentes sistemas operativos y bases de datos, se presentan los siguientes problemas para su administración:

- No existe un proceso automático que permita el aprovisionamiento de accesos, ya sea a los sistemas operativos o a las bases de datos.

- La inexistencia de un sistema que permita administrar tanto la identificación como la autenticación, de todos aquellos usuarios con acceso a los sistemas operativos o a las bases de datos.

- La necesidad de detectar y corregir las inconsistencias entre los accesos que se han otorgado y los privilegios locales definidos para el acceso a los sistemas operativos o a las bases de datos; eliminando de esta manera, posibles cuentas huérfanas como también cuentas con privilegios adicionales que no hayan sido aprobadas en su momento.

- En concordancia con lo mencionado anteriormente, se vuelve indispensable contar con ciertas alarmas que comuniquen acerca de estos sucesos, al respectivo administrador del sistema operativo o de la base de datos, para de esta manera, evitar posibles ingresos no autorizados.

- Se hace necesario contar con un proceso automático que permita la identificación de las cuentas de acceso inactivas, presentes en los distintos sistemas operativos o en las bases de datos, por temas de auditoría.

- La necesidad de implementar *workflows*, con la finalidad que el proceso de solicitar requerimientos de acceso a los sistemas operativos o a las bases de datos, sean gestionados por parte de los respectivos aprobadores y jefes de personal; de tal forma, que se minimice los accesos no autorizados como también los errores e inconsistencias en el respectivo proceso de aprobación de estos requerimientos.

- Por temas de auditoría, se vuelve necesario contar con un proceso que permita el registro de logs, de toda la actividad o ciclo de vida de una determinada cuenta de usuario creada en un sistema operativo o en una base de datos; y a su vez, permitir la presentación de esta información, a través de reportes estándar de auditoría.

- Adicionalmente, los administradores cuentan con un gran problema en lo referente al cifrado de las contraseñas de acceso, de los cuales hacen uso los usuarios para acceder a los respectivos sistemas operativos o a las bases de datos; por lo cual, las contraseñas deben ser codificadas o cifradas con el mayor nivel de restricción de acceso posible, de tal forma que se garantice su confidencialidad e integridad.

1.3.3 Administración de Servicios

Los problemas a mencionar, hacen referencia a los siguientes servicios que se manejan dentro de las organizaciones:

- Internet
- Correo Electrónico
- Acceso a la Red Corporativa
  - ✓ A nivel de Sistema Operativo
  - ✓ Conexión inalámbrica

- ✓ Otros métodos de acceso, tales como ***SSL Network Extender***[6]

Existen otros servicios, que al formar parte del dominio de "***Microsoft Active Directory***[7]", el cual es posible integrarlo a un Sistema de Gestión de Identidades, se hace posible también aplicar la teoría de la gestión centralizada de accesos a todos estos servicios; por lo cual, también se identificarán los respectivos problemas con respecto a su administración.

Algunos de los inconvenientes más frecuentes, que se presentan en la administración de accesos a los distintos servicios organizacionales, son:

- No existe un proceso automático que permita el aprovisionamiento de accesos a los servicios organizacionales.

- El problema mencionado anteriormente, es aún más grave, al aparecer nuevos servicios que beneficien el rendimiento de la empresa.

- La inexistencia de un sistema que permita administrar tanto la identificación como la autenticación, de todos aquellos usuarios con acceso a los servicios organizacionales.

- La necesidad de detectar y corregir las inconsistencias entre los accesos que se han otorgado y los privilegios locales definidos para el acceso a los servicios organizacionales; eliminando de esta manera, posibles cuentas huérfanas como también cuentas con privilegios adicionales que no hayan sido aprobadas en su momento.

[6] Es un navegador "plug-in" cliente que proporciona acceso remoto a una determinada red corporativa, para cualquier aplicación basada en IP.

[7] Herramienta desarrollada por Microsoft Corporation, que actúa como un servicio de directorio en una red distribuida de computadoras.

- En concordancia con lo mencionado anteriormente, se vuelve indispensable contar con ciertas alarmas que comuniquen acerca de estos sucesos, al respectivo administrador de los servicios organizacionales, para de esta manera, evitar posibles ingresos no autorizados.

- Se hace necesario contar con un proceso automático que permita la identificación de las cuentas de acceso inactivas, presentes en los distintos servicios organizacionales, por temas de auditoría.

- La necesidad de implementar *workflows*, con la finalidad que el proceso de solicitar requerimientos de acceso a los servicios organizacionales, sean gestionados por parte de los respectivos aprobadores y jefes de personal; de tal forma, que se minimice los accesos no autorizados como también los errores e inconsistencias en el respectivo proceso de aprobación de estos requerimientos.

- Por temas de auditoría, se vuelve necesario contar con un proceso que permita el registro de *logs*, de toda la actividad o ciclo de vida de una determinada cuenta de usuario creada en un servicio organizacional; y a su vez, permitir la presentación de esta información, a través de reportes estándar de auditoría.

- Adicionalmente, los administradores cuentan con un gran problema en lo referente al cifrado de las contraseñas de acceso, de los cuales hacen uso los usuarios para acceder a los respectivos servicios organizacionales; por lo cual, las contraseñas deben ser codificadas o cifradas con el mayor nivel de restricción de acceso posible, de tal forma que se garantice su confidencialidad e integridad.

1.3.4 Administración de Aplicaciones

Para la gestión de accesos a las diferentes aplicaciones organizacionales, ya sean desarrolladas interna o externamente, se evidencian los siguientes problemas:

- La necesidad de mejorar el proceso de monitoreo y control de los accesos a las distintas aplicaciones, a través del manejo de varios estados de acceso: activo, eliminado, revocado, bloqueado, entre otros.

- Adicionalmente, los administradores de las aplicaciones presentan un gran inconveniente al momento de la creación de ***Grupos de Usuario***[8], lo cual es realmente indispensable para el trabajo diario que cumplen los empleados dentro de una organización.

- Debido a la necesidad y a las funciones que cumplen determinados usuarios dentro de una organización, es indispensable que éstos posean varios perfiles de acceso asociados a su única cuenta de usuario creada en la aplicación, que en muchas ocasiones por indisponibilidad técnica propia de las aplicaciones, no es posible efectuarlo.

- No existe un proceso automático que permita el aprovisionamiento de accesos a las distintas aplicaciones.

- La inexistencia de un sistema que permita administrar tanto la identificación como la autenticación, de todos aquellos usuarios con acceso a las aplicaciones.

- La necesidad de detectar y corregir las inconsistencias entre los accesos que se han otorgado y los privilegios locales definidos para el acceso a las aplicaciones; eliminando de esta manera, posibles cuentas huérfanas como también cuentas con privilegios adicionales que no hayan sido aprobadas en su momento.

- En concordancia con lo mencionado anteriormente, se vuelve indispensable contar con ciertas alarmas que comuniquen acerca de estos sucesos, al respectivo administrador de la aplicación, para de esta manera, evitar posibles ingresos no autorizados.

[8] Agrupación de forma lógica de varios usuarios de un sistema, con ciertos permisos y restricciones.

- Se hace necesario contar con un proceso automático que permita la identificación de las cuentas de acceso inactivas, presentes en las distintas aplicaciones, por temas de auditoría.

- La necesidad de implementar *workflows*, con la finalidad que el proceso de solicitar requerimientos de acceso a las aplicaciones, sean gestionados por parte de los respectivos aprobadores y jefes de personal; de tal forma, que se minimice los accesos no autorizados como también los errores e inconsistencias en el respectivo proceso de aprobación de estos requerimientos.

- Por temas de auditoría, se vuelve necesario contar con un proceso que permita el registro de *logs*, de toda la actividad o ciclo de vida de una determinada cuenta de usuario creada en una aplicación; y a su vez, permitir la presentación de esta información, a través de reportes estándar de auditoría.

- Adicionalmente, los administradores cuentan con un gran problema en lo referente al cifrado de las contraseñas de acceso, de los cuales hacen uso los usuarios para acceder a los respectivas aplicaciones; por lo cual, las contraseñas deben ser codificadas o cifradas con el mayor nivel de restricción de acceso posible, de tal forma que se garantice su confidencialidad e integridad.

1.4. Gestión de Contraseñas

Una correcta administración de las contraseñas de acceso a los diferentes sistemas, es indispensable en la actualidad, donde existe un sin número de personas mal intencionadas que haciendo uso de ciertos técnicas, intentan cifrar estas contraseñas de acceso; y de esta manera acceder a los distintos sistemas, con el fin de efectuar robos de información sensible o en ciertos casos cometer fraudes informáticos, que representan grandes pérdidas económicas para las organizaciones.

1.4.1 Administración de Plataformas

Por lo mencionado anteriormente, es necesario citar los diferentes inconvenientes con los que cuentan los administradores de los sistemas, para llevar a cabo una correcta gestión de las contraseñas de acceso, las cuales son:

- La preocupación primordial para todo administrador, es la seguridad que presentan las respectivas contraseñas de acceso, esto es:

    - ✓ La generación de nuevas contraseñas de acceso, deberá ser efectuado a través de algoritmos de alta seguridad, con el fin de proporcionar una alta seguridad en el proceso de autenticación a los sistemas.

    - ✓ La ***encriptación***[9] de las contraseñas de acceso, se deberá efectuar de modo seguro, con la finalidad que ninguna persona tenga conocimiento de las mismas.

- No presentar un procedimiento que permita la definición de una adecuada política organizacional, para la gestión de contraseñas de acceso a los sistemas.

- No existe un proceso que facilite la sincronización de las contraseñas de acceso, entre "*Microsoft Active Directory*" y todos aquellos sistemas, aplicaciones o servicios, que se manejan dentro de una organización.

- La necesidad de contar con un portal Web, que permita el cambio de las contraseñas de acceso a los sistemas, el cual deberá:

    - ✓ Permitir a los propios usuarios, cambiar sus contraseñas de acceso a los distintos sistemas.

[9] Proceso para hacer ilegible información considerada importante.

- ✓ Como también, autorizar al personal de *helpdesk* para la ejecución de esta tarea, en el momento de ser requerido.

- Debido al gran número de sistemas que se manejan dentro de las organizaciones, es muy complicado para un administrador, la respectiva gestión de las contraseñas de acceso por cada uno de estos sistemas.

1.5. Gestión de Auditoría

Es realmente importante que todos los sistemas implementados en una organización, presenten una eficiente gestión de auditoría, debido a que en la actualidad a través de ingresos no autorizados a los sistemas, es muy común el robo de información sensible y confidencial para las organizaciones, que posteriormente será revelada a terceras personas.

Con la finalidad de determinar exactamente aquellos ingresos no autorizados, es necesario conocer el nombre del usuario, la fecha de ingreso y toda la actividad efectuada en el sistema; para lo cual, los sistemas deben contar con la capacidad de registrar todos los accesos y actividades efectuadas en éstos, a través de *logs* de auditoría.

Pero un sistema que presente una buena gestión de auditoría, no solamente es útil por lo mencionado anteriormente, sino que también, ayuda al momento de verificar la disponibilidad y autenticación de las cuentas de acceso a los sistemas.

Adicionalmente, es importante mencionar, que en la actualidad las organizaciones ***IT*** [10] buscan ciertas características importantes en el ámbito de la auditoría, tales como:

1.5.1 Cumplimiento

Obviamente, esta característica es el principal requerimiento dentro de una empresa.

[10] Technology Information o Tecnología de la Información, es un término enfocado al estudio, diseño, desarrollo, implementación, soporte o dirección de los sistemas de información computarizados, en particular de software de aplicación y hardware de computadoras

Hace uso de ciertas regulaciones, como SOX, que permite auditar toda aquella información relacionada a las actividades de las cuentas de acceso a los sistemas, bases de datos y servicios, que se manejan dentro de las organizaciones.

Específicamente, estas actividades se refieren a:

- Registro de quién, cómo, cuándo, dónde y por qué, de todos los diferentes accesos a los sistemas.

- Registro de los procesos de creación, modificación y eliminación de cuentas de acceso a los sistemas.

- Cambio de los respectivos perfiles de usuario o privilegios de acceso a los sistemas.

- Registro de todos los cambios de contraseña, efectuados sobre un determinado sistema.

- Eventos operacionales, tales como, el inicio o el paro del servicio de los sistemas, como también, el proceso de respaldo de información de los sistemas.

1.5.2 Monitoreo

Esta característica, además de hacer uso de *logs* de auditoría y componentes de medida, como las métricas, también maneja cuadros de indicadores, que se construyen a partir de indicadores de rendimiento, con la finalidad de alertar sobre el funcionamiento que presentan los sistemas.

1.5.3 Análisis

Adicionalmente, la información de auditoría puede ser usada para asesorar una eficiencia en la administración de los sistemas, a través de un análisis profundo de esta información.

Otra ventaja importante que ofrece un análisis de este tipo, es el estudio de posibles riesgos que se presentan en la administración de un sistema, lo cual ayuda a mantener un control sobre estos inconvenientes en un futuro.

1.6. Autenticación

También es importante mencionar el tema de la autenticación a los sistemas, debido a que una correcta gestión de accesos, debe poseer fuertes y seguros métodos con respecto a este concepto; por lo que un administrador de sistema, debe tomar en cuenta lo siguiente para lograrlo:

1.6.1 Smart Card

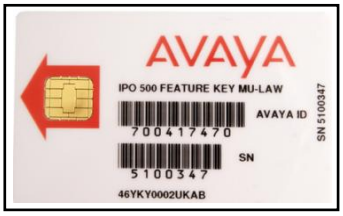

Figura 1 - 01 - Tarjeta Inteligente **[C]**

Son pequeñas tarjetas inteligentes formadas por circuitos integrados, que permiten la ejecución de cierta lógica programada, con la finalidad de brindar servicios de seguridad.

La seguridad es una de las propiedades más importantes de estas tarjetas inteligentes y se aplica a múltiples niveles, tales como:

- Autenticación a los sistemas o almacenamiento de información digital.

- Brindan una gran seguridad al momento de efectuar transacciones del negocio, reduciendo la intervención humana.

- Adicionalmente, estas tarjetas proveen una fuerte autenticación al momento de usar la tecnología ***SSO***[11], la cual se explica más adelante.

1.6.2 Token de Seguridad

Figura 2 - 01 – Token de Seguridad **[D]**

Un token de seguridad, también conocido como token de autenticación o token criptográfico, es un dispositivo electrónico que se le proporciona a un usuario autorizado, con la finalidad de facilitar el proceso de autenticación a los sistemas.

Este dispositivo muestra un código de identificación, que cambia constantemente; generalmente cada cinco minutos. Primero el usuario ingresa una clave y luego la tarjeta muestra el código de identificación, que se lo usa para el ingreso al sistema.

Existe más de una clase de token de autenticación, pero para el presente estudio, es recomendable el uso de estos tokens, generadores de códigos de identificación, que brindan una gran seguridad al momento del proceso de autenticación.

1.6.3 Sistemas Biométricos

La autenticación biométrica se refiere a la tecnología de medir y analizar las características físicas y del comportamiento humano, con el propósito de validar el acceso a los sistemas.

Algunas de estas tecnologías que se utilizan en la actualidad son: el reconocimiento de las huellas dactilares, de las retinas, del iris, de los patrones faciales o la geometría de la palma de la mano, que representan ejemplos de características

[11] Single Sign On es un procedimiento de autenticación que habilita al usuario para acceder a varios sistemas, con una sola instancia de identificación.

físicas o estáticas; mientras que ejemplos de características del comportamiento o dinámicas: la firma, el paso y el tecleo. La voz se considera una mezcla de características físicas y de comportamiento.

En un sistema biométrico, la persona se registra en éste, cuando una o más de sus características físicas y de conducta son procesadas por un algoritmo numérico, e introducida en una base de datos. Idealmente, cuando el usuario logra autenticarse, casi todas sus características concuerdan; entonces, cuando algún otro usuario intenta identificarse y sus características no coinciden completamente, el sistema no le permite el respectivo acceso.

1.6.4 Single Sign On - SSO

Es uno de los principales métodos de autenticación, que ayuda a simplificar y mejorar la seguridad, en lo referente al control de acceso a los sistemas.

A través de esta tecnología, las organizaciones pueden brindar un acceso seguro a los recursos empresariales, sin que los usuarios tengan que recordar y mantener diferentes contraseñas o credenciales de autenticación para cada sistema. Esto ayuda, a fortalecer la seguridad en el acceso a los sistemas, mejorar la experiencia del usuario, como también a reducir los costos con respecto al uso de múltiples contraseñas de acceso.

En otras palabras, los usuarios que poseen acceso a varios sistemas, ya no deben poseer diferentes credenciales de acceso para cada aplicación, sino que a través de una sola autenticación y una misma credencial de acceso, lo pueden lograr.

Es importante mencionar, que lo dicho anteriormente, es altamente recomendado por conceptos de seguridad de la información, tal cual se cita en la Norma ISO 27002, en el tema de Control de Accesos: "*Todos los usuarios deberían disponer de un único identificador propio para su uso personal y exclusivo. Se debería elegir una técnica de autenticación adecuada que verifique la identidad reclamada por un usuario*." [12] **[E]**

[12] Información extraída de la fuente: http://iso27000.wik.is/

2. MARCO TEORICO – SISTEMA DE GESTIÓN DE IDENTIDADES

Una solución, a la problemática planteada en el capítulo anterior, es sin duda, un Sistema de Gestión de Identidades o también conocida como ***IDM***[13], por las siguientes razones:

- **Administración de Usuarios**

  - Evita la participación de varios administradores para la gestión de cada uno de los sistemas utilizados en la organización.

  - Simplifica el proceso de gestionar usuarios mediante la creación y mantenimiento de perfiles de acceso.

  - Mejora de la gestión y control de accesos a los sistemas, por parte del área de Seguridad Informática, permitiendo conocer los privilegios de acceso que posee cada uno de los usuarios en los sistemas.

  - Permite el proceso de autogestión y control de las contraseñas de acceso a los diferentes sistemas informáticos; es decir, los propios usuarios pueden efectuar el cambio automático de sus contraseñas de acceso a los sistemas, sin ayuda de terceras personas.

- **Reducción de Costos**

  - Mejora la productividad del negocio.

  - Permite una integración rápida de aplicaciones, bases de datos o sistemas operativos, que se encuentran funcionales en una organización.

  - Permite el aprovisionamiento automático de las cuentas de acceso a los sistemas.

[13] Identity Management, herramienta de gestión de identidades.

- La herramienta ayuda a que los respectivos usuarios gestionen sus propias cuentas y contraseñas de acceso a los sistemas.

- **Reducción de Riesgos de Seguridad**

  - En la salida de personal o cambio de roles dentro de las organizaciones, no existe una eliminación inmediata y adecuada de los accesos a los distintos recursos empresariales, provocando de esta manera, que estos permanezcan activos y puedan ser reutilizados por usuarios o personas no autorizadas, que pueden realizar acciones ilícitas como fraudes o robos de información sensible para la organización.

  - Los usuarios se pueden identificar con total seguridad y protección al acceder a los sistemas; es decir, el sistema presenta métodos seguros de autenticación.

- **Cumplimiento de Regulaciones**

  - Evita un posible levantamiento de no conformidades en auditorías o controles realizados, de manera reincidente.

Por lo mencionado, el presente capítulo está enfocado al estudio de las distintas características y funcionalidades que ofrece esta solución.

2.1. Introducción

Es necesario definir ciertos conceptos que se emplean a lo largo del presente capítulo.

- **Identidad:** "*Es la representación de un individuo o entidad dentro de un* ***sistema IT heterogéneo.***[14]*"*

Para ampliar este concepto, se muestra la siguiente imagen, donde se observan distintas identidades:

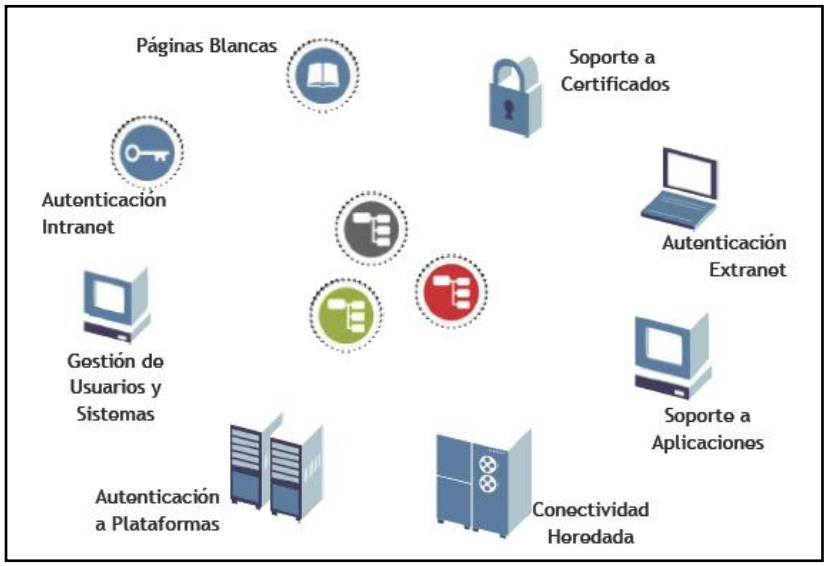

Figura 1 - 02 – Ejemplos de Identidades **[F]**

Como se puede observar en el gráfico, una identidad puede ser algo físico, como cualquier hoja en blanco, o algo digital, como las diferentes cuentas de acceso a los sistemas, esto incluye las contraseñas de acceso y los certificados digitales para el proceso de autenticación.

- **Sistema de Gestión de Identidades:** Sistema integrado de políticas, procesos organizacionales y reglas de negocio, que se encarga de la gestión de todo el ciclo

[14] Sistema compuesto por hardware con características físicas distintas entre sí, y software con características operativas distintas entre sí, pero que se pueden comunicar utilizando medios comunes.

de vida de las identidades; tal es el caso, de los accesos a los sistemas de información.

Se presenta la siguiente estructura, donde se muestra las principales funcionalidades de un sistema de gestión de identidades:

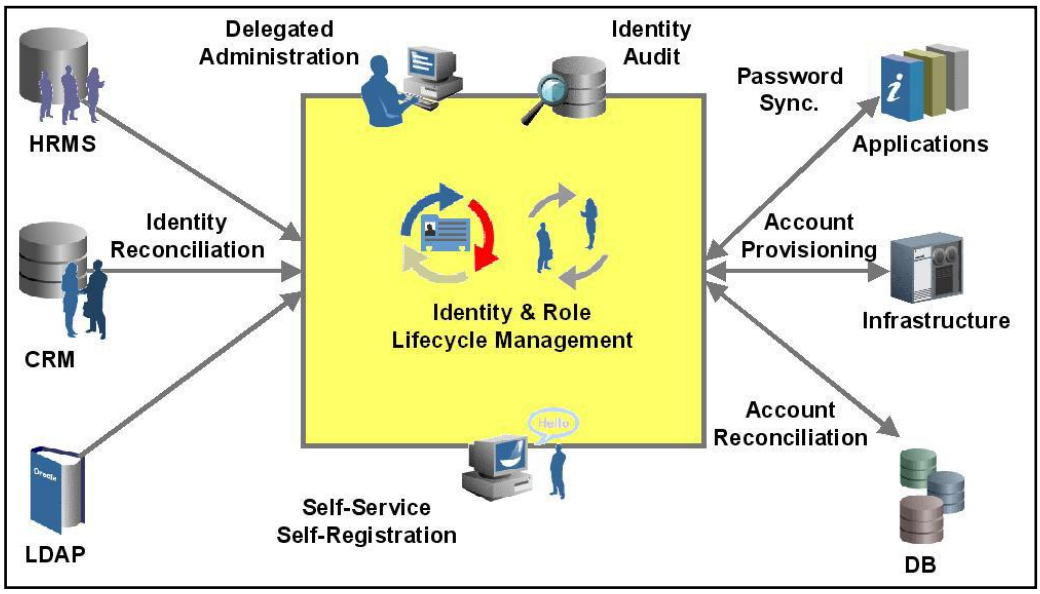

Figura 2 - 02 – Sistema de Gestión de Identidades **[G]**

Como se puede observar en la imagen, un sistema de gestión de identidades permite principalmente: el aprovisionamiento automático de las cuentas de acceso, ya sea a las aplicaciones, sistemas en general, o bases de datos; como también, el sincronizar información entre sistemas ***HRMS***[15] o ***CRMS***[16] con un repositorio central, el cual es manejado por el sistema de gestión de identidades.

Además de lo mencionado anteriormente, un sistema de gestión de identidades presenta las siguientes áreas funcionales, que encapsulan una serie de actividades, como se muestra a continuación:

[15] Human Resource Management Service o Servicio de Administración de Recurso Humano, se refiere a sistemas y procesos, en los cuales se hace presente la interacción del recurso humano con las tecnologías de la información.

[16] Customer Relationship Management o Manejo de Relaciones con Clientes, es un sistema que administra un repositorio de datos que contiene información relacionada a los clientes.

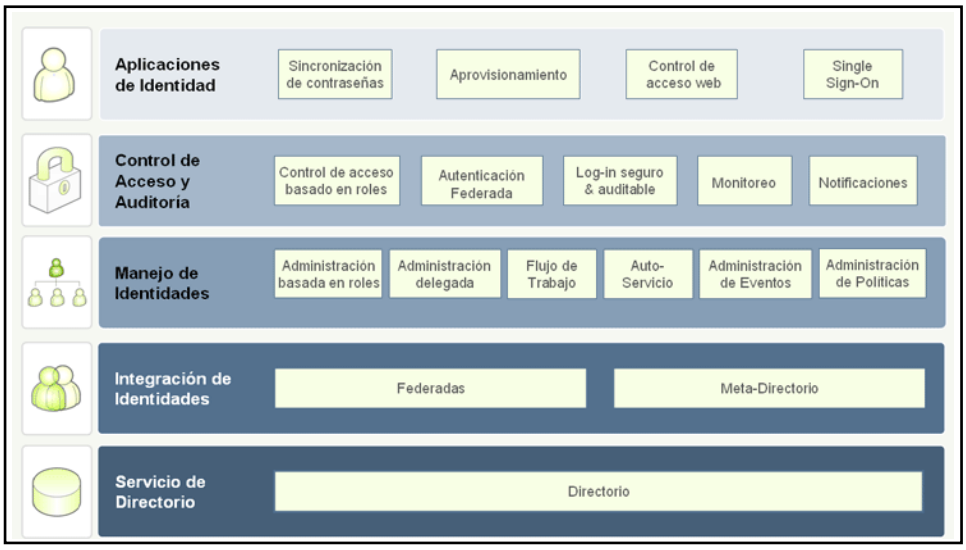

Figura 3 - 02 –Áreas Funcionales de un Sistema de Gestión de Identidades **[H]**

En otras palabras, un sistema de gestión de identidades es una solución completa, que permite facilitar y controlar todos aquellos accesos a los sistemas, de una manera centralizada y segura. Ahora, es indispensable mencionar las respectivas características y los beneficios que ofrecen cada una de estas áreas funcionales, para lo cual, se presentan las siguientes tablas:

ÁREAS FUNCIONALES DE UN SISTEMA DE GESTIÓN DE IDENTIDADES		
FUNCIONALIDAD	**CARACTERISTICAS**	**BENEFICIOS**
Aprovisionamiento Automático de Accesos	• Componente fundamental para la creación, modificación y eliminación de cuentas de acceso. • Integración con varios sistemas.	• Automatización de los procesos que efectúan los administradores de sistemas. • Reducción en los tiempos de aprovisionamiento de accesos a los empleados, socios y clientes. • Homologación de políticas de acceso a los recursos organizacionales. • Unificación de repositorios que contienen información de usuarios.

Cuadro 1 – 02 - Áreas Funcionales de un Sistema de Gestión de Identidades **[I]**

ÁREAS FUNCIONALES DE UN SISTEMA DE GESTIÓN DE IDENTIDADES		
FUNCIONALIDAD	**CARACTERISTICAS**	**BENEFICIOS**
Autenticación Reducida	• Utilizar el mismo identificador de usuario y contraseña de acceso, a los distintos recursos organizacionales.	• Facilidad para el usuario en el manejo de las credenciales de acceso, al reducir el número de identificadores de usuario y claves de acceso, que necesita para su uso laboral. • Mejora la seguridad, en lo referente al acceso a los sistemas, evitando que se compartan tanto identificadores de usuarios como claves de acceso. • Reducción de incidencias, en lo referente al olvido de las contraseñas de acceso a los sistemas.
Sincronización de Contraseñas	• Uso de una misma credencial de acceso, en todos los sistemas integrados al IDM. • Cambio automático de esta credencial de acceso, que será la misma para el ingreso a todos los sistemas integrados al IDM.	• Reducción del número de credenciales de acceso, requeridas para el ingreso a los sistemas. • Disminución del costo por incidencias, en relación al olvido de las contraseñas de acceso.
Autenticación Fuerte	• Combinación de métodos de autenticación: - Uso de identificadores de usuario y contraseñas de acceso. - Uso de certificados digitales. - Uso de *smart cards*. - Sistemas biométricos.	• Flexibilidad para combinar distintos mecanismos de autenticación, permitiendo adaptar el nivel de seguridad, en función del tipo de acceso o activo. • Permite el uso de: certificados digitales, tarjetas inteligentes, como también la incorporación de firmas digitales.

Cuadro 2 – 02 - Áreas Funcionales de un Sistema de Gestión de Identidades **[J]**

ÁREAS FUNCIONALES DE UN SISTEMA DE GESTIÓN DE IDENTIDADES		
FUNCIONALIDAD	**CARACTERISTICAS**	**BENEFICIOS**
Autoservicio y Gestión de Solicitudes de Acceso	• Uso de *workflows* de solicitudes y autorizaciones de acceso a los sistemas. • Presenta la delegación de funciones. • Recuperación automática de las contraseñas de acceso.	• Permite implantar procesos de administración distribuida, donde los respectivos responsables (Jefes, Administradores de Contrato) solicitan los accesos, a aquellos ejecutivos que lo necesiten. • Facilita la administración de usuarios, mediante la delegación de funciones. • Permite a los propios usuarios, cambiar sus contraseñas de acceso a los sistemas, sin ayuda de terceras personas.
Perfiles de Usuario	• Administración adecuada de los roles empresariales. • Ingeniería e identificación de roles empresariales.	• Simplifica la administración y la operación de los perfiles de usuario. • Permite mantener un alto nivel de seguridad, en el acceso a los recursos empresariales. • Permite identificar los privilegios de acceso que poseen cada uno de los perfiles de usuario. • La ingeniería de roles empresariales es un proceso dinámico, que permite la identificación de los derechos de acceso que posee un determinado usuario.

Cuadro 3 – 02 - Áreas Funcionales de un Sistema de Gestión de Identidades **[K]**

ÁREAS FUNCIONALES DE UN SISTEMA DE GESTIÓN DE IDENTIDADES		
FUNCIONALIDAD	**CARACTERISTICAS**	**BENEFICIOS**
Auditoría y Cumplimiento	• Registro de las autorizaciones de acceso a los recursos empresariales (quién, qué, cuándo). • Auditoría en los accesos a los distintos recursos empresariales. • Contraste de cumplimiento de normativas y políticas empresariales. • Alertas por incumplimiento a las normativas y políticas empresariales.	• Permite generar informes de auditoría, en lo referente a la asignación de recursos. • Ayuda a elaborar contrastes de cumplimiento, tomando como referencia, normativas y políticas internas. • Permite la configuración de alertas, en caso de presentarse incumplimientos a las normativas y políticas empresariales.
Control de los Usuarios Administradores	• Control de los accesos que poseen los usuarios administradores (*root*, *admin*, super-usuarios, DBA). • Auditoría en la asignación de privilegios de accesos a los recursos empresariales.	• Permite la autenticación de los usuarios administradores, a los diferentes recursos empresariales, para así evitar posibles ingresos no autorizados. • Permite la asignación temporal de privilegios, importante en casos de subcontratación de administradores de sistemas. • Registro de cualquier asignación de privilegios, por temas de auditoría.

Cuadro 4 – 02 - Áreas Funcionales de un Sistema de Gestión de Identidades **[L]**

En estos cuatro cuadros, se mencionan las principales ventajas que ofrece un sistema de gestión de identidades, por cada una de sus áreas funcionales.

Además de toda la información expuesta, es importante explicar un poco más acerca de la importancia de esta solución, para lo cual se menciona lo siguiente:

2.1.1 Aprovisionamiento y No Aprovisionamiento de Cuentas de Acceso

Disponer de un repositorio común, unificado y consolidado, es recomendable en cualquier organización que mantenga elevados volúmenes de datos, cuentas, permisos, entre otros.

Uno de los aspectos más importantes en la gestión de identidades, es la necesidad de gestionar usuarios, cuentas y políticas de acceso a los sistemas. Es importante una creación inmediata de nuevos empleados, clientes o colaboradores externos, como también, de una eficiente eliminación de las cuentas de acceso a los sistemas, de aquellos usuarios que han finalizado su relación laboral con la compañía.

2.1.2 Gestión de Contraseñas

La sincronización de las distintas contraseñas de acceso a los sistemas, evita los inconvenientes que sufren los usuarios, al acceder a los diferentes sistemas con múltiples cuentas y contraseñas.

Un sistema que permita la autogestión de las contraseñas de acceso, evita la gran cantidad de llamadas que recibe el personal de *helpdesk*, como también, el tiempo de espera del usuario afectado.

2.1.3 Gestión de Roles

Una correcta gestión de los roles empresariales, es considerado como un componente clave en los sistemas de gestión de identidades. Permite, de una forma muy efectiva, la creación y asignación de grupos con privilegios de acceso, de acuerdo al rol que desempeñan los usuarios en las organizaciones.

2.1.4 Gestión de Solicitudes, Administración Delegada y Autoservicio

Mediante una administración delegada, las organizaciones pueden repartir la carga de trabajo en la gestión del usuario a los correspondientes responsables (por departamento, aplicación, administración delegada, localización geográfica, o cualquier otro criterio). En todos los casos se debe garantizar el control de los derechos sobre los administradores delegados para visualizar, actualizar o borrar únicamente los datos sobre los que es responsable.

La implementación de *workflows*, permite establecer y automatizar un flujo de aprobaciones y acciones encadenadas, acorde a la política y modo de trabajo de la organización; como por ejemplo, la acción de solicitar accesos a los sistemas organizacionales.

2.2 Control de Acceso a los Sistemas

Un sistema de gestión de identidades está enfocado principalmente a la gestión y al control de los accesos a los diferentes sistemas organizacionales, por lo cual, es necesario mencionar algunas características que emplea esta solución, para lograr este objetivo.

2.2.1 Seguridad AAA

La seguridad AAA combina 3 funciones de seguridad, que le permite mantener el control de los accesos ya sea a los sistemas o dispositivos de red. Este tipo de seguridad significa:

- **Autenticación:** Proceso por el cual, una entidad prueba su identidad ante otra. Normalmente, la entidad es un usuario o computador.

  Este proceso se obtiene mediante la presentación de una propuesta de identidad (nombre de usuario) y la demostración de estar en posesión de las credenciales de acceso, que permiten comprobarla.

Ejemplos de estas credenciales de acceso: las contraseñas de acceso, tokens de seguridad o certificados digitales.

- **Autorización:** Se refiere a la concesión de privilegios de acceso a una entidad, basándose en su identidad, en los privilegios que solicita, y el estado actual del sistema. Las autorizaciones también pueden estar basadas en restricciones, tales como, restricciones horarias, localización de la entidad solicitante o la prohibición de realizar ingresos múltiples simultáneos del mismo usuario.

- **Auditoría:** Se refiere al seguimiento, del consumo de los distintos recursos organizacionales, utilizados por los usuarios. Esta información se almacena en algún repositorio de datos, para su entrega en algún momento posterior.

  La información que se registra, por lo general, es la identidad del usuario, el tipo de servicio que se le proporciona, cuando comenzó a usarlo, y cuando terminó.

2.2.2 Políticas de Control de Acceso a los Sistemas

La definición de políticas organizacionales de acceso a los sistemas, es imprescindible; debido a que la información que se maneja dentro de las organizaciones, corresponde al activo más importante que posee, por su criticidad e importancia; por ello, se debe plasmar procesos confiables que la proteja.

Para el presente estudio, es necesario que en una organización, se definan tanto los roles empresariales como los perfiles de usuario, acordes con las reglas del negocio. Esto se debe, a que un sistema de gestión de identidades, maneja *workflows* de autorización, lo cual permite a los ejecutivos con personal a su cargo, solicitar accesos a los distintos recursos organizacionales.

Lo mencionado, tiene como beneficio:

- Minimizar los accesos no autorizados, a información privilegiada y sensible de la organización.

- Eliminar inmediatamente los accesos a los diferentes recursos organizacionales, ante salida de personal o cambios de funciones laborales.

- Disponer de un eficiente control de acceso a los sistemas, basado en los roles empresariales o perfiles de usuario.

- Contar con información de auditoría, en lo referente a las solicitudes de acceso a los recursos organizacionales.

2.2.3 Single Sign On - SSO

Proceso de autenticación que permite a los usuarios acceder a varios sistemas informáticos, a través de una sola instancia de identificación.

Esta tecnología, es una de las principales funcionalidades que presenta un sistema de gestión de identidades.

Tal como se menciona en el capítulo anterior, este proceso de autenticación, es altamente recomendado por conceptos de seguridad de la información, tal cual se cita en la Norma ISO 27002, en el tema de Control de Accesos.

Los beneficios que ofrece esta tecnología, son:

- La gestión de las contraseñas de acceso a los sistemas, es efectiva y fácil de implementar.

- Incrementa la seguridad, en lo referente al acceso a los sistemas informáticos.

- Reduce los costos relacionados con la gestión de las contraseñas de acceso, e incrementa la productividad y la satisfacción del usuario.

- Disminuye las llamadas a *helpdesk*, por motivos de cambio de contraseñas de acceso a los sistemas.

Existen dos tipos de SSO:

- *Enterprise Single Sign On (E-SSO)*

  Esta tecnología, después de una autenticación primaria, recoge las peticiones de autenticación de otras aplicaciones secundarias, y rellena automáticamente los campos de *login*, haciendo uso de la credencial de acceso primaria.

  E-SSO permite interactuar únicamente, con sistemas que pueden deshabilitar la presentación de la pantalla de *login*.

- *Web Single Sign On (WEB-SSO)*

  Este procedimiento de autenticación, trabaja únicamente con aplicaciones y recursos accedidos vía web. Los accesos son interceptados con la ayuda de un ***servidor proxy web***[17] o de un componente instalado en el servidor web destino.

2.3 Arquitectura de un Sistema de Gestión de Identidades

La arquitectura que presenta un sistema de gestión de identidades, no tiene un determinado estándar, debido a que ésta, depende de cada una de las empresas que desarrollan este tipo de software.

[17] Un servidor proxy web, intercepta la navegación de los clientes por páginas web, por temas de seguridad o rendimiento.

Con el fin de identificar los diferentes niveles de arquitectura que presenta un sistema de gestión de identidades, se muestran ciertos diagramas, empleados por tres fabricantes de este tipo de software:

2.3.1 Certant – Technology Solutions

La empresa argentina "*CERTANT – TECHNOLGY SOLUTIONS*", dedicada a la implementación de soluciones empresariales, presenta su propio sistema de gestión de identidades, tomando en cuenta la siguiente arquitectura:

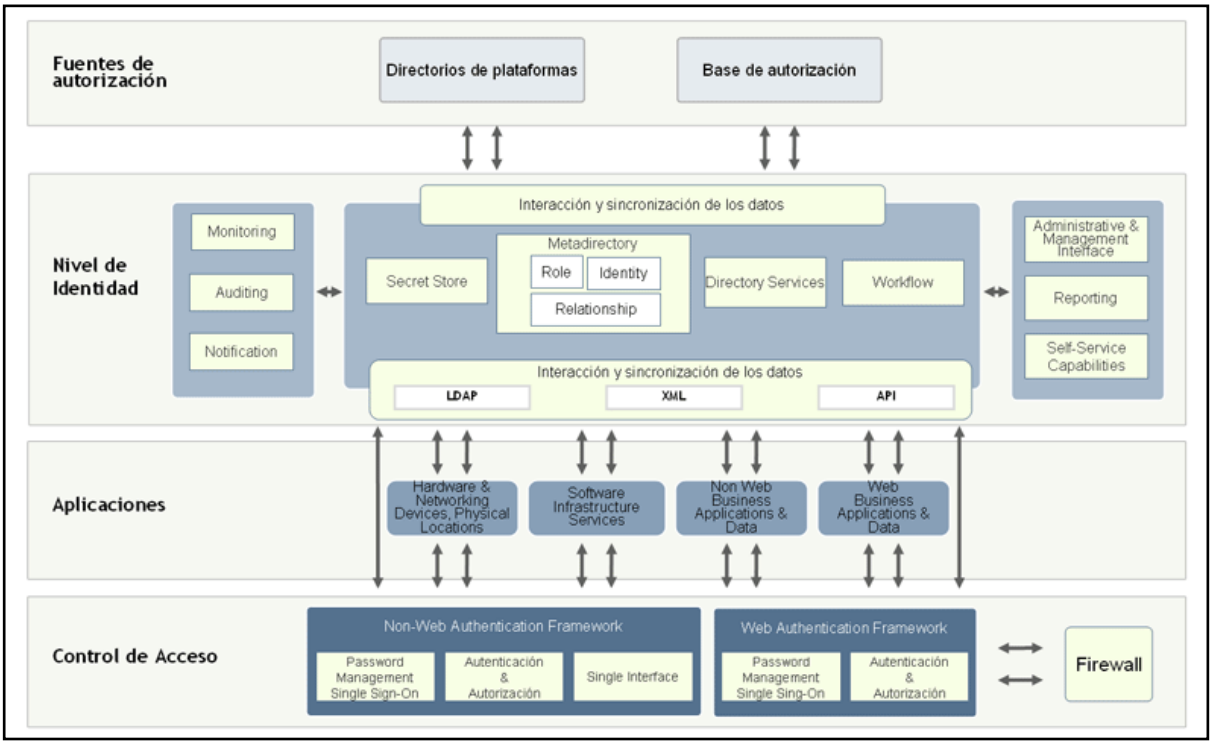

Figura 4 - 02 – Arquitectura CERTANT Technology Solutions **[M]**

Tal como se puede observar, esta arquitectura está conformada por 4 niveles:

- *Fuentes de Autorización*

En este nivel, se hace referencia a lo siguiente:

- Un Directorio de Plataformas, se define como la agrupación de todas aquellas plataformas, integradas al sistema de gestión de identidades, ya sea, sistemas operativos, bases de datos, aplicaciones o servicios organizacionales; donde se muestra su información técnica.

- Una Base de Autorización, hace referencia a las determinadas políticas y normativas de acceso a los diferentes recursos organizacionales.

- *Nivel de Identidad*

Es la fase primordial de un sistema de gestión de identidades, debido a que en este nivel, se presentan importantes funcionalidades de este sistema, mencionando las siguientes:

- Se hace presente las tareas de Monitoreo, Auditoría y Notificación de ciertos procesos, como el aprovisionamiento de las cuentas de acceso a las diferentes plataformas.

- Adicionalmente, es aquí donde se sincronizan los datos entre el repositorio central y las diferentes plataformas integradas.

- Finalmente, a este nivel se hace presente la interacción del usuario con el sistema, ya sea del administrador del sistema o de los usuarios finales, con el fin de gestionar las contraseñas de acceso a los sistemas, generar solicitudes de acceso u obtener reportes o vistas de auditoría.

- *Aplicaciones*

Nivel en el cual, se produce la interacción entre el sistema IDM y las distintas plataformas integradas a éste, permitiendo el intercambio de información.

- *Control de Acceso*

  Principalmente, en esta fase se hace presente el proceso de autenticación; es decir, el control en el acceso a las diferentes plataformas, incluyendo las aplicaciones web.

  Adicionalmente, a este nivel se hace presente el funcionamiento de la tecnología Single Sign On, el cual permite el acceso a los sistemas, haciendo uso de una sola credencial de acceso.

2.3.2 Oracle

Oracle presenta una solución a la gestión de identidades, denominada "*Oracle Identity Management*", la cual está compuesta por una serie de productos que permiten el manejo de la información de usuarios y servicios, brindando una alta seguridad.

El siguiente diagrama muestra estos productos:

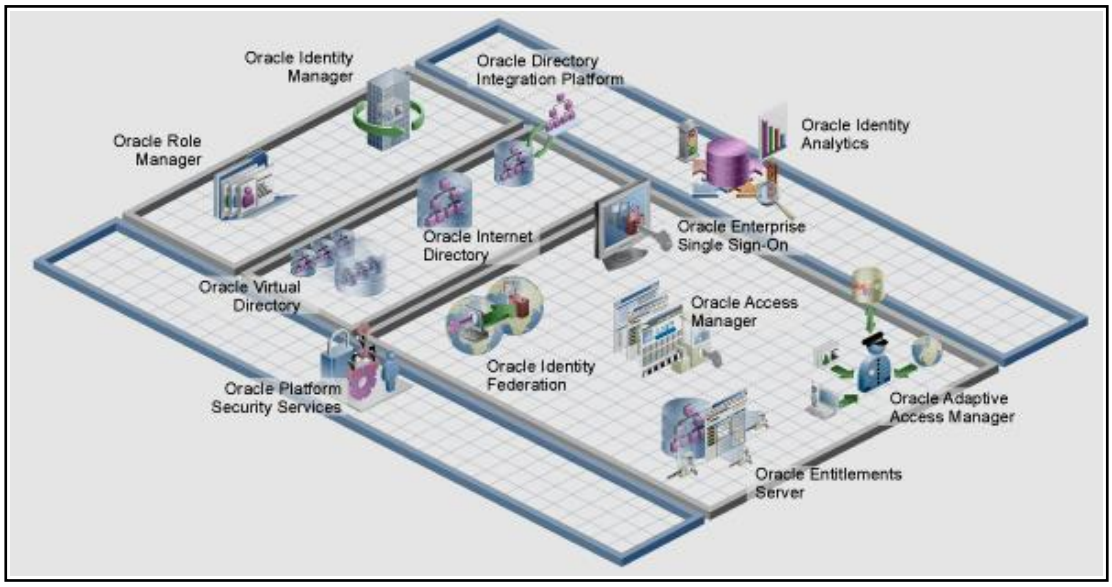

Figura 5 - 02 – Arquitectura Oracle **[N]**

Cada uno de estos productos, permiten la configuración y el manejo de las identidades, con la finalidad de sincronizar e intercambiar información desde diferentes ambientes. Además, permiten que únicamente usuarios autenticados con credenciales válidas, accedan en línea a los recursos del sistema IDM.

En lo referente a la arquitectura de *"Oracle Identity Management"*, a diferencia del sistema expuesto anteriormente, éste no hace referencia a niveles de arquitectura, más bien, a la integración de los productos mencionados en el diagrama anterior, aportando cada uno con su propia funcionalidad al sistema IDM.

Es importante mencionar, que el repositorio central de datos que presenta esta solución, es un programa ***back-end***[18]*,* que maneja simultáneamente múltiples peticiones de usuarios; la siguiente figura muestra este concepto:

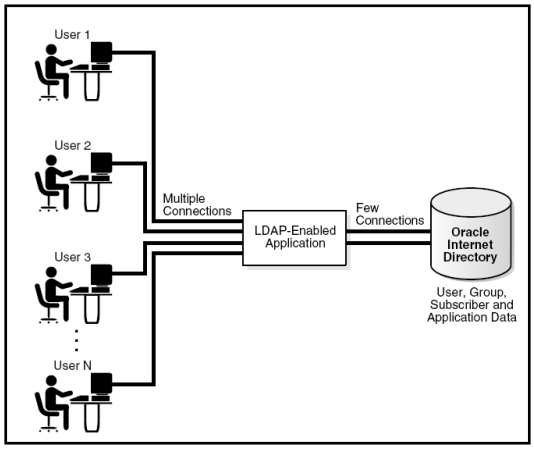

Figura 6 - 02 – Arquitectura Back-End **[O]**

A continuación, se explica el concepto de los productos más relevantes en el funcionamiento de esta solución:

- *Oracle Role Manager*

  Herramienta que permite el manejo y la definición de los roles empresariales, haciendo uso de las respectivas políticas y normativas internas.

[18] Sistemas que procesan datos, obtenidos de las interacciones con los usuarios.

Además, automatiza el aprovisionamiento de perfiles o grupos de usuario, y de esta manera, controlar el acceso hacia la infraestructura IT montada en la organización.

- *Oracle Virtual Directory*

Permite que las aplicaciones tengan acceso a información del sistema IDM, desde diferentes repositorios de datos situados fuera de la organización, esto incluye, servidores de directorios y bases de datos.

- *Oracle Internet Directory*

La funcionalidad de este producto, es añadir, encontrar y manejar información relacionada a usuarios, grupos y otros objetos.

- *Oracle Directory Integration Platform*

Su función es la de compartir información almacenada en la herramienta *"Oracle Internet Directory",* con otros servidores de directorio y aplicaciones.

- *Oracle Access Manager*

La funcionalidad de este producto, es permitir una correcta administración de las identidades, como también de las funciones de seguridad, esto incluye, Web Single Sign On o el acceso a las consolas del sistema IDM.

"*Oracle Access Manager*" presenta una arquitectura de 3 niveles, que proveen una alta seguridad a la información almacenada en este sistema IDM:

  - *Sistema de Identidad*

Provee el manejo de las cuentas de acceso a los sistemas, manejo de grupos dinámicos de usuarios, presenta la funcionalidad de

administración delegada, como también el uso de *workflows* de autorización.

- *Sistema de Acceso*

Este sistema presenta la tecnología Single Sign On, para cualquier aplicación web que se desee integrar. Adicionalmente, soporta una variedad de políticas y normativas de acceso a los distintos sistemas.

- *Servicios de Integración*

Su principal característica, es la de extender todas las funcionalidades de la herramienta "*Oracle Access Manager*", a todos aquellos sistemas integrados a este sistema IDM.

2.3.3 Sun Microsystems

Sun Microsystems, es otra de las empresas que presenta una solución a la gestión de identidades, denominada "*Sun Identity Management*", la cual presenta una arquitectura conformada por cuatro niveles:

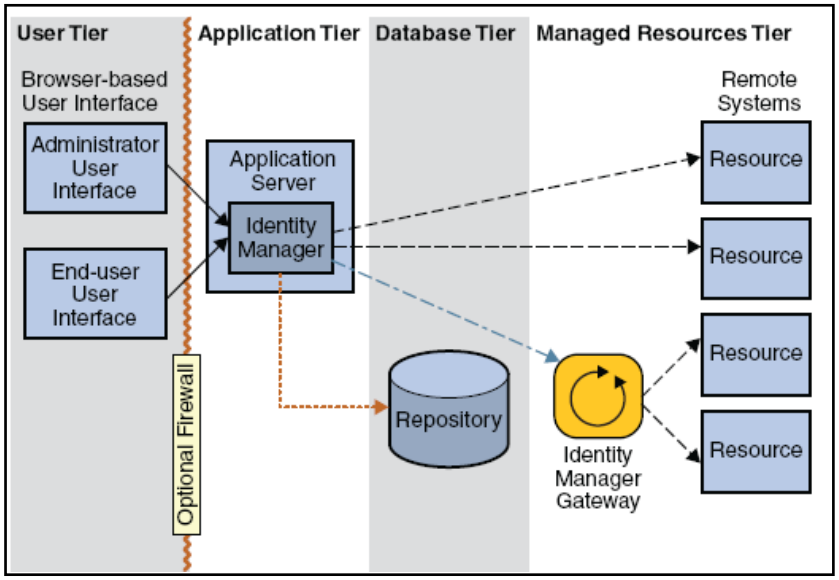

***Figura 7 - 02 – Arquitectura Sun Microsystems* [P]**

- *Nivel de Usuario*

A este nivel, tanto el usuario administrador como los usuarios finales, interactúan directamente con este sistema IDM, a través de las interfaces de usuario que presenta el sistema.

La principal interfaz de usuario, es un navegador web que permite la comunicación directa con este sistema IDM, mediante el protocolo ***HTTPS***[19]. Otras interfaces consisten de páginas ***HTML***[20], y ciertas funcionalidades ***JAVA***[21], a las cuales acceden tanto los usuarios administradores como los finales.

- *Nivel de Aplicación*

En esta capa, se presenta el proceso de aprovisionamiento de cuentas de usuario; es decir, la creación, modificación y eliminación de las cuentas de acceso a los sistemas.

Este proceso se efectúa, a través de adaptadores y conectores que interactúan con los sistemas IT integrados.

- *Nivel de Base de Datos*

A este nivel, se almacena aquella información relacionada al proceso de aprovisionamiento de cuentas, incluyendo el estado de estas transacciones; es decir, se almacena aquella información correspondiente a la creación, modificación y eliminación de cuentas de acceso.

[19] Hypertext Transfer Protocol Secure, es un protocolo de red destinado a la transferencia segura de datos de hipertexto.
[20] Hypertext Markup Language, es un lenguaje utilizado para la construcción de páginas web.
[21] Lenguaje de programación orientado a objetos, desarrollado por Sun Microsystems.

Cabe resaltar, que toda esta información se almacena en un único repositorio de datos. Además, este repositorio guarda los respectivos *logs* de auditoría, que representan las transacciones efectuadas en el sistema.

- *Nivel de Manejo de Recursos*

Esta capa está compuesta por aquellas aplicaciones IT, integradas a este sistema IDM. Esto incluye los respectivos ***gateways***[22] de conexión, quienes se encargan de permitir la interacción de la aplicación Identity Manager con los distintos sistemas IT o aplicaciones integradas.

Adaptadores y conectores proveen las funciones para el respectivo manejo de usuarios, como la creación, modificación, eliminación o lectura de cuentas de usuario, como también la sincronización del cambio de las contraseñas de acceso a las diferentes aplicaciones o sistemas IT integrados.

2.4 Integración de un Sistema de Gestión de Identidades

El proceso de integración de sistemas, aplicaciones, repositorios de datos o servicios organizacionales, con un sistema de gestión de identidades, consiste en lo siguiente:

2.4.1 Sincronización

La sincronización permite la actualización de datos, entre el repositorio central del sistema IDM y los distintos directorios de los sistemas integrados.

[22] Es un ordenador que permite las comunicaciones entre distintos tipos de plataformas, redes, ordenadores o programas.

Además, esta acción asegura que cualquier cambio efectuado en los directorios de los sistemas integrados, se vea inmediatamente reflejada en el sistema de gestión de identidades, por lo cual, la información se mantiene consistente.

Es importante mencionar, que la sincronización se puede efectuar de dos maneras:

- **Una vía:** Se produce cuando únicamente los directorios conectados, proporcionan cualquier cambio al repositorio central del sistema, y no al revés.

- **Doble vía:** Se produce cuando cualquier cambio en el repositorio central del sistema, es suministrado a todos aquellos directorios conectados. También soporta el proceso inverso.

2.4.2 Aprovisionamiento

El aprovisionamiento permite asegurar que un sistema integrado, está siendo notificado de algún cambio en el repositorio central del sistema IDM; como es el caso, de cuentas de usuario y grupos de información.

Adicionalmente, para que el proceso de aprovisionamiento sea eficaz, el sistema integrado debe cumplir con los siguientes requerimientos:

- Tener habilitado el puerto de conexión ***LDAP*** [23], debido a que es necesario el acceso por parte del sistema IDM, a su servicio de directorio, para el intercambio de información.

- Además, el sistema debe permitir el acceso de usuarios autorizados a sus recursos.

[23] Lightweight Directory Access Protocol es 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.

2.4.3 Componentes que Intervienen en el Proceso de Integración

Los componentes que intervienen en este proceso de integración, depende de cada uno de los sistemas IDM, debido a su propia arquitectura.

En el siguiente capítulo, se hace referencia a todos aquellos componentes que intervienen en este proceso; pero en general, los sistemas IDM concuerdan que el proceso de integración, debe constar de al menos:

- Un repositorio en el cual, tanto los componentes del sistema IDM como de los sistemas integrados, almacenen información con respecto a sus funciones.

- Una plataforma de integración, que permita la sincronización de información, entre los diferentes repositorios y el repositorio central del sistema IDM.

  Además, esta plataforma se encarga de los siguientes servicios:

  - *Servicios de Sincronización*

    - Sincronización basada en una calendarización.

    - Intercambio de datos con los directorios integrados.

  - *Servicios de Aprovisionamiento*

    - Aprovisionamiento basado en una calendarización.

    - Manejo de notificaciones, en caso de efectuarse algún cambio en la información de los usuarios, almacenados en el repositorio central del sistema IDM.

3. ESTUDIO DE SOLUCIONES ENFOCADAS A LA GESTIÓN CENTRALIZADA DE ACCESOS

Previo al análisis técnico entre las soluciones enfocadas a la gestión centralizada de accesos, es necesario efectuar un estudio de éstas; para de esta manera, conocer a profundidad los diferentes componentes, características y tecnologías que poseen cada una de ellas.

A continuación se presenta el estudio de estas soluciones, desarrolladas por tres proveedoras de este tipo de software. Es importante mencionar, que en el mercado, existen otras casas fabricantes de este tipo de herramientas.

3.1 Oracle

Oracle presenta una herramienta enfocada a la gestión centralizada de accesos, denominada "*Oracle Identity Management*", la cual permite administrar el ciclo de vida de las identidades, en todos los recursos organizacionales.

Para facilitar el presente estudio, se efectúa una revisión de los diferentes componentes que conforman este software, tomando en cuenta las áreas funcionales que brinda este sistema IDM, como son:

3.1.1 Servicios de Directorio

Para entender conceptos, es necesario definir un directorio, el cual es una colección de entradas con atributos similares, organizados de forma jerárquica. Por ejemplo, una lista que muestra información relacionada a los empleados de una organización.

Un servicio de directorio es uno de los componentes claves de "*Oracle Identity Management*", debido a que el mismo está compuesto por un directorio LDAP, que guarda toda la información de identidad del usuario, incluyendo las credenciales de acceso a los sistemas.

Para dicha función, este sistema IDM hace uso de la siguiente herramienta:

- *Oracle Internet Directory*

Es un directorio LDAP que permite el manejo adecuado de los perfiles de usuario, accesos a los sistemas e información correspondiente a los usuarios.

Este componente se lo maneja como un repositorio central de usuarios para las implementaciones de este sistema IDM, simplificando así, la administración de los usuarios.

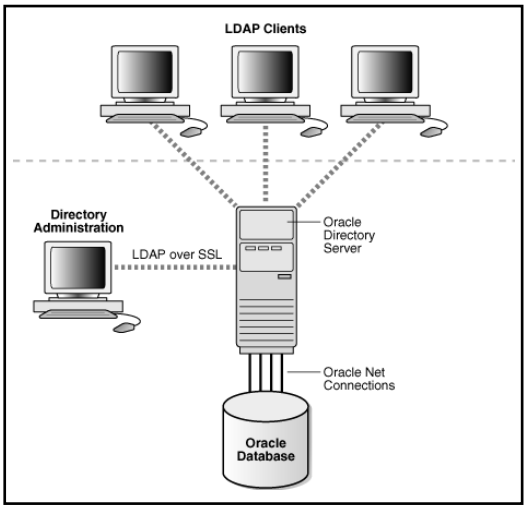

Figura 1 - 03 – Descripción de Oracle Internet Directory **[Q]**

Esta ilustración muestra a "*Oracle Internet Directory*" cumpliendo la función de servidor, al cual se conectan los diferentes clientes y el usuario administrador, a través de una conexión LDAP.

Específicamente, esta herramienta presenta las siguientes características:

- Permite almacenar múltiple información, la cual es manejada a través de un solo repositorio.

- Brinda una alta seguridad a nivel de almacenamiento y respaldo de información, debido a que permite:

  - ✓ Encriptar la información a través del proceso ***Transparent Data Encryption***[24], propio de Oracle.

  - ✓ Asignar adecuadamente responsabilidades, tomando en cuenta la teoría ***separation of duties***[25].

- Provee herramientas avanzadas que facilitan la integración con "*Microsoft Active Directory*", directorios de Sun y Novell, como también de importantes sistemas que se manejan en Recursos Humanos, como es ***PeopleSoft***[26].

- Permite la integración con los sistemas operativos Unix y Linux, con el fin de centralizar el manejo de las cuentas de acceso.

Adicionalmente, con la finalidad de integrar este componente con otros directorios, cuenta con un conector de sincronización, el cual asegura que cualquier cambio efectuado en estos directorios, se vea reflejado inmediatamente en este repositorio central.

3.1.2 Gestión de Identidades

Si se considera el servicio de directorio como el nivel fundamental para almacenar la información de las identidades, la gestión de identidad representa el área que administra el ciclo de vida de éstas.

[24] Proceso de encriptación de datos propio de Oracle, que permite automáticamente encriptar la información al ser escrita en disco, y desencriptada al momento que la aplicación accede a la misma.

[25] La teoría Separación de Tareas, permite asegurarse que un determinado proceso o tarea no sea ejecutado por una sola persona.

[26] Software que permite la gestión de recurso humano, como también la planificación de recursos empresariales.

Oracle presenta una amplia área funcional en lo referente a la gestión de identidades, debido a que encapsula una serie de actividades, tales como, administración de usuarios, la función de autoservicio para los usuarios o el servicio de administración delegada.

Adicionalmente, en este proceso se automatiza la creación, modificación y eliminación, de las cuentas de acceso a los sistemas, a través del uso de *workflows* de autorización como de solicitud.

Para dichas áreas funcionales, este sistema IDM hace uso de los siguientes componentes:

- *Oracle Identity Manager*

  Es una herramienta que ayuda a la gestión de identidades de una forma flexible, cuya función es la de controlar el ciclo de vida de las cuentas de acceso, como también los privilegios de usuario a los sistemas, de una manera centralizada.

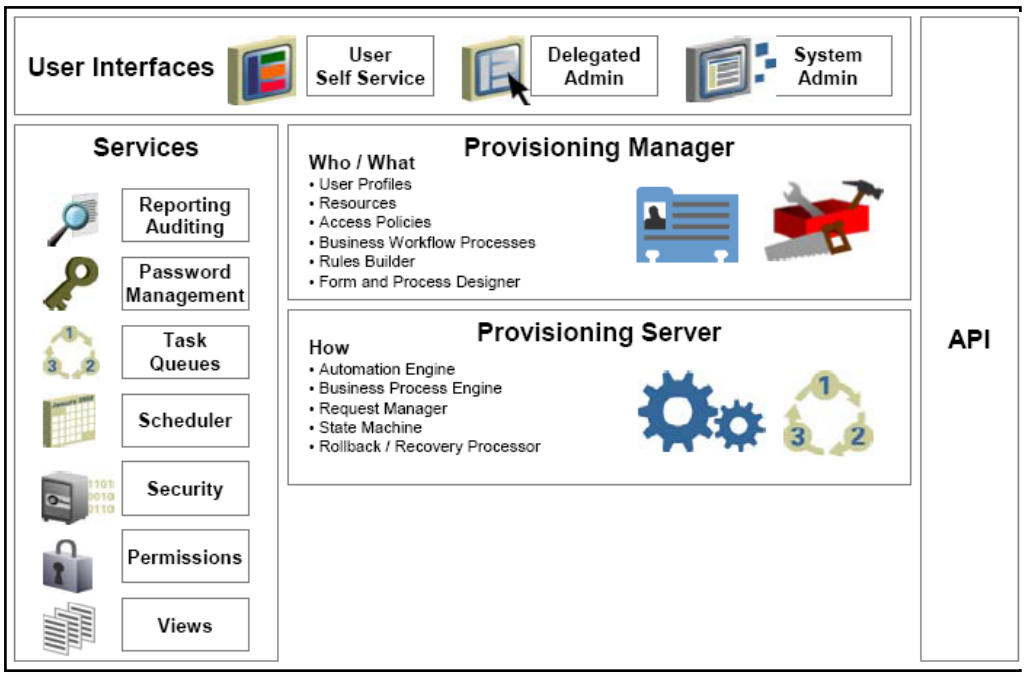

Figura 2 - 03 – Descripción de Oracle Identity Manager **[R]**

Esta ilustración nos muestra las diferentes áreas funcionales que presenta este componente: interfaces de usuario, procesos para el aprovisionamiento de las cuentas de acceso a los sistemas, como también importantes servicios en lo referente al tema de auditoría.

A continuación, se detallan estas funcionalidades:

- *Autoservicio y Administración Delegada*

  Característica que brinda a los propios usuarios, la oportunidad de manejar ciertas funcionalidades del sistema IDM, sin la ayuda de terceras personas; éstas se detallan a continuación:

  - *Manejo de Solicitudes de Acceso a los Sistemas*

    La interfaz de autoservicio que ofrece este componente, permite a los propios usuarios crear solicitudes de aprovisionamiento de acceso los sistemas informáticos.

    Asimismo, los respectivos aprobadores del negocio (jefes de área, gerentes de área, entre otros) pueden hacer uso de esta interfaz web de autoservicio, con la finalidad de aprobar las respectivas solicitudes de acceso a los sistemas, que hayan sido generadas.

  - *Administración Delegada*

    La interfaz de autoservicio, brinda la oportunidad a los propios usuarios del sistema, el delegar funciones o tareas administrativas a un determinado grupo de personas, ya sea de manera fija o temporal; permitiendo así, dar una continuidad a los procesos del negocio.

- *Políticas y Workflows*

Característica que permite definir políticas de acceso a los diferentes recursos organizacionales, utilizando la funcionalidad de los *workflows* que facilitan este proceso.

- *Gestión de Políticas*

Permite establecer una serie de políticas de acceso a los diferentes recursos empresariales, especificando el nivel de acceso. Esto garantiza que los usuarios accedan, únicamente a lo requerido según su rol organizacional.

Además, este componente soporta la Política de Negación, la cual es usada, para negar el acceso de los usuarios a los distintos recursos organizacionales.

- *Gestión de Workflows*

Este componente soporta dos tipos de *workflows*: de aprobación, que es utilizado solamente para procesos propios del negocio, con el fin de manejar las solicitudes de accesos a los recursos organizacionales; y de aprovisionamiento, que de igual manera, permite manejar solicitudes de acceso a los recursos organizacionales, con la diferencia, que únicamente es para procesos propios de IT.

- *Manejo de Errores*

"*Oracle Identity Manager*" permite el manejo de los errores que se presentan durante el proceso de aprovisionamiento de cuentas; permitiendo así, manipular cualquier excepción presentada, sin la necesidad de detener todo este proceso.

- *No Aprovisionamiento Seguro*

Además, esta herramienta permite la configuración de políticas basadas en los roles organizacionales, con el fin de revocar inmediatamente el acceso a todos los recursos empresariales que posee un determinado usuario, al momento que éste deja la organización en su totalidad.

- *Integridad en la Transacción*

También ofrece la oportunidad de efectuar operaciones de ***rollback***[27] y recuperación, en el caso de presentarse algún tipo de error en la ejecución de transacciones de aprovisionamiento de cuentas. De esta manera, se evita que la transacción y la información como tal, se pierda por completo.

- *Seguimiento de Solicitudes en Tiempo Real*

Para tener un mejor control sobre los procesos de aprovisionamiento de cuentas, a través del uso de *workflows*, esta herramienta ofrece la oportunidad tanto a los usuarios como a los administradores, dar un seguimiento al estado de cualquier transacción en tiempo real.

- *Gestión de Contraseñas*

Característica que permite a los propios usuarios del sistema, administrar sus contraseñas de acceso a los sistemas informáticos, sin la ayuda de terceras personas.

- *Gestión de Autoservicio de Contraseñas*

La interfaz web de autoservicio que ofrece este componente, también permite a los usuarios, la administración de sus propias contraseñas de acceso a los sistemas. En caso de olvido de alguna contraseña de acceso,

[27] Operación que permite revertir una transacción, hasta el inicio o hasta un punto de retorno dentro de ésta.

los usuarios podrán hacer uso de este autoservicio, para cambiarlas sin ayuda de terceras personas; comúnmente estas personas representan el servicio de *helpdesk*.

- *Gestión de Políticas Avanzadas de Contraseñas*

Oracle Identity Manager hace uso de políticas muy avanzadas para la gestión de contraseñas de acceso a los diferentes recursos. Algunas políticas complejas que soporta esta herramienta son: extensión de la contraseña, uso de caracteres especiales y alfanuméricos, uso de mayúsculas y minúsculas. Además, esta herramienta permite la aplicación de múltiples políticas por recurso.

- *Gestión de Auditoría*

Característica que permite manejar y administrar el proceso de auditoría, en lo referente al proceso de aprovisionamiento de las cuentas de acceso a los sistemas. También controla y monitorea el ciclo de vida de estas cuentas.

- *Reconciliación de Identidades*

Una de las características más importantes que ofrece este componente, es la detección de posibles cambios en los privilegios de acceso a los sistemas; para lo cual, se toman acciones inmediatas, como rectificar el cambio efectuado o notificar al administrador del sistema.

- *Gestión de Cuentas Huérfanas*

Una cuenta huérfana, es una cuenta que no pertenece a ningún usuario válido en el sistema; representando así, un alto riesgo de seguridad para la organización, por el tema de accesos no autorizados a los sistemas.

Para evitar dicho problema, este componente controla el ciclo de vida de las cuentas de acceso, incluyendo cuentas especiales que pertenecen a los usuarios administradores.

Además, provee un monitoreo continuo de este tipo de cuentas, con la finalidad de identificarlas y actuar según las políticas internas de seguridad.

- *Presentación de Reportes y Auditoría*

"*Oracle Identity Manager*" ofrece la oportunidad de generar reportes con información histórica, en lo referente al aprovisionamiento de las cuentas de acceso a los sistemas informáticos.

El sistema captura toda la información necesaria, para determinar con exactitud "¿Quién/Cuando/Como/Por qué tiene acceso a?". Además, se registra el histórico de: perfiles del usuario, grupos del usuario y todos accesos a los distintos sistemas.

De esta manera, se cumple con varios requerimientos de regulación, como Sarbanes-Oxley, entre otros.

- *Oracle Role Manager*

Es una solución que tiene como objetivo, ofrecer una administración adecuada del ciclo de vida de los roles empresariales, como también de los recursos del negocio.

Asimismo, esta herramienta permite a los propios usuarios, tomando en cuenta sus derechos y su rol organizacional, definir el acceso a los distintos recursos informáticos conforme a la política organizacional.

"*Oracle Role Manager*" soporta varios tipos de roles, entre los principales: de negocio, IT y aprobador de roles organizacionales, los cuales pueden ser configurados tomando en cuenta las políticas internas.

Específicamente, este componente presenta las siguientes características:

- *Gestión del Ciclo de Vida de los Roles Organizacionales*

  Esta herramienta presenta una interfaz web, en la cual los usuarios pueden crear y manejar roles organizacionales, como también manejar el estado de éstos, para controlar el acceso a los diferentes recursos.

  - *Extracción de Roles y Reglas*

    Esta característica permite una mejor administración de los roles organizacionales, de la siguiente manera:

    - Importando usuarios, recursos e información privilegiada, para su análisis y validación. El proceso de análisis permitirá eliminar las posibles cuentas huérfanas y cubrir violaciones a la política de seguridad.

    - Estructurando los roles de manera jerárquica, permite observar los derechos de acceso que poseen, y así asegurarse que éstos sean los correctos.

  - *Repositorio de Derechos y Roles Autorizados*

    Permite manejar la información de la empresa, como relaciones organizacionales dentro de un repositorio global de roles. Siendo éste el repositorio central que contiene la información de los roles, estas relaciones suministran los derechos de autorización a los diferentes sistemas.

- *Delegación de Roles*

  Esta herramienta presenta la característica de delegar roles de administración, que permite a los propios usuarios el autorizar privilegios de acceso a los sistemas, sin violar la política interna existente.

3.1.3 Gestión de Accesos

La gestión de accesos cumple el objetivo de ser el guardián que determina qué usuarios tienen acceso a qué tipo de información y en qué momento, tomando como referencia las políticas organizacionales.

Además, tiene como fin:

- Administrar autorizaciones específicas y derechos de acceso, en torno a los recursos organizacionales.

- Prevenir anticipadamente toda actividad fraudulenta.

- Fortalecer la seguridad en el proceso autenticación a los diferentes sistemas informáticos.

Para dichas áreas funcionales, Oracle hace uso de las siguientes herramientas:

- *Oracle Access Manager*

  Es una solución que combina tanto la gestión de identidades de usuario, como también el control de acceso a los diferentes servicios organizacionales; con el fin de proveer una autenticación centralizada, como también autorizaciones basadas en las políticas internas y auditoría en la administración de las identidades.

Esta herramienta está compuesta por un sistema de acceso, como también de un sistema de identidad. El primero asegura que las aplicaciones estén provistas de una autenticación segura y centralizada, mientras que la otra, se encarga de la administración con respecto a la información de los usuarios, grupos y recursos organizacionales.

Específicamente, este componente presenta las siguientes características:

- *Gestión de Accesos*

  El sistema de acceso provee de una autenticación centralizada, tomando en cuenta autorizaciones y auditoría. Además, este sistema permite habilitar la tecnología Single Sign On, como también asegurar el acceso a todos los recursos organizacionales, ya sean aplicaciones web, recursos ***J2EE***[28] u otros sistemas informáticos.

  - *Autenticación*

    Este sistema de acceso provee de varios métodos de autenticación a los sistemas, los cuales son:

    - Uso de identificadores de usuario y contraseñas.
    - ***Certificados X.509***[29].
    - *Smart cards*.
    - Tokens de seguridad.
    - Autenticación personalizada vía ***APIs***[30].

[28] Plataforma de programación para desarrollar y ejecutar software de aplicaciones, en un lenguaje de programación Java.
[29] Certificados utilizados para garantizar la vinculación entre la identidad de un sujeto y su clave pública.
[30] Interfaz de programación de aplicaciones.

Adicionalmente, permite definir políticas de acceso que ayudan a determinar niveles de autenticación, con el fin de brindar una mayor seguridad.

Este componente provee una autenticación API, con la finalidad de integrar una variedad de métodos de autenticación y dispositivos. Esto incluye sistemas biométricos como autenticación de doble factor.

- *Autorización*

Por defecto, este sistema de acceso provee de políticas de autorización, para asegurar el acceso a los sistemas web como J2EE.

Además, los administradores del sistema podrán hacer uso de una consola web para administrar estas políticas, en la cual se podrán definir reglas para restringir el acceso a los sistemas, ya sea a través del usuario, rol, grupo, hora, día de la semana o la dirección IP.

- *Auditoría*

El servicio de auditoría, provee de *logs* detallados que pertenecen a los eventos monitoreados por "*Oracle Access Manager*". Estos eventos incluyen los accesos satisfactorios y fallidos a los sistemas. Adicionalmente, incluye información con respecto al usuario, fecha de ingreso a los recursos, dirección IP, entre otros.

- *Componentes del Sistema de Acceso*

El sistema de acceso incluye los siguientes componentes:

❖ *Web Gate*

Este componente es un módulo, cuya funcionalidad es la de interceptar todas aquellas solicitudes HTTP para el acceso a los sistemas, y así enviarlas al respectivo servidor de acceso, en el cual las políticas de acceso son aplicadas.

❖ *Servidor de Accesos*

Este componente tiene la función de hacer cumplir todas aquellas políticas, tanto para el acceso a los diferentes recursos organizacionales, como también para los servicios de auditoría, autenticación y autorización.

❖ *Consola - Administrador de Políticas*

Este componente es una herramienta gráfica, que permite crear y administrar políticas de acceso a los recursos organizacionales.

Además, esta herramienta se comunica con el sistema de acceso y también con el servidor de acceso, para de esta manera, actualizar información con respecto a las políticas de acceso ya definidas.

Un usuario administrador hace uso de esta herramienta para:

- Crear y administrar políticas de dominio, que consiste en:

  ✓ Proteger los diferentes tipos de recursos organizacionales.
  ✓ Definir reglas de autenticación, autorización y dominio.
  ✓ Definir políticas de excepción.
  ✓ Determinar derechos administrativos.

- Ejecución de pruebas, para el análisis de las políticas de acceso.

❖ *Consola - Sistema de Acceso*

Esta consola permite:

- Configurar los distintos esquemas de autenticación y autorización.

- Configurar las diferentes opciones con respecto al servicio de auditoría.

- Revocar usuarios específicos del sistema.

- Monitorear el estado del sistema.

o *Gestión de Identidad*

El sistema de identidad, permite a los usuarios administradores o finales, tener acceso a la administración de sus identidades.

Para este fin, la herramienta presenta las siguientes funcionalidades:

▪ *Administración Delegada*

Esta característica permite el delegar la responsabilidad de la gestión de usuarios, permitiendo un trabajo distribuido y eficiente.

Esta funcionalidad es útil, cuando un ejecutivo tiene a su cargo una serie de contratos con proveedores, lo cual resulta una tarea complicada para su efectiva administración; en este caso, la persona puede delegar esta responsabilidad a otros ejecutivos.

- *Gestión de Grupos Dinámicos*

Permite la asignación dinámica de usuarios a un determinado grupo, con la finalidad de mejorar el control de acceso y la tarea administrativa; es decir, los usuarios son asignados automáticamente a un determinado grupo, siguiendo una serie de reglas o filtros (basados en los respectivos atributos de los usuarios), que han sido previamente configurados. Este proceso evita que los propios administradores del sistema, efectúen dicha acción manualmente.

Un grupo se lo usa para representar un determinado rol organizacional.

- *Autoservicio para los Usuarios*

Permite a los propios usuarios del sistema, cambiar su información personal, ya sea números telefónicos, dirección del domicilio, entre otros; tomando en cuenta ciertos niveles de privilegio, por seguridad.

- *Gestión de Contraseñas Pérdidas*

Esta característica permite a los propios usuarios, cambiar automáticamente sus contraseñas de acceso a los diferentes sistemas, en caso de olvidarlas.

Para este fin, el sistema obligará a los usuarios a contestar una serie de preguntas de desafío, con el fin de determinar la identidad del usuario.

- *Componentes del Sistema de Identidad*

El sistema de identidad presenta los siguientes componentes:

❖ *Web Pass*

Este componente actúa como un módulo o ***plugin***[31], que permite el envío de información al respectivo servidor de identidades.

Adicionalmente, este componente presenta una interfaz web, que permite interactuar a través de programación, con el sistema de acceso.

❖ *Servidor de Identidades*

Este componente maneja aquella información relacionada con los usuarios, grupos, organizaciones, entre otros; el cual presenta las siguientes funcionalidades:

- Almacena la información del usuario en un servidor de directorio. Además, mantiene a este directorio actualizado.

- Procesa aquellos requerimientos o solicitudes relacionadas al usuario, grupo o la organización.

▪ *Consola – Sistema de Identidad*

Esta consola provee de una interfaz web, para la configuración y administración de los distintos componentes y aplicaciones que conforman este sistema de identidad.

[31] Módulo de hardware o software que añade una característica o un servicio específico, a un sistema más grande.

- *Auditoría*

Para el servicio de reportes de auditoría, "*Oracle Access Manager*" presenta una interfaz especializada en esta tarea, por lo cual, toda actividad referente a la seguridad y la gestión de accesos a los sistemas, es registrada en una base de datos centralizada.

Algunos de los reportes de auditoría más comunes que presenta esta herramienta, son:

- Estadísticas de acceso a los sistemas informáticos, ya sean satisfactorios o fallidos.

- Estadísticas de autorización de acceso a los sistemas, ya sean aprobadas o negadas.

- Historiales de los grupos de usuario (cambios efectuados en los perfiles de los grupos).

- Historial de las identidades.

- Usuarios que presentan un acceso bloqueado a los recursos organizacionales.

- Cambios de contraseña efectuados.

- Creación, desactivación temporal, reactivación y eliminación de cuentas de acceso.

- Historial de las modificaciones a los perfiles de usuario.

- *Oracle Entitlements Server*

Componente que permite una administración centralizada de todas aquellas políticas de autorización y acceso a los recursos organizacionales.

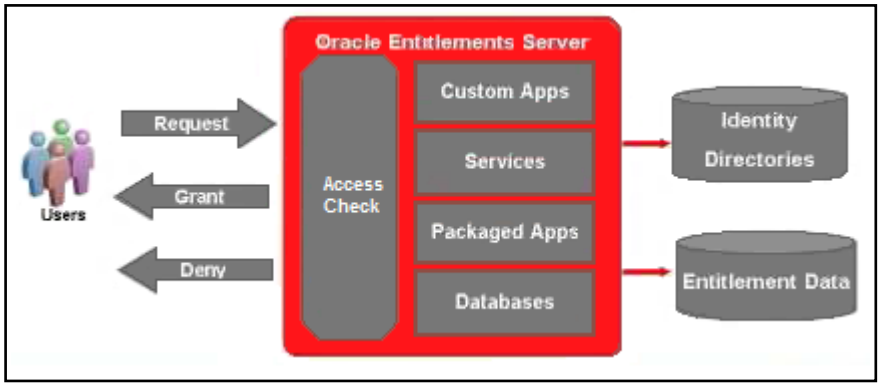

Figura 3 - 03 – Descripción de Oracle Entitlements Server **[S]**

En esta imagen se aprecia, como "*Oracle Entitlements Server"* recepta aquellas solicitudes de acceso a las diferentes plataformas, y las valida basándose en las políticas de autorización y de acceso a los recursos organizacionales.

Además, esta herramienta presenta una consola web de administración, que permite al usuario administrador editar y realizar pruebas con aquellas políticas de autorización y de acceso a los recursos organizacionales, con la particularidad de poder especificar estas políticas a usuarios, grupos o roles.

- *Oracle Identity Federation*

Es una solución que brinda una alta seguridad al momento de intercambiar información de las identidades, entre los distintos proveedores, clientes o socios organizacionales; es decir, provee una mayor seguridad en el acceso a sus aplicaciones desde redes externas a la organización.

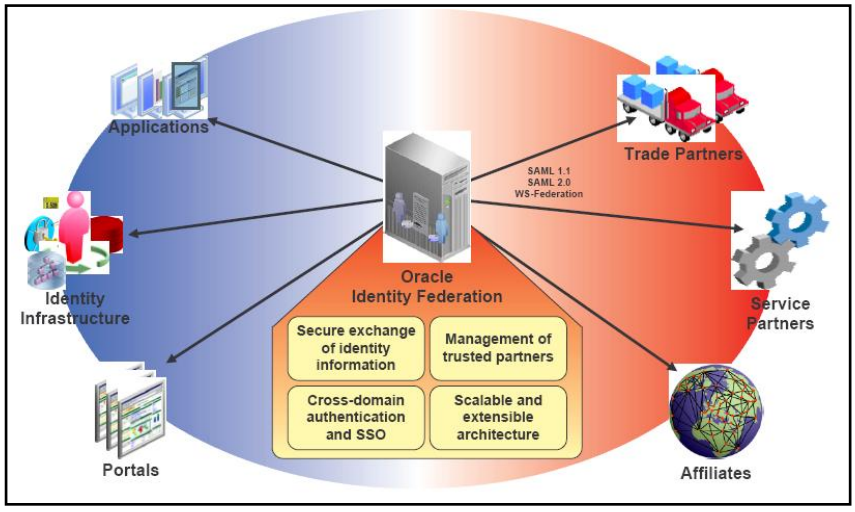

Figura 4 - 03 – Descripción de Oracle Identity Federation **[T]**

La ilustración revela el ambiente en el cual se maneja “Oracle Identity Federation”, proporcionando una alta seguridad en el intercambio de información de las identidades con: aplicaciones externas, socios, afiliados, como también con portales externos. Para que el acceso a la información sea seguro, la herramienta utiliza la tecnología Single Sign On, la cual provee una autenticación robusta.

Adicionalmente, esta herramienta hace uso de una consola administrativa, con el fin de poder configurar los respectivos protocolos de conexión a redes externas, la autenticación que hacen uso los proveedores, los equipos de conexión correspondientes a los proveedores, entre otras tareas administrativas para conexiones entre distintos dominios.

- *Oracle Enterprise Single Sign On - ESSO*

Herramienta que permite a los usuarios acceder a los distintos recursos organizacionales, haciendo uso de una sola credencial de acceso.

La siguiente imagen, muestra exactamente este proceso de autenticación.

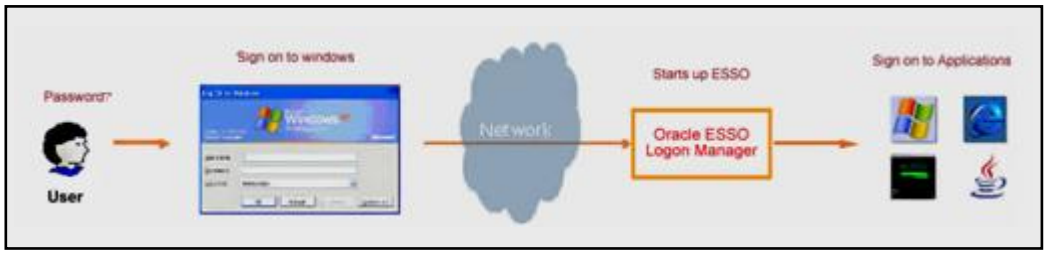

Figura 5 - 03 – Descripción de Single Sign On **[U]**

Como se observa, el usuario ingresa su credencial de acceso en la pantalla de inicio de Windows, una vez que accede a la red corporativa, “Oracle ESSO” hace uso de esta misma credencial de acceso para el ingreso a las distintas aplicaciones, sin que el usuario se autentique nuevamente.

A continuación, se detalla los componentes que conforman esta herramienta:

- *Oracle ESSO Logon Manager*

  Este componente provee de ciertas interfaces para el proceso de autenticación, tanto en la red corporativa como en las distintas aplicaciones.

  La consola de administración de Oracle ESSO, interactúa con este componente para facilitar la administración de sus atributos.

- *Oracle ESSO Password Reset*

  Este componente provee un mecanismo de recuperación de las contraseñas de acceso, el cual permite a los propios usuarios, cambiarlas desde la pantalla de autenticación de Windows.

- *Oracle ESSO Authentication Manager*

Este componente permite la implementación de varios métodos de autenticación adicionales, tales como el uso de tokens de seguridad, tarjetas inteligentes y sistemas biométricos, con la finalidad de aumentar el control en el acceso a los sistemas informáticos.

- *Oracle ESSO Provisioning Gateway*

Este componente se encarga de distribuir las credenciales de acceso a "*Oracle ESSO*". Adicionalmente, el usuario administrador puede añadir credenciales de acceso tanto para nuevos sistemas como para nuevos usuarios. También es posible modificar o eliminar antiguas credenciales de acceso.

- *Oracle Authentication Services para Sistemas Operativos*

Este componente provee una autenticación y administración de las cuentas de acceso de una manera centralizada, para plataformas especiales tales como ***Unix*** [32] y ***Linux***[33]. La solución consiste del funcionamiento de la herramienta "*Oracle Internet Directory",* previamente detallado, integrado con los sistemas operativos Unix o Linux a través de protocolos de conexión como LDAP.

Esta herramienta es indispensable en tiempos actuales, donde la gran mayoría de las organizaciones hacen uso de este tipo de servidores por su gran funcionalidad y rendimiento. También, evitan posibles brechas de seguridad debido a la aplicación de políticas de acceso inconsistentes con este tipo de servidores.

[32] Sistema operativo portable, multitarea y multiusuario, desarrollado por un grupo de empleados de los laboratorios Bell de AT&T.

[33] Sistema operativo de libre distribución UNIX para computadoras personales, servidores y estaciones de trabajo.

3.2 Sun Microsystems

Sun Microsystems también presenta una herramienta enfocada a la administración centralizada de identidades, brindando una alta seguridad en el acceso a los diferentes recursos organizacionales.

Para facilitar el estudio de esta herramienta, se efectuará una revisión de los diferentes componentes que conforman este software, tomando en cuenta sus áreas funcionales.

3.2.1 Servicios de Directorio

Para este fin, Sun Microsystems hace uso de una herramienta denominada "*Sun Directory Enterprise Edition*", la cual se encarga de proveer un servicio de directorio centralizado, para así permitir el almacenamiento y la administración de las identidades, como también de los privilegios de acceso a los sistemas. Para su efectiva administración, este software presenta una consola web de administrador.

Además, permite la sincronización de datos entre "*Microsoft Active Directory*" y este servicio de directorios, que incluye: contraseñas de acceso, grupos de usuarios, entre otra información de las identidades.

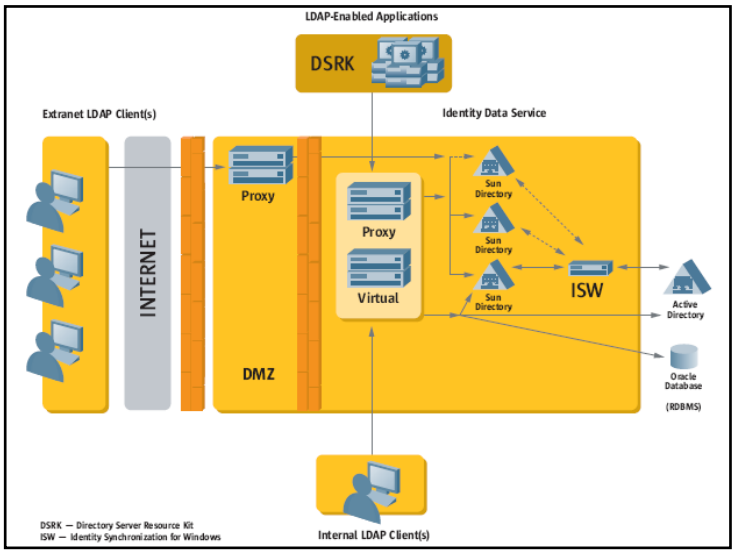

Figura 6 - 03 – Descripción de Sun Directory Enterprise Edition [V]

Como se muestra en la ilustración, las diferentes aplicaciones integradas al sistema IDM, se conectan a través del protocolo LDAP con el directorio virtual y el servicio de directorio proxy, para la respectiva administración de sus identidades. Además, la integración de este directorio con "*Microsoft Active Directory*", se lo realiza a través de un componente de sincronización de datos exclusivo para la plataforma Microsoft.

Específicamente, este servicio presenta las siguientes características:

- Un repositorio centralizado para la respectiva administración y almacenamiento de: identidades, sistemas e información relacionada a los recursos de una red corporativa.

- Un directorio de servicios proxy, el cual permite controlar el acceso basado en un determinado criterio. También intercepta operaciones no autorizadas.

- Presenta una característica de compresión de información, con el fin de ahorrar espacio en el disco duro como en la memoria de este servidor centralizado de directorios.

- Presenta una consola administrativa, permitiendo una completa gestión de esta herramienta.

3.2.2 Gestión de Identidades

Para este concepto, Sun Microsystems utiliza herramientas que se enfocan al proceso de aprovisionamiento de usuarios, administración del ciclo de vida de las identidades, como también al manejo de los roles organizacionales.

Dichas herramientas, se mencionan a continuación:

- *Sun Identity Manager*

Componente que se encarga de automatizar el proceso de aprovisionamiento /no aprovisionamiento; es decir, la creación, actualización y eliminación de las cuentas de acceso a los sistemas IT.

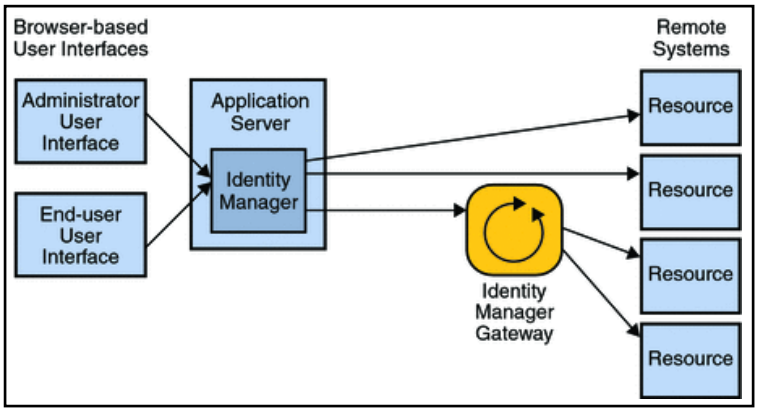

Figura 7 - 03 – Descripción de Sun Identity Manager **[W]**

Esta figura nos explica el proceso de conexión entre “Sun Identity Manager” y los diferentes recursos organizacionales. Esta conexión consiste de una serie de adaptadores que permiten el intercambio de datos entre las plataformas. Existen ciertos recursos que necesitan de un *gateway* para la respectiva conexión, tal es el caso de los productos Microsoft.

Específicamente, este componente presenta las siguientes características:

- *Gestión de Roles Organizacionales*

  “Sun Identity Manager” aprovecha la definición de los roles organizacionales, con la finalidad de mejorar el proceso de aprovisionamiento y la auditoría de las respetivas identidades. Además, permite al usuario administrador otorgar derechos de acceso a los diferentes sistemas informáticos, de una manera más eficiente.

- *Aprovisionamiento y Sincronización de las Identidades*

Permite el aprovisionamiento y la sincronización de las identidades correspondientes a los sistemas informáticos.

Para el proceso de aprovisionamiento de las cuentas de usuario, este componente haces uso de una serie de *workflows* para evitar posibles accesos no autorizados.

Con el fin de efectuar la comunicación entre este componente y los diferentes sistemas IT, esta herramienta utiliza un sin número de adaptadores y conectores, con la ayuda de protocolos API´s.

- *Auditoría*

Además, permite que se cumplan las diferentes políticas de auditoría existentes en la organización. Estas políticas especifican el tipo de acceso que un determinado usuario debería o no poseer.

Este componente, también provee de políticas basadas en la administración del ciclo de vida de las identidades y en los procesos de auditoría de éstas. Esto permite el control de los procesos de aprovisionamiento y auditoría.

Adicionalmente, permite revisiones automatizadas de la información de las identidades, con el fin de detectar y notificar posibles violaciones a las políticas establecidas.

Asimismo, se encarga de proveer una serie de reportes de cumplimiento, los cuales que pueden ser personalizados. Estos reportes presentan información de los procesos de aprovisionamiento y sincronización de las identidades.

- *Administración de Identidades Federadas*

  Esta herramienta también mantiene un control del proceso de aprovisionamiento de las identidades que corresponden a ambientes externos, como es el caso de proveedores y clientes.

Además, este componente se caracteriza por presentar dos interfaces web de usuario:

- Interfaz para el usuario administrador: permite administrar usuarios, crear y asignar recursos, definir derechos y niveles de acceso, establecer políticas de auditoría, como también configurar otras tareas administrativas.

- Interfaz para los usuarios finales: permite hacer uso de las tareas de autoservicio, tales como, cambiar automáticamente las distintas contraseñas de acceso a los sistemas o delegar ciertas tareas laborales a otros usuarios, en caso de necesitarse.

- *Sun Role Manager*

Componente que ayuda a una eficiente administración del ciclo de vida de los roles organizacionales. A continuación, se explica este proceso de administración:

- Un repositorio central es creado, con la finalidad de contener información de los usuarios, sus respectivos accesos y sus privilegios de usuario.

- Luego se efectúa las relaciones usuario-jefe y jefe-privilegios de acceso, con el fin de automatizar el control de acceso a los recursos organizacionales.

- Una vez que el repositorio y las relaciones estén disponibles, ciertas técnicas de extracción de roles son utilizadas, para así definir los respectivos roles organizacionales.

Esta herramienta presenta las siguientes características:

- *Gestión de Roles*

  Permite una correcta gestión de los roles organizacionales, tomando en cuenta los atributos de los usuarios y sus respectivos derechos de acceso, que poseen los distintos sistemas informáticos.

  Esta herramienta permite la definición de nuevos roles organizacionales, basándose en ***templates***[34] de usuarios, como referencia.

  También presenta un impacto de análisis, para observar y entender como los usuarios pueden ser afectados, si son sometidos a cambios en sus roles organizacionales.

- *Aplicación de Políticas*

  Este componente, presenta un monitoreo constante en lo referente a los problemas de acceso a los recursos organizacionales, cuando éstos están en contra de la política de seguridad interna. Tal es el caso de accesos no autorizados.

  Además, provee una adecuada gestión del ciclo de vida de aquellas políticas que han sido violadas, aspecto importante por temas de auditoría.

[34] Plantillas ya elaboradas, que contienen un diseño, patrón y estilo, ya definido.

- *Cuadro de Cumplimiento*

  Provee de vistas que muestran aquellas faltas a las políticas de acceso definidas. Asimismo, esta herramienta muestra un análisis histórico de estas faltas cometidas, como también de las aprobaciones de los diferentes roles organizacionales.

3.2.3 Gestión de Accesos

En lo referente a este concepto, Sun Microsystems se enfoca en una administración adecuada de los accesos a las aplicaciones y servicios web, brindando una alta seguridad al intercambiar la información almacenada en estos sistemas, con clientes, proveedores o cualquier ente externo a la organización.

Para dicha función, Sun Microsystems hace uso de la siguiente herramienta:

- *Sun Single Sign On Enterprise*

  Es una herramienta que provee seguridad, al presentar un control centralizado de accesos. Además, hace uso del método de autenticación Single Sign On para aplicaciones internas o externas a la organización, como también para los servicios web.

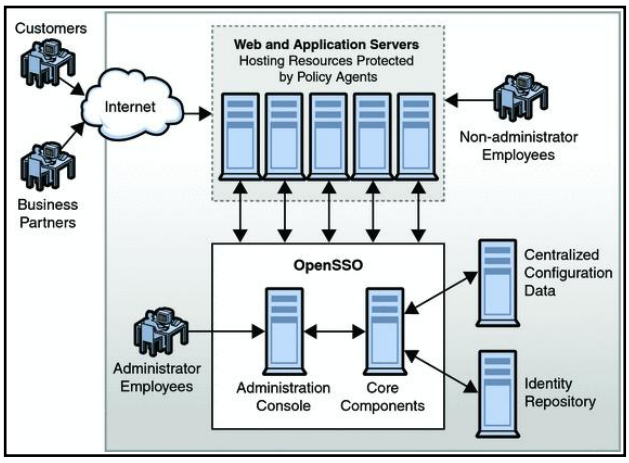

Figura 8 - 03 – Descripción de Sun Single Sign On Enterprise **[X]**

La imagen nos muestra el ambiente funcional que presenta “Sun Single Sign On Enterprise”, en el cual existen ciertos agentes llamados “*Policy Agents*”, que interceptan cualquier solicitud de acceso a los distintos recursos organizacionales. Estas solicitudes son enviadas a “Sun Single Sign On Enterprise”, el cual solicita las credenciales de acceso para su correspondiente validación contra el repositorio de identidades.

Específicamente, este componente presenta las siguientes características:

- *Gestión de Accesos*

  Esta herramienta se encarga de la administración de aquellos accesos a redes externas, tales como clientes y proveedores; con la característica de brindar una alta seguridad a través de la tecnología Single Sign On y políticas de seguridad.

  Además, permite al usuario administrador la configuración de ***agentes***[35], servidores, como también de la aplicación de políticas de seguridad, desde una sola consola de administración.

- *Federación de Identidades*

  Esta característica permite a la organización compartir sus identidades digitales, como credenciales de acceso, de una forma segura entre distintos dominios, permitiendo así la autenticación de usuarios externos a los recursos organizacionales.

A continuación, se muestran otras características importantes que presenta esta herramienta:

[35] Sistemas que facilitan el intercambia de la información entre el cliente y el servidor.

- Presenta una consola de configuración, que permite al usuario administrador configurar e implementar varias instancias de esta herramienta.

- Además, provee de varios flujos de tarea, con el fin de guiar a los usuarios a lo largo de las funciones que presenta esta herramienta.

- Finalmente, presenta la posibilidad de implementar un servicio de seguridad token, tomando como referencia, ciertos estándares basados en la creación y validación de estos dispositivos.

3.2.4 Gestión de Auditoría

En lo referente a la gestión de auditoría, Sun Microsystems se enfoca a automatizar el proceso de registrar y mostrar la información de las identidades, como la información personal de los usuarios, accesos a los diferentes recursos organizacionales, entre otros.

Para este objetivo, Sun Microsystems hace uso de la siguiente herramienta:

- *Sun Identity Compliance Manager*

  Componente que se encarga de automatizar el proceso de consolidación de la información organizacional, es decir, una colección de la información correspondiente a los usuarios, recursos organizacionales, como también los diferentes accesos a éstos.

  Adicionalmente, esta herramienta hace uso de varias vistas o reportes, con la finalidad de mostrar la información mencionada anteriormente, que permitirá cumplir con los requerimientos de auditoría.

  Estos procesos de consolidación como de muestreo de información a través de reportes, pueden ser personalizados y calendarizados, dependiendo del caso.

3.3 BMC Software

El último software a estudiar corresponde a la organización BMC Software, denominado "*BMC Identity Management Suite*", el cual consiste de una serie de productos diseñados para proveer grandes soluciones en el área de la gestión de identidades, tales como:

- Aprovisionamiento y administración de usuarios.
- Gestión de contraseñas.
- Gestión de auditoría y cumplimiento.
- Gestión de acceso web.
- Gestión de requerimientos de identidades.
- Gestión de federación de identidades.

Para facilitar el presente estudio, se efectúa una revisión de los diferentes componentes que conforman este software, tomando en cuenta las áreas funcionales que brinda este sistema IDM, como son:

3.3.1 Servicios de Directorio

BMC Software utiliza un servicio de directorio, con la finalidad de almacenar información correspondiente a los recursos organizacionales, en un sólo repositorio de datos.

Para dicha función, este sistema IDM presenta la siguiente herramienta:

- *BMC Control SA/Directory Manager*

Es una solución a la administración de directorios, la cual es un repositorio centralizado de datos que contiene información de las identidades, como usuarios, recurso organizacionales, entre otros.

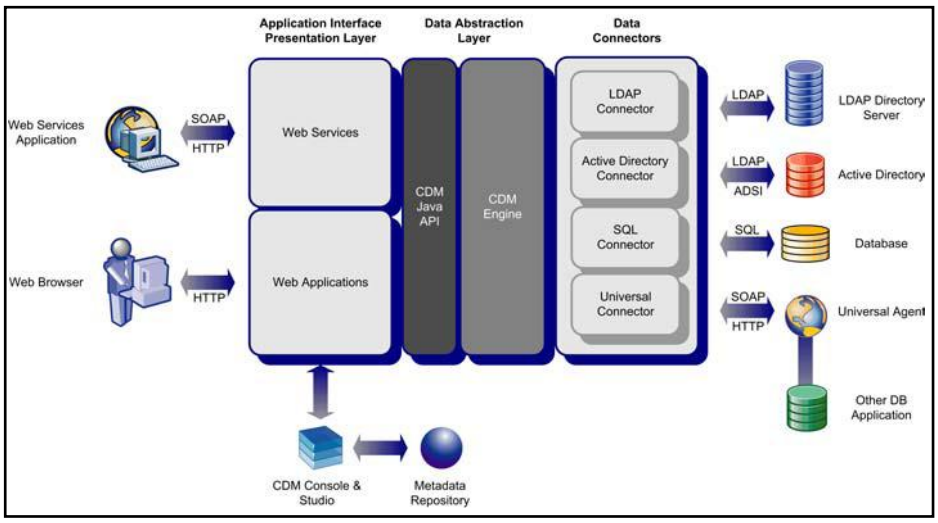

Figura 9 - 03 – Descripción de BMC Control SA/Directory Manager **[Y]**

Esta ilustración muestra la arquitectura lógica que presenta "*BMC Control SA/Directory Manager*", en la cual resalta 3 capas:

- Capa de Presentación: A este nivel, los distintos usuarios como las aplicaciones de servicios web, interactúan directamente con este sistema IDM a través del protocolo HTTP.

- Capa de Abstracción: Abarca los procesos de integración como de sincronización de la información correspondiente a las identidades. El repositorio central de las identidades se hace presente en este nivel.

- Capa Lógica: Corresponde a todos aquellos servicios (agentes, conectores), que permiten la conexión entre el sistema IDM y las distintas plataformas integradas.

Esta herramienta presenta las siguientes características:

- Utiliza la funcionalidad de los *workflows*, para la administración de la información almacenada en el directorio.

- La conexión que mantiene este repositorio con los demás, es a través de un ambiente de conexión LDAP, la cual brinda una alta seguridad a la misma.

- Provee de vistas con información de los perfiles de usuario, como también de los derechos de acceso a los recursos organizacionales.

- Además, esta herramienta soporta accesos simultáneos a la información almacenada en este repositorio.

- Presenta una consola de administración de la herramienta, en la cual se muestra información correspondiente a las aplicaciones, sus conexiones LDAP, los respectivos roles y sus derechos de acceso a los diferentes recursos organizacionales.

3.3.2 Gestión de Identidades

BMC Software con el fin de mantener una adecuada gestión de las identidades, lleva a cabo una completa administración del ciclo de vida de éstas, como también de su proceso de aprovisionamiento; es decir, creación, actualización y eliminación de las cuentas de acceso a los recursos organizacionales.

Además, se preocupa por la gestión y sincronización de las contraseñas de acceso a los diferentes sistemas informáticos; permitiendo a los propios usuarios, cambiarlas a través de un proceso automático.

Para dichas áreas funcionales, este sistema IDM hace uso de las siguientes herramientas:

- *BMC User Administration Manager*

Componente que tiene como función, tanto el proceso de aprovisionamiento como la gestión de seguridad de las cuentas de acceso a los recursos organizacionales.

Para lo mencionado, esta herramienta presenta las siguientes características:

- *Aprovisionamiento Automático de Usuarios*

  Presenta una eficiente administración en el proceso de aprovisionamiento/ no aprovisionamiento de las diferentes cuentas de acceso a los sistemas, basándose en los derechos de acceso y roles organizacionales de los usuarios.

  Es importante mencionar, que usuarios externos a la organización, como clientes o proveedores, son creados y eliminados a través de este sistema IDM. Luego de este proceso, las diferentes cuentas de acceso a los sistemas informáticos son automáticamente creadas o eliminadas, tomando en cuenta las respectivas políticas de seguridad.

- *Gestión de Workflows*

  Para el proceso de administración de usuarios a través del uso de *workflows*, esta herramienta trabaja a la par con el siguiente producto:

  - *BMC Identity Request Manager*

    Es una herramienta enfocada al proceso de administración de usuarios, a través del uso de *workflows*. Este proceso corresponde a la acción de crear, actualizar y eliminar cuentas de acceso a los diferentes recursos organizacionales.

Únicamente, usuarios con personal a cargo tienen acceso a este producto, debido a que por seguridad, ellos son los únicos responsables de solicitar accesos para los diferentes usuarios. Una vez que estas solicitudes hayan sido efectuadas, estas serán gestionadas por uno o varios usuarios aprobadores, cuya función es la de autorizar o negar los accesos solicitados.

El proceso detallado anteriormente, es altamente recomendado por temas de seguridad, pero éste es posible modificarlo de acuerdo a las políticas de seguridad de cada organización.

Adicionalmente, este producto es útil por temas de auditoría, debido a que almacena logs de los procesos anteriormente mencionados.

- *Administración Delegada*

Esta herramienta presenta el servicio de administración delegada, que permite a los propios usuarios delegar tareas administrativas a una determinada persona, ya sea de manera fija o temporal, al momento de que el usuario necesite ausentarse de su puesto de trabajo. Esto da una continuidad a los procesos laborales de manera ininterrumpida.

- *Políticas de Acceso*

Permite la configuración de políticas de acceso a los sistemas informáticos, basándose en las políticas de seguridad de cada organización.
Se menciona algunas políticas importantes que soporta esta herramienta:

- *No Aprovisionamiento Seguro*

Permite la revocación inmediata de los accesos a los diferentes recursos organizacionales que posee un usuario, una vez que éste deja la organización en su totalidad.

- *Seguimiento de Solicitudes de Acceso en Tiempo Real*

  Permite al usuario administrador, dar un seguimiento en tiempo real del estado de cualquier solicitud efectuada, conociendo específicamente, información del usuario solicitante, el perfil de acceso solicitado, entre otros.

- *Gestión de Contraseñas mediante Autoservicio*

Característica que permite a los propios usuarios, gestionar sus contraseñas de acceso a los diferentes sistemas informáticos, sin ayuda de terceras personas; para lo cual, esta herramienta trabaja conjuntamente con el siguiente producto:

- *BMC Password Manager*

  Es un producto que tiene como objetivo:

  - Cambiar y sincronizar todas las contraseñas de acceso a los sistemas informáticos.

  - Cambiar las contraseñas de acceso, únicamente para determinados sistemas.

  - Habilitar aquellas cuentas de acceso que presentan un estado bloqueado.

  - Visualizar el estado de las cuentas de acceso a los sistemas, ya sean activas, bloqueadas o inactivas.

  Cabe mencionar que algunos usuarios por sus funciones laborales y por seguridad, no deben tener acceso a esta herramienta. Estos usuarios deben pedir soporte al personal de *helpdesk*.

- *Consola Administrativa*

Esta herramienta utiliza una consola administrativa, que permite al usuario administrador tener acceso a información privilegiada de los usuarios y de los sistemas integrados; es decir, a través de esta consola se puede visualizar información correspondiente a:

- Cuentas de acceso a los sistemas informáticos.

- Registro de las transacciones que corresponden a los procesos de: aprovisionamiento de las cuentas de acceso y cambios de contraseñas.

- Grupos de usuarios.

- Todos los sistemas integrados al sistema IDM.

- Información de los usuarios, como sus datos personales, dirección de correo electrónico, números telefónicos, entre otros.

- Perfiles de usuario.

3.3.3 Gestión de Accesos

BMC Software en lo referente a la gestión de accesos, tiene como objetivo el administrar adecuadamente los accesos a los distintos recursos organizacionales, basándose en la definición de políticas de seguridad.

Además, tiene como fin:

- Fortalecer el proceso de autenticación en el acceso a los diferentes recursos organizacionales.

- Permite un intercambio seguro de la información, entre la organización y entes externos (clientes, proveedores).

Para dichas funciones, BMC Software hace uso de las siguientes herramientas:

- *BMC Web Access Manager*

Este componente cumple la función de administrar y asegurar aquellas credenciales de acceso, que corresponden a los recursos organizacionales como a las aplicaciones web.

Además, esta herramienta controla y fortalece los privilegios de acceso que poseen los distintos usuarios, a través de la definición de políticas basadas en los roles organizacionales.

Cabe mencionar, que este producto también presenta un ***framework***[36], con el fin de utilizar la tecnología Single Sign On para proveer una mayor seguridad en el proceso de autenticación a los distintos recursos web.

- *BMC Identity Federation Manager*

Este componente hace uso de identidades federadas y atributos de acceso, con la finalidad de permitir a los usuarios a externos acceder a los diferentes recursos organizacionales, de una manera segura.

También permite que los propios usuarios de una organización, a través de la herramienta "*BMC Web Access Manager*", intercambien información de las identidades con otros sistemas externos de control de acceso.

[36] Plataforma desde la cual, un proyecto de software puede ser organizado y desarrollado.

3.3.4 Gestión de Auditoría

BMC Software en lo referente a este concepto, tiene como objetivo la implementación de estándares de auditoría para una organización, conjuntamente con la generación y vistas de reportes de cumplimiento.

Para dichas funciones, BMC Software hace uso de la siguiente herramienta:

- *BMC Identity Compliance Manager*

  Herramienta que permite la gestión de aquellos estándares de auditoría presentes en una organización, basándose en las regulaciones SOX.

  Adicionalmente, este producto presenta las siguientes funcionalidades:

  - Permite identificar y reportar posibles faltas a las políticas organizacionales establecidas.

  - Provee de ciertas vistas referentes a los estados de cumplimiento y rendimiento de las auditorías.

  - Provee de varios reportes de auditoría, que muestran información correspondiente al cumplimiento de las políticas establecidas.
  - Permite receptar notificaciones o alertas que corresponden a los procesos que utilizan *workflows*.

  Específicamente, esta herramienta presenta las siguientes características:

  - *Módulo de Cumplimiento*

    La herramienta presenta un módulo de cumplimiento, el cual se encarga de la implementación de las políticas de control. Además, permite al usuario administrador monitorear el cumplimiento de las auditorías establecidas.

Es necesario mencionar, ciertos ejemplos que se manejan en este módulo:

- Derechos de acceso: Se monitorea los permisos de acceso que poseen los grupos de usuarios, y así asociarlos directamente a cada uno de los usuarios existentes en el sistema IDM.

- Cambios de contraseña: Se monitorea el cumplimiento a las políticas de contraseñas de acceso establecidas.

- Cuentas huérfanas: Una cuenta huérfana es aquellas que no está conectada a ningún usuario. Si alguna cuenta de este tipo existe en el sistema IDM, este módulo se encarga de encontrarla y reportarla, previniendo de esta manera, posibles accesos no autorizados.

- *Módulo de Reportes*

También presenta un modulo de reportes, que permite realizar consultas específicas para obtener información con respecto a las auditorías.

Se cita algunos ejemplos que se manejan en este módulo:

- Actividad de usuarios: Lista los perfiles de usuario, cuentas de acceso a los sistemas y grupos de usuarios.

- Perfiles: Lista los derechos de acceso que poseen cada uno de los perfiles de usuario.

- Auditoría: Permite listar toda actividad de auditoría en un determinado rango de fechas. Un ejemplo, son las transacciones efectuadas al momento de crear, modificar o eliminar las cuentas de acceso a los sistemas.

4. ANÁLISIS DE SOLUCIONES ENFOCADAS A LA GESTIÓN DE IDENTIDADES

Para determinar si la solución expuesta a la gestión centralizada de accesos a los sistemas, mediante la implementación de un sistema de gestión de identidades IDM, es viable y beneficioso para una organización, en el presente capítulo se exponen tres importantes análisis: costo/beneficio, técnico y factibilidad de uso de la solución.

A continuación se detallan estos análisis, tomando como referencia información real y confiable, con la finalidad que los resultados obtenidos sean los esperados.

4.1 Análisis Costo/Beneficio

Para conocer si el sistema de gestión de identidades IDM, es factible financieramente, se presenta un completo análisis costo/beneficio de esta solución. Para obtener los mejores resultados, es necesario definir un escenario real de trabajo, el cual por motivos de infraestructura y de facilidad en la obtención de información, el escenario propuesto es el siguiente:

- **Lugar del escenario:** Empresa de telefonía móvil.
- **Número de empleados:** 2000 personas aproximadamente.
- **Número de sistemas implementados:** 15 sistemas.
- **Número de administradores por cada sistema:** 1 administrador.
- **Sistema de gestión de identidades IDM:** "*BMC Identity Management Suite*"- Versión 5.5, elaborado por la empresa "*BMC Software*".
- **Vida útil de un sistema implementado en esta empresa:** 3 años.

4.1.1 Análisis – Costo

El objetivo de este análisis, es determinar el costo total de la solución para implementar el sistema IDM "*BMC Identity Management Suite V5.5*", basándose en el escenario real de trabajo expuesto previamente. Para este fin, se consideran estos tres aspectos:

- *Costo de Implementación*

  - *Costo de Licenciamiento*

  = Costo de la licencia anual por usuario * Número de usuarios * Número de años de funcionamiento de la solución
  = $ 40 dólares * 2000 empleados * 3 años
  = ***$ 240.000 dólares por los 3 años de funcionamiento de la solución(A)***

  - *Costo de Instalación y Configuración*

  = ***$ 200.000 dólares (B)***

  Nota: *Este valor incluye el mantenimiento y soporte de hardware como software. También cubre la capacitación técnica para el primero año de funcionamiento de la herramienta, como también los costos por la integración de la solución con 5 sistemas.*

  - *Costo Adicional de Hardware e Infraestructura*

  Únicamente el costo de un nuevo servidor, en el cual se instale la solución.
  = ***$ 20.000 dólares (C)***

  - *Costo Adicional de Software*

  Costo por la adquisición de nuevos sistemas operativos y bases de datos.
  = $ 15.000 dólares (D)

- *Costo Adicional de Integración*

= Costo por el desarrollo de integración que requiere cada sistema * (Número total de sistemas a integrar – Número de sistemas ya integrados en el proceso de instalación y configuración de la solución)
= $ 7.000 dólares * (15 sistemas – 5 sistemas)
= $ 7.000 dólares * 10 sistemas
= $ 70.000 dólares (E)

Costo Total de Implementación = *A + B + C + D + E*
= $ 240.000 dólares + $ 200.000 dólares + $ 20.000 dólares + $ 15.000 dólares + $ 70.000 dólares
= $ 545.000 dólares por los 3 años de funcionamiento de la solución (CTI)

- *Costo Administrativo*

  - *Costo de Actualización y Mantenimiento de Hardware e Infraestructura*

= $ 4.000 dólares anuales * 2 años restantes del funcionamiento de la solución
= $ 8.000 dólares por los 2 años restantes del funcionamiento de la solución (F)

Nota: *El costo para el primer año de funcionamiento de la solución, se lo cubre en el valor (C) dedicado a la compra de hardware adicional.*

- *Costos de Actualización y Soporte de Software*

= $ 40.000 dólares anuales * 2 años restantes del funcionamiento de la solución

= ***$ 80.000 dólares por los 2 años restantes del funcionamiento de la solución (G)***

Nota: *El costo para el primer año de funcionamiento de la solución, se lo cubre en el valor (B) dedicado a la instalación y configuración de la herramienta.*

- *Costo de Recurso Humano (Administradores)*

= Salario anual de un administrador * Número de administradores del sistema IDM * Número de años de funcionamiento de la solución

= $ 14.400 dólares * 1 administrador * 3 años de funcionamiento de la solución

= ***$ 43.200 dólares por los 3 años de funcionamiento de la solución (H)***

Costo Total Administrativo = *F + G + H*

= $ 8.000 dólares + $ 80.000 dólares + $ 43.200 dólares

= $ 131.200 dólares por los 3 años de funcionamiento de la solución (CTA)

- *Costo de Capacitación*

  - *Costo Técnico*

= Costo/hora de la capacitación técnica * Número de horas de la capacitación * Número de usuarios técnicos * Número de años de funcionamiento de la solución

= $ 100 dólares * 15 horas * 6 usuarios técnicos * 2 años

= ***$ 18.000 dólares por los 2 últimos años de funcionamiento de la solución (I)***

Nota: *El costo para el primer año de funcionamiento de la solución, se lo cubre en el valor (B) dedicado a la instalación y configuración de la herramienta.*

- *Costo Usuario*

Este costo no es valorado, debido a que la capacitación para los usuarios del sistema IDM, es una responsabilidad tanto del administrador del sistema como de los usuarios técnicos.

Costo Total de Capacitación = *I*
= $ 18.000 dólares por los 2 últimos años de funcionamiento de la solución (CTC)

COSTO TOTAL DE LA SOLUCIÓN = CTI + CTA + CTC
= $ 545.000 dólares + $ 131.200 dólares + $ 18.000 dólares
= $ 694.200 dólares por los 3 años de funcionamiento de la solución (CTS)

4.1.2 Análisis – Beneficio

Para el presente análisis, es importante tomar en cuenta dos aspectos: Por un lado, exponer los beneficios que ofrece la implementación de un sistema de gestión de identidades IDM y por el otro, detectar aquellos procesos existentes en la organización como también los costos que éstos representan, debido a la falta de implementación de un procedimiento automático y centralizado para la gestión de accesos.

Los beneficios que ofrece la implementación de un sistema IDM, son los siguientes:

- *Automatización de Procesos Manuales*

Para este beneficio, se consideran dos procesos:

- *Aprovisionamiento/No Aprovisionamiento Manual de Cuentas de Acceso*

  Para obtener el costo que representa este proceso a la organización, se debe tomar en cuenta lo siguiente:

  - *Número de transacciones efectuadas al mes*

  = (Número de solicitudes mensuales de creación de cuentas por cada sistema + Número de solicitudes mensuales de modificación de cuentas por cada sistema + Número de solicitudes mensuales de eliminación de cuentas por cada sistema) * Número de sistemas implementados en la organización
  = (70 solicitudes + 40 solicitudes + 30 solicitudes) * 15 sistemas
  = ***2.100 transacciones mensuales***

  - *Tiempo que requiere un usuario administrador para efectuar una sola transacción*

  = ***20 minutos aproximadamente***

  - *Costo que representa el efectuar una sola transacción por parte del usuario administrador*

  = Tiempo que requiere un usuario administrador para efectuar una sola transacción * Salario mensual del administrador / Tiempo mensual en minutos correspondiente al trabajo de un administrador
  = 20 minutos * $ 1.200 dólares / 44.640 minutos
  = ***$ 0.54 centavos de dólar***

Costo por el proceso de aprovisionamiento/no aprovisionamiento manual de cuentas de acceso

= Número de transacciones efectuadas al mes * Costo que representa el efectuar una sola transacción por parte del usuario administrador

= 2.100 transacciones mensuales * $ 0.54 centavos de dólar * 12 meses

= $ 13.608 dólares anuales (A)

- *Cambio Manual de Contraseñas de Acceso*

Para obtener el costo que representa este proceso a la empresa, se toma en cuenta lo siguiente:

- *Número de transacciones efectuadas al mes*

= Número de solicitudes mensuales de cambio de contraseña por cada sistema * Número de sistemas implementados en la organización

= 200 solicitudes * 15 sistemas

= ***3.000 transacciones mensuales***

- *Tiempo que requiere un usuario administrador para efectuar una sola transacción*

= ***20 minutos aproximadamente***

- *Costo que representa el efectuar una sola transacción por parte del usuario administrador*

= Tiempo que requiere un usuario administrador para efectuar una sola transacción * Salario mensual del administrador / Tiempo mensual en minutos correspondiente al trabajo de un administrador

= 20 minutos * $ 1.200 dólares / 44.640 minutos

= ***$ 0.54 centavos de dólar***

Costo por el proceso de cambio manual de contraseñas de acceso
= Número de transacciones efectuadas al mes * Costo que representa el efectuar una sola transacción por parte del usuario administrador
= 3.000 transacciones mensuales * $ 0.54 centavos de dólar * 12 meses
= ***$ 19.440 dólares anuales (B)***

- *Minimizar Fallas Humanas*

Este beneficio se lo obtiene a través de la automatización de procesos manuales, detallado en el punto anterior.

- *Reducción de Llamadas a Helpdesk*

Para determinar el costo que representa la atención de llamadas en el tema de gestión de usuarios, por parte del personal *helpdesk*, se debe considerar:

= Número de llamadas atendidas mensualmente por el personal de *helpdesk* en el tema de gestión de usuarios * Costo por cada llamada atendida
= 2.000 llamadas aproximadamente * $ 0.8 centavos de dólar * 12 meses
= $ 19.200 dólares anuales (C)

- *Optimización del Tiempo Laboral*

El presente beneficio contiene dos aspectos a tomar en cuenta:

  - *Tiempo laboral perdido en el cambio manual de contraseñas de acceso a los sistemas*

    Para obtener el costo que representa este proceso a la empresa, se detalla lo siguiente:

- *Tiempo que requieren los usuarios para cambiar manualmente sus contraseñas de acceso a los sistemas*

= Tiempo que requiere un usuario para cambiar la contraseña de acceso a un sistema * Número total de empleados * Número de sistemas implementados en la organización
= 35 minutos en promedio * 2.000 empleados * 15 sistemas
= ***1´050.000 minutos que corresponde a 17.500 horas***

Costo que representa que los empleados dediquen su tiempo laboral en el cambio manual de las contraseñas de acceso a los sistemas

= Tiempo que requieren los usuarios para cambiar manualmente sus contraseñas de acceso a los sistemas * Salario mensual promedio de un empleado / Tiempo mensual en horas correspondiente al trabajo de un empleado
= 17.500 horas * $ 900 dólares / 744 horas
= $ 21.169 dólares mensuales * 12 meses
= $ 254.028 dólares anuales (D)

- *Tiempo laboral perdido en el proceso de autenticación a los sistemas informáticos*

Con el fin de conocer el costo que representa este proceso a la empresa, se debe tomar en cuenta lo siguiente:

- *Tiempo que requieren los usuarios para autenticarse a los sistemas informáticos*

= Tiempo que requiere un usuario al día para autenticarse contra un mismo sistema * Número total de empleados * Número de sistemas implementadas en la organización * Número de días laborables al mes
= 30 segundos en promedio * 2.000 empleados * 15 sistemas * 23 días

= ***20´700.000 segundos mensuales que corresponde a 5.750 horas***

Costo que representa que los empleados dediquen su tiempo laboral en el proceso de autenticación a los sistemas informáticos

= Tiempo que requieren los usuarios para autenticarse a los sistemas informáticos * Salario mensual promedio de un empleado / Tiempo mensual en horas correspondiente al trabajo de un empleado

= 5.750 horas mensuales * $ 900 dólares / 744 horas

= $ 6.956 dólares mensuales * 12 meses

= $ 83.472 dólares anuales (E)

- *Minimizar Costos Operacionales*

Para este beneficio, se debe considerar el siguiente aspecto:

- *Depuración Manual de Cuentas de Acceso*

Para determinar el costo que representa este proceso a la organización, se debe tomar en cuenta lo siguiente:

- *Número de depuraciones de cuentas de acceso efectuadas al mes*

= Número de depuraciones de cuentas de acceso por cada sistema * Número de sistemas implementados en la organización

= 1.000 cuentas de acceso depuradas * 15 sistemas

= ***15.000 cuentas de acceso depuradas al mes***

- *Tiempo que requiere un usuario administrador para efectuar la depuración de una sola cuenta de acceso*

= 1 minuto aproximadamente

- *Costo que representa la depuración de una sola cuenta de acceso por parte del usuario administrador*

= Tiempo que requiere un usuario administrador para efectuar la depuración de una sola cuenta de acceso * Salario mensual del administrador / Tiempo mensual en minutos correspondiente al trabajo de un administrador
= 1 minuto * $ 1.200 dólares / 44.640 minutos
= ***$ 0.03 centavo de dólar***

Costo que representa el proceso de la depuración manual de las cuentas de acceso

= Número de depuraciones de cuentas de acceso efectuadas al mes * Costo que representa la depuración de una sola cuenta de acceso por parte del usuario administrador * 12 meses
= 15.000 cuentas de acceso depuradas * 0.03 centavos de dólar * 12 meses
= ***$ 5.400 dólares anuales (F)***

- *Maximizar la Seguridad de la Información*

Con el fin de maximizar la seguridad de la información dentro de la organización, es importante incrementar el control de accesos a los diferentes sistemas informáticos.

El no mantener un control en este aspecto, deriva en una gran cantidad de ingresos no autorizados a los sistemas, lo cual provoca inmensas pérdidas económicas para la organización.

El costo por no implementar un control en este proceso, asciende alrededor de unos ***$ 500.000 dólares anuales (G)***, debido al tema de fraudes por suscripción, los cuales son provocados por usurpación de identidades.

BENEFICIO TOTAL DE LA SOLUCIÓN = *A + B + C + D + E + F + G*

= $ 13.608 dólares + $ 19.440 dólares + $ 19.200 dólares + $ 254.028 dólares + $ 83.472 dólares + $ 5.400 dólares + $ 500.000 dólares

= $ 895.148 dólares anuales * 3 años de funcionamiento de la solución

= $ 2´685.444 dólares en los 3 años de funcionamiento de la solución (BTS)

4.1.3 Resumen Financiero Del Análisis Costo/Beneficio

Es importante efectuar un resumen financiero, en el cual se muestre detalladamente todos los costos que fueron tomados en cuenta para el presente análisis. Para esta representación, se hace uso del siguiente flujo de caja:

FLUJO DE CAJA PROYECTADO (EN DÓLARES AMERICANOS)				
	AÑO 0	**AÑO 1**	**AÑO 2**	**TOTAL**
BENEFICIOS DE LA SOLUCIÓN				
Automatización de Procesos Manuales Minimizar Fallas Humanas				
• Aprovisionamiento/no aprovisionamiento manual de cuentas de acceso	$ 13.608	$ 13.608	$ 13.608	**$ 40.824**
• Cambio manual de contraseñas de acceso	$ 19.440	$ 19.440	$ 19.440	**$ 58.320**
Reducción de Llamadas Helpdesk				
• Atención de llamadas en lo referente a la gestión de usuarios	$ 19.200	$ 19.200	$ 19.200	**$ 57.600**
Optimización del Tiempo Laboral				
• Tiempo laboral perdido en el cambio de contraseñas de acceso a los sistemas	$ 254.028	$ 254.028	$ 254.028	**$ 762.084**
• Tiempo laboral perdido en el proceso de autenticación a los sistemas	$ 83.472	$ 83.472	$ 83.472	**$ 250.416**
Minimizar Costos Operacionales				
• Depuración manual de cuentas de acceso	$ 5.400	$ 5.400	$ 5.400	**$ 16.200**
Maximizar la Seguridad de la Información				
• Fraudes por suscripción	$ 500.000	$ 500.000	$ 500.000	**$ 1´500.000**
COSTO TOTAL DE LOS BENEFICIOS DE LA SOLUCIÓN (BTS)	$ 895.148 dólares	$ 895.148 dólares	$ 895.148 dólares	**$ 2´685.444 dólares**

Cuadro 2 - 04 – Flujo de Caja correspondiente a los Beneficios de la Solución [Z]

FLUJO DE CAJA PROYECTADO (EN DÓLARES AMERICANOS)				
	AÑO 0	**AÑO 1**	**AÑO 2**	**TOTAL**
COSTOS DE LA SOLUCIÓN				
Costo de Implementación				
• Costo de Licenciamiento	$ 80.000	$ 80.000	$ 80.000	**$ 240.000**
• Costo de instalación y configuración	$ 200.000			**$ 200.000**
• Costo adicional de hardware e infraestructura	$ 20.000			**$ 20.000**
• Costo adicional de software	$ 15.000			**$ 15.000**
• Costos de integración adicionales	$ 70.000			**$ 70.000**
Costo Administrativo				
• Costo de actualización y mantenimiento del hardware e infraestructura		$ 4.000	$ 4.000	**$ 8.000**
• Costos de actualización y soporte del software		$ 40.000	$ 40.000	**$ 80.000**
• Costos del Recurso Humano	$ 14.400	$ 14.400	$ 14.400	**$ 43.200**
Costo de Capacitación				
• Costo Técnico		$ 9.000	$ 9.000	**$ 18.000**
COSTO TOTAL DE LA SOLUCIÓN (CTS)	$ 399.400 dólares	$ 147.400 dólares	$ 147.400 dólares	**$ 694.200 dólares**

Cuadro 2 - 04 – Flujo de Caja correspondiente a los Costos de la Solución **[1]**

4.1.4 Resultado del Análisis Costo/Beneficio

Efectuado ambos análisis, ahora es posible determinar si el sistema de gestión de identidades IDM, es beneficioso o no para la organización; para lo cual, se elabora el siguiente cuadro donde se muestra los costos obtenidos de cada uno de los análisis realizados previamente.

COSTO TOTAL DE LA SOLUCIÓN (CTS)	BENEFICIO TOTAL DE LA SOLUCIÓN (BTS)	ANÁLISIS DE VIABILIDAD	RESULTADO
$ 694.200 dólares	$ 2´685.444 dólares	CTS < BTS	**La solución es VIABLE**

Cuadro 3 - 04 - Análisis Costo/Beneficio de la Solución **[2]**

El cuadro nos muestra que la solución planteada es totalmente viable para la organización, debido a que el costo total que se requiere para la implementación del sistema de gestión de identidades IDM (CTS), es menor frente al costo (BTS) que representa la falta de implementación de un proceso automático y centralizado para la gestión de accesos a los sistemas informáticos.

4.2 Análisis Técnico

Con el fin de determinar cuál de las tres soluciones estudiadas en el capítulo anterior, es la más apta tecnológicamente y funcionalmente, se presenta un análisis comparativo entre los componentes que poseen cada una de éstas; y de esta manera, concluir objetivamente qué herramienta cubre los requerimientos que exige un sistema de gestión de identidades IDM para su óptimo accionar.

Previo al análisis comparativo, es importante mostrar cuáles son los diferentes componentes que presentan las tres soluciones, diferenciándolas por cada una de las áreas funcionales que ofrece un sistema de gestión de identidades IDM.

A continuación, se muestra una tabla con esta información:

COMPONENTES DE LAS SOLUCIONES				
ÁREAS FUNCIONALES		SOLUCIONES		
		ORACLE	**SUN MICROSYSTEMS**	**BMC SOFTWARE**
	SERVICIO DE DIRECTORIO	• Oracle Internet Directory	• Sun Directory Enterprise Edition	• BMC Control SA/Directory Manager
	GESTIÓN DE IDENTIDADES	• Oracle Identity Manager • Oracle Role Manager	• Sun Identity Manager • Sun Role Manager	• BMC User Administration Manager
	GESTIÓN DE ACCESOS	• Oracle Access Manager • Oracle Entitlements Server • Oracle Identity Federation • Oracle Enterprise Single Sign-On • Oracle Authentication Services para Sistemas Operativos	• Sun Single Sign On Enterprise	• BMC Web Access Manager • BMC Identity Federation Manager
	GESTIÓN DE AUDITORÍA	• Oracle Internet Directory • Oracle Access Manager	• Sun Identity Compliance Manager	• BMC Identity Compliance Manager

Cuadro 4 - 04 – Componentes de las Soluciones **[3]**

Una vez elaborado este cuadro, se puede determinar:

- Las tres soluciones cubren cada una de las áreas funcionales, con al menos un componente.

- La herramienta Oracle cuenta con un mayor número de componentes enfocados a la gestión de accesos, en comparación con las demás soluciones.

Elaborado el resumen de los diferentes componentes que presentan las soluciones a ser estudiadas, se muestra el respectivo análisis comparativo mencionado en un principio. Cabe indicar, que este análisis presenta un enfoque desde el punto de vista en seguridad informática, debido a que el sistema de gestión de identidades IDM tiene como objetivo proporcionar una alta seguridad en el manejo de la información de las identidades.

Para este análisis, es necesario detallar las distintas características que presentan cada uno de los componentes de las soluciones, para lo cual se muestra la siguiente tabla:

CARACTERÍSTICAS DE LOS COMPONENTES			
	SOLUCIONES		
	ORACLE	SUN MICROSYSTEMS	BMC SOFTWARE
SERVICIOS DE DIRECTORIO	• Compuesto por un directorio LDAP. • Almacena múltiple información, la cual es administrada a través de un sólo repositorio central. • Permite la sincronización de datos de este repositorio central con los demás repositorios. • Presenta encriptación y respaldo de datos. • Permite la integración con "*Microsoft Active Directory"* • Presenta una consola de administración, que permite monitorear y manejar la información almacenada en este repositorio. • Integración con sistemas operativos Unix y Linux.	• Permite el almacenamiento y administración de las identidades, como también los privilegios de acceso a los sistemas, de una manera centralizada. • Permite la sincronización de información con "*Microsoft Active Directory*" • Presenta la característica de compresión de información, con el fin de ahorrar espacio de almacenamiento en el repositorio central. • Presenta una determinada consola de administración.	• Presenta un repositorio centralizado de datos, el cual administra aquella información relacionada a los usuarios y a las aplicaciones. • Este repositorio se conecta a los distintos repositorios, a través del protocolo LDAP. • Provee de vistas con información relacionada a los perfiles de usuario y los derechos de acceso a los sistemas. • Presenta una consola de administración, la cual muestra información correspondiente a los sistemas, los usuarios, sus respectivos roles organizacionales y sus derechos de acceso a los sistemas.

Cuadro 5 - 04 – Características de los Componentes en cuanto los Servicios de Directorio **[4]**

CARACTERÍSTICAS DE LOS COMPONENTES			
	SOLUCIONES		
	ORACLE	SUN MICROSYSTEMS	BMC SOFTWARE
GESTIÓN DE IDENTIDADES	• Administra el ciclo de vida de las cuentas de usuario, como también sus respectivos privilegios de acceso. • Administra el ciclo de vida de los roles empresariales. • Se encarga del proceso de aprovisionamiento/desprovisionamiento de las cuentas de acceso a los sistemas. • Presenta la característica de autoservicio, permitiendo a los propios usuarios, gestionar sus contraseñas de acceso a los sistemas. • Presenta la característica de administración delegada, que incluye la delegación de roles empresariales • Permite definir políticas de acceso a los diferentes sistemas, basándose en los roles empresariales de los usuarios. • Presenta *workflows* tanto de aprovisionamiento como de aprobación de solicitudes de acceso a sistemas. • Presenta características de manejo de errores, operaciones de rollback y recuperación, en caso de posibles fallos en el proceso de aprovisionamiento.	• Se encarga de la administración del ciclo de vida de las identidades. • Efectúa el proceso de aprovisionamiento/desprovisionamiento de cuentas de acceso a los sistemas. • Permite una administración del ciclo de vida de los roles empresariales. • Hace uso de los roles empresariales, con el fin de otorgar derechos de acceso a los sistemas. • Para el proceso de aprovisionamiento de cuentas de acceso, presenta la funcionalidad de los *workflows*. • Presenta un proceso de aprovisionamiento de cuentas de acceso externas a la organización. (proveedores, clientes)	• Administra el ciclo de vida de las cuenta de usuario. • Permite el proceso de aprovisionamiento/desprovisionamiento de las cuentas de acceso a los sistemas. • Hace uso del accionar de los *workflows*, para el proceso de aprovisionamiento/desprovisionamiento de cuentas de acceso a los sistemas. • Presenta la característica de administración delegada. • Permite definir políticas de acceso a los sistemas, tomando como referencia las políticas de seguridad de la organización. • Permite el seguimiento en tiempo real, de las respectivas solicitudes de acceso a los sistemas. • Presenta la característica de autoservicio de usuario.

Cuadro 6 - 04 – Características de los Componentes en cuanto a la Gestión de Identidades **[5]**

CARACTERÍSTICAS DE LOS COMPONENTES			
	SOLUCIONES		
	ORACLE	SUN MICROSYSTEMS	BMC SOFTWARE
GESTIÓN DE ACCESOS	• Provee una autenticación centralizada, tomando en cuenta autorizaciones y auditoría. • Provee de varios métodos seguros de autenticación. • Permite la definición de políticas de autorización y de acceso a los sistemas. • Las políticas pueden ser aplicadas específicamente a usuarios, grupos o roles empresariales. • Permite la asignación de usuarios a un determinado grupo, de una manera dinámica. • Posee un ambiente de pruebas para la definición de políticas de acceso y autorización. • Brinda seguridad al intercambiar información de las identidades, entre la organización y los distintos entes externos. • Presenta el proceso de autenticación Single Sign On. • Permite la autenticación y administración centralizada de cuentas para las plataformas Unix y Linux.	• Administra los accesos correspondientes a los servicios y aplicaciones web. • Para fortalecer el proceso de autenticación, presenta la tecnología Single Sign On. • Permite la configuración de políticas de acceso a los sistemas, con el fin de aumentar la seguridad. • Permite compartir las identidades de usuario, entre la organización y sus entes externas, de una forma segura. • Presenta la posibilidad de usar tokens de seguridad, como método alternativo de autenticación.	• Permite administrar las respectivas credenciales de acceso a los sistemas. • Permite la definición de políticas basadas en los roles empresariales, con el fin de asegurar los privilegios de acceso a los sistemas. • Proporciona seguridad en el acceso a los recursos empresariales, en caso que cualquier usuario externo lo requiera. • Presenta el proceso de autenticación Single Sign On.

Cuadro 7 - 04 – Características de los Componentes en cuanto a la Gestión de Accesos **[6]**

CARACTERÍSTICAS DE LOS COMPONENTES			
	SOLUCIONES		
	ORACLE	SUN MICROSYSTEMS	BMC SOFTWARE
GESTIÓN DE AUDITORÍA	• Permite la configuración de reportes de auditoría. • Permite el control y monitoreo de las cuentas de acceso a los sistemas: o Detecta, notifica y actúa al producirse cambios no autorizados, en los privilegios de acceso de las cuentas de usuario. o Identifica y actúa al encontrar cuentas huérfanas. • Presentación de reportes que muestran información histórica del proceso de aprovisionamiento de las cuentas de usuario. • Presentación de reportes que muestran información relacionada a los perfiles de usuario, grupos de usuario y accesos que posee un usuario. • Registro de: o Accesos satisfactorios/ fallidos a los sistemas. o Estados de usuario, incluyendo la desactivación temporal y reactivación. o Cambios de contraseñas. • Provee de *logs* detallados con respecto a los accesos a los sistemas; conociendo el usuario, fecha de ingreso, IP de la máquina, otros.	• Presenta una colección de información relacionada con los usuarios, las aplicaciones, como también de los accesos a los sistemas. • Hace uso de reportes y vistas, con el fin de mostrar la información mencionada anteriormente. • Presenta la posibilidad de configurar y calendarizar los respectivos reportes de auditoría.	• Permite identificar posibles faltas a las políticas establecidas. • Permite la definición de políticas de control. • Provee el monitoreo y cumplimiento de las políticas establecidas; en el caso de controlar los derechos de acceso, cambios de contraseña, cuentas huérfanas, entre otros. • Permite la configuración de los reportes de auditoría. • Presenta un módulo de reportes, que permite obtener información relacionada a la actividad de los usuarios, perfiles de acceso, transacciones, entre otros.

Cuadro 8 - 04 – Características de los Componentes en cuanto a la Gestión de Auditoría **[7]**

En base a mi experiencia en el manejo de un Sistema de Gestión de Identidades, y tomando en cuenta las funcionalidades que presenta cada uno de los componentes de las tres herramientas, se puede determinar lo siguiente:

4.2.1 Análisis correspondiente a los Servicios de Directorio

En cuanto al análisis de los Servicios de Directorio, se determina que la solución "*Oracle Identity Management*", pese a que las tres herramientas cuentan con características similares, proporciona funcionalidades más relevantes en relación a las demás, tal cual se detalla a continuación:

- Es importante que la solución presente un modo de encriptación de datos, debido a que por temas de seguridad informática, este proceso permite que la información sensible de las identidades, se almacene de una forma segura y confiable, evitando de esta manera que personas no autorizadas tengan acceso a la misma.

- De igual manera, es indispensable la presencia de un proceso que permita el respaldo seguro de la información almacenada en el repositorio central de datos, con el fin de evitar que ésta desaparezca.

- Debido también, a que la solución permite la administración de cuentas de acceso a los sistemas operativos Unix y Linux, ya que en la actualidad, la gran mayoría de organizaciones hacen uso de este tipo de sistemas, por la seguridad y rendimiento que ofrecen.

4.2.2 Análisis - Gestión de Identidades

En lo referente a este análisis, se determina de igual manera, que la herramienta "*Oracle Identity Management*" presenta mayores beneficios para una adecuada administración de las identidades, por los siguientes motivos:

- Esta solución permite la definición de políticas de acceso a los diferentes sistemas, basándose en los respectivos roles organizacionales, lo cual brinda una

mayor seguridad en este aspecto, evitando posibles accesos no autorizados y por ende el robo de información sensible para la organización.

- Una de las características más importantes desde el punto de vista de seguridad informática, es la de presentar las opciones de rollback y recuperación de información, al momento de presentarse algún tipo de error en el proceso de aprovisionamiento/no aprovisionamiento de cuentas de acceso a los sistemas, a través del uso de *workflows*; permitiendo de esta manera, que las transacciones efectuadas cumplan con la propiedad de integridad.

- De igual manera, la herramienta permite el manejo de errores o excepciones, al momento de presentarse fallas en el proceso normal de aprovisionamiento/ no aprovisionamiento de cuentas de acceso a los distintos sistemas, a través del uso de *workflows*; permitiendo así, que todas las transacciones realizadas durante este proceso, se efectúen completamente.

- En lo referente a la característica de administración delegada, tanto Oracle como BMC Software hacen uso de esta funcionalidad, con la diferencia que el primero presenta una característica adicional, la cual permite al propio usuario el delegar su rol organizacional, es decir sus privilegios de acceso a otro usuario. Esto ayuda a brindar una mayor continuidad en los procesos organizacionales.

4.2.3 Análisis - Gestión de Accesos

De la misma manera, se determina que la herramienta "*Oracle Identity Management*", provee de grandes beneficios para lograr una óptima gestión de los accesos a los diferentes sistemas informáticos. Los siguientes aspectos, explican lo dicho:

- Fortalece el proceso de autenticación a los distintos sistemas informáticos, a través del uso de varios métodos seguros, tales como: certificados, tokens de seguridad o tarjetas inteligentes; lo cual brinda una mayor seguridad en el acceso a los diferentes sistemas y al mismo tiempo, reduciendo al máximo posibles accesos no autorizados.

- Las tres soluciones permiten la definición de políticas de acceso, con el fin de incrementar la seguridad en el acceso a los sistemas informáticos, pero Oracle presenta una funcionalidad adicional e importante, la cual consiste en definir políticas de acceso aplicadas especialmente a un determinado usuario, a un grupo, o a un rol organizacional en especial, lo que permite una mayor restricción en el acceso a los sistemas, aumentando por ende, la seguridad en este aspecto.

- Además, esta herramienta, a través de su consola de administración, ofrece la oportunidad de efectuar pruebas de funcionamiento, haciendo uso de las respectivas políticas de acceso, lo cual ayuda al administrador del sistema, a estudiar detenidamente el funcionamiento y el impacto que tiene la implementación de dichas políticas en un ambiente real.

- A diferencia de las demás herramientas, Oracle permite una autenticación centralizada de las cuentas de acceso, tanto al Sistema Operativo Unix como a Linux, lo cual es realmente indispensable en el actualidad, por el hecho que la mayoría de las organizaciones hacen uso de este tipo de Sistemas Operativos, por su gran rendimiento y seguridad, por lo que se vuelve necesario la administración de las respectivas credenciales de acceso a estos sistemas.

4.2.4 Análisis - Gestión de Auditoría

En cuanto a este análisis, se determina que la herramienta "*Oracle Identity Management*", presenta una mejor gestión de la información de auditoría, por proveer una serie de importantes características, como se detalla a continuación:

- Una funcionalidad importante que muestra Oracle en relación a las otras soluciones, consiste en detectar, notificar y actuar al producirse cambios no autorizados en los privilegios de acceso a los sistemas; esto no solo permite comunicar al usuario administrador, sino que también a través de la definición de políticas, se pueden tomar acciones inmediatas para contrarrestar estas anormalidades, sin la intervención humana; es decir, el proceso es automático y seguro.

- De igual manera, en concordancia con el punto anterior, la herramienta también permite detectar, notificar y actuar al presentarse posibles cuentas huérfanas, lo cual es realmente indispensable desde el punto de vista de seguridad informática, debido a que el no llevar un control adecuado en este aspecto, puede provocar accesos no autorizados a los diferentes sistemas, y por ende grandes fraudes para la organización.

- En cuanto al tema de logs o registros de auditoría, Oracle también sobresale de los demás, debido a que esta herramienta permite el registro de los siguientes actividades:

    - ✓ Registra todos los accesos, ya sean satisfactorios o fallidos, al momento que los usuarios intentan acceder a los distintos sistemas informáticos.

    - ✓ Además, permite el registro de los estados de disponibilidad que poseen los usuarios, ya sea: activo, eliminado, revocado, e inclusive desactivación temporal y reactivación.

    - ✓ Y por último, el registro de todos aquellos cambios de contraseñas de acceso, efectuados por un determinado usuario para el acceso a los diferentes sistemas.

4.3 Análisis de Factibilidad de Uso de la Solución

El presente análisis de factibilidad de uso de la solución, comprende dos aspectos a tomar en cuenta: el impacto de la herramienta sobre los usuarios, entendiéndose por éstos, a usuarios administradores como usuarios finales; y también el impacto sobre los procesos de la organización.

Para este objetivo, es necesario contar con información real y confiable acerca del uso e impacto que el sistema de gestión de identidades IDM presenta en una organización, para lo cual, se efectúa un trabajo de campo en una prestigiosa empresa de telefonía móvil presente en nuestro país.

En esta empresa se encuentra implementado el sistema de gestión de identidades "*BMC Identity Management Suite Versión 5.5*" desarrollado por la organización "*BMC Software*", desde hace ya dos años. Para recabar información, se procedió a entrevistar a tres ejecutivos de esta empresa, de las cuales dos personas fueron administradores del sistema en su momento, y la otra corresponde al administrador actual del sistema.

4.3.1 Impacto de la Solución sobre los Usuarios

Para analizar la factibilidad de uso de la herramienta en este tema, se toma en cuenta los siguientes seis aspectos:

- *Complejidad del Sistema*

En cuanto a la complejidad del uso de la solución, los respectivos administradores concuerdan que el sistema en sí, es complejo por los siguientes aspectos:

- La persona que administre el sistema, deberá poseer una alta experiencia en lo referente a la administración de sistemas robustos y grandes.

- Es indispensable que el respectivo administrador del sistema, posea altos conocimientos técnicos, en cuanto a: lenguaje de programación Java, administración de una base de datos Oracle, administración de Sistemas Operativos, como también conocer el funcionamiento de una conexión LDAP; debido a que estos son conocimiento necesarios que permiten una adecuada administración del sistema, como también el entender su funcionamiento.

- Además, es necesario que el usuario administrador cuente con al menos tres personas para su apoyo en la administración del sistema, debido a que esta labor requiere de tiempo. Estas personas también deberán poseer los mismos conocimientos mencionados en el punto anterior.

- El proceso de integración de una nueva aplicación al sistema de gestión de identidades IDM, es complejo, debido a que en este proceso se requiere conocer el funcionamiento de los componentes del sistema como tal, por ejemplo módulos de aprovisionamiento, *gateways*, agentes de conexión, entre otros.

- La definición de políticas de acceso a los diferentes sistemas administrados, también es una tarea compleja, debido a que es necesario determinar el impacto que causará la implementación de dichas políticas en la organización, como también efectuar pruebas de funcionamiento de las mismas, antes de ponerlas en un ambiente real.

- En cuanto a la configuración de nuevos reportes de auditoría, es una tarea que requiere de tiempo, debido a que no es una actividad fácil de efectuarla. Se requiere de ayuda por parte del proveedor de la solución, los cuales deberán efectuar un sin número de pruebas de funcionamiento, antes de implementar en el ambiente real.

- *Técnica de Trabajo*

En lo referente a la técnica de trabajo utilizada por los administradores del sistema, concuerdan que es necesario contar con una previa y adecuada capacitación en el uso de la herramienta, por parte del proveedor especializado; debido a que la consola administrativa del sistema, ofrece un sin número de opciones de configuración, además toda la información de las identidades se encuentra organizada por ***entidades***[37], lo cual hace indispensable conocer a profundidad las funcionalidades que ofrece esta consola.

Cabe mencionar que además de lo expuesto anteriormente, los administradores del sistema han aprendido a manejar la consola administrativa, a través de la ayuda de manuales de usuario, que deben ser exigidos al respectivo proveedor.

[37] Una entidad es la representación de un objeto o concepto del mundo real, que se describe en una base de datos.

- *Adaptación al Sistema*

En cuanto a la adaptación al sistema, los administradores concuerdan que no existe ningún inconveniente en este aspecto, siempre y cuando la persona encargada de administrar el sistema posea:

- El perfil adecuado; es decir, conocimientos en programación Java, administración de una base de datos Oracle, como también administración de Sistemas Operativos.

- Una capacitación adecuada en el uso de la herramienta, por parte del proveedor especializado.

- Un soporte personalizado por parte del proveedor, para cubrir cualquier duda o inquietud que se presente.

- Un apoyo de al menos tres personas, con conocimientos en el tema.

- *Resistencia al Sistema*

En este punto, es necesario tomar en cuenta dos aspectos:

  - *Administrador del Sistema*

  Según la experiencia de los usuarios administradores entrevistados, en la fase de implementación de la solución existe una cierta resistencia a la herramienta, debido a que en esta etapa, no existe aún una adecuada capacitación en el tema por parte del proveedor de la solución y los respectivos manuales de usuario no proporcionan toda la información requerida, lo cual complica la administración del sistema en los primeros meses de implementación.

- *Usuarios*

  De igual manera, en los primeros meses de funcionamiento de la solución, existe por lo general una cierta resistencia por parte de los usuarios, debido a un desconocimiento en cuanto al funcionamiento de la herramienta, el ingreso al sistema, los beneficios de la solución, entre otros aspectos.

- *Interfaz de Usuario del Sistema*

En lo referente a la interfaz de usuario que presenta la solución, los administradores concuerdan que la interfaz de usuario correspondiente a la consola administrativa, es compleja de manejarla y poco amigable al usuario.

De igual manera, la interfaz del sistema hacia los usuarios finales, es poco amigable hasta confusa en ciertos aspectos, lo que provoca que éstos busquen ayuda al servicio de *helpdesk*, como también quejas por este motivo.

- *Limitaciones del Sistema*

Según la experiencia de los administradores de la solución, mencionan que el sistema presenta ciertas limitaciones en cuanto al funcionamiento de la herramienta como tal, lo que provoca una ineficiente administración del sistema.

Algunas de estas limitaciones, se citan a continuación:

- La solución no presenta un sistema de alarmas, al momento de suscitarse alguna actividad anormal en el funcionamiento de la herramienta.

- El sistema no garantiza que las transacciones se efectúen completamente, debido a que no es posible manejar fallas o excepciones durante estos procesos, lo cual hace que el usuario administrador, realice depuraciones de cuentas de acceso en forma manual, cada tres meses por lo general.

- Aunque el sistema permite identificar posibles cuentas huérfanas, no existe un proceso automático que corrija estos sucesos, lo que provoca que el propio administrador del sistema, lo realice de forma manual.

- El sistema no permite personalizar o efectuar cambios en las interfaces de usuario que presenta el sistema.

4.3.2 Impacto de la Solución sobre otros Procesos

En este punto se procederá a efectuar un análisis, en cómo afecta la implementación de este sistema de gestión de identidades IDM, en otros procesos organizacionales a tomar en cuenta, para lo cual, se menciona lo siguiente:

- La implementación de esta solución, ayuda en gran forma a la disminución de la carga operativa en el área IT, debido a que este sistema al encargarse de la gestión de usuarios, logra lo siguiente:

  - ✓ Disminuir la generación de tickets o incidentes, en el tema de gestión de usuarios.

  - ✓ Evita que cada uno de los administradores de los sistemas implementados en la organización, efectúen el proceso de aprovisionamiento de usuarios en forma manual; evitando de esta manera, posibles errores en este proceso, como es el caso de la asignación incorrecta de perfiles de acceso.

  - ✓ También impide que los propios administradores de los sistemas, tengan la responsabilidad de ejecutar el cambio de las contraseñas de acceso a los sistemas.

  - ✓ Evita de igual manera que los administradores de los sistemas, efectúen manualmente depuraciones de cuentas de usuario, cada cierto período.

- Es de gran ayuda en temas de auditoría, debido a que previene la existencia de posibles errores en el proceso de aprovisionamiento de accesos, como la asignación incorrecta de perfiles de acceso, lo que provoca en ciertas ocasiones malestar en sus solicitantes.

- Disminuye el tiempo de respuesta ante cualquier solicitud de aprovisionamiento de accesos o cambio de contraseñas, debido a que estos procesos a través del sistema de gestión de identidades IDM, son automáticos.

- Para el área de Seguridad de la Información, la implementación de esta solución, ayuda en el proceso de mantener un alto nivel de seguridad en la gestión de los respectivos accesos a los sistemas, al permitir la eliminación automática de los accesos que posee un determinado usuario, al salir éste de la organización.

5. CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones

Una vez aplicado el proceso de recolección de información, estudio y análisis de la misma, se desprenden una serie de conclusiones relevantes que básicamente representan los resultados obtenidos a lo largo de esta investigación, las cuales se mencionan de una manera clara y concisa.

1) La implementación de un Sistema de Gestión de Identidades IDM, por sus características tecnológicas como por la infraestructura que necesita para su operación normal, está orientada a organizaciones grandes. Estas entidades deben presentar: una amplia infraestructura tecnológica, administrar un gran número de sistemas informáticos, esto incluye sistemas operativos, bases de datos, servicios organizacionales y aplicaciones en general, y además manejar un alto número de recurso humano. Esto con el fin de aprovechar la funcionalidad y los grandes beneficios que proveen este tipo de soluciones.

   Para tener una clara idea de lo mencionado anteriormente, se expone un ejemplo real. Una organización grande enfocada a la telefonía móvil, presenta una enorme infraestructura tecnológica donde se manejan 230 sistemas informáticos, de los cuales: 30 sistemas operativos, 100 bases de datos, 20 servicios organizacionales y 80 aplicaciones en general. Además, esta organización cuenta con alrededor de 2000 empleados para sus funciones. Es importante aclarar, que los valores mencionados son cantidades aproximadas.

2) El análisis financiero correspondiente al costo total de la solución (CTS), muestra que la implementación de un sistema de estas características, representa una inversión económica elevada para una organización, debido principalmente a su instalación, configuración y sobretodo el licenciamiento por el uso de la herramienta. Pero este alto valor económico, es sumamente inferior al costo (BTS) que representa la falta de un proceso automático y centralizado de accesos a los sistemas; por lo cual, se puede

concluir, que la implementación de un Sistema de Gestión de Identidades IDM en una organización grande, es un proyecto viable, por los grandes beneficios que ofrece en la gestión centralizada de accesos a los sistemas informáticos.

El siguiente cuadro muestra claramente lo dicho:

COSTO TOTAL DE LA SOLUCIÓN (CTS)	BENEFICIO TOTAL DE LA SOLUCIÓN (BTS)	ANÁLISIS DE VIABILIDAD	RESULTADO
$ 694.200 dólares	$ 2´685.444 dólares	CTS < BTS	**La solución es VIABLE**

Cuadro 1 - 05 - Análisis Costo/Beneficio de la Solución **[2]**

3) El análisis técnico comparativo entre los componentes que presentan las soluciones de Oracle, Sun Microsystems y BMC Software, determina que la herramienta desarrollada por Oracle, "*Oracle Identity Management*", es el software que ofrece sin duda, las mejores funcionalidades tecnológicas para llevar a cabo una eficiente gestión centralizada de los accesos a los sistemas informáticos, en las cuatro áreas funcionales: Servicios de Directorio, Gestión de Identidades, Gestión de Accesos y Gestión de Auditoría. El análisis también muestra, que esta solución presenta un importante enfoque en temas de seguridad informática, lo cual es realmente necesario para salvaguardar aquella información de las identidades, que es información sensible e importante para cualquier organización. Por último, un aspecto preponderante para el resultado de este análisis, es el gran número de componentes que cuenta esta solución de Oracle frente a las demás, para cubrir cada una de las áreas funcionales del sistema.

4) El análisis de factibilidad de uso de la solución "*BMC Identity Management Suite Versión 5.5*", desarrollada por la empresa BMC Software, muestra que esta herramienta es factible de utilizarla y administrarla, siempre y cuando, se tomen en cuenta estos aspectos:

- Es indispensable que el usuario administrador del sistema posea altos conocimientos técnicos, en cuanto a: lenguaje de programación Java, administración de una base de datos Oracle, administración de sistemas operativos, arquitectura de una conexión LDAP, como también conocer a profundidad las herramientas que ofrece la solución.

- Además, este conocimiento del usuario administrador, debe ir acompañado de un alto soporte personalizado y profesional por parte del proveedor de la solución, permitiendo así, cubrir al máximo cualquier duda o problema presentado en el sistema.

- De igual manera, para evitar que exista una cierta resistencia en el uso de la herramienta por parte de los usuarios finales del sistema, es necesario que éstos cuenten con una amplia capacitación por parte del proveedor de la solución, en donde se exponga el correcto funcionamiento de la misma.

Finalmente, es importante destacar, que la solución presenta dos aspectos a mejorar: el primero se debe a una interfaz de usuario poco amigable, tanto para el usuario administrador como para los usuarios finales, y el segundo a pequeñas limitaciones en el funcionamiento de la herramienta. Si bien estos criterios son importantes, no representan un impedimento para el uso y el funcionamiento normal de la solución.

5) Luego de haber estudiado la arquitectura que presentan tres sistemas de gestión de identidades IDM: "*Oracle Identity Management*", "*Sun Identity Management*" y "BMC Identity Management Suite", se determina que no existe una arquitectura estándar para este tipo de soluciones, debido a que cada una de ellas emplea diferentes niveles de arquitectura, lo cual incide directamente en el funcionamiento de los sistemas.

6) El funcionamiento que presenta cada una de los tres soluciones estudiadas, "*Oracle Identity Management*", "*Sun Identity Management*" y "BMC Identity Management Suite", hacen referencia a un mismo enfoque, que se puede resumir en cuatro áreas funcionales:

- ***Servicios de Directorio:*** Cuenta con un repositorio centralizado de datos.

- ***Gestión de Identidades:*** Administra el ciclo de vida completo de las identidades.

- ***Gestión de Accesos:*** Administra y controla el acceso a los diferentes recursos organizacionales.

- ***Gestión de Auditoría:*** Provee de procesos automáticos para registrar y administrar información de las identidades.

Pero existe una gran diferencia en el accionar y rendimiento de estas tres soluciones, la cual radica principalmente, en el número de herramientas que poseen estas soluciones para cubrir cada una de las áreas funcionales mencionadas, como también en las características propias que poseen cada una de estas herramientas.

7) El procedimiento en sí para llevar a cabo la integración de una nueva aplicación con el sistema de gestión de identidades IDM, es una tarea compleja, debido a que principalmente, se necesita conocer la tecnología de la cual hace uso la nueva aplicación a integrar, como también la ejecución y el control de una serie de pruebas de funcionamiento de este proceso, lo cual incluye las tareas de sincronización de datos y el aprovisionamiento de las diferentes cuentas de acceso entre ambas plataformas.

8) En la actualidad, la gran mayoría de las organizaciones, no cuentan con una solución que permita gestionar los accesos a los sistemas de una manera centralizada y segura, provocando de esta manera, la aparición de un sin número de irregularidades a nivel de accesos lógicos, lo que causa en muchas ocasiones, enormes pérdidas económicas para las organizaciones. En nuestro país, únicamente tres organizaciones denominadas grandes mantienen implementado una solución como la estudiada en esta investigación.

Esto se debe a ciertos factores:

- Desconocimiento de la existencia de esta solución en el mercado.

- Desconocimiento en temas de seguridad informática.

- Inexistencia de áreas de control en las organizaciones, como Seguridad de la Información o Seguridad Informática.

- El alto costo de instalación, mantenimiento y administración de la herramienta.

- Debido a que la mayoría de las organizaciones en el país, no cuentan con una amplia infraestructura tecnológica.

9) Siguiendo en este mismo tema, los usuarios administradores también presentan una serie de inconvenientes por la falta de un proceso centralizado para la gestión de accesos a los sistemas, debido a que este procedimiento lo efectúan de una forma manual y desorganizada, lo que en muchas ocasiones provoca errores e inconsistencias en la información.

10) La tarea de obtener información para el respectivo análisis de las soluciones enfocadas a la gestión de identidades, resultó una tarea compleja, debido a la falta de cooperación como desconocimiento en aspectos financieros y funcionales de las soluciones, por parte de ciertas empresas proveedoras de esta herramienta. Esto impidió ampliar aún más el análisis y el estudio de las soluciones.

5.2. Recomendaciones

Una vez concluida la presente investigación, se considera importante que se tomen en cuenta las siguientes recomendaciones:

1) Se sugiere profundizar la presente investigación, específicamente en el estudio de diferentes soluciones a las expuestas, de tal manera, de comparar sus características tanto funcionales como tecnológicas. Este nuevo estudio permitirá la obtención de nuevos y amplios conocimientos, para comprender aún más los beneficios de la gestión centralizada de accesos a los sistemas informáticos.

2) Debido a la dificultad para la obtención de información financiera de las soluciones estudiadas, sería importante que se efectúe un análisis comparativo costo/beneficio entre estas soluciones, y así determinar cuál de ellas es una solución viable y beneficiosa para una organización en especial.

3) Un aspecto valioso a tomar en cuenta, dentro del proyecto de implantación de un Sistema de Gestión de Identidades IDM en cualquier organización, es el apoyo y compromiso que debe existir por parte de cada una de las gerencias que conforman la organización, debido a que esta solución no sólo requiere de la participación activa del usuario administrador ni de las áreas de control existentes, sino de todos los usuarios que pertenecen a la organización. De no ser así, todos los beneficios y las funcionalidades que ofrece esta solución no se verían reflejados en su totalidad.

4) En consecuencia con lo mencionado anteriormente, es importante una definición clara de los siguientes aspectos, a tomar en cuenta en el contrato final de compra de la solución:

- Se debe manejar un acuerdo de soporte SLA (*Service Level Agreement*) o un acuerdo a Nivel de Servicio, con el fin de definir claramente el tiempo de respuesta ante cualquier error presentado en la herramienta. Esto incluye la definición de los distintos niveles de escalamiento de los errores.

- Puntualizar cuál será la metodología a emplear en las diferentes fases del proyecto.

- Exigir la obtención del código fuente de la solución y todos los manuales de usuario que ofrece la herramienta, debido a que serán de suma utilidad por temas de soporte, en caso de presentarse alguna falencia en el funcionamiento normal del sistema.

Lo mencionado evitará una mala administración de la herramienta, o peor aún, que el proyecto fracase.

5) Por temas académicos, es recomendable que estudiantes que pertenecen a estudios de nivel superior, reciban información de la existencia de software “grande” en el mercado, como lo es un Sistema de Gestión de Identidades IDM. Esto ayudaría enormemente a que los estudiantes posean una mayor visión en el aspecto financiero como tecnológico que presentan este tipo de herramientas, lo cual será un valioso aporte para su desempeño profesional.

GLOSARIO DE TÉRMINOS

1. **LEY DE SARBANES OXLEY - SOX:** Ley Federal de Estados Unidos que permite monitorear a las empresas, para de esta manera evitar que los procesos llevados en éstas sean alteradas de manera dudosa.
   (http://es.wikipedia.org/wiki/Ley_Sarbanes-Oxley)

2. **REMOTE FUNCTION CALL - RFC:** También conocida como Llamada a Función Remota, es un procedimiento de intercambio de información entre un determinado cliente y el servidor. (http://es.wikipedia.org/wiki/RPC)

3. **CUENTAS HUÉRFANAS:** Son cuentas activas que desapercibidas y olvidadas, proporcionan acceso fácil a aplicativos y datos susceptibles a personas de fuera de la compañía.

   La presencia de este tipo de cuentas es un alto riesgo para las organizaciones, debido a que éstas pueden ser utilizadas para acceder a los sistemas informáticos, sin autorización. (http://www.gbm.net/bt/bt35/hss/administracion_de_identidades.php)

4. **WORKFLOWS:** Es el estudio de los aspectos operacionales de una actividad de trabajo: cómo se estructuran las tareas, cómo se realizan, cuál es su orden correlativo, cómo se sincronizan, cómo fluye la información que soporta las tareas y cómo se le hace seguimiento al cumplimiento de las tareas.

   Una aplicación de flujos de trabajo automatiza la secuencia de acciones, actividades o tareas utilizadas para la ejecución del proceso, incluyendo el seguimiento del estado de cada una de sus etapas y la aportación de las herramientas necesarias para gestionarlo.
   (http://es.wikipedia.org/wiki/Flujo_de_trabajo)

5. **LOGS:** Un log es un registro oficial de eventos durante un rango de tiempo en particular. Para los profesionales en seguridad informática es usado para registrar datos o información sobre quién, qué, cuándo, dónde y por qué un evento ocurre para un dispositivo en particular o aplicación. (http://es.wikipedia.org/wiki/Log_(registro))

6. **SSL NETWORK EXTENDER:** Es un navegador *plugin* cliente que proporciona acceso remoto a una determinada red corporativa, para cualquier aplicación basada en IP. (http://www.iscor.com.mx/cp_segweb.htm)

7. **MICROSOFT ACTIVE DIRECTORY:** Herramienta desarrollada por "*Microsoft Corporation"*, que actúa como un servicio de directorio en una red distribuida de computadoras. (http://es.wikipedia.org/wiki/Active_Directory)

8. **GRUPOS DE USUARIO:** El concepto de grupo de usuarios, permite agrupar de forma lógica a los usuarios de un sistema, y establecer permisos y restricciones a todo el grupo de una vez. Un usuario puede pertenecer a tantos grupos como sea necesario, poseyendo implícitamente la suma de los permisos de todos ellos. Esta forma de administrar la protección del sistema es mucho más flexible y potente que el establecimiento de permisos en base a usuarios individuales.
   (http://fferrer.dsic.upv.es/cursos/Windows/basico/ch05s03.html)

9. **ENCRIPTACIÓN:** Es el proceso para hacer ilegible información considera importante. La información una vez encriptada sólo puede leerse aplicándose una clave.

   Se trata de una medida de seguridad que es usada para almacenar o transferir información delicada que no debe ser accesible a terceros. Pueden ser contraseñas, números de tarjetas de crédito, conversaciones privadas, entre otros.

   Para encriptar información se utilizan complejas fórmulas matemáticas y para desencriptar, se debe usar una clave como parámetro para esas fórmulas.
   (http://www.alegsa.com.ar/Dic/encriptacion.php)

10. **IT – INFORMATION TECHNOLOGY:** Tecnología de la Información, es un término enfocado al estudio, diseño, desarrollo, implementación, soporte o dirección de los sistemas de información computarizados, en particular de software de aplicación y hardware de computadoras. (http://en.wikipedia.org/wiki/Information_technology)

11. **SSO – SINGLE SIGN ON:** Es un procedimiento de autenticación, que habilita al usuario para acceder a varios sistemas informáticos con una sola instancia de identificación. (http://es.wikipedia.org/wiki/Single_Sign-On)

12. **IDM:** Término que hace referencia a *Identity Management*, específicamente a la gestión de identidades. (http://wikitel.info/wiki/Identidad_en_Internet)

13. **IDENTIDAD:** Es la representación de un individuo o entidad dentro de un sistema IT heterogéneo. (http://www.sap.com/spain/services/education/pdf_edutech/B14.pdf)

14. **SISTEMA IT HETEROGÉNEO:** Un sistema heterogéneo es aquel que se encuentra compuesto por hardware con características físicas distintas entre sí, y software con características operativas distintas entre sí, pero que se pueden comunicar utilizando medios comunes.
    (http://www.itistmo.edu.mx/Pag%20Informatica/APUNTES_archivos/page0003.htm)

15. **SISTEMA DE GESTIÓN DE IDENTIDADES:** Sistema integrado de políticas, procesos organizacionales y reglas de negocio, que se encarga de la gestión de todo el ciclo de vida de las identidades; tal es el caso, de los accesos a los sistemas de información. (http://www.borrmart.es/articulo_redseguridad.php?id=818)

16. **HRMS - HUMAN RESOURCE MANAGEMENT SERVICE:** Servicio de Administración de Rescurso Humano, se refiere a sistemas y procesos en los cuales se hace presente la interacción del recurso humano con las tecnologías de la información.
    (http://es.wikipedia.org/wiki/Sistema_de_Administraci%C3%B3n_de_Recursos_Humanos)

17. **CRMS - CUSTOMER RELATIONSHIP MANAGEMENT:** Manejo de Relaciones con Clientes, es un sistema que administra un repositorio de datos que contiene información relacionada a los clientes.
    (http://definanzas.com/2008/06/02/crms-sistemas-de-gestion-de-clientes/)

18. **SERVIDOR PROXY:** Un servidor proxy es un equipo intermediario situado entre el sistema del usuario e Internet. Puede utilizarse para registrar el uso de internet y también para bloquear el acceso a un ambiente web.
    (http://www.java.com/es/download/help/proxy_server.xml)

19. **PROGRAMA BACK-END:** Sistemas informáticos que procesan datos, obtenidos de las interacciones con los usuarios. (http://es.wikipedia.org/wiki/Front-end_y_back-end)

20. **HTTPS - HYPERTEXT TRANSFER PROTOCOL SECURE:** Es un protocolo de red basado en el protocolo HTTP, destinado a la transferencia segura de datos de hipertexto; en otras palabras, es la versión segura de HTTP.
    (http://es.wikipedia.org/wiki/Hypertext_Transfer_Protocol_Secure)

21. **HTML - HYPERTEXT MARKUP LANGUAGE:** Es el lenguaje de marcado predominante para la construcción de páginas web. Es usado para describir la estructura y el contenido en forma de texto, así como para complementar el texto con objetos tales como imágenes. HTML se escribe en forma de etiquetas, rodeadas por corchetes angulares (<,>). (http://es.wikipedia.org/wiki/HTML)

22. **JAVA:** Es un lenguaje de programación orientado a objetos desarrollado por *Sun Microsystems* a principios de los años 90. El lenguaje en sí, toma mucha de la sintaxis de C y C++, pero tiene un modelo de objetos más simple y elimina herramientas de bajo nivel, que suelen inducir a muchos errores, como la manipulación directa de punteros o memoria.
    (http://es.wikipedia.org/wiki/Lenguaje_de_programaci%C3%B3n_Java)

23. **GATEWAYS:** Es un ordenador que permite las comunicaciones entre distintos tipos de plataformas, redes, ordenadores o programas. Para lograrlo traduce los distintos protocolos de comunicaciones que éstos utilizan. Es lo que se conoce como puerta de acceso. (http://tecnologia.glosario.net/terminos-viricos/gateway-9738.html)

24. **LDAP - LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL:** Es 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. LDAP también es considerado una base de datos a la que pueden realizarse consultas.
(http://es.wikipedia.org/wiki/LDAP)

25. **TRANSPARENT DATA ENCRIPTION:** Proceso de encriptación de datos propio de *Oracle*, que permite automáticamente encriptar la información al ser escrita en disco, y desencriptada al momento que la aplicación accede a la misma.
(http://www.oracle.com/technology/oramag/oracle/05-sep/o55security.html)

26. **SEPARATION OF DUTIES:** La teoría Separación de Tareas, evita que una sola persona tenga control de una transacción de inicio a fin; es decir, más de una persona es requerida para completar una tarea.
(http://seguridaddescifrada.blogspot.com/2009/08/separation-of-duties-una-ilusion-en-ti.html)

27. **PEOPLESOFT:** Compañía que suministra software de planificación de recursos empresariales, gestión de recursos humanos, gestión de las relaciones con los clientes y gestión de nómina a grandes empresas.
(http://es.wikipedia.org/wiki/PeopleSoft)

28. **ROLLBACK:** En tecnologías de base de datos, es una operación que devuelve a la base de datos a algún estado previo. Permite revertir una transacción, hasta el inicio o hasta un punto de retorno dentro de ésta. (http://es.wikipedia.org/wiki/Rollback)

29. **J2EE:** Plataforma de programación para desarrollar y ejecutar software de aplicaciones, en un lenguaje de programación Java. (http://www.solotuweb.com/vc~id~1654.html)

30. **CERTIFICADOS X.509:** Certificados utilizados para garantizar la vinculación entre la identidad de un sujeto y su clave pública. (http://es.wikipedia.org/wiki/X.509)

31. **API:** Es una interfaz de programación de aplicaciones, constituida por un conjunto de funciones y procedimientos que ofrece un subprograma, para ser utilizado por otro software como una capa de abstracción. (http://es.wikipedia.org/wiki/Interfaz_de_programaci%C3%B3n_de_aplicaciones)

32. **PLUGIN:** Es una aplicación que se relaciona con otra, para aportarle una función nueva y generalmente muy especifica. Esta aplicación adicional es ejecutada por la aplicación principal e interactúan por medio de una API. (http://es.wikipedia.org/wiki/Complemento_(inform%C3%A1tica))

33. **UNIX:** Es un sistema operativo portable, multitarea y multiusuario; desarrollado, en principio, en 1969 por un grupo de empleados de los laboratorios *Bell de AT&T*. (http://es.wikipedia.org/wiki/Unix)

34. **LINUX:** Término empleado para referirse al sistema operativo libre similar a *Unix* que usualmente utiliza herramientas de sistema *GNU*. Su desarrollo es uno de los ejemplos más prominentes de software libre; todo el código fuente puede ser utilizado, modificado y redistribuido libremente bajo los términos de la GPL (Licencia Pública General de GNU) y otras licencias libres. (http://es.wikipedia.org/wiki/GNU/Linux)

35. **TEMPLATE:** Plantilla ya elaborada, que contiene un diseño, patrón y estilo, ya definido. (http://www.alegsa.com.ar/Dic/plantilla.php)

36. **AGENTE:** En el modelo cliente/servidor, es la parte del sistema que facilita el intercambio de la información entre el cliente y el servidor.
(http://www.mastermagazine.info/termino/3798.php)

37. **FRAMEWORK:** Es una estructura conceptual y tecnológica de soporte definida, normalmente con módulos de software definidos, en base a la cual otro proyecto de software puede ser organizado y desarrollado.
(http://es.wikipedia.org/wiki/Framework)

38. **ENTIDAD:** En bases de datos, una entidad es la representación de un objeto o concepto del mundo real que se describe en una base de datos. Una entidad se describe en la estructura de la base de datos, empleando un modelo de datos. (http://www.alegsa.com.ar/Dic/entidad.php)

REFERENCIAS

[A] Calderón Galo, Problemas a Nivel de Acceso a los Sistemas, 2009/09

[B] Calderón Galo, Problemas a Nivel de Acceso a los Sistemas, 2009/09

[C] http://www.telephonesonline.com.au/images/T/Avaya_IP500_Smart_Card_A-LAW.jpg, Tarjeta Inteligente – Smart Card, 2009/09

[D] http://es.wikipedia.org/wiki/Archivo:RSA-SecurID-Tokens.jpg, Token de Seguridad, 2009/09

[E] http://iso27000.wik.is/Area_Normas/ISO%2f%2fIEC_27002/11._Control_de_Accesos/11.5._Control_de_acceso_al_sistema_operativo/11.5.2._Identificaci%C3%B3n_y_autenticaci%C3%B3n_de_usuario, Norma ISO 27002 – Identificación y Autenticación de Usuarios, 2009/10

[F] http://www.sap.com/spain/services/education/pdf_edutech/B14.pdf, Concepto de Identidad, 2009/10

[G] http://www.tecsidel.es/tecsidel/fileadmin/downloads/NewSI/Gesti_n_de_Identidades_-_Tecsidel_IdM.pdf, Sistema de Gestión de Identidades, 2009/10

[H] http://www.tecsidel.es/tecsidel/fileadmin/downloads/NewSI/Gesti_n_de_Identidades_-_Tecsidel_IdM.pdf, Áreas Funcionales de un Sistema de Gestión de Identidades, 2009/10

[I] Calderón Galo, Áreas Funcionales de un Sistema de Gestión de Identidades, 2009/11

[J] Calderón Galo, Áreas Funcionales de un Sistema de Gestión de Identidades, 2009/11

[K] Calderón Galo, Áreas Funcionales de un Sistema de Gestión de Identidades, 2009/11

[L] Calderón Galo, Áreas Funcionales de un Sistema de Gestión de Identidades, 2009/11

[M] http://www.certant.com/es/img/arquitectura_idm.png, Arquitectura CERTANT Technology Solutions, 2009/11

[N] http://download.oracle.com/docs/cd/E12839_01/oid.1111/e10186.pdf, Arquitectura Oracle, 2009/11

[O] http://download.oracle.com/docs/cd/E12839_01/oid.1111/e10186.pdf, Arquitectura Back-End, 2009/11

[P] http://docs.sun.com/source/821-0058/images/identityMgr_tiers.gif, Arquitectura Sun Microsystems, 2009/11

[Q] http://download.oracle.com/docs/cd/E12839_01/oid.1111/e10029/img/oidag007.gif, Descripción de Oracle Internet Directory, 2009/12

[R] http://www.oracle.com/technology/products/id_mgmt/oxp/pdf/identity_manager_wp_10gr3.pdf, Descripción de Oracle Identity Manager, 2009/12

[S] http://www.oracle.com/technology/products/id_mgmt/oes/pdf/ds_oes.pdf, Descripción de Oracle Entitlements Server, 2010/01

[T] http://www.oracle.com/technology/products/id_mgmt/coreid_fed/pdf/identity_federation_wp.pdf, Descripción de Oracle identity Federation, 2010/01

[U] http://www.oracle.com/technology/products/id_mgmt/oes/pdf/oes_entitlements.pdf, Descripción de Single Sign On, 2010/01

[V] http://www.sun.com/software/products/directory_srvr_ee/directoryserver.pdf, Descripción de Sun Directory Enterprise Edition, 2010/01

[W] http://docs.sun.com/source/820-5819/images/identityMgr__noRepo.gif, Descripción de Sun Identity Manager, 2010/01

[X] http://docs.sun.com/source/820-3740/images/overview2.gif, Descripción de Sun Single Sign On Enterprise, 2010/01

[Y] http://documents.bmc.com/supportu/documents/51/89/55189/55189.pdf, Descripción de BMC Control SA/Directory Manager, 2010/01

[Z] Calderón Galo, Flujo de Caja correspondiente a los Beneficios de la Solución, 2010/01

[1] Calderón Galo, Flujo de Caja correspondiente a los Beneficios de la Solución, 2010/01

[2] Calderón Galo, Análisis Costo/Beneficio de la Solución, 2010/01

[3] Calderón Galo, Componentes de las Soluciones, 2010/01

[4] Calderón Galo, Características de los Componentes en cuanto los Servicios de Directorio, 2010/01

[5] Calderón Galo, Características de los Componentes en cuanto a la Gestión de Identidades, 2010/01

[6] Calderón Galo, Características de los Componentes en cuanto a la Gestión de Accesos, 2010/01

[7] Calderón Galo, Características de los Componentes en cuanto a la Gestión de Auditoría, 2010/01

BIBLIOGRAFÍA

- CERTANT Technology Solutions. Diagrama de Arquitectura IDM. Internet. http://www.certant.com/es/arquitectura_idm.html. Acceso: 29 - 09 – 2009

- ORACLE. ORACLE Identity Management Documentation. Internet. http://download.oracle.com/docs/cd/E12839_01/im.htm. Acceso: 14 - 09 - 2009

- ORACLE. Introducing Oracle Access Manager. Internet. http://download.oracle.com/docs/cd/E15217_01/doc.1014/e12494/overview.htm#CJAECHII. Acceso: 29 - 09 - 2009

- ORACLE. Oracle Fusion Middleware. Internet. http://download.oracle.com/docs/cd/E12839_01/oid.1111/e10186.pdf. Acceso: 27 - 09 – 2009

- SUN Microsystems. Identity and Access Management Software for Enterprise. Internet. http://www.sun.com/software/identity/inside.jsp. Acceso: 02 - 10 – 2009

- SUN Microsystems. Installation Steps (Sun Identity Manager 8.1 Installation). Internet. http://docs.sun.com/app/docs/doc/820-5594/ahtdx?l=en_US&a=view. Acceso: 02 - 10 - 2009

- SIA. Gestión Avanzada de Identidades. Internet. http://www.sia.es/noticias/IL_idM%2B.pdf. Acceso: 02 - 09 - 2009

- ORACLE. Introducción a Oracle Identity Management. Internet. http://www.oracle.com/dm/09h2lad/28532_oracle-idm-whitepaper_cast.pdf. Acceso: 05 - 09 - 2009

- ORACLE. Resource Library – Oracle Identity Management. Internet. http://www.oracle.com/products/middleware/identity-management/resource-library.html. Acceso: 17 - 09 - 2009

- Cser, Andras. The Forrester Wave: Identity and Access Management, Q1 2008. Internet. http://www.oracle.com/corporate/analyst/reports/infrastructure/sec/forresterwave-idm.pdf. Acceso: 02 - 09 – 2009

- TECSIDEL. Gestión de Identidades TECSIDEL IDM. Internet. http://www.tecsidel.es/tecsidel/fileadmin/downloads/NewSI/Gesti_n_de_Identidades_-_Tecsidel_IdM.pdf Acceso: 19-10-2009

- SeguridadSAP. Tipos de Usuarios en SAP. Internet. http://blog.segu-info.com.ar/2009/06/tipos-de-usuario-en-sap.html Acceso: 24-10-2009

- NOVELL. Verificación de Identidad conforme a la norma HSPD-12. Internet. http://www.novell.com/es-es/industries/government/identity.html Acceso: 26-10-2009

- CA. Widespread Bad Practice in 'Privileged User' Management Threatens Security in European Organizations. Internet. http://www.ca.com/Files/SupportingPieces/20_10_09_quocirca_sec_survey_results_pr_219251.pdf Acceso: 27-10-2009

- Medina, José Manuel. Gestión de La Identidad Digital en Red: Gestión de Identidades y Control de Acceso. Internet. http://1enise.inteco.es/ponencias/ENISE-P13_Jose_Manuel_Medina.pdf Acceso: 29-10-2009

- ORACLE. Understanding Identities, Policies and Credentials. Internet. http://download.oracle.com/docs/cd/E12839_01/core.1111/e10043/stores.htm#JISEC2628 Acceso: 02-11-2009

- ORACLE. Introduction to Oracle Fusion Middleware Audit Framework. Internet. http://download.oracle.com/docs/cd/E12839_01/core.1111/e10043/audintro.htm#CEGBJGFI
  Acceso: 04-11-2009

- MICROSOFT. Gestión de Identidades: Solución a la automatización del acceso a la información. Internet.
  download.microsoft.com/download/b/0/c/b0c210bd-6d80-4d40-9a43-60c7b643ab04/w86-microsoft-folleto.pdf
  Acceso: 19-10-2009

- NOVELL. Gestión de Identidad y Acceso: La llave a la agilidad empresarial .Internet. www.sap.com/spain/services/education/pdf_edutech/B14.pdf
  Acceso: 22-10-2009

- Wikipedia. Smart Card. Internet.
  http://en.wikipedia.org/wiki/Smart_card
  Acceso: 12-11-2009

- Wikipedia. Token de Seguridad. Internet.
  http://es.wikipedia.org/wiki/Token_de_seguridad
  Acceso: 12-11-2009

- Wikipedia. Biometría. Internet.
  http://es.wikipedia.org/wiki/Biometría
  Acceso: 13-11-2009

- The Open Group. Single Sign On. Internet.
  http://www.opengroup.org/security/sso/
  Acceso: 13-11-2009

- Aladdin. Gestión de Contraseñas: Single Sign On. Internet.
  http://www.aladdin.es/news/2006/eToken/gestion_contrasenyas.aspx
  Acceso: 14-11-2009

- IPSCA. SSO Single Sign On. Internet.
  http://web.ipsca.com/en/Products_SSO_Single_Sign_On
  Acceso: 15-11-2009

- ORACLE. Introducción a Oracle Identity Management. Internet. http://www.oracle.com/technology/global/lad-s/documentation/collaterals/Whitepaper-Introduccion-a-Oracle-Identity-Management.pdf. Acceso: 17 -11 -2009

- ORACLE. Oracle Identity Management. Internet. http://www.oracle.com/technology/products/id_mgmt/index.html. Acceso: 17 -11 -2009

- ORACLE. Oracle Identity Management Documentation. Internet. http://download.oracle.com/docs/cd/E12839_01/im.htm. Acceso: 17 -11 -2009

- ORACLE. Documentación de Oracle. Internet. http://www.oracle.com/technology/global/lad-es/documentation/index.html. Acceso: 18 -11-2009

- ORACLE. Understanding Oracle Identity Management. Internet. http://download.oracle.com/docs/cd/E12839_01/install.1111/e12002/overview.htm. Acceso: 18 -11-2009

- ORACLE. Introduction to Directory Services. Internet. http://download.oracle.com/docs/cd/E12839_01/oid.1111/e10029/intro.htm#g1007364 Acceso: 18 -11-2009

- ORACLE. Identity Management – Oracle Identity Management. Internet. http://www.oracle.com/us/products/middleware/identity-management/index.htm. Acceso: 18 -11-2009

- ORACLE. Oracle Internet Directory. Internet. http://www.oracle.com/technology/products/oid/pdf/oid_ds_11g.pdf. Acceso: 18 -11-2009

- ORACLE. Oracle Role Manager. Internet. http://www.oracle.com/technology/products/id_mgmt/orm/pdf/oracle_role_manager_WP.pdf. Acceso: 19-11-2009

- ORACLE. Oracle Access Manager. Internet.
  http://www.oracle.com/technology/products/id_mgmt/coreid_acc/pdf/access_manager_wp_10gr3.pdf.
  Acceso: 21 -11 -2009

- ORACLE. Oracle Identity Federation. Internet.
  http://www.oracle.com/technology/products/id_mgmt/coreid_fed/pdf/identity_federation_wp.pdf.
  Acceso: 22 -11 -2009

- ORACLE. Oracle Authentication Services for Operating Systems. Internet.
  http://www.oracle.com/technology/products/oid/htdocs/oracleauthenticationservices_wp.pdf.
  Acceso: 23 -11 -2009

- SUN MICROSYSTEMS. Sun Identity Manager. Internet.
  http://docs.sun.com/app/docs/coll/1514.6?l=en_US.
  Acceso: 25 -11 -2009

- SUN MICROSYSTEMS. Sun Identity Manager. Internet.
  http://www.sun.com/software/products/identity_mgr/ds_identitymgr.pdf.
  Acceso: 25 -11 -2009

- SUN MICROSYSTEMS. Documentación de Productos. Internet.
  http://docs.sun.com/app/docs/prod/access.mgr?l=es#hic.
  Acceso: 27 -11 -2009

- SUN MICROSYSTEMS. Software Products. Internet. http://www.sun.com/software/.
  Acceso: 28 -11 -2009

- SUN MICROSYSTEMS. Sun Identity Management. Internet.
  http://developers.sun.com/identity/index.jsp.
  Acceso: 28 -11 -2009

- SUN MICROSYSTEMS. Sun Identity Manager Overview. Internet.
  http://docs.sun.com/app/docs/doc/820-5819/giaik?l=en_US&a=browse.
  Acceso: 29 -11 -2009

- SUN MICROSYSTEMS. Sun Directory Server Enterprise Edition. Internet.
  http://www.sun.com/software/products/directory_srvr_ee/directoryserver.pdf.
  Acceso: 29 -11 -2009

- BMC SOFTWARE. BMC Identity Management Suite CONTROL-SA/DIRECTORY MANAGER. Internet. http://documents.bmc.com/supportu/documents/51/89/55189/55189.pdf. Acceso: 01 -12 -2009

- BMC SOFTWARE. BMC Identity Management Suite/BMC Password Manager. Internet. http://documents.bmc.com/supportu/documents/27/57/62757/62757.pdf. Acceso: 02 -12 -2009

- BMC SOFTWARE. BMC Identity Management Suite/Identity Request Manager. Internet. http://documents.bmc.com/supportu/documents/29/72/62972/Output/wwhelp/wwhimpl/js/html/wwhelp.htm. Acceso: 03 -12 -2009

- BMC SOFTWARE. BMC Identity Management Suite/BMC User Administration Manager. Internet. http://documents.bmc.com/supportu/documents/27/55/62755/62755.pdf Acceso: 06 -12 -2009

- BMC SOFTWARE. BMC Web Access Manager for J2EE. Internet. http://documents.bmc.com/supportu/documents/31/64/63164/63164.pdf. Acceso: 11 -12 -2009

- BMC SOFTWARE. BMC Identity Federation Manager. Internet. http://documents.bmc.com/supportu/documents/31/77/63177/63177.pdf. Acceso: 13 -12 -2009

- BMC SOFTWARE. BMC Identity Management Suite. Internet. http://documents.bmc.com/supportu/documents/09/11/70911/Output/wwhelp/wwhimpl/js/html/wwhelp.htm. Acceso: 18 -12 -2009