GESTIÓN DE IDENTIDADES Y CONTROL DE ACCESO DESDE UNA PERSPECTIVA ORGANIZACIONAL

José A. Montoya S.
Bancolombia
Medellín, Colombia
josmonto@bancolombia.com

Zuleima Restrepo R.
Bancolombia
Medellín, Colombia
zrestrep@bancolombia.com

(Tipo de Artículo: **Reflexión**. Recibido el 01/11/2011. Aprobado el 09/04/2012)

RESUMEN
En el mundo actual, de mercados globalizados, las organizaciones necesitan incrementar la agilidad del negocio para el desarrollo de estrategias que les permitan competir de forma eficiente, cumplir con regulaciones y ser flexibles ante el entorno cambiante de regulaciones, normas y leyes; para esto necesitan contar con mecanismos que garanticen la disponibilidad de la información y el acceso seguro a las aplicaciones y recursos a través de múltiples sistemas y permitan el uso de servicios en línea para empleados, clientes, proveedores y socios de negocio. En este documento se describe de forma general los conceptos alrededor de la gestión de identidades y control de acceso; tales como servicios de directorios, gestión de identidades, gestión de roles y gestión del control de acceso. Además se listan los principales beneficios y desventajas que se presentan en la implementación de una solución de gestión de identidades y control de acceso, el estado actual a nivel organizacional y algunos casos de éxito a nivel latinoamericano.

Palabras clave
Autenticación, autorización, control de acceso, seguridad informática, permisos, sistemas de gestión de identidades.

AN APPROACH TO IDENTITY MANAGEMENT AND ACCESS CONTROL FROM ORGANIZATIONAL PERSPECTIVE

ABSTRACT
In the modern world of global markets, organizations need to increase the business agility in order to develop market strategies that allow them to compete efficiently, comply with government regulations and be flexible enough in the changing environment of regulations and laws. In order to accomplish this objectives, organizations need to have methods that assure the information availability and the secure access to applications and resources across multiple systems and allow users such as employees, customers, suppliers and business partners to access online services. This document describes concepts related to identity and access management such as identity management, role management and access management as well as the principal benefits and disadvantages found when implementing an Identity and access management solution, the current situation at organizational level and some successful experiences in Latino America.

Keywords
Authentication, authorization, access control, computer security, permission, identity management systems.

GESTION D'IDENTITES ET CONTRÔLE D'ACCES D'APRES UNE PERSPECTIVE ORGANISATIONNELLE

RÉSUMÉ
Dans le monde actuel, avec des marchés globalisés, les entreprises nécessitent d'accroître l'agilité d'affaires pour le développement des stratégies qui permettaient de concurrencer d'une manière efficace, respecter les contrôles et d'être flexible devant l'environnement changeant de contrôles, règles et lois ; pour accomplir ceci, il est nécessaire d'avoir des mécanismes qui garantissent la disponibilité de l'information et l'accès sécurisé aux applications et ressources à travers de multiples systèmes et en permettant l'usage de services en ligne pour des employés, des clients, des fournisseurs et associés. On décrit d'une manière générale les concepts au sujet de la gestion d'identités et contrôle d'accès ; comme des services de répertoire, gestion d'identités, gestion des rôles et gestion du control d'accès. En plus, on énumère les principaux bénéfices et inconvénients qui se présentent pendant l'implémentation d'une solution de gestion d'identités et contrôle d'accès, l'actualité dans les entreprises et quelques cas de succès en Amérique Latine.

Mots-clés
Authentification, autorisation, contrôle d'accès, sécurité informatique, permissions, systèmes de gestion d'identités.

1. INTRODUCCIÓN

Las organizaciones se enfrentan a diversos retos en su afán de ser competitivas y rentables, por lo que requieren incrementar la agilidad en los procesos de negocio y mejorar la seguridad y la disponibilidad de la infraestructura que los soporta. El uso de múltiples sistemas, aplicaciones y estándares facilita la proliferación de diversas identidades digitales para clientes, empleados y socios de negocio.

La complejidad se hace evidente cuando coexisten diversos repositorios de identidades que operan de forma independiente y con diferentes estándares, lo que da como resultado el incremento en los costos de administración, en las inconsistencias de los datos y en las apariciones de brechas de seguridad.

La gestión de identidades y control de acceso, IAM por sus siglas en inglés, es una solución que permite realizar la gestión del ciclo de vida de las identidades y controlar el acceso a los diferentes recursos, con el objetivo de mitigar riesgos, reducir costos y permitir que el negocio evolucione de manera segura y flexible.

El objetivo principal de este artículo es presentar de manera clara y concisa los aspectos generales, ventajas, desventajas, componentes y características de una solución de gestión de identidades y control de acceso, además de describir las necesidades de su implementación. Sirve como punto de partida que brinda las bases necesarias y los elementos de juicio generales acerca de la problemática que resuelve la implementación de un proyecto de este tipo.

2. ESTADO ACTUAL ORGANIZACIONAL

Las organizaciones actuales, con el ánimo de crear oportunidades de negocio y ventajas competitivas que les ayuden a obtener el mejor beneficio en los mercados globalizados, desarrollan estrategias de negocio orientadas a Internet, en la que el acceso a la información se logra a través de sitios públicos, de extranet o de intranets.

Adicionalmente, los usuarios de los servicios ya no solamente son empleados, sino también socios de negocio, terceros y clientes. De esto se desprende una serie de retos que afectan las estrategias que desarrolla la organización y la forma como puede generar soluciones eficientes y competitivas. En la Figura 1 se muestran algunos de estos retos.

Fig. 1: Retos organizacionales actuales [1]

2.1 Cumplimiento regulatorio

A diario se implementan nuevas regulaciones que afectan, de una u otra manera, a las organizaciones y la forma en la que interactúan con el mercado. Hasta ahora, las organizaciones han enfrentado el cumplimiento regulatorio implementando una serie de esfuerzos individuales centrados en los controles que la regulación define y por medio de productos que ayuden a satisfacer los requisitos del Estado [6]. La complejidad de este enfoque puede ser abrumadora debido al número de regulaciones que se promueven a diario y al número de aplicaciones que se deben implementar para satisfacerlos. Lo que se propone como solución es una infraestructura unificada que permita, de manera económica, eficiente y sostenible, la implementación de controles estandarizados y automatizados necesarios para el cumplimiento regulatorio.

2.2 Sobrecarga de la mesa de ayuda

Con la proliferación de usuarios y contraseñas como resultado de la implementación de varias aplicaciones y sistemas, una de las tareas más comunes y repetitivas es que la mesa de ayuda a los usuarios debe destinar un alto porcentaje de operadores para apoyar cambios de contraseña y desbloqueo de cuentas de usuario. Estos procesos consumen tiempo y recursos, lo que disminuye la productividad de los usuarios debido al tiempo que invierten en las solicitudes. Lo que se propone como solución es una infraestructura que permita la unificación de identidades y la autogestión de contraseñas y desbloqueo de cuentas de usuario, liberando a la mesa de ayuda y permitiendo concentrar sus esfuerzos en otras áreas.

2.3 Costos en la administración

Actualmente, las organizaciones deben destinar una parte de su presupuesto para el sostenimiento de varios operarios que realicen la administración de las cuentas de usuario y las actividades realizadas por medio de la mesa de ayuda, para la gestión de usuarios y aplicaciones que ayuden a cumplir con las regulaciones. Con la disminución en la carga de tareas asignadas a la mesa de ayuda y con la implementación de una infraestructura robusta y confiable que ayude a cumplir con las regulaciones y simplifique la gestión de usuarios, roles y control de acceso se logra una reducción significativa de los costos asociados con dichas tareas, o se podría destinar el conocimiento de las personas al mejoramiento y evolución de los sistemas.

2.4 Seguridad (Cuentas huérfanas)

Teniendo en cuenta la cantidad de accesos creados por cantidad de aplicaciones, cada vez es más complicado implementar controles que garanticen que los usuarios son creados y eliminados en el momento apropiado, o que las credenciales de inicio sean iguales en todos los sistemas (principio de integridad de la información). Lo que se busca es una solución que permita la gestión del ciclo de vida de las identidades de acuerdo a las novedades que se presenten en las aplicaciones de nómina y recursos humanos, evitando que cuentas de usuario permanezcan activas aun cuando la relación del usuario con la organización ha dejado de existir, así mismo, reducir la cantidad de permisos que un usuario determinado puede utilizar cuando cambia de función o

puesto de trabajo, pero teniendo en cuenta que poco se des-aprovisiona en los sistemas que ya no utiliza.

2.5 Requerimientos de auditoría

El incumplimiento de los requerimientos de auditoría puede dar como resultado problemas para el cumplimiento de los niveles de seguridad certificados lo que puede resultar en incidentes de seguridad, vulnerabilidades explotadas y en algunos casos implicaciones legales y pérdidas económicas y de imagen [7]. Lo que se busca es implementar una arquitectura que permita el acceso eficiente a la información requerida por los entes auditores que avalan el cumplimiento de los controles de seguridad establecidos y cumplimiento de los niveles de calidad y seguridad —dando tranquilidad a los revisores—.

2.6 Errores de privilegios

Un privilegio mal asignado o la incapacidad de retirar el permiso en el momento adecuado conllevan a accesos no autorizados a la información y los recursos protegidos ocasionando incidentes en donde se comprometa la confidencialidad e integridad de la información y los recursos. Lo que se busca es una solución que permita la asignación efectiva de permisos, dependiendo de las funciones que desempeña cada usuario dentro de la organización.

Finalmente, la organización se puede ver expuesta a multas, fraudes e ineficiencia en procesos de negocio como resultado de la incapacidad para enfrentar de manera adecuada los retos presentados anteriormente y que están relacionados con el incumplimiento de las normas y regulaciones, incidentes de seguridad generados por falta de auditoría y de controles que garanticen acceso adecuado a los recursos.

3. GESTIÓN DE IDENTIDADES Y CONTROL DE ACCESO

La gestión de identidades y control de acceso por sus siglas en inglés IAM [2] es un término que se puede entender como el conjunto de procesos de negocio, tecnologías, infraestructura y políticas que permite realizar la gestión de las identidades de usuario y controlar el acceso de éstas a los diferentes recursos organizacionales. De este modo queda claro que, como tal, la gestión de identidades y control de acceso no debe entenderse como una tecnología o herramienta que se implementa en una organización de forma general y con esto se obtienen los beneficios esperados. Por el contrario, la gestión de identidades y control de acceso involucra diferentes procesos y áreas en la organización, desde la alta gerencia hasta las áreas de soporte y apoyo; cuya implementación y buenos resultados depende de la disposición y grado de compromiso que demuestre cada uno de los diferentes actores al interior de la compañía en el desarrollo de un proyecto de este tipo [3].

3.1 Ventajas

Los principales beneficios [2] que se pueden lograr por medio de la implementación de una solución de gestión de identidades y control de acceso son:

- Protección tanto de los datos de usuarios como de los datos asociados con los recursos organizacionales; con esto se disminuyen los riesgos relacionados con el aseguramiento de la información, robo de identidad, propiedad intelectual, amenazas globales y crimen organizado.

- Control de acceso eficiente basado en roles. El acceso a los recursos es determinado por los roles asignados según el cargo desempeñado dentro de la organización, es decir, cada usuario solo debe tener acceso a la información y recursos necesarios para el buen desempeño de las funciones para las cuales fue contratado, de acuerdo con los procesos organizacionales. A esto también se le denomina el menor privilegio, es decir, los usuarios solo tienen acceso a lo que deben tener. Por ejemplo, una persona del área comercial o ventas no debe poseer acceso a los salarios de toda la compañía.

- Mayor cumplimiento de regulaciones actuales relacionadas con la protección de datos de usuario, datos organizacionales y generación de reportes de auditoría.

- Reducción de costos en tareas administrativas asociadas con la gestión de cuentas de usuario y en los servicios de mesa de ayuda por medio de la disminución de llamadas para cambios de contraseña, desbloqueo de cuentas de usuarios y requerimientos para la creación, modificación, eliminación de cuentas de usuario en aplicativos o plataformas dentro de la organización.

- Incremento de la productividad por medio de la eliminación del tiempo ocioso entre la creación de la cuenta de usuario y la asignación de los roles necesarios para el acceso a las aplicaciones requeridas para el desempeño de las funciones relacionadas con el cargo.

- Administración delegada de usuarios, recursos y políticas para controlar el acceso a las aplicaciones.

- Autoservicio: Son funcionalidades incorporadas dentro de una solución de gestión de identidades y control de acceso, por medio de las cuales los usuarios pueden realizar la autogestión y recuperación de contraseñas y flujos de trabajo que automatizan la creación de solicitudes de recursos requeridos para el desarrollo de sus funciones, por ejemplo, una persona del área comercial puede crear la solicitud para que le sea asignado un Smartphone para el acceso a la documentación disponible en la intranet desde una ubicación remota.

- Automatización: Se logra automatizar diferentes procesos dentro de la organización, algunos de ellos son: procesos de creación, modificación y eliminación de las cuentas de usuario en las diferentes aplicaciones integradas bajo una solución de gestión de identidades y control de acceso,

creación de flujos de trabajo para la aprobación manual o automática de solicitudes relacionadas con la identidad del usuario y los recursos requeridos, asignación de roles y permisos basados en el cargo de los empleados, activación y desactivación de las cuentas de usuario dentro de la organización basado en las novedades de nómina como por ejemplo: vacaciones, incapacidades, licencias, entre otras.

- Integración de servicios y de repositorios de datos de usuarios bajo una misma arquitectura, lo que facilita la administración de las cuentas de usuario y posibilita que un usuario solo necesite manejar una cuenta de usuario para acceder diferentes aplicaciones y servicios empresariales.

- Consistencia en los datos relacionados con la identidad de los usuario lo que garantiza que si un datos es modificado en el repositorio central, dicho cambio se va a ver reflejados en las aplicaciones integradas en una solución de gestión de identidades y control de acceso. Por ejemplo, si a un empleado le cambian el contrato y el cargo desempeñado desde la aplicación de recursos humanos, dicha información se debe ver reflejada en la intranet, el directorio de empleados y en el acceso a las aplicaciones según los roles asociados al cargo [8].

3.2 Desventajas

Las principales desventajas que se pueden observar en la implementación de una solución de gestión de identidades y control de acceso son:

- Una solución de gestión de identidades y control de acceso permite que un usuario solo maneje una contraseña para acceder a las diferentes aplicaciones integradas bajo dicha solución. Esta característica incrementa el riesgo de que si no se utiliza un esquema de autenticación robusto factor dos —uso de *token*, tarjeta coordenadas, certificados digitales de cliente— o un plan de sensibilización adecuado para el uso de contraseñas fuertes, dichas claves pueden ser vulneradas fácilmente a través de un *keylogger* o *mouselogger* permitiendo, de este modo, eventos de tipo de suplantación de identidad, robo de información, entre otros.

- En una solución de gestión de identidades y control de acceso, el acceso a las aplicaciones del negocio se realiza por medio de la autenticación de los usuarios contra el repositorio unificado de identidades. Si se presentan fallos en los procesos de autenticación y autorización, esto afectaría a todas las aplicaciones integradas bajo este esquema mientras que en un esquema tradicional las fallas afectan solo a las aplicaciones puntuales. Esta desventaja se subsana por medio de la implementación de la instalación y configuración de componentes redundantes, por ejemplo, el despliegue de servicios de directorios en alta disponibilidad con mecanismos de replicación.

- En la mayoría de casos, la implementación de una solución de gestión de identidades y control de acceso requiere una reestructuración de procesos y del modelo operativo de las organizaciones sobre el cual se implementa. En dichos casos se requiere invertir tiempo, esfuerzos y recursos en la ingeniería de roles para lograr una buena definición.

- Una buena implementación de una solución de gestión de identidades y control de acceso requiere realizar un trabajo muy detallado y específico para la definición de los roles de negocio y su relación con los roles técnicos —por ejemplo, accesos a bases de datos, plataformas con roles de administradores, entre otros—. Si dicho proceso no se realiza de forma adecuada, se puede presentar que la gestión de los roles técnicos o de aplicación no queda dentro del alcance lo cual obliga a implementar otros esquemas de control complementarios.

- La implementación de una solución de gestión de identidades y control de acceso requiere de una inversión considerable de dinero, tiempo y recursos, lo cual dificulta la estructuración de un caso de negocio y el respectivo retorno de inversión a corto plazo. El retorno de inversión de un proyecto de este tipo es a largo plazo.

- Dependiendo de la complejidad de las aplicaciones que se van a integrar y la forma en la cual realizan los procesos de autenticación y autorización, es necesario tener un conocimiento adecuado de éstas y en algunos casos se requiere realizar modificaciones para que los mecanismos de autenticación y autorización se configuren de acuerdo al esquema diseñado por medio de la solución de gestión de identidades y control de acceso. En este sentido es necesario destinar dinero, tiempo y recursos para la entrega de dicho conocimiento y la realización de las modificaciones requeridas para su integración.

3.3 Componentes de una solución de Gestión de identidades y Control de Acceso

Una solución de gestión de identidades y control de acceso cuenta con los siguientes componentes.

Servicio de directorios. Un servicio de directorios es un componente de la red que permite que un directorio sea administrado de forma central y al mismo tiempo provee información para las aplicaciones organizacionales que interactúen con éste. Un servidor de directorios permite almacenar no solamente usuarios, sino también recursos según sea las necesidades del negocio [5]. En éste se tienen las siguientes consideraciones:

- Información estructurada y extensible

La estructura de la información es definida por medio de un esquema. El esquema del servicio de directorios hace referencia al conjunto de reglas que determinan que información puede ser almacenada dentro de un servidor de directorios y además determina la manera en que esta información será utilizada en operaciones

tales como la búsqueda. Cada vez que el Servidor de Directorios pretende almacenar o modificar una "entrada" —unidad de información que representa una entidad dentro del servicio de directorios—, el servidor verifica que dichas reglas se apliquen acorde a lo establecido. Además, cuando un cliente u otro servidor de directorios comparan dos valores de atributos, consultan al servidor de directorios para determinar el algoritmo de comparación a usar. Para el desarrollo del esquema es importante tener en cuenta la importancia de combinar la información que necesitan los diferentes servicios y aplicaciones que son atendidos por el servidor de directorios, con el fin de unificar datos redundantes de manera que quede el menor número de entidades posibles.

Además, el esquema del servicio de directorios puede ser utilizado para imponer restricciones de tamaño, rango, y formato de los valores almacenados en el directorio —mejorando la calidad de los datos almacenados—. Ahora bien, dentro del esquema de un servicio de directorios participan los siguientes elementos:

Atributos: los tipos de atributos incluyen la siguiente información: (1) un nombre que identifica de manera única el tipo de atributo [10], (2) un OID —*object identifier*, una cadena compuesta por una serie de dígitos decimales que tienen una jerarquía determinada y que son controlados por la IANA, ANSI e ISO, entre otros— que también identifica de manera única el tipo de atributo, (3) un indicador de sí el tipo de atributo permite o no múltiples valores, (4) una sintaxis de atributo asociada y conjunto de reglas de comparación. Dentro de las sintaxis de atributos se especifica la manera exacta a través de la cual los atributos son representados y el algoritmo de comparación que será utilizado en el momento en el que se realice una comparación o búsqueda, (5) un indicador de uso, de utilización interna por los servidores de directorios y (6) restricciones respecto al tamaño, rango de valores que pueden ser aceptados por este tipo de atributo.

Clases de objetos: una clase de objetos modela algún objeto del mundo real tal como una persona, una impresora o un dispositivo de red. Cada entrada en el servidor de directorios pertenece a una o varias clases de objetos. Las necesidades principales que se suplen cuando una entrada pertenece a un grupo determinado de clases de objetos son: (1) determinar cuáles tipos de atributos DEBEN ser incluidos en dicha entrada, (2) determinar cuáles tipos de atributos PUEDEN ser incluidos en la entrada en cuestión y (3) proveer el mecanismo para que los clientes puedan obtener un subconjunto de entradas cuando realizan operaciones de consulta.

Toda definición de una clase de objetos incluye la siguiente información: (1) un nombre que identifica de manera única la clase, (2) un OID —*object identifier*— que igualmente identifica de manera única la clase a la cual pertenece, (3) un conjunto de atributos que son obligatorios para la definición de la clase, (4) un conjunto de atributos opcionales dentro de la definición de la clase y (5) el tipo de clase a la cual pertenece: estructural, auxiliar o abstracta.

Además, al igual que como se maneja dentro de los atributos en un servicio de directorios, dentro de las clases de objetos también se pueden especificar relaciones de herencia que permiten simplificar el modelamiento de características de cada una de las clases de objetos que pertenecen a un servicio de directorios determinado.

- Modelo de información jerárquico

El modelo de información depende de la configuración del espacio de nombres (*namespace*) dentro del servicio de directorio, el cual es definido de manera jerárquica en forma de árbol. En la raíz del árbol se configura el dominio de la organización a través de los componentes de dominio (*domain component*) y que son representados por medio de la cadena dc. Los objetos del directorio en los nodos del árbol se denominan contenedores, los cuales a su vez pueden contener otros contenedores u objetos terminales también conocidos como las ramas del árbol y que dentro del árbol del servidor de directorios corresponde a las entradas las cuales a su vez están compuestas por atributos.

- Optimizado para las búsquedas

Las operaciones de obtención de datos son más importantes que las operaciones de actualización y por esta razón los servidores de directorios son diseñados para que las operaciones de búsqueda sean realizadas de manera rápida y óptima, mientras que las operaciones de escritura son más pobres en rendimiento y consumen más recursos. Por otro lado, los servidores de directorios son optimizados para almacenar y gestionar millones de objetos relativamente pequeños.

Adicionalmente, las transacciones normalmente se realizan sobre pequeñas unidades de datos y no sobre grandes volúmenes de datos como sucede en el caso de las bases de datos.

Meta-directorios: son servicios de directorio que tienen la capacidad de recolectar y almacenar información de varios y diversos servidores de directorios [1]. En algunos casos los meta-directorios tienen la capacidad de integrar información disponible en bases de datos. La información de las diversas fuentes es agregada para proveer una vista única de dichos datos. Cabe anotar que en la consolidación de los datos, la información puede ser transformada según las reglas que se tengan definidas en el meta-directorio para los procesos de recolección e importación de los datos.

Los meta-directorios le permiten a la organización integrar en un único repositorio la información existente en diversas fuentes de tal modo que se puedan realizar búsquedas de manera centralizada y no varias búsquedas en varios servidores de directorios. Algunos de los beneficios de un meta-directorio son:

- Existe un único punto de referencia que provee un mayor nivel de abstracción para las aplicaciones que requieren información dispersa por toda la organización en diferentes fuentes de información.

- Existe un único punto de administración, lo que reduce la carga administrativa evitando tener que realizar múltiples accesos a diferentes servidores de directorios.

- Se puede eliminar la información redundante al poseer un repositorio unificado de datos.

En el diseño de un meta-directorio se deben resolver varios temas a nivel de gobernación de la información y a nivel técnico. Dentro del gobierno de la información se tiene los siguientes aspectos:

- Definición de los dueños de la información. Estas personas deben velar porque la información se mantenga actualizada, que sea útil para los procesos dentro de la organización y que se cumplan las políticas de seguridad para su manejo.

- Responsabilidades administrativas bien definidas que permiten que la información esté disponible cuando sea requerida y se garantice su disponibilidad, confidencialidad e integridad.

- Cumplimiento con los requerimientos legales. En este se define los procesos de auditoría y el manejo de la información requerida para los procesos de cumplimiento.

- Definición del formato de los datos y diseño del esquema con los atributos requeridos para almacenar la información.

- Definición de políticas y mecanismos para la seguridad de la información.

- Definición de políticas de acceso a la información y los responsables de crear dichas políticas.

A nivel técnico se tienen los siguientes aspectos:

- Definición y diseño de la arquitectura.

- Definición, diseño y normalización del espacio de nombres y la estructura del árbol del directorio.

- Diseño de los mecanismos y procedimientos para la sincronización de los datos con otros servicios de directorios. Acá es muy importante definir la fuente de autoridad con relación a los datos, pues los datos pueden ser modificados en el meta-directorio o en los diferentes servicios de directorio con los cuales este interactúa. De esta manera, se debe garantizar que los datos solo se modifican en un solo punto y la información sea replicada a los diferentes repositorios que interactúa dentro de este proceso.

Un aspecto importante de los meta-directorios, es que estos funcionan por medio de agentes que se encargan de recolectar los datos en los diferentes servidores de directorios y enviarlos al meta-directorio para su consolidación.

En la Figura 2 se presenta un ejemplo de meta-directorio, en el cual se integra la información proveniente de los servicios de directorios de empleados y terceros. La comunicación con los servicios de directorios se realiza a través del protocolo LDAP y la información almacenada en éste es consultada por las aplicaciones de negocio y las aplicaciones integradas por medio del portal corporativo, las cuales sólo deben consultar un repositorio de información y no dos como sería en el caso de no contar con el meta-directorio.

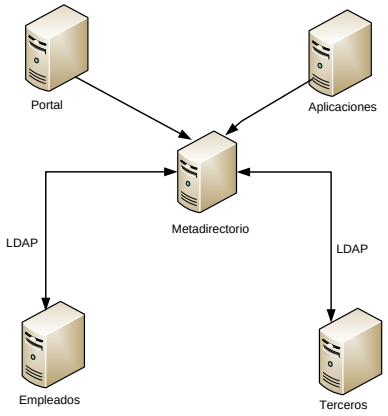


Fig. 2: Topología de un Meta-directorio [1]

Directorios Virtuales: tienen un concepto similar al meta-directorio, estos se encargan de crear una vista unificada de la información que procede de diferentes fuentes dentro de la organización. La principal diferencia es que el directorio virtual no hace uso de agentes para la recolección de los datos, en cambio se encarga de crear una vista única por medio de sentencias ejecutadas en tiempo real y que son construidas por medio del mapeo de campos en un esquema virtual [1]. En este sentido los directorios virtuales poseen un mayor nivel de flexibilidad dado que no tienen que realizar el almacenamiento de los datos en un repositorio central y con esto se elimina la necesidad de tener que implementar procesos de sincronización y replicación de datos entre servicios de directorios.

Otra diferencia es que los directorios virtuales son más flexibles al momento de integrar la información almacenada en las diferentes fuentes de información. Por lo general, se puede incluir repositorios tales como servicios de directorios, bases de datos y otras fuentes integradas por medio de tecnologías de integración tales como Web Services.

Gestión de identidades. Como se ha mencionado anteriormente, las organizaciones actuales cuentan con un número significativo de aplicaciones y sistemas que son utilizadas por los diferentes actores para la realización de las tareas propias de sus cargos. Por lo general, cada aplicación maneja su propio repositorio con la información de las cuentas de usuario, lo que se

transforma en múltiples cuentas y contraseñas para un mismo usuario en diferentes aplicaciones. La gestión de identidades permite gestionar el ciclo de vida de las identidades de los usuarios dentro de la organización, tales como empleados, terceros y socios de negocios. En este sentido, permite gobernar la creación, desarrollo y eliminación de las entidades y sus atributos dentro de un repositorio unificado de identidades. En general, este proceso se compone de:

- Diseño de la identidad digital

Una identidad digital es un objeto que contiene una serie de datos o atributos que describen de manera única a una persona o cosa, conocido también como sujeto o entidad, y también contiene información de la relación del sujeto con otras entidades.

Para el diseño de una identidad digital es necesario realizar un inventario de los diferentes atributos o características que componen un usuario en término de las aplicaciones y sistemas desplegados dentro de la organización. Esto con el fin de evitar manejar información redundante y garantizar que la información de los usuario se mantiene actualizada, es confiable y cumple con una serie de políticas de seguridad definidas para el conjunto de identidades y de acceso a los recursos organizacionales.

Luego de contar con el inventario de atributos se realiza una evaluación de gestor de identidades y de los repositorios que interactúan con este para realizar el mapeo de atributos inventariados y realizar la extensión del esquema para la incorporación de nuevos atributos y clases de objetos, por medio de los cuales se realiza el almacenamiento de la identidad digital de los usuarios. En este sentido, se busca que la identidad de un usuario sea única y que en todos los repositorios conectados con el gestor de identidades se maneje la misma información actualizada de cada uno de los usuarios.

En la Figura 3 se muestra el modo como se estructura la información que compone la identidad digital de un usuario.

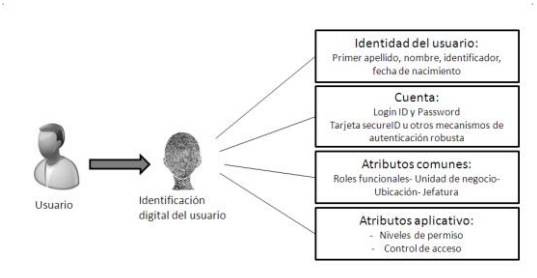


Fig. 3: Identidad Digital [1]

En este caso, se cuenta con:

- Atributos propios de la identidad del usuario tales como nombres, apellidos, número de documento de identificación, entre otros.
- Atributos comunes, tales como roles funcionales, unidad de negocio a la que pertenece, entre otros.
- Atributos propios de la cuenta tales como *login*, *password* y atributos que identifican el mecanismo de autenticación usado.
- Atributos a nivel de aplicación, tales como niveles de control de acceso, etc.

- Gestión del ciclo de vida de las identidades

Las identidades siguen un ciclo de vida asociado con la relación del usuario y la organización. Dicho ciclo de vida se compone de las siguientes etapas:

1. *Creación*: en esta etapa se realiza la creación de la identidad digital del usuario y sus atributos. La creación se puede realizar de diferentes formas: (1) por un administrador de forma manual o automática por medio de flujos de reconciliación con fuentes de autoridad, por ejemplo la nómina; (2) por medio de una solicitud de creación, la cual debe ser aprobada por un usuario administrador y se realiza de forma manual o por medio de flujos de trabajo y (3) creada por el usuario mismo a través de una consola de autoservicio.

2. *Aprovisionamiento*: por medio del aprovisionamiento se le asigna al usuario una serie de recursos dentro de la organización. Un recurso se puede entender como una cuenta de correo, un teléfono celular, la activación del acceso a una aplicación o un sistema, la tarjeta de acceso a un edificio, entre otros. En el caso de una aplicación o sistema se realiza la propagación de la identidad del gestor de identidades hacia la aplicación o sistema.

   Por medio de la asignación de recursos automática basada en políticas de acceso se busca que cuando el nuevo empleado inicie sus labores tenga todos los recursos, permisos y accesos necesarios para la ejecución de las labores asociadas al cargo, incrementando de esta manera la productividad.

3. *Mantenimiento*: en esta etapa se realiza el manejo de las novedades que pueda tener una identidad de un usuario en el tiempo de permanencia dentro de la organización. De este modo, la identidad del usuario puede cambiar con el tiempo, ya sea porque hay cambio en los atributos, por ejemplo cambia la dirección de residencia, se le asignan nuevos roles derivados de nuevas funciones o por cambios en el cargo desempeñado, entre otros.

   El mantenimiento de las identidades dentro de una organización es una de las actividades que más costos puede acarrear dado que son actividades, por lo general, desarrolladas por un área de soporte. Un ejemplo de esto son las actividades de desbloqueo y reseteo de contraseñas de las cuentas de los usuarios. En este sentido, mientras más actividades desarrolle el usuario final, más ahorros se van a producir debido a que el número de llamadas y de incidencias en la mesa de ayuda van a disminuir.

4. *Des-aprovisionamiento*: El des-aprovisionamiento se puede dar porque las funciones del usuario dentro

de la organización no ameritan el uso de un determinado recurso asignado, se da un cambio en el cargo y las funciones relacionadas o porque la relación del usuario con la organización termina, en este último caso es de igual importancia que el aprovisionamiento. Una insuficiencia para manejar el des-aprovisionamiento de cuentas dentro de la organización puede conllevar a brechas de seguridad derivadas en accesos no autorizados, ya sea por el mismo usuario luego de haber abandonado la organización o personas que sepan de este hueco de seguridad, fraude o robo de información por parte de personas con mala intención.

- Definición de mecanismos de aprovisionamiento y sincronización

Los mecanismos de aprovisionamiento y reconciliación permiten que la información fluya entre las fuentes de autoridad, el gestor de identidades y los repositorios de información de las aplicaciones y sistemas dentro de la organización.

En esta etapa es necesario definir el sentido en el que fluye la información de las identidades de los usuarios a través del ciclo de vida: (1) Fuentes de autoridad, que son los repositorios de información en donde se dan los cambios en las identidades de los usuarios y desde las cuales se replican los cambios a los de más repositorios. Por ejemplo: la base de datos de la nómina, un gestor de identidades, la base de datos de recursos de humanos, entre otros, (2) aprovisionamiento, que implica que la información viaja en un solo sentido desde la fuente de autoridad hacia el repositorio de información. En este caso, se produce el aprovisionamiento cuando una identidad es replicada del gestor de identidades hacia un servicio de directorios o el repositorio de identidades de una aplicación y (3) sincronización, que implica que el gestor de identidades ejecuta una tarea programada por medio de la cual realiza la sincronización de cambios producidos en un repositorio de información o fuente de autoridad en un lapso de tiempo determinado. En este caso se maneja una marca de tiempo que indica cuando fue la última vez que se realización de la sincronización.

- Definición de los mecanismos de autenticación

Gestión de roles: en la gestión de roles se gestiona el ciclo de vida de los roles asociados a los diferentes usuarios al interior de la organización. En este escenario se identifican dos tipos de roles: (1) Roles de negocio, que determinan el lugar del usuario dentro de la jerarquía organizacional y (2) Roles de aplicación, definidos en el ámbito de las aplicaciones y sistemas empresariales y que permite la asociación de permisos sobre los recursos.

Existen dos enfoques para relacionar los roles de negocio con los roles de aplicación: (1) Top – Down, que se parte de lo general para llegar a lo particular. En este caso se parte de los roles de negocio y para cada uno de ellos se realizar el inventario de las funcionalidades de cada aplicación que necesita acceder. Cada funcionalidad se relaciona con permisos, los cuales a su vez están asociados a roles de aplicación y (2) Button-Top, que se parte de lo particular para llegar a lo general. En este caso se parte de los permisos que se requieren para acceder las funcionalidades de las aplicaciones o sistemas de la organización, estos permisos se asocian roles de aplicación, los cuales a su vez por medio de políticas bien definidas se asocian a roles de negocio.

Por medio de la gestión de roles se busca garantizar que cada usuario recibe las autorizaciones que corresponden al rol de negocio y a las funciones desempeñadas dentro la organización mejorando los aspectos de seguridad y cumplimiento.

La gestión de roles es un componente intermedio que se encuentra entre la gestión de identidades y el control de acceso. Es así como la gestión de identidades se encarga del gobierno de las identidades, la gestión de roles asigna los roles de acuerdo al cargo y funciones del usuario y la gestión del control de acceso se encarga de definir las políticas que regulan el acceso a los diferentes recursos dentro de la organización.

Gestión y control de acceso: la gestión del acceso hace referencia al control, monitoreo y auditoría del acceso a los recursos ya sea por medio de los servicios ofrecidos en la red interna o externa de la organización. Este proceso se basa en la definición de políticas de seguridad que emplean el uso de mecanismos de autenticación, autorización y confianza.

Las políticas son una reflexión de los objetivos de seguridad y del negocio que han sido creados de acuerdo con otras políticas organizacionales que ayudan al cumplimiento de normas y regulaciones.

El control de acceso está relacionado con la responsabilidad que tienen los usuarios sobre el manejo de la información y los recursos. La responsabilidad se divide en tres tipos: (1) Dueños, que son los creadores de la información y recursos y esta responsabilidad puede ser delegada o asignada, (2) Custodios, que son los usuarios encargados de la gestión diaria de la información y los recursos; los custodios son los encargados de velar porque las políticas de acceso son cumplidas y que los usuarios solo pueden acceder los recursos para los cuales se les ha otorgado el permiso y, por lo general, los custodios son los administradores u operadores de las aplicaciones o sistemas y (3) Usuarios, que son personas, grupos, programas o cualquier otra entidad que hace uso de la información y los recursos.

El principio del menor privilegio está basado en la idea de que el usuario no debe recibir más accesos a los recursos de los que realmente necesita para la realización de sus funciones. En el proceso de autenticación se realiza la validación de que el usuario

si sea quién dice ser. Por medio de la autenticación se responden las preguntas ¿quién eres? y ¿cómo sé que puedo confiar en ti? Éste proceso se realiza por medio de la validación de las credenciales de usuario [11].

Dentro del mundo digital existen varios mecanismos de autenticación de usuario o más común mente conocido como factores de autenticación: (1) Algo que se sabe, lo que se basa en datos o información que el usuario conoce, por ejemplo una contraseña, (2) Algo que se tiene, y que se basa en algún tipo de objeto que el usuario posee, por ejemplo un *token* o un certificado digital, (3) Algo que se es, que se basa en el uso de dispositivos biométricos que ayudan a validar algunas de las características fisiológicas del usuario, por ejemplo el iris, las huellas digitales, el tono de la voz, rasgos faciales, entre otros y (4) cualquier combinación de las tres anteriores. Mientras más factores de autenticación tenga el sistema más seguro será. Los esquemas de autenticación más usados son:

Cookies: son archivos manejados por los navegadores Web, que permiten almacenar datos básicos del usuario y sirven de enlace entre transacciones que son difíciles de conectar por cualquier otro medio. Uno de los ejemplos más comunes es el uso de cookies en carritos de compra o en tiendas online para recordar los artículos consultados y adicionados por el usuario para su posterior compra. Las cookies son usadas como mecanismo de identificación del usuario a través de diferentes sesiones.

Muchas aplicaciones Web utilizan cookies como mecanismo adicional para verificar que el usuario se ha autenticado previamente y posee una sesión activa. En otros casos, se utilizan las cookies como un elemento de apoyo para la implementación de una funcionalidad de single *sign-on* para diferentes aplicaciones que funcionan en un mismo dominio de red.

Usuario y contraseña: que es el mecanismo más comúnmente utilizado para la autenticación de los usuarios, lo que ha conllevado a la proliferación de cuentas de usuario dado el número de aplicaciones que un usuario debe acceder para la ejecución de sus tareas dentro de la organización.

Este esquema es un claro ejemplo de un factor de autenticación de nivel 2 porque se cuenta con un nombre de usuario —algo que se tiene— y con una contraseña —algo que se sabe—, pero en este caso el nombre de usuario es un dato público —cualquier persona lo puede saber— y por tal razón este esquema de autenticación es tan débil como un factor de autenticación de nivel 1.

Una problemática que surge de este esquema es el gobierno de las contraseñas y la necesidad de implementar políticas que regulen su uso en las aplicaciones y sistemas desplegados en la organización. De este hecho se desprende lo siguiente:

- Las contraseñas fáciles de recordar son débiles y fáciles de vulnerar.
- Las contraseñas seguras son difíciles de recordar.
- El manejo que se le da a las contraseñas en muchos casos no es el adecuado, por ejemplo, muchos usuario para recordar la contraseña de varios sistemas las mantienen anotadas en un papel que lo pegan al frente del monitor.
- La implementación de políticas de contraseñas en diferentes aplicaciones, las cuales cada una cuenta con su repositorio de usuarios y contraseñas es difícil de realizar.

Esta problemática es abordada por la gestión de identidades, en la cual se busca consolidar la información de los usuarios en un repositorio unificado e implementar políticas de contraseñas robustas, pero fáciles de manejar para los diferentes usuarios de los sistemas dentro de la organización.

Certificados digitales: basados en criptografía de llave pública, en el cual una entidad certificadora avala la identidad del usuario contenida dentro del certificado digital. Este es un método que no ha tenido mucha acogida por las siguientes razones:

- La infraestructura para el manejo de los certificados digitales es compleja y muy costosa.
- Los certificados digitales deben ser manejados de forma segura por el usuario final. Además cada cierto tiempo deben ser renovados.
- En comparación con otros métodos, los certificados digitales son más difíciles de manejar para el usuario final y requieren un conocimiento más avanzado.

Dispositivos biométricos: que se basan en el reconocimiento de características fisiológicas propias de cada persona. Como se había mencionado anteriormente, por medio de éstos se pueden reconocer rasgos faciales, huellas dactilares, características del iris, geometría de la mano, características de la voz…,

La principal ventaja de un mecanismo de autenticación biométrica, es que ésta está basada en características propias del sujeto, lo que hace que su vulneración sea más complicada, pero de acá surge la principal desventaja, una vez vulnerada la característica, el método queda inservible. Otra desventaja es que hay personas que no se encuentran dentro del conjunto de los patrones estándares que reconoce el dispositivo biométrico haciendo que para estos caso no se pueda realizar su aplicación.

Tokens: se realizan por medio de dispositivos que se encargan de generar una serie de dígitos aleatorios que el servidor de seguridad es capaz de validar. El uso de tokens va por lo general acompañado de un usuario y una contraseña. En este sentido este es un mecanismo de factor dos “Lo que se sabe+ lo que se tiene”.

Existen varios modelos y mecanismos de control de acceso:

Control de acceso discrecional: es definido por el Trusted Computer System Evaluation Criteria, documento definido por el departamento de defensa de los Estados Unidos, como un mecanismo de restricción del acceso a recursos basado en la identidad del sujeto y/o los grupos a los cuales pertenece. En este método, al custodio se le da la posibilidad de decidir a cuales usuarios se les otorga el acceso. Una vez otorgado, el usuario se puede convertir en un custodio del recurso y a su vez puede otorgar el acceso a otros usuarios. La principal desventaja de este mecanismo es que no se puede tener una administración centralizada de los permisos de acceso a los recursos ya que estos dependen del usuario. Un ejemplo de la implementación de un mecanismo de acceso discrecional son las listas de control de acceso ACL por sus siglas en inglés.

Control de acceso mandatorio: En este, el dueño de la información define la política y los custodios y usuarios están en la obligación de cumplirla. En este, los usuarios no pueden sobrescribir o modificar la política.

Control de acceso basado en roles (RBAC): Este control se basa en la idea de que a los usuarios se les otorga el permiso de acceso a los recursos basado en los roles que posee. Este mecanismo cuenta con dos características importantes: (1) Todos los accesos son controlados por medio de los roles asignados al usuario. En este esquema a los diferentes usuarios se les asigna un conjunto de roles y el dueño del recurso se encarga de definir permisos, los cuales a su vez se relacionan con los roles y (2) Los roles pueden ser definidos de forma jerárquica, es decir, un rol puede ser miembro de otro rol, lo que implica que cuando a un usuario se le asigna un determinado rol este recibe la asignación de los roles que son miembros del rol asignado. Esto se muestra en la Figura 4, donde un usuario con rol de arquitecto recibe además los permisos asignados al de ingeniero.

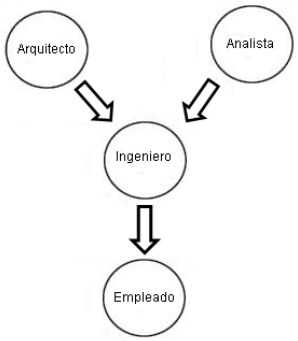


Fig. 4: Jerarquía de roles [1]

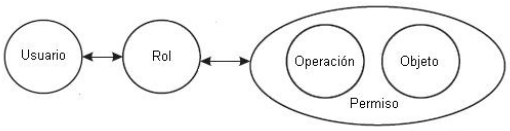
Un esquema de autorización basado en roles se basa en las siguientes tres reglas: (1) A todos los usuarios se les debe asigna un rol. Si a un usuario no se le asigna ningún rol, éste no podrá realizar ninguna acción relacionada con el acceso a los recursos, (2) Para que un usuario pueda hacer uso de los permisos asociados a los roles asignados, éste debe realizar el inicio de una sesión por medio de la cual se da la activación de los roles que le han sido otorgados y (3) Un usuario puede realizar solo las acciones para las cuales ha sido autorizado por medio de la activación de los roles.
Con RBAC, los administradores de las aplicaciones y sistemas crean los roles de acuerdo a las funciones realizadas en la organización, otorgan permisos a esos roles y asignan los usuarios a los roles de acuerdo a las responsabilidades y tareas que debe desarrollar.

Una de las ventajas del uso de RBAC es que el control y mantenimiento de las políticas de acceso se manejan de una manera centralizada, lo que garantiza flexibilidad, separación de tareas, seguridad en el acceso a los recursos y a la información y que los usuarios cuentan solo con los permisos de acceso a los recursos de acuerdo a las funciones asignadas dentro de la organización.

Como tal, la asignación de roles según las funciones desempeñadas por el usuario, requieren de la identificación de las diferentes funciones o cargos dentro de la organización, la especificación del conjunto de privilegios que se requiere para desempeñar cada función y la configuración de las políticas que regulen el acceso de los usuario a los recursos basado en los privilegios asignados.

En la Figura 5 se muestra una esquematización las políticas de control de acceso. En esta figura se puede notar que en la configuración de una política de control de acceso se integran los siguientes elementos:

- Usuarios asociados a los roles.
- Roles a los cuales se les asignan los permisos.
- Permisos. Estos se definen como una operación que se puede realizar sobre un determinado objeto. En esta figura se da un ejemplo claro, en donde la creación (operación) de un reclamo (objeto) puede ser realizada por un cliente (rol).



Política de control de acceso

Objeto	Operación	Rol
Reclamo	Crear	Cliente
Reclamo	Visualizar	Operador Soporte
Reclamo	Visualizar	Cliente
Reclamo	Modificar	Operador Soporte

Fig. 5: Esquematización política control de acceso [4]

4. ARQUITECTURA EJEMPLO

En los puntos anteriores se analizaron los diferentes componentes que integran una solución de gestión de identidades y control de acceso [9]. A continuación se ilustra la forma en la cual los diferentes componentes interactúan entre sí para dar como resultado una arquitectura integrada, robusta y confiable. En la Figura 6 se muestra una arquitectura básica de gestión de identidades y control de acceso.

- Fuentes de autoridad: Compuesta por la nómina y recursos humanos. En estos repositorios de aplicaciones se almacena la información de los usuarios y son los encargados de disparar los eventos dadas las novedades de contratación, terminación de contrato, vacaciones, incapacidades, licencias, etc. Por ejemplo, cuando se contrata un empleado, se almacena en una tabla de eventos la información del usuario para ser creada en el gestor de identidades y replicada en los demás sistemas. Para el caso de las vacaciones se almacena en la tabla de eventos la información del usuario para indicarle al gestor de identidades que dicha cuenta se debe deshabilitar en un determinado período y a su vez realizar la des-habilitación en las diferentes aplicaciones y sistemas.

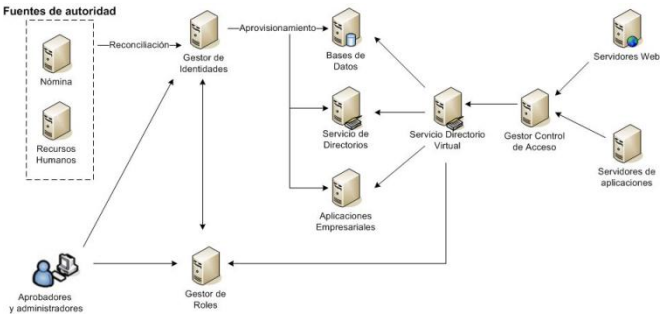


Fig. 6: Arquitectura básica de gestión de identidades y control de acceso [9]

- Gestor de identidades: En este se gestiona el ciclo de vida de las identidades de usuario y se realizan los procesos de reconciliación (sincronización) con las fuentes de autoridad y aprovisionamiento con las aplicaciones y sistemas empresariales integrados con la solución de gestión de identidades y control de acceso. Por ejemplo, cuando se contrata a un empleado, por lo general, el primer acceso que se debe configurar es el acceso a la red, el cual se logra por medio de la creación de una cuenta de usuario en el servicio de directorios corporativo. Si dicho usuario es un administrador de base de datos, la cuenta de usuario debe ser creada en el motor de base de datos que va a administrar.

- Gestor de roles: En este se gestiona la información de los roles y dicha información es sincronizada con la identidad del usuario en el gestor de identidades. En este se crean reglas y condiciones por medio de las cuales se define si un determinado usuario puede o no pertenecer a un determinado rol. Además algunos gestores de roles ofrecen la posibilidad de realizar análisis y detectar cuando se dan violaciones a las reglas y condiciones.

- Servicio de directorio virtual: Por medio de este servicio se crea un directorio virtual en donde se expone de forma unificada la identidad de los usuario teniendo en cuenta que dicha información se puede encontrar en diferentes repositorios, por ejemplo, las cuentas de los empleados se pueden cargar del servicio de directorios corporativo y los diferentes roles asignados se pueden cargar de una base de datos que es donde el gestor de roles almacena dicha información. De manera similar las cuentas de usuario proveedores y externos se pueden cargar de un servicio de directorios adicional en donde se almacene esta información.

- Gestor control de acceso: En este componente se realiza la configuración de las políticas de control de acceso tomando la información de usuarios y roles consolidada en el servicio de directorios virtual.

- Servidores Web y de aplicaciones: En estos servidores se realiza la instalación de agentes que permiten proteger las aplicaciones aquí desplegadas. Estos agentes se comunican con el gestor de control de acceso y obtienen la información de las políticas creadas.

5. CASOS DE ÉXITO

A nivel latinoamericano varias empresas en su necesidad de mitigar algunas de sus necesidades tecnológicas han invertido tiempo y capital en soluciones de Gestión de identidades y control de acceso obteniendo buenos resultados, mejorando la calidad y minimizando la administración de los procesos de recepción de control de acceso, esto conlleva a una notable reducción de costos a nivel de administración de identidades. A continuación algunos casos de éxito reales.

5.1 Sector financiero: DAVIVIENDA

Esta entidad bancaria con el fin de sopesar varias de sus necesidades tecnológicas implementó una solución de Identity and Access Management y de esta manera logró cumplir con los siguientes aspectos:

- Integrar las aplicaciones en una sola y única plataforma, de esta manera los empleados de la entidad bancaria podrían acceder a los diferentes aplicativos de manera rápida y segura
- Asegurar el cumplimiento de sus políticas de seguridad
- Mejorar la administración de la gestión de identidades, tanto de los empleados como de los clientes
- Reducción de la carga de trabajo en el área de gestión de identidades a un 60%.
- Autoservicio a los usuarios.

5.2 Sector pensiones y cesantías: ING

Con la implementación de una solución de Gestión de identidades ING mejoró el aprovisionamiento de usuarios facilitando la gestión de identidades de los usuarios, mejorando la operación de las autorizaciones de las personas para acceder a los activos de información, simplificando procedimientos de acceso y mejorando las actividades de gobierno de seguridad y cumplimiento regulatorio.

5.3 Sector comunicaciones: CLARO

Con el fin de reducir la carga operativa que generaban los clientes Claro decidió contratar una solución de Identidades IAM, realizaron una prueba de concepto y evaluaron casos de implementación exitosa en el

sector. El manejo de identidades está siendo automatizado por medio de la solución de IAM, de esta manera mejora la eficiencia de los procesos.

6. CONCLUSIONES

A lo largo de este documento se han presentado las principales características de la gestión de identidades y control de acceso y cómo una solución de este tipo apoya a las organizaciones para el desarrollo de nuevas estrategias, cumplimiento de normas y regulaciones y proveer el acceso seguro a la información y los recursos. La implementación de una solución de gestión de identidades y control de acceso requiere una inversión considerable de tiempo, dinero y recursos como también una serie de cambios en los procesos organizacionales. El retorno de inversión es palpable a través de una serie de factores tales como:

- Gestión unificada del ciclo de vida de las identidades acorde con las novedades presentadas en los sistemas de nómina y recursos humanos.
- Aprovisionamiento y des-aprovisionamiento adecuado en aplicaciones y sistemas empresariales.
- Asignación eficiente de roles y permisos de acceso de acuerdo al cargo y funciones desempeñadas por el usuario al interior de la organización.
- Control efectivo del acceso a los recursos tanto en intranets como en *extranets* por medio de la definición de políticas de acceso acorde con las políticas de seguridad de la organización.
- Disminución de la carga operativa en la mesa de ayuda en los temas relacionados con la gestión de las cuentas de usuario, desbloqueo y cambio de contraseñas.
- Recolección oportuna de la información necesaria para la elaboración de informes de auditoría y cumplimiento.
- Disminución de costos en tareas relacionadas con la administración de usuarios, roles y políticas de acceso.

Como tal, una solución de gestión de identidades y control de acceso puede presentar una serie de desventajas relacionadas con la implementación y el cambio organizacional que esta requiere, pero comparadas con los beneficios que se pueden obtener y las mejoras en los procesos organizacionales, dichas desventajas no representan un factor de decisión y más bien se pueden transformar en aspectos a tener en cuenta para lograr una implementación exitosa.

7. REFERENCIAS

[1] P. J. Windley. "Digital Identity". O´Reilly, 2005

[2] J. Scheidel. 2010. "Designing an IAM Framework with Oracle Identity and Access Management". McGraw Hill.

[3] H. L. Corbin. "IAM Success Tips: Planning & Organizing Identity Management Programs". CreateSpace, 2008.

[4] J. Edward; Sr. Coyne & J. M. Davis. "Role Engineering for Enterprise Security Management". Artech House, 2007.

[5] T. A. Howes; M. C. Smith & G. S. Good. "Understanding and deploying LDAP Directory Services". Addison-Wesley, 2003.

[6] D. A Grier. "The Value of a Goog Name". *IEEE Computer*, Vol. 43, No. 6, pp. 7-9, 2010.

[7] D. R Kuhn; E. J. Coyne & T. R. Weil. "Adding Attributes to Role-Based Access Control". *Computer*, Vol. 43, No. 6, pp. 79-81, 2010.

[8] D. F Ferreiolo & D. R Kuhn. "Role-Based Access Controls". *Proceedings National Computer Security Conference*, pp. 554-563, 1992.

[9] M. B. Polman. "Oracle Identity Management Governance, Risk and Compliance Architecture". Auerbach Publications, 2008.

[10] A. Jason. "The Basics of Information Security: Understanding the fundamentals of InfoSec in Theory and Practice". Syngress, 2011.

[11] D. Todorov. "Mechanics of User Identification and Authentication: Fundamentals of Identity Management". Auerbach Publications, 2007.