GESTIONAR CENTRALIZADAMENTE LAS IDENTIDADES EN ORGANIZACIONES

Amaya Pérez, Edel José.
edeljose@gmail.com
Universidad Piloto de Colombia.

Abstract*—This document describes the concepts related to the centralized management of identities and the different components and processes that comprise it are explained, further emphasizing the importance that this practice has been taking in today's organizations also seeks to exalt the problems they is 're faced with not having a tool to centrally manage all tasks of government organizational identity , in addition to this are listed some of the manufacturers and the various solutions they offer today to meet this need that increasingly takes more relevance to the areas of IT organizations today.*

Resumen*—En este documento se explican los conceptos relacionados con la gestión centralizada de identidades así como los diferentes componentes y procesos que lo conforman, adicionalmente se resalta la importancia que esta práctica ha venido tomando en las organizaciones actuales, además se busca exaltar la problemática a la que se enfrentan estás, al no contar con una herramienta que permita administrar centralizadamente todas las tareas de gobierno de identidad organizacional, además de esto se listan algunos de los fabricantes y las distintas soluciones que estos ofrecen en la actualidad, para suplir esta necesidad que cada vez toma más relevancia en las áreas de TI de las organizaciones actuales.*

Keywords*—Security, identity management, Internet, access control, user authentication, user authorization, protocols, directories, technology, software, applications, technological tools, user management, role management, segregation of duties.*

Palabras clave*—Seguridad, gestión de identidades, Internet, control de acceso, autenticación de usuarios, autorización de usuarios, protocolos, directorios, tecnología, software, aplicativos, herramientas tecnológicas, gestión de usuarios, gestión de roles, segregación de funciones.*

I. INTRODUCCIÓN

Vivimos en un mundo donde la tecnología, a través de los tiempos ha conseguido un avance y un crecimiento desmesurado, lo que la ha llevado a convertirse en un factor de alta importancia para las organizaciones actuales, a la vez ha generado un sin número de desafíos y situaciones a las que se han tenido que enfrentar las personas, empresas de todos los sectores y a su vez las áreas de TI con el fin de mantenerse a la vanguardia, contrarrestar el impacto de los riesgos a los que se encuentran expuestos, poder brindar servicios de calidad de forma eficiente y efectiva.

Así como los avances que ha presentado la tecnología en general, también hemos sido testigo del esfuerzo y compromiso permanente que han realizado organizaciones de diferentes tipos como fabricantes de hardware, software, organismos de estandarización, por apoyar con el desarrollo de dispositivos, herramientas, estándares y normas, que han permitido a las áreas de TI, mejorar la seguridad de los sistemas, eliminar las complejidades de los procesos, gestionar adecuadamente los activos, cumplir requerimientos legales, establecer políticas, agilizar los procesos vitales de las organizaciones y brindar los elementos que permitan ubicar las áreas de TI como el gran aliado estratégico que permite apoyar el cumplimiento de los objetivos del negocio.

En esta búsqueda de mejorar y agilizar los procesos y debido al crecimiento de los servicios en TI, resulta inevitable hablar y documentarse de un tema de altísima importancia para el funcionamiento adecuado de cualquier organización y muchísimo más para las áreas de TI como lo es la administración de la identidad y el control de acceso.

Sin duda alguna la tecnología es el soporte de cualquier empresa en el día de hoy, no importa la industria en que se encuentre o los productos y servicios que venda su funcionamiento está ligado a la correcta ejecución de diferentes aplicativos. Bajo esta premisa no todos los desarrolladores de aplicaciones (de las múltiples que existen en el mercado) tienen en cuenta la integración de protocolos de seguridad de terceros, basándose como, por ejemplo, en protocolos de autenticación propios, lo cual genera brechas de

seguridad al obligar al usuario común a tener diferentes métodos de autenticación para diferentes aplicaciones.

Definición Gestión de identidades

Se puede definir la administración de identidades como todo un conjunto de políticas y procesos organizacionales que busca facilitar y controlar tanto el acceso físico a las instalaciones, como a los sistemas de información, siendo en definitiva la última instancia de acceso a todos los recursos corporativos.

II. ANTECEDENTES

Las diferentes organizaciones cada día han basado su negocio en un mundo digital, donde las herramientas tecnológicas son las encargadas de soportar la actividad diaria de todos los empleados y procesos. Una parte de este soporte digital está representado en aplicativos como CRM, ERP, correo electrónico y demás en donde su principal factor de seguridad es la autenticación basada en usuario y contraseña.

Muchas de estas aplicaciones son desarrolladas con el fin de tener diferentes métodos de autenticación entre ellas la denominada autenticación local o basada en formulario, este tipo de autenticación consiste en que los sistemas o aplicaciones proporcionan sus propias interfaces de usuario para el inicio de sesión, así mismo, contiene sus propios métodos para realizar la respectiva validación de las credenciales de acceso, sin embargo, en estos métodos no se soportan los diferentes protocolos de autenticación existentes, los cuales aportan mejores niveles de seguridad a los diferentes sistemas.

Al existir aplicativos que no cumplen con los requerimientos mínimos de seguridad en el acceso, autorización de usuarios y mucho menos utilizan un único sistema de autenticación basados en una única llave de ingreso a los sistemas por lo que se crea una gran brecha de seguridad al obligar a los diferentes usuarios de aplicaciones a tener varias credenciales de autenticación.

Todas las organizaciones a través de los años se han enfrentado a diferentes retos relacionados con la gestión a adecuada de los usuarios, así mismo hemos sido testigo de los avances y esfuerzos realizados por los diferentes fabricantes y entidades de estandarización, quienes han puesto al servicio de las áreas de TI un sin número de herramientas, soluciones de software y hardware que han facilitado la gestión de accesos y roles para los diferentes tipos de usuarios.

En el marco de esta evolución vale la pena destacar que en un inicio las organizaciones no disponían de procedimientos o políticas de gestión de accesos e identidades, ni mucho menos de sistemas que permitieran realizar esta importante labor de forma automática.

Con el paso del tiempo y debido a la problemática causada por la inefectividad en la realización de tareas relacionadas con la gestión adecuada de las identidades, surgieron herramientas que en un principio suplían la necesidad de gestionar independientemente los diferentes procesos relacionados con el control de acceso, como por ejemplo, el desarrollo e implementación de protocolos de autenticación, entendiendo que este es un aspecto fundamental de la seguridad de los sistemas, validar correctamente la identidad de cualquier tipo de usuarios que intenta iniciar sesión en un dominio, aplicación o a los recursos de infraestructura TI como redes y servidores[5], los protocolos de autenticación son un tipo de protocolo criptográfico que tiene como fin único autenticar entidades que pretenden establecer una comunicación de forma segura a una red o sistema de información.

Debido al surgimiento y evolución de los protocolos de autenticación aparecen también los sistemas basados en directorios, los cuales surgen como un aporte al componente de servicios de información de identidades, como un ejemplo a este componente podemos mencionar el protocolo LDAP (Protocolo compacto de acceso a directorios), el cual permite administrar directorios, es decir, acceder a bases de cuentas y usuarios de una red mediante protocolos TCP/IP, LDAP se encuentra estandarizado y en su tercera versión y actualmente se ha utilizado masivamente para el manejo de cuentas y le ha brindado a las diferentes áreas de TI, los métodos para poder conectarse, desconectarse, buscar, realizar comparaciones, insertar nuevas entradas, cambiar entradas y eliminarlas dentro del directorio.[4]

Luego del surgimiento de las tecnologías y mecanismos que facilitan la gestión centralizada de las identidades, también se empiezan a encontrar en el mercado las distintas soluciones, aplicativos y procesos que buscan el cumplimiento de los siguientes objetivos dentro de la organización: [1]

- Los usuarios tengan acceso a los sistemas y funcionalidad requerida para el desarrollo de sus funciones.
- Se controlen adecuadamente los accesos a información sensible y los conflictos de segregación de funciones.
- Se verifique que los usuarios correspondan a la persona a la que están asociados.
- Se tenga un entendimiento de los procesos para agregar, cambiar y eliminar accesos.
- Se tenga disponibilidad permanente de la información de los accesos utilizados.

Una vez entendido los objetivos de una solución informática para la gestión de identidades, se puede tomar como ejemplo la robusta solución denominada Administración de Identidades y Acceso (Identity and Access Management - IAM), la cual fue desarrollada e implementada por la entidad PWC PricewaterhouseCoopers, quienes ofrecen sus servicios en Colombia desde el año 2000, esta herramienta busca el cumplimiento de los objetivos de una gestión centralizada de identidades mencionados anteriormente, sus principales ventajas y funcionalidades se describen en la siguiente imagen.[1]

Figura 1. Principales beneficios de un sistema de gestión de identidades [1]

Esta imagen es una fiel explicación de la gestión adecuada de las identidades ya que cumple con los objetivos principales de un sistema de estas características, en resumen, ayuda a la reducción de los costos ya que la cantidad de recursos humanos y administrativos se reduce gracias a la gestión automática de cuentas de usuarios, ayuda al cumplimiento de la regulación nacional, así mismo aporta en el incremento de la seguridad de las organizaciones, ya que aporta en temas importantes como la segregación de funciones y gestión adecuada del acceso y roles de usuarios.

Además, un sistema de las dimensiones y ventajas como IAM, es capaz de aumentar la productividad en la empresa, mejorando los tiempos de respuesta en el proceso como el aprovisionamiento de cuentas, de esta manera contribuye en la mejora de la experiencia de los usuarios finales tales como empleados, proveedores, socios.

Adicionalmente para aclarar un poco más el esquema de funcionamiento de este tipo de aplicativos, donde se toma como inicio los usuarios que generalmente interactúan y mantienen una relación directa con la organización, estos actores son gestionados por medio de la herramienta y de esta manera se garantizan los diferentes componentes básicos como la autenticación, autorización, gestión de cuentas y de directorios de usuarios, con esto se facilita y se garantiza la asignación de los roles y privilegios para las diferentes aplicaciones como por ejemplo, los sitios web, ERPs, y demás aplicativos existentes en la organización donde se lleve a cabo su implementación, la siguiente imagen describe el proceso y funcionamiento del sistema IAM[1]:

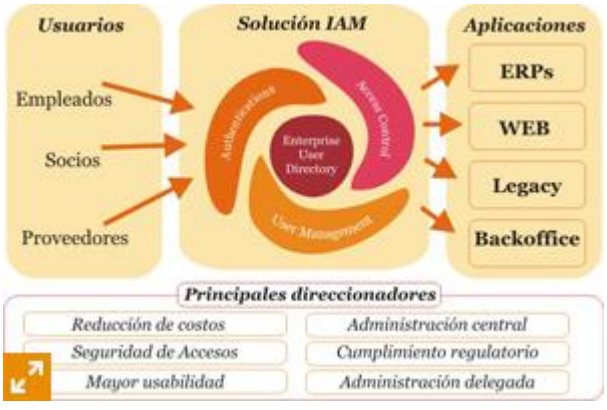

Figura 2. Componentes de un sistema de gestión de identidades [1]

Una vez entendido el esquema de funcionamiento de los sistemas centralizados de gestión de identidades, resulta importante explicar que además de garantizar un proceso adecuado de su funcionamiento se debe adoptar una metodología la cual permita por medio de la experiencia durante las diversas implementaciones realizadas en diferentes tipo de organizaciones, al igual que los diferentes casos de éxitos, lo cual conlleva a integrar los diferentes elementos requeridos para el análisis, definición, e implementación efectiva de la solución de administración centralizada de identidades y accesos, la siguiente imagen muestra la metodología utilizada en el producto IAM tomado como ejemplo en este artículo:

Figura 3. Metodología de un sistema de gestión de identidades [1]

Esta metodología toma como elementos primordiales lo siguientes ítems y requisitos para la adecuada implementación del producto IAM [1]:

- Repositorio corporativo de identidades: que es la base para la correcta implementación ya que proporciona los diferentes actores y usuarios que intervienen o mantienen algún tipo de relación con la organización.
- Definición de fuentes autoritativas: este ítem proporciona las diferentes herramientas o procesos que gestionan la gobernabilidad de los datos e información en las diferentes áreas que posee la organización.
- Definición de roles y políticas: este ítem proporciona al sistema la definición de las políticas organizacionales en cuanto a la definición de los privilegios y roles de los diferentes actores en cada uno de los aplicativos con los que estos interactúan dentro de sus funciones.
- Automatización del aprovisionamiento de cuentas: en este ítem e establece el proceso adecuado para el aprovisionamiento y des aprovisionamiento de cuentas de usuarios en las diferentes aplicaciones, permitiendo toda la gestión de ellas por medio de un sistema de directorio único y centralizado
- Establecimiento de mecanismos de control de acceso: este ítem controla que usuario y tienen permitido el acceso a los diferentes aplicativos o herramientas dentro de la organización permitiendo segregar las funciones dependiendo del rol del usuario en cada sistema.

La solución o producto de gestión de identidades que se implemente en la organización también debe proporcionar un modelo de madurez que permita visualizar la evolución en el tiempo, es decir, que debe proporcionar las herramientas y métodos para identificar el estado actual d y el deseado de la organización, con la implementación del sistema, a continuación se muestra el modelo de madurez que proporciona el producto IAM para garantizar el mapa de ruta a seguir con las organizaciones donde se implementa la herramienta:

Figura 4. Modelo de madurez de un sistema de gestión de identidades [1]

El modelo básicamente toma como punto de inicio la autenticación, por lo que garantiza que la solución de gestión de identidad cuenta son los diferentes métodos para integrarse con las diferentes aplicaciones y llevar cabo la autenticación de los usuarios, la autorización, gestión de privilegios, gestión de usuarios, alimentar las diversas fuentes de autoritativas, y además debe garantizar el cumplimiento de las diferentes normativas a las que se rige la organización.

III. PROBLEMA

La mayoría de organizaciones actuales y en especial las unidades de TI se enfrentan en su día a día con el aumento desmesurado de la cantidad de usuarios de distintos tipos, y la complejidad de la gestión de los privilegios de acceso para estos usuarios, lamentablemente, en su gran mayoría todos estos inconvenientes son ocasionados por la administración manual e independiente de los procesos de aprovisionamiento, gestión y asignación de privilegios, todos estos procedimientos tienden a ser poco coordinados, lo que conlleva a una gestión muy deficiente de la administración de identidades en las organizaciones, lo que termina exponiendo en gran medida a altos costos y riesgos de seguridad, y a su vez genera un alto grado de insatisfacción en la prestación de los servicios de TI y por ende en la productividad de los recursos humanos.[2]

Con miras a lograr la eliminación de la ineficiencia causada por la gestión manual e independiente de las identidades en las organizaciones resulta necesario implementar mecanismos de automatización de todo el ciclo de vida de identidad de los usuarios, estas soluciones de gestión de identidad aglutinan todo un conjunto de herramientas que ayudan a establecer la política corporativa de gobierno de identidad en las organizaciones, y ayudan a mitigar y resolver un gran número de problemáticas como las que se describen a continuación.

A. Pérdida de seguridad.

Un factor de alto impacto en la organización y la cual origina la gran mayoría de las problemáticas, las cuales se derivan de la falta de control en los procedimientos de gestión efectiva de la identidad, un alto porcentaje de los incidentes y eventos son ocasionados por empleados descontentos, o por cuentas huérfanas de empleados que ya no se encuentran vinculados a la organización. [6]

B. Incumplimiento de normativas

Todas las organizaciones sin importar su tamaño tienen la obligación de cumplir las normativas de controles internos, además de someterse a las reglamentaciones legales de su país, el no gestionar adecuadamente los datos de los usuarios puede ocasionar fuertes sanciones o pérdida de prestigio en el mercado. [6]

C. Incremento de los costos

El no contar con una solución de gestión de identidad siempre va a generar mayor dedicación de recursos a la administración de las cuentas de usuarios, en algunos casos las organizaciones terminar pagando licencias a usuarios que ya no están vinculados, o en algunos casos no gestionar adecuadamente los datos asume costos relacionados al incumplimiento de regulaciones. [6]

D. Reducción de la productividad

Siempre que la gestión de usuarios se realice de forma independiente ocasiona retrasos en el proceso de aprovisionamiento de cuentas y gestión de privilegios, lo que genera malestar en los usuarios finales afectando la calidad del servicio. [6]

E. Pérdida de calidad de los datos

El desorden ocasionado por la gestión independiente de identidades conlleva a mantener información inconsistente entre los diferentes sistemas y aplicaciones, ya que usuarios mantendrían roles y privilegios heredados de cargos anteriores lo que aumenta la probabilidad de incidentes de seguridad, que podrían generar un alto impacto en los servicios de la organización. [6]

IV. SOLUCIÓN

En el mercado actual se pueden encontrar diferentes fuentes de identidad que permiten realizar la administración de identidades de forma independiente en las organizaciones, de las cuales se pueden destacar soluciones como el directorio activo, sistemas de recursos humanos, bases de datos independientes, aplicaciones a la medida, software de terceros o tan simple como el uso de cuentas locales en sistemas operativos Windows, Linux, o Unix, sin embargo, gestionar independientemente las identidades conlleva un desgaste administrativo, un desorden en la

asignación de privilegios y a su vez aumenta los riesgos asociados al control de accesos de los usuarios y gestión adecuada de los roles dentro de las organizaciones.

El contar con una solución para la gestión centralizada de identidades en las organizaciones garantiza que todos los usuarios obtengan y el nivel de acceso adecuado a aquellos recursos protegidos, igualmente permite reducir costos administrativos gracias a la gran mayoría de procesos automatizados para los controles de seguridad que ofrecen este tipo de herramientas, permitiendo de esta manera cumplir las reglamentaciones de ley y simplificando los procesos de cumplimiento de las auditorias

De acuerdo a las mejores prácticas entregadas por los diferentes fabricantes y personal de seguridad resulta importante resaltar que la administración de identidades dentro de una organización debe contemplar en definitiva los siguientes componentes:

F. Control de acceso

Componente que se encarga de la gestión y configuración de las políticas, estándares, autenticación, autorización, Single Sign-On (SSO)/Reduced Sign-On, definición de roles empresariales y de aplicación, así como el acceso a información sensible / Segregación de funciones. [1]

G. Administración de usuarios

Este componente abarca procedimientos como el aprovisionamiento de usuarios, análisis y aprobación de acceso, administración delegada, autoservicio, administración de activos físicos y la gestión de contraseñas de acceso. [1]

H. Servicios de información de identidades

Componente de la gestión de identidades encargado de la definición y normalización de directorios y repositorios, así como la sincronización de los datos. [1]

I. Auditoría y cumplimiento

En este componente se establecen los mecanismos para la revisión de los registros de logs de accesos y eventos. [1]

J. Servicios federados

Este componente administra las autorizaciones a socios y proveedores externos, permitiendo establecer una relación de confianza entre la organización y sus contactos externos. [1]

Para lograr la solución a las problemáticas ocasionadas por la falta de una adecuada gestión de identidades en las organizaciones se debe hacer uso de soluciones informáticas que agrupen todos los componentes y funcionalidades que permitan a la organización realizar las actividades de gestión de identidad desde un punto único.

En la actualidad existen un sin número de fabricantes y herramientas que proporcionan el servicio de gestión centralizada de las identidades, podemos encontrar soluciones gratuitas de código abierto (Open Source), entre las cuales se puede resaltar la aplicación WBSVision, esta herramienta fue desarrollada en al año 2008 por la empresa española WhiteBearSolutions, y es una muy completa solución de gestión y federación de identidades, incluye servicios de directorios, servicios de autenticación y seguridad, servicios de red, así mismo permite provisionar y controlar el acceso de usuario a los diferentes recursos, repositorios y aplicaciones, en base a perfiles, roles y reglas de negocio definidas en la organización, en definitiva esta es un muy buena opción pensando en sus bajos costos de implementación y soporte.[6]

Además de las soluciones Open Source, también en se encuentran en el mercado una gran cantidad de soluciones de carácter propietarios, que, dependiendo de las ventajas funcionales, de uso, facilidad en la implementación y diversificación en la integración con los sistemas y aplicaciones externas varían tanto los costos y tiempos de puesta en servicio además del producto IAM que se tomó como referencia para explicar los componentes y procesos de una solución de este tipo, se realiza a continuación una breve descripción algunos fabricantes y las soluciones de gestión de identidad que ofrecen actualmente [3]:

A. CA Technologies

Este fabricante de mucho prestigio, ofrece la herramienta denominada Secure Cloud IDaaS solution, y ofrece una completa suite de gestión de identidad. [3]

B. IBM

Este fabricante ofrece también su sistema de gestión de identidades denominado IBM Security Identity Manager, proporciona y automatiza toda la gestión de usuarios y privilegios. [3]

C. Microsoft

El producto llamado Microsoft identity manager, el cual ofrece un servicio Premium de Microsoft basado en la nube Azure Active directory.

D. Oracle

La herramienta bandera de Oracle para la gestión de identidad se llama Oracle Identity Governance (OIG), y es una completa suite que centraliza la seguridad de las aplicaciones y servicios web, además proporción un solo punto de contacto para el soporte. [3]

E. SAP

Ofrece varias soluciones para la gestión de identidades y el control de acceso y resulta una alternativa viable para las organizaciones que utilizan los productos SAP, ya que ofrece una excelente integración con toda la suite de productos SAP. [3]

F. Salesforce.

Es la solución ofrecida por Salesforce que permite el control de acceso y privilegios, además es ofrecida dentro de la oferta de servicios en la nube. [3]

Todos los fabricantes y herramientas descritas anteriormente ofrecen diversas formas de cumplir con la necesidad puntual de contar con un sistema que permita gestionar centralizadamente las identidades en las organizaciones, la decisión final de cuál de estas utilizar está en la realización de una revisión exhaustiva de las facilidades de integración con las aplicaciones propias de cada organización, así mismo se deben valorar otros aspectos como el tamaño de la organización, la cantidad de datos críticos que esta procese, o el presupuesto que se tenga dispuesto para este fin.

V. CONCLUSIONES

Tomando como referencia que, en la actualidad, para cualquier organización, sin importar su tamaño, resulta muy necesario el uso e implementación de un sistema de gestión de identidades, ya que este proporciona un sin número de beneficios a las áreas de TI y a la organización como tal.

Sin embargo, este tipo se soluciones no se encuentran totalmente extendidas en todas las organizaciones esto debido al gran número de obstáculos que no han facilitado el acceso a este tipo de herramientas, las dificultades han sido de diversos tipos, tanto externas como por ejemplo el alto costo de la implementación por parte de los fabricantes de las soluciones propietarias, o de tipo interno como carecer de un marco estructurado de las políticas de identidad organizacional.

Otras barreras que han impedido una expansión globalizada de las soluciones son los altos tiempos requeridos para la implementación y despliegue de las soluciones, o incluso los recursos tecnológicos necesarios para su funcionamiento, como por ejemplo Sistemas operativos licencias de bases de datos, servidores web.

No obstante, a pesar de las dificultades que conlleve su implementación las organizaciones en general deben orientar sus esfuerzos en la puesta en marcha de su sistema de gestión de identidad, ya que con esto logran solucionar todas las problemáticas asociadas a los altos costos de administración o a la falta de seguridad, además que con la implementación de la solución pueden cumplir las diferentes regulaciones.

Por ultimo destacar que si los problemas son de carácter económico se puede evaluar el uso de las herramientas de código abierto, que cumplen en gran proporción los objetivos de la gestión centralizada de las identidades.

VI. REFERENCIAS

[1] PricewaterhouseCoopers Colombia, "*Administración de Identidades y Accesos (Identity and Access Management - IAM)*", Disponible en: http://www.pwc.com/co/es/servicios/consultoria/tecnologia/administracion-de-identidades-y-accesos.html.

[2] CA, *Administración de identidades y accesos basada en contenidos*, Disponible en: http://www.ca.com/~/media/Files/SolutionBriefs/latam/CS1930_Content-Aware_IAM_SB_0212_LAS.pdf.

[3] Solutions Review, *Identity and Access Management Solutions Directory*, Disponible en: http://solutionsreview.com/identity-management/identity-management-solutions-directory.

[4] CCM, *Protocolo ligero de acceso a directorios (LDAP)*, Disponible en: http://es.ccm.net/contents/269-protocolo-ldap.

[5] MICROSOFT, *Introducción a los protocolos de autenticación*, Disponible en: https://msdn.microsoft.com/es-es/library/cc739177(v=ws.10).aspx.

[6] WBSGO, *Por qué implantar un sistema de gestión de identidad open source*, Disponible en: http://www.whitebearsolutions.com/por-que-implantar-un-sistema-de-gestion-de-identidad-open-source-wbsvision.