RETIRO Y AUTOGESTIÓN DEL USUARIO EN ALMACENES DE CADENA CON DIRECTORIO ACTIVO

Juan F. Hincapié Z.
Universidad de San Buenaventura
juanfdohz@gmail.com

Rodolfo A. Marín G.
COTRAFA
rmarin@cotrafa.com.co

Jerry A. Murillo C.
Universidad de San Buenaventura
jealmuco@gmail.com

(Tipo de Artículo: **Reflexión**. Recibido el 25/11/2012. Aprobado el 27/12/2012)

RESUMEN
Los almacenes de cadena son organizaciones en donde el personal es numeroso, diverso, de alta rotación y alto retiro; además la gran variedad de negocios que tienen tales organizaciones, hacen que posean muchas aplicaciones a las cuales muchos usuarios deben ingresar y en la mayoría de veces éste acceso se vuelve administrativamente costoso. Por tanto se hace necesario el establecimiento de un procedimiento informático (administración de usuarios) que permita al propio usuario gestionar sus contraseñas y que además le permita a la organización controlar la desactivación automática de los accesos al momento del retiro (terminación de contrato) del usuario. Para lograr esto existen variedad de herramientas en el mercado que satisfacen dicha necesidad, pero su implementación y soporte es demasiado costoso; por eso este artículo pretende mostrar algunos conceptos importantes y la manera en que otras herramientas y metodologías pueden realizar un adecuado proceso de autogestión y retiro del usuario en los almacenes de cadena a un menor costo.

Palabras clave
Almacenes de cadena, autogestión, contraseñas, desactivación automática**,** directorio activo, dominio, empleados, interconexión, LDAP, proceso, script, retiro de usuario, soporte, servicio web.

DISENGAGEMENT AND SELF-MANAGEMENT OF USERS IN RETAILERS HAVING ACTIVE DIRECTORY

ABSTRACT
Retailers are companies where the staff is large and diverse; there is high turnover and high disengagement. Because of their wide variety of businesses, these companies have many applications which are accessed by many users representing most of the times high costs administratively. Therefore it is necessary establishing a data-processing (user management) that allows to the user managing his passwords and that also allow to the company to take control of the automatic turn-off of the access when user disengages (contract termination). To achieve this there are variety of tools on the market that meet this need, but their implementation and support are too expensive; for this reason this article tries to show some important concepts and the way other tools and methodologies can perform adequate self-management process and user disengagement in retailers at a lower cost.

Keywords
Retailers, active directory, automatic disabling, domain, employees, interconnection, LDAP, organizational unit, password, process, user disengagement, script, Self-Management, support, web services.

DESENGAGEMENT ET AUTOGESTION DES USAGERS DANS HYPERMARCHES QU'UTILISENT REPERTOIRE ACTIF

Résumé
Les hypermarchés sont des entreprises avec beaucoup de personnel, qui est divers, de haute rotation et haute désengagement ; à cause de la grande variété de ses affaires, ces entreprises ont beaucoup de logiciels sur lesquels les usagers doivent se connecter et la plupart du temps cet accès devient couteux d'après le point de vue administratif. Par conséquent il est nécessaire d'établir une procède informatique (administration des usagers) qui permette au même usager de gérer ses mots de passe et que permettre a l'entreprise de contrôler le désamorçage automatique des accès dans le moment du désengagement (terminaison du contrat) d'usager. Pour réussir ca il y a variété d'outils sur la marché qui satisfont ces besoins, mais son implémentation et support sont très coûteux, c'est pour ca qui dans cet article nous prétendons de montrer quelques concepts importants et la manière dans lequel des autres outils et méthodologies peuvent réaliser un processus approprié d'autogestion et désengagement des usagers dans les hypermarchés à un coût plus bas.

Mots-clés
Hypermarchés, autogestion, mots de passe, désamorçage automatique, répertoire actif, domaine web, employés, interconnexion, protocole léger d'accès à un répertoire (LDAP), processus, script, désengagement d'usager, support, service de la toile.

1. INTRODUCCIÓN

Cada vez los Sistemas de Información (SI) como bases de datos, sitios Web, servidores de almacenamiento y servidores de archivos, son necesarios y por tanto, en las empresas se debe procurar no olvidar el control que debe tener la administración sobre las actividades realizadas por los diferentes usuarios de los SI.

Ahora bien, el constante cambio y rotación de los empleados de los almacenes de cadena invita a la administración para que esté muy atenta a las funcionalidades y controles que deben tener sus colaboradores. En los almacenes, el perfil de los usuarios es variable y el soporte es altamente demandante siendo necesaria la implementación de herramientas que permitan un manejo adecuado de los usuarios de los aplicativos.

Sin importar la actividad económica, cada organización realiza el ingreso de sus empleados nuevos a los SI, pero un gran porcentaje de estas pasa por alto retirar los usuarios de los empleados que dejan de laborar, colocando en riesgo a la organización, dado que otro empleado puede utilizar dichos accesos y cometer diferentes fraudes o llevar a la indisponibilidad de los SI.

Otra problemática del día a día es la variedad de SI, que lleva a los almacenes de cadena a incurrir en altos costos en la administración de los usuarios; por ejemplo, la probabilidad de que los usuarios olviden sus contraseñas y bloqueen sus cuentas es bastante alta, y en consecuencia los costos en el tema de soporte se convierten en un asunto álgido y de difícil control que puede afectar la continuidad de los servicios en los diferentes puntos de atención.

Al Observar el panorama del flujo de usuarios en los almacenes de cadena, surgen dos preguntas: ¿cómo controlar que los usuarios que salen de la empresa sean desactivados automáticamente de los sistemas de información?, ¿cómo permitir a los usuarios que puedan ellos mismos cambiar sus contraseñas y desbloquear su usuario de una manera segura?, máxime si se tiene en cuenta que la fortaleza empleada en la contraseña y la cantidad de las mismas han hecho que los usuarios se decidan por crear contraseñas sencillas o que las escriban en pequeños recortes cerca al computador e incluso algunos deciden crear archivos maestros de contraseñas [1].

La respuesta a dichas preguntas podría resumirse, en la implementación de un sistema (con el proceso y procedimiento respectivo) que permita realizar un control de todas las personas que se retiran de la organización, así mismo, dicho sistema debe permitir mediante políticas de seguridad una conexión interactiva entre el usuario y sistemas centralizados de autenticación de manera que se puedan minimizar los riesgos de suplantación de identidades y manipulación indebida de información; ahora bien, conocidas las respuestas a la problemática de control de usuarios activos y la autogestión de las contraseñas y cuentas de usuario, surgen otros interrogantes ¿qué empresas cuentan con la implementación de estos sistemas de información?, ¿cuentan las empresas con la infraestructura necesaria para la implementación de estos sistemas?, ¿qué costo genera dicha implementación?, entre otra cantidad de situaciones.

Con todo el contexto se puede afirmar que existen diferentes empresas en el mercado que manejan dichas soluciones y que son llamadas comúnmente (Identity Management), entre las cuales se encuentran multinacionales de amplio reconocimiento como IBM, Oracle, Novell, Computer Associates. Cada una de ellas brinda la posibilidad de manejar las identidades de una manera muy completa, pero que implica para las organizaciones tener que incurrir en altos costos de implementación y soporte.

Pero, ¿toda esa costosa tecnología es capaz por sí sola de realizar las actividades que permitan minimizar el riesgo que tienen los Almacenes de Cadena debido a la alta rotación de los usuarios?

2. SISTEMAS DE GESTIÓN DE IDENTIDAD

Un sistema de gestión de identidades (idM por sus siglas en inglés – identity management) se refiere a cómo las personas o empleados se identifican, autorizan y administran en una o varias redes informáticas; incluye la manera en que a los usuarios se les genera una identidad, la protección de la misma, la tecnología de soporte a dicha protección y la interacción con distintos sistemas [2].

Es un compendio de procesos de negocio, de infraestructura tecnológica y políticas que permite a los sistemas conectados determinar quién tiene acceso, a que componentes está autorizado, al tiempo que protege la privacidad y el acceso de la información confidencial [3].

Su implementación requiere de cuatro factores principales, la definición de roles, la propagación de las cuentas de usuarios, inicialización del sistema y la integración con sistemas de “Single SignOn” [2]. Pero tal y como se menciona anteriormente la posible implementación de un sistema IdM requiere de inversión alta en implementación y soporte [4].

Los grandes almacenes de cadena pueden llegar a tener entre 30.000 y más usuarios distribuidos en distintas aplicaciones y algunas cadenas de almacenes de corte mediano pueden llegar a tener incluso 8000.

En el siguiente cuadro se observa el valor que tiene la implementación de un sistema de manejo de identidades de las casas fabricantes Novell y Oracle, donde se incluye todo el proceso de soporte, implementación, actualización y licenciamiento.

Consideraciones: los valores son proyectados a 5 años y los valores son en dólares [4].

Massive= 40 mil usuarios.
Largue= 8 mil usuarios.

Tabla 1. Costos Sistema de Gestión de Identidades Novell y Oracle [4]

	Novell IAM			Oracle IAM		
	Massive	Large	Medium	Massive	Large	Medium
5 Yr TCO w/o User Training	$ 5,225,703.96	$ 2,518,732.40	$1,677,616.48	$ 6,745,802.22	$ 3,477,426.68	$2,137,845.27
5 Yr TCO w/ User Training	$ 21,066,973.80	$ 5,726,589.54	$2,865,711.72	$ 30,512,468.89	$ 8,290,176.68	$3,920,345.27
	Massive	Large	Medium	Massive	Large	Medium
Licensing	$ 1,085,000.00	$ 395,416.67	$ 145,797.62	$ 1,159,375.00	$ 427,187.50	$ 172,187.50
Average / user	$ 27.13	$ 52.72	$ 58.32	$ 28.98	$ 56.96	$ 68.88
Maintenance	$ 231,640.00	$ 84,141.67	$ 30,748.81	$ 231,875.00	$ 85,437.50	$ 34,437.50
Summary						
First Year	$ 1,316,640.00	$ 479,558.33	$ 176,546.43	$ 1,391,250.00	$ 512,625.00	$ 206,625.00
Subsequent Years	$ 231,640.00	$ 84,141.67	$ 30,748.81	$ 231,875.00	$ 85,437.50	$ 34,437.50
Five Year PV	$ 2,119,297.06	$ 758,246.21	$ 269,941.31	$ 2,095,535.38	$ 795,604.84	$ 325,954.57
	Massive	Large	Medium	Massive	Large	Medium
Entry-level servers	9.10	5.25	15.45	10.50	6.50	7.80
Mid-level servers	10.83	9.36	5.50	12.00	8.29	3.33
High-end servers	9.67	-	-	9.50	6.00	1.33
Five Year PV	$ 122,683.33	$ 31,461.11	$ 30,300.00	$ 126,050.00	$ 68,700.00	$ 24,133.33
	Massive	Large	Medium	Massive	Large	Medium
Contractor	$ 135.35	$ 135.35	$ 135.35	$ 164.17	$ 164.52	$ 165.95
ProServ Firm	$ 192.16	$ 192.16	$ 192.16	$ 190.00	$ 190.00	$ 190.00
Vendor Engineer	$ 210.94	$ 210.94	$ 210.94	$ 216.67	$ 216.67	$ 216.67
Reported Total Hours	12,460	5,710	4,785	11,232	1,668	2,378
Internal Hours	4,038	2,121	1,686	5,254	2,205	1,373
Contractors	7,220	3,687	2,939	9,453	4,703	3,667
Engineering	385	99	67	2,130	1,438	188
Sum Total	11643	5907	4692	16837	8345	5228
Services Fees	$ 1,263,508.73	$ 624,664.09	$ 495,360.32	$ 2,135,527.78	$ 1,145,061.98	$ 693,312.70
	Massive	Large	Medium	Massive	Large	Medium
Upgrades						
Contractor Hours	219.22	219.22	219.22	454.00	454.00	454.00
Cost of Upgrades / Patches	$ 42,125.54	$ 42,125.54	$ 42,125.54	$ 86,260.00	$ 86,260.00	$ 86,260.00
Five Year PV	$ 177,448.11	$ 168,195.08	$ 151,853.15	$ 363,358.50	$ 344,411.17	$ 310,948.00
	Massive	Large	Medium	Massive	Large	Medium
Audit reports						
Hours / year	54.08	54.08	54.08	301.60	301.60	301.60
Cost of Reporting	$ 2,163.12	$ 2,163.12	$ 2,163.12	$ 12,064.00	$ 12,064.00	$ 12,064.00
Five Year PV	$ 9,111.84	$ 8,636.70	$ 7,797.55	$ 50,817.96	$ 48,168.05	$ 43,488.02
	Massive	Large	Medium	Massive	Large	Medium
Administrator Salaries	$ 1,144,358.83	$ 841,637.93	$ 683,877.54	$ 1,359,189.38	$ 926,308.73	$ 684,907.48
Administrator Training	$ 10,990	$ 8,506	$ 7,637	$ 21,108	$ 15,086	$ 11,587
Cost of downtime	$ 358,766.81	$ 68,861.93	$ 23,026.40	$ 553,624.95	$ 106,263.13	$ 35,532.79
Cost of Upgrades / Patches	$ 177,448.11	$ 168,195.08	$ 151,853.15	$ 363,358.50	$ 344,411.17	$ 310,948.00
Cost of Reporting	$ 9,111.84	$ 8,636.70	$ 7,797.55	$ 50,817.96	$ 48,168.05	$ 43,488.02
Present Value of 5 Years of Operations Costs	$ 1,700,675.11	$ 1,095,837.39	$ 874,191.22	$ 2,348,099.13	$ 1,440,236.79	$1,086,462.95

Se puede observar que el costo en 5 años para los grandes almacenes de cadena puede oscilar entre **1´700.000** USD y **2´350.000** USD.

Si se considera que los márgenes de rentabilidad del retail (Almacenes de cadena) son relativamente bajos [5] comparados (2,2% en promedio) con otros sectores, como por ejemplo, el de la telefonía celular en donde la principal empresa obtuvo un margen aproximado del 26% en el año 2011 [6]; se encuentra entonces que incurrir en esos altos costos de tecnología hace que sea bastante difícil.

En consecuencia, innovar con un "económico" desarrollo que permita controlar los usuarios retirados de la organización y que su vez permita la autogestión de usuarios para desbloqueo y actualización de la contraseña, permitirá a dichas organizaciones ahorros importantes que aportan al no deterioro de sus indicadores financieros y a disminuir los incidentes de pérdida de dinero e información por parte de la utilización no autorizada de usuarios ya retirados.

3. ASPECTOS IMPORTANTES

A continuación una mirada a algunos aspectos importantes a tener en cuenta en el desarrollo del software con el que se puede innovar en los almacenes de cadena y en otras organizaciones.

3.1. Costos

Los valores que se deben invertir en la implementación, soporte, actualización y licenciamiento entre otros, de un sistema práctico y sencillo "desarrollado en casa" "in house", el cual entre sus componentes posee interfaces, archivos planos y Web Services, los cuales son herramientas menos costosas en su puesta en marcha y en su mantenimiento.

El desarrollo y puesta en marcha de un sistema in house, está diseñado para soportar todos los usuarios que tengan interacción con los servicios soportados por los servidores del Directorio Activo, al igual que los que pueda soportar la aplicación de gestión humana (GH) que para el caso planteado a continuación se habla de un aproximado de 40 mil usuarios.

Tabla 2. Costos sistema propio de retiro y autogestión de usuarios (inhouse)

Costos de mano de obra, costos de implementación, soporte, actualizaciones, licenciamiento herramienta Web Services.

Mano de Obra	8400
Instalación de servicios web services	5000
Actualizaciones	3000
Mantenimiento y control	10000
Total USD	**26400**

Como se puede apreciar en la Tabla 1 y la Tabla 2 la diferencia en los costos es bastante considerable, aunque es importante anotar que las herramientas de Oracle y Novell son más completas que la solución propuesta en el presente artículo, pero si bien es cierto que lo que se pretende controlar es la autogestión del usuario y la desactivación del usuario cuando ya no haga parte de la empresa, con dicha herramienta se puede gestionar al usuario en estos dos aspectos.
A continuación una explicación de cómo podría ser la función de retiro de usuarios del aplicativo propio (inhouse).

3.2. Manejo del retiro del usuario

Las herramientas de gestión humana (existentes en todas las organizaciones, sobre todo para temas de nómina y prestaciones sociales) tienen la posibilidad de enviar o compartir toda la información de acuerdo a las necesidades del solicitante, por tanto, son características fundamentales de éstas herramientas los campos que relacionan a un individuo (empleado interno o externo) con las distintas funciones que realizan en la empresa y a su vez los campos que documentan el ingreso y retiro del empleado.

Además de las herramientas de GH, debe existir la herramienta tecnológica llamada Directorio Activo la cual permite la creación de usuarios dando acceso a servicios colaborativos y en red, y a distintos sistemas de información acorde a las funciones a desarrollar; esta herramienta es una de las más comunes y usadas por los Almacenes de Cadena, además es el primer servicio donde normalmente se da vida a un usuario de aplicación.

Por lo tanto, hay que interrelacionar el sistema de GH con la herramienta tecnológica de control de acceso a aplicaciones (Directorio Activo) como sistema centralizado, esta interrelación consiste en poder lograr que archivos y procedimientos de gestión humana (empleados retirados) lleguen al directorio activo y éste a su vez valide si los empleados retirados coinciden con algún usuario de este directorio y proceda a realizar la función de inhabilitar. Es importante tener en cuenta que en el directorio activo se está usando el campo ID el cual deberá estar relacionado con el campo "cédula" del sistema de GH. En dicho sistema debe existir un registro muy importante como la fecha en que ingresa el empleado y la fecha fin de su contrato laboral, esta última fecha es también llamada fecha de retiro.

La plataforma de GH debe generar archivos de retirados todos los días, en donde, como propuesta se plantea que genere los retirados de los últimos 30 días, de tal forma que un archivo generado, por ejemplo, el 24 de abril contendrá los usuarios "retirados de la empresa" del 24 de marzo al 23 de abril y podrá tener los siguientes campos, en donde el campo con integridad referencial deberá ser el ID del empleado.

Para que lo anterior sea satisfactorio se propone la siguiente estructura para la interfaz del sistema de GH al Directorio Activo (DA):

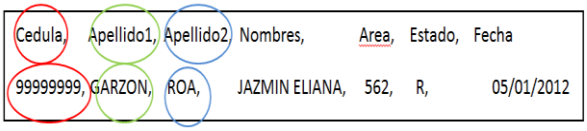

Fig. 1. Interfaz Sistema Gestión Humana.

Esta interfaz está destinada exclusivamente al retiro de usuarios, los campos área, estado y fecha son características propias del sistema de GH.

En la raíz del Directorio Activo se debe crear una Unidad organizacional (Por sus siglas en inglés – Organitacional Unit -OU-) "equipos y usuarios deshabilitados". Una vez generados los archivos por el sistema de gestión humana, deberán ser colocados automáticamente en una carpeta del controlador de dominio, la cual puede ser predeterminada con anterioridad y a continuación se ejecuta con ayuda del programador de tareas el script [7] que se muestra en el apéndice.

Como resultado de la ejecución del Script los usuarios del directorio activo que en el campo "UserDN" coincidan serán deshabilitados, se les quitará los grupos del directorio activo, serán llevados a una OU especial y en un log serán registrados "el usuario, la OU en la que se encontraban y los grupos que tenían

en el momento de ser deshabilitados, se deberán guardar en un archivo diario con los respectivos retiros para así controlar la fecha y la hora en que son retirados dado que el script está programado a una hora especial del día.

Es importante tener en cuenta que el archivo resultante debe ser monitoreado y estar dentro de las actividades de la persona encargada de dicha labor, además de salvaguardar, depurar y gestionar adecuadamente dicho archivo.

Lo anterior demuestra que no sólo el componente tecnológico soluciona el problema, sino que se debe contar con personal de monitoreo que constantemente realice gestión. Además, todos los procedimientos deben estar documentados, oficializados y promulgados para que las tareas no dejen de realizarse.

Comprometer al personal que administra el software de GH y áreas que contratan servicios externos para que en los distintos contratos se establezca la obligación de matricular en el sistema de GH a cada una de las personas que prestarán servicios dentro de la organización, deben ser muy rigurosos con la matrícula de aquellos que requieren acceso a los sistemas de la organización. Deben informar en que momento dejan de prestar servicio en los almacenes de cadena. Y cada empleado antes de retirarse deberá reclamar un paz y salvo. Para el pago de avances y logros en los proyectos, este documento será exigible para personal que deba interactuar con sistemas de información y deberá ser anexado a las distintas facturas de cobro que periódicamente pasa el "tercero, contratista o socio de negocios" para que le sean cancelados sus servicios en virtud del contrato.

El documento deberá relacionar fecha, identificación (cédula), nombre completo y sistemas de información con los que interactúan y si deben seguir o no activos, además, en el caso de que las personas hayan cambiado de área o si han cambiado el uso de uno o varios sistemas deben expresarlo.
La persona encargada de autorizar el pago es el responsable de informar mediante "llamada de servicio al HelpDesk" la inhabilitación de los usuarios o cambio en los sistemas usados por el usuario.

Es importante recordar que el estándar internacional ISO27001, en su anexo de "Objetivos de control y Controles" en su apartado A.8.3 "Terminación o cambio de cargo" propone que: "los derechos de acceso de todos los empleados, contratistas y usuarios de terceras partes a las instalaciones de procesamiento de información y la información, deberán ser retirados a la terminación de su cargo, contrato o acuerdo, o deben ser ajustados al cambio."

3.3. Autogestión del usuario

Se debe tener presente que gran parte de las llamadas al "help desk" tiene que ver con bloqueo, desbloqueo y reseteo de contraseñas, y por tanto, es de esperar que el procedimiento que se propone baje ese número de llamadas en un 87%, es decir, con el sistema "inhouse" implementado sólo se recibirán en el help desk un 13% del total de llamadas por el concepto.

Para reducir los niveles de llamadas al help desk por los motivos anteriores, se propone la creación de una aplicación Web que se encargará de recoger la información de la persona que tiene problemas con su usuario y una vez validada la información el usuario, puede proceder a colocar la contraseña que desee, siguiendo los requisitos de creación de contraseñas que se tengan parametrizados en el directorio activo. La aplicación Web usará un "Web Services" para ir al sistema de GH a consultar la información del usuario y para hacer la respectiva gestión en el directorio activo.

La comunicación entre el directorio activo y el Web Service ha de realizarse haciendo uso del Protocolo ligero de acceso a directorios (LDAP, por sus siglas en ingles), el cual es utilizado para leer y escribir en el Directorio Activo. Para lograr que esta comunicación sea segura y confidencial se utiliza la tecnología Capa de sockets seguros (SSL) - Seguridad de la capa de transporte (TLS). Esto se hace mediante la instalación de un certificado con un formato correcto de una entidad emisora de certificados (CA) de Microsoft.
El Web Services se encarga de recoger la información digitada por el usuario (Cédula y Usuario del Directorio Activo), luego consulta en el sistema de gestión humana, los datos correctos del usuario y a su vez trae otros datos de forma aleatoria (sistema reto-respuesta); estos son presentados al usuario en forma de "selección múltiple", dicho usuario deberá responder adecuadamente los datos que le pertenecen, además para mejorar las medidas de seguridad se puede adicionar que el usuario deba llenar alguna palabra o frase para que en la próxima ocasión sea escrita tal cual como fue escrita la primera vez y si ha escogido de forma acertada, la aplicación Web presenta dos cuadros para escribir y reescribir la contraseña que el usuario desee. El Web Services se encarga de enviar tales credenciales al DA.

En la Fig. 2**,** se muestra la relación entre los componentes de hardware y software a la hora de realizar las respectivas validaciones del usuario a partir de que el usuario solicita el servicio a través del formulario de la aplicación Web.

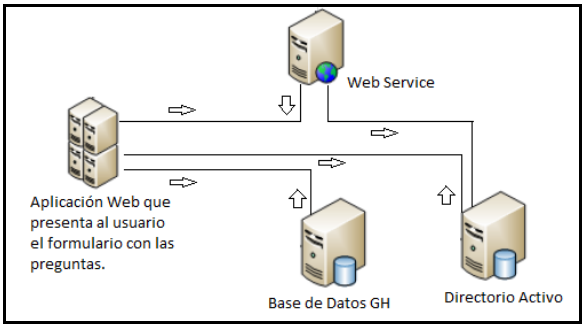

Fig. 2. Flujo de la información en la autogestión.

Con lo anterior se pretende mostrar diversas formas de implementación de sistemas de información que cumplen de alguna manera con ciertas funciones de un manejador de identidades (identity management), con un costo y manejo de ejecución bajo.

Para poder hablar entonces de algunas funciones del manejador de identidades, partimos del hecho que los almacenes de cadena cuentan con una aplicación de GH que registra todo el personal que ingresa a la empresa, igualmente cuentan con un sistema de información donde al personal se le asigna un usuario para el ingreso, por lo tanto se necesita de una herramienta que permita interrelacionar estos 2 sistemas de información y permitir el manejo de los usuarios, que para este caso el manejo propuesto es inactivarlos y que cada persona pueda autodesbloquear y autorenovar la contraseña, de allí que se propone la implementación de un Web Services para dicha interconexión.

El Web Services es un sistema de información seguro y fácil de implementar como lo menciona Javier Vacas Gallego "los Web Services son la mejor alternativa posible ya que posee diversas posibilidades respecto a la integración de la seguridad, así como una complejidad mínima en el tratamiento de los datos. Esto es ideal para una comunicación ágil y eficaz [8].

Web Services recoge información representada en scripts por parte de las 2 aplicaciones, gestión humana y directorio activo, las integra y ejecuta cada función permitiendo como se menciona anteriormente la desactivación de los usuarios en los sistemas de información de la empresa y el cambio de contraseña de los usuarios, adicionalmente se propone que el intercambio de información entre los sistemas de información se realice a través del protocolo de acceso ligero a directorios LDAP v3 que contiene TLS (Transport Layer Security), lo cual permitirá agilidad y seguridad de la información en los 2 procesos que se están planteando de gestión de usuarios.

El Web Services deberá usar la tecnología XML que permite el uso de un conjunto de utilidades que facilitan el acceso a todos los usuarios de forma rápida, sencilla e intuitiva; además al centralizar la función de autogestión en una sola aplicación posibilitará una única fuente documental de controles [9].

En la Fig. 3, se observa cómo sería el proceso que debe llevar a cabo el sistema de autogestión, para lograr que el usuario pueda desbloquearse y crear una nueva contraseña, permitiendo continuar con las actividades sin tener que llamar al "Help Desk".

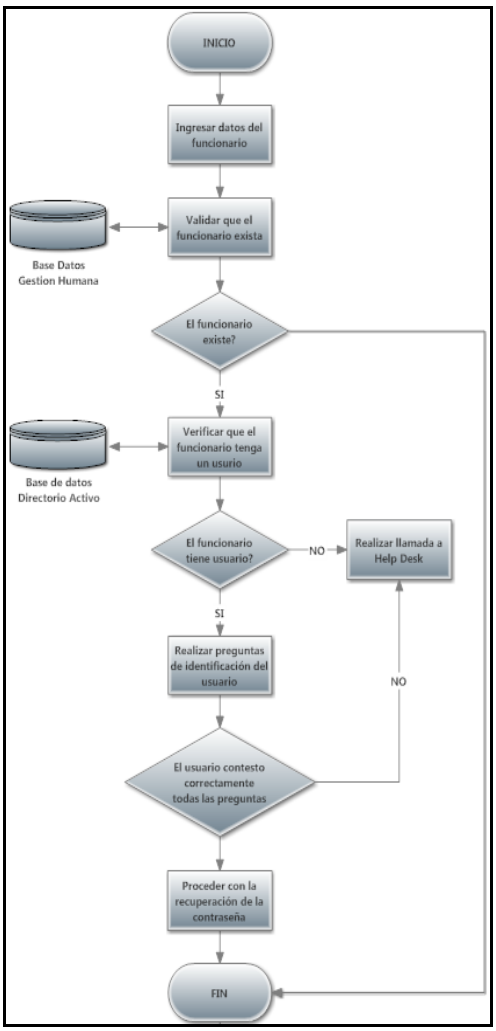

Fig. 3. Flujo de la autogestión para el desbloqueo y cambio de contraseña

4. CONCLUSIONES

El manejo y gestión de usuarios es un tema demasiado delicado y extenso, todos los sistemas de información de las empresas tienen como punto principal: la ejecución de procesos que dan valor a sus actividades económicas, a su vez son los usuarios quienes ejecutan dichos procesos, convirtiéndose en elementos fundamentales para el normal desarrollo de SI.

El sistema de autogestión propuesto pretende reducir el número de llamadas al "Help Desk" facilitando así el aumento de la productividad y la reducción de costos.

La herramienta Web Services permite interconectar SI para lograr un control más efectivo del movimiento de los usuarios en la red de datos de la empresa.

Dentro de este esquema de administración de usuarios el DA es el eje principal, ya que sobre este se encuentra el registro de todos los usuarios.

Con la integración de varias herramientas tecnológicas, DA y Web Services se pueden construir soluciones que pueden sustituir algunas funciones de IdM.

La innovación en las empresas es fundamental, se necesitan otras formas de hacer las cosas y que a su vez generen valor a la compañía.

Que un usuario dependa 100% del “Help Desk” es un inconveniente alto porque los costos antes de disminuir en el tiempo van en aumento, por eso estas herramientas sencillas pueden ser un diferenciador de calidad en el servicio y de valor para la empresa. Para el usuario es mejor dedicar dos minutos al Web Services, que 7 minutos (apro.) tratando de que el analista del Help Desk brinde la ayuda correspondiente.

El retiro de usuarios de forma automática y oportuna ahorra tiempos y dinero a las organizaciones, dado que las explicaciones a las revisorías y auditorías por el no retiro son costosas en esas dos variables, y si a eso le sumamos los posibles fraudes que pueden ocasionarse por el manejo de usuarios que ya no están en la organización, es claro que ahorra dolores de cabeza.

Es importante también mencionar que la tecnología de **IdM**s a pesar de ser tan costosa y de poseer un grado alto de madurez, por sí sola no soluciona la problemática planteada y por lo tanto se hace necesario que todas estas tecnologías tengan un gran componente documental y procedimental que alerte a las personas que de otra manera tienen que ver con los distintos procesos de la organización.

APENDICE: Script que deshabilita usuarios [9]

```
Option Explicit
'On Error Resume Next
Dim strUserDN, objUser, objOU, strNTName, strOUDN, Group, GroupDN
Dim objRootDSE, strDNSDomain, objTrans, strNetBIOSDomain, objgroup
Dim objFSO, strFilePath, objFile, strFileOut, objReportTextFile, Groupmembership

Const ADS_NAME_INITTYPE_DOMAIN = 1
Const ADS_NAME_TYPE_NT4 = 3
Const ADS_NAME_TYPE_1179 = 1
ConstForAppending = 8
ConstADS_Property_Delete = 4

'Creacion del objeto
Set objFSO = CreateObject("Scripting.FileSystemObject")

' Determinar el dominio
Set objRootDSE = GetObject("LDAP://RootDSE")
strDNSDomain = objRootDSE.Get("defaultNamingContext")

'Especifica el archivo de entrada
strFilePath = InputBox("Cual es el nombre del archivo?" &VbCrLf&VbCrLf& _
   "Si el archivo no esta en el mismo directorio del VBS" &VbCrLf& _
      "por favor coloque el pathcompleto.","Usuarios a procesar","Usuarios_a_inhabilitar.txt")
If strFilePath = vbCancel Then
   MsgBox "Cancelado !!."
   WScript.quit
EndIf

'Verificar que el archivo de entrada exista
If Not objFSO.FileExists(strFilePath) Then
   MsgBox "El Archivo" & strFilePath & " no existe. ",_
   vbCritical, "Error"
   WScript.Quit
End If

'Genera log de salida
strFileOut = "salida.txt"
If strFilePath = vbCancel Then
   MsgBox "ProcesoCancelado."
   WScript.quit
End If

'Verifica que el archivo log exista
If Not objFSO.FileExists(strFileOut) Then
   MsgBox "El archivo  SALIDA.txt no existe.  The script will quit now.",_
vbCritical, "Error"
   WScript.Quit
 End If

' Ubicamos la OU a mover los usuarios a inhabilitar.
strOUDN = InputBox ("OU donde va a mover los usuarios procesados...?","Unidad Organizacional",_
   "OU=Equipos y usuarios Deshabilitados," &strDNSDomain)
If strOUDN = vbCancel Then
   MsgBox "Cancelado."
   WScript.quit
End If
'Asociamos a la OU
Err.Clear
Set objOU = GetObject("LDAP://" &strOUDN)
If Not Err.Number = 0 Then
   MsgBox "Por favor verifica la OU,  Proceso cancelado."
   WScript.Quit
End If
' Abrir el archivo de entrada yrecorrerlo.
Set objFile = objFSO.OpenTextFile(strFilePath, 1)

Set objReportTextFile = objFSO.OpenTextFile(strFileOut, ForAppending, True)

Set objTrans = CreateObject("NameTranslate")
objTrans.Init ADS_NAME_TYPE_NT4, strDNSDomain
```

```
objTrans.Set ADS_NAME_TYPE_1179, strDNSDomain
strNetBIOSDomain = objTrans.Get(ADS_NAME_TYPE_NT4)
' Remover  trailing backslash.
strNetBIOSDomain = Left(strNetBIOSDomain, _
Len(strNetBIOSDomain) - 1)
objTrans.Init ADS_NAME_INITTYPE_DOMAIN, strNetBIOSDomain

Do Until objFile.AtEndOfStream
strNTName = Trim(objFile.ReadLine)
  If strNTName<> "" Then
    On Error Resume Next
objTrans.Set ADS_NAME_TYPE_NT4, strNetBIOSDomain& "\"
&strNTName
    If Err.Number<> 0 Then
      On Error GoTo 0
Wscript.Echo "User "&strNTName _
&" not found in Active Directory"
End if
    err.clear
    on Error GoTo 0
'Remover usario de los grupos a los que pertenecia
err.clear
on Error Resume Next
strUserDN = objTrans.Get(ADS_NAME_TYPE_1179)
    Set objUser = GetObject("LDAP://" &strUserDN)
objUser.Put "msExchHideFromAddressLists", True
' 512eshabilitado 514 desabilitado
objUser.put "UserAccountControl", 514
objuser.Put "delivContLength", "1"
objUser.SetInfo
objReportTextFile.write(strNTName)
    Erase GroupMembership
GroupMembership = objUser.GetEx("memberOf")
    For each Group in GroupMembership
GroupDN = Replace(Group,"/","\/")
       Set objGroup = GetObject("LDAP://" &GroupDN)
    objReportTextFile.write(vbtab& objGroup.cn)
    objGroup.PutEx ADS_PROPERTY_DELETE, "member",
Array(strUserDN)
objGroup.SetInfo
       Next
objReportTextFile.Writeline(vbcrlf)
objOU.MoveHere "LDAP://" &strUserDN, vbNullString

EndIf
Loop
Msgbox "Proceso Terminado, revisar por favor"
```


AGRADECIMIENTOS

Los autores agradecen muy especialmente al señor Héctor Fernando Vargas Montoya por la ayuda y dedicación en la corrección de este artículo. Agradecimientos también al señor Oscar Mauricio Sánchez Medina por compartir sus experiencias con respecto al desarrollo de scripts en plataforma de Directorio Activo.

REFERENCIAS

[1] A. Hovav & R. Berger. Tutorial: Identity Management Systems and Secured Access Control, Communications of AIS; Issue 25, p. 5, 2009.

[2] M. K. Srinivasan & P. Rodrigues, "Analysis On Identity Management Systems With Extended State-Of-The-Art Idm Taxonomy Factors," in International Journal of Ad hoc, Sensor & Ubiquitous Computing (IJASUC) Vol.1, No.4, December 2010.

[3] M. Berman & J. Cooper, Identity Management For The Rest Of Us: How To Grow A New Infrastructure, presented at the Educause Mid-Atlantic Regional Conference, Baltimore, MD, 2006.

[4] S. Curtis, The Impact of Total Cost of Ownership in IAM investment Decisions. Rencana LLC. 2010.

[5] FENALCO, Los Grandes Almacenes E Hipermercados En Colombia: "Más Allá De Las Cifras". p. 22, Noviembre 2011.

[6] Comunicación Celular S.A., Balance General al 31 de diciembre de 2011. Online [Agosto. 2012].

[7] O. M. Sánchez M., Analista de Directorio Activo, compilación de distintos scripts. Online [Septiembre. 2012].

[8] J. Vacas, J. Borrell & J. C. Muiño. Arquitectura Corporativa de Web Services. Bellaterra, Junio, 2008.

[9] A. Baldwin, M. Cassasa, Y. Beres & S. Shiu. Assurance For Federated Identity Management, Journal of Computer Security, Vol. 18 Issue 4, p.14, 2010.