PROPUESTA DE DISEÑO DE UN GESTOR DE IDENTIDADES DIGITALES EN EL MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

FRANCISCO JOSE ARIZA PASTOR

Proyecto de grado para optar al titulo
Especialista en Seguridad Informática

Asesor, Ingeniero Álvaro Escobar
Director de la Especialización en Seguridad informática

UNIVERSIDAD PILOTO DE COLOMBIA
ESPECIALIZACIÓN DE SEGURIDAD INFORMÁTICA
BOGOTÁ
2014

Agradecimientos

A Ileana por su paciencia, comprensión y apoyo incondicional.

A mis hijos Valeria y Matías por soportar mi ausencia.

A mis padres y hermanos por su apoyo y aliento a continuar.

A mi asesor, el Ingeniero Álvaro Escobar por su confianza.

CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

LISTA DE CUADROS

RESUMEN

Actualmente el Ministerio de Tecnología de la Información y las Comunicación a través de la oficina de tecnología y la información, otorga accesos en forma independiente utilizando los módulos de seguridad de cada una de las aplicaciones y/o plataformas tecnológicas. Además, el registro de nuevos usuarios se realiza a través de una comunicación formal a través de la mesa de ayuda para aprobación de la oficina de TI, esta forma de trabajo ocasiona que no se lleve un control estricto del ciclo de vida de la gestión de identidad, las cuentas de los usuarios; todo esto trae como consecuencia un incremento en el riesgo sobre la confidencialidad, disponibilidad e integridad de la información del Ministerio. El Ministerio cuenta en la actualidad con 1.100 usuarios y con 13 aplicaciones implementadas.

El presente proyecto propone el diseño de una arquitectura integral de manejo de identidades digitales a través de una solución que brinde un único acceso a los diferentes sistemas de información de la entidad.

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 esta propuesta 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.

1. PROPUESTA DE DISEÑO DE UN GESTOR DE IDENTIDADES DIGITALES EN EL MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

1.1 PLANTEAMIENTO DEL PROBLEMA

El Ministerio de tecnologías de la Información y las Comunicaciones, con el ánimo de crear oportunidades de negocio y ventajas competitivas que le ayuden a obtener el mejor resultado en la comunicación con el ciudadano, ha desarrollado 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.

En la actualidad se cuenta con un sin números de aplicación que soporta el plan de negocio de la entidad, en la cuales se almacenan los datos de los proveedores de redes y servicios de la industria TIC de Colombia, esta información se encuentra distribuida en los siguientes sistemas de información:

- ASMS (Sistema de Gestión del Espectro Radioeléctrico)
- ALFANET (Sistema de flujo de documentos)
- SAGE (Nueva versión del Sistema de Gestión del Espectro Radioeléctrico)
- BDI (Bases de Datos de Investigaciones)
- BDU (Bases de Datos Única de Clientes)
- SEVEN (Sistema Financiero y Administrativo)
- KACTUS (Nómina y Recursos Humanos)
- REGISTROTIC (Registro Único de Operadores – Auraportal)
- REGISTRO POSTAL (Auraportal)
- SER (Sistema Electrónico de Recaudos)
- Cobro Coactivo
- ZAFIRO (expedientes digitalizados)
- Procesos judiciales.

En el momento cada sistema de información maneja formas de autenticación diferentes, control de acceso, seguridad y bases de datos diferentes, lo que ocasiona que cada funcionario realice un ingreso diferente para cada uno de estos aplicativo, ocasionando la

destinación de una parte del presupuesto de la entidad para el sostenimiento de varios funcionarios que realizan la administración de las cuentas de usuario.

Contar con sin números de sistema de información genera una proliferación de usuarios y contraseñas, lo que conlleva a una inadecuada gestión de la seguridad en la entidad.

1.2 PREGUNTA DE INVESTIGACIÓN

¿Es posible implementar un sistema donde los usuarios realicen por única vez el procedimiento de identificación y autenticación para el acceso a los diferentes servicios suministrados dentro de la infraestructura informática del MINTIC?

1.3 JUSTIFICACIÓN

El Ministerio de Tecnología de la Información y las Comunicaciones, hoy debe gestionar un número cada vez mayor de usuarios, aplicaciones, sistemas y puntos de control, al mismo tiempo que debe garantizar el acceso a la información. Esta situación provoca una gestión poco optimizada y con un alto coste de mantenimiento, que se convierte en una pesada enfermedad a la que se debe poner remedio.

La propuesta a desarrollar en el Ministerio de Tecnología de la Información y las Comunicaciones tiene como objetivo promover un modelos de gestión de roles de usuarios, que permita la creación de un solo punto de acceso, para llevar a buen término una gestión eficaz de los sistemas de información, lo que va permitir mantener más seguro el ambiente tecnológico de la entidad.

1.4 OBJETIVO GENERAL

Establecer una propuesta de arquitectura integral de gestión de identidades digitales para la simplificación del proceso de administración de la autenticación y autorización de la seguridad en los sistemas informáticos existentes en el Ministerio de Tecnologías de la Información y las Comunicaciones.

1.5 OBJETIVOS ESPECÍFICOS

1. Determinar las ventajas y desventajas de la implementación de una solución para el manejo de identidades digitales.
2. Realizar una evaluación de las soluciones de gestión de identidades disponible en el mercado.
3. Presentar una arquitectura integral de manejo de identidades digitales.

2. MARCO TEÓRICO

La realidad tecnológica de las infraestructuras que ofrecen soporte a los procesos de tecnologías de la información, instaladas tanto en el sector público como en el sector privado, indica que una parte muy importante de los sistemas únicamente pueden utilizar sistemas basados en contraseñas. No parece, sin embargo, que este obstáculo sea insuperable, y de hecho la industria de las tecnologías de la información ha provisto una serie de soluciones tecnológicas al problema, de las cuales las incluida en la categoría de gestión de la identidad y del acceso son las más completas. Muchas entidades, públicas y privadas, en efecto, se enfrentan al problema de la proliferación de cuentas de usuario y sus correspondientes contraseñas, fenómeno que deriva de la necesidad, impuesta a veces de forma artificial por muchas aplicaciones y sistemas, de tener que disponer de una cuenta de usuario y una contraseña para cada aplicación y sistema con el que se trabaja.

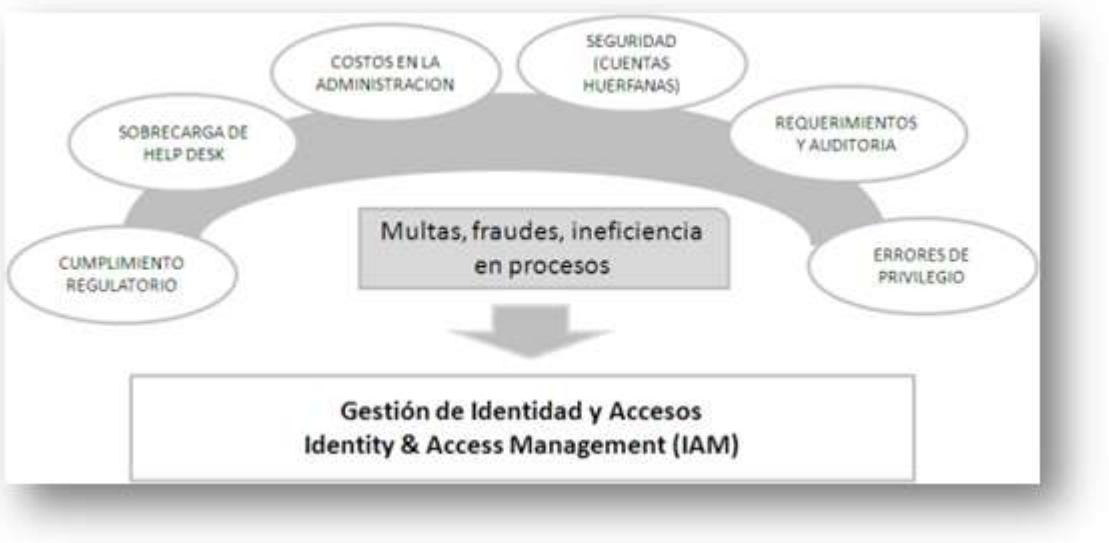
Esta situación resulta difícil de controlar, ya que cada proveedor de la Administración dispone de su propia tecnología, decidiendo si utiliza o no autenticación certificada. Por el contrario, el factor de decisión para la compra del producto ha de ser su funcionalidad y calidad, y no tanto el sistema de autenticación empleado. A esta situación hay que añadir la presión legal que supone la aplicación estricta de las leyes de protección de los datos de carácter personal, que ha obligado a un detallado control de acceso, incrementando aún más la aparición de cuentas de usuario y contraseñas. Curiosamente en estos casos, incluso con aplicaciones nuevas, los proveedores y ésta parece ser también la opinión de algunas Administraciones Públicas, quizá reflejando las opiniones de los técnicos de sector privado apuestan por el uso de sistemas basados en contraseña, y no en certificados, con el argumento de que “no se trata de aplicaciones donde haya que firmar nada”.

En definitiva partimos de la base que los sistemas ya instalados y muchos de los sistemas que se instalarán, precisarán en el futuro aceptar mecanismos de autenticación por contraseña. Por lo anterior es necesario generar mecanismos que permitan identificar el ciclo de vida de los funcionarios dentro de la entidad, para tener el pleno control de la caducidad de las credenciales de los usuarios que acceden a los aplicativos de la organización, lo cual va permitir tener un control total sobre la identidades digitales de los distintos funcionarios, pero para llegar hasta este punto es pertinente promover la políticas necesaria para el desarrollo de un gestor de identidades, el cual va permitir la administración de roles y contraseñas de los usuarios que se crean en la diferentes herramientas tecnológicas que posee el Ministerio de Tecnología de la Información y las Comunicaciones.

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.

Figura 1. Retos de la Entidades Actuales



Fuente P. J. Windley. —Digital Identity . O´Reilly, 2005

2.1 CUMPLIMIENTO REGULATORIO

A diario se implementan nuevas regulaciones que afectan, de una u otra manera, tanto a las entidades públicas como privadas y la forma en la que interactúan con el ciudadano. 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 [2]. 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 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 [3]. 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 [4] 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 [5].

3.1 VENTAJAS

- Los principales beneficios [4] 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 asociado al cargo [6].

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 estructurar nuevamente los 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 [7]. En éste se tienen las siguientes consideraciones:

3.3.1 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 directorio 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 [8], (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.

3.3.2 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.

3.3.3 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.

3.3.4 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:

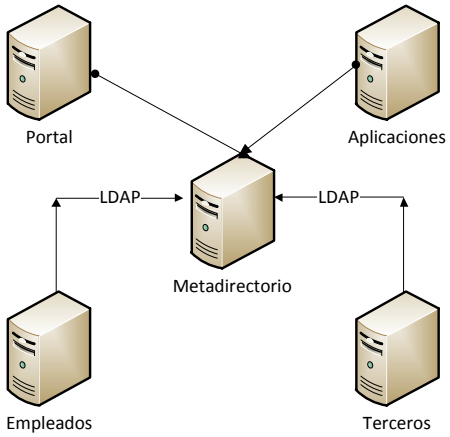
- Definición y diseño de la arquitectura.
- Definición, diseño y normalización del espacio de nombres y la estructura del árbol del directorio.
- Diseño de los mecanismos y procedimientos para la sincronización de los datos con otros servicios de directorios. Acá es muy importante definir la fuente de 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 se 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.

Figura 2. Topología de un Meta –directorio



Fuente P. J. Windley. —Digital Identity . O´Reilly, 2005

3.3.5 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.

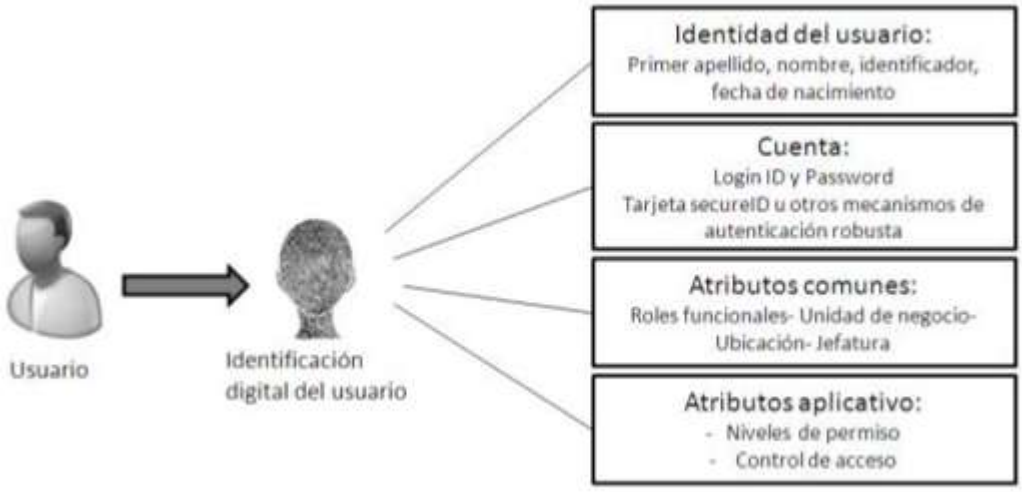
Para el diseño de una identidad digital es necesario realizar un inventario de los diferentes atributos o características que componen un usuario en término de las aplicaciones y

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.

Figura 3. Identidad digital

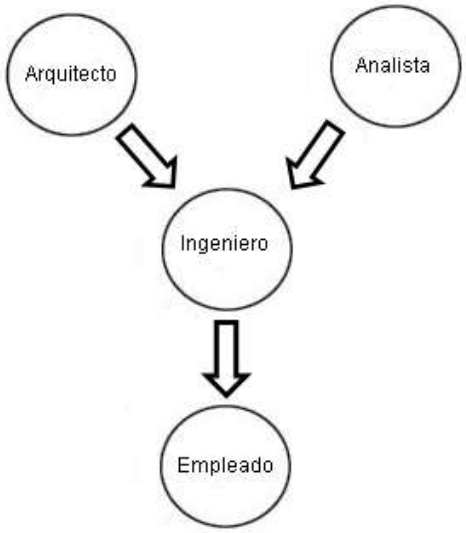


Fuente P. J. Windley. —Digital Identity . O´Reilly, 2005

3.3.6 Control de acceso basado en roles RBCA. 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.

Figura 4. Jerarquía de roles



Fuente Role Engineering for Enterprise Security Management

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

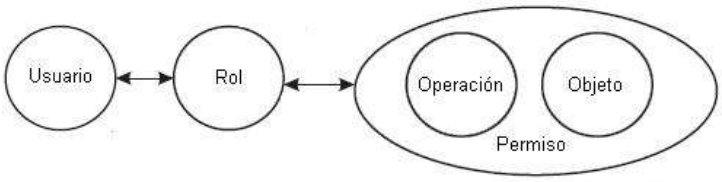
de tareas, seguridad en el acceso a los recursos y a la información y que los usuarios cuentan solo con los permisos de acceso a los recursos de acuerdo a las funciones asignadas dentro de la organización.

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).

Figura 5. Esquematización política control de acceso



Política de control de acceso

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

Fuente Role Engineering for Enterprise Security Management

3.4 PLATAFORMA TECNOLÓGICA ACTUAL DE MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

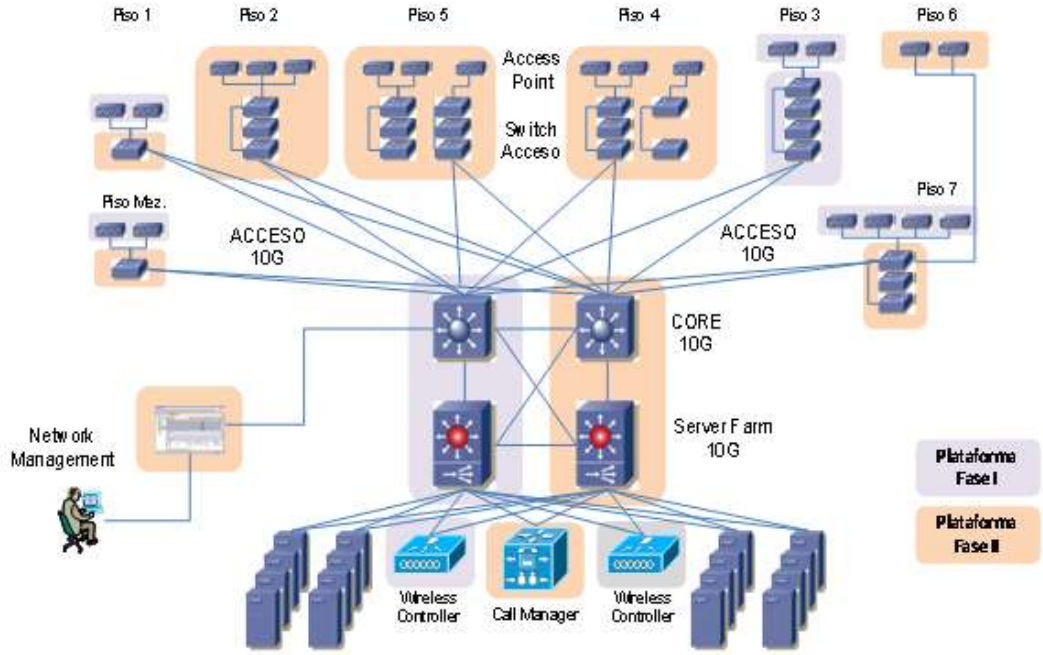
Dada la necesidad que tiene el Ministerio de Tecnologías de la Información y las Comunicaciones de operar y mantener la plataforma de los sistemas de información del sector de las comunicaciones, actualmente cuenta con una infraestructura de comunicaciones LAN entre los pisos 1 al 7 del edificio Murillo Toro con una troncal de fibra óptica de 10 GBPS que los conecta, en donde por cada piso existe un armario de comunicaciones al cual llega los respectivos tramos de fibra que conforman la estructura de backbone de la red, el piso 3 ubicado en la oficina del Grupo Soporte Operacional y Tecnológico se encuentra el armario principal que soporta las conexiones principales de esta red y además confluyen todos los canales principales de la entidad como son última milla de acceso a internet con Columbus Networks, canal RAVEC hacia Minhacienda, canal de conexión de ETB con la Agencia Nacional del Espectro, así mismo en el centro de cableado se proporcionan los siguientes servicios: Seguridad a través de un firewall Cisco PIX 525, servicio de WiFi con un equipo Cisco Wireless LAN 5500, equipos de swicheo de core 3COM 4050 en XRN y equipos de borde en cada uno de los pisos entre 3COM y Cisco, enrutamiento para cada uno de los canales de internet, Ravec y ETB-Ane.

La entidad dispone de una conexión desde el centro de cableado hacia el Data center que es el encargado de alojar los servidores de la entidad quienes cumplen cada uno con servicios de manejo de aplicativos (Alfanet, BDI, ASMS, Seven, Kactus, SER, Registrotic, servicio administración de blakberry, Imágenes), servicio de correo electrónico Exchange 2013, servicio proxy, antivirus McAfee, antispam, DNS, DHCP, administración de backups por medio de una SAN HP Eva, administración de impresoras. El Data center cuenta con un sistema de detección contra incendios, y doble aire acondicionado a fin de tener respaldo permanente de los equipos de computación y de almacenamiento

En cuanto a la parte de infraestructura eléctrica, el Ministerio dispone de un módulo de transferencia automática de circuito en media tensión, alimentada de un circuito normal y de un circuito suplente de diferentes subestaciones, disponible 7x24 x 365, esto permite que el fluido eléctrico normal sea continuo; en la parte regulada se dispone de un sistema ininterrumpido de potencia de 120 KVA, para cubrir los puntos de voz y datos y equipos de computación y de comunicaciones y una UPS de 30 KVA que soporta el centro de datos y el centro de cableado de la entidad.

Para proporcionar los servicios anteriormente mencionados, el Ministerio cuenta con la infraestructura que se presenta en la Figura 6.

Figura 6. Red Lan del MinTic



Fuente: Diseño suministrado por la oficina de TI del MinTic

La prestación de servicios de red que la entidad atiende de manera permanente a través del Grupo Soporte Operacional y Tecnológico son las siguientes:

- Servicio de acceso a los diferentes sistemas de información.
- Servicio de correo electrónico bajo plataforma Exchange 20103en lo servidores
- Servicio de correo electrónico en los clientes Outlook y clientes remotos vía OWA
- Acceso a Internet a 30 MB
- Servicio de asignación y control de usuarios – DA.
- Servicio de DNS y DHCP
- Servicio de Blackberry BES y BIS
- Servicio de VPN remoto con autenticación de Firewall
- Servicio de Storage Área Network - Almacenamiento Masivo de Red (SAN)
- Acceso remoto a aplicaciones de otros clientes tales como: SIIF, SIUST, SUTI, SUIFD-DNP, ASPA
- Servicio de telefónica IP

3.4.1 Sistemas de Información y hardware utilizado. A lo largo de los años los sistemas de información en el Ministerio de tecnologías de la Información y las comunicaciones han venido evolucionando constantemente, durante el transcurso de cada etapa de implementación tecnológica se ha puesto como énfasis en la seguridad de los sistemas. Actualmente se adelanta una transformación en las políticas de seguridad de los aplicativos con el fin de garantizar la disponibilidad y la confidencialidad de los mismos.

En la actualidad el Ministerio cuenta con los siguientes recursos informáticos para la operación y toma de decisiones de su proceso:

- BDU es la base de datos central de proveedores de servicios de TIC del país. Contiene información de todos los operadores que solicitaron servicios antes y después de la ley 1341, ya que se carga información de los nuevos operadores proveniente de SISC. BDU integra información de los proveedores de redes y comunicaciones, postal y radio, con datos administrativos, técnicos y financieros (estado de cuenta), igualmente contiene información de sanciones, multas y espectro. La cual se encuentra desarrollada en Visual Basic y con un motor de base de datos de SQL Server.
- SAGE es un sistema que permite realizar el proceso de habilitación del espectro, lo que implica tener todos los cuadros técnicos, la información de gestión e ingeniería para asignar el espectro. El sistema cuenta con herramientas de predicción y simulación que permiten determinar si se pueden asignar ciertas frecuencias pues cuenta con el mapa de Colombia digitalizado con la topología y coordinadas. El Sage es usado por MINTIC y la ANE, la Agencia se encarga de hacer el análisis técnico mientras que MINTIC emite la resolución. En la actualidad tienen planeadas algunas mejoras importantes en SAGE como la generación de la resolución desde el sistema puesto que ahora solo se emite el cuadro técnico. Este aplicativo se encuentra desarrollado en C++ y con motor de base de datos de SQL server.
- SER (sistema electrónico de recaudo). Que facilita el pago electrónico de obligaciones financieras de los Clientes, Operadores de servicios de telecomunicaciones, la actualización de la información administrativa y financiera y la presentación y/o pago de las autoliquidaciones de los Operadores. Este sistema de información se encuentra desarrollado en .NET con una base de datos SQL Server.
- Registro Tic apoya el proceso de habilitación general de los servicios para los operadores que se acogen a la ley 1341, también permite realizar el proceso de inscripción para mantener las licencias existentes; lo que se obtiene finalmente es una certificación donde se otorga permiso para los servicios solicitados. Este aplicativo se encuentra desarrollado en C++ y con motor de base de datos de SQL server.

- BDI (Base de Datos de Investigación). Es un aplicativo donde se encuentran todas las investigaciones de los operadores de redes y servicios incluyendo los de los servicios postales. Se encuentra desarrollado Visual Basic, base de datos SQL Server.

Cuadro 1 Total de Servidores

Arquitectura Servidores	**Cantidad**
Arquitectura BL25P	10
Arquitectura BL25P G2	01
Arquitectura BL460C G7	04
Arquitectura BL685C G6	03
Arquitectura BL465C G5	01
Arquitectura Rack HP	02
Arquitectura Rack Dell	03
Arquitectura Torre Compaq HP	06
Total de servidores	**30**
Fuente: Oficina de TI del MinTic	

Cuadro 2 Armarios por piso

Piso	**Cuartos de cableados**	**Cantidad switches**	**Cantidad puertos en uso**
Siete (7)	1 Armario	3 Sws 3COM: 2 de 48 y 1 de 24 puertos	72
Seis (6)	1 Armario	4 Sws 3COM de 48 y un Hub de 48 puertos	240
Quinto (5)	1 Armario	4 Sws 3COM de 48 puertos	240
Cuarto (4)	1 Armario (piso en obra)	Habían 5 Sws 3COM de 48 puertos	Se encuentra en obra
Tercero (3)	2 Armarios	Rack nuevo: 4Sws Cisco de 48. Rack viejo: 4 Sws 3COM de 48 puertos, 2 Core 3COM con 24 puertos ocupados, más 9 módulos GBIC ocupados	299
Segundo (2)	1 Armario	3 Sws 3COM de 48 y un Cisco de 48	192

Primero (1)	1 Armario (Innovación)	Un (1) Sws 3COM de 48 y un (1) 3COM de 24 puertos	41
Mezzanine	1 Armario	2 Sws 3COM de 48 puertos	90
Sótano	Sin Armario	Sin datos	Sin datos
Fuente: Oficina de TI del MinTic			

Debido a la variedad de sistemas de información con que cuenta el MINTIC, ingresar y administrar cada uno de los sistemas, se vuelve complicada la administración de los equipos para el área de TI los cuales tienen la responsabilidad de la seguridad de los sistemas informáticos. Se debe añadir también el riego que existe al no contar con una bitácora centralizada de monitoreo de seguridad de todos los sistemas.

Con un sistema de manejo de identidades digitales se pretende tener un solo punto de administración para el manejo de seguridad de todos los sistemas, adicionalmente se busca facilitar al usurario final el acceso a los diferentes sistemas informáticos del Ministerio.

Como se ha mencionado el uso de una amplia variedad de sistemas informático y arquitecturas de servicio (cliente-servidor, computación en la nube, computación en granja) ha ocasionado un incremento en la complejidad del manejo de las identidades. Se debe comprender que el usuario es el elemento central de un sistema de manejo de identidades, dicho usuario puede ser funcional o técnico. [10] La expresión mínima que el usuario identifica cuando realiza el proceso de autenticación y acceso al recurso es:

- ***Acción de seguridad***. Se realiza cuando el usuario requiere la autorización necesaria o la activación del mecanismo de seguridad.

- ***Conclusión de la Seguridad***. Acceso autorizado a un sistema informático.

4. PROPUESTA DE DISEÑO

Dentro la propuesta de diseño para el gestor de entidades, esta se centró en dos fases:

- La evaluación de las soluciones propuestas para determinar cuál de ellas cubre las necesidades existentes del MINTIC.
- Propuesta de arquitectura para la implementación de la solución de manejo de identidades digitales seleccionada.

4.1 SELECCIÓN DE SOLUCIONES PARA EL MANEJO DE IDENTIDADES DIGITALES.

Para el estudio de las soluciones para el manejo de un gestor de identidades se determinaron los siguientes aspectos: El primer aspecto que se tuvo en cuenta fue las empresas líderes en prestaciones para el usuario. Estos fueron obtenidos de estudio realizado por (Gartner RAS) [9]. Cuyos resultados se presenta en la figura 7. Las principales cualidades que inciden en la decisión de la adquisición de un software para el manejo de identidades según el estudio son las siguientes:

- Inteligencia: Que cuente con herramientas que permita el monitoreo de todos los eventos ocurridos, de una forma fácil y confiable, que permita la auditorias de los eventos.

- Administración: El manejo integral de la solución, permitiendo el control de flujo general para la autenticación y autorización.

- Autenticación: Inicio único de sesión.

- Autorización: Todo lo relacionado con el control de aplicaciones específicas, hasta el control de los servidores, servidores de archivos, cortafuegos.

Figura 7. Ingresos recibidos por la venta de software de manejo de identidades digitales

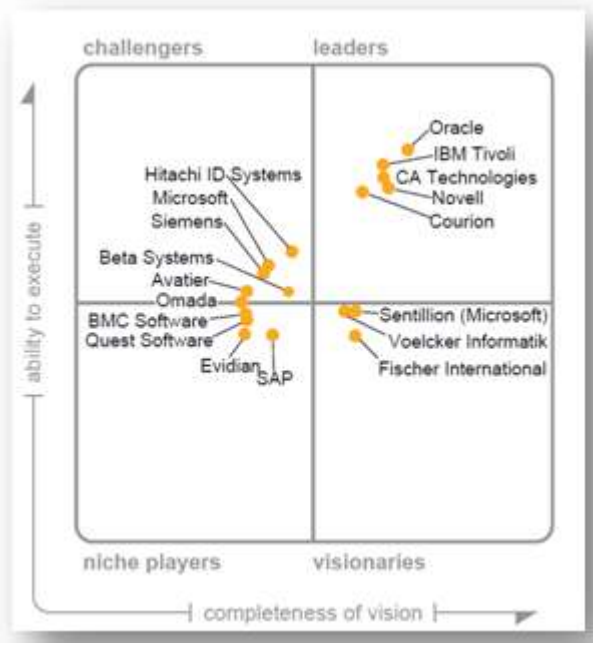
Worldwide Identity and Access Management Revenue by Vendor, 2006–2008 ($M)

	2006	2007	2008	2008 Share (%)	2007–2008 Growth (%)
IBM	368	390	398	11.8	2.2
EMC	295	311	326	9.7	5.0
CA	332	324	320	9.5	-1.3
VeriSign	215	225	248	7.3	10.2
Oracle	105	171	180	5.3	5.6
Novell	97	104	117	3.5	12.0
Aladdin Knowledge Systems	77	91	107	3.2	17.9
SafeNet Inc.	88	98	106	3.1	8.4
Gemalto	42	62	98	2.9	59.2
HP	47	64	87	2.6	36.1

Fuente: ftp://ftp.software.ibm.com/software/au/downloads/IDC_Report.pdf

Otro aspecto que se tuvo en cuenta para el análisis de una solución de un gestor de identidades fue el ingreso que reciben las compañías, de acuerdo a la Internacional Data Corporate (IDC). Los resultados de este estudio se presentan en la Figura 8.

Figura 8. Prestaciones para el usuario



Fuente (Gartner RAS)

Con base al estudio se determinó que las soluciones más robustas en este ramo son IBM Tivoli Management y Oracle Identity Management, lo anterior debido que en la figura 5 nos muestra que son las soluciones líderes en cuanto a prestaciones se refiere, en cuanto a la capacidad de ejecución y la investigación realizada en el ámbito de manejo de identidades digitales. Por otra parte en la gráfica de ingresos figura 4 se puede observar claramente que ambas compañías han venido incrementado su ingreso por concepto de las ventas de sus aplicaciones.

4.2 EVALUACIÓN DE LAS SOLUCIONES PARA EL GESTOR DE IDENTIDADES.

La evaluación se realizó teniendo en cuenta 5 aspectos fundamentales definidos por las necesidades de la entidad:

- Herramienta estándar para integración
- Interfaz de autoservicio.
- Manejo de roles.

- Reporte y auditorias
- Administración centralizada.

4.2.1 Herramientas estándar para integración. La evaluación se basó en determinar si las herramientas de conexión o interfaces con sistemas informáticos externos, que contienen ambas soluciones, están basada en herramientas o lenguajes de programación estándar. Para el software IBM Tivoli Identity Management se encontró que cuenta con los siguientes lenguajes como mecanismo para el desarrollo de interfaces [11]:

- XML (lenguaje de marcado extendido)
- RMI (método de invocación remota).
- DAML (lenguaje de marcado de acceso directo)
- J2EE
- Java
- JavaScript.
- HTML (lenguaje de marcado)
- Corba
- C.
- Perl

Para el caso de Oracle Identity Manager se encontró que también se encuentra basado en estándares en cuanto a HERRAMIENTAS Y LENGUAJES DE PROGRAMACIÓN. [12]

XML Lenguaje de Marcado extendido
DSML (lenguaje de marcado de directorio de servicios)
Java

También se encontró que las dos soluciones posee la interfaz LDAP (protocolo directo de acceso a directorios).

Como conclusión preliminar para este aspecto, de acuerdo con la información encontrada, se puede asumir que ambas soluciones poseen los elementos estándares necesarios para la integración con los estemas informáticos existentes.

En especial la interfaz del protocolo LDAP que nos ayudara a integrarlo con el controlador de dominio de Windows. IBM tivoli Identity Management maneja dicha conexión por medio de un conector, mientras Oracle identity Manangement lo maneja por medio de GINA (Conjunto de librerías que se ejecutan al momento de realizar un LOGON es un equipo de WINDOWS).

4.2.2 Interfaz de Autoservicio. En este aspecto se buscó que el gestor de identidades fuera capaz de contar con la facilidad de que los propios usuarios puedan realizar ciertas actividades en relación a su usuario, tales como: Cambio de contraseña, Actualización de información personal, reinicio de su contraseña. Con base a lo anterior, los resultados que se encontraron fueron:

IBM: Se encontró que la herramienta pose la interfaz par que el usuario realice ciertas actividades administrativas con respecto a su identificación de usuario. La interfaz es realizada por medio de la herramienta de acceso WebSEAL. El privilegio de autoservicio se le asigna por medio de un rol estándar llamado USURS, el cual solo le otorga los derechos de visualizar su propia información y solicitar accesos a sus recursos [11]

Oracle: El software también pose la característica de autoservicio para los usuarios, la cual lo realiza por medio de la herramienta IA-5 de su suite.

Ambas herramientas cuentan con esta característica.

4.2.3 Manejo de roles. Sobre este aspecto conforme a la necesidades requerida por la entidad se estableció que el gestor de identidades deberá contar con un modelo de Control de Acceso basado en Roles RBAC8 Por su siglas en inglés: Roles Based Access Control) para el otorgamiento de las autorizaciones correspondientes a cada usuario del sistema. Se encontró que la solución de IBM Tivoli Idebtity Management cuenta con el modelo RBAC para otorgar y controlar el acceso a los recursos o sistemas informáticos, también cuenta con los modelos Control de Acceso Discrecional DAC(por su siglas en inglés Discretional Acces Control) y Control de Acceso Mandatorio MAC (Mandatory Access Control)

Oracle: maneja el control o autorización por medio de Listas de Control de Acceso ACL (Access Control List)

Una vez analizado las dos soluciones se encontró que Oracle no cumple con el requerimiento exigido por la entidad.

4.2.4 Reporte y auditoria. Dentro del análisis se estudió que la solución contará con la facilidad de obtener reportes que permitan la realización de auditorías los cuales fueron los siguientes:

IBM: La solución genera una amplia gama de reportes que permite realizar una adecuada inspección de seguridad, pudiendo realizar la exportación de dichos reportes a formatos como PDF o CSV.

Oracle: Dentro de análisis se encontró que esta solución genera reportes que permiten realizar una adecuada inspección de la seguridad en los sistemas informáticos. Para ellos se requiere la instalación de un módulo adicional con relación a la solución base que es el ORACLE Acces Manager.

Como conclusión de la evaluación, se considera que el modulo adicional de Oracle origina una modificación al diseño propuesto, por lo que se considera que no cumple el requisito especifico.

4.2.5 Administración Centralizada. Ambas soluciones cuentan con una base centralizada para el manejo de las identidades digitales de los diferentes sistemas informáticos. Para el caso de IBM Tivoli Identity Maanagement, las funciones que se manejan de forma centralizada son: configuración del sistema, configuración de interfaces, políticas de seguridad, auto servicios de usuarios, contraseñas, delegaciones administrativas, flujo de trabajo, reportes. Por el lado de ORACLE Identity Management utiliza su módulo adicional ORACLE Access Manager para centralizar las siguientes actividades: [12] configuración del sistema de acceso, políticas de seguridad, delegaciones administrativas, reportes, auto servicios del usuario, contraseña. Para efecto de este trabajo y considerando que la solución requiere de un módulo adicional ORACLE Identity Management no cumple el requisito solicitado.

4.3 INSTRUMENTO DE EVALUACIÓN

Para la comparación de ambas soluciones de manejo de identidades se desarrolló como metodología de evaluación, una lista de chequeo la cual muestra las variables que se utilizaron para medir la eficiencia de las plataformas seleccionadas. Las variables que se tuvieron en cuenta fueron las que se explicaron anteriormente. Las variables de medición fueron evaluadas con 2 posibles valores, que califican de 5 puntos cuando se cumple con el requerimiento evaluado y un valor de cero puntos si no se cumple. La tabla 1 presenta los resultados obtenidos por las dos plataformas evaluadas mediante el instrumento de evaluación.

Tabla 1 Resultados de evaluación de las soluciones IBM y Oracle

Requerimiento	IBM Tivoly Identity Mananger	Oracle Identity Manager
Herramienta estándar para integración	5	5
Interfaz de autoservicio	5	5
Manejo de roles	5	0
Reporte y auditoria	5	5
Administración centralizada	5	5
Suma de Puntuación	25	20

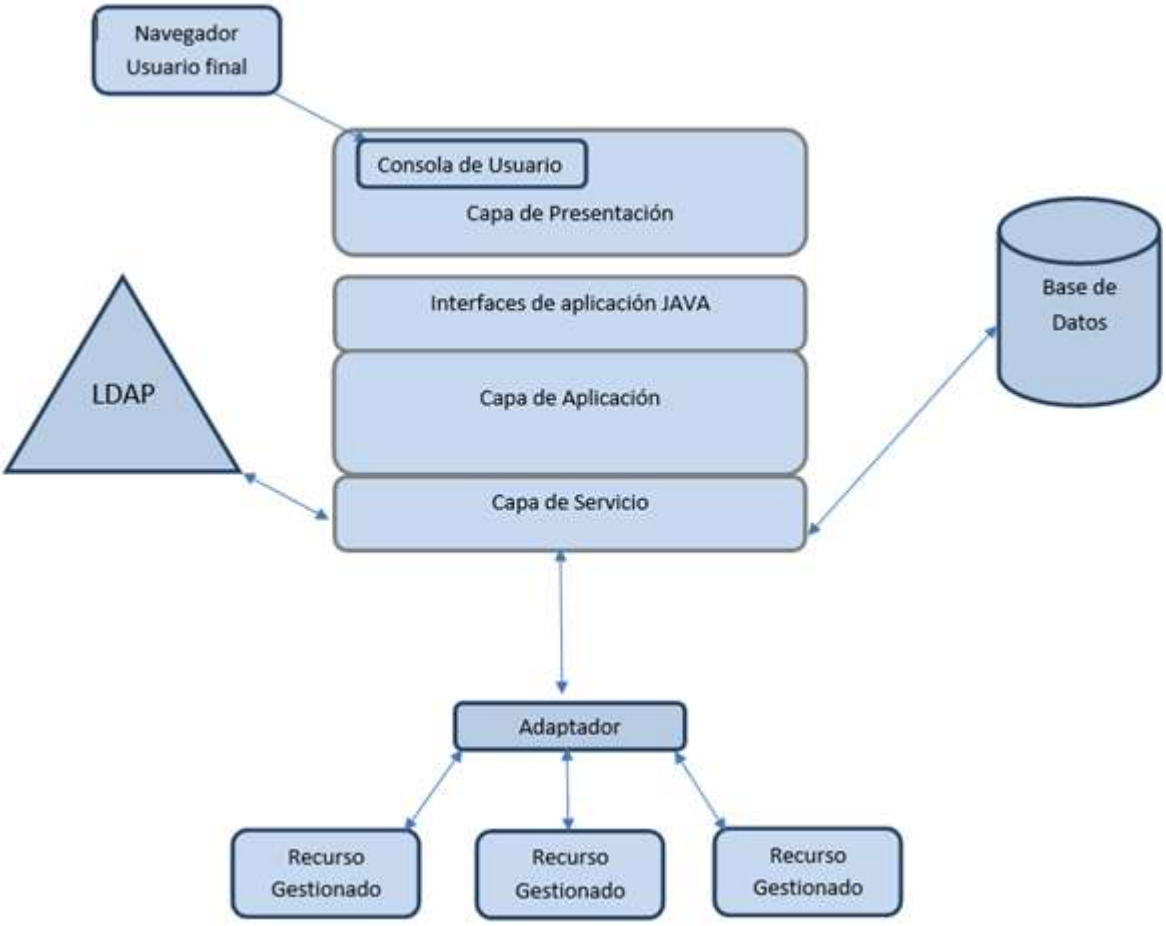
Fuente: Creación propia basada en la soluciones de IBM Tivoli y Oracle

Con base a los resultados obtenidos, se concluye que la solución que mejor se adapta a las necesidades de tecnología de información estratégica de la empresa es IBM Tivoli Identity Management.

5. ARQUITECTURA PROPUESTA

La propuesta desarrollada está compuesta por dos grandes áreas funcionales como son: la presentación (capa de interfaz de usuario) y el aprovisionamiento (capa de aplicación y capa de servicio). En la figura 9 se muestra la arquitectura lógica propuesta para la implementación de la solución.

Figura 9 Arquitectura lógica propuesta



Fuente Creación basada en (Buecker, Filip, Cordoba, & Parker, 2009)

5.1 CAPA DE PRESENTACIÓN

Esta capa es la encargada de la interfaz gráfica del usuario. Dicha interfaz es proporcionada por la consola del usuario. La consola del usuario es utilizada para el acceso al sistema tanto para los usuarios funcionales como por el administrador de la solución. Se determinó que la mejor forma de acceder a dicha consola es por medio de un navegar de internet, ya que es una aplicación ampliamente utilizad por todo el personal. El navegador de internet oficial utilizado en el MinTic es Internet Explorer 9.

5.2 CAPA DE APLICACIÓN

La capa de aplicación es la se encarga de proveer las funciones de la solución, mediante diversos módulos, a la capa de interfaces. Los módulos que se utilizaron para elaboración de la arquitectura son [11]:

- Manejo de control de acceso. Es el modulo encargado de controlar las operaciones básicas (agregar, modificar y borrar) en los clientes remotos.

- Manejo de Identidades. Es la parte central de la solución, ya que por medio de este se manejan las tareas administrativas de las identidades digitales.

- Manejo del sistema. Es donde se opera lo relacionado con el sistema de manejo de identidades digitales Tivoli Identity Management.

- Manejo de políticas. Es el encargado de las políticas relacionadas con el sistema, así como también de las políticas aplicadas a las identidades digitales.

- Servicios de autorización y autenticación. Es el responsable de realizar las labores de autorización y autenticación del sistema y parte esencial para la realización del proceso de inicio de sesión único.

5.3 CAPA DE SERVICIOS

Esta capa es la que está conectada, mediante un adaptador, de forma directa a los recursos que se necesiten incorporar para el manejo de las identidades digitales. Esta capa está conformada por módulos que permite realizar la intermediación entre las aplicaciones existentes y la solución. Un componente importante de esta capa es el módulo de servicio de datos. Lo anterior debido a que este módulo es el que realiza la conexión directa al directorio Activo de Windows 2008 server, dentro del directorio activo almacena todos los usuarios de los sistemas informáticos existentes, a través del directorio activo, se determina los usuarios que existen, que autorizaciones tienen y que políticas de seguridad se aplican. Dentro de la capa de servicio se plantearon otros componentes dentro del diseño de la arquitectura los cuales son [11]:

- Autorización: Componente que otorga a las interfaces las reglas de autorización de operación de los clientes entre los sistemas de información conectados a la solución.
- Autenticación: Modulo que proporciona los componentes de autenticación utilizado en el diseño los cuales fueron (usuario y contraseña).
- Roles: establece los cambios a los roles de autorización cuando un usuario cambia de rol.
- Políticas de seguridad: Aplica de acuerdo al servicio utilizado.
- Servicio remoto: Servicio esencial encargado de realizar la interacción entre el software de manejo de identidades digitales y los sistemas de información existentes en la empresa.
- Correo electrónico: servicio encargado de notificar los eventos que surgen dentro de la solución de manejo de identidades digitales.
- Flujo de trabajo: Este servicio permite llevar a cabo procesos de auditoria en cuanto a las actividades realizadas por los usuario como son: sistemas de acceso, tipo de transacciones realizadas, tiempo de ejecución entre otros.

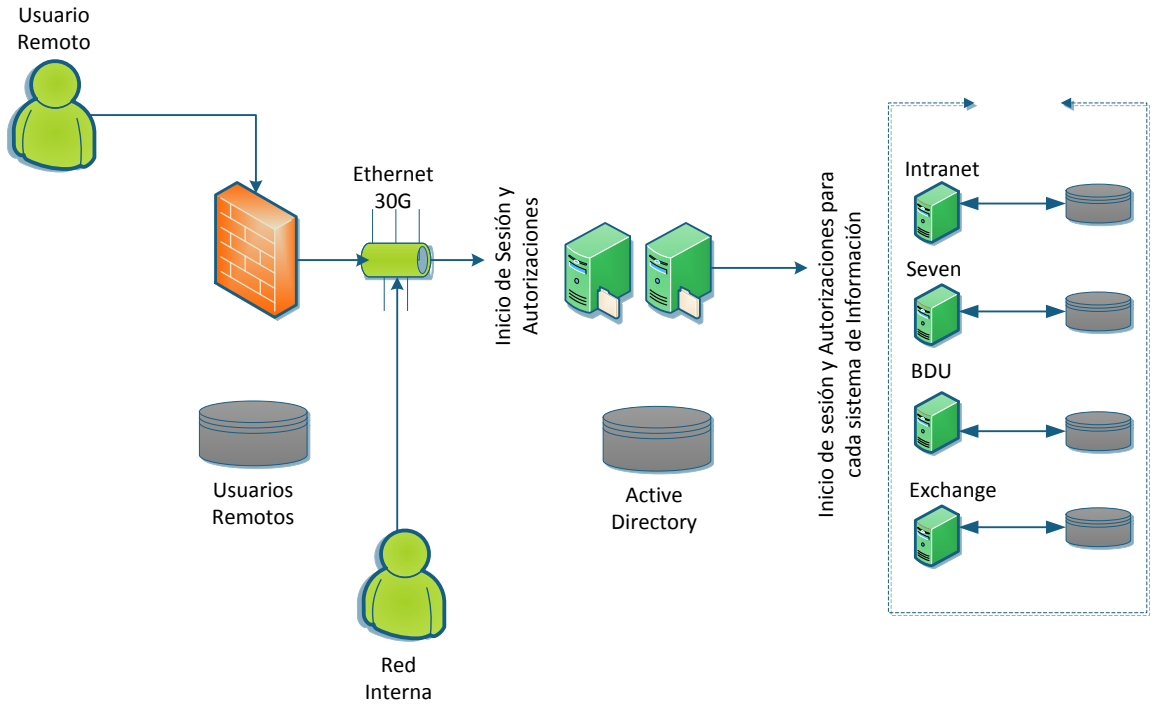
5.4 ADAPTADORES

Para lograr la integración de los diferentes sistemas de información con que cuenta el MinTic. De acuerdo a la solución de IBM Tivoli Management, se encontró que es necesaria la utilización de los adaptadores.

5.5 ARQUITECTURA FÍSICA

IBM Tivoli Identity Magement Soporta sin número de configuraciones que satisfacen las necesidades del manejo de identidades digitales. La arquitectura física para el manejo de las autorizaciones e inicio de sesión tanto para usuarios funcionales como para usuarios de soporte operacional en los sistemas de información del MinTic se muestra en la figura 10.

Figura 10. Arquitectura física actual para el inicio de sesión

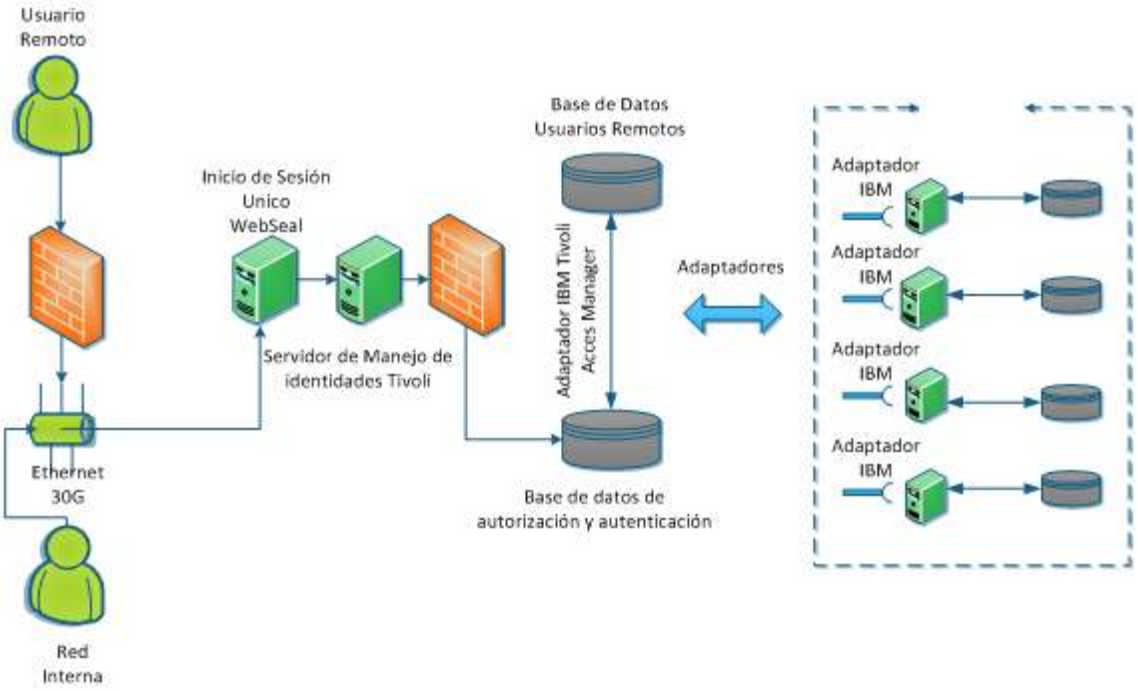


Fuente: Oficina de TI MinTic.

En la arquitectura actual mostrada en la figura 10 se observa la forma en que los usuarios se conectan a los diferentes sistemas de información vía red interna y externa. Cada vez que un usuario utiliza cualquier sistema de información existente, tiene que realizar, en primera instancia, la autenticación que le permita ingresar a su pc personal. Este proceso, en un entorno de Directorio Activo de Microsoft Windows, es conocido como WinLogon. Una vez ya iniciada su sesión, tiene que realizar el mismo procedimiento para cada sistema de información, es decir, ingresando usuario y contraseña correspondiente para cada sistema, los cuales son distintos al usuario del directorio activo. Adicional al proceso anterior, el usuario remoto, necesitan realizar otro proceso de autenticación

correspondiente al sistema de Red privada Virtual para lograr la conexión y autorización correspondiente de acceso a la red interna.

Figura 11. Arquitectura física propuesta para el inicio único de sesión



Fuente Creación propia

Dentro de la arquitectura diseñada, se remplazó el servidor de autenticaciones para ser utilizado como servidor WEBSEAL el cual otorga la función de inicio de sesión único y el servidor restante fue utilizado para la instalación del servidor de manejo de identidades digitales Tivoli Identity Management, el cual realiza la tarea de gestionar los procesos de autenticación y autorización de usuarios por medio de los adaptadores correspondientes hacia los diferentes sistemas de información existentes.

Otro aspecto relevante dentro de la elaboración de la arquitectura es que la mayoría de las conexiones se realiza por medio del adaptador de directorio activo. Como resultado de la arquitectura propuesta, los usuarios y administradores de tecnología de la información del MinTic tiene un único punto de acceso hacia los sistemas de información, para obtener las autorizaciones correspondientes a su rol desempeñado en el flujo de los procesos.

5.6 IMPLEMENTACIÓN

Toda implementación tecnológica dentro del Ministerio de tecnología de la Información y las Comunicaciones requiere de un proceso de autorización por parte de la alta gerencia en especial si el proceso afecta de manera significativa a la entidad. Por ello, toda propuesta desde ser presentada en su forma conceptual, ya que con la alta dirección visualiza las implicaciones de la propuesta, autorizando de esa forma a continuar con la siguiente etapa del proceso que es la obtención de costos y del valor de recuperación de la inversión; una vez obtenida la autorización para la inversión, se realiza la fase de adquisición e implementación de la solución sugerida.

Debido a que todo proceso de autorización, desde la propuesta conceptual hasta la adquisición e implementación, puede llevar de 6 a 12 meses, la presente propuesta solo cubre la etapa inicial, siendo un diseño conceptual de la arquitectura de un gestor de identidades.

CONCLUSIONES

A lo largo de los años, la complejidad de los sistemas de información que posee el Ministerio de tecnologías de la información Y las comunicaciones ha crecido considerablemente, lo cual ha dificultado la administración de la seguridad de los mismos.

Con el diseño de arquitectura propuesto se cubre la simplificación de acceso y administración de la seguridad de los aplicativos informáticos en los siguientes aspectos:

- Usuarios. En la arquitectura actual los usuarios generalmente cuentan con cinco usuarios diferentes, así como la contraseña respectiva, para poder utilizar los diferentes sistemas de información existentes. Con el diseño propuesto, se tiene una sola cuenta de usuario con su respectiva contraseña para logar el acceso adecuado hacia todos los sistemas de información.

- Oficina de TI. Al ser los responsable de la gestión de la seguridad de todos los sistemas informáticos, por medio del diseño propuesto, se logra centralizar la gestión de la seguridad de todos los sistemas de información existente del Ministerio, logrando una gran disminución en la tareas del personal de sistema y de la mesa de ayuda.

La arquitectura propuesta define que se puede implementar un sistema donde los usuarios realicen por única vez el procedimiento de identificación y autenticación para conectarse a una solución de manejo de identidades digitales en primera instancia por medio de un adaptador y en segunda instancia los sistemas informáticos que se requieran agregar al diseño y no cuenten con un soporte para la conexión, lo pueden realizar a través del directorio activo de Microsoft Windows Server, señalado que dicho enlace no cambia la mejora lograda en cuanto al acceso hacia los sistemas informáticos.

BIBLIOGRAFÍA

BUECKER, A., Filip, D, W., Cordoba, J. P., & Parker, A. (2009). Identity Management Design. New York, USA: International Technical Support Organization.

CORBIN H. Links.IAM Success Tips: Planning & Organizing Identity Management Programs. CreateSpace, 2008. 52p.

FERRAIOLO David F.Role-Based Access Controls. Proceedings National Computer Security Conference.1992. pp. 554-563.

Gartner RAS Core Research. http://www.gartner.com/technology/media-products/reprints/oracle/article157/article157.html.

GRIER David Alan. The Value of a Goog Name. Computer, Vol. 43, No.6. 2010. pp. 79-81.

HOWES Timothy A. Understanding and deploying LDAP Directory. Addison- Wesley.2003. 200p

IBM.com. de http://www-01.ibm.com/support/docview.wss?uid=swg21396546
IBM Public Folder de http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.itamesso.doc_8.0/IBM_TAM_E-SSO_RemoteAccessIntegrationGuide_v8.0.0.pdf.

IDC. (2009). World Wide Identity and Access Management 2009-2013. Framinghan, MA: IDC.

JASON Andress. The Basics of Information Security: Understanding the fundamentals of InfoSec in Theory 8 and Practice. Syngress. 2011.

JOSANG Audun. Usability and Privacy in Identity Management Architectures. Australasian Information Security Workshop. Ballaarat, Australia: Australian Computer Society.2007.

KUHN Richard D. Adding Attributes to Role-Based Access Control. Computer. Vol. 43. 2010.79-81pp.

POHLAM Marlin. Oracle Identity Management. Taylor & Francis Group.2008.141p.

SCHEIDEl Jeff. Designing an IAM Framework with Oracle Identity and Access Management. McGraw Hill. 2010.

TARBUCK Edward J. Davis John M. Role Engineering for Enterprise Security Management.2007

WINDLE Philip J. Digital Identity. O´Reilly. 2005. 20p.

PROPUESTA DE DISEÑO DE UN GESTOR DE IDENTIDADES DIGITALES EN EL MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

Francisco Ariza Pastor

Universidad Piloto de Colombia, Especialización de Seguridad Informática

franciscoarizapastor@gmail.com

***Resumen*— Actualmente el Ministerio de Tecnología de la Información y las Comunicación a través de la oficina de tecnología y la información, otorga accesos en forma independiente utilizando los módulos de seguridad de cada una de las aplicaciones y/o plataformas tecnológicas. Además, el registro de nuevos usuarios se realiza a través de una comunicación formal a través de la mesa de ayuda para aprobación de la oficina de TI, esta forma de trabajo ocasiona que no se lleve un control estricto del ciclo de vida de la gestión de identidad, las cuentas de los usuarios; todo esto trae como consecuencia un incremento en el riesgo sobre la confidencialidad, disponibilidad e integridad de la información del Ministerio. El Ministerio cuenta en la actualidad con 1.100 usuarios y con 13 aplicaciones implementadas.**

El presente proyecto propone el diseño de una arquitectura integral de manejo de identidades digitales a través de una solución que brinde un único acceso a los diferentes sistemas de información de la entidad.

***Palabras clave*— Identidades digitales, control de acceso, complejidad, rol, sistemas informáticos.**

***Abstract*— Currently the Ministry of Information Technology and Communication through the office technology and information, provides access independently using security modules for each of the applications and / or technology platforms. Furthermore, registration of new users is through a formal communication through the help desk for approval by the IT office, this way of working brings that tight control of lifecycle management is not carried identity, user accounts; this results in an increased risk on confidentiality, availability and integrity of the information ministry. The Ministry currently has 1,100 users and 13 deployed applications.**

This project proposes the design of an integrated architecture for managing digital identities through a single solution that provides access to various information systems of the organization.

***Index Terms*— Digital identities, access control, complexity, role, information systems.**

I. INTRODUCCIÖN

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 esta propuesta 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.

II. Planteamiento del problema

El Ministerio de tecnologías de la Información y las Comunicaciones, con el ánimo de crear oportunidades de negocio y ventajas competitivas que le ayuden a obtener el mejor resultado en la comunicación con el ciudadano, ha desarrollado 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.

En la actualidad se cuenta con un sin números de aplicación que soporta el plan de negocio de la entidad, en la cuales se almacenan los datos de los proveedores de redes y servicios de la industria TIC de Colombia, esta información se encuentra distribuida en los siguientes sistemas de información:

- ASMS (Sistema de Gestión del Espectro Radioeléctrico)
- ALFANET (Sistema de flujo de documentos)
- SAGE (Nueva versión del Sistema de Gestión del Espectro Radioeléctrico)
- BDI (Bases de Datos de Investigaciones)
- BDU (Bases de Datos Única de Clientes)
- SEVEN (Sistema Financiero y Administrativo)
- KACTUS (Nómina y Recursos Humanos)
- REGISTROTIC (Registro Único de Operadores – Auraportal)
- REGISTRO POSTAL (Auraportal)
- SER (Sistema Electrónico de Recaudos)
- Cobro Coactivo
- ZAFIRO (expedientes digitalizados)
- Procesos judiciales.

En el momento cada sistema de información maneja formas de autenticación diferentes, control de acceso, seguridad y bases de datos diferentes, esto ocasiona que cada funcionario realice un ingreso diferente para cada uno de estos aplicativo, ocasionando la destinación de una parte del presupuesto de la entidad para el sostenimiento de varios funcionarios que realizan la administración de las cuentas de usuario.

Contar con sin números de sistema de información genera una proliferación de usuarios y contraseñas, lo que conlleva a una inadecuada gestión de la seguridad en la entidad.

III. ESTADO ACTUAL DE LA ORGANIZACIÓN

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 denegocio 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]

- Cumplimiento regulatorio a diario se implementan nuevas regulaciones que afectan, de una u otra manera, tanto a las entidades públicas como privadas y la forma en la que interactúan con el ciudadano. 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 [2]. 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.

- 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.

- 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.

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

- 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 [3]. 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.

- 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.

IV. VENTAJAS DE UN GESTOR DE INDENTIDADES

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].

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:

- 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.

- 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.

- 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 asociado al cargo [6].

V. COMPONENTES DE UNA SOLUCIÓN DE GESTIÓN DE IDENTIDADES

1) 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 2 se muestra el modo como se estructura la información que compone la identidad digital de un usuario.

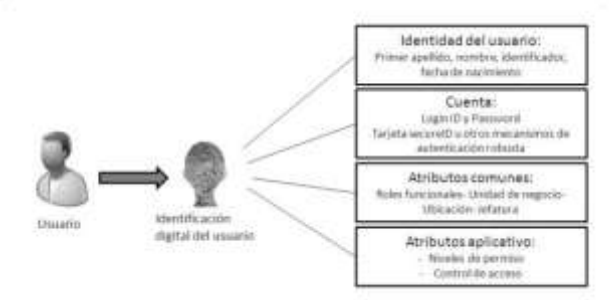


Fig. 2 Identidad digital [1]

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.

2) Meta Directorio

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 [5]:

- 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 la Figura 3 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.

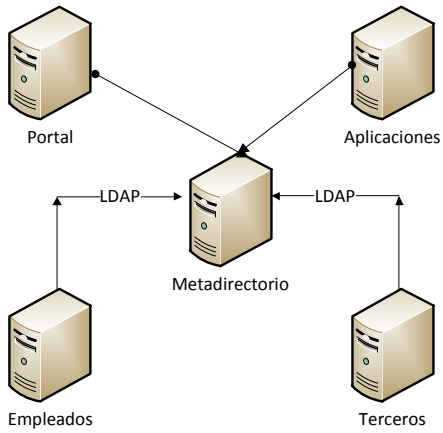


Fig. 3 Topología de un Meta-directorio

3) Control de acceso basado en roles RBCA

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.

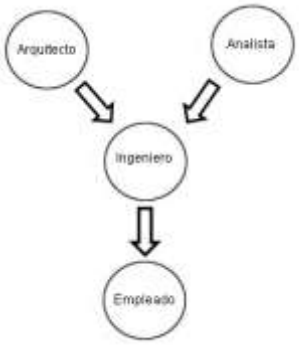


Fig.4 jerarquía de roles

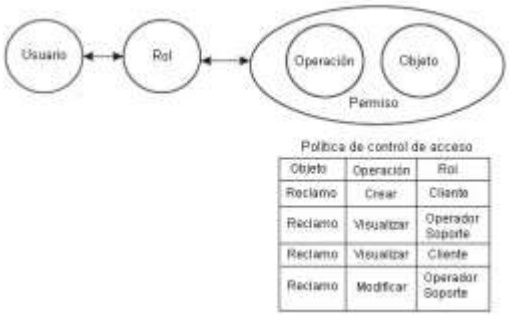
Un esquema de autorización basado en roles se basa en las siguientes tres reglas: (1) A todos los usuarios se les debe asigna un rol. Si a un usuario no se le asigna ningún rol, éste no podrá realizar ninguna acción relacionada con el acceso a los recursos, (2) Para que un usuario pueda hacer uso de 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]

VI. ARQUITECTURA PROPUESTA

La propuesta desarrollada está compuesta por dos grandes áreas funcionales como son: la presentación (capa de interfaz de usuario) y el aprovisionamiento (capa de aplicación y capa de servicio). En la figura 6 se muestra la arquitectura lógica propuesta para la implementación de la solución.

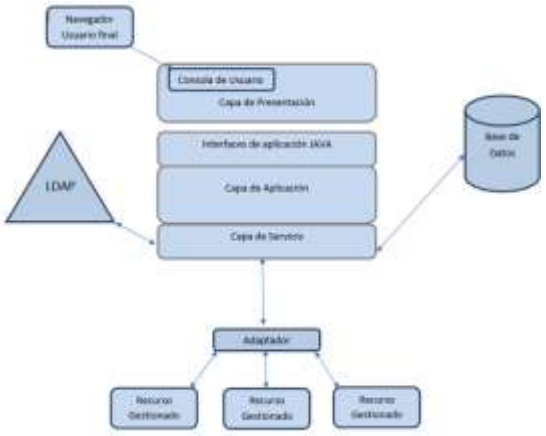


Fig. 6 Arquitectura logica [6]

1) Arquitectura lógica

- CAPA DE PRESENTACIÓN: Esta capa es la encargada de la interfaz gráfica del usuario. Dicha interfaz es proporcionada por la consola del usuario. La consola del usuario es utilizada para el acceso al sistema tanto para los usuarios funcionales como por el administrador de la solución. Se determinó que la mejor forma de acceder a dicha consola es por medio de un navegar de internet, ya que es una aplicación ampliamente utilizad por todo el personal. El navegador de internet oficial utilizado en el MinTic es Internet Explorer 9.

- CAPA DE APLICACIÓN: La capa de aplicación es la se encarga de proveer las funciones de la solución, mediante diversos módulos, a la capa de interfaces. Los módulos que se utilizaron para elaboración de la arquitectura son [6]:

- Manejo de control de acceso. Es el modulo encargado de controlar las operaciones básicas (agregar, modificar y borrar) en los clientes remotos.
- Manejo de Identidades. Es la parte central de la solución, ya que por medio de este se manejan las tareas administrativas de las identidades digitales.
- Manejo del sistema. Es donde se opera lo relacionado con el sistema de manejo de identidades digitales Tivoli Identity Management.
- Manejo de políticas. Es el encargado de las políticas relacionadas con el sistema, así como también de las políticas aplicadas a las identidades digitales.
- Servicios de autorización y autenticación. Es el responsable de realizar las labores de autorización y autenticación del sistema y parte esencial para la realización del proceso de inicio de sesión único.

- CAPA DE SERVICIOS: Esta capa es la que está conectada, mediante un adaptador, de forma directa a los recursos que se necesiten incorporar para el manejo de las identidades digitales. Esta capa está conformada por módulos que permite realizar la intermediación entre las aplicaciones existentes y la solución. Un componente importante de esta capa es el módulo de servicio de datos. Lo anterior debido a que este módulo es el que realiza la conexión directa al directorio Activo de Windows 2008 server, dentro del directorio activo almacena todos los usuarios de los sistemas informáticos existentes, a través del directorio activo, se determina los usuarios que existen, que autorizaciones tienen y que políticas de seguridad se aplican. Dentro de la capa de servicio se plantearon otros componentes dentro del diseño de la arquitectura los cuales son [6]:

- Autorización: Componente que otorga a las interfaces las reglas de autorización de operación de los clientes entre los sistemas de información conectados a la solución.
- Autenticación: Modulo que proporciona los componentes de autenticación utilizado en el diseño los cuales fueron (usuario y contraseña).
- Roles: establece los cambios a los roles de autorización cuando un usuario cambia de rol.
- Políticas de seguridad: Aplica de acuerdo al servicio utilizado.
- Servicio remoto: Servicio esencial encargado de realizar la interacción entre el software de manejo de identidades digitales y los sistemas de información existentes en la empresa.
- Correo electrónico: servicio encargado de notificar los eventos que surgen dentro de la solución de manejo de identidades digitales.
- Flujo de trabajo: Este servicio permite llevar a cabo procesos de auditoria en cuanto a las actividades realizadas por los usuario como son: sistemas de acceso, tipo de transacciones realizadas, tiempo de ejecución entre otros.

- ADAPTADORES: Para lograr la integración de los diferentes sistemas de información con que cuenta el MinTic. De acuerdo a la solución de IBM Tivoli Management, se encontró que es necesaria la utilización de los adaptadores.

1) Arquitectura física

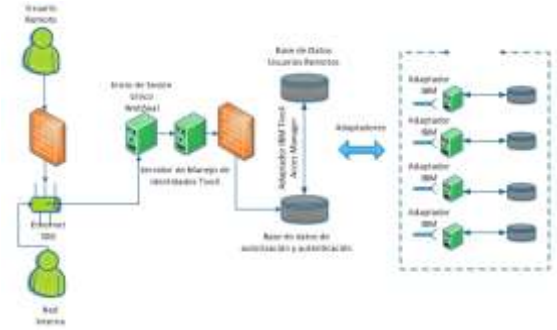


Fig. 7 Arquitectura física propuesta para el inicio único de sesión

Dentro de la arquitectura diseñada, se remplazó el servidor de autenticaciones para ser utilizado como servidor WEBSEAL el cual otorga la función de inicio de sesión único y el servidor restante fue utilizado para la instalación del servidor de manejo de identidades digitales Tivoli Identity Management, el cual realiza la tarea de gestionar los procesos de autenticación y autorización de usuarios por medio de los adaptadores correspondientes hacia los diferentes sistemas de información existentes.

Otro aspecto relevante dentro de la elaboración de la arquitectura es que la mayoría de las conexiones se realiza por medio del adaptador de directorio activo. Como resultado de la arquitectura propuesta, los usuarios y administradores de tecnología de la información del MinTic tiene un único punto de acceso hacia los sistemas de información, para obtener las autorizaciones correspondientes a su rol desempeñado en el flujo de los procesos.

VII. IMPLEMENTACIÓN

Toda implementación tecnológica dentro del Ministerio de tecnología de la Información y las Comunicaciones requiere de un proceso de autorización por parte de la alta gerencia en especial si el proceso afecta de manera significativa a la entidad. Por ello, toda propuesta desde ser presentada en su forma conceptual, ya que con la alta dirección visualiza las implicaciones de la propuesta, autorizando de esa forma a continuar con la siguiente etapa del proceso que es la obtención de costos y del valor de recuperación de la inversión; una vez obtenida la autorización para la inversión, se realiza la fase de adquisición e implementación de la solución sugerida.

Debido a que todo proceso de autorización, desde la propuesta conceptual hasta la adquisición e implementación, puede llevar de 6 a 12 meses, la presente propuesta solo cubre la etapa inicial, siendo un diseño conceptual de la arquitectura de un gestor de identidades.

REFERENCIAS

[1] P. J. WINDLEY. ―DIGITAL IDENTITY. O´REILLY, 2005

[2] J. SCHEIDEL. 2010. ―DESIGNING AN IAM FRAMEWORK WITHORACLE 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] BUECKER, A., FILIP, D, W., CORDOBA, J. P., & PARKER, A. (2009). IDENTITY MANAGEMENT DESIGN. NEW YORK, USA: INTERNATIONAL TECHNICAL SUPPORT ORGANIZATION.