MODELO PARA LA EVALUACIÓN Y SELECCIÓN DE UN SOFTWARE DE SEGURIDAD PARA CONTROLAR EL CICLO DE VIDA DE LA IDENTIDAD DIGITAL

GUILLERMO ANDRÉS VELASCO BURBANO

UNIVERSIDAD ICESI
FACULTAD DE INGENIERÍA
DEPARTAMENTO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES
SANTIAGO DE CALI
2011

MODELO PARA LA EVALUACIÓN Y SELECCIÓN DE UN SOFTWARE DE SEGURIDAD PARA CONTROLAR EL CICLO DE VIDA DE LA IDENTIDAD DIGITAL

GUILLERMO ANDRÉS VELASCO BURBANO

Trabajo de grado Tipo: Solución de un problema concreto

Director
ANDRÉS NAVARRO CADAVID
Ph.D. Director – Grupo de Informática y Telecomunicaciones, i2T

UNIVERSIDAD ICESI
FACULTAD DE INGENIERÍA
DEPARTAMENTO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES
SANTIAGO DE CALI
2011

CONTENIDO

Pág.

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

GLOSARIO DE TÉRMINOS

Appliance: Pila de aplicaciones que contiene el sistema operativo, el software de aplicación y las dependencias necesarias (configuración y datos) para el funcionamiento. Todo está preinstalado, pre integrado, y listo para funcionar.

IM - Identity Management: Gestión de la Identidad

IAM – Identity and Access Management: Gestión de la Identidad y acceso

ISO/IEC 27001: Information technology - Security techniques - Information security management systems – Requirements

PCI: Security Standards Council

RFI - request for information: Proceso estándar de negocio que permite a las organizaciones recolectar información en el mercado, para identificar bondades y requerimientos que puedan suplir una necesidad de negocio.

RFP - request for proposal: Proceso estándar de negocio, el cual permite a las organizaciones adelantar procesos licitatorios de una manera estructurada y organizada. El cual dará como resultado la identificación, calificación y selección del oferente que califique como la mejor opción según los criterios de selección establecidos por la empresa, para el cubrimiento de una necesidad.

RFP: Request for proposal

SGSI: Sistemas de Gestión de Seguridad de la Información

SOX: Sarbanes–Oxley Act

RESUMEN

Las organizaciones y grandes grupos empresariales en su búsqueda por garantizar la seguridad, cumplimiento y control de los distintos accesos a sus aplicaciones de negocio, han abocado múltiples esfuerzos para encontrar una solución de software dé seguridad que permita de una manera eficiente y segura, garantizar el Ciclo de vida de la Identidad digital de sus empleados, contratistas y externos en la organización.

Este documento pretende ofrecer a las organizaciones un modelo para la evaluación y selección de un Software de Seguridad, a través de la definición de la Arquitectura del Sistema, gracias a la aplicación de unas plantillas preestablecidas que permiten de una manera mucho más formal, las esquematización y caracterización de las variables y atributos más significativos de la plataforma. Además se incorporan en el modelo variables propias del proyecto licitatorio y de la organización lo cual permitirá a los lectores e interesados en aplicar el modelo, modificar y adaptar estas características según la conveniencia o situación propia de la organización.

El modelo permitirá a las organizaciones evaluar las diferentes plataformas de Gestión de Identidad, a partir de siete agrupadores que se componen por un total de ciento siete preguntas definidas y caracterizadas dentro del modelo; lo cual permite a las empresas llegar a una calificación y valoración del Sistema por medio del diligenciamiento de la matriz de calificación, la cual es diligenciada y calificada por el panel de expertos.

El modelo desarrollado se aplicó al caso de estudio del Grupo Empresarial Coomeva y las conclusiones fueron comparadas con el proceso que normalmente se utiliza para la evaluación y selección de este tipo de proyectos de software.

1. INTRODUCCIÓN

1.1. CONTEXTO DE TRABAJO

Gran parte de los Grupos Empresariales u Organizaciones de un tamaño similar o superior a 10.000 empleados (directos e indirectos), tienen una grande problemática puesto que a medida que han ido creciendo y expandiéndose en el mercado, de igual manera han ido incrementando sus productos y/o servicios ofrecidos, estos van directamente relacionados con la cantidad de aplicaciones y por ende repositorios de usuarios donde se da el proceso de autenticación o acceso, luego se hace necesario buscar de qué forma se podría hacer gobierno y controlar de manera eficiente el Ciclo de Vida de la identidad del Usuario; que para el caso de estudio serán los empleados, contratistas y terceros, desde el momento en que llegan a la organización hasta el retiro de la misma (Provisionamiento y De-provisionamiento), además de las diferentes novedades que se puedan relacionar con dichos usuarios (Licencias, Vacaciones, Promociones, etc.), buscando que se establezcan mecanismos seguros de autenticación, autorización y auditoria para el acceso a los aplicativos de negocio.

Este trabajo se realizara bajo el contexto de organizaciones denominadas o conocidas como Grupos Empresariales, Grupos Corporativos o Holding Empresarial, este tipo de organización cuentan con una serie de características entre las cuales se contemplan los siguientes aspectos:

- Hay una dependencia jerárquica de la casa matriz o grupo corporativo que la representa.

- La casa matriz es capaz de tomar decisiones las cuales pueden afectar a cada una de las empresas que constituyen el grupo empresarial.

- La casa matriz tiene una participación económica fuerte sobre cada una de las empresas del grupo.

- Cada una de las empresas, unidades o sectores que conforman el Holding Empresarial, basan sus negocios en diferentes actividades y sectores de la industria.

- El Holding empresarial, aprovecha las sinergias y participación del mercado, para establecer y fomentar economías de escala.

- Sus empresas tienen operaciones en la mayor parte del territorio Colombiano, lo cual les permite ofrecer sus productos y servicios a toda la comunidad

- Tienen una participación importante en las propuestas e iniciativas que desarrolle o quiera implementar el Estado y Gobierno Colombiano.

- Suelen contar con un *back office* (procesos administrativos, contables, financieros, etc.) administrados por la casa matriz o una de las empresas del grupo.

- Invierten parte de sus ingresos en Desarrollo Social y Desarrollo profesional.

- El Holding empresarial puede generar una cantidad aproximada de:

  - Más de 10.000 empleos directos
  - Más de 22.000 empleos indirectos

- Son organizaciones vanguardistas que innovan sus productos y servicios mediante el uso de Tecnología, pueden llegar a destinar y presupuestar inversiones del orden de más de veinte millones de dólares (US$20 millones de dólares) por año.

- Se conforman por un número superior a tres empresas.

- Dentro de sus estados financieros se pueden considerar la siguientes cifras importantes:

  - Ingresos totales que pueden llegar al orden de más de cincuenta millones de dólares (US$50 millones de dólares) por año.

o Activos corrientes y no corrientes que pueden sumar más de un billón quinientos mil de dólares (US$ 1.500.000 millones de dólares).

o Pasivos y patrimonio que pueden sumar más de un billón quinientos mil de dólares (US$ 1.500.000 millones de dólares).

o Registrar excedentes que pueden ser del orden de más de seis millones de dólares (US$ 6 millones de dólares)

1.2. PLANTEAMIENTO DEL PROBLEMA

Actualmente existen en el Mercado una cantidad de soluciones que ofrecen controlar por medio de una plataforma de Software y/o Hardware el Ciclo de vida de la Identidad Digital y sus accesos (IAM), sin embargo no existe un modelo para la evaluación y selección de este tipo de Software de Seguridad, por lo cual muchas de las organizaciones al no contar con un esquema de evaluación que considere todas las variables y requerimientos de la plataforma, han implementado soluciones que no han logrado los resultados esperados y finalmente han vuelto a sus esquemas manuales para evitar colapsos en la operación.

1.3. OBJETIVOS

1.3.1 Objetivo general. Desarrollar un modelo para la evaluación y selección de un Software de Seguridad el cual permita a las organizaciones controlar el Ciclo de Vida de la Identidad de los Usuarios; generando mecanismos seguros de autenticación, autorización y auditoria para el acceso a los aplicativos o servicios de negocio, unificando la administración de usuarios y perfiles de acceso.

1.3.2. Objetivos Específicos

- Caracterizar los principales atributos y características funcionales y técnicas, a considerar para el aseguramiento de una plataforma que garantice la adecuada gestión y cubrimiento del ciclo de vida de la identidad.

- Diseñar un modelo para le evaluación y selección de la plataforma basado en las características definidas para el software de Seguridad.

- Validar el modelo propuesto aplicándolo al caso de estudio desarrollado en el Grupo Empresarial Coomeva.

1.4. RESUMEN DE ESTRATEGIA Y MODELO PROPUESTO

La elaboración de este documento y el modelo propuesto, se da con una etapa inicial donde se realiza el respectivo proceso de estudio del mercado de algunas plataformas tecnológicas que pudiesen satisfacer las necesidades técnico/funcionales deseadas en el sistema Gestor de Identidades.

A partir de esa investigación inicial se construye el documento de arquitectura del sistema, SAD, en el cual se identificaron los distintos actores del sistema (Stakeholders), sus expectativas y requerimientos sobre la plataforma, se identificaron las restricciones técnicas y de negocio, se definieron diferentes escenarios de calidad y se plantearon los motivadores del negocio. Esto permitió esquematizar y caracterizar en el Modelo de Evaluación un total de 107 preguntas, agrupadas en siete categorías de evaluación.

Tabla 1. Caracterización del Modelo de evaluación del Software

MODELO DE EVALUACIÓN DE SOLUCIÓN TECNOLÓGICA PARA LA GESTIÓN DE LA IDENTIDAD		Numero de Preguntas
GENERALES RFP	GENERALES	5
	ECONÓMICA	1
EMPRESA	Generales	3
	Modelo de Operación	3
	Económico	5
FUNCIONALES	Administración de Acceso	3
	Administración de Identidades	5
	Administración de Eventos y Seguridad de Información	4
	Generales	4
TÉCNICOS	Generales	9
	Restricciones de Tecnología	4
	QAs	13
	Telecomunicaciones e Infraestructura	24
	Administración de Usuarios	3
	Seguridad	3
	Licenciamiento	3
	Soporte y Garantía	3
	Administración del aplicativo	2
	Normatividad	2
DESCRIPCIÓN DEL SOFTWARE		3
IMPLEMENTACIÓN PROYECTO		1
Restricciones del Negocio		4
	Total	107

Estas variables y requerimientos sobre la plataforma fueron llevadas a un Modelo de Evaluación y Selección construido en un archivo de Excel, el cual consta de varias hojas que se describen a continuación:

- Hoja - Resumen: Vista que muestra el totalizado de variables y agrupadores definidos para el sistema.

- Hoja - RFP: Contiene la Matriz con el Modelo para la evaluación de la Solución Tecnológica para la Gestión de la Identidad - request for proposal (RFP)

- Hoja - RAS: Contiene la relación y clasificación de los atributos y requerimientos del sistema.

- Hoja - Escenarios de QAs: Contiene y estructuran todos aquellos escenarios y atributos de calidad definidos para la plataforma.

- Hoja - Variables de Calificación: Contiene los criterios y variables de calificación del sistema.

- Hoja - Calificación: Lugar donde se realiza el proceso de valoración a cada una de las preguntas dadas por el proveedor de la solución.

- Hoja - RESULTADOS: Lugar donde se realiza el proceso de evaluación y análisis grafico de las calificaciones dadas por el Panel de expertos

Para la validación del Modelo se aplicó al Caso de estudio en el Grupo Empresarial Coomeva, de manera que se envió el documento a cuatro proveedores posicionados a nivel Mundial como líderes de la Industria de Soluciones de Software de Gestión de Identidad, IAM. Una vez fue asegurada la entrega, recepción y disponibilidad de los fabricantes de participar de esta evaluación, se dio un tiempo total de un mes, para la retroalimentación, análisis de preguntas y recepción de respuestas donde finalmente se logró la respuesta de tres de los encuestados.

Una vez entregadas las respuestas de parte de los Proveedores, el panel de expertos, califico las soluciones según los criterios establecidos lo cual permitió generar unos resultados consolidados de cada una de las plataformas evaluadas.

1.5. RESUMEN DE RESULTADOS OBTENIDOS

El modelo propuesto fue aplicado al caso de estudio del Grupo Empresarial Coomeva, donde se invitó a cuatro proveedores que cuentan con las soluciones de IAM – Identity And Access Management mejor posicionadas a nivel mundial, para que aplicaran el modelo propuesto basados en las arquitectura definida y aplicarla a cada una de las soluciones ofrecidas por ellos.

Una vez recibida la respuesta y documentación relacionada, se procedió a realizar la calificación y valoración de sus respuestas con base a los criterios y variables definidas para este fin.

El análisis se realizó por cada uno de los agrupadores o categorías establecidas en el modelo, definiendo para cada de ellas un porcentaje o meta, su calificación y respectivo cumplimiento frente a la meta, las siete categorías analizadas en el modelo fueron las siguientes:

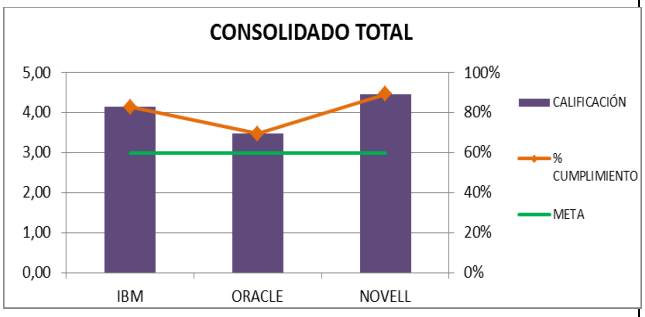
- **Categoria 1 – Generales RFP**
- **Categoria 2 –Empresa**
- **Categoria 3 – Funcionales**
- **Categoria 4 – Técnicos**
- **Categoria 5 y 6 – Descripcion del Software y Entregables**
- **Categoria 7 – Restricciones del Negocio**

Finalmente del resultado del proceso se logró obtener una calificación consolidada de las soluciones evaluadas, lo cual permitió a la organización determinar cuál de las soluciones era la que mejor se adaptaba a las necesidades y expectativas del negocio.

Figura 1. Resultados del proceso de evaluación de la Plataforma IAM

Resultado Consolidado x Solución IAM

PROMEDIO TOTAL PROVEEDOR			
EMPRESA	CALIFICACIÓN	% CUMPLIMIENTO	META
IBM	4,15	83%	60%
ORACLE	3,48	70%	60%
NOVELL	4,47	89%	60%



Finalmente el resultado promediado consolidado del Modelo de evaluación del software de seguridad para el control y administración de la Identidad de los usuarios, determino que la mejor opción costo vs beneficio vs requerimientos arquitecturales del sistema aplicadas a este caso de Negocio, es la solución de Novell en primera opción y en su segunda posición la de IBM. Si bien la solución de Oracle podría considerarse el tema precio sigue siendo uno de los factores por los cuales las organizaciones no implementan este tipo de producto.

Lo resultados de la aplicación del Modelo propuesto, demuestran que la herramienta puede ser aplicable y fácilmente adaptable a industrias y organización que gocen de las características plateadas en este documento, las cuales requieran implementar o evaluar una solución de este tipo para el control y aseguramiento del Ciclo de Vida de la Identidad digital de sus usuarios.

2. MARCO TEÓRICO

En el panorama actual de las organizaciones donde la competencia aumenta de manera apresurada, las empresas han ido aumentando su cantidad de servicios y aplicaciones con el fin de satisfacer diferentes necesidades del mercado, cumplir exigencias de ley o simplemente lanzar servicios diferenciadores que garanticen la supervivencia y el retorno de las grandes inversiones en distintos proyectos, los cuales se convierten finalmente en productos o servicios para sus clientes y usuarios.

La demanda y crecimiento acelerado de las empresas también tiene una serie de secuelas relacionadas con el aumento del riesgo, fallas en la seguridad de los sistemas de información, carencia o nulidad de controles, lo que usualmente genera anotaciones de revisoría o auditorías externas e internas por el no cumplimiento de las políticas que se estén aplicando en el entorno auditado.

2.1. GOBERNABILIDAD Y RIESGO DE LAS TI

Bajo esta situación las organizaciones han comenzado a tomar medidas urgentes para adoptar mejores prácticas que permitan implementar políticas de Gobierno de TI. Según el OECD (Organization for Economic Co-operation and Development) se define el Gobierno Corporativo como *"El sistema con el cual las corporaciones y sus negocios, son dirigidos y controlados"*, lo que quiere decir, que cada organización también debería determinar de qué manera asegura el Gobierno de la Información y sus tecnologías, en las cuales se da la alineación de las estrategias del Negocio y el modelo del negocio.

Por otro lado la definición de lo que se conoce como Gobierno de TI hace referencia al: *"Framework para el direccionamiento de las estructuras organizacionales y los procesos del negocio, los estándares y su cumplimiento; lo que garantiza que los sistemas de información soportan y habilitan el logro de las estrategias y objetivos del negocio"* (1 - Pg.4) lo que además se especifica en cinco principios para adoptar las estrategias de gobierno los cuales son:

- La normatividad y regulación: En Colombia, Circular 052 para entes Financieros, Sistema de Administración de Riesgos (SAR) para entidades de Salud, en otros países como los Estados Unidos Sarbanes – Oxley(SOX), entre otras.

- El creciente valor del capital intelectual.

- La necesidad de alinear los proyectos de Tecnología a la estrategia de la organización, con la finalidad de entregar valor y aportar al logro de los objetivos del negocio.

- El aumento de los hilos de información (complejidad) y por ende los riesgos de la falta de control sobre estos canales, lo que puede llevar a fugas de información que podrían afectar directamente la reputación organizacional.

- El aumento de requerimientos para el cumplimiento (compliance) del manejo de la información y de la privacidad o confidencialidad de la misma: En Colombia la ley Habeas Data para todo tipo de organización.

Todo esto, da a entender que el adecuado manejo de las tecnologías de la información, junto con el efectivo manejo y control del riesgo claramente se convierten en un "driver" habilitador de los objetivos del negocio y las corporaciones. Por ende cada una de las iniciativas y proyectos que se lleven a cabo deben asegurar el adecuado manejo del riesgo y el gobierno de la información, lo que va estrechamente ligado a la estrategia de negocio y aspectos operaciones de la seguridad de la información.

La proliferación y el aumento de la complejidad de las aplicaciones, los sofisticados y globalizados hilos de información, en combinación con el cumplimiento de los requerimientos "flood computer" y la privacidad relacionada a las distintas normatividades a nivel mundial, se han convertido en los "drivers" para las organizaciones que pretenden aumentar sus estrategias orientadas a la seguridad de la información*"* (2 - Pg.5).

A pesar que muchas empresas, piensan que sus sistemas de información son seguros, la cruda realidad es que no lo son, esto se observa diariamente en diarios y periódicos donde se hace evidente el aumento de casos típicos como: ataque de piratas informáticos (Hackers), ciber – crímenes, virus informáticos, fraudes internos o externos, los cuales pueden ser generados desde las aplicaciones o servicios expuestos en la Internet. Lo que finalmente repercute de manera directa en problemas conocidos como la caída o lentitud de las aplicaciones, denegaciones de servicios y finalmente la perdida de disponibilidad, integridad y confidencialidad (CID) de la información.

Luego se hace muy relevante que los procesos de las organizaciones sean diseñados, implementados y apropiados acordes al entorno empresarial y clima organizacional, esto según Alan Calder y Steven Warthinks deberían reflejarse en los siguientes aspectos (1 - Pg.6):

- Políticas, procesos y procedimientos los cuales deben ser diseñados de una manera que refleje el estilo y cultura de la organización.

- Los procesos y procedimientos que sean adoptados deben reflejar los riesgos y sus valoración propia de la corporación

- Es importante que la organización entienda en detalles las políticas, procesos y procedimientos.

- Dar la importancia del caso a la seguridad de la información, el cual esta soportado de manera directa con la Tecnología e Infraestructura. Esto ya que es necesario hacer seguimiento continuo a las políticas establecidas, asegurando que la identificación de riesgos sea un trabajo continuo y garantizado.

Según las observaciones de los autores es claro que los procesos de la organización deben cumplir con las alineaciones estratégicas del negocio y la cultura propia de la organización, como factor importante se debe considerar las TICs (Tecnologías de la Información y Comunicación) y el enfoque orientado al análisis de riesgos, como componentes claves para que sean los habilitadores de las estrategias, objetivos y metas del Negocio.

El enfoque de orientación a riesgos en las TICs, va directamente relacionado con los temas de seguridad de la información de la organización; puesto que lleva a las mismas a cuestionarse y realizar análisis complejos y exhaustivos sobre la situación actual y futura de sus esquemas de seguridad informática, llevándolas al desarrollo de modelos de gestión de riesgos que permitirán a las empresas elaborar planes de acción, gobierno o control, para identificar cada riesgo, clasificarlo, valorarlo y priorizarlo, donde se adoptan una serie de planes de acción sobre cada uno de los riesgos y se determinan las estrategias conocidas dentro de la metodología para evitarlos, transferirlos, mitigarlos, aceptarlos, etc. Este análisis permitirá dar una valoración cuantitativa y cualitativa de cada y su impacto en la organización.

2.2. EVOLUCIÓN DEL MERCADO ALREDEDOR DE LA SEGURIDAD DE LA INFORMACIÓN Y LA GESTIÓN DE LA IDENTIDAD

2.2.1. Riesgos Crecientes en las empresas. Periódicos y fuentes reconocidas en distintos medios de información, reportan situaciones que indican los crecientes riesgos encontrados en diferentes organizaciones citando situaciones críticas de algunas entidades como:

- "Violación en la Seguridad Expone datos de millones de tarjetas de crédito: Hasta 40 millones de números de tarjetas pueden haber estado expuestas, en lo que se conoce como la mayor violación de datos financieros en una serie de casos recientes"[1].

- "En medio de la desaceleración económica, el robo de la identidad sigue siendo una preocupación para los clientes del Banco: Una encuesta encontró que el 54 por ciento de los clientes de un banco muestra preocupación acerca por la seguridad de su dinero y el riesgo del robo de la identidad"[2].

- "Fuga de datos de un Banco amenaza 248.000 clientes en Estados Unidos: Casi un cuarto de millón de consumidores de Carolina del Norte se han visto afectados por una violación reciente de los datos del Bank de New York Mellon. El hecho podría someter a 248.000 habitantes de Carolina del Norte al robo de su identidad"[3].

- "En marcha un tercer ataque informático contra Sony: Un grupo de 'hackers' identificados en el chat Internet Relay, podría estar planeando un nuevo ataque contra los servidores de Sony que tendría como objetivo conseguir información y publicarla en la red. Los 'hackers' han asegurado que actualmente tienen acceso a uno de los servidores y han fijado el ataque para los próximos días[4].

---

[1] INFORMATION WEEK. The Business Value of Technology. Steven Marlin Information Week June 17, 2005. 06:00 PM. http://www.informationweek.com/news/164900904.
[2] The Wall Street Journal. Digital Network. Oct. 2008. http://www.secureidentityssystem.com/assets/files/Oct-WSJ-IDtheftConcern.pdf.
[3] ConsumerAffairs.com Jun 2008. http://www.consumeraffairs.com/news04/2008/10/nc_mellon_corp.html
[4] CNET.com. Exclusive:Third attack against Sony planned. May 2011. http://news.cnet.com/8301-31021_3-20060227-260.html.

En particular este última noticia causa curiosidad puesto que se da bajo la cuna de la aparición de organizaciones que se han llamado *legiones* las cuales dicen defender la libertad de la información y el no a la censura en Internet; al mismo tiempo que ocurre con la prohibición en ciertos países del acceso a sitios como WikiLeaks (http://www.wikileaks.ch), el surgimiento del grupo Anonymous y en particular en Colombia el desarrollo de leyes como la denominada *"Ley Lleras - proyecto de ley que busca regular la propiedad intelectual en internet en Colombia"*, demuestra que el tema de las seguridad informática en los sistemas de información no es despreciable en un mercado global de las corporaciones, donde las aplicaciones empresariales poco a poco han migrado de la plataforma cliente - servidor y sus confiables zonas desmilitarizadas – DMZ, hacia un mundo de comunicaciones globales y plataformas tipo WEB; en donde se da un intercambio de servicios a través de Web Services que son consumidos por otras empresas o usuarios y en donde de una u otra forma los riesgos de las aplicaciones y la información que circula a través de estas, se incrementan por la "desprotección" y exposición de servicios a la red de redes - Internet.

2.2.2 Evolución de la seguridad informática. La seguridad de la información ha llevado un proceso evolutivo interesante el cual comienza aproximadamente en los años 80s, contextualizando en esta época se dio el *bum* de las redes de confianza, donde había una armonía entre todas las personas amantes de las tecnologías, donde un nuevo protocolo, dispositivo, programa o lenguaje de programación era aplaudido por la comunidad de activistas de las TICs, las empresas, universidades y comunidades que crecían sin control y aprovechaban las tecnologías de comunicación para poder acortar distancias y lograr romper las barreras físicas de la información.

Toda esta armonía fue irrumpida en el momento en que algunas personas cayeron en cuenta del poder de la información que corría o fluía por todos estos medios o sistemas de información; el primer caso documentado por la comunidad como violación a un sistema de información, fue presentado en el libro The Cuckoo's Egg por el autor Cliff Stoll en el año 1989[5], en este libro el autor relata cómo descubre un aparente error contable en los sistemas de información de la compañía, donde al parecer había una diferencia de 75 centavos de dólar en ciertas transacciones, por lo cual comienza a investigar y cae en cuenta que alguien se ha introducido en sus sistemas y ha robado los accesos del súper usuario (root), de esta forma inicia un seguimiento detallado de las actividades del intruso, en lo que es considerado el primer caso documentado de una persecución a un cracker.

[5] STOLL, Cliff. The Cuckoo-s Egg: Tracking a Spy Through the Maze of Computer Espionage. Estados Unidos, 1989. ISBN 0-385-24946-2.

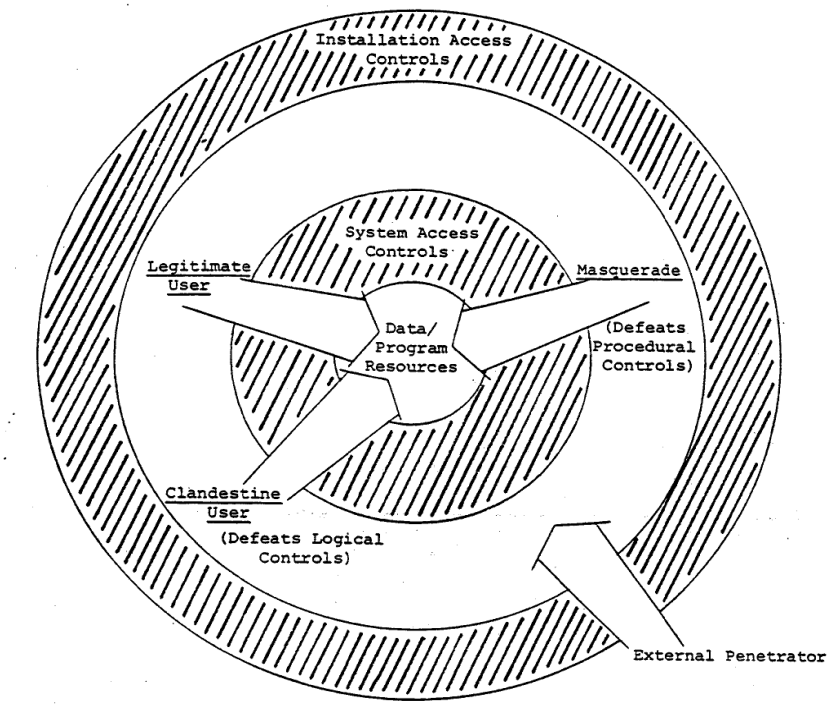
A manera visionaria en el año 1980, el autor del documento denominado: Computer Security Threat Monitoring and Surveillance[6], expuso los primeros términos relacionados con la seguridad de la información, los cuales se ven resumidos en el siguiente aparte:

> *"Amenaza: la posibilidad de un intento deliberado y no autorizado de:*
> *a) Acceder a información*
> *b) Manipular información*
> *c) Convertir un sistema en no-confiable o inutilizable*
>
> *Riesgo: Exposición accidental e impredecible de información, o violación de la integridad de operaciones debido al malfuncionamiento del hardware o diseño incorrecto o incompleto del software.*
>
> *Vulnerabilidad: una falla conocida o su sospecha tanto en el hardware como en el diseño del software, o la operación de un sistema que está expuesto a la penetración de su información por una exposición accidental.*
>
> *Ataque: Una formulación específica o ejecución de un plan para llevar a cabo una amenaza.*
>
> *Penetración: Un ataque exitoso; la habilidad de obtener acceso no-autorizado (indetectable) a archivos y programas o el control de un sistema computarizado"[7].*

Conceptos y definiciones que a la fecha siguen siendo conocidas y asociadas a la seguridad de la información, donde además se puede identificar distintos tipos de amenazas y controles que los administradores de las TI, siguen diferenciando desde el momento del diseño de las redes, de la infraestructura de servidores, sistemas operativos, hasta la concepción y estructuración de los programas informáticos propios de la organización, ver figura 2.

[6] J.P. Anderson. Computer Security Threat Monitoring and Surveillance. Technical Report Washington, PA, April 1980.
[7] Ibid. p. 15.

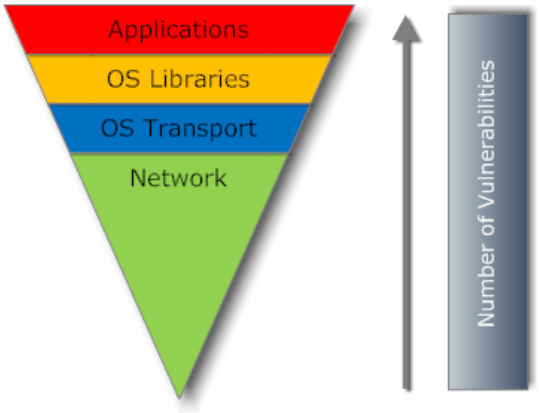
Figura 2. Casos Generales de Amenazas



Fuente: J.P. Anderson. Computer security threat monitoring and surveillance. Technical Report Technical Report. Washington, Pag 8.

En cada una de estos componentes o capas se dan una serie de amenazas que pueden atravesar todo el modelo OSI, entre las amenazas más conocidas se referencia roles de personas como los Crackers y Phreakers, temas culturales denominados Ingeniería Social, hasta las técnicas de la informática como: Scanning, Smurf o broadcast storm, Sniffing, Spoofing, Virus Troyanos, Exploits, Denegación de Servicios, Bombardeo de Email (SPAM), Phishing, Inyección SQL, entre otros. Este tipo de amenazas y que parte del modelo OSI es la más impactada por la relación fehaciente sobre las vulnerabilidades encontradas, se observa en la figura 3.

Figura 3. Numero de vulnerabilidades en redes, Sistemas Operativos y aplicaciones.



Fuente: http://www.sans.org/top-cyber-security-risks/trends.php

En este orden de ideas la evolución de la seguridad informática muestra sus avances desde los años 80´s, donde se concentraba en simplemente aislar la información de las personas por medio de implementación de mecanismos físicos que restringieran el acceso a los distintos centros de datos y a las computadoras como tal, luego en los años 90´s con la masificación del Internet y sus servicios, la información supera las barreras físicas y es por eso que se hace importante el establecimiento de controles a las vulnerabilidades electrónicas de los distintos componentes o las plataformas por donde se movía dicha información, las amenazas dejaron de ser solo externas y personas inescrupulosas entendieron que la información era muy valiosa para distintas compañías.

Durante esta década hasta el segundo milenio, comienzan a desarrollarse aplicaciones de seguridad que permitirían “blindar” a las empresas de ciertos tipos de ataques, establecer perímetros de seguridad internos y externos y por ende generar mayor confidencialidad y protección de la información.

Lastimosamente así como la seguridad iba desarrollando barreras de protección, habían personas u organizaciones que a la par y apalancados en conocimientos tecnológicos e informáticos, iban desarrollando herramientas para penetrar, evitar o sortear todas estas barreras y controles, elementos que ya fueron referenciados en este documento.

Ya para el año 2000 y a la fecha, la seguridad de la información sufre una transformación importante en el sentido de que surgen entes internacionales los cuales se interesan en investigar y desarrollar *FrameWorks* o conjuntos de buenas prácticas para afrontar todos los temas relacionados a la seguridad de la información, de una manera organizada, por pasos y que pueda ser certificable por otros entes de control, lo que aseguraría y permitiría establecer relaciones de confianza en una globalización general de la industria.

Como por ejemplo el estándar más reconocido de la industria es la norma internacional de seguridad de la información ISO/IEC 27001 en la cual se especifican los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI), además permite establecer controles que sirven a las organizaciones a esquematizar la seguridad de todos los componentes de la corporación tantos físicos, humanos e informáticos, ver tabla 2.

Tabla 2. Norma ISO 27001, Anexo A, Objetivos de control y controles.

A.5 POLITICA DE SEGURIDAD
A.6 ORGANIZACIÓN DE SEGURIDAD DE INFORMACION
A.7 GESTION DE ACTIVOS
A.8 SEGURIDAD DE LOS RECURSOS HUMANOS
A.9 SEGURIDAD FISICA Y DEL ENTORNO
A.10 GESTION DE COMUNICACIONES Y OPERACIONES
A.11 CONTROL DE ACCESO
A.12 ADQUISICION, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACION
A.13 GESTION DE LOS INCIDENTES Y LAS MEJORAS EN LA SEGURIDAD DE INFORMACION
A.14 GESTION DE CONTINUIDAD DEL NEGOCIO
A.15 CUMPLIMIENTO

Fuente: http://www.iso.org

Los marcos de referencia asociados a temas de Gobierno de TI (COBIT), o modelos relacionados con la gestión y administración de los riesgos, llevan al siguiente paso en la evolución de la seguridad informática, puesto que estas normas deben llevarse a la realidad no solo en documentos físicos o almacenados en algún repositorio de la compañía, sino que también deben hacerse realidad por medio de la automatización o adopción de herramientas y plataformas tecnológicas que sean habilitadoras de las definiciones de Gobierno, Riesgo y Seguridad de la información, propias de cada organización.

Para el año 2000 toma relevancia los temas relacionados al análisis de las vulnerabilidades de los sistemas de información, dispositivos de red e infraestructura de servidores, es por esto que comienzan el surgimiento de herramientas o "appliance" que se configuran para realizar estos análisis, que permitan la generación de reportes y realizar análisis de riesgos y planes de acción para mitigarlos o cerrarlos. Al nivel de aplicaciones empiezan a escucharse conceptos como el "Single Sign On" el cual es un primer acercamiento a una solución de la problemática expuesta, puesto que con este tipo de soluciones las organizaciones buscaron por un lado *eficientizar* el trabajo de los clientes y usuarios, controlar los accesos y por otro asegurar que el acceso desde un dispositivo sea único y confiable. El tiempo demostró que este tipo de soluciones no eran tan eficientes como se *"vendían"* y que por el contrario aumentaba los riesgos de la organización al exponer a que con el robo de una sola identidad, el individuo perpetrador, pudiera moverse dentro de la compañía de manera integral y sin mayores obstáculos. Todo el camino descrito en la etapa evolutiva de la seguridad de la información desde los 80 al 2000, se puede resumir en la figura 4.

Figura 4. Evolución de la seguridad informática en las últimas décadas.

Fuente: Presentación IAM Novell, http://www.novell.com/solutions/identity-and-access/

Para los siguientes años se dio la evolución de ese primer concepto asociado a la administración del ciclo de vida de la identidad de las personas el cual se conoció como *single sign on*, en ese momento se hizo evidente y necesario la incorporación de los factores de gobernabilidad, riesgo y cumplimiento

mencionados con anterioridad, lo cual dio cabida al surgimiento de conceptos relacionados con el manejo de los roles de la organización, el control de accesos a las aplicaciones asociadas al rol o cargo, la correlación de eventos, alarmas y reportes del servicio en su totalidad.

La integración de la identidad adicionando el manejo del ciclo de vida dentro de la corporación con todas sus variaciones y el cumplimiento de los entes de control de una manera mucho más eficiente, óptima, estandarizada y que además tuviera un ROI demostrable para la organización. Todo este camino descrito en la etapa evolutiva de la seguridad de la información desde el 2000 al presente, se puede resumir en la figura 5.

Figura 5. Evolución de la seguridad informática en las últimas décadas.

Fuente: Presentación IAM Novell, http://www.novell.com/solutions/identity-and-access/

2.3. TENDENCIAS DEL MERCADO

El despliegue generalizado de los sistemas de recolección, procesamiento y distribución de la información personal junto con su identificación en el servicio, hace a cada persona vulnerable al robo en línea de los datos de identidad, lo cual perjudica la confianza en las distintas tecnologías de la información sobre las cuales se soporta. Esto ha llevado a la industria a la expansión de la investigación sobre variados temas de la gestión de la identidad, incluyendo la mejora de la confiabilidad y la privacidad[8] .

La información personal es usualmente usada para realizar transacciones y ofrecer servicios personalizados. La información de la identidad de la persona, como el nombre, los atributos propios como edad, sexo, profesión, hasta incluso datos biométricos permiten la liberación y transferencia de datos sin fronteras administrativas [9] . El uso de atributos de identificación personal los cuales constituyen la identidad digital, hacen parte integral de todo el servicio o transacción que va a través de la red, envolviendo temas de gobierno, reglas de negocio y comprometiendo al mismo individuo. Esto lleva a que las relaciones de confianza se vuelvan claves y acordes a las necesidades de las distintas partes involucradas en la prestación del servicio.

En general se podría hablar que la tendencia del mercado alrededor de la seguridad de la información debe apalancar las distintas iniciativas empresariales soportadas en factos claves como:

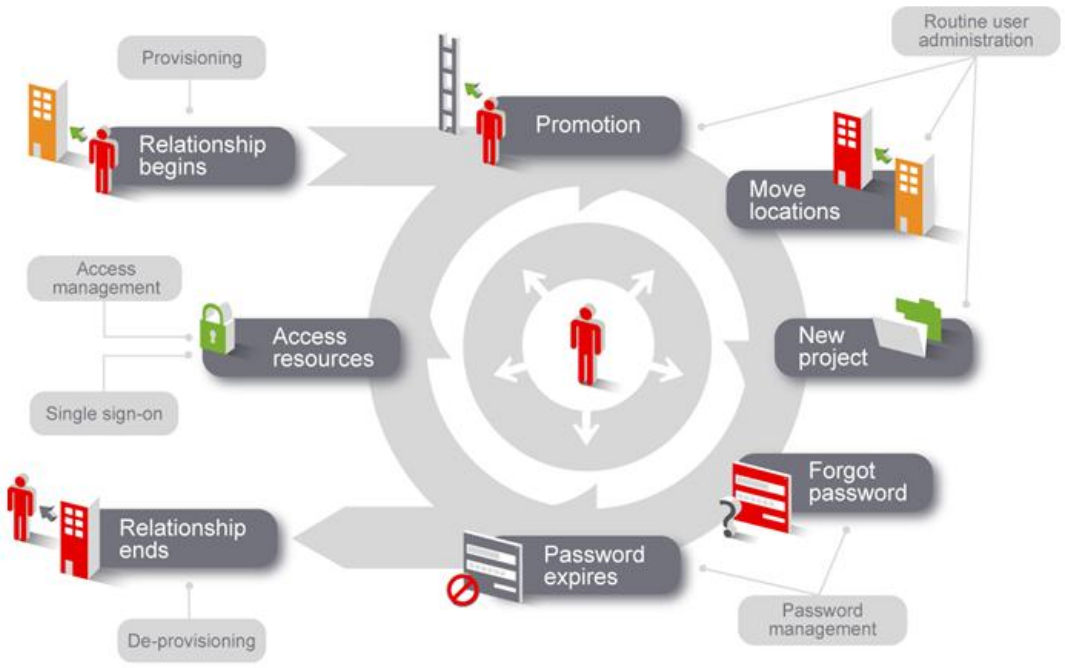
- Soporte de soluciones e iniciativas de GRC (Governance, Risk and Compliance) para las TI
- Evitar violaciones de regulaciones gubernamentales y de la industria
- Evitar fuga de propiedad intelectual
- Disminuir el costo del cumplimiento mediante la integración, consolidación y automatización
- Uso de estándares abiertos e independencia de la plataforma

2.3.1. Acceso y Manejo del ciclo de vida de la identidad. El ciclo de vida de la identidad denominado o administrado por el proceso conocido como Identity

[8] Piotr Pacyna, Anthony Rutkowski, Amardeo Sarma & Kenji Takahasi. Trusted Identit y for All: Toward Interoperable Trusted Identit y Management Systems, COMPUTER – IEEE Computer Society, 0018-9162/09/$25.00 © 2009 IEEE.
[9] Ibid.

Access Management (IAM) (Gestión de Identidades y Accesos), tiene como objetivo principal la identificación única e integral del individuo o persona en uno o varios sistemas de información, sin importar el lugar, el espacio o el momento (como un país, red, u organización) y además controlar de manera adecuada los acceso autorizados y permitidos a los recursos de dicho sistema, ver figura 6:

Figura 6. Ciclo de vida de la Identidad.



Fuente: Presentación IAM Novell, http://www.novell.com/solutions/identity-and-access/

Estudios adelantados por la empresa Deloitte, indican que el adecuado manejo del riesgo, gobernabilidad y el cumplimiento puede llegar a producir valor para la organización ya que para las empresas "el cumplimiento debe ser uno de los drivers principales para que las corporaciones inviertan en soluciones de identidad, puesto que va directamente relacionado con variables críticas para el negocio como son"[10] .

[10] DELOITTE, Markus Bonner. http://www.oracle.com/global/hu/events/20070215_SecurityBB/01%20Deloitte%20eloadas%20-%20Compliance%20Governance%20Risk%20in%20Identity%20and%20Access%20Management.pdf

Motivación empresarial:

- Mejorar la productividad: Optimización, estabilidad, flexibilidad.
- Seguridad: Riesgo y cumplimiento

Motivación legal:

- Incremento en la cantidad de normas regulatorias (Circular 052, SOX, PCI, etc.)

- Minimización del riesgo operativo en los informes financieros, deben ser veraces y certificables, que es el caso de la regulación SOX aplicada en los Estados Unidos.

- Las auditorías internas y externas están cada vez más centradas en el control de los procesos de TI.

- Mayor responsabilidad legal de las personas responsables de ejecutar y garantizar los mecanismos de control. Como es el caso de los representantes legales de las empresas (usualmente los gerentes).

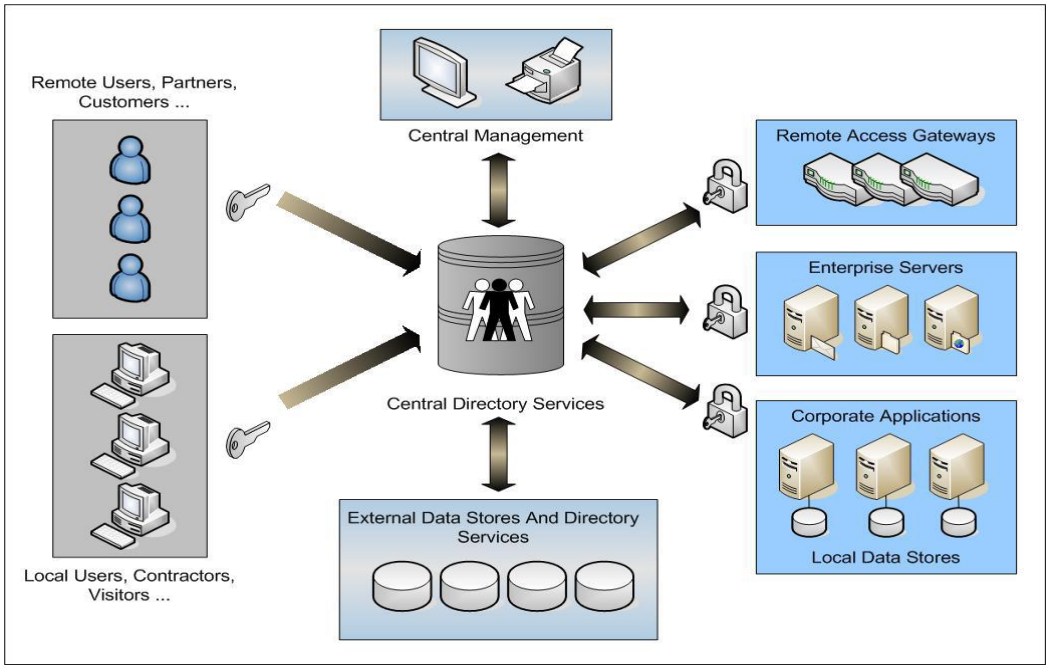
Según el autor Axel Larsson, una plataforma de este tipo obliga a las organizaciones a reemplazar las conexiones múltiples ad-hoc que se solían hacer entre distintos sistemas y aplicaciones, a un solo puente hacia el sistema de gestión de identidades y accesos, lo cual impacta al reducir los costos operativos y administrativos y además permite que se puedan soportar más aplicaciones, al aumentar la longevidad y la utilidad de los sistemas de información (administrativos) tipo *legacy*, así como la información albergada en las mismas[11]. Ver figura 7.

La gestión centralizada de la información de identidad a través de una solución o plataforma de Gestión de Identidades y Accesos, permitiría la consolidación del acceso de toda la información de la identidad, la cual está dispersa en diferentes bases de datos que contienen la información del usuario y las políticas de acceso. Los cambios realizados sobre la identidad en aquella consola centralizada permitirán sincronizar los cambios con los distintos repositorios internos y externos para garantizar la información de la identidad del usuario, su coherencia, disponibilidad, integridad y confidencialidad, al igual que las políticas de autenticación y acceso definidas por la empresa.

[11] LARSSON, Alex. LARSSON, Axel. Drew University. A Case Study: Implementing Novell Identity Management at Drew University, Drew University, 2003.

Con la administración de identidades, la visibilidad de los accesos es elevada, esto permite que los administradores de TI, áreas de auditoría u organismos de control, creen una imagen real y en línea, del número y tipo de cuentas que usa determinado usuario sobre toda la organización, además de las políticas que lo rigen. Luego los riesgos de accesos no autorizados se reducen, los errores asociados con el almacenamiento de datos múltiples se eliminan, el acceso a través de cuentas desconocidas o ilegítimas van al mínimo y las actividades de acceso de los usuarios son monitoreadas y registradas para cumplir los estrictos requisitos regulatorios (compliance).

Figura 7. Centralización de la administración de cuentas – Solución de Gestión de la Identidad



Fuente: A10 Networks WhitePaper, Identity Management and Sarbanes-Oxley Compliance, Pg 9 - Sep 2005. http://frwebgate.access.gpo.gov

2.4. PROYECTOS DE SOFTWARE Y SU RELACIÓN CON LA ARQUITECTURA COMPUTACIONAL

Muchas organizaciones a partir de la necesidad de desarrollar una serie de servicios, productos o simplemente por el cumplimiento de temas normativos y de ley, han adelantado una cantidad importante de iniciativas o proyectos los cuales terminan en la búsqueda de soluciones, plataformas o appliance de software, que de una manera relativamente rápida o sencilla, ayuden al despliegue y cubrimiento de la necesidad.
Para realizar este tipo de procesos muchas de estas empresas, realizan la búsqueda de soluciones tecnológicas que satisfagan los requerimientos de negocio, a partir de investigaciones de mercado en las cuales se pueden realizar a través de un proceso de recolección de información, RFI, o cuando se tienen mucho más claros y asentados los requerimientos del sistema se realiza a partir de procesos licitatorios tipo RFP.

Por otro lado, en la última década se han desarrollado, definido y clarificado conceptos importantes alrededor de los que se conoce como Arquitectura de los sistemas computaciones o Arquitectura de Software, entre estas definiciones se puede destacar la siguiente: “Una Arquitectura refleja un conjunto de decisiones significativas sobre la organización de un sistema, la selección de elementos estructurales que componen el sistema y sus respectivas interfaces, junto con su comportamiento especificado a través de las colaboraciones entre estos elementos” [12]. Además, bajo estos principios se determina que el establecimiento de una arquitectura sirve de manera general para:

- Definir la estructura del sistema
- Definir el comportamiento del sistema
- Lograr enfocar el análisis en los elementos significativos del sistema
- Generar propiedades genéricas para el sistema
- Identificar las necesidades de todos los stakeholders (ejemplo: usuario final, administrador de sistema, vendedor, cliente, desarrollador, gerente de proyecto, etc.)
- Reflejar las decisiones del sistema con base a unos criterios establecidos

La cual para estructurarse de una manera adecuada, puede utilizar una serie de plantillas en los cuales se consideran los elementos claves para el desarrollo de un documento que describe la arquitectura del sistema o el software (SAD), elementos que de manera resumida se especifican a continuación.

[12] Universidad ICESI, Maestría en Gestión de Informática y Telecomunicaciones, Introducción a la Arquitectura de Sistemas Computacionales, pagina 10

Primero se debe considerar que un elemento de arquitectura hace referencia *a una pieza fundamental a considerar cuando se realiza la construcción o definición de un sistema.* Lo cual quiere decir que los siguientes elementos son vitales para la adecuada definición de la arquitectura de un sistema computacional:

- Stakeholders - Interesados: Hace referencia a una persona, grupo o entidad que está interesada, que genera requerimientos, objetivos o refleja sus aspiraciones y expectativas en la elaboración de la arquitectura del sistema.

- Architectural Descriptions - Descripción de arquitectura (AD): Son una serie de entregables que permiten documentar la arquitectura del sistema. Con estos documentos los cuales los Stakeholders, pueden tener una mayor claridad, entendimiento y satisfacción demostrada, sobre el cumplimiento de todas sus expectativas en la definición de la arquitectura.

- View - Vista: Es una representación de uno o más elementos de la estructura de la arquitectura, que ilustran o representan un set de componentes del sistema y sus respectivas relaciones. Una descripción de una arquitectura se compone de una o varias vistas.

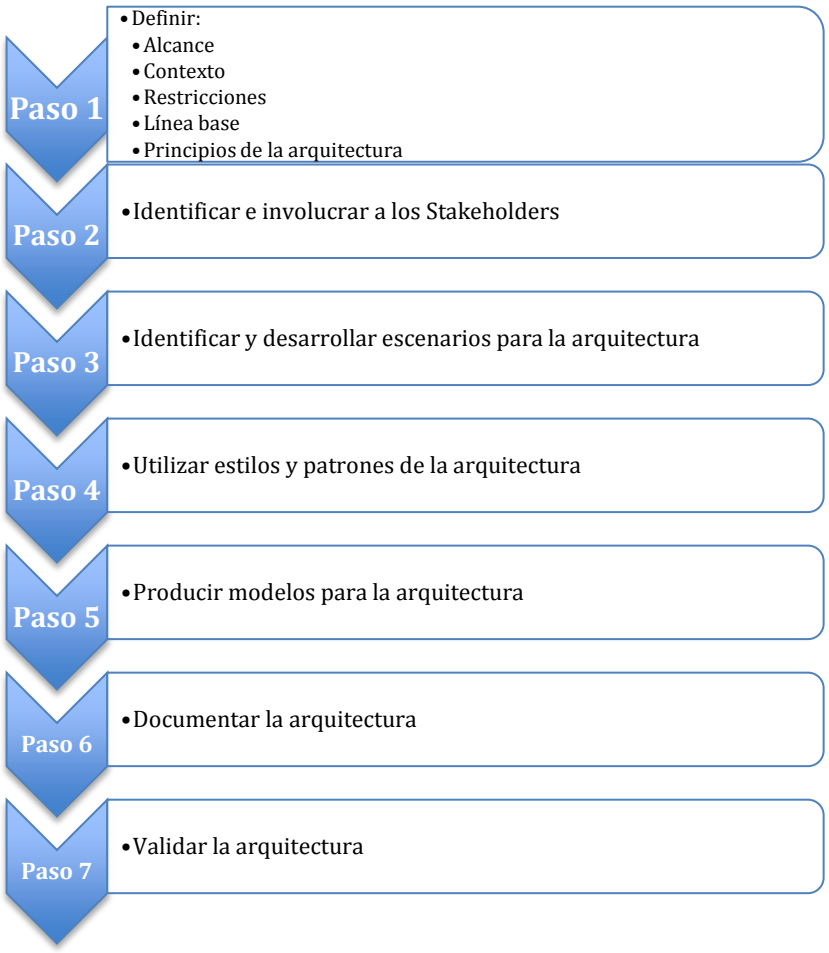
- ViewPoints - Puntos de Vista: Es una especificación que describe los patrones, plantillas y sus conversiones para un determinado Stakeholders y sus correspondientes expectativas. En estas se identifican las relaciones con otros puntos de vista, sus guías, diagramas, principios y plantillas, las cuales servirán como guías para crear el documento de arquitectura AD. Un punto de vista es un patrón para construir una vista. Entre los puntos de vista más utilizados se encuentra el punto de vista funcional, punto de vista de despliegue, punto de vista de información, entre otros.

- Architectural Perspective o Perspectiva de arquitectura: Se define como la colección de actividades, tácticas y pautas, utilizadas para asegurar la identificación de un grupo de atributos y propiedades de **calidad**, las cuales deben considerarse alrededor de un variado número de vistas de la arquitectura del sistema. Entre las perspectivas más utilizadas están la seguridad, eficiencia, fiabilidad, mantenimiento, entre otros.

Según el autor Nick Rozanski y Eoin Woods en su libro Software Systems Architecture, el proceso para la elaboración de una arquitectura de software se

podría representar como una secuencia de pasos ordenados, que se esquematizan de manera resumida en la siguiente figura.

Figura 8. Esquematización del Proceso para la construcción de una Arquitectura de Software



Fuente: Detalles del proceso referirse al capítulo 7, página 73, Rozanski, Nick y Woods, Eoin. Software systems architecture

Sin embargo, a pesar de que se ha documentado mucho sobre el tema de arquitectura de los sistemas e inclusive se han generado estándares internacionales para describir la arquitectura de los sistemas computacionales como el estándar *IEEE 1471*, no es muy común encontrar proyectos de software a nivel empresarial, donde se utilicen este tipo de herramientas, buenas prácticas y

templates; para elaborar y construir documentos que describan la arquitectura del sistema, SAD: Software Architecture Description, y que por ende se apliquen estas técnicas que permitan mediante un proceso mucho más formal, la selección, evaluación y adjudicación de las licitaciones de este tipo que se estén adelantando en los distintos tipos de organizaciones.

3. MODELO DE EVALUACIÓN DE SOFTWARE DE SEGURIDAD

3.1. INTRODUCCIÓN

Bajo el panorama anteriormente descrito se plantea como estrategia la adopción del modelo de descripción de la arquitectura del sistema, SAD, basado en las plantillas elaboradas por la Universidad de Los Andes en el curso Arquitectura de Software[13].

Ahora bien, mediante la aplicación y esquematización de un documento de arquitectura se pretende describir de una manera mucho más formal, los requerimientos funcionales y no funcionales, así como lograr la identificación de los atributos arquitectónicamente significativos, la elaboración de escenarios de calidad; considerando todas las variables importantes y relevantes de cada Organización como son las restricciones propias del Negocio, las restricciones de Tecnología, la expectativas de los Stakeholders, los Motivadores de Negocio, etc. Todas estas características serán determinantes al momento de evaluar y seleccionar la plataforma que cumpla la mayor parte de variables o requerimientos del Negocio.

Una vez elaborado el documento de Arquitectura de Sistema SAD, se construirá un modelo que permita la evaluación y selección de un Software de Seguridad para el controlar del Ciclo de Vida de la Identidad, el cual podrá ser fácilmente adoptado por distintas organizaciones y que será un insumo importante en los distintos procesos de Licitación o de búsqueda de software con este tipo de características.

[13] Universidad de los Andes, Departamento de Ingeniería de Sistemas y Computación, Plantilla Documento de Arquitectura en: http://sistemas.uniandes.edu.co/~isis3702/dokuwiki/doku.php?id=sad.

3.2. DOCUMENTO DE ARQUITECTURA DEL SISTEMA (SAD)

3.2.1. Descripción General del Sistema a Desarrollar. Esta sección describe la funcionalidad y el propósito del sistema o subsistemas cuya arquitectura es descrita en este documento:

La solución o plataforma tecnología que se busca se define como IAM o Identity and Access Management (Gestión de Identidad y Acceso) el cual a nivel general se puede describir como un sistema encargado de automatizar los procesos de creación, actualización y eliminación de usuarios y perfiles de acceso a los aplicativos o servicios dispuestos por la organización, incluyendo mecanismos de seguridad a las funciones de autenticación, autorización, y auditoria (AAA), todas estas asociadas a los aplicativos o servicios durante la permanencia de los usuarios (empleados, contratistas y/o terceros) al interior de la organización o bien lo que se conoce como el ciclo de vida de la Identidad.

Tabla 3. Solicitudes del usuario

Id	Solicitudes del usuario	Descripción	Func.	Arq. Sig.
1	Conectores de Aplicaciones	El sistema debe soportar conectores a aplicaciones desarrolladas In house en JAVA, Proccesss Server, PHP, . NET, Cobol		X
2	Conectores de Bases de Datos	El sistema debe soportar integración Nativa con motores de Bases de Datos tipo Oracle, Sybase, DB2, SQL Server		X
3	Único repositorio	El sistema debe integrar los distintos usuarios y generar un único ID (único usuario y clave de acceso) para los distintos accesos a las aplicaciones y/o servicios	X	
4	Sincronización 7 x 24 x 365 días	El Sistema debe sincronizar y actualizar la información con los distintos repositorios en cada momento y hora del día sin restricción de horario (7 x 24 x 365 días)		X Eficiencia
5	Pantallas de administración	El sistema debe permitir mediante una interfaz web el ingreso y administración de cada uno de los componentes que conformen la	X	

Id	Solicitudes del usuario	Descripción	Func.	Arq. Sig.
		solución (administración, configuración, parametrización de nuevos servicios).		
6	Pantallas de usuario final (Portal de autoservicio)	El sistema debe permitir mediante una interfaz web el ingreso de los usuarios finales, para poder auto gestionar algunos servicios propios de su identidad (Mecanismos de autoservicio) como el cambio y recordación de clave, actualización de datos generales, etc.).	X	
7	Compatibilidad con dispositivos	El sistema debe permitir que el portal de autogestión pueda ser accedido desde dispositivos móviles (Celulares, eBooks, Palms, etc)		X
8	Plataforma abierta	La plataforma debe ser abierta en el sentido que pueda correr en diferentes Sistemas Operativos y/o arquitectura de servidores donde se vaya a desplegar		X Mantenimiento
9	Alta disponibilidad	El sistema debe garantizar esquemas de alta disponibilidad continuidad tecnológica en caso de un incidente y/o problema		X Fiabilidad
10	Flexibilidad de la Plataforma	El sistema debe ser fácilmente adaptable a nuevas plataformas, aplicaciones y/o servicios que sean implementados o desplegados		X Mantenimiento
11	Sincronización y conciliación de repositorios	El sistema debe permitir la sincronización y actualización de los múltiples repositorios en un tiempo no mayor a 5 minutos		X Eficiencia
12	Sincronización efectiva y eficiente	El sistema debe soportar un promedio de 10000 usuarios diarios, con una proyección estimada de un 10% por cada año		X Mantenimiento
13	Storage On-line y esquema de backup	El sistema debe permitir configurar la información transaccional on-line y definir cual se almacena mediante un proceso de backup.		X
14	Esquemas de seguridad de la plataforma: Perfiles de Acceso	El sistema debe garantizar que los accesos a las distintas aplicaciones y/o servicios, sean otorgados según los lineamientos de seguridad y perfilización establecidos en las matrices de perfiles.		X Seguridad

Id	Solicitudes del usuario	Descripción	Func.	Arq. Sig.
15	Esquemas de seguridad de la plataforma: Nombramiento y contraseñas	El sistema debe permitir definir estándares para el nombramiento de usuarios y contraseñas que serán sincronizadas con los diferentes aplicativos o servicios	X	
16	Esquemas de seguridad de la plataforma: Mecanismos de autenticación	El sistema debe contar con mecanismos de autenticación de doble y triple factor (token, huella digital, iris, etc.) para controlar el acceso a servicios críticos definidos por la organización		X Seguridad
17	Esquemas de seguridad de la plataforma: Informes de auditoria	El sistema debe permitir generar informes programados y en tiempo real para conocer el comportamiento de los usuarios sobre las aplicaciones y servicios habilitados	X	
18	Esquemas de seguridad de la plataforma: Correlación de eventos	El sistema debe permitir configurar alertas sobre eventos *extraños* definidos por los administradores de seguridad	X	
19	Conectores de Aplicaciones	El sistema debe permitir conectarse con Sistemas ERP y CRM, definidos por la organización		X Mantenimiento
20	Diseño de flujos de trabajo	El sistema debe permitir el diseño e implementación de flujos de trabajo (workflows) a través de la herramienta de administración web	X	
21	Simulación de ambientes	La solución debe contar con herramientas de diseño y simulación de modelos de aprovisionamiento antes de la implementación	X	
22	Módulos del sistema	La solución debe contar con módulos independientes de administración como: - Administración de identidad - Administración del Acceso - Administración de Eventos y seguridad de información - Gobernabilidad	X	
23	Arquitectura basada en eventos	La solución debe basar su arquitectura a través del manejo de eventos disparados por las distintas aplicaciones, repositorios o plataformas.		X

Id	Solicitudes del usuario	Descripción	Func.	Arq. Sig.
24	Arquitectura basada en conciliación	o por conciliación de repositorios		X
25	Diseño de reglas de negocio	El sistema debe permitir definir y administrar reglas de negocio, roles y perfiles organizacionales.	X	
26	Arquitectura basada en Meta Directorios	La solución debe contar con “Meta Directorios” para el manejo e integración de repositorios		X
27	Pantallas y visualización de la plataforma	La solución debe ser 100% Web-Enabled en todos sus componentes de administración	X	
28	Granularidad sobre la plataforma	El sistema debe permitir la configuración de roles, perfiles y usuarios de administración de manera granular por las distintas opciones de la solución		X Seguridad
29	Eventos reportados desde el sistema de Gestión Humana	El sistema debe “*recepcionar”* de manera automática, todos los eventos o novedades presentadas en el sistema de administración de gestión humana (ingreso de personal, promociones, vacaciones, retiros, etc.)		X
30	Crecimiento de la solución	La solución debe garantizar el desarrollo o disponibilidad de conectores **nativos** adicionales, los cuales permitan la integración a nuevas plataformas, aplicaciones, sistemas operativos, sistemas de correo electrónico, mainframes, lenguajes de programación o de scripting, PBX, bases de datos y otros.		X Mantenimiento
31	Acceso Web Single Sign On	La plataforma debe contar con un módulo para la configuración de aplicaciones que requieran tener acceso Web Single Sign-On (Web-SSO)		X
32	Mecanismos Federados	El sistema debe contar con mecanismos de identidad federada para conexiones futuras a sistemas de otras empresas del grupo o aquellas donde se tenga algún tipo de participación o convenio	X	

Id	Solicitudes del usuario	Descripción	Func.	Arq. Sig.
33	Diseño de Reportes	El sistema debe tener un módulo para el diseño, personalización y generación de reportes de acuerdo a las necesidades del negocio.	X	
34	Bitácoras de gestión	El sistema debe contar con rastros de auditoría que permitan identificar los cambios en los accesos de los usuarios, sus privilegios y demás funcionalidades, realizadas por los Administradores de la plataforma.	X	
35	Multi Idioma	El sistema debe soportar varios idiomas (inglés, español, etc.)	X	
36	Multi Empresa	El sistema debe soportar la configuración y parametrización de distintas empresas.	X	

3.2.2. Stakeholders. Esta sección presenta una lista de los stakeholders involucrados en el proyecto. Para cada uno de ellos, se deben listar los *concerns* que van a ser tenidos en cuenta en el documento de arquitectura. Esta información se presenta en forma de matriz, donde las filas representan los stakeholders y las columnas los concerns. Cada celda determina el grado de relevancia del concern para el stakeholder (Tabla 2). Finalmente, basados en los concerns relevantes a cada stakeholder se determina los puntos de vista que se le presentarán.

El standard ANSI/IEEE 1471-2000 propone que al menos los siguientes stakeholders sean considerados: usuarios, clientes, desarrolladores y administradores.

• Customer • Application software developers • Infrastructure software developers • End users • Application system engineers • Application hardware engineers	• Project manager • Communications engineers • Chief Engineer/Chief Scientist • Program management • System and software integration and test engineers • Safety engineers and certifiers	• External organizations • Operational system managers • Trainers • Maintainers • Auditors • Security engineers and certifiers

Tabla 4. Listado de los Stakeholders

Stakeholder	Descripción
Mesa de Ayuda	Equipo de personas encargado de recibir, atender y/o re direccionar todas las solicitudes de los usuarios y/o clientes, en un primer nivel de conocimiento técnico.
Equipo de Proyecto	Miembros del equipo del proyecto de Gestión de Identidades
Ingenieros de Riesgo y Seguridad informática	Grupo de ingenieros responsables por definir, estandarizar y ejecutar políticas relacionadas con la seguridad de la información.
Gestión Humana	Grupo de personas responsables por la selección, administración, bienestar, capacitación y entrenamiento de los empleados.
Gerencia General	Persona responsable de administrar los elementos de ingresos y costos de una compañía y de la definición de estrategias a corto, mediano y largo plazo.
CIO Chief Information Officer – Gerente de Tecnología	Chief information officer (CIO) o Gerente de Tecnología es la persona responsable por el gerenciamiento de las TICs (Tecnologías de información y Telecomunicaciones) y su alineamiento a las estrategias y objetivos empresariales.
Administradores del Sistema	Ingeniero responsable por la administración y configuración de la plataforma tecnológica
CISO Chief Information Security Officer – Jefe de Seguridad de la Información	Ingeniero responsables por la Gestión de la Seguridad de la Información de la compañía
Usuarios Finales	Empleados, contratistas y terceros
Gerente de Proyecto	Persona responsable por la administración y cumplimiento de los objetivos del proyecto
Asociados u Organizaciones Externas	Clientes externos que pueden ser inversionistas, interesados o entes externos
Auditores	Grupo de personas encargadas de revisar, examinar y evaluar los resultados de la gestión administrativa y financiera de una dependencia o entidad, con el propósito de informar, recomendar o dictaminar acerca de ellas.
Desarrolladores	Equipo de ingenieros responsables de analizar, diseñar e implementar aplicaciones informáticas.
Gerencia Financiera	Área responsable por la administración financiera de la compañía.

Tabla 5. Stakeholders y Expectativas

Stakeholder	Expectativas
Mesa de Ayuda	Disminuir los tiempos de soporte requeridos por la Mesa de Ayuda, Gestión de Clientes y Seguridad Informática para la atención de solicitudes de creación, actualización, perfilización o eliminación de usuarios, cambio de contraseñas y eventos relacionados con el servicio
Mesa de Ayuda	Disminuir en el número de requerimientos a la Mesa de Ayuda relacionados con tareas de administración de usuarios y/o perfiles.
Gerente General - CIO	Ahorros económicos a corto y mediano plazo gracias a la disminución en el número de solicitudes y soporte requerido con los procesos de administración de usuarios (menos personal necesario, mayor productividad)
Gerencia General, Auditores, Ingenieros de Seguridad de la Información	Disminuir los riesgo de pago de multas o sanciones económicas por incumplimiento de regulaciones o políticas internas relacionadas con procesos de administración de usuarios
Auditores, Ingenieros de Seguridad de la Información	Fortalecer las políticas de seguridad asociadas a los procesos de administración de usuarios y aplicaciones
Gestión Humana	Tener mejores tiempos de respuesta en la asignación, retiro o cambio de los accesos a las aplicaciones o servicios de los Colaboradores durante el tiempo en la organización.
Auditores, Ingenieros de Seguridad de la Información	Contar con un método estándar de autenticación, autorización y auditoria para el control de los permisos de acceso a los servicios o aplicaciones
CIO, Auditores, Ingenieros de Seguridad de la Información	Garantizar que con la solución se pueda dar el cumplimiento de requerimientos regulatorios relacionados con la administración de usuarios en los sistemas (Circular 052, PCI, etc.).
CIO	Aumentar la productividad de las personas encargadas de las tareas administrativas relacionadas con el servicio de provisión de usuarios, puesto que al automatizar este proceso podrán participan en otras tareas o proyectos
CIO, Ingenieros de Seguridad de la Información	Mejorar la seguridad de los servicios ofrecidos, ya que se espera contar con puntos centrales para la definición y administración de perfiles y roles de acceso a los servicios.

Stakeholder	Expectativas
Desarrolladores	Ofrecer mecanismos de integración rápida y flexible para la administración y autenticación de usuarios, en los nuevos desarrollos
CIO	Ofrezca esquemas de licenciamiento flexibles y de fácil implementación, especialmente por el crecimiento en el número de usuarios que demandarán el servicio.
Administradores del Sistema	Proceso de instalación y despliegue rápido y sencillo.
GH	Permitir que un evento tal como la salida de un empleado pueda disparar una alarma en tiempo real que permita modificar los derechos de acceso en todos los sistemas en cuestión de minutos
CISO	Contar con un sistema analizador de eventos de seguridad que permite la captura, almacenamiento y explotación de los registros de operaciones que ocurren a lo largo de la infraestructura, esto permite reaccionar ante amenazas y establecer procesos de remediación y notificación ante potenciales brechas en las políticas de seguridad implementadas.
CIO - CISO	En un mediano plazo ayudar al cumplimiento de la norma ISO 27001, gracias a la implementación de una solución que permita asegurar de manera clara y coherente el manejo del proceso de Gestión de seguridad e identidad.
Gerente General - CIO	En un futuro la solución debe permitir el crecimiento y expansión del aprovisionamiento de usuarios a todas las comunidades externas como proveedores, terceros, accionistas y asociados. Se estima que las comunidades externas puedan llegar a sumar un 3000% de los usuarios inicialmente contemplados.

3.2.3. Restricciones Arquitecturales

3.2.3.1. Motivadores de Negocio. Esta sección busca identificar los motivadores de negocio de la organización. Normalmente estos motivadores son encontrados, respondiendo a las preguntas:

- Cómo genera utilidad la organización
- De dónde provienen las utilidades de la organización?
- Cuáles son los elementos claves del negocio?

En resumen, un motivador de negocio es una descripción corta que define clara y específicamente los resultados deseados de negocio de una organización así como las actividades necesarias para lograrlos. Los motivadores de negocio deben ser: Específicos, Medibles, Agresivos pero viables, Orientados al resultado y limitados en el tiempo. El objetivo es hacer una lista priorizada de motivadores de negocio.

Ayuda para su uso:

- **El nombre del motivador**: Sigue en general la regla: <verbo> + <elemento a medir> + <área de énfasis>
  - Ejemplo: Incrementar ventas en las áreas metropolitanas

- **La descripción del motivador:** Sigue en general la regla: <Retorno esperado del negocio>+ Mediante+ <Actividad planeada de negocio>
  - Ejemplo: Incrementar ventas en 15 % mediante la apertura de nuevas oficinas

La medida: Define en una frase como valorar el impacto en el negocio del motivador. Se organiza por rangos y se determina para cada rango, la unidad de medida del impacto. Adicionalmente, se definen los valores mínimos y máximos para cada rango de impacto.

Tabla 6. Descripción del motivador de negocio

Nombre del Motivador de Negocio	**Descripción del Motivador de Negocio**	
Automatizar los Procesos de administración de usuarios	Automatizar los Procesos administrativos de provisionamiento de usuarios mediante la implementación de la plataforma a un 75% sobre los proceso manuales	
Medida del Impacto		
Cantidad de nuevos usuarios provisionados en las aplicaciones, respecto a cantidad de solicitudes recibidas por Mesa de Ayuda en formatos electrónicos durante un mes.		
Rangos	**Cota Mínima**	**Cota Máxima**
Ninguno	0	20
Bajo	20	40
Moderado	40	60
Fuerte	60	80
Muy Fuerte	80	Mayor
Asociación del Motivador	Definido Por:	CIO
	Ejecutado Por:	Proveedor

con el Negocio	Ubicación en el Portafolio del negocio	Mejorar la oportunidad del servicio

Nombre del Motivador de Negocio	Descripción del Motivador de Negocio	
Productividad de los colaboradores	Lograr que los nuevos colaboradores tengan acceso de manera oportuna a las aplicaciones y servicios previstos, al momento de ingresar en la organización mediante una solución de aprovisionamiento que pueda reducir estos tiempos en 85% de lo actual.	
Medida del Impacto		
Cantidad de nuevos colaboradores provisionados automáticamente en las aplicaciones de acuerdo a la fecha de ingreso del mismo, respecto a reportes de Mesa de ayuda con incidentes sobre esta falta de accesos		
Rangos	**Cota Mínima**	**Cota Máxima**
Ninguno	0	20
Bajo	20	40
Moderado	40	60
Fuerte	60	80
Muy Fuerte	80	Mayor
Asociación del Motivador con el Negocio	Definido Por:	Gestión Humana
	Ejecutado Por:	Proveedor
	Ubicación en el Portafolio del negocio	Contribuir al Incremento de la productividad

Nombre del Motivador de Negocio	Descripción del Motivador de Negocio	
Disminuir tiempos de atención y soporte	Disminuir en un 50% los tiempos de soporte requeridos por la Mesa de Ayuda, Gestión de Clientes y Seguridad Informática para la atención de solicitudes relacionadas con la administración de usuarios mediante la implementación de la plataforma tecnológica.	
Medida del Impacto		
Cantidad de casos registrados por Mesa de Ayuda relacionados a temas de administración de usuarios en un mes.		
Rangos	**Cota Mínima**	**Cota Máxima**
Ninguno	500	400
Bajo	400	300
Moderado	300	200
Fuerte	100	50
Muy Fuerte	50	Menor
Asociación del Motivador con el Negocio	Definido Por:	CIO
	Ejecutado Por:	Proveedor
	Ubicación en el Portafolio del negocio	Minimizar el número de casos que afecten el servicio

Nombre del Motivador de Negocio	Descripción del Motivador de Negocio		
Generar ahorros económicos	Generar ahorros económicos mediante la implementación de una Plataforma que permita evitar el crecimiento de personal al disminuir el número de solicitudes y soporte requerido con los procesos de administración de usuarios.		
Medida del Impacto			
Reporte mensual sobre cantidad de casos registrados por Mesa de Ayuda en temas de administración de usuarios, respecto a los meses y años pasados.			
Rangos	**Cota Mínima**		**Cota Máxima**
Ninguno	500		400
Bajo	400		300
Moderado	300		200
Fuerte	100		50
Muy Fuerte	50		Menor
Asociación del Motivador con el Negocio	Definido Por:	Gerencia General	
	Ejecutado Por:	Proveedor	
	Ubicación en el Portafolio del negocio	Generación de ahorros mediante la optimización de procesos	

Nombre del Motivador de Negocio	Descripción del Motivador de Negocio		
Cumplimiento Normativo y Regulatorio	Mejorar los procesos relacionados a la Gestión de la identidad y el Acceso mediante la implementación de la solución tecnológica, de manera que facilite el cumplimiento oportuno de auditorías, regulaciones y normatividad vigente.		
Medida del Impacto			
Numero de no conformidades reportadas en los procesos de auditoria/revisoría externa o interna relacionada el tema de seguridad de la identidad.			
Rangos	**Cota Mínima**		**Cota Máxima**
Ninguno	5		En adelante
Bajo	4		3
Moderado	3		2
Fuerte	2		1
Muy Fuerte	0		
Asociación del Motivador con el Negocio	Definido Por:	Gerencia General - CISO	
	Ejecutado Por:	Proveedor	
	Ubicación en el Portafolio del negocio	Cumplimiento regulatorio	

Nombre del Motivador de Negocio	Descripción del Motivador de Negocio		
Disminución del riesgo	Disminución del riesgo de pago de multas o sanciones económicas por incumplimiento de regulaciones o políticas internas relacionadas con procesos de administración de usuarios, mediante la implementación de la solución tecnológica		
Medida del Impacto			
Numero de no conformidades reportadas en los procesos de auditoria/revisoría externa o interna relacionada el tema de seguridad de la identidad.			
Rangos	**Cota Mínima**		**Cota Máxima**
Ninguno	5		En adelante
Bajo	4		3
Moderado	3		2
Fuerte	2		1
Muy Fuerte	0		
Asociación del Motivador con el Negocio	Definido Por:	Gerencia General, CISO, Auditores	
	Ejecutado Por:	Proveedor	
	Ubicación en el Portafolio del negocio	Disminución del riesgo	

Nombre del Motivador de Negocio	Descripción del Motivador de Negocio		
Visibilidad sobre los riesgos y eventos de seguridad	Visibilidad sobre el 100% de los eventos de seguridad de la información relacionados con la administración de usuarios, mediante la implementación de la solución tecnológica		
Medida del Impacto			
Cantidad de eventos detectados y reportados por los Ingenieros de seguridad informática, relacionados con “ataques”, fallas o posibles riesgos relacionados a la administración de usuarios en un mes.			
Rangos	**Cota Mínima**		**Cota Máxima**
Ninguno	0		0
Bajo	1		4
Moderado	4		8
Fuerte	8		12
Muy Fuerte	12		Mayor
Asociación del Motivador con el Negocio	Definido Por:	CISO, Auditores	
	Ejecutado Por:	Proveedor	
	Ubicación en el Portafolio del negocio	Disminución del riesgo	

3.2.4. Restricciones de Tecnología. Esta sección describe las restricciones de tecnología impuestas por la organización y/o el dominio del problema

Tabla 7. Restricciones de tecnología

ID Restricción 1	**Tipo:** Tecnología (x) Negocio ( )	**Nombre** **Integración Active Directory**
Descripción:	El sistema debe integrarse con repositorio Active Directory de la plataforma Microsoft	
Establecida por:	Gerencia de Tecnología	
Alternativas:	Ninguna	
Observaciones:	Este se ha definido como el repositorio por defecto para el holding empresarial	

ID Restricción 2	**Tipo:** Tecnología (x) Negocio ( )	**Nombre** **Integración LDAP**
Descripción:	El sistema debe integrarse con repositorios abiertos tipo LDAP	
Establecida por:	Gerencia de Tecnología	
Alternativas:	Algún otro repositorio abierto donde se pueda migrar la información actualmente almacenada en el LDAP	
Observaciones:	Actualmente es el repositorio establecido para todos los usuarios externos (asociados, comunidades, afiliados, etc.)	

ID Restricción 3	**Tipo:** Tecnología (x) Negocio ( )	**Nombre** **Integración Plataforma de Correo**
Descripción:	El sistema debe soportar integración Nativa con plataformas de Correo tipo Exchange Server de Microsoft y Linux tipo Qmail	
Establecida por:	Gerencia de Tecnología	
Alternativas:	Ninguna	
Observaciones:	Actualmente son las dos plataformas de correo utilizadas por el Grupo Empresarial.	

ID Restricción 4	**Tipo:** Tecnología (x) Negocio ( )	**Nombre** **Integración Sistema de Recurso Humanos**
Descripción:	La plataforma debe permitir integrarse con el sistema de Recursos Humanos y el repositorio de usuarios definido para contratistas y/o terceros.	
Establecida por:	Gerencia de Gestión Humana	
Alternativas:	Ninguna	
Observaciones:	Desde el sistema principal de Gestión Humana, se deben disparar todos los eventos relacionados con los empleados, temporales y contratistas.	

3.2.5. Restricciones de Negocio. Esta sección describe las restricciones de negocio impuestas por la organización y/o el dominio del problema

ID Restricción 1	**Tipo:** Tecnología ( ) Negocio (x)	**Nombre** Modalidad Servicio o Compra directa
Descripción:	El proponente debe presentar la propuesta de solución considerando una alternativa en modalidad de servicio (infraestructura, servidor, hardware y software como SaaS) o en modalidad de compra directa donde se adquirirá cada componente de la plataforma.	
Establecida por:	Gerencia Financiera	
Alternativas:	Ninguna, se debe ofertar bajo estos dos modelos	
Observaciones:		

ID Restricción 2	**Tipo:** Tecnología ( ) Negocio (x)	**Nombre** Costos y valores estimados de la solución
Descripción:	Para el proyecto el Grupo Empresarial cuenta con un presupuesto aprobado de US$1'000.000 los cuales deben ser ejecutados a tres años, para una fase inicial donde se contemplan 10.000 empleados directos e indirectos.	
Establecida por:	Gerencia General	
Alternativas:	Ninguna	
Observaciones:	Desde el sistema principal de Gestión Humana, se deben disparar todos los eventos relacionados con los empleados, temporales y contratistas.	

ID Restricción 3	**Tipo:** Tecnología ( ) Negocio (x)	**Nombre** Etapas de implementación
Descripción:	La solución y presupuesto aprobado serán ejecutado por fases, es decir, la fase inicial solo contemplara aplicaciones o servicios compartidos por todo el Grupo Empresarial (ejemplo: Correo Electrónico, Directorio Activo, etc.) y algunas otras del Core propio de cada negocio. En adelante, el esquema y etapas subsiguientes serán considerados como fases adicionales (sub proyectos) donde cada empresa del grupo analizara y presupuestara el plan de expansión para el cubrimiento de sus aplicaciones o servicios que cada una defina.	
Establecida por:	Gerente de Proyecto	
Alternativas:	Ninguna	
Observaciones:	Desde el sistema principal de Gestión Humana, se deben disparar todos los eventos relacionados con los empleados, temporales y contratistas.	

3.2.6. Atributos de Calidad

Tabla 8. Árbol de utilidad

Atributo de Calidad:		Eficiencia
Tiempo	ID	Descripción
Tiempos de sincronización	E1	El sistema debe garantizar la sincronización y actualización de los múltiples repositorios en un tiempo no mayor a 5 minutos, bajo una operación normal del servicio los 365 días del año.
Atributo de Calidad:		Fiabilidad
Recuperabilidad	ID	Descripción
Esquemas de alta disponibilidad	F1	El sistema estará en capacidad de responder las peticiones de acceso de los usuarios y distintas aplicaciones en un 95% ante una falla o incidente sobre la plataforma principal y en un periodo no superior a 10 minutos.
Atributo de Calidad:		Mantenimiento
Flexibilidad	ID	Descripción
Plataforma abierta y adaptable	M1	La plataforma debe asegurar su implementación en distintos sistemas operativos, arquitecturas de servidores y motores de bases de datos
Integración con variadas plataformas	M2	El sistema debe garantizar la integración y adaptabilidad a nuevas aplicaciones, appliance y en general nuevos servicios desplegados por el negocio.
Escalabilidad		
Crecimiento de usuarios	M3	El sistema debe garantizar el crecimiento estimado de un 10% en usuarios por año (10.000 Iniciales:: 1000 adicionales por año)
Crecimiento de servicios o aplicaciones	M4	El sistema debe garantizar el crecimiento estimado de 10 aplicaciones por año las cuales ingresaran a la plataforma centralizada de IAM.
Disponibilidad de conectores nativos	M5	El sistema debe garantizar el desarrollo de conectores **nativos**, los cuales permitan la inclusión y despliegue de nuevos servicios de manera oportuna y fácilmente implementable
Atributo de Calidad:		Seguridad
Integridad	ID	Descripción
Integralidad de las identidades	S1	El sistema debe asegurar la integralidad de cada uno de los repositorios interconectados, de manera que el 100% de los usuarios parametrizados cuenten con los accesos y atributos adecuados.
Confidencialidad		
Perfiles de acceso	S2	El sistema garantizara el acceso adecuado del 100% de los usuarios autorizados, con los servicios y opciones que se hayan definido en los perfiles de acceso.
Llaves y tokens	S3	El sistema permitirá la configuración de usuarios VIP que

de acceso		requieran autenticación con token, huella digital, iris, entre otros.
Granularidad de Accesos	S4	El sistema debe estar diseñado por módulos y componentes separados, lo cual permitan la configuración de accesos a los usuarios finales de manera granular
Auditoria		
Reportes y cumplimiento	S5	El sistema debe tener la capacidad de diseñar y generar reportes, según la normatividad vigente o propia de cada negocio. Luego se espera que cuente con reportes predefinidos para SOX, Circular 052, PCI, entre otros.
Registro Logs y transacciones	S6	El sistema debe permitir configurar bitácoras de seguimiento a cualquier nivel de usuario, en particular para los administradores de la plataforma de forma que permita evidenciar quien, cuando, como y donde realizo un cambio.

Tabla 9. Escenarios de Calidad

Escenario de Calidad #	**E1**	**Stakeholder:**	**Administrador del sistema**
Atributo de Calidad	Eficiencia		
Justificación	El sistema debe garantizar la sincronización y actualización de los distintos repositorios a su directorio central, con el fin de garantizar una correcta operación de todos sus componentes en un tiempo adecuado		
Fuente	Sistema		
Estímulo	Proceso de actualización y/o conciliación		
Artefacto	Módulo de administración de identidades y administración del acceso		
Ambiente	Operación Normal		
Respuesta	El sistema informa al administrador de la plataforma, que el proceso de sincronización se ejecutó con éxito o con errores, generando además un log sobre el reporte de la actividad.		
Medida de la Respuesta	La sincronización de aproximadamente 10.000 cuentas, debe ejecutarse en un tiempo no superior a los 5 minutos.		

Escenario de Calidad #	F1	Stakeholder:	CISO
Atributo de Calidad	Fiabilidad		
Justificación	El servicio debe contar con un esquema de alta disponibilidad, que ante un incidente, problema o riesgo materializado pueda asegurar la continuidad tecnológica de la operación de la plataforma		
Fuente	Incidente o problema que afecte la plataforma		
Estímulo	Activar el sistema de alta disponibilidad y/o contingencia		
Artefacto	Sistema		
Ambiente	Operación Normal		
Respuesta	El sistema *levanta* o inicia de manera automática la contingencia de la plataforma		
Medida de la Respuesta	El tiempo en el cual el sistema restablece operación a un porcentaje mínimo del 95% de su operación normal, no es superior a 10 minutos		

Escenario de Calidad #	M1	Stakeholder:	CIO
Atributo de Calidad	Mantenimiento		
Justificación	El sistema debe ser altamente adaptable en su arquitectura y componentes, puesto que las distintas empresas del grupo continuamente innovan cambiando o adquiriendo variedad de plataformas o arquitecturas de última tecnología		
Fuente	Nuevos servicios de las Empresas del grupo		
Estímulo	Desarrollo y adaptabilidad de nuevos componentes		
Artefacto	Sistema		
Ambiente	Operación Normal		
Respuesta	La solución permite la integración de la nueva arquitectura tecnológica, sin afectar los componentes ya existentes		
Medida de la Respuesta	Implementación adecuada del nuevo componente o adaptador desarrollado		

Escenario de Calidad #	M2	Stakeholder:	CIO
Atributo de Calidad	Mantenimiento		
Justificación	El sistema debe ser altamente adaptable en su arquitectura y componentes, puesto que las distintas empresas del grupo adquieren o desarrollan nuevas aplicaciones, appliance y en general nuevos servicios.		
Fuente	Nuevos servicios de las Empresas del grupo		
Estímulo	Desarrollo y adaptabilidad de nuevos componentes		
Artefacto	Sistema		
Ambiente	Operación Normal		
Respuesta	La solución permite la integración del nueva servicio, sin afectar los componentes ya existentes		
Medida de la Respuesta	Implementación adecuada del nuevo servicio o conector desarrollado		

Escenario de Calidad #	M3	Stakeholder:	CIO
Atributo de Calidad	Mantenimiento		
Justificación	El sistema y su infraestructura, debe estar diseñado de manera que sea capaz de soportar un crecimiento estimado por año de 1000 usuarios (10%) para todo el Grupo Empresarial		
Fuente	Nuevos usuarios		
Estímulo	Incremento en el número de Identidades Digitales		
Artefacto	Módulo de administración de identidades y administración del acceso		
Ambiente	Operación Normal		
Respuesta	La solución permite el ingreso y registro de nuevos usuarios, sin afectar el desempeño de la aplicación		
Medida de la Respuesta	El nuevo usuario se registra y sincroniza en los múltiples repositorios en un tiempo no mayor 2 Minutos		

Escenario de Calidad #	M4	Stakeholder:	CIO
Atributo de Calidad	Mantenimiento		
Justificación	El sistema y su infraestructura, debe estar diseñado de manera que soporte un crecimiento estimado de 10 aplicaciones o nuevos servicios por año para todo el Grupo Empresarial		
Fuente	Nuevas aplicaciones o servicios a desplegar		
Estímulo	Incremento en el número de aplicaciones soportadas por la plataforma		
Artefacto	Módulo de administración de identidades y administración del acceso		
Ambiente	Operación Normal		
Respuesta	La solución permite la adición, integración y sincronización de los nuevos repositorios de acceso de las aplicaciones desplegadas sin afectar el desempeño de la solución.		
Medida de la Respuesta	Cantidad de nuevas aplicaciones desplegada efectivamente sobre la plataforma		

Escenario de Calidad #	M5	Stakeholder:	Administrador del Sistema
Atributo de Calidad	Mantenimiento		
Justificación	El sistema debe ser altamente adaptable en su arquitectura y componentes, puesto que las distintas empresas del grupo adquieren continuamente una variedad de plataformas o arquitecturas de última tecnología		
Fuente	Nuevos servicios de las Empresas del grupo		
Estímulo	Desarrollo y adaptabilidad **NATIVA** de nuevos componentes		
Artefacto	Sistema		
Ambiente	Operación Normal		
Respuesta	La solución permite la adaptabilidad **NATIVA** de los nuevos servicios, sin afectar los componentes ya existentes		
Medida de la Respuesta	Implementación adecuada del nuevo servicio en un tiempo no superior a dos días		

Escenario de Calidad #	S1	Stakeholder:	CIO - CISO
Atributo de Calidad	Seguridad		
Justificación	El sistema al contar con una cantidad importante de aplicaciones y por ende repositorios de autenticación (11 en una etapa inicial) es vital para el Negocio, asegurar que todos las Identidades Digitales se encuentren totalmente sincronizadas en cada uno de estos repositorios		
Fuente	Sistema		
Estímulo	Proceso de autenticación y/o conciliación		
Artefacto	Módulo de administración de identidades y administración del acceso		
Ambiente	Operación Normal		
Respuesta	El sistema informa al administrador de la plataforma, que el proceso de sincronización se ejecutó con éxito o con errores indicando cuales identidades no fueron exitosamente sincronizadas y el detalle del fallo en el proceso		
Medida de la Respuesta	Sincronización e integralidad de la información en un 100% de todas las identidades digitales.		

Escenario de Calidad #	S2	Stakeholder:	CIO - CISO
Atributo de Calidad	Seguridad		
Justificación	El sistema debe garantizar el acceso adecuado de cada una de las identidades, según los perfiles, roles y accesos especificados para cada uno los usuarios y en cada una de las aplicaciones o servicios que se encuentre matriculados.		
Fuente	Usuario autenticándose		
Estímulo	Proceso de autenticación y/o conciliación		
Artefacto	Módulo de administración de identidades y administración del acceso		
Ambiente	Operación Normal		
Respuesta	El sistema permite el ingreso correcto del usuario, según los accesos y perfiles parametrizados		
Medida de la Respuesta	El 100% de los usuarios y sus respectivas identidades se encuentran correctamente autenticadas		

Escenario de Calidad #	S3	Stakeholder:	CIO - CISO
Atributo de Calidad	Seguridad		
Justificación	Teniendo en cuenta que el Grupo Empresarial cuenta con usuarios definidos como VIP (Gerentes, Directores, Oficiales de Cumplimiento, etc.) se hace necesario contar con mecanismos adicionales de autenticación(tokens) sobre los servicios accedidos		
Fuente	Usuario VIP autenticándose		
Estímulo	Proceso de autenticación		
Artefacto	Módulo de administración de identidades y administración del acceso		
Ambiente	Operación Normal		
Respuesta	El sistema permite el ingreso correcto del usuario VIP, autenticando con los tokens o llaves adicionales establecidas para el usuario.		
Medida de la Respuesta	El 100% de los usuarios y sus respectivas identidades se encuentran correctamente autenticadas		

Escenario de Calidad #	S4	Stakeholder:	CIO - CISO
Atributo de Calidad	Seguridad		
Justificación	Teniendo en cuenta que el Grupo Empresarial por exigencia, normatividad o decisiones de cada negocio, requieren perfilizar opciones y/o funciones propias de la plataforma IAM, se hace necesario poder dar granularidad de los accesos hasta en un mínimo detalle de la plataforma		
Fuente	Parametrización de la plataforma		
Estímulo	Configuración de usuarios, grupos y opciones propios del sistema IAM		
Artefacto	Módulo de administración del acceso		
Ambiente	Operación Normal		
Respuesta	El sistema permite configurar un usuario final o grupo de usuarios, con la granularidad esperada		
Medida de la Respuesta	El 100% de los usuarios finales, cuenta con los accesos definidos para el perfil		

Escenario de Calidad #	S5	Stakeholder:	Gerencia General – CIO – CISO- Auditor
Atributo de Calidad	Seguridad		
Justificación	Cada una de las empresas que conforman el Holding Empresarial pueden o deben cumplir ciertos requerimientos de ley y/o normatividad vigente , luego se hace necesario contar con reportes prediseñados para SOX, Circular 052, PCI, entre otros; además contar con herramientas de diseño para usuario final que permitan la actualización y configuración de nuevos reportes		
Fuente	Normatividad, regulación y requerimientos de ley		
Estímulo	Generación y configuración de reportes		
Artefacto	Módulo administración de eventos y seguridad de información		
Ambiente	Operación Normal		
Respuesta	El sistema permite la configurar nuevos reportes y generar los definidos bajo la normatividad aplicada		
Medida de la Respuesta	- Implementación adecuada del nuevo reporte en un tiempo no superior a dos días - 100% de los Reportes prediseñados ejecutados según la normatividad vigente		

Escenario de Calidad #	S6	Stakeholder:	CIO – CISO - Auditor
Atributo de Calidad	Seguridad		
Justificación	Por normatividad y cumplimiento, es necesario que las empresas puedan consultar los LOGS generados en las transacciones realizadas por los administradores de la plataforma, para poder identificar y hacer trazabilidad sobre los cambios que realicen. Esta información debe consultarse en línea y a través de un sitio web		
Fuente	Usuario Autorizado Solicita Bitácora		
Estímulo	Generación de reportes		
Artefacto	Módulo administración de eventos y seguridad de información		
Ambiente	Operación Normal		
Respuesta	El sistema genera reporte según los criterios y filtros establecidos		
Medida de la Respuesta	100% de los reportes generados con éxito		

3.3. MODELO PROPUESTO PARA LA EVALUACIÓN DEL SISTEMA

Partiendo del resultado del ejercicio anterior, en cual se considera como insumo principal el resultado de la construcción del documento que describe la arquitectura del sistema, SAD. También se tendrá en cuenta para la construcción del modelo una serie de variables que se identificaron dentro del ejercicio, las cuales se pueden definir como requerimientos propios del proyecto y del negocio, que para el caso de estudio se tendrá en cuenta temas como: Fases de ejecución del proyecto, tiempos de entrega, presupuesto, tipo de oferta (servicios, compra directa), esquemas de implementación y soporte, además de algunas otras restricciones propias del negocio.

La estrategia de construcción del modelo de evaluación del software de seguridad, permite caracterizar las distintas plataformas evaluadas, mediante la agrupación de siete categorías las cuales se clasifican en: Generales RFP, Empresa, Funcionales, Técnicos, Descripción del Software, Implementación del proyecto y Restricciones del Negocio, lo que finalmente permite evaluar la propuesta mediante la valoración un total de ciento siete preguntas definidas y caracterizadas dentro del modelo, las cuáles de manera resumida se esquematizan en la tabla 10.

Tabla 10. Caracterización del Modelo de Evaluación, Arquitectura definida para el sistema de Gestión de la Identidad

MODELO DE EVALUACIÓN DE SOLUCIÓN TECNOLÓGICA PARA LA GESTIÓN DE LA IDENTIDAD		Numero de Preguntas	Tipo de Pregunta
GENERALES RFP	GENERALES	5	Texto
	ECONÓMICA	1	Texto
EMPRESA	Generales	3	Texto
	Modelo de Operación	3	Texto
	Económico	5	Texto
FUNCIONALES	Administración de Acceso	3	Selección Múltiple
	Administración de Identidades	5	Selección Múltiple
	Administración de Eventos y Seguridad de Información	4	Selección Múltiple
	Generales	4	Selección Múltiple
TÉCNICOS	Generales	9	Selección Múltiple
	Restricciones de Tecnología	4	Selección Múltiple
	QAs	13	Selección Múltiple
	Telecomunicaciones e Infraestructura	24	Texto / Selección Múltiple
	Administración de Usuarios	3	Selección Múltiple
	Seguridad	3	Texto
	Licenciamiento	3	Texto
	Soporte y Garantía	3	Texto
	Administración del aplicativo	2	Texto
	Normatividad	2	Texto
DESCRIPCIÓN DEL SOFTWARE		3	Texto
IMPLEMENTACIÓN PROYECTO		1	Texto
Restricciones del Negocio		4	Selección Múltiple
	Total	107	

3.3.1 Criterios de calificación. Ahora bien, a partir de la identificación y definición de estos requerimientos que parten de la definición del documento de arquitectura y de las variables propias del Negocio y del proyecto, se platea un esquema de calificación sencillo y de fácil manejo el cual permita realizar una valoración y calificación, partiendo de la definición de cuatro variables cualitativas, las cuales tienen su homologación a un valor cuantificable que permita realizar una calificación de cada una de las preguntas y que finalmente determine por cada uno de los agrupadores definidos, la sumatoria de la calificación dada por el panel de expertos, a la respuesta dada por los proveedores de la solución. La escala de calificación se encuentra representada en la siguiente tabla:

Tabla 11. Esquema de Calificación del Modelo de Evaluación

CALIFICACIÓN Cualitativa	Puntaje
Cumple Totalmente	5
Cumple Parcialmente	3
No Cumple, pero si pueden hacerlo en el tiempo requerido	2
No Cumple, no pueden hacerlo en el tiempo requerido	1

3.3.2. Diseño y construcción de Matriz de evaluación. Para el diseño de la matriz de evaluación del software de Seguridad Informática, se seleccionó la herramienta Excel de Microsoft, ya que permitirían de una manera rápida y ordenada, diseñar y esquematizar todas aquellas variables importantes y relevantes del proceso de evaluación de la solución. La matriz permite que los proponentes o proveedores del software sean calificados bajo la misma, la cual además podría en un momento dado ser exigible o hacer parte integral de los términos de referencia que se hayan desarrollado, tipo RFP.

El archivo desarrollado está compuesto de las siguientes hojas que permiten al panel de expertos ir a los detalles requeridos para responder a cada una de las preguntas planteadas:

- Hoja denominada *Resumen*, donde se esquematizan el total de preguntas tal como se observó en la Tabla 10. Caracterización del Modelo de Evaluación, Arquitectura definida para el sistema de Gestión de la Identidad

- Hoja denominada *RAS*, donde se esquematizan y clasifican los atributos y requerimientos del sistema los cuales fueron identificados en el documento de arquitectura, SAD. Cada uno de los requerimientos se clasifico dentro del modelo teniendo en cuenta los siguientes tipos de características:

✓ Funcionales: Requerimiento considerado de carácter funcional.
✓ Modulo Funcional: Modulo al cual se relaciona el requerimiento funcional.
✓ Arquitectónicamente Significantes: Requerimientos (no funcionales) que son considerados técnicamente vitales en la caracterización del sistema.
✓ Atributo de Calidad: Requerimientos arquitectónicamente significativos, que consideran un escenario de calidad para su satisfacción.
✓ Mapeo QAs (Escenario de Calidad): Relación de requerimiento con los escenarios de calidad descritos en la hoja *Escenarios de QAs*.

Estos requerimientos y su clasificación se representan en la siguiente tabla:

Tabla 12. Identificación y Clasificación de Requerimientos RAS

Id	Descripción	Funcionales	Modulo Funcional	Arq. Significantes	Atributo de Calidad	Mapeo QAs
1	El sistema debe soportar conectores a aplicaciones desarrolladas In house en JAVA, Proccesss Server, PHP, . NET, Cobol			X		
2	El sistema debe soportar integración Nativa con motores de Bases de Datos tipo Oracle, Sybase, DB2, SQL Server			X		
3	El sistema debe integrar los distintos usuarios y generar un único ID (único usuario y clave de acceso) para los distintos accesos a las aplicaciones y/o servicios	X	Administración de Acceso			
4	El Sistema debe sincronizar y actualizar la información con los distintos repositorios en cada momento y hora del día sin restricción de horario (7 x 24 x 365 días)			X	Eficiencia	E1 - S1
5	El sistema debe permitir mediante una interfaz web el ingreso y administración de cada uno de los componentes que conformen la solución (administración, configuración, parametrización de nuevos servicios).	X	Administración de Identidades			
6	El sistema debe permitir mediante una interfaz web el ingreso de los usuarios finales, para poder auto gestionar algunos	X	Administración de Identidades			

Id	Descripción	Funcionales	Modulo Funcional	Arq. Significantes	Atributo de Calidad	Mapeo QAs
	servicios propios de su identidad (Mecanismos de autoservicio) como el cambio y recordación de clave, actualización de datos generales, etc.).					
7	El sistema debe permitir que el portal de autogestión pueda ser accedido desde dispositivos móviles (Celulares, eBooks, Palms, etc.)			X		
8	La plataforma debe ser abierta en el sentido que pueda correr en diferentes Sistemas Operativos y/o arquitectura de servidores donde se vaya a desplegar			X	Mantenimiento	M1
9	El sistema debe garantizar esquemas de alta disponibilidad (continuidad tecnológica en caso de un incidente y/o problema			X	Fiabilidad	F1
10	El sistema debe ser fácilmente adaptable a nuevas plataformas, aplicaciones y/o servicios que sean implementados o desplegados			X	Mantenimiento	M2
11	El sistema debe permitir la sincronización y actualización de los múltiples repositorios en un tiempo no mayor a 5 minutos			X	Eficiencia	E1
12	El sistema debe soportar un promedio de 10000 usuarios diarios, con una proyección estimada de un 10% por cada año			X	Mantenimiento	M3

Id	Descripción	Funcionales	Modulo Funcional	Arq. Significantes	Atributo de Calidad	Mapeo QAs
13	El sistema debe permitir configurar la información transaccional on-line y definir cual se almacena mediante un proceso de backup			X		
14	El sistema debe garantizar que los accesos a las distintas aplicaciones y/o servicios, sean otorgados según los lineamientos de seguridad y perfilización establecidos en las matrices de perfiles.			X	Seguridad	S2
15	El sistema debe permitir definir estándares para el nombramiento de usuarios y contraseñas que serán sincronizadas con los diferentes aplicativos o servicios	X	Administración de Acceso			
16	El sistema debe contar con mecanismos de autenticación de doble y triple factor (token, huella digital, iris, etc.) para controlar el acceso a servicios críticos definidos por la organización			X	Seguridad	S3
17	El sistema debe permitir generar informes programados y en tiempo real para conocer el comportamiento de los usuarios sobre las aplicaciones y servicios habilitados	X	Administración de Eventos y Seguridad de Información			
18	El sistema debe permitir configurar alertas sobre eventos *extraños* definidos por los administradores de	X	Administración de Eventos y Seguridad de Información			

Id	Descripción	Funcionales	Modulo Funcional	Arq. Significantes	Atributo de Calidad	Mapeo QAs
	seguridad					
19	El sistema debe permitir conectarse con Sistemas ERP y CRM, definidos por la organización			X	Mantenimiento	M5
20	El sistema debe permitir el diseño e implementación de flujos de trabajo (workflows) a través de la herramienta de administración web	X	Administración de Identidades			
21	La solución debe contar con herramientas de diseño y simulación de modelos de aprovisionamiento antes de la implementación	X	Administración de Identidades			
22	La solución debe contar con módulos independientes de administración como: - Administración de identidad - Administración del Acceso - Administración de Eventos y seguridad de la Información - Gobernabilidad	X	Generales			
23	La solución debe basar su arquitectura a través del manejo de eventos disparados por las distintas aplicaciones, repositorios o plataformas.			X		
24	o por conciliación de repositorios			X		
25	El sistema debe permitir definir y administrar reglas de negocio, roles y perfiles	X	Administración de Identidades			

Id	Descripción	Funcionales	Modulo Funcional	Arq. Significantes	Atributo de Calidad	Mapeo QAs
	organizacionales.					
26	La solución debe contar con "Meta Directorios" para el manejo e integración de repositorios			X		
27	La solución debe ser 100% Web-Enabled en todos sus componentes de administración	X	Generales			
28	El sistema debe permitir la configuración de roles, perfiles y usuarios de administración de manera granular por las distintas opciones de la solución			X	Seguridad	S4
29	El sistema debe "*recepcionar*" de manera automática, todos los eventos o novedades presentadas en el sistema de administración de gestión humana (ingreso de personal, promociones, vacaciones, retiros, etc.)			X		
30	La solución debe garantizar el desarrollo o disponibilidad de conectores **nativos** adicionales, los cuales permitan la integración a nuevas plataformas, aplicaciones, sistemas operativos, sistemas de correo electrónico, mainframes, lenguajes de programación o de scripting, PBX, bases de datos y otros.			X	Mantenimiento	M5
31	La plataforma debe contar con un módulo para la configuración			X		

Id	Descripción	Funcionales	Modulo Funcional	Arq. Significantes	Atributo de Calidad	Mapeo QAs
	de aplicaciones que requieran tener acceso Web Single Sign-On (Web-SSO)					
32	El sistema debe contar con mecanismos de identidad federada para conexiones futuras a sistemas de otras empresas del grupo o aquellas donde se tenga algún tipo de participación o convenio	X	Administración de Acceso			
33	El sistema debe tener un módulo para el diseño, personalización y generación de reportes de acuerdo a las necesidades del negocio.	X	Administración de Eventos y Seguridad de Información			
34	El sistema debe contar con rastros de auditoría que permitan identificar los cambios en los accesos de los usuarios, sus privilegios y demás funcionalidades, realizadas por los Administradores de la plataforma.	X	Administración de Eventos y Seguridad de Información			
35	El sistema debe soportar varios idiomas (inglés, español, etc.)	X	Generales			
36	El sistema debe soportar la configuración y parametrización de distintas empresas.	X	Generales			

- Hoja denominada *Escenarios de QAs*, donde se estructuraron todos aquellos escenarios y atributos de calidad identificados en el capítulo del documento de arquitectura, SAD. Estos escenarios se esquematizan de una manera objetiva y resumida, para que los proveedores y panel de expertos, puedan tener claridad sobre el tipo de calidad esperada y con la cual será valorada la solución tecnológica. Los mismos se pueden observar en la tabla a continuación mostrada:

Tabla 13. Escenarios de Calidad - QAs

Stake holder	Atributo de Calidad	Justificación	Fuente	Estímulo	Artefacto	Ambiente	Respuesta	Medida de la Respuesta
Administrador del sistema	Eficiencia	El sistema debe garantizar la sincronización y actualización de los distintos repositorios a su directorio central, con el fin de garantizar una correcta operación de todos sus componentes en un tiempo adecuado	Sistema	Proceso de actualización y/o conciliación	Módulo de administración de identidades y administración del acceso	Operación Normal	El sistema informa al administrador de la plataforma, que el proceso de sincronización se ejecutó con éxito o con errores, generando además un log sobre el reporte de la actividad.	La sincronización de aproximadamente 10.000 cuentas, debe ejecutarse en un tiempo no superior a los 5 minutos.
CISO	Fiabilidad	El servicio debe contar con un esquema de alta disponibilidad, que ante un incidente, problema o riesgo materializado pueda asegurar la continuidad tecnológica de la operación de la plataforma	Incidente o problema que afecte la plataforma	Activar el sistema de alta disponibilidad y/o contingencia	Sistema	Operación Normal	El sistema levanta o inicia de manera automática la contingencia de la plataforma	El tiempo en el cual el sistema restablece operación a un porcentaje mínimo del 95% de su operación normal, no es superior a 10 minutos
CIO	Mantenimiento	El sistema debe ser altamente adaptable en su arquitectura y componentes, puesto que las distintas empresas del grupo continuamente innovan cambiando o adquiriendo variedad de plataformas o arquitecturas de última tecnología	Nuevos servicios de las Empresas del grupo	Desarrollo y adaptabilidad de nuevos componentes	Sistema	Operación Normal	La solución permite la integración de la nueva arquitectura tecnológica, sin afectar los componentes ya existentes	Implementación adecuada del nuevo componente o adaptador desarrollado
CIO	Mantenimiento	El sistema debe ser altamente adaptable en su arquitectura y componentes, puesto que las distintas empresas del grupo adquieren o desarrollan nuevas aplicaciones,	Nuevos servicios de las Empresas del grupo	Desarrollo y adaptabilidad de nuevos componentes	Sistema	Operación Normal	La solución permite la integración del nueva servicio, sin afectar los componentes ya existentes	Implementación adecuada del nuevo servicio o conector desarrollado

Stake holder	Atributo de Calidad	Justificación	Fuente	Estímulo	Artefacto	Ambiente	Respuesta	Medida de la Respuesta
		appliance y en general nuevos servicios.						
CIO	Mantenimiento	El sistema y su infraestructura, debe estar diseñado de manera que sea capaz de soportar un crecimiento estimado por año de 1000 usuarios (10%) para todo el Grupo Empresarial	Nuevos usuarios	Incremento en el número de Identidades Digitales	Módulo de administración de identidades y administración del acceso	Operación Normal	La solución permite el ingreso y registro de nuevos usuarios, sin afectar el desempeño de la aplicación	El nuevo usuario se registra y sincroniza en los múltiples repositorios en un tiempo no mayor 2 Minutos
CIO	Mantenimiento	El sistema y su infraestructura, debe estar diseñado de manera que soporte un crecimiento estimado de 10 aplicaciones o nuevos servicios por año para todo el Grupo Empresarial	Nuevas aplicaciones o servicios a desplegar	Incremento en el número de aplicaciones soportadas por la plataforma	Módulo de administración de identidades y administración del acceso	Operación Normal	La solución permite la adición, integración y sincronización de los nuevos repositorios de acceso de las aplicaciones desplegadas sin afectar el desempeño de la solución.	Cantidad de nuevas aplicaciones desplegada efectivamente sobre la plataforma
Administrador del Sistema	Mantenimiento	El sistema debe ser altamente adaptable en su arquitectura y componentes, puesto que las distintas empresas del grupo adquieren continuamente una variedad de plataformas o arquitecturas de última tecnología	Nuevos servicios de las Empresas del grupo	Desarrollo y adaptabilidad **NATIVA** de nuevos componentes	Sistema	Operación Normal	La solución permite la adaptabilidad **NATIVA** de los nuevos servicios, sin afectar los componentes ya existentes	Implementación adecuada del nuevo servicio en un tiempo no superior a dos días

Stake holder	Atributo de Calidad	Justificación	Fuente	Estímulo	Artefacto	Ambiente	Respuesta	Medida de la Respuesta
CIO - CISO	Seguridad	El sistema al contar con una cantidad importante de aplicaciones y por ende repositorios de autenticación (11 en una etapa inicial) es vital para el Negocio, asegurar que todos las Identidades Digitales se encuentren totalmente sincronizadas en cada uno de estos repositorios	Sistema	Proceso de actualización y/o conciliación	Módulo de administración de identidades y administración del acceso	Operación Normal	El sistema informa al administrador de la plataforma, que el proceso de sincronización se ejecutó con éxito o con errores indicando cuales identidades no fueron exitosamente sincronizadas y el detalle del fallo en el proceso	Sincronización e integralidad de la información en un 100% de todas las identidades digitales.
CIO - CISO	Seguridad	El sistema debe garantizar el acceso adecuado de cada una de las identidades, según los perfiles, roles y accesos especificados para cada uno los usuarios y en cada una de las aplicaciones o servicios que se encuentre matriculados.	Usuario autenticándose	Proceso de autenticación y/o conciliación	Módulo de administración de identidades y administración del acceso	Operación Normal	El sistema permite el ingreso correcto del usuario, según los accesos y perfiles parametrizados	El 100% de los usuarios y sus respectivas identidades se encuentran correctamente autenticadas
CIO - CISO	Seguridad	Teniendo en cuenta que el Grupo Empresarial cuenta con usuarios definidos como VIP (Gerentes, Directores, Oficiales de Cumplimiento, etc.) se hace necesario contar con mecanismos adicionales de autenticación(tokens) sobre los servicios accedidos	Usuario VIP autenticándose	Proceso de autenticación	Módulo de administración de identidades y administración del acceso	Operación Normal	El sistema permite el ingreso correcto del usuario VIP, autenticando con los tokens o llaves adicionales establecidas para el usuario.	El 100% de los usuarios y sus respectivas identidades se encuentran correctamente autenticadas

Stake holder	Atributo de Calidad	Justificación	Fuente	Estímulo	Artefacto	Ambiente	Respuesta	Medida de la Respuesta
CIO - CISO	Seguridad	Teniendo en cuenta que el Grupo Empresarial por exigencia, normatividad o decisiones de cada negocio, requieren perfilizar opciones y/o funciones propias de la plataforma IAM, se hace necesario poder dar granularidad de los accesos hasta en un mínimo detalle de la plataforma	Parametrización de la plataforma	Configuración de usuarios, grupos y opciones propios del sistema IAM	Módulo de administración del acceso	Operación Normal	El sistema permite configurar un usuario final o grupo de usuarios, con la granularidad esperada	El 100% de los usuarios finales, cuenta con los accesos definidos para el perfil
Gerencia General, CIO, CISO, Auditor	Seguridad	Cada una de las empresas que conforman el Holding Empresarial pueden o deben cumplir ciertos requerimientos de ley y/o normatividad vigente , luego se hace necesario contar con reportes prediseñados para SOX, Circular 052, PCI, entre otros; además contar con herramientas de diseño para usuario final que permitan la actualización y configuración de nuevos reportes	Normatividad, regulación y requerimientos de ley	Generación y configuración de reportes	Módulo administración de eventos y seguridad de información	Operación Normal	El sistema permite la configurar nuevos reportes y generar los definidos bajo la normatividad aplicada	- Implementación adecuada del nuevo reporte en un tiempo no superior a dos días - 100% de los Reportes prediseñados ejecutados según la normatividad vigente
CIO - CISO	Seguridad	Por normatividad y cumplimiento, es necesario que las empresas puedan consultar los LOGS generados en las transacciones realizadas por los administradores de la plataforma, para	Usuario Autorizado Solicita Bitácora	Generación de reportes	Módulo administración de eventos y seguridad de información	Operación Normal	El sistema genera reporte según los criterios y filtros establecidos	100% de los reportes generados con éxito

Stake holder	Atributo de Calidad	Justificación	Fuente	Estímulo	Artefacto	Ambiente	Respuesta	Medida de la Respuesta
		poder identificar y hacer trazabilidad sobre los cambios que realicen. Esta información debe consultarse en línea y a través de un sitio web						

- Como tal, el modelo de evaluación y selección del software de seguridad, se esquematizo en la matriz de evaluación denominada *MODELO PARA LA EVALUACIÓN DE UNA SOLUCIÓN TECNOLÓGICA PARA LA GESTIÓN DE LA IDENTIDAD - REQUEST FOR PROPOSAL (RFP)*, en la cual se especifican y caracterizan un total de ciento siete preguntas, agrupadas por siete temas y en la que además se define una columna donde ira el Nombre del Proveedor de la solución tecnológica a evaluar y una columna de cometarios u observaciones adicionales, con la cual se puede en un momento dado utilizar por el proveedor para dar las aclaraciones, retroalimentación y preguntas que pueda en un momento dado surgir sobre el proceso. El modelo de evaluación se relaciona a continuación y se encuentra en el archivo de Excel bajo el nombre *RFP*:

Tabla 14. Modelo para la evaluación de una solución tecnológica para la Gestión de la Identidad – Request for Proposal (RFP)

MODELO PARA LA EVALUACIÓN DE UNA SOLUCIÓN TECNOLÓGICA PARA LA GESTIÓN DE LA IDENTIDAD - REQUEST FOR PROPOSAL (RFP)				NOMBRE PROVEEDOR	
Aspecto		**No**	**Ítem**	**Respuesta**	**Observación Adicional**
GENERALES RFP	**GENERALES**	**1**	Indique el nombre de la compañía, la dirección y teléfonos de contacto.		
		2	Indique el esquema de capacitación al personal técnico y funcional		
		3	Indique el esquema de compra o contratación.		
		4	Mencione casos de éxito Nacionales e Internacionales en implementación de soluciones IAM (Identity and Access Management)		
		5	Relacione las empresas cliente que se puedan visitar en caso de requerirse ampliación o verificación en práctica de la información suministrada.		
	ECONÓMICA	**6**	Indique el valor aproximado de la solución en modalidad de compra y/o de servicio (indicando con base en que variable se calcularía) y el esquema que el proponente estime sea el más conveniente de acuerdo al alcance solicitado.		

MODELO PARA LA EVALUACIÓN DE UNA SOLUCIÓN TECNOLÓGICA PARA LA GESTIÓN DE LA IDENTIDAD - REQUEST FOR PROPOSAL (RFP)			NOMBRE PROVEEDOR	
Aspecto	**No**	**Ítem**	**Respuesta**	**Observación Adicional**
EMPRESA	**7**	¿En qué países tiene operaciones la empresa?		
Generales	**8**	¿En qué ciudades de Colombia tiene oficinas?		
	9	¿Cuál es la mayor instalación en Colombia y/o el exterior? ¿Cuántas identidades digitales se lograron estandarizar?		
Modelo de Operación	**10**	Describa la figura comercial en caso de que usted no sea el fabricante; anexe certificados del fabricante que lo acrediten como canal oficial.		
	11	¿Posee un esquema de servicio de atención y manejo de reclamaciones? ¿Cuál es? ¿Cuáles son los horarios? ¿Qué medios emplea?		
	12	Indique evidencias de resultados de tasa de usabilidad obtenidos en las soluciones implementadas basados en los procesos y servicios impactados por la solución.		
Económico	**13**	¿Qué tipo de costos adicionales a la implantación se deben contemplar con su solución		

MODELO PARA LA EVALUACIÓN DE UNA SOLUCIÓN TECNOLÓGICA PARA LA GESTIÓN DE LA IDENTIDAD - REQUEST FOR PROPOSAL (RFP)				NOMBRE PROVEEDOR	
Aspecto		**No**	**Ítem**	**Respuesta**	**Observación Adicional**
			(capacitaciones, herramientas de gestión, generadores de reportes, manutención, viajes, etc.)?		
		14	¿Cómo sería el esquema de costos para un servicio integral de este tipo?		
		15	Montada la solución, en caso de requerirse una customización particular, ¿Con base en que se cotizaría y de quien sería su propiedad?		
		16	Si su solución tiene esquema de contingencia, ¿Cuál es su costo?		
		17	Según la información suministrada, ¿Cuál puede ser el tiempo promedio de implantación de una solución de este tipo?		
FUNCIONALES	**Administración de Acceso**	**18**	¿El sistema integra los distintos usuarios y genera un único ID (único usuario y clave de acceso) para los distintos accesos a las aplicaciones y/o servicios?		
		19	¿El sistema permite definir estándares para el nombramiento de usuarios y contraseñas que serán sincronizadas		

MODELO PARA LA EVALUACIÓN DE UNA SOLUCIÓN TECNOLÓGICA PARA LA GESTIÓN DE LA IDENTIDAD - REQUEST FOR PROPOSAL (RFP)			NOMBRE PROVEEDOR	
Aspecto	**No**	**Ítem**	**Respuesta**	**Observación Adicional**
		con los diferentes aplicativos o servicios?		
	20	¿El sistema cuenta con mecanismos de identidad federada para conexiones futuras a sistemas de otras empresas del grupo o aquellas donde se tenga algún tipo de participación o convenio?		
Administración de Identidades	**21**	¿El sistema permite mediante una interfaz web el ingreso y administración de cada uno de los componentes que conformen la solución (administración, configuración, parametrización de nuevos servicios)?		
	22	¿El sistema permite mediante una interfaz web el ingreso de los usuarios finales, para poder auto gestionar algunos servicios propios de su identidad (Mecanismos de autoservicio) como el cambio y recordación de clave, actualización de datos generales, etc.)?		
	23	¿El sistema permite el diseño e implementación de		

MODELO PARA LA EVALUACIÓN DE UNA SOLUCIÓN TECNOLÓGICA PARA LA GESTIÓN DE LA IDENTIDAD - REQUEST FOR PROPOSAL (RFP)			NOMBRE PROVEEDOR	
Aspecto	**No**	**Ítem**	**Respuesta**	**Observación Adicional**
		flujos de trabajo (workflows) a través de la herramienta de administración web?		
	24	¿La solución cuenta con herramientas de diseño y simulación de modelos de aprovisionamiento?		
	25	¿El sistema permite definir y administrar reglas de negocio, roles y perfiles organizacionales?		
Administración de Eventos y Seguridad de Información	**26**	¿El sistema permite generar informes programados y en tiempo real para conocer el comportamiento de los usuarios sobre las aplicaciones y servicios habilitados?		
	27	¿El sistema permite configurar alertas sobre eventos extraños definidos por los administradores de seguridad?		
	28	¿El sistema cuenta con un módulo para el diseño, personalización y generación de reportes de acuerdo a las necesidades del negocio?		
	29	¿El sistema cuenta con rastros de auditoría que permitan identificar los cambios en los accesos		

MODELO PARA LA EVALUACIÓN DE UNA SOLUCIÓN TECNOLÓGICA PARA LA GESTIÓN DE LA IDENTIDAD - REQUEST FOR PROPOSAL (RFP)				NOMBRE PROVEEDOR	
Aspecto		**No**	**Ítem**	**Respuesta**	**Observación Adicional**
			de los usuarios, sus privilegios y demás funcionalidades, realizadas por los Administradores de la plataforma?		
	Generales	**30**	La solución cuenta con módulos independientes de administración como: - Administración de identidad - Administración del Acceso - Administración de Eventos y seguridad de la Información - Gobernabilidad		
		31	¿La solución es 100% Web-Enabled en todos sus componentes de administración?		
		32	¿El sistema soporta varios idiomas (inglés, español, etc.)?		
		33	¿El sistema soporta la configuración y parametrización de distintas empresas?		
TÉCNICOS	**Generales**	**34**	¿El sistema soporta conectores a aplicaciones desarrolladas In house como JAVA, Proccesss Server, PHP, NET, Cobol?		
		35	¿El sistema soporta integración Nativa con motores de Bases de Datos tipo Oracle,		

MODELO PARA LA EVALUACIÓN DE UNA SOLUCIÓN TECNOLÓGICA PARA LA GESTIÓN DE LA IDENTIDAD - REQUEST FOR PROPOSAL (RFP)			NOMBRE PROVEEDOR	
Aspecto	**No**	**Ítem**	**Respuesta**	**Observación Adicional**
		Sybase, DB2, SQL Server?		
	36	¿El sistema permite que el portal de autogestión pueda ser accedido desde dispositivos móviles (Celulares, eBooks, Palms, etc.)?		
	37	¿El sistema permite configurar la información transaccional on-line y permite definir cual se almacena mediante un proceso de backup?		
	38	¿La solución basa su arquitectura a través del manejo de eventos disparados por las distintas aplicaciones, repositorios o plataformas?		
	39	¿La solución basa su arquitectura mediante la conciliación de repositorios?		
	40	¿La solución cuenta con “Meta Directorios” para el manejo e integración de repositorios?		
	41	¿El sistema "recepciona” de manera automática, todos los eventos o novedades presentadas en el sistema de administración de gestión humana (ingreso de personal, promociones,		

MODELO PARA LA EVALUACIÓN DE UNA SOLUCIÓN TECNOLÓGICA PARA LA GESTIÓN DE LA IDENTIDAD - REQUEST FOR PROPOSAL (RFP)			NOMBRE PROVEEDOR	
Aspecto	**No**	**Ítem**	**Respuesta**	**Observación Adicional**
		vacaciones, retiros, etc.)?		
	42	¿La plataforma cuenta con un módulo para la configuración de aplicaciones que requieran tener acceso Web Single Sign-On (Web-SSO)?		
Restricciones de Tecnología	**43**	¿El sistema se integra con el repositorio Active Directory de la plataforma Microsoft?		
	44	¿El sistema se integra con repositorios abiertos tipo LDAP?		
	45	¿El sistema soporta integración Nativa con plataformas de Correo tipo Exchange Server de Microsoft y Linux tipo Qmail?		
	46	¿La plataforma se integra con el sistema de Recursos Humanos y el repositorio de usuarios definido para contratistas y/o terceros?		
Qas Escenarios de Calidad	**47**	E1		
	48	F1		
	49	M1		
	50	M2		
	51	M3		
	52	M4		
	53	M5		

MODELO PARA LA EVALUACIÓN DE UNA SOLUCIÓN TECNOLÓGICA PARA LA GESTIÓN DE LA IDENTIDAD - REQUEST FOR PROPOSAL (RFP)			NOMBRE PROVEEDOR	
Aspecto	**No**	**Ítem**	**Respuesta**	**Observación Adicional**
	54	S1		
	55	S2		
	56	S3		
	57	S4		
	58	S5		
	59	S6		
Telecomunicaciones e Infraestructura	**60**	¿Cuál es el consumo de ancho de banda por cliente que se requiere?		
	61	Si la solución es Web enabled. Relacione los navegadores (con su versión) con los cuales trabaja la solución.		
	62	Describa la adaptabilidad para múltiples arquitecturas de red y plataformas: cliente/servidor, Intranet, etc.		
	63	Especifique sobre que plataforma de sistema operativo y motor de base de datos la solución presenta mejores rendimientos.		
	64	¿Sobre qué sistemas operativos a nivel de clientes trabaja la solución ofrecida?		
	65	Presente el Esquema General de la Plataforma (diagrama de despliegue), incluyendo los diferentes componentes técnicos (servidores, impresoras, etc.)		

MODELO PARA LA EVALUACIÓN DE UNA SOLUCIÓN TECNOLÓGICA PARA LA GESTIÓN DE LA IDENTIDAD - REQUEST FOR PROPOSAL (RFP)			NOMBRE PROVEEDOR	
Aspecto	**No**	**Ítem**	**Respuesta**	**Observación Adicional**
	66	¿Con qué frecuencia actualizan las versiones del Software a nivel de servidores y clientes?		
	67	¿Cómo es el manejo del log de eventos de los equipos? Descríbalo		
	68	¿Los Logs de eventos de la infraestructura (Hardware y Software) se integran con sistemas de monitoreo tales como Tivoli y HP BAC?		
	69	Suministre las características técnicas de las estaciones de trabajo y dispositivos de usuario final que requiere la solución propuesta.		
	70	¿La solución propuesta se integra con aplicaciones de productividad como (MS Office, MS Exchange), aplicaciones ERP, etc.?		
	71	¿La solución cuenta con algún esquema de contingencia, alta disponibilidad y/o DRP?		
	72	Describa el dimensionamiento de servidores de Aplicación y Base de datos		
	73	¿La solución incluye servidores o éstos los debe asumir la Empresa?		

MODELO PARA LA EVALUACIÓN DE UNA SOLUCIÓN TECNOLÓGICA PARA LA GESTIÓN DE LA IDENTIDAD - REQUEST FOR PROPOSAL (RFP)			NOMBRE PROVEEDOR	
Aspecto	**No**	**Ítem**	**Respuesta**	**Observación Adicional**
	74	¿La solución cuenta con interfaces visuales para validar el estado del servicio en tiempo real desagregado por cada componente de Hardware?		
	75	Describa esquemas de implementación de plataforma en la Nube.		
	76	Describa esquemas de virtualización del Software.		
	77	¿La solución se integra con aplicativos de ERP y CRM?		
	78	Especifique como se integra la solución con otros aplicativos (SOA, web service, etc.)		
	79	¿La solución permite personalizarse con imágenes o logos propios de la compañía?		
	80	Si para que la solución opere, se requiere el desarrollo de algunos componentes, explique: ¿Cómo se realizaría el desarrollo de estas interfaces?		
	81	Especifique las herramientas de modelamiento de procesos utilizada por la solución		
	82	¿El software cuenta con motor de reglas de		

MODELO PARA LA EVALUACIÓN DE UNA SOLUCIÓN TECNOLÓGICA PARA LA GESTIÓN DE LA IDENTIDAD - REQUEST FOR PROPOSAL (RFP)			NOMBRE PROVEEDOR	
Aspecto	**No**	**Ítem**	**Respuesta**	**Observación Adicional**
		negocio?		
	83	¿Cuáles son los web service del aplicativo?		
Administración de Usuarios	**84**	¿La solución cuenta con usuarios o roles preestablecidos (permisos sobre funciones del aplicativo) que se autentiquen con contraseñas?		
	85	¿La solución genera reportes que permitan verificar las operaciones realizadas discriminadas por usuario?		
	86	¿La interfaz de usuario, tiene menús sencillos y claros, ventanas con áreas de trabajo amplias, colores amigables que no saturen la visión o distraigan el proceso?		
Seguridad	**87**	Especificar qué mecanismos de control y de seguridad utiliza el software.		
	88	¿Qué nivel de confidencialidad maneja, es decir la información sólo puede ser accedida por las personas autorizadas?		
	89	¿Su empresa cuenta o contempla un Sistema de Gestión de Seguridad de la Información? ¿Cuenta con certificados al		

MODELO PARA LA EVALUACIÓN DE UNA SOLUCIÓN TECNOLÓGICA PARA LA GESTIÓN DE LA IDENTIDAD - REQUEST FOR PROPOSAL (RFP)				NOMBRE PROVEEDOR	
Aspecto		**No**	**Ítem**	**Respuesta**	**Observación Adicional**
			respecto?		
	Licenciamiento	**90**	¿Cómo se manejan los esquemas de licenciamiento según las herramientas de software y hardware a utilizar? ¿Están incluidas o se licencian de manera independiente?		
		91	Si se requiriere adquirir algún licenciamiento adicional especifique si este puede ser en modalidad Corporativa o que modalidad propone.		
		92	¿Cuántas licencias se entregan o cual es la cantidad de usuarios que cubriría la solución sin costos adicionales a la propuesta?		
	Soporte y Garantía	**93**	¿Tiene un esquema de mantenimiento preventivo y/o correctivo para el software? Indique protocolos, tiempos, frecuencias, etc.		
		94	¿Cuánto es el periodo de garantía del servicio y todos sus componentes, que cubre y desde que momento empieza a contar?		
		95	¿Cuenta con soporte		

MODELO PARA LA EVALUACIÓN DE UNA SOLUCIÓN TECNOLÓGICA PARA LA GESTIÓN DE LA IDENTIDAD - REQUEST FOR PROPOSAL (RFP)				NOMBRE PROVEEDOR	
Aspecto		**No**	**Ítem**	**Respuesta**	**Observación Adicional**
			7x24? ¿Cómo funciona?		
	Administración del aplicativo	**96**	¿Cuáles son los módulos de la plataforma?		
		97	¿Cuál es la información parametrizable de cada módulo?		
	Normatividad	**98**	¿Qué normatividad legal vigente contempla la plataforma?		
		99	Mencione las normas internacionales de Seguridad de la Información utilizadas.		
DESCRIPCIÓN DEL SOFTWARE		**100**	Descripción del Software		
		101	Características y Funcionalidades		
		102	Diagrama de la de Arquitectura del SW		
IMPLEMENTACIÓN PROYECTO		**103**	Descripción de Entregables		
RESTRICCIONES DEL NEGOCIO		**104**	¿El proponente presento propuesta de solución considerando una alternativa en modalidad de servicio (infraestructura, servidor, hardware y software como SaaS) y otra en modalidad de compra directa donde se adquirirá cada componente de la plataforma?		

MODELO PARA LA EVALUACIÓN DE UNA SOLUCIÓN TECNOLÓGICA PARA LA GESTIÓN DE LA IDENTIDAD - REQUEST FOR PROPOSAL (RFP)			NOMBRE PROVEEDOR	
Aspecto	**No**	**Ítem**	**Respuesta**	**Observación Adicional**
	105	¿La propuesta es inferior o igual US$1’000.000 considerando una ejecución a tres años y con una fase inicial que contempla 10.000 empleados directos e indirectos?		
	106	¿La propuesta considera etapas subsiguientes o fases adicionales (sub proyectos) donde cada empresa del grupo analizara y presupuestara el plan de expansión para el cubrimiento de sus aplicaciones o servicios que defina?		
	107	¿La propuesta se contempló en fases, donde la fase inicial solo contemplara aplicaciones o servicios compartidos por todo el Grupo Empresarial (ejemplo: Correo Electrónico, Directorio Activo, etc.) y algunas otras del Core propio de cada negocio?		

Calificación y análisis de resultados

- Finalmente para la consolidación y análisis de resultados se construyeron dos hojas adicionales en el modelo, la primera denominada *Calificación* en la cual se realiza el proceso de valoración a cada una de las preguntas según la respuesta dada por el proveedor de la solución y en donde se aplican los Criterios de calificación establecidos en la sección 3.3.1. Esta calificación la dará el panel de expertos definido por el grupo Empresarial.

Tabla 15. Ejemplo de Calificación de la solución valorada por el panel de expertos

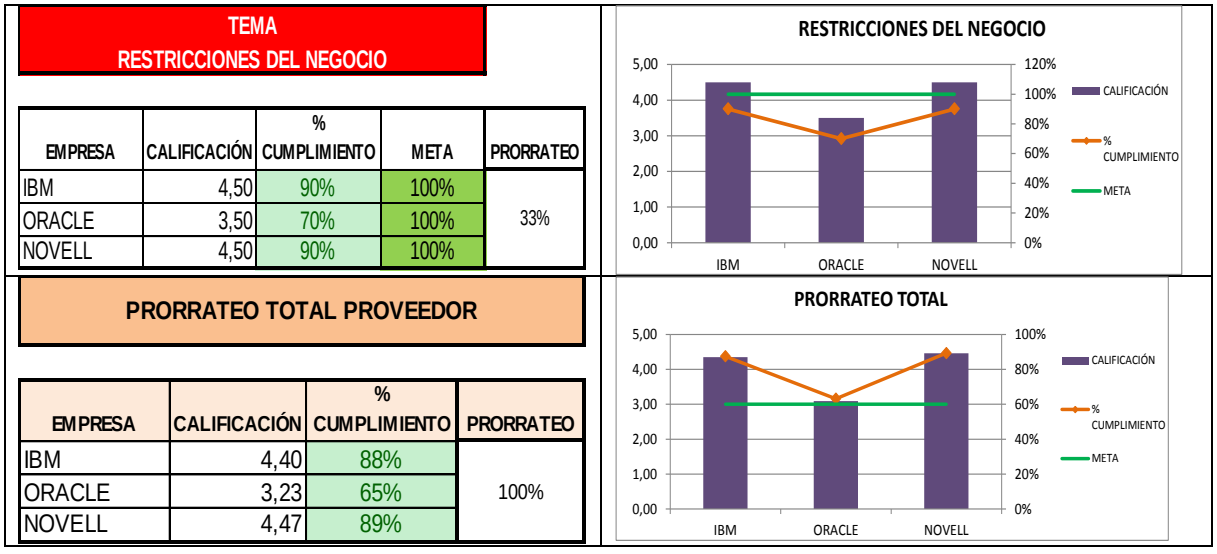
MODELO PARA LA EVALUACIÓN DE UNA SOLUCIÓN TECNOLÓGICA PARA LA GESTIÓN DE LA IDENTIDAD - REQUEST FOR PROPOSAL (RFP)			Proveedor 1	Proveedor 2	Proveedor 3	Proveedor 4
Aspecto		No	Calificación	Calificación	Calificación	Calificación
GENERALES RFP	GENERALES	1	5	5	5	1
		2	5	3	5	1
		3	5	3	3	1
		4	5	3	5	1
		5	5	3	5	1
	ECONÓMICA	6	5	2	5	1
EMPRESA	Generales	7	3	5	3	1
		8	5	3	5	1
		9	2	1	5	1
	Modelo de Operación	10	2	5	5	1
		11	5	3	5	1
		12	5	1	5	1
	Económico	13	3	2	3	1
		14	1	2	3	1
		15	3	3	2	1
		16	5	2	2	1
		17	2	2	5	1

La segunda hoja denominada RESULTADOS, es donde se realiza el proceso de evaluación grafica de las calificaciones dadas por el Panel de expertos, la cual surge del análisis promediado de las respuestas, que serán agrupadas por los siete temas definidos bajo el modelo. En esta hoja se contara además con los cuadros donde la empresa definirá cual ítem o agrupador tiene mayor importancia, puesto que permite ajustar las metas objetivas, según el cumplimiento esperado. El diseño y flexibilidad de la misma permite que la empresa que dese utilizar el

modelo, pueda ajustar los porcentajes y pesos acordes a sus necesidades o características propias de la organización o según las prioridades que defina el Negocio para hacer el respectivo prorrateo por cada una de las siete categorías analizadas.

Por ejemplo, si para una empresa el tema mas importante son las Restricciones de Negocio, lugar donde se definieron las variables de Negocio como el presupuesto, posibilidad de realizar la implementación por fases o por disponibilidad del flujo de caja, podrían determinar que la categoría denominada "TEMA RESTRICCIONES DEL NEGOCIO" de color rojo, tenga un peso de 33% con respecto a las demás categorías, lo que quiere implica que la persona que este utilizando el modelo debe ajustar la columna PRORRATEO con los valores recalculados de cada categoría adicional, que para el ejemplo seria el valor de 13%, lo que finalmente mostraría en la grafica final denominada "PRORRATEO TOTAL PROVEEDOR" el cambio en los resultados según la alteración que se dio en el peso de cada categoría. El ejemplo mencionado se observa en la figura a continuación listada:

Figura 9. Ejemplo Análisis grafico al Prorratear con un mayor valor la categoría RESTRICCIONES DEL NEGOCIO



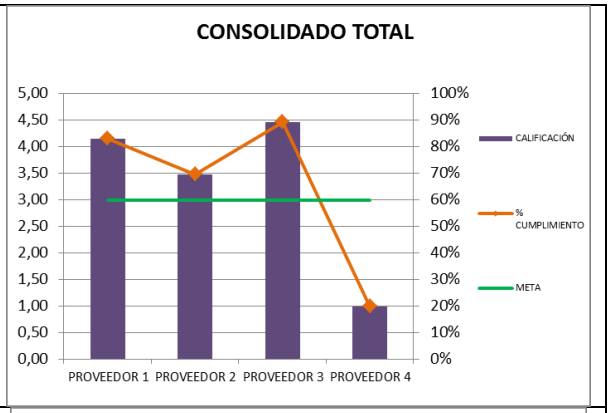
Para el caso de estudio no se utilizo la columna prorrateo puesto que todos los valores fueron analizados como un promedio, sin dar mayor valor a ninguna de la categorías analizadas, luego se definió como meta el valor de 60% a nivel general para el totalizado de respuestas y cada uno de los grupos, el cual surge del establecimiento de un valor definido como aceptable según los Criterios de

calificación establecidos. Para el tema en particular denominado restricciones de negocio se definió una meta del 100%, al considerar que son variables críticas que darán la viabilidad del proyecto en términos que impactan directamente el Negocio, como el presupuesto, esquemas de contratación y fases de implementación.

Figura 10. Ejemplo Análisis grafico de resultados

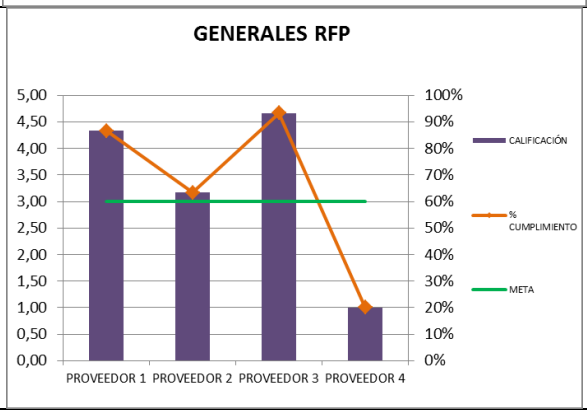
PROMEDIO TOTAL PROVEEDOR

EMPRESA	CALIFICACIÓN	% CUMPLIMIENTO	META
PROVEEDOR 1	4,15	83%	60%
PROVEEDOR 2	3,48	70%	60%
PROVEEDOR 3	4,47	89%	60%
PROVEEDOR 4	1,00	20%	60%



TEMA
GENERALES RFP

EMPRESA	CALIFICACIÓN	% CUMPLIMIENTO	META
PROVEEDOR 1	4,33	87%	60%
PROVEEDOR 2	3,17	63%	60%
PROVEEDOR 3	4,67	93%	60%
PROVEEDOR 4	1,00	20%	60%



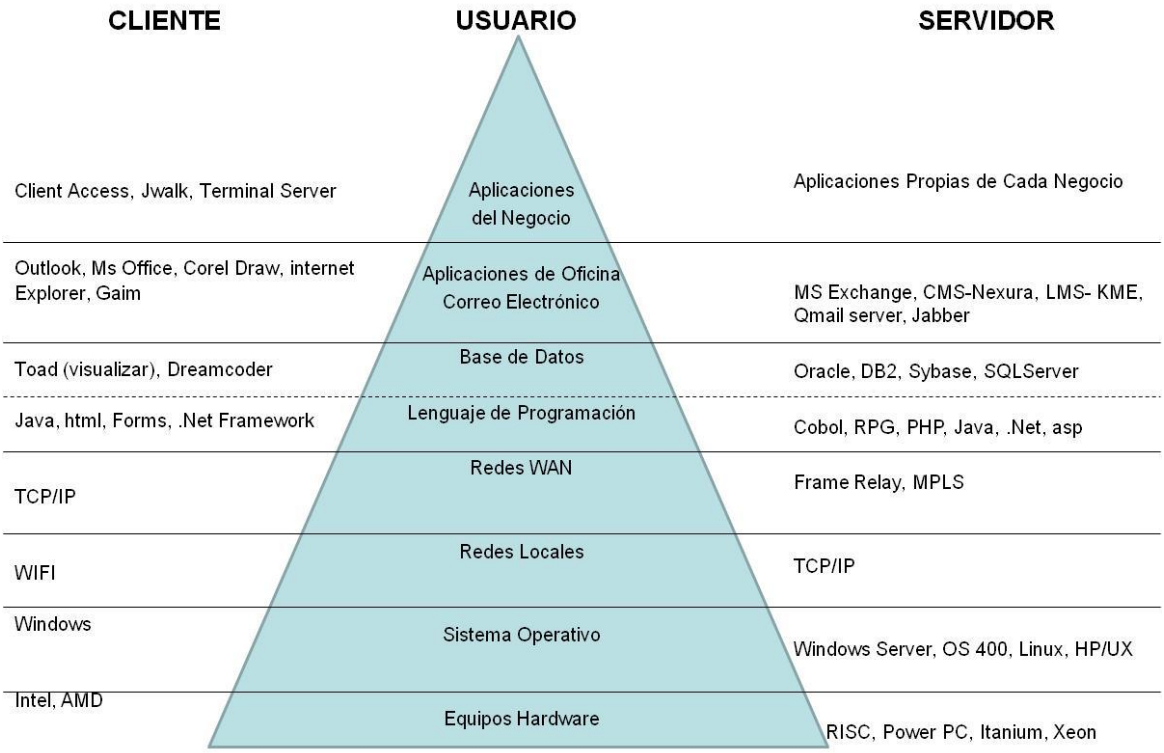
3.4. APLICACIÓN DEL MODELO

3.4.1. Contexto de Aplicación. Para la aplicación del modelo propuesto para la evaluación y selección del sistema de seguridad, se tuvo en cuenta el caso real del Grupo Empresarial Coomeva, donde se desarrolló el proyecto Corporativo que buscaba la selección de un software de seguridad que permitiera controlar el Ciclo de Vida de la Identidad de los usuarios.

Contextualizando de manera resumida este holding Empresarial ofrece a sus asociados una variedad de Servicios Financieros, de Prevención, Asistencia y Solidaridad, Recreación y Turismo, Educación, Desarrollo Empresarial y Servicios de Salud. Cuenta en la actualidad con más de 10.000 empleados contratados de manera directa o indirecta (empresas temporales), además de un número considerable de contratistas y terceros, que por labores propias de su operación, acceden a distintos sistemas, aplicaciones y servicios ofrecidos dentro de las instalaciones.

El grupo Coomeva ha tenido un crecimiento importante en la última década, razón por la cual se han forjado una cantidad considerable de nuevas unidades de negocio, lo que ha culminado con la creación de nuevos productos y servicios para su mercado. En este orden de ideas la compañía durante varios años ha adquirido o desarrollado nuevos productos de software, los cuales tienen diferentes tipos de arquitecturas e infraestructuras tecnológicas que se esquematizan de manera consolidada en la pirámide corporativa de plataformas tecnológicas a continuación representada:

Figura 11. Plataforma Tecnológica Coomeva – Estándares Corporativos



Fuente: Coomeva - Unidad de Tecnología Informática, 2011

Finalmente, el proyecto contempló ejecutarse por fases donde la primera, tiene un alcance inicial al control de los usuarios internos (empleados directos e indirectos, contratistas y terceros) de la organización, sobre los cuales están integrados en el servicio conocido como Directorio Activo (DA), que según las estadísticas de distribución de usuarios matriculados en el 2009, se estima tiene un crecimiento anual del 3% (Ver tabla 16).

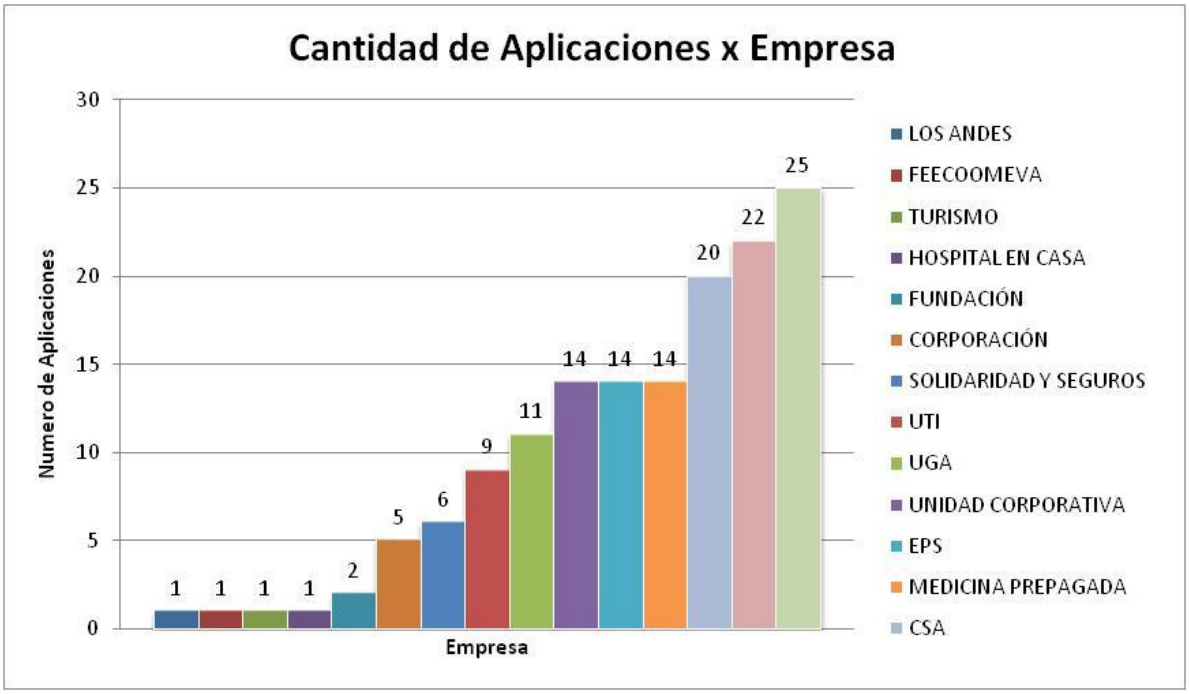
Tabla 16. Cantidad de Usuarios en el Directorio Activo distribuidos por empresa.

EMPRESA	USUARIOS DA	%
CLÍNICA FARALLONES S.A.	62	0,64
CLUB CAMPESTRE LOS ANDES	24	0,25
COOMEVA COOPERATIVA FINANCIERA	1337	13,8
COOMEVA EPS	5390	55,65
COOMEVA MEDICINA PREPAGADA	887	9,16
COOMEVA SERVICIOS ADMINISTRATIVOS	678	7
CORPORACIÓN COOMEVA	105	1,08
FONDO DE EMPLEADOS FECOOMEVA	34	0,35
FUNDACIÓN COOMEVA	35	0,36
GESTIÓN DE ASOCIADOS	481	4,97
HOSPITAL EN CASA S.A.	113	1,17
SOLIDARIDAD Y SEGUROS	182	1,88
TURISMO COOMEVA	54	0,56
UNIDAD CORPORATIVA	130	1,34
UNIDAD DE TECNOLOGÍA INFORMÁTICA	173	1,79
	9685	**100**

Fuente: Coomeva - Unidad de Tecnología Informática, Sep. 2009.

La cantidad de usuarios internos creados sobre el repositorio central (DA), multiplicado por la cantidad de aplicaciones (146 en total) que para el 2011 se encuentran implementadas y soportadas dentro del centro de datos (Ver figura 11), evidencia la problemática del Grupo Empresarial en cuanto a la dificultad para administrar los usuarios en las distintas aplicaciones y por ende la dificultad que surge para la Gestión del Ciclo de vida de la identidad de cada persona que ingresa en la organización.

Figura 12. Cantidad de Aplicaciones distribuidas por empresa.



Fuente: Coomeva - Unidad de Tecnología Informática, 2011.

Bajo este panorama el grupo empresarial COOMEVA realizo una búsqueda de una solución robusta de software y/o hardware que facilite el diseño e implementación de un esquema de Gestión de Identidades Corporativo, que controle de manera eficiente el Ciclo de Vida de la identidad del Usuario (Empleado, Contratista y/o Tercero) desde el momento en que llega a la organización hasta el retiro de la misma (Provisionamiento y De-Provisionamiento), al mismo tiempo que se establezcan mecanismos seguros de autenticación, autorización y auditoria para el acceso a los aplicativos de negocio definidos. En un mediano o corto plazo, esta solución de Gestión de Identidad debería poder extenderse hacia la comunidad de asociados, proveedores y/o usuarios de servicios de Coomeva (Externos), los cuales fácilmente llegarían a unos 300.000 Clientes en Colombia.

3.4.2. Proceso de Aplicación. Para la aplicación y validación del modelo según el caso de estudio, se decidió hacer partícipes de esta propuesta a las Empresas de Soluciones tecnologías que actualmente tienen la mayor representación del

Mercado en soluciones IAM: Identity and Access Management (Gestión de Identidad y Acceso) a Nivel Mundial y que cuentan con su respectiva representación en el mercado Colombiano.

Las empresas seleccionadas son las respectivamente listadas a continuación:

Figura 13. Fabricantes de Soluciones IAM invitados al proceso de aplicación del modelo.

Cada una de estas empresas fue invitada a participar del proceso de evaluación de su respectiva herramienta, a partir de la convocatoria vía correo electrónico y previo al contacto telefónico, con cada uno de los representantes de estas firmas.

Todas las empresas aceptaron participar del proceso, razón por la cual fue enviado a cada una los documentos desarrollados en el proceso de licitación del RFP, más la matriz con la definición de la arquitectura del sistema según lo propuesto en el capítulo 3 de este documento.

Para la retroalimentación de modelo, etapa de resolución de dudas, preguntas y posterior entrega con las respuestas se definió un lapso de tiempo no superior a un mes, de donde finalmente se recibió la respuesta de tres de los cuatro proveedores invitados: IBM, Novell y Oracle.

Con la respuesta dadas por cada fabricante, se procedió a realizar la calificación o valoración de cada una de las preguntas realizadas según los Criterios de calificación establecidos en este documento. Lo que finalmente permitió obtener unos resultados consolidados de evaluación de cada una de las soluciones, de los cuales se entrará en detalle en el capítulo subsiguiente.

De manera general el proceso llevado a cabo para la aplicación del modelo, se procedimentó en el siguiente flujo de proceso:

Figura 14. Flujo general para la evaluación y selección de la herramienta de seguridad IAM

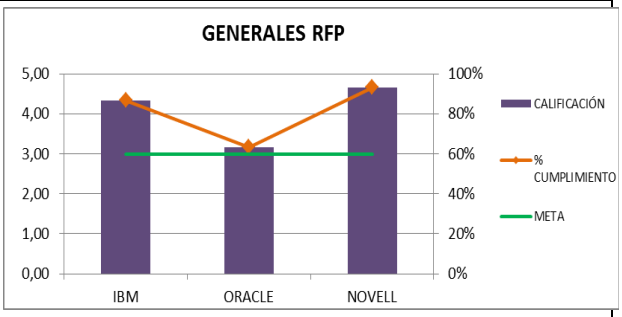
4. ANÁLISIS DE RESULTADOS

Luego de aplicar el modelo de evaluación y selección propuesto a los proveedores del software de Seguridad Informática según el planteamiento establecido en este documento, se realizó el análisis de los resultados según la información y respuestas presentadas por cada uno de ellos.

El análisis de resultados se desarrolló por cada uno de las siete categorías de agrupación establecidas y el correspondiente valor acumulado o totalizado del comparativo entre las Plataformas tecnológicas evaluadas, la cual se obtuvo al promediar las calificaciones otorgadas a cada una de las repuestas presentadas.

Categoria 1 – Generales RFP

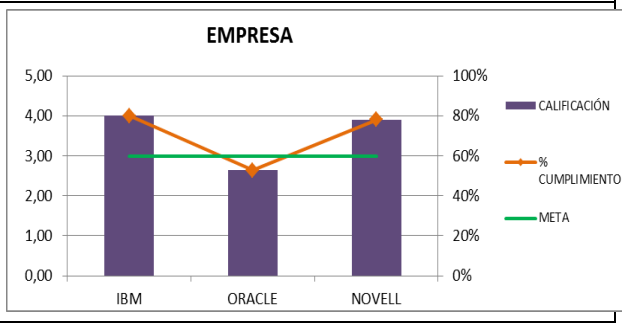
TEMA GENERALES RFP			
EMPRESA	CALIFICACIÓN	% CUMPLIMIENTO	META
IBM	4,33	87%	60%
ORACLE	3,17	63%	60%
NOVELL	4,67	93%	60%



Para esta categoría se puede afirmar que las soluciones ofrecidas y su respectivo fabricante, brindan en términos generales buenas garantías y confiabilidad, en cuanto a su representación, conocimiento y posicionamiento en el mercado Colombiano e Internacional. Sin embargo la disminución del promedio del caso Oracle básicamente se da por factores económicos de la solución, lo cual ya es conocido a nivel general por la industria y el mercado de las TI.

Categoria 2 –Empresa

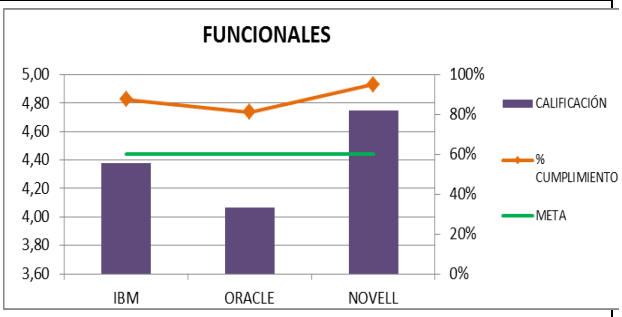
TEMA EMPRESA			
EMPRESA	CALIFICACIÓN	% CUMPLIMIENTO	META
IBM	4,00	80%	60%
ORACLE	2,64	53%	60%
NOVELL	3,91	78%	60%



En esta categoría, se concluye el fuerte posicionamiento en el mercado de la empresa IBM, sin embargo es interesante ver como en Colombia no ha tenido importantes instalaciones alrededor de su producto. De igual forma la información suministrada por la solución de Oracle para el componente de usabilidad de la solución le resta bastantes puntos en términos generales. Finalmente el tema de costos sigue teniendo un alto impacto en las organizaciones, en este caso asociados a los servicios post venta, los cual decrementa puntos a los tres proveedores. Esto reafirma que la tendencia mundial en la venta de productos Tecnológicos, es propiciar esquemas donde los clientes sigan generando ingresos por soporte, garantías y adecuaciones, luego de finalización del entregable inicial planteado.

Categoria 3 – Funcionales

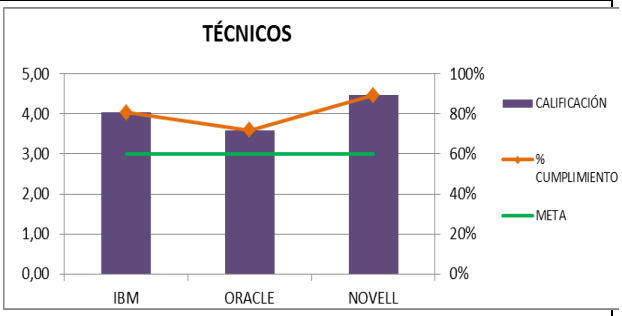
TEMA FUNCIONALES			
EMPRESA	CALIFICACIÓN	CUMPLIMIENTO	META
IBM	4,38	88%	60%
ORACLE	4,06	81%	60%
NOVELL	4,75	95%	60%



Para el tema funcional, se analiza que las herramientas ofrecidas aún tienen debilidades en aspectos de administración y facilidad para los usuarios finales. Lo cual indica que seguirá existiendo la dependencia técnica interna o externa del Negocio, para las solicitudes de los usuarios finales de la solución.

Categoria 4 – Técnicos

TEMA TÉCNICOS			
EMPRESA	CALIFICACIÓN	CUMPLIMIENTO	META
IBM	4,03	81%	60%
ORACLE	3,59	72%	60%
NOVELL	4,47	89%	60%

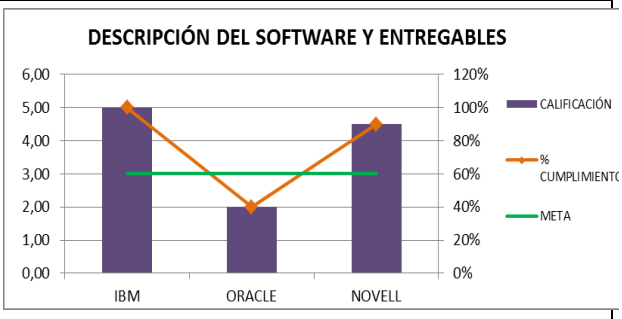


Desde la perspectiva técnica, sobre la cual el Grupo de Expertos que califican la solución usualmente hace mucho énfasis por el importante componente tecnológico, se puede concluir que las soluciones ofrecidas por IBM y Novell, cumplen la mayor parte de requerimientos arquitectónicamente significativos y escenarios de calidad exigidos en la construcción de este modelo. Caso contrario ocurre con la solución de Oracle, en la cual parte de los escenarios de calidad no cumplieron totalmente las expectativas de los Stakeholders, además del tema

técnico de facilidad de integración con otras plataformas propias del Negocio. A nivel general las plataformas de Oracle e IBM, aun no tienen la portabilidad deseada por la arquitectura definida para el sistema y caso de negocio.

Categoria 5 y 6 – Descripcion del Software y Entregables

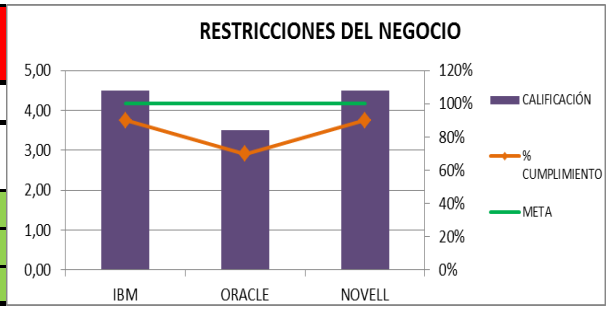
TEMA DESCRIPCIÓN DEL SOFTWARE Y ENTREGABLES			
EMPRESA	CALIFICACIÓN	% CUMPLIMIENTO	META
IBM	5,00	100%	60%
ORACLE	2,00	40%	60%
NOVELL	4,50	90%	60%



Bajo este tema se podría afirmar que todas las soluciones están bien documentadas y soportadas técnicamente y funcionalmente. Sin embargo la baja calificación de uno de los proveedores radica en un comportamiento más de índole de presentación. Lo cual indica la importancia de que en este tipo de procesos se relacionen todos y cada uno de los entregables asociados, ya que el jurado calificador someterá a su juicio, la manera misma sobre como los oferentes manejan el proceso licitatorio.

Categoria 7 – Restricciones del Negocio

TEMA RESTRICCIONES DEL NEGOCIO			
EMPRESA	CALIFICACIÓN	% CUMPLIMIENTO	META
IBM	4,50	90%	100%
ORACLE	3,50	70%	100%
NOVELL	4,50	90%	100%

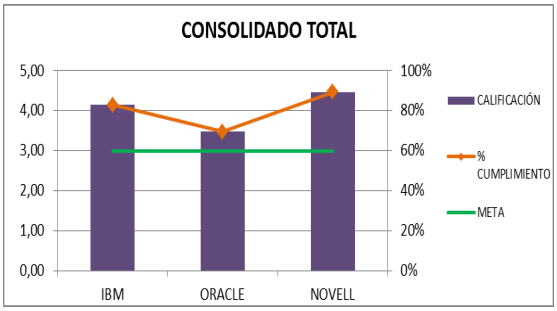


En esta categoría se puede observar que la meta definida es el 100%, ya que bajo la misma se esquematizaron las preguntas relacionadas a restricciones propias del Negocio, las cuales deben cumplirse en su totalidad y por ende su alta penalización. Al analizar los resultados se reafirma el hecho que la solución ofrecida por Oracle supera el presupuesto asignado para el proyecto, lo cual sería un factor decisivo y prepondérate para el Negocio, al momento de seleccionar la plataforma final de la solución.

Resultado Consolidado x Solución IAM

PROMEDIO TOTAL PROVEEDOR

EMPRESA	CALIFICACIÓN	% CUMPLIMIENTO	META
IBM	4,15	83%	60%
ORACLE	3,48	70%	60%
NOVELL	4,47	89%	60%



Finalmente el resultado promediado consolidado del Modelo de evaluación del software de seguridad para el control y administración de la Identidad de los usuarios, determino que la mejor opción costo vs beneficio vs requerimientos arquitecturales del sistema aplicadas a este caso de Negocio, es la solución de Novell en primera opción y en su segunda posición la de IBM. Si bien la solución de Oracle podría considerarse el tema precio sigue siendo uno de los factores por los cuales las organizaciones no implementan este tipo de producto.

5. CONCLUSIONES Y FUTURO TRABAJO

La propuesta desarrollada en este trabajo contemplaba el desarrollo de un modelo para la evaluación y selección del software de seguridad para controlar el ciclo de vida de la identidad digital, en su elaboración se consideró la construcción y elaboración de un documento que describiera la arquitectura del sistema buscado (SAD) y ciertas variables características del proyecto y propias del Negocio. Lo cual permitió caracterizar un total de siete agrupadores o categorías, que contienen un total de 107 preguntas con las cuales se puede evaluar la solución ofrecida por los diferentes proveedores del software.

Una vez definidas y caracterizadas la variables y requerimientos de la plataforma se logró diseñar la Matriz con el Modelo propuesto, lo cual permitió a los proveedores responder el formulario de requerimientos y necesidades para la plataforma, y que una vez entregados los resultados permitiese al grupo de expertos valorar, calificar y analizar las distintas soluciones posicionadas en el mercado.

Finalmente el modelo fue aplicado al caso de estudio del Grupo Empresarial Coomeva, donde se logró identificar aquellas fortaleces y debilidades agrupadas por cada categoría analizada sobre cada una de las plataformas evaluadas, con lo cual se logró emitir un concepto final para la selección de la mejor Plataforma IAM, según las variable y requerimientos de la organización.

Al lograr unos resultados favorables de la aplicación del modelo, se puede concluir que el mismo brindara a las organizaciones o industrias interesadas en adquirir este tipo de soluciones, una herramienta que podrá ser adaptada y parametrizada de acuerdo a las necesidades propias de cada organización, sus metas y cumplimiento esperado en la plataforma.

Una de las lecciones aprendidas en el desarrollo de este documento, indica que en general las empresas u organizaciones por la misma agilidad o poco tiempo para salir con soluciones Tecnológicas exigidas por el Negocios, usualmente no aplican este tipo de buenas prácticas para realizar un trabajo bien elaborado como la elaboración y construcción de un documento de arquitectura del sistema, mediante el cual permita manejar los proceso de licitación y selección de plataformas de software de una manera mucho más formal y garantizando la calidad esperada por la organización.

Finalmente se plantea como trabajo futuro la medición cualitativa y cuantitativa del impacto esperado por el Negocio, luego de la implementación de la solución de Gestión de Identidades. Esta labor se podría realizar partiendo de las definiciones planteadas en el capítulo 2 del DOCUMENTO DE ARQUITECTURA DEL SISTEMA (SAD), con los componentes: Motivadores de Negocio y los mismos escenarios de calidad, que podrían ser utilizados para realizar el proceso de medición y garantía sobre la plataforma adquirida.

BIBLIOGRAFÍA

CLIFF Stoll, The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage. Estados Unidos, 1989, ISBN 0-385-24946-2.

CNET, Exclusive: Third attack against Sony planned, May 2011, http://news.cnet.com/8301-31021_3-20060227-260.html

ConsumerAffairs.com, Jun 2008, http://www.consumeraffairs.com/news04/2008/10/nc_mellon_corp.html

DELOITTE, Markus Bonner. http://www.oracle.com/global/hu/events/20070215_SecurityBB/01%20Deloitte%20eloadas%20-%20Compliance%20Governance%20Risk%20in%20Identity%20and%20Access%20Management.pdf

Grupo Empresarial Coomeva, Informes de Gestión Anual 2010, XVLVII Asamblea General Ordinaria de Delegados, Santiago de Cali, marzo 25 de 2011. http://www.coomeva.com.co/33370

INFORMATIONWEEK, The Business Value Of Technology, Steven Marlin InformationWeek, June 17, 2005 06:00 PM -- http://www.informationweek.com/news/164900904

INTERNATIONAL IT GOVERNANCE: An Executive Guide to ISO 17799/ISO 27001. 1 ed. Gran Bretaña - Londres: 4p, 5p, 6p. ISBN: 0 7494 4748 6.

J.P. Anderson. Computer security threat monitoring and surveillance. Technical Report Technical Report, Washington, PA, Abril 1980

LARSSON, Axel. Drew University. A Case Study: Implementing Novell Identity Management at Drew University, Drew University, 2003.

LESK, Michael & MACKIE, Jeffrey. Identity Management's Misaligned Incentives, IEEE SECURITY & PRIVACY - THE IEEE COMPUTER AND RELIABILITY SOCIETIES, 1540-7993/10/$26.00 © 2010 IEEE.

MARTINEZ TORRES, José Antonio. Seguridad informática. Grupo de Usuarios de GNU/Linux de la Laguna GULAG, Feb 2009. http://www.antoniomtz.org

NETEGRITY WHITE PAPER: Identity and Access Management: The Promise and the Payoff - How An Identity and Access Management Solution Can Generate Triple-digit ROI, Pag-2, Jun 2008

PIOTR PACYNA, Anthony Rutkowski, Amardeo Sarma & Kenji Takahashi. Trusted Identit y for All: Toward Interoperable Trusted Identit y Management Systems, COMPUTER - IEEE Computer Society, 0018-9162/09/$25.00 © 2009 IEEE

RACHNA, Dhamija & DUSSEAULT, Lisa. The Seven Flaws of Identity Management: Usability and Security Challenges, IEEE SECURITY & PRIVACY - IEEE Computer Society, 1540-7993/08/$25.00 © 2008 IEEE.

ROZANSKI, Nick y WOODS, Eoin. \Software systems architecture: working with stakeholders using viewpoints and perspectives. \Upper Saddle River, New Jersey: Addison-Wesley, c2005. ISBN 0321112296 Sig. Topográfica: 005.3/R893s arquitectudinales

SARBANES–OXLEY Act, H.R. 3763, H. Rept. 107–414, H. Rept. 107–610. http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_bills&docid=f:h3763enr.tst.pdf

STEVEN, John. Introduction to Identity Management Risk Metrics, IEEE SECURITY & PRIVACY - IEEE Computer Society, 1540-7993/06/$20.00 © 2006 IEEE.
The Wall Street Journal, Digital Network, Oct 2008, http://www.secureidentitysystems.com/assets/files/Oct-WSJ-IDtheftConcern.pdf

UNIVERSIDAD DE LOS ANDES. Proyecto de Mejoramiento del Proceso de Originación de Crédito del Banco de los Alpes, Documento de Arquitectura del Sistema(SAD), Especialización en construcción de software, Bogotá 2010

http://es.scribd.com/doc/44594204/JARC-ARQSW-DocumentoArquitecturaSw-v-5-0

UNIVERSIDAD ICESI, Maestría en Gestión de Informática y Telecomunicaciones, Introducción a la Arquitectura de Sistemas Computacionales, pagina 10.

UNOPS Oficina de Proyectos de las Naciones Unidas, Manual de Adquisiciones, Revisión 4, Septiembre 2010. www.unops.org
Wikipedia®, Empresas multinacionales (EMN) o empresas transnacionales Multinacional, 9 de noviembre de 2011. http://es.wikipedia.org/wiki/Multinacional

Wikipedia®, Grupo de empresas, grupo empresarial, grupo industrial, conglomerado empresarial o conglomerado industrial, 21 septiembre de 2011. http://es.wikipedia.org/wiki/Multinacional.

UNIVERSIDAD DE LOS ANDES, Departamento de Ingeniería de Sistemas y Computación, Plantilla Documento de Arquitectura, http://sistemas.uniandes.edu.co/~isis3702/dokuwiki/doku.php?id=sad

ANEXOS

Anexo A. Ver archivo adjunto en Excel Modelo de evaluación y selección de la plataforma IAM.xlsx