TESIS

MAESTRÍA EN ADMINISTRACIÓN DE NEGOCIOS

Cálculo del impacto económico de soluciones de “Gestión de Identidades y Accesos” en las organizaciones

Tesista: Ing. Juan Pablo Rotella

Director: Mg. Lic. Alejandro Vazquez

Mendoza, 2016

DEDICATORIA

A mi familia por el apoyo y la infinita paciencia.

A todo aquel que crea de utilidad esta pequeña contribución.

AGRADECIMIENTOS

A la Universidad Tecnológica Nacional, por brindarme, formación de grado y posgrado.

A Alejandro, por la dirección durante el tiempo de desarrollo de esta Tesis.

RESUMEN

Para enfrentar las actuales amenazas de seguridad de la información y exigencias del mercado, las organizaciones cuentan con un presupuesto limitado y distintas iniciativas que priorizar. Las soluciones de “Gestión de Identidades y Accesos”, o como se las denomina generalmente “Identity and Access Management”, han demostrado valor a la hora de resolver estos problemas. Sin embargo, por sus características resulta complejo cuantificarlo de forma asertiva.

En el presente trabajo, el autor en primer lugar introduce al estado del arte y el contexto actual de las soluciones IAM. Además, distintos modelos que puedan ser aplicados para evaluar el impacto económico de estos proyectos y finalmente un análisis comparativo de los mismos.

El estudio define un punto base de análisis e investigación para aplicar en distintas organizaciones de Argentina y la región que implementen y/o investiguen soluciones de este tipo.

Palabras claves: Gestión de Identidades y Accesos, Identity and Access Management, IAM, Rentabilidad, Métricas, Evaluación de proyectos, Impacto Económico, Seguridad informática.

ABSTRACT

To meet today's information security threats and market demands, organizations have a limited budget and need to prioritizing diferent initiatives. Projects of Identity and Access Management, or as they are usually called IAM, have proven value in solving these problems but by its nature is complex to quantify them assertively.

In this paper, the author first introduces the state of the art and the current context of IAM Solutions. Then different models that can be applied to assess the economic impact of these projects and finally a comparative analysis of them.

The study defines a base point for analysis and research applied in different organizations in Argentina and the region.

Keywords: Identity and Access Management, IAM, Profitability, Metrics, Project Evaluation, Economic Impact, Information Security.

ÍNDICE

LISTA DE TABLAS

LISTA DE FIGURAS

LISTA DE ABREVIATURAS

ALE: Annual Loss Expectancy.

ANSI: American National Standards Institute.

ARO: Annual Rate of Occurrence.

CERT: Computer Emergency Response Team.

CIO: Chief Information Officer.

CISO: Chief Information Security Officer.

CSO: Chief Security Officer.

CTO: Chief Technology Officer.

DAG: Data Access Governance.

EMM: Enterprise Mobility Management.

ENISA: European Union Agency for Network and Information Security.

GUID: Globally Unique IDentifier.

IaaS: Infraestructure as a Service

IAM: Identity and Access Management.

IDaaS: Identity as a Service.

IEC: International Electrotechnical Commission.

IGA: Identity Governance and Administration.

INCITS: InterNational Committee for Information Technology Standards.

ISO: International Organization for Standardization.

ITU: International Telecommunication Union.

NIST: National Institute of Standards and Technology.

OASIS: Organization for the Advancement of Structured Information Standards.

PaaS: Platform as a service.

PAM: Privileged Identity Management.

PCI-DSS: Payment Card Industry Data Security Standard.

RBAC: Role Based Access Control.

ROI: Return on Investment.

ROSI: Return on Security Investment.

SaaS: Software as a Service.

SAML: Security Assertion Markup Language.

SCIM: System for Cross-Domain Identity Management.

SIEM: Security Information and Event Management.

SLE: Single Loss Expectancy.

SOD: Segregation Of Duties.

SOX: Sarbanes-Oxley Act.

SSO: Single Sign On.

TI: Tecnologías de la Información.

TIR: Interna de Retorno.

UEBA: User and Entity Behavioral Analytics.

VAN: Valor Presente Neto.

1 INTRODUCCIÓN

1.1 RESUMEN

El presente capítulo es una introducción a la Tesis, sus objetivos, hipótesis y estructura.

En la sección 1.2 se formula y fundamenta la problemática investigada. En la sección 1.3 se especifican los objetivos del trabajo. Posteriormente la sección 1.4 detalla las hipótesis planteadas. En la sección 1.5 se describe la metodología utilizada. Finalmente, la sección 1.6 resume la estructura del documento.

1.2 FORMULACIÓN Y FUNDAMENTACIÓN DEL PROBLEMA A INVESTIGAR

En la actualidad las empresas y gobiernos de todo el mundo gastan cada año más de 3,5 trillones de dólares en inversiones en Tecnologías de la Información y se espera un crecimiento sostenido en el futuro (Gartner, 2015). Debido a la dependencia de la tecnología, la necesidad de que las medidas de seguridad sean suficientes adquiere un rol fundamental (Beaver, 2008). La amplia definición de seguridad generalmente se refiere a la confidencialidad, integridad y disponibilidad de los activos de información (Mizzi, 2010).

Las amenazas de seguridad de la información afectan a todo tipo de organizaciones, incluso grandes empresas como Sony o Lockheed Martin fueron atacados y perdieron datos confidenciales recientemente (Demetz & Bachlechner, 2013). Los incidentes de seguridad informática no sólo están aumentando en número, su impacto es cada vez mayor y están dirigidos a una amplia matriz de información y vectores de ataque. No es de extrañar, que exista una creciente preocupación entre los ejecutivos y expertos en seguridad, tanto del sector público como del privado. Según el "US State of Cybercrime Survey" del CERT realizado en 2015, el 76 % de los encuestados afirmo estar más preocupados por las amenazas de ciberseguridad que en los 12 meses anteriores.

Recientes estudios muestran que los atacantes son cada vez más eficaces a la hora de aprovechar los puntos débiles de la seguridad y para ocultar y encubrir sus actividades. Además de forma involuntaria los usuarios y los equipos de TI se han convertido en parte del problema de seguridad, con el agravante de que hay una fuerte contradicción entre la percepción del grado de preparación en materia de seguridad con la que realmente existe (Cisco Systems Inc., 2015).

Las organizaciones se enfrentan a un número creciente de regulaciones como por ejemplo SOX o PCI-DSS y como resultado están obligados que aumentar sus gastos en actividades de cumplimiento y seguridad (Demetz & Bachlechner, 2013). Además, el papel de la seguridad ya no es sólo de mitigación de riesgos y cumplimiento, también se trata de la consecución de otros objetivos clave del negocio, tales como reducción de costos (McQuaide, 2003).

A raíz de lo anterior, las empresas invierten en contramedidas para prevenir o al menos reducir la probabilidad y el impacto de las brechas de seguridad (Demetz & Bachlechner, 2013). La criticidad y la probabilidad de ser explotados difieren de activo a activo y por eso no todos deben recibir el mismo nivel de atención (Bagchi & Udo, 2003). La determinación del nivel de riesgo aceptable y la selección de la mejor contramedida no es una tarea fácil, no existe una metodología estándar y a menudo los administradores de seguridad tienen que decidir entre demasiadas alternativas (Bistarelli, Fioravanti, & Peretti, 2005).

Dentro del amplio espectro de proyectos, herramientas y soluciones, se destacan las de Identity and Access Management. Ya que no solo son un producto de seguridad, sino un conjunto de procesos y tecnologías de apoyo para la gestión integral, unificada y segura de las identidades de una organización. Sirven como un factor diferenciador al ofrecer a clientes internos y externos una mejor y más segura experiencia. También agregan valor volviendo más simples y robustos los procesos organizacionales (McQuaide, 2003).

Como en cualquier otro tipo de proyecto se requieren soluciones efectivas y eficientes desde el punto de vista técnico, pero además las organizaciones deben prestar atención a la viabilidad económica. Con un presupuesto limitado y un gran número de activos a proteger las inversiones deben ser evaluadas deliberadamente (Gordon & Loeb, 2006). Valorar las inversiones en seguridad es un proceso crucial que las empresas deben realizar, ya que actúa como intermediario entre las decisiones relativas a cuestiones

financieras y las implementaciones de seguridad. Tienen que encontrar el equilibrio entre la posibilidad de mitigar los riesgos de amenazas y los costos asociados (Demetz & Bachlechner, 2013).

Los tomadores de decisiones ejecutivas quieren saber el impacto que la seguridad está teniendo en la organización (ENISA, 2012). No les interesa conocer de infraestructura o tecnología, necesitan responder preguntas como ¿Cuándo debe invertir la organización en seguridad?, ¿Cuánto le está costando la falta de seguridad a la empresa?, ¿Qué impacto tiene la falta de seguridad en la productividad?, ¿Qué impacto tendría un fallo de seguridad catastrófica?, ¿Cuáles son las soluciones más rentables?, ¿Qué impacto tendrán las soluciones sobre la productividad?, entre otras (Sonnenreich, 2006).

Un problema común que se presenta a los CSO y CISO, e incluso a los CIO y CTO, es que están en desventaja al competir contra otras funciones corporativas por financiación debido a las características particulares de este tipo de proyectos. A diferencia de otras inversiones no generan ingresos monetarios, aunque resultaran en ahorros de costos mediante la prevención brechas de seguridad o reduciendo la probabilidad de su ocurrencia y su impacto (Demetz & Bachlechner, 2013). Además, hay una gran dificultad para identificar y cuantificar sus beneficios, especialmente para traducirlos en términos económicos y por lo tanto mostrar su potencial rentabilidad (Solms & Solms, 2004).

El presente trabajo estudia y compara diferentes modelos para evaluar proyectos de Identity and Access Management de forma de conocer si son aplicables y su precisión a la hora de medir el impacto económico en las organizaciones.

1.3 OBJETIVO

Exponer un marco conceptual para la evaluación de proyectos de Identity and Access Management, lo suficientemente robusto para lograr estimaciones completas y certeras del valor económico agregado aportado y así demostrar su viabilidad económica.

1.3.1 OBJETIVOS ESPECÍFICOS

Los objetivos específicos del trabajo son:

- Investigar el estado del arte y el contexto actual en lo referido a soluciones de Identity and Access Management.
- Identificar los principales drivers que tienen las empresas que evalúan e invierten en proyectos de Identity and Access Management.
- Investigar modelos de evaluación de proyectos de seguridad informática y en especial aplicables a Identity and Access Management.

1.4 HIPÓTESIS DE TRABAJO

Se plantean las siguientes hipótesis:

- "Es posible cuantificar y comprobar con precisión y rigor científico el valor económico agregado de proyectos de Identity and Access Management".
- "Bajo determinadas condiciones los proyectos de Identity and Access Management tienen rentabilidad positiva, y por lo tanto son capaces de aportar valor agregado a las empresas".

1.5 METODOLOGÍA EMPLEADA

El presente es un trabajo de compilación bibliográfica de fuentes y autores relevantes, empleando la técnica de "análisis de contenido" para la recolección de datos, que ordena y expone distintos modelos propuestos para evaluar proyectos de Identity and Access Management.

1.6 ESTRUCTURA DEL TRABAJO

El presente trabajo de Tesis se estructura en capítulos que se describen a continuación.

- Marco teórico: El capítulo introduce el estado de la cuestión que presenta conceptos básicos importantes y puntualiza sobre distintos tópicos relevantes como Rol Based Access Control, Federación y Single Sign On.
- Estudio del contexto: El capítulo describe el contexto sobre el cual se realiza el estudio, analizando el presente y futuro de las soluciones de gestión de identidades y accesos. También expone las soluciones y herramientas IAM disponibles en el mercado.
- Evaluación económica: El capítulo comprende un estudio de los costos, beneficios y la evaluación cuantitativa del riesgo de IAM. Además, un resumen y comparación de los distintos modelos propuestos para el análisis económicoo de estos proyectos de seguridad y finalmente un ejemplo de aplicación.
- Conclusiones: En este capítulo a partir de los resultados de cada una de las etapas anteriores, se obtendrán las conclusiones del trabajo de investigación en relación con las hipótesis planteadas.

2 MARCO TEÓRICO

2.1 RESUMEN

El presente capítulo describe el marco teórico del trabajo.

En la sección 2.2 se detallan definiciones básicas relacionadas a la gestión de identidades y accesos. En la sección 2.3 el panorama general de las normas y estándares relacionadas. Posteriormente la sección 2.4 profundiza sobre el estándar RBAC. La sección 2.5 describe el Framework IAM y sus componentes. El punto 2.6 identifica los principales drivers de los sistemas IAM. Finalmente, la sección 2.7 especifica algunas estrategias y buenas prácticas generales para una implementación IAM.

2.2 CONCEPTOS BÁSICOS IAM

2.2.1 ENTIDAD

Una entidad es un concepto heterogéneo, puede ser una persona física, un animal, una persona jurídica, una organización, un activo, un dispositivo, una aplicación de software, un servicio, etc. En el contexto de las telecomunicaciones, ejemplos de entidades incluyen puntos de acceso, elementos de red, aplicaciones de software, servicios y dispositivos, interfaces, etc. (ISO/IEC, 2011).

Para clarificarlo se propone las siguientes definiciones:

> "Something that has separate and distinct existence and that can be identified in context." (ITU, 2010)

> "Item inside or outside an information and communication technology system, such as a person, an organization, a device, a subsystem, or a group of such items that has recognizably distinct existence." (ISO/IEC, 2011)

2.2.2 IDENTIDAD

El concepto anterior es importante para poder comprender que son las identidades:

> "A representation of an entity in the form of one or more attributes that allow the entity or entities to be sufficiently distinguished within context" (ITU, 2010)

> "Set of attributes related to an entity" (ISO/IEC, 2011)

Con base en las definiciones precedentes, podemos afirmar que una identidad es una representación de una entidad por medio de uno o varios atributos que la identifican en un dominio o contexto específico. Entendiendo por atributos lo siguiente:

> "Information bound to an entity that specifies a characteristic of the entity" (ITU, 2010)

> "Characteristic or property of an entity that can be used to describe its state, appearance, or other aspects" (ISO/IEC, 2011)

Y por dominio o contexto:

> "An environment with defined boundary conditions in which entities exist and interact." (ITU, 2010)

> "Environment where an entity can use a set of attributes for identification and other purposes" (ISO/IEC, 2011)

Un atributo de una identidad describe el estado y otras cualidades de una entidad relevante en un dominio determinado. Cada atributo tiene su propia semántica para regir la interpretación de los valores que puede adquirir. Tiene un tipo, valor y un contexto operacional (ISO/IEC, 2011).

Uno o varios de estos atributos permiten determinar de forma única y distinguible a una identidad de otras en el sistema. A este concepto se lo denomina identificador único:

> "One or more attributes used to identify an entity within a context." (ITU, 2010)

> "identity information that unambiguously distinguishes one entity from another one in a given domain" (ISO/IEC, 2011)

El propósito del sistema determina cuál de los atributos que describen una entidad se utilizan para conformar una identidad. Por lo tanto, dentro de un sistema una identidad será el conjunto de los atributos relacionados con una entidad que son relevantes para el dominio particular de aplicación del sistema (ISO/IEC, 2011).

La identidad de una entidad sirve para hacer relevante la información conocida en sus interacciones con los servicios y el acceso de los recursos proporcionados por un

dominio. Un dominio especifica el tipo y la gama de valores permisibles de atributos para ser utilizados para la identificación u otros propósitos (ISO/IEC, 2011).

2.2.3 IDENTIDAD VIRTUAL

Si bien la noción de identidad en el mundo físico es bastante clara, lo mismo no puede decirse para las identidades digitales que son el objeto de estudio de este trabajo.

Se propone la siguiente definición general:

> "A digital representation of the information known about a specific individual, group or organization" (ITU, 2010)

Es necesario entonces vincular este concepto al campo de estudio del trabajo con la siguiente definición:

> "A digital identity abstracts from a real world person, implementing a unique digital representation of the entity. Also, this profile details relationships to other entities or parties and contains associated access rights and credentials" (Windley, 2005)

Si la desglosamos, una identidad virtual está compuesta por las siguientes partes principales (Chong, 2004):

- Identificador: Una pieza de información que identifica de forma exclusiva el sujeto de esta identidad dentro de un contexto dado. Ejemplos de identificadores son direcciones de correo electrónico o identificadores únicos globales (GUID).
- Credenciales: Datos públicos o privados que podrían ser utilizados para probar la autenticidad de una identidad.
- Atributos: Datos que ayudan a describir la identidad. Atributos básicos que se pueden utilizar a través de una serie de contextos de negocios o aplicación.

- Atributos específicos de Contexto: Datos que ayudan a describir la identidad, pero que sólo se hace referencia y se utiliza dentro del contexto específico donde se utiliza la identidad.
- Entitlements: Son los derechos y privilegios asociados con las identidades.

2.2.4 GESTIÓN DE IDENTIDADES

Para precisar el concepto de gestión de identidades, se propone las siguientes definiciones:

> "A set of functions and capabilities used for assurance of identity information (e.g., identifiers, credentials, attributes); assurance of the identity of an entity and supporting business and security applications." (ITU, 2010)
>
> "Processes and policies involved in managing the lifecycle and value, type and optional metadata of attributes in identities known in a particular domain" (ISO/IEC, 2011)
>
> "Identity management is the set of business processes, and a supporting infrastructure for the creation, maintenance, and use of digital identities. " (Lewis, 2003).

De lo anterior, se infiere que el propósito de la gestión de identidades es la administración integral y segura de las mismas en un contexto dado.

2.2.5 GESTIÓN DE ACCESOS

Se entiende por gestión o control de accesos lo siguiente:

> "A procedure used to determine if an entity should be granted access to resources, facilities, services, or information based on pre-established rules and specific rights or authority associated with the requesting party" (ITU, 2010)

Un proceso fundamental del mismo es la autenticación, que es por el cual las identidades son comprobadas.

> "A process to achieve sufficient confidence in the binding between the entity and the presented identity." (ITU, 2010)

La autorización es la determinación de si se permite una identidad realizar una acción o acceso a un recurso (Chong, 2004).

La información que se puede utilizar para la identificación se basa en atributos específicos de la entidad denominados credenciales:

> "A set of data presented as evidence of a claimed identity and/or entitlements" (ITU, 2010)

2.2.6 Enterprise Identity and Access Management

De las secciones anteriores, concluimos que la gestión de identidades y accesos es una disciplina de seguridad que aborda la necesidad crítica de garantizar un acceso adecuado a los recursos a través de ambientes tecnológicos heterogéneos (Wagner, 2010).

Para lograrlo, existen estándares y tecnología a disposición de las empresas:

> "A domain may use an identity management system to support its interaction with entities, e.g. authentication. Identity Management covers the lifecycle of identity information from initial enrolment to archiving or deletion. Identity

> Management includes the governance, policies, processes, data, technology, and standards, which may include" (ISO/IEC, 2011)

IAM no es un producto, sino que es un framework de diferentes tecnologías que pueden ser integradas en una infraestructura de IT de las organizaciones (Royer, Enterprise Identity Management – What's in for Organisations, 2007).

2.3 NORMAS Y ESTÁNDARES RELACIONADOS

Existen muchas normas y estándares relacionados a la gestión de identidades y accesos aplicados a diferentes ámbitos. A continuación, se mencionan algunos de las más importantes.

ISO y más específicamente la norma ISO / IEC JTC 1, SC27 IT Security techniques WG5 Identity Access Management and Privacy techniques, está llevando a cabo algunos trabajos de normalización para la gestión de identidades. Tales como la elaboración de un marco que incluya la definición de términos relacionados con la identidad.

Las normas publicadas y elementos de trabajo actual incluyen lo siguiente:

- ISO/IEC 24760-1 A framework for identity management—Part 1: Terminology and concepts.
- ISO/IEC CD 24760-2 A Framework for Identity Management—Part 2: Reference architecture and requirements.
- ISO/IEC WD 24760-3 A Framework for Identity Management—Part 3: Practice.
- ISO/IEC 29115 Entity Authentication Assurance.
- ISO/IEC WD 29146 A framework for access management.
- ISO/IEC WD 29003 Identity Proofing and Verification.
- ISO/IEC 29100 Privacy framework.
- ISO/IEC 29101 Privacy Architecture.
- ISO/IEC 29134 Privacy Impact Assessment Methodology.

Por su parte ITU desarrolla estándares a través de Identity Management Global Standards Initiative (IDM-GSI), que se centra en normas necesarias para el despliegue de capacidades de gestión de identidad.

Su fin es lograr identidades digitales seguras y confiables utilizadas en telecomunicaciones, redes de control, y una variedad de otros servicios. IDM-GSI armoniza, en colaboración con otros organismos, diferentes enfoques en todo el mundo.

Algunos de los trabajos publicados son:

- X.1250: Baseline capabilities for enhanced global identity management and interoperability.
- X.1251: A framework for user control of digital identity.
- X.1252: Baseline identity management terms and definitions.
- X.1253: Security guidelines for identity management systems.
- X.1254: Entity authentication assurance framework.
- X.1255: Framework for discovery of identity management information.
- X.1275: Guidelines on protection of personally identifiable information in the application of RFID technology.
- Y.2720: NGN identity management framework.
- Y.2721: NGN identity management requirements and use cases.
- Y.2722: NGN identity management mechanisms.

Por su parte el NIST también trabaja sobre diferentes iniciativas relacionadas la gestión de identidades y accesos. Posiblemente el más relevante es el estándar ANSI INCITS 359-2004 que define las bases de RBAC, el cual trataremos en la siguiente sección con mayor profundidad.

2.4 ROLE BASED ACCESS CONTROL

2.4.1 HISTORIA

Role-based access control o control de acceso basado en roles, formalizado en 1992 por David Ferraiolo y Rick Kuhn (Ferraiolo & Kuhn, 1992), se ha convertido en el modelo predominante para el control de acceso avanzado, ya que además de proveer seguridad ha demostrado otros beneficios como reducir costos operativos. Es por esto, que se considera uno de los pilares de la gestión de accesos e identidades virtuales.

Una variedad de proveedores de TI comenzó a desarrollar productos basados en este modelo en 1994. Para el año 2000, el modelo Ferraiolo-Kuhn se integró con el marco de Sandhu (Sandhu, Coyne, Feinstein, & Youman, 1996) para crear un modelo unificado para RBAC, publicado como el modelo del NIST RBAC (Sandhu, Ferraiolo, & Kuhn, 2000) y adoptado como un estándar ANSI / INCITS en 2004.

Hoy en día, la mayoría de los proveedores de tecnología de la información han incorporado RBAC a sus líneas de productos y es un estándar ampliamente adoptado en todas las soluciones IAM. A partir de 2010, la mayoría de las empresas de más de 500 empleados están utilizando en mayor o menor medida RBAC, de acuerdo con el Research Triangle Institute.

El modelo NIST RBAC es una definición estandarizada que puede aplicarse independientemente de la tecnología que se utilice para soportarlo. Aunque originalmente fue desarrollado por el Instituto Nacional de Estándares y Tecnología, está protegido por copyright y distribuido como INCITS 359-2004 por el Comité Internacional de Normas de Tecnología de la Información.

2.4.2 TÉRMINOS CLAVES

Los siguientes términos tienen significados especializados que componen esta norma.

Se define a un componente como:

> "As used in this standard, component refers to one of the major blocks of RBAC features, core RBAC, hierarchical RBAC, SSD relations, and DSD relations." (ANSI INCITS, 2004)

Se define a un objeto como:

> "As used in this standard, an object can be any system resource subject to access control, such as a file, printer, terminal, database record, etc." (ANSI INCITS, 2004)

Se define a una operación como:

> "An operation is an executable image of a program, which upon invocation executes some function for the user." (ANSI INCITS, 2004)

Se define a un permiso como:

> "Permission is an approval to perform an operation on one or more RBAC protected objects." (ANSI INCITS, 2004)

Se define a un Rol como:

> "A role is a job function within the context of an organization with some associated semantics regarding the authority and responsibility conferred on the user assigned to the role." (ANSI INCITS, 2004)

Se define a un usuario como:

> "A user is defined as a human being. Although the concept of a user can be extended to include machines, networks, or intelligent autonomous agents, the

definition is limited to a person in this document for simplicity reasons.” (ANSI INCITS, 2004)

2.4.3 MODELO DE REFERENCIA

El modelo de referencia RBAC se estructura en cuatro componentes Core RBAC, Hierarchical RBAC, Static Separation of Duty Relations, and Dynamic Separation of Duty Relations (ANSI INCITS, 2004).

Cada componente del modelo se define por los siguientes subcomponentes (ANSI INCITS, 2004):

- Conjuntos de elementos básicos
- Relaciones de RBAC que implican esos conjuntos de elementos
- Un conjunto de funciones de mapeo

Core RBAC define una colección mínima de elementos, conjuntos de elementos y sus relaciones con el fin de lograr un sistema de control de accesos basado en roles completo. Esto incluye la asignación usuario-rol y las relaciones de asignación de permiso-rol, considerada fundamental en cualquier sistema RBAC. Además, Core RBAC introduce el concepto de activación de rol como parte de la sesión de un usuario dentro de un sistema informático. Core RBAC se requiere en cualquier sistema RBAC, en cambio los otros componentes son independientes entre sí y se pueden implementar por separado (ANSI INCITS, 2004).

El componente Hierarchical RBAC añade las relaciones para soportar jerarquías de roles. Una jerarquía es matemáticamente un orden parcial que define una relación de orden entre roles. Además, Hierarchical RBAC va más allá de la simple asignación de roles a usuarios y permisos mediante la introducción del concepto de conjunto de usuarios autorizados y permisos autorizados de un rol (ANSI INCITS, 2004).

Un tercer componente del modelo, Static Separation of Duty Relations (SSD), añade las relaciones de exclusividad entre los roles con respecto a las asignaciones de usuario. Debido a la posibilidad de inconsistencias con respecto a la separación estática de las relaciones de derecho y relaciones de herencia, el componente de relaciones SSD define las relaciones tanto en presencia como en ausencia de jerarquías de roles (ANSI INCITS, 2004).

El cuarto componente del modelo, Dynamic Separation of Duty Relations, define las relaciones de exclusividad con respecto a las funciones que se activan como parte de una sesión de usuario (ANSI INCITS, 2004).

No es parte del alcance de este trabajo hacer un análisis profundo de cada componente, sin embargo, se detallará el modelo Core RBAC para establecer una base de conocimiento.

2.4.4 CORE RBAC

Core RBAC incluye cinco elementos básicos de datos llamados usuarios (USERS), roles (ROLES), objetos (OBS), operaciones (OPS) y permisos (PRM) (ANSI INCITS, 2004).

El modelo RBAC en su conjunto se define fundamentalmente en términos de usuarios individuales que están siendo asignados a los roles y permisos asignados a los roles. Como tal, un rol es un medio para asignar una relación N a N entre los usuarios y los permisos individuales. Además, el modelo Core RBAC incluye un conjunto de sesiones (SESSIONS) donde cada sesión es una asignación entre un usuario y un subconjunto activado de roles que están asignados al usuario (ANSI INCITS, 2004).

El propósito de cualquier mecanismo de control de accesos es proteger los recursos del sistema. Consistente con los modelos preexistentes de control de accesos, un objeto es una entidad que contiene o recibe información. Para un sistema que implementa

RBAC, los objetos pueden representar contenedores de información o recursos del sistema no renovables. El conjunto de objetos cubiertos por RBAC incluye todos los objetos enumerados en los permisos que se asignan a los roles (ANSI INCITS, 2004).

Para RBAC es central el concepto de las relaciones de rol, alrededor de la cual un rol es una construcción semántica para la formulación de políticas. La Figura 2-1 ilustra la asignación de usuario (UA) y las relaciones de asignación de permisos (PA). Las flechas indican una relación de N a N. Esta disposición proporciona una gran flexibilidad y granularidad de asignación de permisos a roles y usuarios a los roles. Sin esto existe un peligro mayor, un usuario puede obtener un mayor acceso a los recursos de los necesarios debido a un control limitado sobre el tipo de acceso que se puede asociar con los usuarios y los recursos. Cualquier aumento en la flexibilidad para controlar el acceso a los recursos también fortalece la aplicación del principio de mínimos privilegios.

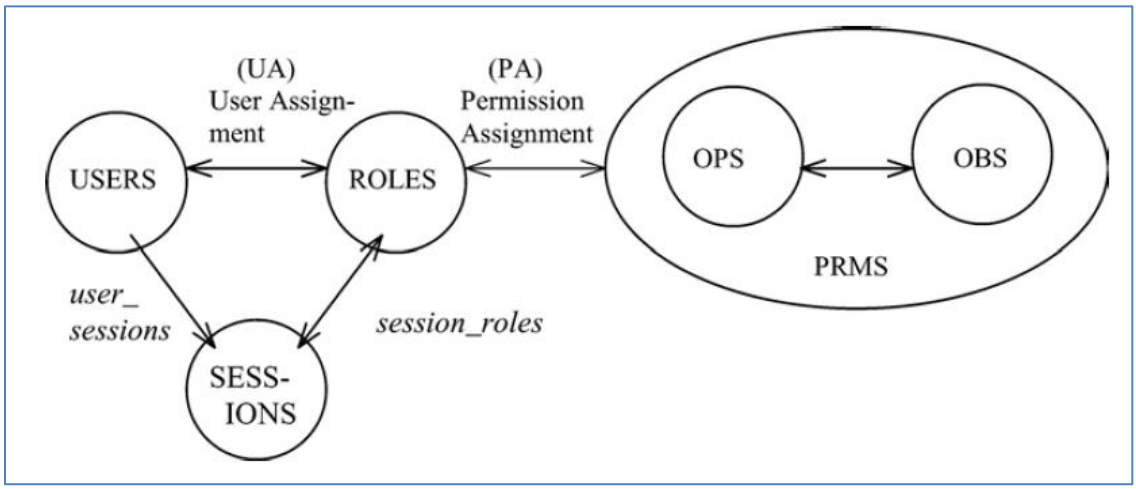

FIGURA 2-1 CORE RBAC

FUENTE: ANSI INCITS, 2004

Cada sesión es una asignación de un usuario a posiblemente muchos roles, es decir, un usuario establece una sesión durante la cual el usuario activa un subconjunto de los roles que tiene asignados. Cada sesión está asociada con un único usuario y cada

usuario está asociado con una o más sesiones. La función session_roles nos da los roles activados por la sesión y la función session_users nos da al usuario que está asociado con una sesión. Los permisos disponibles para el usuario son los permisos asignados a los roles que están actualmente activos en todas las sesiones del usuario.

Formalmente las especificaciones de Core RBAC son:

- *USERS, ROLES, OPS,* and *OBS* (users, roles, operations and objects respectively).
- $UA \subseteq USERS \times ROLES$, a many-to-many mapping user-to-role assignment relation.
- *assigned_users*: $(r{:}ROLES) \rightarrow 2^{USERS}$, the mapping of role r onto a set of users.
  Formally: $assigned\_users(r) = \{u \in USERS \mid (u, r) \in UA\}$
- $PRMS = 2^{(OPS \times OBS)}$, the set of permissions.
- $PA \subseteq PERMS \times ROLES$, a many-to-many mapping permission-to-role assignment relation.
- *assigned_permissions*(r: *ROLES*) $\rightarrow 2^{PRMS}$, the mapping of role r onto a set of permissions. Formally:
  $assigned\_permissions(r) = \{p \in PRMS \mid (p, r) \in PA\}$
- *Op*(p: *PRMS*) $\rightarrow$ {op$\subseteq$OPS}, the permission to operation mapping, which gives the set of operations associated with permission p.
- *Ob*(p: *PRMS*) $\rightarrow$ {ob$\subseteq$OBS}, the permission to object mapping, which gives the set of objects associated with permission p.
- *SESSIONS* = the set of sessions
- *session_users* (s: *SESSIONS*) $\rightarrow$ *USERS*, the mapping of session s onto the corresponding user.
- *session_roles* (s: *SESSIONS*) $\rightarrow 2^{ROLES}$, the mapping of session s onto a set of roles.
  Formally: $session\_roles(s_i) \subseteq \{r \in ROLES \mid (session\_users(s_i), r) \in UA\}$
- *avail_session_perms*(s:*SESSIONS*) $\rightarrow 2^{PRMS}$, the permissions available to a user in a session = $\bigcup_{r \in session\_roles(s)} assigned\_permissions(r)$

2.5 FRAMEWORK IAM

Identity and Access Management es un término complejo que significa diferentes cosas para diferentes personas. Con frecuencia, los profesionales de TI han tendido a encasillar su significado en ciertos problemas relacionados a la seguridad de las identidades virtuales. Por ejemplo, se ha percibido como un sinónimo SSO, Metadirectorio, RBAC y otras ideas similares (Chong, 2004).

En el ámbito de las empresas, las tecnologías de la información y la seguridad informática tomaremos como definición la siguiente:

> "Identity and access management refers to the processes, technologies and policies for managing digital identities and controlling how identities can be used to access resources" (Chong, 2004)

En concordancia podemos mencionar a otros autores que lo definen como:

> "Identity and access management is the security discipline that enables the right individuals to access the right resources at the right times for the right reasons. IAM addresses the mission-critical need to ensure appropriate access to resources across increasingly heterogeneous technology environments, and to meet increasingly rigorous compliance requirements. This security practice is a crucial undertaking for any enterprise. It is increasingly business-aligned, and it requires business skills, not just technical expertise. Enterprises that develop mature IAM capabilities can reduce their identity management costs and, more importantly, become significantly more agile in supporting new business initiatives" (Wagner, 2010)

> "The notion of identity and access management encompasses a broad range of techniques, technologies and processes that support the use of real world properties of real world entities as digital identifiers in computer networks and applications" (Pato, 2005)

> "Identity management is not a single product but a set of processes and supporting technologies for maintaining a person's complete set of identity information, spanning multiple business and application contexts. Identity management unifies a person's disparate identity data to improve data consistency, data accuracy, and data and systems security in an efficient manner" (Forrester, 2011)

> "The policies, processes, and technologies that digital businesses employ to establish identities and control access to their resources across dynamic ecosystems of value." (Forrester, 2015)

De lo anterior se puede concluir que:

- IAM se trata de la gestión de la vida de extremo a extremo de las identidades digitales. Una solución de gestión de identidades de clase empresarial no debe estar compuesta por silos aislados de tecnologías de seguridad, sino más bien, consiste en un conjunto bien integrado de tecnologías que tratan el espectro de escenarios en cada etapa del ciclo de vida de la identidad (Chong, 2004).
- IAM no es sólo tecnología, sino más bien, se compone de tres elementos indispensables: políticas, procesos y tecnologías. Políticas se refieren a las restricciones y normas que hay que seguir con el fin para cumplir con las regulaciones y mejores prácticas de negocio, procesos describen las secuencias de pasos que conducen a la realización de tareas de trabajo o eventos y tecnologías son las herramientas automatizadas que ayudan a lograr objetivos

de negocio más eficiente y precisa al mismo tiempo las limitaciones y directrices que se especifican en las políticas (Chong, 2004).

- La analogía de un triángulo es perfecta para describir las relaciones e interacciones de las políticas, procesos y tecnologías en un sistema sano de gestión de identidades y accesos. Cada organización es diferente y la combinación adecuada de tecnologías, políticas y procesos de una empresa pueden no ser necesariamente el equilibrio adecuado para todas las empresas. Por lo tanto, cada organización tiene que encontrar su propio equilibrio representado por la singularidad de su triángulo (Chong, 2004).
- El sistema IAM de una organización no permanece estático en el tiempo. Las nuevas tecnologías adoptadas, nuevos modelos de negocio y las limitaciones cambiarán el gobierno corporativo y procesos en forma constante. Como mencionamos antes, cuando uno de los elementos cambia, es el momento de buscar un nuevo equilibrio. Es por lo tanto importante entenderlo como un viaje y no un destino (Chong, 2004).

2.5.1 COMPONENTES PRINCIPALES

IAM es un framework que facilita la gestión de identidades virtuales. Incluye la tecnología necesaria para apoyar la gestión del ciclo de vida completo identidad con un enfoque automatizado. Esto asegura que los accesos de privilegios se conceden de acuerdo con la política corporativa y que todos los individuos y los servicios están adecuadamente autenticados, autorizados y auditados (Al-Khouri, 2011).

En este framework, destacan tres componentes claves (Chong, 2004):

- Directory services.
- Access Management.
- La gestión del ciclo de vida de identidad.

El primer componente es “Directory Services”, como se mencionó anteriormente una identidad digital consiste en un conjunto de tipos lógicos de datos, identificador, las credenciales y los atributos. Estos datos necesitan ser almacenados y organizados de forma segura. Los servicios de directorio proporcionan la infraestructura para satisfacer esas necesidades. Los derechos y las políticas de seguridad a menudo controlan el acceso y uso de las aplicaciones de negocio y la infraestructura informática dentro de una organización (Chong, 2004).

Es segundo componente es “Access Management”, que se refiere al proceso de control y la concesión de accesos para satisfacer las solicitudes de recursos. Este proceso normalmente se efectuará a través de una secuencia de acciones de autenticación, autorización y auditoría (Chong, 2004).

Finalmente, el tercer componente es la gestión del ciclo de vida de la identidad. Cada etapa de este ciclo tiene escenarios que son candidatos para aplicar una gestión automatizada. Por ejemplo, durante la creación de una identidad digital, los datos necesitan ser propagado e inicializados en diferentes sistemas. Todos los eventos deben tener una gestión eficaz, segura y precisa, que es exactamente lo que la gestión del ciclo de vida de identidad se trata (Chong, 2004).

Uno de los principales desafíos para la gestión de datos entre los diferentes sistemas de una organización es la falta de integración. La visión completa de los atributos, las credenciales y privilegios de un usuario determinado a menudo están distribuidos a en múltiples sistemas (Chong, 2004).

2.5.2 TECNOLOGÍAS ASOCIADAS

Forrester ha identificado cuatro conjuntos de tecnologías, que además pueden asociarse entre sí, y que son necesarias para implementar de forma completa un ecosistema IAM:

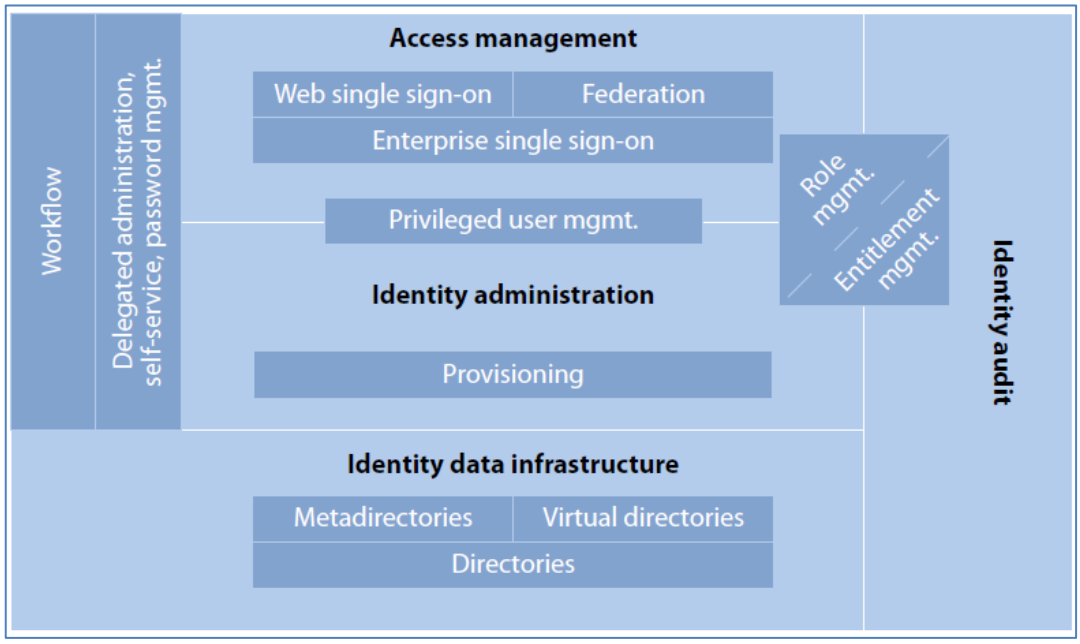

FIGURA 2-2 TECNOLOGÍAS DE IAM

FUENTE: FORRESTER, 2011

Forrester además precisa que es necesario (Forrester, 2011):

- Establecer una infraestructura de datos de identidad. Este segmento abarca productos que forman la capa de información de la identidad como directorios, metadirectorios y directorios virtuales.
- Administrar cuentas y privilegios. Son productos que gestionan las cuentas de los usuarios, atributos, y credenciales incluyen el aprovisionamiento, gestión de contraseñas y usuarios privilegiados. Esta categoría también incluye los elementos funcionales de autoservicio, administración delegada y el paradigma de gestión de accesos basado en roles.
- Controlar el acceso a los recursos de TI. Este es el dominio de productos como enterprise single-sign-on, web-single-sesion y federación.
- Auditoría de las actividades administrativas y de acceso. Las organizaciones requieren la capacidad de demostrar que cuentan con los controles

administrativos y de acceso se están realizando de acuerdo a la política de seguridad. Productos de auditoría de identidad ayudan con este esfuerzo. Esto incluye herramientas de auditoría que combinan y correlacionar actividades y eventos a través de la infraestructura de identidad, así como herramientas de recertificación. También incluye productos de gestión de roles.

2.5.3 SINGLE SIGN ON

Un usuario típico de la empresa tiene que iniciar sesión varias veces con el fin de tener acceso a las diversas aplicaciones de negocio que utilizan para cumplir con sus responsabilidades. Desde el punto de vista del usuario, varios inicios de sesión y la necesidad de recordar múltiples contraseñas representan pérdida de productividad y una pobre experiencia de uso (Chong, 2004).

Desde el punto de vista de gestión, los incidentes de olvido contraseñas definitivamente aumentan los costos de administración de sistemas, y combinado con malos hábitos de gestión de passwords tales como escribir contraseñas papel, incrementan las posibilidades de brechas de seguridad (Chong, 2004).

Es a partir de estos problemas que surge el concepto de inicio de sesión único o single sign on. La capacidad para iniciar la sesión una vez y acceder a varios sistemas, se ha convertido en uno de los principales drivers de proyectos de gestión de identidad (Chong, 2004).

En términos generales, existen cinco clases de soluciones de SSO. El tipo más adecuado para cada aplicación depende de varios factores como las limitaciones impuestas por la infraestructura y la capacidad de modificar las aplicaciones. (Chong, 2004).

1. Web SSO.
2. Operating System Integrated Sign-On.

3. Federated Sign-On.
4. Identity and Credential Mapping.
5. Password Synchronization.

Las soluciones de SSO web están diseñadas para hacer frente a requerimientos de aplicaciones web. En estas soluciones, los usuarios no autenticados son redirigidos en el browser a un sitio web para iniciar sesión con sus respectivas identificaciones de usuario y credenciales. Sobre una autenticación exitosa, cookies u otros métodos son utilizados por las aplicaciones web para validar sesiones del usuario autenticado (Chong, 2004).

Operating System Integrated Sign-On se refiere a módulos de autenticación e interfaces integradas en el sistema operativo. El subsistema de seguridad proporciona tal capacidad a través de módulos específicos e interfaces estandarizadas. Distintas aplicaciones pueden utilizar estas interfaces para autenticar sus usuarios (Chong, 2004).

Federated Sign-On requiere que la infraestructura de autenticación de las aplicaciones sea compatible con relaciones de confianza e operen a través de protocolos estándares. Federated Sign-On significa que la responsabilidad de autenticación se delega a un componente de la infraestructura de autenticación de confianza (Chong, 2004).

Identity and Credential Mapping son tecnologías que utilizan caches para realizar un seguimiento de las identidades y credenciales para utilizarlas cuando correspondan. La memoria caché se puede actualizar de forma manual o automáticamente cuando una credencial cambia. Cuando una aplicación no puede ser modificada para integrarse a este modelo, un agente de software puede ser instalado para controlar los eventos de inicio de sesión de la aplicación. Cuando el agente detecta este tipo de eventos, obtiene la información del cache y la ingresa de forma automática en el login de la aplicación (Chong, 2004).

La técnica de sincronización de contraseñas o Password Synchronization se utiliza para sincronizar las contraseñas directamente en las bases de datos de aplicaciones, de forma que los usuarios y las aplicaciones no tengan que gestionar múltiples cambios de contraseñas. La sincronización de contraseñas por sí sola no proporciona inicio de sesión único, sin embargo aporta grandes ventajas a la gestión de contraseñas y facilidad de uso (Chong, 2004).

2.5.4 ENTITLEMENT MANAGEMENT

Entitlement Management es un concepto que se refiere al conjunto de tecnologías utilizadas para conceder y revocar los derechos y privilegios de acceso a identidades. Está estrechamente relacionado con la autorización, que es el proceso real de hacer cumplir las reglas de acceso, políticas y las restricciones que están asociados con las funciones de negocio y datos (Chong, 2004).

Las aplicaciones empresariales de hoy en día utilizan con frecuencia autorización basada en roles funcionales y automatización de flujos de trabajo o workflows para lograr mayor eficiencia y seguridad (Chong, 2004).

También es importante para la mayoría de las organizaciones tener una visión consolidada de todos los derechos que una determinada identidad posee. Para cumplir con este requisito, los sistemas de gestión de accesos suelen aprovechar metadirectorios centralizados para centralizar su información (Chong, 2004).

2.5.5 IDENTITY AGREGATION

Con frecuencia, la empresa tendrá no sólo un sistema con identidades, sino varios, cada uno sirviendo diferentes funciones de negocios pero almacenando datos duplicados y relacionados. Las aplicaciones que necesitan para integrarse con esas funciones de negocio se ven obligadas a conciliar las diferencias.

Mover los datos de identidades a un gran sistema de gestión de identidades podría parecer una respuesta obvia a este problema. Sin embargo, hay muchos factores como problemas técnicos, de compatibilidad, del negocio y otros que evitan que dicha solución sea adoptada ampliamente en el corto plazo. A esto se lo denomina Identity Aggregation:

> "Identity aggregation therefore refers to the set of technologies that help applications aggregate identity information from different identity systems, while reducing the complexity of data reconciliation, synchronization and integration." (Chong, 2004)

Hay varios desafíos técnicos que las tecnologías de agregación de identidad debe contribuir a subsanar: (Chong, 2004)

- El mantenimiento de las relaciones de transformaciones de datos. Esto puede proporcionar varios beneficios a las aplicaciones que deben manipular los datos en diferentes sistemas. La primera ventaja consiste en proporcionar aplicaciones con una vista consolidada o una vista agregada de los datos en los sistemas individuales. Para esto se requiere mantener metadatos que describen el esquema en representación de la vista consolidada y su relación con el esquema de datos en los diferentes sistemas.
- La optimización de las operaciones CRUD (Create, Read, Update and Delete): CRUD es un acrónimo que significa Crear, Leer, Actualizar y Borrar. Es decir, define las operaciones primitivas básicas para la manipulación de datos. La razón por la que se planteó como un reto técnico es debido a que implica operaciones de múltiples sistemas cuyos rendimientos que pueden variar significativamente dependiendo de las relaciones de datos.
- Sincronización de datos. Por lo general esto es necesario cuando existen atributos de identidad duplicados en varias bases de datos distintas y/o los datos se replican a un almacén intermedio de identidades. Sin embargo, el uso de la

sincronización de datos también puede introducir otros problemas de diseño que requieren de resolución de conflictos de datos.

2.5.6 AUDITORÍA

Auditoría en el contexto de IAM, se trata de llevar el registro de "quién hizo qué, y cuándo" dentro de la infraestructura de TI. Las regulaciones federales como la Ley Sarbanes-Oxley son factores clave para los requisitos de auditoría relacionados con la identidad (Chong, 2004).

Un proceso de auditoría típico consta de las siguientes fases (Chong, 2004):

1. Planificación y ejecución de la auditoría.
2. Recolectar y almacenar los datos.
3. Análisis y retroalimentación.

Las pistas de auditoría pueden ser generadas por diferentes componentes de infraestructura y/o aplicaciones para diferentes propósitos. Estos datos deben ser recogidos y almacenados.

Luego los datos pueden ser procesados y analizados de forma automática o manualmente. El análisis de auditoría debe ser diseñado para llevar a conclusiones sobre las acciones correctivas necesarias, si las hay, para mejorar los sistemas de TI y procesos.

Existen varias consideraciones que son importantes para el diseño de sistemas de auditoría (Chong, 2004):

- Localidad de generación y almacenamiento de auditoría.
- La separación de la función del auditor.
- Flujo de eventos auditados.

Una vez que se genera un registro de auditoría, hay dos modelos principales a tener en cuenta para su almacenamiento: distribuido y centralizado. En el modelo distribuido, los datos de auditoría se mantienen típicamente en el sistema en el que los datos se generaron. Con el enfoque centralizado, los datos se envían a un centro de almacenamiento de datos central (Chong, 2004).

La separación de funciones es una práctica común para ayudar a minimizar la ocurrencia de actividades ilegales como consecuencia de actos que podría eludir los controles de rendición de cuentas. En el campo de la auditoría de TI, es una práctica común separar la función de administrador del sistema desde el rol del auditor. Esto impide que el administrador del sistema pueda encubrir pistas de auditoría de actividades no autorizadas.

Además, también se espera que las infraestructuras de auditoría sean (Chong, 2004):

- Eficiente
- Disponible
- Precisa
- De no repudio

2.5.7 FEDERACIÓN

Federación es un movimiento dominante en lo referido a gestión de identidades en la actualidad. Se refiere al establecimiento de acuerdos comerciales, confianza criptográfica y los identificadores de usuario o atributos a través de dominios de seguridad y de política para permitir interacciones comerciales entre dominios en forma transparente (OASIS, 2005).

Federación ofrece una forma de SSO, sin embargo es más que sólo eso. Implica la delegación de responsabilidades a través de relaciones de confianza entre las partes

federadas. La autenticación es sólo una forma de responsabilidad delegada (Chong, 2004).

Otras definiciones son:

> "Identity for use in multiple domains, which together form an identity federation" (ISO/IEC, 2011)
>
> "Agreement between two or more domains specifying how identity information will be exchanged and managed for cross-domain identification purposes" (ISO/IEC, 2011)

Hay tres elementos de tecnología que son cruciales para el concepto de federación (Chong, 2004):

- Un protocolo de federación que permite a las partes para comunicarse.
- Una infraestructura de confianza flexible que soporta una variedad de modelos de confianza.
- Un marco extensible que soporta la gestión de la política de los requisitos de gobierno diferentes.

Los protocolos de federación son los "lenguajes" que son utilizados por las partes federadas para comunicarse entre sí. Ya que federación implica que la responsabilidad se delega, el protocolo debe permitir los individuos obtener la capacidad de probar que una determinada identidad ha completado con éxito una acción o tiene derecho a una colección de privilegios sin esto ser errores ni manipulación (Chong, 2004).

Existen diferentes modelos de federación que pueden ser aplicados, de acuerdo a las necesidades de la empresa, las tecnologías involucradas, la infraestructura, etc. Los modelos más comunes son (Chong, 2004):

- Hub-and-spoke.
- Hierarchical.

- Peer-to-peer Web of Trust.

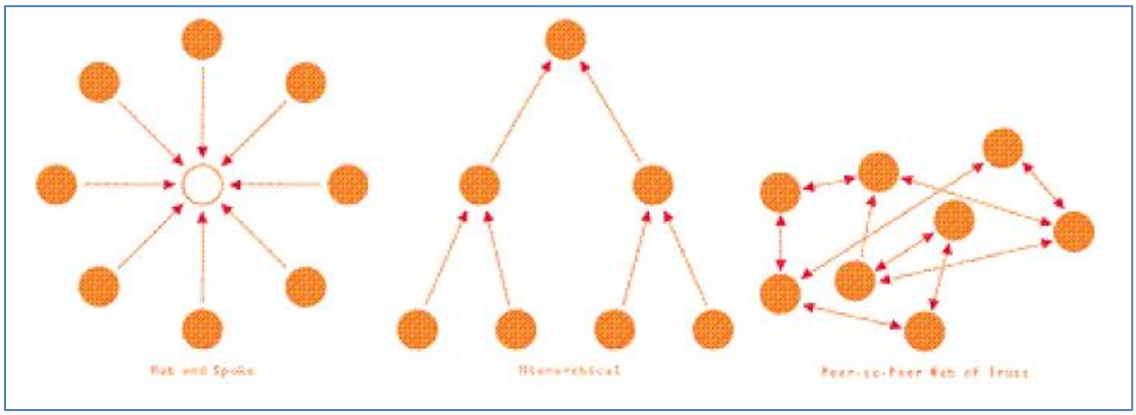

FIGURA 2-3 MODELOS DE FEDERACIÓN

FUENTE: CHONG, 2004

El modelo hub-and-spoke es el más sencillo de entender. En este modelo, hay una entidad central que es de confianza de las partes federadas.

En el modelo jerárquico, ambas partes tienen una relación de confianza indirecta en caso de que ambos tengan una ruta de confianza en sus respectivas ramas en el árbol jerárquico a una autoridad raíz común.

El modelo peer-to-peer representa un conjunto de relaciones de confianza directa ad-hoc.

Federación integra la capa de gestión de identidades de distintos dominios y para esto es clave disponer de mecanismos y formatos de comunicación estandarizados entre ellos. Un estándar ampliamente difundido es Security Assertion Markup Language o SAML (OASIS, 2005).

SAML, desarrollado por el Comité Técnico de Organization for the Advancement of Structured Information Standards (OASIS), es un marco basado en XML para la comunicación de autenticación de usuarios, entitlement y la información de atributos.

Como su nombre indica, SAML permite a las entidades de negocio hacer afirmaciones sobre la identidad, atributos y derechos de un sujeto a otras entidades (OASIS, 2005).

Algunas ventajas de este estándar son: (OASIS, 2005)

- Neutralidad frente a plataformas y tecnologías.
- Acoplamiento flexible de directorios.
- Una experiencia mejorada para usuarios finales, permitiendo SSO.

SAML se define en términos de assertions, protocol bindings, and profiles (OASIS, 2005).

Una assertion es un paquete de información que suministra una o más declaraciones hechas por una autoridad SAML. SAML define tres tipos diferentes de declaración de afirmación: (OASIS, 2005)

- Autenticación: La identidad que figura fue autenticada por un medio particular en un momento particular. Este tipo de assertion se genera típicamente por una autoridad SAML denominada proveedor de identidad, que está a cargo de la autenticación de usuarios y hacer el seguimiento de otra información sobre ellos.
- Atributo: El sujeto específico está asociado con los atributos suministrados.
- Decisión de Autorización: Una petición para permitir o denegar que un sujeto específico pueda acceder al recurso especificado.

SAML define una serie de protocolos de petición/respuesta que permiten a los proveedores de servicios diferentes operaciones como solicitar de una autoridad SAML una o más assertions (OASIS, 2005).

El intercambio de mensajes SAML de petición-respuesta se denomina SAML protocol bindings. Por ejemplo, SAML SOAP binding define cómo los mensajes de protocolo SAML pueden ser comunicadas dentro de los mensajes SOAP (OASIS, 2005).

Un profile de SAML define las restricciones y/o extensiones en soporte del uso de SAML para una aplicación en particular, con el objetivo de mejorar la interoperabilidad mediante la eliminación de parte de la flexibilidad inevitable en un estándar de uso general (OASIS, 2005).

Este estándar tiene múltiples aplicaciones como Attribute-Based Authorization, al igual que en el escenario SSO Web, este modelo de autorización tiene un sitio web que comunica la información de una identidad a otro sitio web en apoyo de alguna transacción. Sin embargo, la información de identidad puede ser alguna característica en lugar de, o además de, la información acerca de cuándo y cómo se ha autenticado la persona. El modelo de autorización basada en atributos es importante cuando identidad particular del individuo es o no es importante, no debe ser compartida por razones de privacidad, o es insuficiente por sí solo (OASIS, 2005).

2.6 DRIVERS

IAM ha convertido en una herramienta no sólo para la seguridad, sino también la agilidad del negocio. A medida que las empresas explotan las tecnologías digitales tanto para crear nuevas fuentes de valor para los clientes y aumentar su agilidad operativa, los procesos de negocio vitales invariablemente atraviesan diferentes grupos de usuarios y dispositivos (Forrester, 2015).

En una encuesta realizada por KPMG en 2008, se encontró que las principales razones para implementar soluciones IAM estaban relacionados con la agilidad del negocio, la contención de costes, eficiencia operativa, gestión de riesgos de TI y el cumplimiento normativo (KPMG, 2008). Sirven como un factor diferenciador al ofrecer a clientes internos y externos una mejor y más segura experiencia. También agregan valor volviendo más simples y robustos los procesos organizacionales (McQuaide, 2003).

Los cinco principales drivers comerciales para la implementación de los componentes de una solución IAM son (Witty, 2003):

- Facilitar los negocios.
- Reducción de costos.
- Eficiencia operacional.
- La gestión de riesgos de TI.
- Cumplimiento regulatorio.

Algunos drivers son más aplicables a uno de los componentes de la solución de IAM que otros. La reducción de costos y la gestión de riesgos de TI son las razones principales para la mayoría de las implementaciones de IAM para usuarios internos.

Mientras que la facilitación de negocios es el principal impulsor para las implementaciones que se ocupan del control de acceso de usuarios externos.

Debido a que todos los componentes de IAM ayudan con el cumplimiento normativo, la mayoría de las empresas aplican este driver de negocio como un motivador de apoyo para la implementación de un programa de seguridad de la información (Witty, 2003).

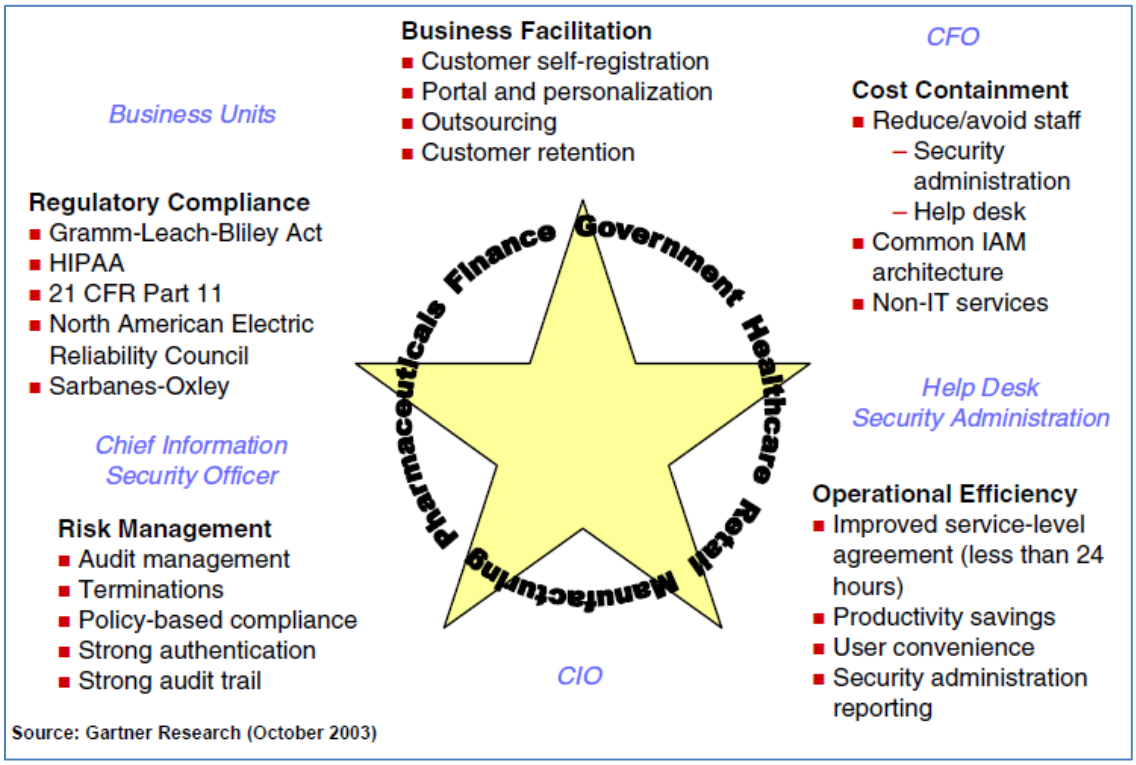

FIGURA 2-4 DRIVERS IAM

FUENTE: WITTY, 2003

2.6.1 FACILITACIÓN DE NEGOCIOS

Para proporcionar un acceso más rápido a la información empresarial, más simple para los clientes, socios comerciales y empleados, también se debe proporcionar la

infraestructura de seguridad apropiada para ese entorno. Las razones para implementar una solución IAM de facilitación de negocios incluyen:

Registro automático de clientes, cuando el número de clientes llega a cientos de miles, las empresas no pueden manejar las necesidades de gestión de seguridad de todos los usuarios a través de medidas manuales. Deben automatizar o no serán capaces de prestar sus servicios de forma adecuada. Con la automatización, las empresas delegan los costos administrativos a departamentos o clientes usuarios finales. (Witty, 2003)

Portal y personalización de Aplicaciones, los servicios empresariales se están entregando a través de portales que proporcionan una interfaz de acceso común, así como para ofrecer servicios personalizados para el usuario final. Estos portales deben autenticar y autorizar a los usuarios. La entrega de servicios personalizados puede aprovechar el repositorio de información que también se utiliza para la autenticación y autorización. (Witty, 2003)

Outsourcing, cuando las empresas externalizan sus operaciones de TI, el proveedor de servicios a menudo asume la responsabilidad de la administración de seguridad para sus clientes. Para que este modelo sea rentable y eficiente para ambas partes, a menudo se usan productos de aprovisionamiento automático de usuarios para proporcionar esta función. (Witty, 2003)

Retención de clientes, los clientes demandan. Si la empresa no hace que sea fácil para ellos usar su servicio, buscaran otros competidores que si lo hagan. El costo de la obtención de un nuevo cliente es alto, el costo de retener un cliente puede ser aún mayor. Funcionalidades como el restablecimiento de contraseñas de autoservicio y funcionalidad de inicio de sesión único pueden ser de valor en este aspecto (Witty, 2003).

2.6.2 REDUCCIÓN DE COSTOS

Los niveles actuales de personal de mesa de ayuda y control de accesos no pueden adaptarse a las necesidades crecientes de las empresas para las actividades de administración de seguridad del día a día. Las empresas requieren medidas de reducción de costos y las soluciones IAM son una de las pocas dentro del programa de seguridad de la información que además pueden proporcionar un ahorro directo (Witty, 2003).

Reducir o evitar la adición de personal, en una empresa típica, el personal de help desk, administradores de sistemas y los administradores de seguridad manejan las solicitudes de acceso de usuarios. La adición de un sistema o aplicación en el entorno de TI a menudo significa que alguien sea capacitado en la nueva tecnología, o la adquisición de talento adicional para manejarlo desde una perspectiva de administración de la seguridad. Es posible reducir estos costos mediante el uso de la gestión de contraseñas, aprovisionamiento de usuarios y otras funcionalidades de IAM (Witty, 2003).

Arquitectura IAM común, mediante el establecimiento de una arquitectura común se puede eliminar los costos asociados con el diseño y desarrollo de aplicaciones, reducir o eliminar el hardware y el software que está apoyando las actividades de administración de accesos específica de la plataforma y la facilidad de integración de aplicaciones, proporcionando una infraestructura de autenticación y autorización común. Directorios, administración de contraseñas, aprovisionamiento de usuarios y productos de Access Management son la columna vertebral de una arquitectura IAM (Witty, 2003).

Servicios no TI, servicios como el aprovisionamiento automático de accesos y workflows impacta en una mejor gestión de activos físicos como smartphones, laptops entre otros. Esto genera beneficios en forma indirecta para la organización (Witty, 2003).

2.6.3 EFICIENCIA OPERACIONAL

Las empresas necesitan procesos eficientes de gestión de accesos. La gestión de contraseñas, aprovisionamiento de usuarios, SSO y otras funcionalidades IAM cumplen con este driver (Witty, 2003).

Acuerdos de nivel de servicio mejorados, lograr tiempos de respuesta de solicitudes de accesos que sean acordes a la dinámica actual de las empresas, sólo pueden lograrse a través de la automatización. Con un promedio de 18 cuentas de usuario por colaborador, la creación de las mismas, incluyendo las aprobaciones, no es factible de forma manual (Witty, 2003).

Ahorros de productividad, la automatización de los procesos de IAM da como resultado ahorro de tiempo en muchas áreas (Witty, 2003):

- Los empleados y contratistas que producen ingresos tienen acceso a los recursos necesarios y pueden empezar a trabajar sin demoras.
- La reducción de los plazos para la aprobación de las solicitudes de acceso significa menos tiempo dedicado por los mandos medios y superiores de estas aprobaciones.
- Permitir que los usuarios cambien sus contraseñas no sólo elimina el costo de solicitudes, sino que también reduce el tiempo dedicado por los usuarios a cambiar la contraseña.

La comodidad del usuario, la gestión de contraseñas y productos de SSO empoderan a los usuarios lo cual repercute en una mejor experiencia de trabajo. Ellos son componentes críticos para asegurar la retención de clientes (Witty, 2003).

Administración de informes de Seguridad, las empresas deben producir informes para fines de administración de seguridad del día a día. La obtención de esta

información de una instalación centralizada aumenta la eficiencia operativa (Witty, 2003).

2.6.4 GESTIÓN DE RIESGOS DE TI

La capacidad de probar la seguridad de la infraestructura de control de acceso es un requisito importante para las actividades de administración de seguridad y auditoría. Además, la capacidad de implementar y mantener los requisitos reglamentarios es imprescindible para ciertas industrias. Todos los componentes de la solución IAM, ayudan en su aseguramiento (Witty, 2003).

Gestión de Auditoría, responder a las auditorías de manera oportuna ahorra dinero a los auditores, administradores de sistemas, administradores de seguridad y los administradores (Witty, 2003).

Desvinculaciones, desactivar el acceso de los usuarios desvinculados inmediatamente repercute en una reducción de la exposición para las empresas (Witty, 2003).

El cumplimiento basado en directivas, aplicar y mantener políticas de IAM, como las políticas de formación de la contraseña, funciones y privilegios automáticamente, son de gran beneficio para las empresas y reduce costos de gestión (Witty, 2003).

Autenticación robusta, para las industrias como los servicios financieros y cuidado de la salud, proporcionando un mecanismo de autenticación robusta que no sea el ID de usuario y la contraseña es un requisito basado en la confidencialidad y la sensibilidad de la información que se tiene acceso (Witty, 2003).

Pista de auditoría robusta, el no repudio y la integridad de las pistas de auditoria son requisitos en muchas industrias que son suplidos con estas soluciones (Witty, 2003).

2.6.5 CUMPLIMIENTO REGULATORIO

El reglamento de los servicios financieros, salud y otras industrias requieren el establecimiento de una infraestructura de control de acceso seguro. Leyes como Sarbanes-Oxley o PCI-DSS pueden requieren de una correcta gestión de accesos que puede lograrse a través de soluciones IAM (Witty, 2003).

2.7 ESTRATEGIA DE IMPLEMENTACIÓN

Existen muchos enfoques posibles a la hora de implementar un sistema IAM, Gartner propone tomar en cuenta los siguientes factores para comprobar si la empresa esta lista (Wagner, 2010):

- Capacidades IAM actuales. Una comprensión clara de las capacidades existentes IAM hará que sea posible identificar las áreas de tecnología de IAM que requieren mejoras funcionales.
- Procesos y tecnologías necesarias. La evaluación de las mejoras necesarias para abordar brechas identificadas permitirán a los profesionales de TI tomar decisiones informadas y priorizadas sobre los procesos y tecnologías necesarias.

Además, propone desarrollar y madurar un programa de IAM en cuatro fases principales (Wagner, 2010):

- Estrategia y plan: Definir las necesidades IAM, basadas en una clara comprensión de los requisitos específicos, el perfil de riesgo de la empresa y de los cambios en curso en los comportamientos individuales. Establecer y comunicar el valor de negocio de IAM. Identificar las tecnologías apropiadas.
- Arquitectura de la solución: Considerar soluciones tecnológicas específicas, teniendo en cuenta factores tales como fortaleza de la autenticación requerida, el costo total de propiedad y la facilidad de implementación y uso. Considerar los cambios del mercado en curso, incluyendo los nuevos modelos de entrega y precios.
- Selección de la solución: Elegir tecnologías para hacer frente a las necesidades identificadas, tomando en cuenta proveedores de productos y de servicios

establecidos, así como nuevos agentes del mercado. Negociar contratos con acuerdos de nivel de servicio adecuado.

- Funcionar y evolucionar: Llevar a cabo una evaluación de la madurez programa de IAM en curso. Considerar la tecnología y cambios en los procesos. Desarrollar y comunicar métricas que informen el valor.

3 ESTUDIO DEL CONTEXTO

3.1 RESUMEN

El presente capítulo describe el contexto a nivel mundial del presente estudio.

En la sección 3.2 se detalla el segmento IGA y un estado de situación de los principales analistas. En la sección 3.3 una vista general del segmento IDDAS. Finalmente, la sección 3.4 identifica las principales tendencias en el mercado.

3.2 MERCADO IGA

3.2.1 DESCRIPCIÓN DEL MERCADO

Identity And Access Management Suites (Forrester, 2016) o IGA denominadas así por Gartner, son soluciones capaces gestionan los ciclos de vida de identidades y accesos a través de múltiples sistemas en un entorno heterogéneo. Para lograr esto, agregan y correlacionan los datos de identidades y accesos dispares que están distribuidos por todo el entorno de TI (Gartner Inc., 2016).

Estos datos agregados sirven de base para las funciones básicas IAM, incluyendo la gestión del ciclo de vida de la identidad, entitlement management, las solicitudes de acceso, orquestación de flujos de trabajo, certificación de accesos, presentación de informes y análisis, así como funciones auxiliares, incluida la función y la gestión de políticas, la gestión de contraseñas, y revisión de cuentas (Gartner Inc., 2016).

Estas soluciones no sólo ayudan a reducir las amenazas de una empresa, también son vitales para reducir el costo de la administración de las identidades y el costo del cumplimiento normativo. Más allá de la seguridad básica y funciones operativas, IGA también puede mejorar las prestaciones de autoservicio como el recupero de contraseñas (Forrester, 2016).

IGA surgió cuando los mercados para la administración de usuarios y aprovisionamiento (UAP) y de gobernabilidad de identidades y accesos (IAG) se fusionaron. Ahora es ampliamente reconocido como un mercado distinto que está en una fase temprana con vendedores maduros y rentables. Las funcionalidades asociadas con las capacidades básicas se entregan en una de manera relativamente consistente por la mayoría de productos en el mercado. La mayor diferenciación entre los productos se encuentra en las capacidades de auxiliares (Gartner Inc., 2016).

En 2015, se estimó el tamaño del mercado de IGA en $ 1,78 mil millones, con una tasa anual de crecimiento del 19% desde 2014 hasta 2015 ($ 1.50 mil millones a $ 1,78 mil millones) (Gartner Inc., 2016).

Gartner en sus reconocidos Magic Quadrant identifica y clasifica las principales soluciones disponibles. Para el informe de 2016, Gartner clasificó capacidades del producto, experiencia del cliente, conocimiento del mercado y estrategia de producto y la innovación entre los criterios más importantes. SailPoint ha sido nombrado líder en la categoría Gartner's Identity Governance and Administration (IGA) Magic Quadrant (Gartner Inc., 2016).

FIGURA 3-1 IGA MAGIC QUADRANT

FUENTE: GARTNER, 2016

Por su parte Forrester en su prestigioso informe Wave, realiza una evaluación comprensiva, analizando y puntuando 16 criterios de IAM sobre los nueve proveedores más importantes en la categoría. El informe detalla conclusiones acerca de lo bien que cada proveedor cumpla con los criterios y cuál es su posición en relación a los demás (Forrester, 2016).

Sailpoint van a la cabeza, seguida de cerca por RSA y DELL. Estos proveedores mostraron coherencia con sus suites IAM, que abarcan el aprovisionamiento de identidades, certificados, Web SSO y federación. Ofrecen interfaces fáciles de usar, una visión diferenciada, liderazgo y una sólida ejecución (Forrester, 2016).

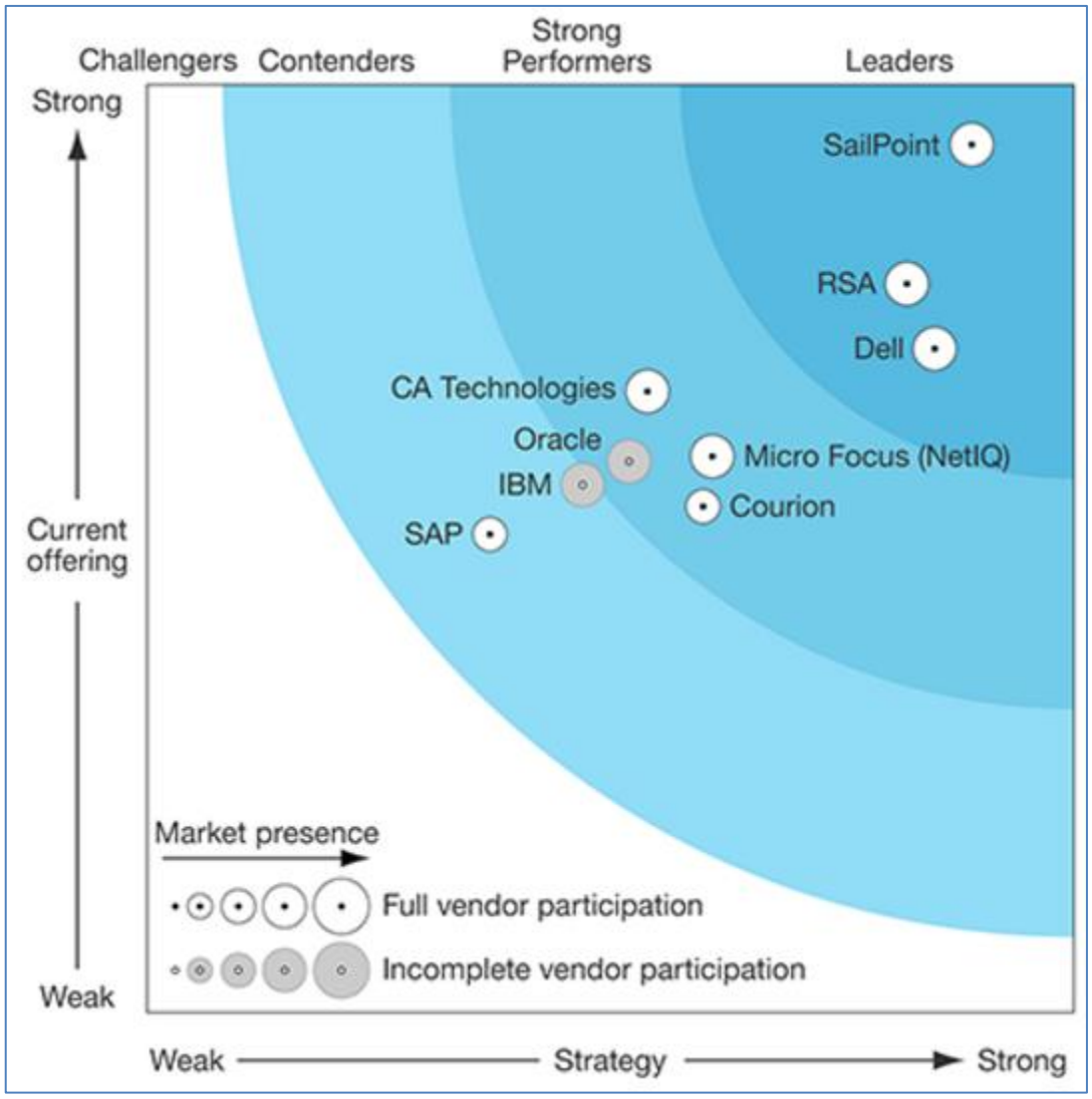

FIGURA 3-2 IDENTITY AND ACCESS MANAGEMENT SUITES WAVE

FUENTE: FORRESTER, 2016

3.2.2 DESCRIPCIÓN DE LOS CUADRANTES Y WAVES

A continuación, se describen los cuadrantes mágicos de Gartner:

- **Leader (líderes)** IGA entregan un amplio conjunto de herramientas para el gobierno y la administración de las identidades y los accesos. Estos proveedores han construido con éxito una base de clientes instalada y una significativa fuente de ingresos, además tiene altos índices de viabilidad y crecimiento. Los líderes también muestran evidencia de una visión y ejecución superior de los requisitos previstos relacionados con la tecnología, metodología o vectores (Gartner Inc., 2016).
- **Challengers (retadores)** IGA entregan un conjunto de herramientas relativamente fuertes de gobierno y de administración de identidades y accesos. Algunos tienen grandes clientes que utilizan su solución. Muestran una sólida ejecución, y la mayoría tienen importantes ventas y presencia de marca. Sin embargo, los retadores no han demostrado las funciones, escala de despliegue o visión de los líderes IGA. Más bien, su visión y ejecución de la tecnología, metodología o medios de suministro tiende a ser más centrado o restringido a las plataformas, zonas geográficas específicas o servicios (Gartner Inc., 2016).
- **Visionaries (visionarios),** los vendedores en este cuadrante proporcionan productos que cumplan muchos requisitos de clientes IGA, pero pueden no tener los medios tales como presupuesto, personal, presencia geográfica, visibilidad, etc. para ejecutar como lo hacen los líderes. Debido al tamaño más pequeño, puede haber una preocupación inicial de algunos compradores potenciales con respecto a la viabilidad a largo plazo. Se destacan por su enfoque innovador de la tecnología, metodología y vectores. A menudo pueden tener características únicas, y pueden estar centrado en una industria específica o un conjunto específico de casos de uso, más que otros. Los visionarios son a menudo los líderes de la tecnología en evolución (Gartner Inc., 2016).

- **Niche Players (jugadores de nicho)** proporcionan la tecnología para casos de uso o metodologías específicas. Se enfocan principalmente en aplicaciones de un proveedor específico, datos o de infraestructura. Los vendedores de este cuadrante tienen a menudo una pequeña base instalada, una inversión limitada en IGA, una huella limitada geográficamente u otros factores que los inhiben a proporcionar un conjunto más amplio de capacidades. La inclusión en este cuadrante, sin embargo, no refleja negativamente en el valor del proveedor, las soluciones de nicho pueden ser muy eficaces en su área de trabajo (Gartner Inc., 2016).

A continuación, se describen las waves de Forrester:

- **Leaders (líderes)** demuestran cobertura integral en sus ofertas de IAM (Forrester, 2016).
- **Strong Performers (participantes fuertes)** de buen rendimiento frente a la mayoría de necesidades (Forrester, 2016).
- **Challengers (retadores)** sus soluciones se especializan en administración de accesos, no disponen de una suite completa que cubra todos los aspectos de IAM (Forrester, 2016).

3.2.3 CRITERIOS DE INCLUSIÓN

Gartner evalúa los siguientes criterios para la inclusión de soluciones (Gartner Inc., 2016):

- Herramientas de apoyo para múltiples ciclos de vida distintos de identidades.
- Capacidades para la gestión de datos maestros relacionados con la identidad y los accesos.
- Capacidades para consumir datos de múltiples sistemas.

- Herramientas para minería y la gestión de privilegios, incluyendo la administración de un catálogo de derechos.
- Funcionalidad para gestionar la relación entre las identidades y los entitlements o privilegios, incluida la capacidad de saber quién tiene acceso a qué, y quién es el responsable de mantener una cuenta o acceso.
- Herramientas para administrar el proceso de solicitud de accesos de extremo a extremo a través de interfaces de usuario amigables para los usuarios.
- Capacidades de flujo de trabajo integrales.
- Herramientas para el descubrimiento e ingeniería de roles.
- Herramientas y capacidades para la gestión de las políticas como las que gobiernan la asignación automática de accesos, la visibilidad, la delegación y el escalamiento de los procesos de aprobación y las dependencias e incompatibilidades entre los derechos de acceso.
- Herramientas que permitan a los actores específicos certificar datos relacionados con la identidad y el acceso.
- Herramientas para conciliar los datos de los sistemas de destino con los datos de IGA para múltiples ambientes técnicos distintos.
- Herramientas y conectores para propagar automáticamente los cambios en los sistemas de destino.
- Herramientas para administrar y sincronizar las contraseñas entre los diferentes sistemas de destino.
- Herramientas de apoyo a la auditoría de datos de identidades, y administración y el cumplimiento SOD.
- Estadísticas e informes de actividades y acciones de identidades y accesos.
- Arquitectura subyacente para la recopilación de datos y acciones de cumplimiento.

- Un total de ingresos de al menos $ 15 millones para productos IGA o suscripciones, Incluido el mantenimiento de los ingresos, durante un período de 12 meses consecutivos (año fiscal).
- Venden y mantienen su propio producto o servicio IGA desarrollados internamente, en lugar de la oferta como una proveedor o distribuidor de terceros.
- Han vendido su producto o servicio IGA a los clientes en diferentes mercados verticales o industrias (es decir, vendedores que sólo venden su producto dentro de una industria en particular o vertical están excluidos)

Por su parte Forrester los siguientes criterios (Forrester, 2016):

- Capacidad completa de Identity Management. Esto incluye la gestión de identidades en repositorios de aplicaciones SaaS y on-premise, minería y gestión de roles, gestión de solicitudes y aprobaciones de accesos y campañas de recertificación y gobierno de accesos.
- Gestión de políticas de seguridad, SSO y federación.

3.2.4 CRITERIOS DE EVALUACIÓN

Gartner evalúa los siguientes criterios:

Capacidad de ejecución. Esto incluye los siguientes criterios (Gartner Inc., 2016):

- Producto como servicio: Bienes y servicios ofrecidos por el proveedor para el mercado. Esto incluye capacidades del producto y servicio actual, la calidad y el conjunto de sus características. Ya sea ofrecido de forma nativa o a través de acuerdos y asociaciones.
- Viabilidad general: Incluye una evaluación general de la organización de su salud financiera, el éxito financiero y práctico de la unidad de negocio, además

la probabilidad de que la unidad de negocio crezca y siga invirtiendo en el producto.

- Ejecución de Ventas/Precio: Capacidades del proveedor en todas las actividades de pre-venta. Esto incluye la gestión de oferta, los precios y la negociación, pre-venta de apoyo, y la eficacia global del canal de ventas.
- Respuesta al mercado: Capacidad de responder, cambiar de dirección, ser flexible y lograr el éxito competitivo frente a los competidores, las necesidades del cliente y la evolución dinámica del mercado. Este criterio también se considera la historia del vendedor.
- Ejecución de marketing: La claridad, calidad, creatividad y la eficacia de los programas diseñados para entregar los mensajes de la organización para influir en el mercado. La promoción de la marca y de negocios, aumentar el conocimiento de los productos y establecer una identificación positiva con el producto, marca y la organización en la mente de los compradores.
- Experiencia del cliente: Relaciones, productos, servicios y programas que permiten a los clientes tener éxito con los productos evaluados. Específicamente, esto incluye la asistencia técnica o soporte de los clientes. Esto también puede incluir herramientas auxiliares, programas de apoyo a los clientes, la disponibilidad de grupos de usuarios, acuerdos de nivel de servicio, entre otros.
- Operaciones: La capacidad de la organización para cumplir sus objetivos y compromisos. Factores incluidos son la calidad de la estructura organizacional, habilidades, experiencias, programas, sistemas y otros vehículos que permiten la organización operar con eficacia y eficiencia de forma continua.

Completitud de la visión. Esto incluye los siguientes criterios: (Gartner Inc., 2016)

- Entendimiento del mercado: Capacidad del proveedor para entender los deseos y necesidades de los compradores y para traducirlos en productos y servicios.

Los vendedores que muestran el más alto grado de visión escuchan y entienden los deseos y necesidades de los compradores.

- Estrategia de marketing: Un claro y diferenciado conjunto diferenciado de mensajes exteriorizado a través de la página web, publicidad, atención al cliente programas y declaraciones de posicionamiento.
- Estrategia de venta: Estrategia para la venta de productos que utilice la red apropiada de ventas directa e indirectas, comercialización, servicios y de la comunicación que amplían el alcance y la profundidad en el mercado, habilidades, conocimientos, tecnologías, los servicios y la base de clientes.
- Estrategia de oferta de productos: El enfoque del proveedor para el desarrollo de productos y la entrega que hace hincapié en la diferenciación, la funcionalidad, la metodología y los conjuntos de características que se asignan a las necesidades actuales y futuras.
- Modelo de negocio: La solidez y la lógica de la propuesta de negocio subyacente del proveedor.
- Estrategia vertical/industria: La estrategia del proveedor para dirigir los recursos, las capacidades para satisfacer las necesidades específicas de los distintos sectores del mercado, incluidos los mercados verticales.
- Innovación: Recursos directos, indirectos, relacionados y su sinergia invertidos en innovación.
- Estrategia geográfica: La estrategia del proveedor para dirigir los recursos, capacidades y ofertas para satisfacer las necesidades específicas de las zonas geográficas, ya sea directamente o a través de socios, canales y filiales.

Por su parte Forrester evalúa a los vendedores contra 16 criterios, agrupado en tres de alto nivel (Forrester, 2016):

Oferta actual. Incluye 6 criterios: (Forrester, 2016)

- El aprovisionamiento de cuentas de usuario y la identidad de la administración.

- La certificación, la separación de funciones (SOD), y la administración de funciones de la empresa.
- Inicio de sesión único (SSO).
- Federación.
- Soporte en la nube.
- Reportes e informes.

Estrategia. Incluye 8 criterios (Forrester, 2016):

- La diferenciación y características únicas.
- La dotación de personal del proveedor.
- Planes futuros.
- La satisfacción del cliente.
- Socios y ecosistema de aplicación.
- La capacidad multiusuario y solución de fijación de precios.
- La integración y OEM.
- Relaciones.
- Finanzas y estabilidad.

Presencia del mercado. Incluye 2 criterios (Forrester, 2016):

- Base instalada.
- Verticales.

3.2.5 FORTALEZAS Y DEBILIDADES DE LOS PRINCIPALES VENDEDORES

EMC (RSA) con sede en Massachusetts RSA, la División de Seguridad de EMC, ofrece su solución IGA como software o como un servicio. El producto es originario de Aveksa, que fue adquirida en 2013. La solución se compone de varios módulos que se licencian por separado. Es una buena opción para las organizaciones con fuertes

requerimientos de gobierno de identidades y accesos. RSA tiene clientes en todos los principales mercados verticales de la industria (Gartner Inc., 2016).

En octubre de 2015, Dell (que también tiene un producto) anunció su intención de adquirir EMC. Hasta que la fusión concluya, las dos empresas deben operar de forma independiente (Gartner Inc., 2016).

Varios cambios estructurales, como la falta de innovación reciente en comparación con años anteriores, han causado EMC se retrasen en comparación con el año pasado (Gartner Inc., 2016).

Sus principales fortalezas son:

- La sólida oferta de IGA, en combinación con la herramienta de Archer que predomina en el mercado GRC (Governance, Risk and Compliance), conduce a ventas cruzadas y un aumento de oportunidades en organizaciones que enfrentan las obligaciones de cumplimiento normativo.
- EMC ha creado un ecosistema de socios sólido.
- Su producto califica por encima de la media de todas las áreas, excepto para el ciclo de vida de las identidades y auditoría, y obtuvo puntaje muy alto en facilidad de implementación.

Sus principales debilidades son:

- Aunque los clientes son positivos en sus descripciones del producto, su satisfacción con el soporte y el mantenimiento de EMC sigue por debajo de la mayoría de los otros proveedores
- Después de la propuesta de adquisición de Dell de EMC puede tener dos productos IGA. Esto genera incertidumbre respecto a la estrategia futura.
- El producto es difícil de personalizar. Funciona mejor cuando las organizaciones pueden implementar la solución adaptándose a la forma en que está diseñado, en lugar de tratar de hacer una amplia personalización.

Micro Focus (NetIQ) basada en Reino Unido, surge de la fusión de MicroFocus en noviembre de 2014, con el Attachmate Group y ofrece sus soluciones de software NetIQ Identity Manager y Access Review junto a varios módulos opcionales. Además, MicroFocus es compatible con una versión de SailPoint en virtud de un acuerdo OEM como NetIQ Access Governance Suite (AGS) (Gartner Inc., 2016).

NetIQ Identity Manager, Access Review y AGS se evaluaron como una solución combinada para los fines de esta Magic Quadrant. Los productos de NetIQ son especialmente atractivos para las organizaciones que están buscando una solución flexible que proporciona la capacidad de escalar en el tiempo, con fuerte automatización y capacidades de aprovisionamiento (Gartner Inc., 2016).

Entre sus clientes se distribuyen uniformemente a lo largo de múltiples mercados verticales, encabezados por la salud, bancario, valores y seguros y la educación. Los clientes de Micro Focus se encuentran ampliamente distribuidos en toda el mundo (Gartner Inc., 2016).

Sus principales fortalezas son:

- Micro Focus es capaz de alinear e integrar su oferta de IGA con su cartera de productos adyacentes de análisis para hacer frente a la creciente demanda de enfoques IAM basados en riesgo.
- Cuenta con una red de canales bien desarrollado, en todo el mundo que proporciona la experiencia local, y ayuda a vender sus productos a nivel mundial.
- Micro Focus sigue siendo altamente calificado para soporte y mantenimiento por referencia clientes.

Sus principales debilidades son:

- Micro Focus se encuentra en medio de una transformación significativa de su línea de productos que se IGA en torno a Access Review, por lo que el

desarrollo de características para ponerse al día con las normas del mercado ha sido lento.

- Micro Focus no promueve sus capacidades verticales de la industria en todo su potencial.
- Sin AGS, las capacidades de Micro Focus para la certificación de acceso e identidad de análisis no es tan robusto como otros vendedores en este Cuadrante Mágico.

Oracle con sede en California ofrece su Oracle Identity Governance (OIG) Suite como una solución de software que consta de varios módulos. La solución es especialmente adecuada para las organizaciones con procesos complejos que requieren flexibilidad en el producto y están dispuestos a invertir en servicios profesionales. Con el lanzamiento de la versión 11gR2 PS3, Oracle ha logrado fortalecer varios aspectos de productos y ahora ofrece una solución completamente unificada IGA. Oracle tiene clientes distribuidos con el apoyo de sus socios en todo el mundo (Gartner Inc., 2016).

Sus principales fortalezas son:

- El producto de Oracle es flexible y personalizable, tiene un modelo de datos muy eficiente que le da un muy buen desempeño.
- La integración de Oracle de IGA con su solución de gestión de dispositivos móviles permite a los usuarios combinar tecnologías en un programa de movilidad IAM y empresarial unificada.
- La adición de solución de IGA de Oracle como parte de la plataforma Fusion Middleware para una cartera de otros productos de IAM de Oracle pueden aprovechar las sinergias entre los productos, por lo que es atractivo para los clientes existentes de Oracle que ven el proveedor como un socio estratégico.
- La presencia global y los canales en todo el mundo de Oracle permiten su producto se despliegue con facilidad.

Sus principales debilidades son:

- El producto es más complejo de trabajar que otros productos que se evaluaron. Formar y retener talento interno para el producto de Oracle es complejo.
- Los valores de referencia del producto están en el cuartil más bajo de todas las puntuaciones de los proveedores, al igual que las calificaciones de soporte y mantenimiento.
- Junto con una reorganización más amplia y una realineación estratégica, existe cierta incertidumbre en torno a la dirección futura del producto.

SailPoint con sede en Texas ofrece su solución de software IdentityIQ con varios módulos opcionales y su solución IdentityNow como un servicio. SailPoint IdentityIQ es adecuado para organizaciones con estrictos requisitos de gobierno (Gartner Inc., 2016).

SailPoint adquirido recientemente Whitebox Security y con ello, un producto completo DAG. La mayoría de sus clientes están en la banca, valores y seguros. El resto son distribuidos uniformemente entre otras verticales. Los clientes de SailPoint están repartidos por todo el mundo, con América del Norte y Europa líder en términos de despliegues (Gartner Inc., 2016).

Sus principales fortalezas son:

- Un buen funcionamiento y una gran red de socios da impulso SailPoint a vender e implementar sus productos en todo el mundo. Además, ofrece una gran cantidad de servicios profesionales.
- La estrategia de productos de SailPoint es amplia y orientada hacia el futuro. Whitebox Security, renombrado como SecurityIQ, dan a la empresa más opciones para solidificar su posición de líder.
- El enfoque de SailPoint de marketing, junto con su éxito en mercados críticos, tales como servicios financieros, son responsables de la fuerte la conciencia y el reconocimiento de marca que hace que sea un proveedor evaluado con frecuencia.

Sus principales debilidades son:

- El precio por usuario para el mercado de medianas y pequeñas empresas es significativamente más alto que las normas del mercado. Para esas organizaciones, SailPoint ofrece IdentityNow basado en la nube como una opción más asequible, pero que no es tan completo como IdentityIQ.
- El producto es difícil de personalizar. Funciona mejor cuando las organizaciones pueden implementar la solución adaptándose a la forma en que está diseñado, en lugar de tratar de hacer una amplia personalización.
- Encontrar el talento con experiencia es complejo.

IBM con sede en Nueva York ofrece IBM Security Identity Governance and Administration suite como software o como un servicio. La solución consiste en tres módulos que pueden ser objeto de licencia por separado. IBM es una buena opción para grandes organizaciones con procesos complejos que necesitan de automatización y de gobierno y están dispuestos a invertir en servicios profesionales (Gartner Inc., 2016).

Una quinta parte de sus clientes están en la banca, valores y seguros, con el resto de manera uniforme distribuido en todos los demás sectores verticales. Los clientes de IBM IGA se encuentran ampliamente distribuidos en todo el mundo (Gartner Inc., 2016).

Sus principales fortalezas son:

- Los clientes pueden aprovechar las sinergias entre la solución IGA, IBM Security Guardium Database e IBM Seguridad QRadar (SIEM), que atrae a los clientes actuales que están ya están comprometidos con IBM para las tecnologías de seguridad de la información.
- Su amplia presencia global permite que los productos se vendan de manera efectiva en todas partes.
- IBM cuenta con una red de canales de gran éxito.

Sus principales debilidades son:

- El modelo de precios de IBM, a menudo basadas en unidades de valor por usuario (UVUs), es opaca y causa confusión especialmente en ofertas que involucran a múltiples tipos de grupos de usuarios.
- El producto proporciona un marco flexible para el análisis de políticas y la ejecución de SOD, pero no se aplica de forma coherente. No existe un marco de auditoría de propósito general, y la mayoría escenarios requieren la creación y programación de las reglas avanzadas que podrían desencadenar flujos de trabajo personalizados.
- Cambios de nombres en los últimos dos años se han creado confusión considerable en el ecosistema de socios, integradores y centros de compra potenciales.

3.2.6 CRITERIOS DE SELECCIÓN

Las organizaciones deben considerar todos los productos de los proveedores de IGA sin importar el cuadrante al cual pertenezcan, la decisión de adquisición de estas herramientas debe basarse en sus requerimientos funcionales y operativos específicos. Los principales factores a tomar en cuenta son (Gartner Inc., 2016):

- El costo total relacionado con la implementación de la herramienta.
- Servicios.
- Período de tiempo estimado necesario para desplegar la herramienta.
- ¿El proveedor tiene una red de socios eficiente de trabajo que pueda entregar rápidamente servicios especializados de todo el despliegue y operación?
- Apoyo disponible a nivel local, en el idioma de su organización y durante horas regulares de trabajo dentro de sus zonas geográficas

- ¿Es fácil de integrar esta tecnología en su infraestructura existente? ¿Su organización TI será capaz de soportarlo?
- ¿Puede el vendedor puede aportar una herramienta que permite aplicar mejoras prácticas y personalización para sus procesos específicos?
- ¿Sus usuarios de negocios encontrarán que es fácil trabajar con esta tecnología? ¿Cómo se pondrá a su disposición?
- ¿El vendedor ayuda a su organización entregar cumplimiento de las políticas de seguridad y reglamentos de manera más efectiva?
- ¿Este proveedor está alineado con sus requerimientos tecnológicos y del negocio actual y del futuro?

3.3 MERCADO IDAAS

3.3.1 DESCRIPCIÓN DEL MERCADO

Los vendedores calificados como B2E Cloud IAM (Forrester, 2015) o IDAAS (Gartner, 2015) provienen de distintos orígenes. Sus genealogías varían en gran medida, al igual que su capacidad para proporcionar funcionalidades IAM en profundidad y soporte para diferentes casos de uso. Sus aspiraciones para dar servicio a los clientes por la geografía, la industria y la segmentación de clientes de tamaño también varían (Gartner, 2015).

Un vendedor en el mercado de gestión de identidades y accesos como servicio, ofrece un servicio predominantemente basado en la nube, en un modelo de prestación multiusuario o dedicada y centrada en el gobierno y administración de identidades. (Gartner, 2015). Existen dos tipos de vendedores en este mercado, aquellos que tienen soluciones IGA establecidas y aquellos cuyas soluciones nacieron en la nube que suelen tener una oferta más simple y rápida de implementar (Forrester, 2015).

Estas soluciones por lo general reducen la complejidad, los costos de licencias y mantenimiento y elimina las barreras a la adopción. Proporciona una visión unificada de acceso de los usuarios a las aplicaciones y un portal único para los empleados acceder a las mismas (Forrester, 2015).

También ofrecen la flexibilidad ya que pueden escalar el número de usuarios y las aplicaciones hacia arriba o abajo según sea necesario durante el plazo de contrato con algún proveedor. Dado que los equipos de seguridad sólo tienen que gestionar las políticas de IAM y ya no se encuentren afectos a las responsabilidades operativas de mantenimiento de la propia solución se reduce la cantidad de empleados involucrados. Esto las hace especialmente atractivas para muchas pequeñas y medianas empresas que

no pueden permitirse el lujo de cuatro a cinco empleados para apoyar una solución IAM. Incluso las grandes empresas están evaluando soluciones IAM en la nube con la esperanza de convertir el gasto de gasto de capital a gastos operativos (Forrester, 2015).

Las soluciones actuales ofrecen soporte para las aplicaciones heredadas on-premise, así como para las aplicaciones SaaS. Sin embargo, Forrester descubrió que hoy en día el 20% de las organizaciones utilizan para IDaaS para aplicaciones internas y un 80% para gestionar el acceso a las aplicaciones SaaS. Soportan SSO desde y en los dispositivos móviles de manera rentable construidas sobre estándares como OpenID (Forrester, 2015).

Los vendedores IDaaS en general han tenido especial cuidado en el desarrollo de su arquitectura de red y alojan sus servicios en una IaaS provista de redundancia suficiente para garantizar los acuerdos de nivel de servicio. Sin embargo, un fallo del sistema principal con el IDaaS tiene el potencial de dejar temporalmente sin acceso a los clientes a ciertas aplicaciones. Las organizaciones se enfrentan a riesgos similares cuando se administran sus propios servicios de IAM y cuando los componentes tales como servidores de federación fallan. Aquellos que optan por aceptar los riesgos del uso de IDaaS, deben tener procesos que aseguren la continuidad del negocio (Gartner, 2015).

El reemplazo de software de IAM tradicional no es común. Las implementaciones IGA son antiguas y se han desplegado para apoyar a los sistemas heredados, no solo aplicaciones SaaS. Sin embargo, hay vendedores que pueden soportar múltiples casos de uso y potencialmente reemplazar herramientas IAM on-premise. La decisión de externalizar implementaciones complejas de IAM no es simple y se debe tomar en cuenta muchos factores (Gartner, 2015).

Muchos de los inhibidores para la adopción exitosa de IAM on-premise, podrían aliviarse o eludirse por el paso a IDaaS, algunos ejemplos son (Gartner, 2015):

- Personal con conocimientos y habilidades insuficientes o inadecuadas.
- Implementaciones de IAM duplicadas dentro de organizaciones por distintos motivos estratégicos y de negocio.
- Insuficiente planificación antes de la selección y aplicación de herramientas.
- La corrupción del alcance del proyecto.
- Baja eficiencia operativa, lo que resulta en mucho tiempo tomado para las funciones de IAM.
- Baja eficacia operativa IAM, lo que resulta en resultados de la auditoría de violaciones de acceso.

También se puede reducir el costo total de propiedad. Estos costos incluyen (Gartner, 2015):

- Los gastos de personal.
- Los costos de inversión y mantenimiento de software en curso.
- Costos de actualización.
- Infraestructura para implementaciones flexibles y la continuidad del negocio.

La mayoría de los proveedores incluidos en esta investigación se basan en EE.UU. Los clientes tienen preocupación por la información almacenada en la nube. A pesar de la utilización de los centros de datos locales o regionales, los clientes internacionales tienen preocupación por la capacidad del gobierno de EE.UU. para obtener acceso a los datos. Este es actualmente el riesgo de que los clientes deben evaluar y luego determinar si es aceptable (Gartner, 2015).

Gartner en sus reconocidos Magic Quadrant mide vendedores en sus capacidades generales de IAM para múltiples casos de uso. Los vendedores en este Cuadrante Mágico deben proporcionar un cierto nivel de funcionalidad en todas las siguientes áreas funcionales (Gartner, 2015):

- IAM. Como mínimo, el proveedor de servicio es capaz de automatizar la sincronización de identidades en poder del servicio u obtenidos de repositorios de identidad de los clientes que se dirigen a las aplicaciones y otros repositorios. El vendedor también debe proporcionar una manera para que los administradores de los clientes puedan gestionar identidades directamente a través de una interfaz de administración IDaaS, y permitir a los usuarios restablecer sus contraseñas. Además, los proveedores pueden ofrecer mayor funcionalidad, como el apoyo a los procesos del ciclo de vida de la identidad, aprovisionamiento automatizado de cuentas entre sistemas heterogéneos, las solicitudes de acceso, incluyendo autoservicio, y el gobierno sobre el acceso de usuarios a los sistemas críticos a través de flujos de trabajo para la aplicación de políticas, así como para procesos de certificación de acceso. Las capacidades adicionales pueden incluir la administración de funciones y certificación de acceso.
- Acceso. El acceso incluye la autenticación de usuario, inicio de sesión único (SSO) y la aplicación de autorización. Como mínimo, el proveedor proporciona autenticación y SSO para orientar las aplicaciones que utilizan servidores proxy Web y estándares de Federación. La mayoría de los vendedores ofrecen métodos de autenticación adicionales.
- Registro de eventos de identidad y reportes. Como mínimo, el proveedor registra los eventos de IGA y de acceso, pone a disposición los datos de registro a los clientes para su propio análisis, y proporciona la capacidad de generar informes.

FIGURA 3-3 IDAAS MAGIC QUADRANT

FUENTE: GARTNER, 2015

Por su parte Forrester en su prestigioso informe Wave, realiza una evaluación comprensiva, analizando y puntuando 17 criterios de IAM sobre los nueve proveedores más importantes en la categoría. El informe detalla conclusiones acerca de lo bien que cada proveedor cumpla con los criterios y cuál es su posición en relación a los demás (Forrester, 2015).

ONELOGIN y OKTA van a la cabeza. Estos proveedores demostraron amplias capacidades para integrarse a directorios de usuarios, administración de políticas de acceso, y un amplio catálogo de aplicaciones SaaS compatibles. También han demostrado simplicidad relativa entre las ofertas evaluadas y tienen una gran base instalada (Forrester, 2015).

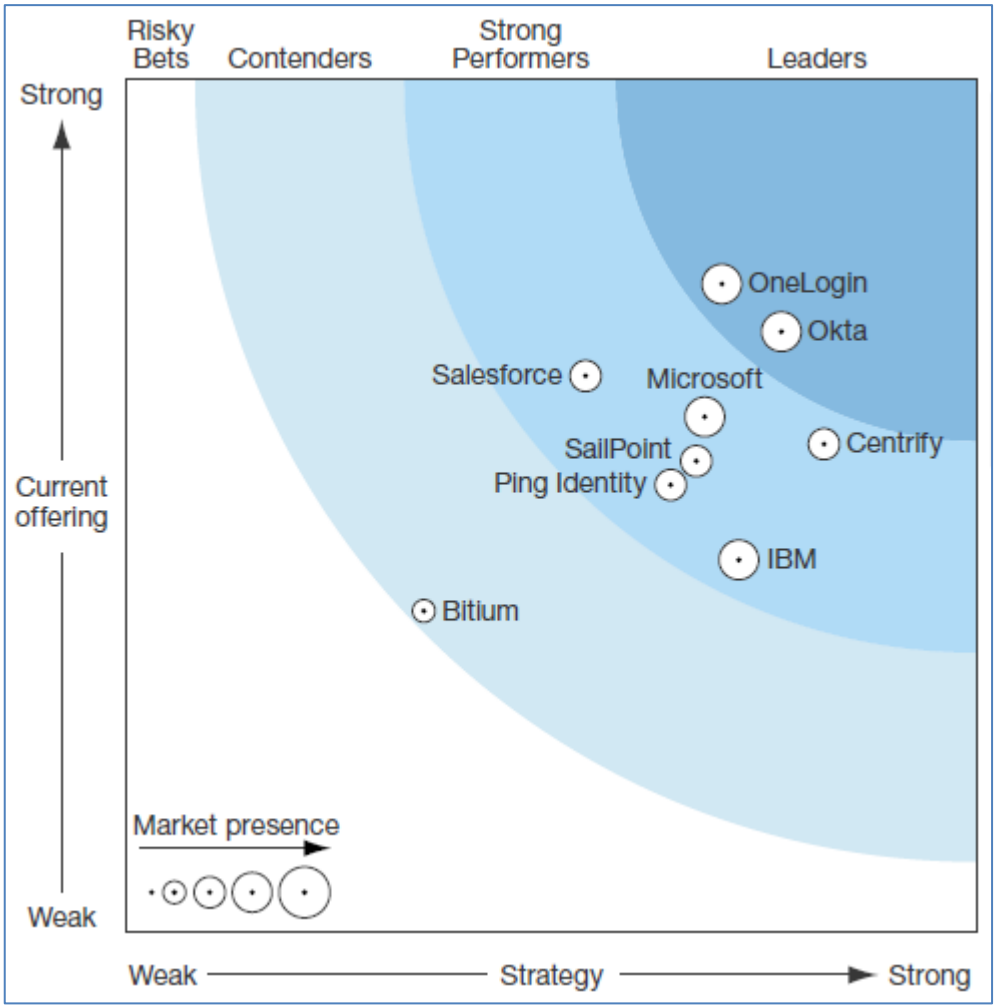

FIGURA 3-4 B2E CLOUD IAM WAVE

FUENTE: FORRESTER, 2016

3.3.2 DESCRIPCIÓN DE LOS CUADRANTES Y WAVES

A continuación, se describen los cuadrantes mágicos de Gartner:

Leader (líderes), los líderes en el mercado IDaaS han logrado fuertes ganancias de los clientes. Proporcionan conjuntos de características que son apropiadas para las necesidades de casos de usos de clientes actuales. Los líderes también muestran evidencia de una fuerte visión y ejecución de los requisitos previstos relacionados con la tecnología, metodología o vectores. Los líderes demuestran típicamente satisfacción del cliente y/o servicio relacionado y apoyo (Gartner, 2015).

Challengers (retadores), también muestran una sólida ejecución, y tienen importantes ventas y presencia de marca. Sin embargo, no han mostrado la integridad de la visión de que tienen los líderes IDaaS. Más bien, su visión y ejecución de la tecnología, metodología y/o vectores tienden a estar más centrado o restringido en las funciones, plataformas, geografías o servicios específicos. Los clientes están relativamente satisfechos, pero piden funcionalidades adicionales, un apoyo más oportuno y niveles de servicio más altos de los que se entregan actualmente (Gartner, 2015).

Visionaries (visionarios), los vendedores de este cuadrante proporcionan productos que cumplen muchos de los requisitos IDaaS del cliente, pero pueden no tener la penetración en el mercado para ejecutar como lo hacen los líderes. Los visionarios son conocidos por su enfoque innovador de la tecnología IDaaS, metodología y/o vectores. Pueden ver IDaaS como una parte clave de una cartera de servicios mucho más amplia. A menudo pueden tener características únicas, y pueden estar centrados en una industria específica o el conjunto específico de casos de uso. Además, tienen una fuerte visión para el futuro del mercado y su lugar en él (Gartner, 2015).

Niche Players (jugadores de nicho), proporcionan la tecnología IDaaS adecuada para un conjunto específico de casos de uso. Pueden centrarse en industrias específicas o tienen una huella limitada geográficamente, pero que puede superar a muchos competidores. Los vendedores de este cuadrante a menudo tienen relativamente menos

clientes que sus competidores, pero pueden tener grandes clientes. Los precios podrían ser considerados demasiado altos para el valor proporcionado por algunos vendedores de nicho. La inclusión en este cuadrante, sin embargo, no refleja negativamente el valor del proveedor en el espectro de servicio más estrechamente enfocado. Soluciones de nicho pueden ser muy eficaces en sus áreas de interés (Gartner, 2015).

A continuación, se describen las waves de Forrester:

- **Leaders (líderes)** proporcionan una gran solución a nivel global con amplias bases instaladas y características creíbles (Forrester, 2015).
- **Strong Performers (participantes fuertes)** ofrecen soluciones robustas y fiables, pero están detrás de líderes en los ámbitos de la movilidad, de base instalada y socios de ecosistemas (Forrester, 2015).
- **Challengers (retadores)** carecen de muchas de las capacidades de otras soluciones evaluadas, una base instalada convincente, y algunas funciones clave de otros vendedores ofrecen (Forrester, 2015).

3.3.3 CRITERIOS DE INCLUSIÓN

Gartner evalúa los siguientes criterios para la inclusión de soluciones: (Gartner, 2015)

- La longevidad de la oferta y que la misma este en uso en múltiples entornos de producción de clientes.
- Número de clientes y usuarios finales, incluyendo los clientes de proveedores de servicios de terceros y sus usuarios finales.
- Los ingresos atribuidos a tasas por el uso del servicio IDaaS es mayor de 4 millones de dólares para el año de estudio.
- Verificabilidad: Referencias de clientes deben estar disponibles.

Por su parte Forrester los siguientes criterios (Forrester, 2015):

- Una oferta IDaaS multiusuario verdadera.
- Una solución capaz de integrarse con Active Directory on-premise.
- Ganancias de al menos 1 millón de dólares en el año de estudio.
- Al menos 40 clientes con soluciones en ambientes productivos.

3.3.4 CRITERIOS DE EVALUACIÓN

Gartner evalúa los siguientes criterios:

Capacidad de ejecución. Esto incluye los siguientes criterios (Gartner, 2015):

- Producto como servicio: Bienes y servicios ofrecidos por el proveedor para el mercado. Esto incluye capacidades del producto y servicio actual, la calidad y el conjunto de sus características. Ya sea ofrecido de forma nativa o a través de acuerdos y asociaciones.
- Viabilidad general: Incluye una evaluación general de la organización de su salud financiera, el éxito financiero y práctico de la unidad de negocio, además la probabilidad de que la unidad de negocio crezca y siga invirtiendo en el producto.
- Ejecución de Ventas/Precio: Capacidades del proveedor en todas las actividades de pre-venta. Esto incluye la gestión de oferta, los precios y la negociación, pre-venta de apoyo, y la eficacia global del canal de ventas.
- Respuesta al mercado: Capacidad de responder, cambiar de dirección, ser flexible y lograr el éxito competitivo frente a los competidores, las necesidades del cliente y la evolución dinámica del mercado. Este criterio también se considera la historia del vendedor.
- Ejecución de marketing: La claridad, calidad, creatividad y la eficacia de los programas diseñados para entregar los mensajes de la organización para influir

en el mercado. La promoción de la marca y de negocios, aumentar el conocimiento de los productos y establecer una identificación positiva con el producto, marca y la organización en la mente de los compradores.

- Experiencia del cliente: Relaciones, productos, servicios y programas que permiten a los clientes tener éxito con los productos evaluados. Específicamente, esto incluye la asistencia técnica o soporte de los clientes. Esto también puede incluir herramientas auxiliares, programas de apoyo a los clientes, la disponibilidad de grupos de usuarios, acuerdos de nivel de servicio, entre otros.
- Operaciones: La capacidad de la organización para cumplir sus objetivos y compromisos. Factores incluidos son la calidad de la estructura organizacional, habilidades, experiencias, programas, sistemas y otros vehículos que permiten la organización operar con eficacia y eficiencia de forma continua.

Completitud de la visión. Esto incluye los siguientes criterios (Gartner, 2015):

- Entendimiento del mercado: Capacidad del proveedor para entender los deseos y necesidades de los compradores y para traducirlos en productos y servicios. Los vendedores que muestran el más alto grado de visión escuchan y entienden los deseos y necesidades de los compradores.
- Estrategia de marketing: Un claro y diferenciado conjunto de mensajes exteriorizado a través de la página web, publicidad, atención al cliente programas y declaraciones de posicionamiento.
- Estrategia de venta: Estrategia para la venta de productos que utilice la red apropiada de ventas directa e indirectas, comercialización, servicios y de la comunicación que amplían el alcance y la profundidad en el mercado, habilidades, conocimientos, tecnologías, los servicios y la base de clientes.
- Estrategia de oferta de productos: El enfoque del proveedor para el desarrollo de productos y la entrega que hace hincapié en la diferenciación, la

funcionalidad, la metodología y los conjuntos de características que se asignan a las necesidades actuales y futuras.

- Modelo de negocio: La solidez y la lógica de la propuesta de negocio subyacente del proveedor.
- Estrategia vertical/industria: La estrategia del proveedor para dirigir los recursos, las capacidades para satisfacer las necesidades específicas de los distintos sectores del mercado, incluidos los mercados verticales.
- Innovación: Recursos directos, indirectos, relacionados y su sinergia invertidos en innovación.
- Estrategia geográfica: La estrategia del proveedor para dirigir los recursos, capacidades y ofertas para satisfacer las necesidades específicas de las zonas geográficas, ya sea directamente o a través de socios, canales y filiales.

Por su parte Forrester evalúa a los vendedores contra 17 criterios, agrupado en tres de alto nivel:

Oferta actual. Incluye 7 criterios: (Forrester, 2015)

- Soporte para directorio de usuarios.
- Administración de políticas de acceso.
- Administración de políticas de aprovisionamiento de cuentas.
- Portal de autoservicio de usuarios.
- Autoservicio desde aplicaciones móviles.
- API de solución y seguridad.
- Reportes y escalabilidad.

Estrategia. Incluye 6 criterios (Forrester, 2015):

- Desarrollo futuro del producto y planes de mercado.
- Satisfacción de los clientes.
- Asociaciones OEM.

- Staff de desarrollo, ventas y de soporte.
- Flexibilidad de precios y transparencia.
- Percepción de los clientes.

Presencia del mercado. Incluye 3 criterios (Forrester, 2015):

- Ganancias.
- Base instalada.
- Presencia geográfica y vertical.

3.3.5 FORTALEZAS Y DEBILIDADES DE LOS PRINCIPALES VENDEDORES

IBM en 2014 adquirió Lighthouse Security Group, un proveedor que suministra IDaaS respaldados por el software de IBM. IBM ha rebautizado la oferta como Cloud Identity Service, que es ofrecido en un modelo multiusuario. Sin embargo, los componentes del servicio se pueden entregar en un modelo dedicado (Gartner, 2015).

Sus principales fortalezas son:

- La oferta funcional de IBM es profunda y se alinea con la funcionalidad proporcionada por el software de IBM desplegado en las instalaciones del cliente.
- La oferta de IBM se hará más profunda a través de la adquisición de capacidades IGA de CrossIdeas, así como la integración de MaaS360 mobile device management de Fiberlink (MDM).
- La adquisición Lighthouse Security Group y la amplitud de recursos de IBM deberían convencer a los clientes que tienen aversión al riesgo. IBM ha ampliado geográficamente sus ubicaciones de centros de datos, soporte y servicios profesionales.

- La compañía tiene algunos clientes muy grandes y puede demostrar una alta escalabilidad.

Sus principales debilidades son:

- Los clientes informan Cloud Identity Service requiere de esfuerzo considerable para su implementación. Esto se debe en parte a la naturaleza compleja de los proyectos que IBM adquiere para los clientes más grandes. IBM tendrá que entregar una oferta de servicios que sea más configurable y fácil de implementar, sin requerir servicios profesionales importantes, con el fin de competir por el mercado.
- Si bien los indicadores apuntan al crecimiento de la oferta de IBM, nuevos clientes aún no se han traducido en referencias.
- A pesar de las reducciones de precios en 2015, los precios de IBM para varios escenarios de casos de uso fueron de las más altas.

Microsoft entró en el mercado en IDaaS de mayo de 2014, con sus servicios enfocados business-to-employee (B2E) Azure Active Directory services. Hay tres niveles de servicio, la oferta Premium proporciona características que están en línea con otros proveedores de IDaaS centrado en la web, e incluye licencias para Microsoft Identity Manager (MIM) que se van a utilizar en los sistemas del cliente. Microsoft también ofrece Azure Active Directory Premium como parte de su Enterprise Mobility Suite, junto con Microsoft Intune y Azure Rights Management (Gartner, 2015).

Sus principales fortalezas son:

- Microsoft se unió a un mercado IDaaS establecido, y es capaz de aprovechar su actual base de clientes. Especialmente clientes de Office 365. La empresa cuenta con unas amplias capacidades de marketing, ventas y soporte.
- Microsoft ya ha demostrado su alta escalabilidad con Azure Active Directory. El servicio apuntala otros servicios de Microsoft Azure. Microsoft tiene una

fuerte presencia internacional de su oferta de servicios, y continúa ampliando su infraestructura como un servicio de presencia (IaaS) en todo el mundo.

- La empresa es capaz de aprovechar las fuentes de datos y aprendizaje automático para apoyar las funciones de inteligencia, tales como la identificación de direcciones IP conocidas malas y dispositivos para ayudar a prevenir la actividad fraudulenta.
- La estrategia de Microsoft demuestra una fuerte comprensión de la tecnología, socio-económico, la seguridad y las tendencias jurisdiccionales que dará forma a su oferta de ir hacia adelante.

Sus principales debilidades son:

- Los componentes on-premises "bridge" de Microsoft son los Servicios de federación de Active Directory y Azure Active Directory Sync. Los clientes deben implementar y administrar estos dos componentes por su cuenta.
- Mientras Azure Active Directory Premium incluye licencias de acceso para MIM, los clientes son responsables de la gestión de esa aplicación a sí mismos o con la ayuda de terceros.
- Microsoft puede proporcionar el aprovisionamiento de usuarios para algunas aplicaciones de la nube. Sin embargo, los competidores tienen una ventaja en términos de la cantidad de aplicaciones disponibles, así como el aprovisionamiento de los roles, grupos y otros atributos.
- Microsoft puede proporcionar aprovisionamiento y SSO para usuarios de la empresa a los sitios de medios sociales, y tiene APIs y kits de desarrollo de software (SDK) para el apoyo de medios sociales. Sin embargo, el servicio aún no ofrece registro sociales envasados y el inicio de sesión a los sistemas de Azure Active Directory o de destino.

Okta tiene una oferta de IDaaS con modelo multiusuario y con componentes ligeros para conectores de repositorio y sistema de destino locales. IDaaS es la actividad

principal de la empresa. Okta ofrece administración de identidad y capacidades de aprovisionamiento, gestión de accesos y la presentación de informes.

Okta también proporciona capacidades de autenticación de phone-as-a-token y añadió Gestión de la Movilidad en 2014 (Gartner, 2015).

Sus principales fortalezas son:

- Estrategias de marketing y ventas de la compañía han sido eficaces, como lo demuestra el reconocimiento de marca y un mayor volumen de clientes. La base de clientes de Okta creció significativamente en 2014 y principios de 2015.
- La inversión continua de Okta en su conjunto de APIs permite a los desarrolladores apoyar la integración con aplicaciones y flujos de trabajo de los clientes.
- Gartner volvió a recibir numerosas referencias, y ha confirmado predominantemente experiencias positivas. Los clientes están comenzando a utilizar la funcionalidad MDM integrada con IDaaS para apoyar las funciones tales como móvil SSO, las políticas de acceso dispositivo y restablecer PIN del dispositivo.
- Okta ha mantenido alta disponibilidad y confiabilidad.

Sus principales debilidades son:

- Okta puede sincronizar las identidades de los directorios de empresas, y se ha añadido la funcionalidad de administración delegada. Sin embargo, el vendedor no tiene un flujo de aprovisionamiento más allá de un solo nivel, ni tiene funciones de gobierno identidad.
- La capacidad de generar informes personalizados y enlatados de Okta son limitadas.
- Okta todavía no soporta el uso de las identidades sociales para registro y de inicio de sesión. Están en proceso de ser implementadas.

- La base de clientes actual de Okta se encuentra predominantemente en los EE.UU, al igual que sus centros de datos, pero Okta ha invertido en la expansión europea y Asia Pacífico en términos de ventas y centros de datos.
- Okta se enfrenta a la creciente competencia de los proveedores más grandes.

Salesforce proporciona Salesforce Identity como parte de su fuerza de ventas. Vende Identity a clientes de Salesforce establecidos y nuevos.

Identidad Connect es componente puente entre las instalaciones de Salesforce que se vende por separado. El servicio incluye la funcionalidad de referencia necesaria para su inclusión, así como el registro social y de inicio de sesión, la funcionalidad de pasarela, federación, y la solicitud de acceso profundo y suministro de usuarios funcionalidad de flujos de trabajo (Gartner, 2015).

Sus principales fortalezas son:

- Salesforce es capaz de ejercer una presión en el mercado, proporcionando así incentivos para mantener su base de clientes.
- Salesforce Identity se aprovecha de la funcionalidad de flujos de trabajo de solicitud de acceso profundo y aprobación inherente a la plataforma Salesforce.
- La estrategia de la fuerza de ventas demuestra una fuerte comprensión de la tecnología, socio-económico, la seguridad y las tendencias jurisdiccionales que dará forma a su oferta de ir hacia adelante.
- Salesforce Identity tiene un fuerte apoyo de los medios y las normas de identidad social.

Sus principales debilidades son:

- Salesforce no es compatible con las capacidades de bóveda de contraseña y de SSO.

- Salesforce Identity no proporciona acceso basado en proxy para aplicaciones web de correo locales.
- El componente puente de Salesforce Identity no proporciona la capacidad de sincronizar los cambios del directorio de la nube a los directorios de empresas. Se necesitan servicios profesionales para ofrecer esta funcionalidad.
- A pesar de una considerable presencia en el mercado de PaaS de Salesforce y las campañas de concienciación recientes, la marca de Salesforce Identity aún no es bien conocida en el mercado. El servicio está en su segundo año de disponibilidad.

3.4 TENDENCIAS

De acuerdo con un reciente estudio de Forrester, la gestión de accesos fue identificada como uno de los problemas de seguridad más relevantes para las organizaciones y es considerado como un componente crítico de sus estrategias de seguridad corporativa. (Forrester, 2011).

3.4.1 TENDENCIAS GENERALES IAM

A nivel general en los próximos años, algunas de las tendencias que más fuerza han adquirido en el ámbito de la gestión de identidades y accesos son (Al-Khouri, 2011):

- Convergencia entre gestión lógica y física de accesos.
- Autenticación robusta.
- Identity Federation.
- Estándares de autorización como SAML y OAuth.
- Identity Assurance.
- Gestión de accesos basada en roles.
- Herramientas para facilitar el cumplimiento de regulaciones.
- Identity Analytics.
- Identity in the Cloud.
- Identity as a Service.
- Movilidad.
- Integración con otras soluciones de seguridad.

3.4.2 TENDENCIAS MERCADO IGA

Los líderes deben tomar nota de las necesidades emergentes en torno a enfoques más conscientes del riesgo y la adopción de la nube. Se espera que para el 2018 reemplazarán más del 50% de las tareas manuales de certificación de accesos y tareas de solicitud de aprobación (Gartner Inc., 2016). Forrester ha observado que con frecuencia los clientes de este mercado están buscando soluciones IGA que soporten las aplicaciones SaaS junto con las aplicaciones on-premise y muchos de ellos están dispuestos a aprovechar las ventajas de costo y velocidad de la nube (Forrester, 2016).

Además, algunas herramientas IGA están evolucionando para soportar un enfoque basado en riesgos, donde las decisiones manuales o automáticas pueden ser informadas según el impacto sobre el riesgo (Gartner Inc., 2016). Lo que comenzó como autenticación basada en riesgo, está evolucionando hacia una forma más rica de identity intelligence y el aprovisionamiento de cuentas de usuario y certificación basado en el riesgo para proteger a las empresas de amenazas nuevas y emergentes (Forrester, 2016).

Los usuarios de empresas y consumidores por igual esperan que las funciones de IGA trabajen sin problemas en múltiples dispositivos y plataformas web, web mobile, aplicaciones móviles nativas y aplicaciones embebidas y a través de fronteras organizacionales (Forrester, 2016).

Gartner observa las siguientes tendencias en el mercado IGA (Gartner Inc., 2016):

- La mayoría de los vendedores han añadido aplicaciones móviles o interfaces web móviles especiales para atender requisitos de negocio específicos, tales como los procesos de aprobación, para restablecer contraseñas, solicitudes y certificaciones.
- Debido a que la experiencia de usuario es un importante criterio de selección, la mayoría de los vendedores ha rediseñado significativamente sus interfaces o están en proceso de hacerlo.

- Se ha comenzado a utilizar herramientas informáticas de gestión de soporte de servicio (ITSSM) para solicitudes de acceso.Varios proveedores han invertido en la integración bidireccional con herramientas ITSSM, y expuesto servicios internos IGA a través de API para facilitar esta integración.
- Gartner ha observado algunas organizaciones han implementado un modelo híbrido de soluciones on-premises y cloud-delivered.
- Los clientes se están dando cuenta de que acceso a aplicaciones y datos están estrechamente relacionados, esto está impulsando el interés en la integración de IGA con productos DAG para las organizaciones más maduras. En 2015, SailPoint adquirió Whitebox, un vendedor de DAG, uniéndose a Courion, Dell, Micro Focus y Saviynt, con ambos tipos de productos que pueden beneficiarse de una mayor integración y oportunidades de ventas adicionales. Además, EMC, IBM y Oracle se han asociado con proveedores de DAG.
- La demanda de integración con los productos de EMM ha crecido, y la mayoría de los vendedores han integrado con éxito con estos productos. Algunos proveedores de IGA tienen productos EMM en su cartera. Pero no todos han integrado sus productos IGA y EMM para aprovechar las sinergias entre ellos.
- La aparición de almacenes de identidades y directorios en la nube ha ejercido presión sobre las herramientas IGA con el propósito de gestionar las identidades de los consumidores. Esto se debe principalmente a que la gestión de la identidad del consumidor es diferente, y sus requisitos sólo se solapan parcialmente con las herramientas IGA que se centran en casos de usos propios de la gestión de las identidades de los empleados y contratistas. Algunos proveedores de IGA están reaccionando a esta presión mediante el descuento de forma agresiva para las identidades externas, como los consumidores, mientras que otros están ofreciendo ediciones especiales de su oferta para la gestión de identidades externas.

- El estado del arte y la adopción de analytics está aumentando rápidamente. Las organizaciones maduras que buscan un enfoque de gestión de identidad consciente del riesgo han llegado a la conclusión de que los métodos de certificación de acceso tradicionales son inexactos, mano de obra intensivos, propensos a errores e insuficientes para abordar adecuadamente los riesgos inherentes. Analytics ayuda mediante la adición de soporte para el análisis de riesgos avanzado, análisis de SOD en todo el espectro de los sistemas operativos institucionales con modelos de autorización complejos tales como ERP y CRM, y el apoyo a la decisión para las aprobaciones y certificaciones, así como permitir la automatización de políticas para reducir las aprobaciones manuales o certificaciones.
- Prácticamente todos los vendedores de IGA ahora son compatibles con SCIM estándar para aprovisionamiento SaaS. El soporte SCIM es incipiente para los proveedores de SaaS, pero la adopción está empezando a crecer y hay varios proveedores de SaaS grandes que soportan el estándar.
- El énfasis en TCO como criterio de selección ha continuado. Esto impulsa la adopción de soluciones "suficientemente buenas" de los proveedores más pequeños dentro y fuera del cuadrante mágico. Esto también está ejerciendo presión sobre las ventas para ofrecer precios y descuentos competitivos.
- Una mayor atención a la protección contra amenazas, incluidas las amenazas internas, está impulsando la integración de los productos de IGA con herramientas generales de detección y análisis de amenazas, específicamente de SIEM y UEBA. Los productos IGA pueden proporcionar contexto de identidad a este tipo de herramientas, y en la dirección opuesta, UEBA puede proporcionar puntuaciones de riesgo y los datos de actividad para IGA.
- Gartner ha notado un mayor interés e inversión en herramientas IGA procedentes de Oriente Medio, especialmente de los países del Consejo de Cooperación del Golfo, debido a un entorno regulatorio en evolución centrado en industrias e infraestructuras críticas.

- La integración entre los productos de IGA y productos de PAM está madurando, impulsado por el interés de los clientes y la competencia de los vendedores que se sitúan en los mercados PAM e IGA. En 2015, varias asociaciones tecnológicas se dieron a conocer entre los vendedores de estos segmentos.
- Hay una clara tendencia que busca aliviar el despliegue complejo de soluciones y actualizar los procesos, la virtualización es cada vez más popular. Varios vendedores también han hecho esfuerzos significativos para hacer que su producto sea más fácil de implementar, administrar, personalizar y depurar.
- Algunos vendedores están proporcionando plantillas de flujos de trabajo para ajustarse mejor a los procesos de negocio comunes, reduciendo de este modo el tiempo y costo inicial y simplificando la personalización.
- Las organizaciones que han tenido plataformas IGA por más de cinco años están empezando a reevaluar a sus proveedores en busca de una mejor experiencia de usuario, la reducción de gastos generales, facilidad de implementación y una mayor escalabilidad.
- Varios vendedores este año están pasando por cambios significativos en la reestructuración y de su oferta de IGA y posicionamiento debido a las adquisiciones, inversiones o cambios en los equipos de gestión de productos.
- Continúa una tendencia de disminución en los precios ya que los vendedores compiten en este punto. TCO sigue siendo un foco para el escrutinio del cliente.

3.4.3 TENDENCIAS MERCADO IDAAS

El mercado IDAAS está creciendo debido a que más profesionales lo ven como una forma de hacer frente a sus principales retos IAM sin los largos tiempos de despliegue de las soluciones on-premise. Otro factor es que existen cada vez más proveedores de

confianza (Forrester, 2015). En 2019, el 25% de las compras de IAM utilizará el modelo IDaaS modelo, frente a menos del 10% en 2014 (Gartner, 2015).

Forrester espera que los vendedores incluyan o mejoren las siguientes funcionalidades a futuro (Forrester, 2015):

- Integración basada en API de seguridad y de internet de las cosas.
- Mobile SSO.
- Mejoras en las capacidades de aprovisionamiento sobre aplicaciones on-premise y SaaS.
- Soporte para campañas de recertificación de accesos.
- Workflows para solicitud de accesos.
- Autenticación basada en riesgo.
- Un portal único basado en la nube que permita acceder a todas las aplicaciones SaaS.
- Conectividad con Active Directory on-premise y otros directorios.
- SAML SSO bidireccional.
- Aplicaciones nativas iOS y Android y soporte para doble factor de autenticación.

Por su parte, Gartner observa las siguientes tendencias (Gartner, 2015):

- Microsoft ha sido muy activo en su base de clientes y ha estado ofreciendo Azure Active Directory Premium durante las renovaciones de contratos existentes. Microsoft también tiene la amplia y creciente base de clientes de Office 365.
- Los vendedores IDaaS han identificado a Microsoft como el vendedor que aparece frecuentemente en situaciones competitivas.
- Salesforce se hizo más activa en el mercado de IaaS en 2014 y principios de 2015, ofrece su producto Salesforce Identity gratis para los usuarios con

licencia de productos de Salesforce. Esto ha ayudado a construir continua lealtad a la plataforma y ha abierto oportunidades de negocio.

- La adquisición de Lighthouse Security Group, por parte de IBM fue altamente sinérgica y fue la última de las tres adquisiciones de IAM por IBM. Los otros eran Trusteer (detección del fraude Web) y CrossIdeas (IGA). IBM ya cuenta con una amplia rama de servicio y la SoftLayer IaaS.
- RSA adquirió la propiedad intelectual de Symplified y contrató a algunos de sus empleados. En abril de 2015, RSA anunció Via, su renombrada oferta IaaS que cuenta con gestión de accesos, así como funcionalidades de administración de usuarios y gestión de identidades, el cual fue obtenido originalmente de la adquisición de Aveksa.
- En 2019, el 40% de los ingresos IDaaS se acumularán a los proveedores de PaaS, frente a menos del 5% en 2014. Las adquisiciones y estrategias competitivas resaltadas anteriormente continúan apoyando esta predicción. Además, la incorporación de IDaaS en las ofertas PaaS ejerce una fuerza commoditization considerable en los mercados.
- El soporte móvil continúa mejorando, en particular para la autenticación y SSO. La mayoría de los proveedores de IaaS admiten interfaces en los dispositivos móviles para aplicaciones web que se encuentran bajo la gestión IDaaS. Los vendedores también comenzaron a soportar las aplicaciones móviles de los clientes, ofreciendo un SDK.

4 EVALUACIÓN ECONÓMICA

4.1 RESUMEN

El presente capítulo resume los diferentes modelos propuestos para evaluar proyectos de seguridad y de gestión de identidades y accesos.

En la sección 4.2 se realiza una introducción al capítulo. En la sección 4.3 se describen lineamientos para la evaluación de costos y beneficios. Posteriormente la sección 4.4 profundiza sobre la evaluación cuantitativa del riesgo. La sección 4.5 lista y describe los principales enfoques y modelos de evaluación de proyectos de seguridad. La sección 4.6 compara los enfoques bajo criterios relevantes para IAM. Finalmente, en la sección 4.7 se lleva a cabo un ejercicio de evaluación económica de un proyecto IAM de ejemplo.

4.2 INTRODUCCIÓN

Identity and Access Management es un elemento clave para la empresa ya que es compatible con la automatización, la aplicación de la seguridad y el cumplimiento. Sin embargo, las empresas encuentran grandes dificultades en las estrategias de implementación. Las discusiones sobre IAM se centran principalmente en el nivel operativo de TI, en lugar de orientarlo a tomadores de decisiones estratégicas a nivel empresarial.

Como en cualquier otro tipo de proyecto se requieren soluciones efectivas y eficientes desde el punto de vista técnico, pero además las organizaciones deben prestar atención a la viabilidad económica. Con un presupuesto limitado y un gran número de activos a proteger las inversiones deben ser evaluadas deliberadamente (Gordon & Loeb, 2006). Valorar las inversiones en seguridad es un proceso crucial que las empresas deben realizar, ya que actúa como intermediario entre las decisiones relativas a cuestiones financieras y las implementaciones de seguridad. Tienen que encontrar el equilibrio entre la posibilidad de mitigar los riesgos de amenazas y los costos asociados (Demetz & Bachlechner, 2013).

Sin embargo, uno de los principales problemas con inversiones en seguridad es a menudo la dificultad para identificar y cuantificar sus beneficios, especialmente para traducirlo en términos económicos y por tanto mostrar su potencial rentabilidad. Las razones para esto son (Magnusson, Molvidsson, & Zetterqvist, 2007):

- La falta de un método de trabajo uniforme para establecer la rentabilidad.
- Las inversiones en TI a menudo detallan sus gastos, pero no sus beneficios.
- La dificultad general para identificar y cuantificar el rendimiento de las inversiones en TI.

Sin un análisis acorde, ningún tomador de decisiones invertirá en un proyecto de seguridad como IAM. Son necesarias entonces metodologías concretas que sirvan como instrumentos de suporte para este tipo de decisiones. En consecuencia, la pregunta "¿Cómo se puede evaluar las inversiones en IAM?" debe ser investigada y tener una respuesta satisfactoria (Royer, 2007).

El origen de la discusión relativa a la evaluación de las inversiones en TI se remonta a finales de 1980, y se ha abordado en consecuencia desde entonces. Varios métodos y marcos se han presentado para la evaluación de los impactos económicos y el valor de las inversiones de seguridad de la información (Royer & Meints, 2009).

Considerando que se han propuesto varios enfoques, diferentes dificultades pueden ser observadas con respecto a los métodos de evaluación, las métricas y la recopilación de datos (Magnusson, Molvidsson, & Zetterqvist, 2007). Se debe considerar también que uno de los puntos de partida para analizar el retorno de la inversión de los proyectos relacionados con la seguridad de TI es la estructura del propio proyecto. En el caso de IAM suele tener un gran impacto estratégico en el conjunto organización (Royer, 2007).

El enfoque financiero clásico no es particularmente apropiado para medir las iniciativas relacionadas con la seguridad. Generalmente una inversión en seguridad no se traduce en un beneficio, sino que está más acerca de la prevención de pérdida por la diminución de riesgos en los activos. Por eso la evaluación cuantitativa del riesgo es fundamental para estos cálculos (ENISA, 2012).

4.3 EVALUACIÓN DE COSTOS Y BENEFICIOS

Con el fin de realizar un análisis costo-beneficio, los tomadores de decisiones necesitan metodologías concretas y procesos de evaluación para evaluar el valor de las inversiones de IAM.

4.3.1 PREMISAS Y PREREQUISITOS

Uno de los puntos de partida para el análisis del retorno de la inversión de los proyectos relacionados con la seguridad es la estructura del proyecto en sí. Como se explica anteriormente, las tecnologías de IAM deben integrarse en el nivel de proceso de una organización. Su introducción probablemente tendrá un impacto enorme en toda la empresa, sus procesos y su estructura. Por lo tanto, los proyectos de IAM deben ser analizados de manera integral, incluyendo factores tales como personas, estructura, tareas y la tecnología (Royer, 2007).

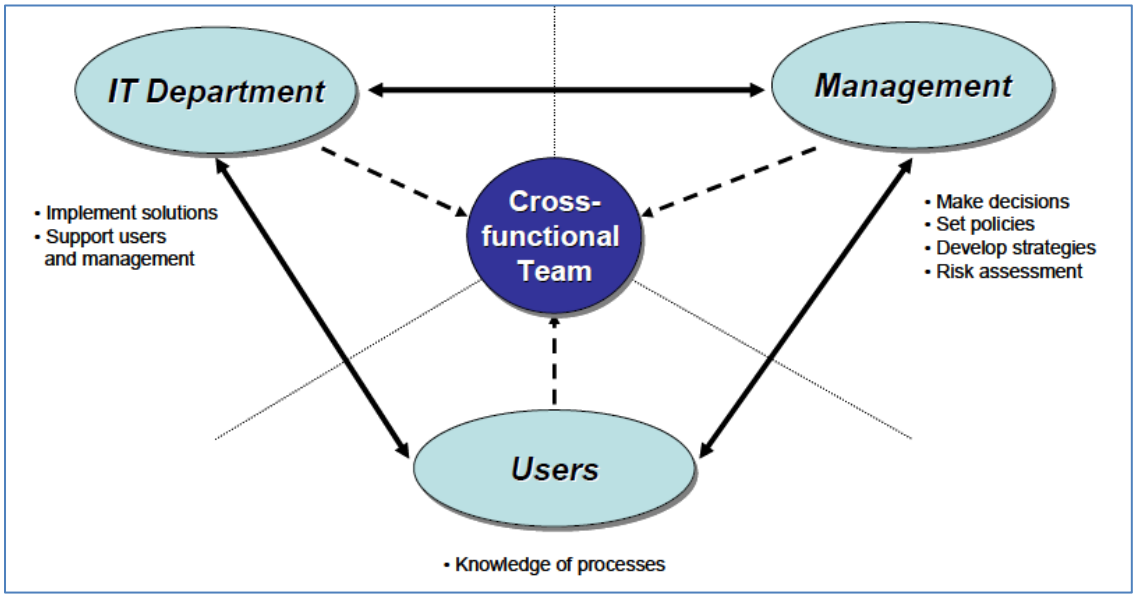

FIGURA 4-1 FACTORES DE ANÁLISIS DE IAM

FUENTE: ROYER, 2007

Así, mientras que la tecnología cambia o se puede cambiar rápidamente, los factores de organización también deben ser tomados en cuenta. Sin una correcta gestión del cambio y la implicación de las partes interesadas, es poco probable que los objetivos estratégicos y las potencialidades de los gastos para la introducción de IAM puedan alcanzarse dentro de un plazo determinado a pesar de la inversión de las empresas (Royer, 2007).

Una forma de mejorar las consecuencias negativas de la introducción de IAM es por medio de equipos multi-funcionales, integrando a todas las partes interesadas en el proceso de introducción de IAM en una organización. De esta manera, el pensamiento estratégico en toda la organización se puede activar, incluyendo todos los aspectos y requisitos, reformular el papel de IAM en la organización y superar las posibles barreras lingüísticas en la comunicación entre las partes interesadas (Royer, 2007).

Además de los diversos problemas heredados de las inversiones en TI generales, las inversiones en seguridad de TI e IAM sufren de problemas adicionales. Estos incluyen

la identificación de los posibles ingresos generados por una inversión de seguridad de TI o el nivel óptimo de las inversiones totales de seguridad. Por otra parte, las inversiones en seguridad se llevan a cabo para mitigar riesgos y para evitar posibles pérdidas. Si efectivamente los riesgos se atenúan y se evita la ocurrencia de incidentes de seguridad y pérdidas potenciales, es difícil determinar si una inversión es rentable. (Royer, 2007).

En la literatura científica se discuten varios métodos y marcos que debería ayudar a evaluar el impacto económico y el valor de las inversiones en seguridad de TI, tales como el ROSI. Sin embargo, métricas que incorporen ajustes organizaciones y factores intangibles parecen necesarias con el fin de evaluar el rendimiento de las inversiones de IAM (Royer, 2007).

Generalmente, cuando se analizan las inversiones en TI, un sistema de evaluación debe cumplir varios requisitos previos con el fin de producir un análisis suficientemente completo y exhaustivo. Los requisitos previos presentados deben ayudar a un equipo multi-funcional para construir adecuadamente un instrumento de apoyo a la decisión (Royer, 2007):

- En primer lugar, los supuestos subyacentes tomados como base para un análisis tienen que ser realistas. Esto se puede lograr mediante el análisis de otros proyectos IAM en el mismo sector utilizando sus resultados como benchmark de referencia.
- El modelado del entorno subyacente también debe tener factores de costos adicionales en cuenta, tales como costos de desarrollo, migración y otros costos relacionados con el ciclo de vida de la inversión.
- En base a los datos recogidos, es importante determinar el impacto y la interacción de los diferentes parámetros para obtener una imagen completa de los efectos de costos que están presentes en el caso analizado. Las evaluaciones utilizando métodos matemáticos financieros estáticos son incompletos. Debe

complementarse con el uso de métodos dinámicos, como la tasa interna de retorno (TIR) o el valor actual neto (VAN). Mientras que los métodos estáticos trabajan con valores medios periódicos, los métodos dinámicos examinan el valor presente real sobre el tiempo de ejecución completa de una inversión. La principal diferencia es la consideración de las entradas y salidas de dinero en efectivo y su valor actual en el tiempo. Esto da una visión más precisa sobre el desarrollo de la inversión de sólo un valor promedio.

- Aunque disponer de una colección y análisis a fondo de los datos actuales es una buena base para una evaluación, uno tiene que hacer frente a las incertidumbres en el desarrollo de los parámetros. Con el fin de pronosticar adecuadamente dichos efectos, métodos tales como el análisis de escenarios ofrecen una buena manera de evaluarlos ya que dan un rango posible para el resultado real de una inversión.
- Para apoyo a la decisión, no es posible determinar todos los datos con 100% de precisión en un plazo aceptable. Por lo tanto, es necesario un cierto grado de compromiso. Por eso para la preparación de los datos hay que tener en cuenta que la mayor parte del tiempo los resultados sólo tienen que ser lo suficientemente precisos para la toma de decisiones. Además, se deben reducir al mínimo las posibles incompatibilidades en la construcción de un sistema de evaluación.
- No solo deben tomarse en cuenta los costos directos, sino también los costos indirectos u ocultos como el costo de oportunidad en la evaluación.
- Por último, los resultados tienen que ser comprensibles para terceros, con el fin de permitir la validación de las hipótesis iniciales y para apoyar el proceso de toma de decisiones. Para lograr esto, los métodos para la evaluación de los riesgos, los costos y los beneficios, deben ser coherentes y estandarizados.

4.3.2 COSTOS

Los costos de implementar una solución IAM se pueden identificar en la inversión inicial requerida por el proyecto y las inversiones que se realizan a posteriori en los diferentes periodos que se consideren según el alcance del estudio y del modelo aplicado.

Las principales variables a cuantificar son las siguientes (North, 2008):

- Licencias de Software y mantenimiento: Varía dependiendo de la herramienta seleccionada, el contrato con el fabricante, el modelo de licenciamiento del fabricante, entre otros. Debe incluirse el costo de todos los componentes a implementar incluyendo los conectores utilizados para provisioning, módulos, etc. y sus costos de soporte en el tiempo.
- Servicios Profesionales: Puede variar dependiendo del proveedor seleccionado, la complejidad de la implementación y el tamaño de la organización entre otros. Debe incluirse todos los costos consultivos y técnicos relacionados a la implementación IAM.
- Recursos internos de Implementación: Al igual que los servicios profesionales puede variar dependiendo de la complejidad de la implementación, el tamaño de la organización y la disponibilidad de recursos. Incluye el costo de todos los recursos internos para la planificación, diseño y gestión de proyectos.
- Recursos internos de Administración, Ingeniería y Soporte de Operaciones: Varía dependiendo de la complejidad de la implementación, el tamaño de la organización y la disponibilidad de recursos. Incluye el costo de todos los recursos internos para el apoyo técnico, actualizaciones y extensiones de la solución.
- Hardware y Software base y su mantenimiento: Su estimación varía especialmente según la solución implementada y la complejidad del proyecto. Incluye el costo de todo el hardware dedicado o compartido de los diferentes ambientes aplicados (como por ejemplo Desarrollo, QA y Producción), ya sea

on-premise o cloud. Y todo el software base montado sobre ellos como sistemas operativos, bases de datos, antivirus, etc. Debe tomarse en cuenta los costos de mantenimiento y licencias en caso de tenerlos. Este ítem podría no aplicar para el caso de soluciones IDAAS.

- Otros costos: Podrían incluirse en forma parcial o total costos indirectos o de otros proyectos relacionados, como por ejemplo de ingeniería de roles.

La siguiente tabla muestra un caso de ejemplo del análisis de costos para la solución Oracle Identity Manager:

Costs	Initial	Year 1	Year 2	Year 3	Total
Software license fees (internal users), incl. adapters	830,000				830,000
Annual maintenance		182,600	182,600	182,600	547,800
Professional services — implementation	780,000	260,000	260,000		1,300,000
Internal labor — planning, design, project management	225,000				225,000
Internal labor — operations support, engineering, administration		250,000	375,000	500,000	1,125,000
Hardware costs	450,000				450,000
Total	$2,285,000	$692,600	$817,600	$682,600	$4,477,800

TABLA 4-1 EJEMPLO COSTOS OIM

FUENTE: NORTH, 2008

4.3.3 BENEFICIOS

Una solución eficaz de gestión de identidades y accesos ofrece cinco ventajas esenciales (McQuaide, 2003):

- Experiencia de usuario mejorada: Una solución IAM correctamente implementada mejorará en gran medida las experiencias de los usuarios, ayudándoles a controlar sus identidades en línea. Mejor gestión de contraseña e incluso la posibilidad crear un "círculo de confianza" en la que las organizaciones participantes pueden verificar la autenticidad de los usuarios en un modelo federado. Esto dará como resultado, usuarios satisfechos y productivos.
- Integración mejorada: Una mejor integración dentro del entorno heterogéneo de una organización es crítico. Las soluciones IAM actuarán como middleware, lo que permite a las organizaciones gestionar las identidades digitales en toda su infraestructura diversa y en expansión. Un enfoque basado en estándares jugará un papel importante en esta integración mejorada, lo que garantiza la protección de la inversión y reduciendo drásticamente el riesgo de integración personalizada.
- Plataforma multipropósito: IAM es una plataforma que sirve para consolidación de múltiples soluciones empresariales. Las organizaciones serán capaces de gestionar múltiples opciones de autenticación a partir de una única plataforma. Además, diferentes niveles de funcionalidad de autorización pueden ser parte de la mezcla. Y todo esto disponible en componentes modulares.
- Administración centralizada: Una solución IAM bien implementada permitirá a las organizaciones simplificar la gestión de identidades digitales y las políticas de seguridad con un solo modelo administrativo. Esto incluye la administración delegada de los usuarios y de autoservicio de usuario a través de diferentes aplicaciones. Esto se traduce en menores costos administrativos y una carga reducida de recursos.
- Seguridad mejorada: Las soluciones IAM asegurarán mayores niveles de seguridad para que coincida con el creciente riesgo de exposición y altos intereses implicados en las organizaciones actuales. Esto se concentra principalmente en la seguridad a nivel de aplicación. Además, una plataforma

IAM será una piedra angular de refuerzo de la seguridad, proporcionando una base de auditoría y la comunicación de las políticas.

Estos beneficios son impulsados por los drivers introducidos en la sección 2.6 y deben cuantificarse de forma correcta, lo cual no es simple debido a la gran cantidad de variables involucradas.

Las principales variables que deberían estimarse son (North, 2008):

- El aumento de la productividad de los usuarios: Este beneficio es producto de una gestión más eficiente de accesos. Como resultado los empleados nuevos y de planta permanente acceden a los recursos de información con mayor velocidad ganando tiempo productivo. Un estudio de Forrester estimo que el aprovisionamiento de accesos de un nuevo colaborador de una organización con una solución IAM puede tardar minutos, frente a varios días requeridos en el caso manual. Lo mismo aplica al cambio de contraseñas.
- Reducción de los costos laborales Help Desk: Con una solución IAM las personas son capaces de auto-gestionar sus contraseñas y accesos reduciendo considerablemente los requerimientos a Help Desk. Un estudio de Forrester estima que podría reducirse hasta un 85% la cantidad de tickets.
- Reducción de costos laborales de administración: Una organización es capaz de ahorrar con una solución IAM, trabajo administrativo dedicado a un rango de tareas y de gestión de accesos e identidades. Este trabajo se asocia con la recertificación y la estandarización.
- Reducción de costos laborales de seguridad: Tareas de seguridad y cumplimiento como el proceso de certificación periódica de accesos requiere de muchos recursos y tiempo especialmente cuando la misma se basa en procesos manuales deben repetirse para cada auditoría. Las soluciones IAM pueden automatizar y reducir costos en forma considerable.

- Reducción del costo de auditorías internas y externas: Las soluciones IAM centralizan información de identidades y accesos que puede ser relevante para diferentes procesos organizacionales, de seguridad y cumplimiento. Además, tienen la capacidad de generar reportes y vistas en forma automatizada reduciendo costos auditorías.
- Ahorro en costos de licencias: Mediante la identificación y eliminación de cuentas no necesarias, huérfanas o no permitidas, puede reducirse el costo de licenciamiento.
- Reducción del riesgo: Este beneficio será tratado en profundidad en la sección 4.4.

La siguiente tabla muestra un caso de ejemplo del análisis de beneficios para la solución Oracle Identity Manager:

Benefits	Year 1	Year 2	Year 3	Total
Incremental productivity: on-boarding new hires	1,920,000	1,920,000	1,920,000	5,760,000
Reduction in labor cost — help desk	384,000	384,000	384,000	1,152,000
Incremental productivity — password reset, calls to help desk	1,000,000	1,000,000	1,000,000	3,000,000
Labor cost savings: Access recertification, new account requests, attestation, audit assistance	640,000	640,000	640,000	1,920,000
Incremental productivity: attestation reviewers, application owners	600,000	600,000	600,000	1,800,000
Audit remediation costs avoided	250,000	250,000	250,000	750,000
Software license cost savings — unused accounts	300,000	300,000	300,000	900,000
Potential cost avoidance — security breach	675,000	675,000	675,000	2,025,000
Total	$5,769,000	$5,769,000	$5,769,000	$17,307,000

TABLA 4-2 EJEMPLO BENEFICIOS OIM

FUENTE: NORTH, 2008

4.4 EVALUACIÓN CUANTITATIVA DEL RIESGO

La evaluación cuantitativa del riesgo es una de las tareas más complejas en la evaluación de proyectos de seguridad. Además, es un requisito necesario para la mayoría de los enfoques actualmente utilizados en la evaluación de proyectos de este tipo.

4.4.1 EL RIESGO

La determinación de los requisitos de seguridad para un sistema dado y la selección de los mecanismos de seguridad apropiados son una parte de la actividad de gestión de riesgos (Theodosios, 2010).

Los pasos básicos son el análisis crítico, el análisis de vulnerabilidades, identificación de amenazas, análisis de riesgos, evaluación de riesgos, selección y aplicación de soluciones de seguridad, el desarrollo de planes de contingencia y los exámenes de la eficacia. Cuanto mejor sea el modelo de riesgo, mejores serán las decisiones de seguridad que se pueden hacer usando sus previsiones (Theodosios, 2010).

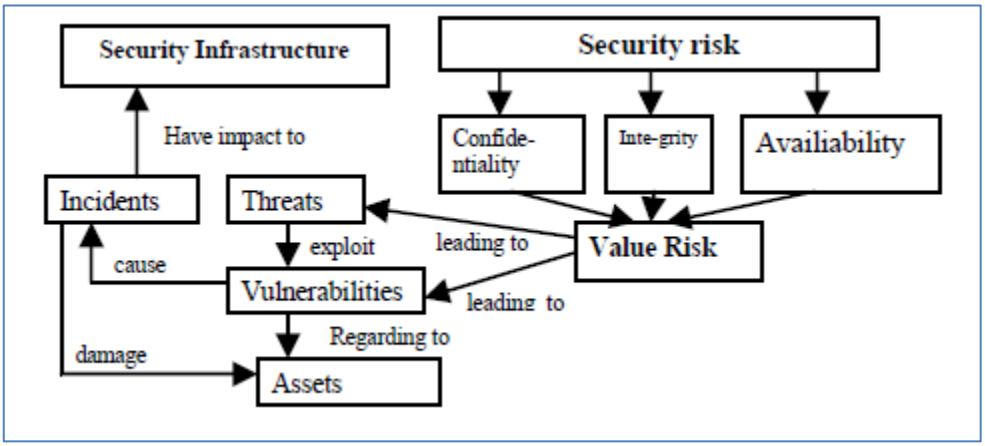

FIGURA 4-2 MODELO DE RIESGO

FUENTE: THEODOSIOS, 2010

Riesgo (R) en la forma más simple es el producto entre la probabilidad del evento P(E) y el posible daño causado, que se describe principalmente como un impacto I(E) (Theodosios, 2010).

$$R(E) = P(E) \bullet I(E)$$

Dónde:

- R(E) = riesgo de un evento.
- E = Evento.
- P = Probabilidad.
- I = Impacto.

El objetivo es reemplazar el riesgo con un riesgo aceptable (Jackson & Al-Hamdani, 2008):

Seguridad de la inversión ≤ Riesgo aceptable ≥ 0

4.4.2 CUANTIFICANDO LA EXPOSICIÓN AL RIESGO

Un método analítico simple para calcular la exposición al riesgo es multiplicar el costo proyectado de un incidente de seguridad (SLE) con su tasa anual estimada de ocurrencia (ARO). La cifra resultante se denomina exposición a la pérdida anual (ALE) (Sonnenreich, 2006).

Existen diferentes técnicas para la medición cuantitativa de la exposición al riesgo, cuyos resultados tienden a variar en la precisión. Para la mayoría de los tipos de riesgo, la exposición se puede encontrar mediante la consulta a estadísticas generadas a partir de décadas de reivindicaciones y estudios demográficos. Por desgracia, todavía no existen datos similares sobre riesgo de seguridad de la información. Por otra parte, la variabilidad de los costos de exposición puede conducir a resultados engañosos cuando se predice a partir de datos actuariales (Sonnenreich, 2006).

Si bien no existen métodos estándar para la estimación de SLE o ARO, hay tablas actuariales que dan valores estadísticos medios basados en los informes de daños en el mundo real. Estas tablas se crean a partir de los datos de investigación académica o estudios independientes (Sonnenreich, 2006).

Single Loss Expectancy o SLE es la cantidad esperada de dinero que se pierde cuando se produce un riesgo. Puede ser considerado como el costo total de un incidente asumiendo su sola aparición (ENISA, 2012).

SLE = AV x EF

Siendo AV es la evaluación del activo y EF un factor de exposición al riesgo expresado dentro de un rango de 0 a 100 por ciento del valor de un activo que será destruido por la materialización del riesgo. Un activo se define como cualquier elemento de un sistema de información que posee un valor (Theodosios, 2010).

Debido a la naturaleza específica de los incidentes cibernéticos, la mayor complejidad es tomar en cuenta todos los activos sobre los cuales tiene impacto. Por ejemplo, un

ordenador portátil robado no sólo tendrá un costo de la sustitución del propio ordenador portátil, también implicará la pérdida de productividad, pérdida de reputación, tiempo de soporte de TI y posiblemente, el costo de la pérdida de la propiedad intelectual (ENISA, 2012).

Es muy difícil obtener datos sobre el verdadero costo de un incidente de seguridad. Esto se debe a que muy pocas empresas realizan un seguimiento de los incidentes de seguridad con éxito (Sonnenreich, 2006). En la actualidad, una de las mejores fuentes de datos actuariales proviene de esfuerzos tales como la encuesta anual de negocios realizados por el Instituto de Seguridad Informática (CSI) y la Oficina Federal de Investigaciones de EE.UU. (FBI) (Sonnenreich, 2006).

El costo total de un incidente debe incluir el costo de las pérdidas directas y el costo de los daños indirectos. No existen valores universales para SLE, las variables que se incluyan dependerán de los objetivos del negocio, los valores culturales y las medidas de seguridad existentes. (ENISA, 2012).

Un costo potencialmente significativo es la pérdida de información altamente confidencial. El costo de un incidente de seguridad en este caso es el valor estimado de la propiedad intelectual que está en riesgo, el uso de modelos contables y de valoración estándar de la industria son métodos para calcularlo (Sonnenreich, 2006).

Otro costo significativo es la pérdida de productividad asociada a un incidente de seguridad. La productividad se mide a menudo usando una combinación de las evaluaciones de desempeño y métricas de ganancia/pérdida. El problema con este enfoque es que el aislamiento del impacto de la seguridad en la productividad de otros factores (tales como bajo rendimiento) es muy complejo. Una forma efectiva es medir la percepción del usuario final respecto a su productividad pérdida (Sonnenreich, 2006).

El impacto en el negocio de un fallo de seguridad se puede clasificar en las siguientes categorías (Su, 2006):

- Impacto financiero.
  - Pérdida de ventas, pedidos o contratos.
  - La pérdida de bienes tangibles.
  - Sanciones / responsabilidades legales.
  - Los gastos imprevistos.
  - Baja del precio de la acción.
- Impacto operativo.
  - Pérdida de control de la gestión.
  - Pérdida de competitividad.
  - Nuevos emprendimientos detenidos.
  - Violación de los estándares.
- Impacto relacionado con el cliente.
  - Retrasos en las entregas a los clientes o clientes.
  - La pérdida de clientes o clientes.
  - Pérdida de confianza de las instituciones clave.
  - Daño a la reputación.
- Impacto relacionado con los empleados.
  - Reducción de la moral del personal / productividad.
  - La lesión o la muerte.

A los efectos de indicadores que comparen la rentabilidad de proyectos como el ROSI, la exactitud del costo incidente no es tan importante como una metodología coherente para calcular y reportar el costo. Por lo tanto, la atención debe centrarse en los factores de costo que son independientemente medibles y se correlacionan directamente con la gravedad de la incidencia de seguridad (Sonnenreich, 2006).

Annual Rate of Occurrence o ARO es una medida de la probabilidad de que un riesgo ocurra en un año (ENISA, 2012).

Una vez más, estos datos son una aproximación y puede depender de muchos factores. La ARO también está en función de las medidas de seguridad existentes, la frecuencia anual de un ataque exitoso disminuirá significativamente después de la implementación de contramedidas eficaces (ENISA, 2012).

Annual Loss Expectancy o ALE es la pérdida monetaria anual que se puede esperar de un riesgo específico en un activo específico (ENISA, 2012). Se calcula de la siguiente forma:

ALE = ARO * SLE

4.4.3 CUANTIFICANDO EL RIESGO MITIGADO

La determinación de los beneficios de reducción del riesgo de un dispositivo de seguridad es tan difícil como la medición de la exposición al riesgo. La mayoría de los problemas se derivan del hecho de que la seguridad no crea directamente nada tangible, sino que evita pérdidas. Una pérdida que ha sido evitada, es una pérdida que probablemente no se conozca (Sonnenreich, 2006).

Un argumento utilizado para justificar las soluciones de seguridad es definir un simple porcentaje de mitigación de riesgo. Por desgracia, hay una serie de graves problemas con esta lógica (Sonnenreich, 2006):

- Los riesgos no son aislables.
- Las soluciones de seguridad no funcionan de manera aislada.
- Las soluciones de seguridad rara vez se implementan para ser tan eficaces como sea posible debido a un impacto inaceptable en la productividad.
- Las soluciones de seguridad se vuelven menos eficaces con el tiempo.

Un mejor enfoque es llevar a cabo una evaluación de la seguridad y realizar una "puntuación" de la evaluación basada en algún algoritmo consistente. Esta puntuación puede representar la cantidad de riesgo que se está mitigado. Mediante la evaluación de la mitigación de riesgos en el contexto de la seguridad global, se evitan los dos problemas de aislamiento mencionado anteriormente. Una buena evaluación también capturar el impacto de las decisiones de implementación tomadas en aras de la facilidad de uso y la productividad. Del mismo modo, un buen algoritmo de puntuación tendrá en cuenta el impacto sobre la eficacia de la solución (Sonnenreich, 2006).

Al evaluar una solución de seguridad, la evaluación puede llevarse a cabo como si la solución ya estuviera en su lugar. La diferencia entre esta puntuación y la real es la cantidad de riesgo que está siendo mitigada por la solución (Sonnenreich, 2006).

La precisión de la puntuación como una medida del riesgo mitigado depende de la calidad del algoritmo de evaluación y puntuación. Siguiendo las directrices de evaluación publicados por los grupos de establecimiento de normas tales como Security Forum (ISF), National Institute of Standards in Technology (NIST) y el International Standards Organization (ISO) dará lugar a la creación de una buena evaluación. Las redes neuronales artificiales se pueden utilizar para crear particularmente buenos algoritmos de puntuación.

4.5 ENFOQUES

Existen diferentes modelos y enfoques a la hora de evaluar proyectos de seguridad informática planteados por diferentes instituciones y autores. A continuación, se presentan algunos de los más significativos y reconocidos.

4.5.1 ENISA

La European Union Agency for Network and Information Security (ENISA) trabaja para desarrollar consejos y recomendaciones sobre buenas prácticas de seguridad de la información. Se ayuda a los Estados miembros de la UE en la aplicación de la legislación pertinente y trabaja para mejorar la resistencia de la infraestructura de información y redes crítica de Europa (ENISA, 2012).

ENISA propone un modelo llamado Return on Security Investment (ROSI) combina la evaluación cuantitativa de los riesgos y el costo de la aplicación de contramedidas de seguridad para este riesgo (ENISA, 2012).

Al final, se compara la ALE con el ahorro de pérdida esperada:

$$ROSI = \frac{Monetary\ loss\ reduction - Cost\ of\ the\ solution}{Cost\ of\ the\ solution}$$

La implementación de una solución de seguridad eficaz disminuye la ALE, es decir cuanto más más eficaz es una solución más reducida es la ALE. Esta reducción de la pérdida monetaria puede ser definida por la diferencia de la ALE sin la solución de seguridad frente al ALE modificada (mALE) por la implementación de la solución de seguridad.

$$ROSI = \frac{ALE - mALE - Cost\ of\ the\ solution}{Cost\ of\ the\ solution}$$

Lo que también es igual a la relación de la mitigación de la solución aplicada a la ALE:

$$ROSI = \frac{ALE * mitigation\ ratio - Cost\ of\ solution}{Cost\ of\ solution}$$

En el modelo propuesto por ENISA se basa en 3 variables, la pérdida estimada potencial o ALE, la mitigación del riesgo estimado y el costo de la solución. De todas ellas el costo de la solución es más fácil de predecir, sin embargo la estimación de la cantidad de dinero ahorrado de pérdidas que no pueden suceder es una tarea difícil que, en el mundo real, requiere algo más que la aplicación directa de fórmulas sencillas.

Estas aproximaciones son a menudo sesgadas por la percepción del riesgo y el cálculo de ROSI puede ser manipulado fácilmente para servir a los intereses del usuario o para justificar una decisión en lugar de iluminarla. La precisión de los datos estadísticos utilizados en el cálculo de ROSI es esencial.

Es una buena práctica para estas evaluaciones extrapolar a partir de datos históricos de la organización sobre los incidentes, en vez de confiar en estudios de proveedores.

4.5.2 GORDON

Lawrence A. Gordon y Martin P. Loeb desarrollaron un modelo económico que determina la cantidad óptima a invertir para proteger a un conjunto específico de información. El modelo es aplicable a las inversiones relacionadas con diversos objetivos de seguridad de la información, tales como la protección de la

confidencialidad, disponibilidad, autenticidad, no repudio, y la integridad de la información (Gordon & Loeb, 2002).

El modelo tiene en cuenta la vulnerabilidad a una violación de la información y la pérdida potencial que produce tal infracción. Se muestra que, para una pérdida potencial dada, una empresa no necesariamente debe centrar sus inversiones en información con mayor vulnerabilidad, dado que los conjuntos de información extremadamente vulnerables pueden ser excesivamente costosos para proteger.

El análisis sugiere que, para maximizar el beneficio esperado de la inversión para proteger la información, una empresa debe gastar sólo una pequeña fracción de la pérdida esperada debido a un fallo de seguridad.

Los autores suponen un tomador de decisiones neutral al riesgo y un modelo de un solo periodo, es decir que todas las decisiones y los resultados se producen de forma instantánea.

Una de las principales conclusiones del trabajo es:

> "the optimal amount to spend on information security never exceeds 37% of the expected loss resulting from a security breach (and is typically much less that 37%). Hence, the optimal amount to spend on information security would typically be far less than even the expected loss from a security breach" (Gordon & Loeb, 2002).

Esta sin embargo ha sido criticada por otros autores como Jan Willemson, quien considera que dicha regla solo se cumple bajo ciertos supuestos y que el modelo puede ser extendido (Willemson, 2006).

En este modelo cada activo se asocia con pérdidas monetarias λ en caso de que ocurra una brecha de seguridad. Estas pueden deberse a un fallo de seguridad en relación con la confidencialidad, integridad o denegación de servicios. El valor de esta variable

normalmente dependerá de la utilización de la información y cambia con el tiempo, por simplicidad en este modelo se toma como una cantidad fija según lo estimado por la empresa (Gordon & Loeb, 2002).

La probabilidad de un intento de violación del conjunto de información dada se denota por **t ∈ [0,1]**, y se denomina probabilidad de amenaza. Se hace la simplificación de asumir que existe una única amenaza para un conjunto de información determinado (Gordon & Loeb, 2002). El parámetro **v** denota la probabilidad de que sin seguridad adicional la brecha ocurra y genere la pérdida **λ**. Como **v** es una probabilidad, entonces **v ∈ [0,1]**. Por lo tanto, el producto **vt λ** representa la pérdida esperada asociada a un activo.

Por supuesto, las empresas pueden y deben invertir en seguridad de la información. En general, se podría esperar que una firma tenga más influencia sobre la vulnerabilidad de un conjunto de información que sobre las amenazas a dicha información.

A los efectos de este modelo, se supone de forma simplificada que las empresas pueden influir en la vulnerabilidad de un conjunto de información mediante la inversión en seguridad de la información, pero la empresa no puede invertir para reducir la amenaza. Por lo tanto, se fija la probabilidad de amenaza en **t > 0**, y se centran en la elección de la firma del nivel de inversión para reducir la vulnerabilidad. Como la probabilidad de amenaza se mantiene constante, para simplificar la notación se define **L = t λ**. L se define como la pérdida potencial o esperada asociada con el conjunto de información.

Sea **z > 0,** denotan la inversión monetaria en seguridad para proteger una información dada. Por lo tanto, **z** se mide en las mismas unidades utilizadas para medir la pérdida potencial **L**. El propósito de la inversión **z** es disminuir la probabilidad de que el conjunto de información será violado.

S (z,v) denota la probabilidad de que un conjunto de información con la vulnerabilidad **v** será violada, condicionada a la realización de una amenaza y dado que la empresa ha

realizado una inversión de seguridad de la información **z** para proteger esa información. Nos referimos a la función **S (z,v)** como la función de probabilidad violación de la seguridad y de su valor en un determinado nivel de **z** y **v** como la probabilidad de fallo de seguridad. Como es común en casi todos los modelos económicos, se hace una abstracción de la realidad y se asume que las funciones postuladas son lo suficientemente robustas y confiables.

La naturaleza de esta problemática lleva a considerar los siguientes supuestos referidos a **S (z, v):**

A1: S (z, 0) = 0 para todo **z**. Es decir, si el conjunto de información es completamente invulnerable, entonces seguirá siendo perfectamente protegido por cualquier cantidad de inversión en seguridad de la información, incluyendo una inversión cero.

A2: Para todo **v, S (0, v) = v**. Es decir, si no hay inversión en seguridad de la información, la probabilidad de un fallo de seguridad, condicionado a la realización de una amenaza, es la información del conjunto vulnerabilidad inherente, **v**.

A3: Para todos **v ∈ (0, 1)**, y todos los **z**, **Sz (z, v) <0 y Szz (z, v) > 0**, donde **Sz** denota la derivada parcial con respecto a la **z** y **Szz** denota la derivada parcial de **Sz** con respecto a **z**. Es decir, como la inversión en aumentos de seguridad, la información se hace más segura, pero a un ritmo decreciente. Por otra parte, se supone que para todo **v ∈ (0, 1)**, **lim S (z,v)** → **0**, cuando **z** → ∞, por lo que mediante la inversión suficiente en seguridad, la probabilidad de un fallo de seguridad, **t** veces **S (z,v)**, se puede acercar arbitrariamente a cero.

El beneficio esperado de una inversión, denotado como **EBIS,** es igual a la reducción de la pérdida esperada de la firma atribuible a la seguridad extra. Es decir:

$$EBIS(z) = [v - S(z, v)]\, L.$$

En la formula anterior, EBIS está escrito como una función de z, ya que la inversión en seguridad de la información es la única variable de decisión de la empresa (v y L son parámetros del conjunto de información). Los beneficios netos esperados de una inversión en seguridad de la información, que se denota ENBIS es igual EBIS menos el costo de la inversión:

$$ENBIS(z) = [v - S(z, v)]\, L - z.$$

Para centrarse en el efecto de la vulnerabilidad, se denota la inversión óptima como **z* (v)**. Se observa que a partir de A1, si un conjunto de información es completamente invulnerable, la inversión óptima en seguridad de la información se hace igual a cero, es decir, **z* (0) = 0**. Se supone que el conjunto de información en estudio no es ni completamente vulnerable ni completamente invulnerable, es decir, **0 < v < 1**.

A partir de la asunción A3, **S (z,v)** es estrictamente convexa en **z**, por lo tanto ENBIS es estrictamente cóncava en **z**. Por lo tanto, un máximo z* > 0 se caracteriza por la condición de primer orden:

$$-S_z(z^*, v)\, L = 1.$$

Donde el lado izquierdo representa los beneficios marginales de la inversión en seguridad y el lado derecho representa el costo marginal dela inversión. Por lo tanto, se debe invertir en la seguridad sólo hasta el punto en el que el beneficio marginal es igual al costo marginal.

Recordemos que el valor de un conjunto de información se mide por la pérdida potencial asociada. Se deduce de la última ecuación, que para un nivel dado de vulnerabilidad, la cantidad óptima de inversión, **z***, aumenta con el aumento en el valor de la información establecida.

Este nivel óptimo de inversión en seguridad de la información se ilustra en la figura 4-3. Los beneficios de una inversión en seguridad de la información, **EBIS (z)**, comienzan en cero y se acercan a vL medida que aumenta el nivel de inversión. Los costos de la inversión se dan por **z**, la línea de 45 º en la figura.

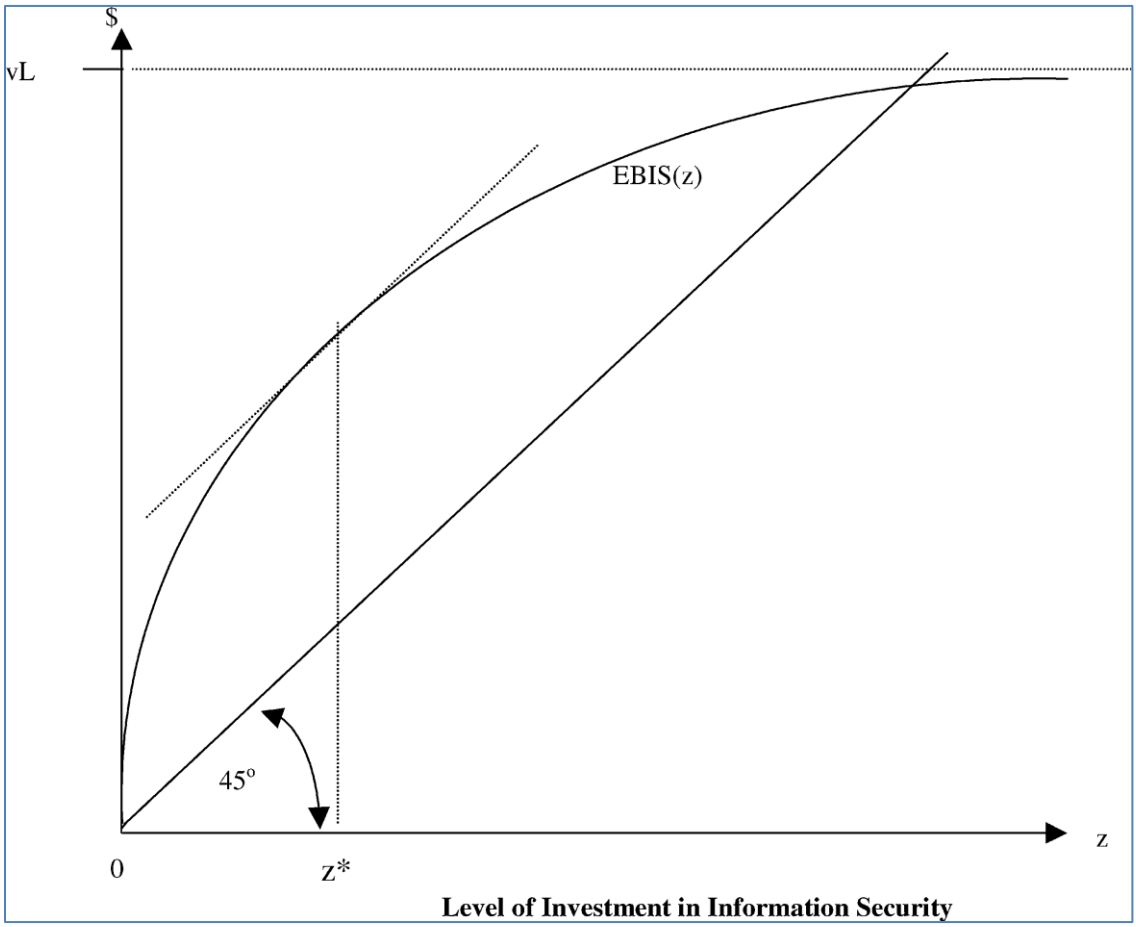

FIGURA 4-3 NIVEL ÓPTIMO DE INVERSIÓN DE SEGURIDAD DE LA INFORMACIÓN

FUENTE: GORDON Y LOEB, 2002

La inversión óptima, z*, es donde se maximiza la diferencia entre beneficios y costos, y en ese punto la tangente a **EBIS (z*)**, tiene una pendiente, en representación de los beneficios marginales, igual al costo marginal de uno. Se observa que la cantidad

óptima de inversión, **z***, es inferior a **vL**, la pérdida que se esperaría en la ausencia de cualquier inversión en seguridad.

4.5.3 BUTLER

Shawn Butler presenta un método de análisis de costo-beneficio llamado SAEM que permite comparar diseños alternativos de seguridad. El objetivo de utilizar SAEM es ayudar a los profesionales de la seguridad y a las partes interesadas del sistema de información a evaluar y decidir si su inversión es consistente con los riesgos esperados y es la de mayor rentabilidad (Butler, 2002).

SAEM se basa en una evaluación del riesgo y el beneficio cuantitativo, en el que un analista o investigador lleva a cabo entrevistas estructuradas de TI y los administradores de seguridad para obtener los datos iniciales. La organización revisa cuidadosamente los resultados de cada paso antes de pasar al siguiente. De ser necesario se pueden revisar los datos y supuestos originales. (Butler, 2002)

SAEM depende de una evaluación de riesgos y una primera evaluación de la eficacia de la tecnología de seguridad. Estas evaluaciones dependen de varios supuestos, tales como:

- La organización ha establecido políticas y procedimientos de seguridad que son suficientes y robustos para las operaciones del negocio.
- Los productos de seguridad se han instalado, configurado y mantenido correctamente
- Los ataques dan lugar a resultados predecibles y varianzas.

Estas evaluaciones pueden variar entre los gerentes de seguridad en base a su experiencia, conocimientos y el medio ambiente del sistema de información.

SAEM proporciona un marco para analizar cómo sus supuestos afectan las decisiones de diseño y un mecanismo para determinar la sensibilidad de las decisiones a los supuestos.

SAEM consta de cuatro fases:

1. Una evaluación de los beneficios de la tecnología.
2. Una evaluación de los efectos de las tecnologías de seguridad en la mitigación de riesgos.
3. Una evaluación de la cobertura.
4. Un análisis de costos.

Los pasos 3 y 4 se pueden hacer en paralelo.

Respecto al paso 1, el beneficio o la eficacia de una tecnología de seguridad es una evaluación de qué tan bien la tecnología mitiga un riesgo. Una tecnología puede mitigar el riesgo de dos maneras, prevenir un ataque que se produzcan o reducir las consecuencias de un ataque con éxito. Las tecnologías de seguridad reducen la consecuencia de un ataque porque el personal de seguridad detecta un ataque, lo que les da la oportunidad de que dejen un ataque en curso o identificar el daño. Por lo tanto, las tecnologías de seguridad se clasifican en categorías en función de su efecto sobre el riesgo.

Después de la clasificación de las tecnologías de seguridad, el siguiente paso en la evaluación de los beneficios de las tecnologías de seguridad es identificar qué tecnologías mitigan cada una de las amenazas.

Quizás la pieza más difícil y controvertida de la evaluación del beneficio es cuantificar la efectividad de las contramedidas. A pesar de que los administradores de seguridad reconocen que las métricas de efectividad precisas son imposibles de conseguir, son capaces de proporcionar estimaciones aproximadas. La eficacia de las tecnologías varía a través de las organizaciones. Por lo tanto, las estimaciones pueden no reflejar la

eficacia real de una tecnología de seguridad, pero hasta que se hagan mejores aproximaciones, los administradores utilizan estas estimaciones para asignar los recursos de seguridad.

La fase 2 en el uso SAEM es evaluar el efecto de cada tecnología tiene la seguridad en la mitigación de riesgos. Es necesario entonces determinar el impacto en la reducción del riesgo. Dado que cada tecnología de seguridad reduce el riesgo de varias amenazas, la comparación de las tecnologías requiere una evaluación general (Butler, 2002).

La decisión de seleccionar una tecnología sobre otra podría estar basada en los principios de diseño de ingeniería, más que estrictamente una evaluación de la eficacia. Además, debe evaluarse en el paso 3 que las tecnologías seleccionadas cubran todos los requisitos técnicos de forma satisfactoria.

El paso 4 es un análisis de los costos del proyecto. El administrador de seguridad puede seleccionar una tecnología también sobre la base del costo, tales como la compra, la formación, el mantenimiento y los costos de instalación. Estos dependen de arquitecturas de sistemas y diseños altamente detallados por lo que es casi imposible determinar los costes de forma aislada a partir de un diseño particular.

Dado que la determinación de los costos de tecnología de seguridad puede requerir una cantidad significativa de tiempo, SAEM dirige la atención en primer lugar a las tecnologías que proporcionarán el mayor beneficio. El gerente de seguridad no pierde el tiempo en las tecnologías de seguridad que proporcionan poco valor.

El autor finalmente recomienda la realización de un análisis de sensibilidad para mitigar los efectos de los errores de estimación de los pasos descriptos.

4.5.4 SONNENREICH

Wes Sonnenreich presentó un modelo para calcular el valor financiero de los gastos de seguridad y las técnicas necesarias para completarlo. El objetivo es poder responder a la pregunta fundamental "Which of these options gives me the most value for my money?" (Sonnenreich, 2006).

El autor plantea la siguiente fórmula para calcular el ROSI de un proyecto:

$$ROSI = \frac{(\text{Risk Exposure} \bullet \%\ \text{Risk Mitigated}) - \text{Solution Cost}}{\text{Solution Cost}}$$

Considerando que:

$$\textit{Risk Exposure} = \text{ALE} = \text{SLE} * \text{ARO}$$

A diferencia de ENISA el modelo de Sonnenreich otorga mayor detalle respecto a la evaluación cuantitativa del riesgo.

En cuanto a la cuantificación del costo de la solución, el autor especifica que no solo deben tomarse en cuenta los precios del producto sino también los costos internos asociados. La productividad es importante, ya que la seguridad viene casi siempre a costa de la comodidad. La mayoría de las soluciones de seguridad pueden crear obstáculos a los diferentes procesos organizacionales o incluso incrementar la productividad. Este impacto en la productividad se puede medir de nuevo ejecutando los estudios de productividad utilizados para estimar la exposición al riesgo.

Según el autor para las inversiones a largo plazo, la mayoría de los profesionales financieros querrán tener en cuenta el valor temporal del dinero. El dinero gastado en la inversión es dinero que podría haber sido invertido en otros lugares. Este costo "ajustado" se llama el valor actual neto o VAN.

Uno de los factores importantes en el cálculo del Valor Actual Neto es la "tasa de descuento" que es la tasa estimada de retorno que se puede conseguir poniendo el dinero en alguna otra forma de inversión. Otra interesante pieza de información puede obtenerse a través de averiguar la tasa de descuento necesaria para que resulte en un valor presente neto de cero. Esto se conoce como la Tasa Interna de Retorno o TIR y básicamente lo que califica es si la inversión es rentable. En general, tener una TIR superior a la tasa de descuento es una buena señal.

En la mayoría de los casos, el valor actual neto y la tasa interna de retorno son mejores indicadores que un simple cálculo retorno de la inversión. Pero si no se puede predecir con exactitud el momento o la magnitud de los costos y beneficios durante la vida útil de la inversión, obtendrá resultados engañosos.

Para el autor, el problema de usar el valor actual neto de las inversiones en seguridad es que la precisión es bastante crítica para obtener resultados comparativamente significativos. Mientras ROSI no tiene en cuenta el valor temporal del dinero, por lo menos puede proporcionar cifras comparables con los datos inexactos pero consistentes. Esto puede ser un caso en el que es mejor ser significativo que preciso.

4.5.5 MIZZI

Para Adrian Mizzi, una organización no debería gastar más en su seguridad de la información que el costo total de la parte de los activos de información que se puede perder a través de un incidente de cualquier tipo (Mizzi, 2010).

En este trabajo se introduce el término "Return on Information Security Investment" (ROISI), que está construido sobre los términos retorno de inversión (ROI) y retorno de inversión de seguridad (ROSI) que se utilizan comúnmente (Mizzi, 2010). A continuación, se detalla el modelo.

El departamento de TI compra licencias y en general gasta dinero en arreglar las vulnerabilidades de los sistemas. La variable F se define como el costo anual para corregir las vulnerabilidades mediante la aplicación de los parches del sistema o actualizaciones para el sistema que contiene la información a proteger.

Una empresa normalmente invertirá un costo de una vez B para poner en práctica mecanismos de defensa que protegen los activos de TI de posibles amenazas. Es muy posible que impliquen un costo anual de mantenimiento M.

El gasto total anual de seguridad ES, para el primer año, de una organización está dado por:

$$E_S = F + B + M. \quad (1)$$

En los años siguientes la organización gasta un total de:

$$E_S = F + M. \quad (2)$$

Cada vez que un sistema es explotado, hay una probabilidad de que haya una pérdida inmediata de ingresos L, que se produce ya sea por las interrupciones del sistema, terceros o empleados internos.

Existen dos componentes de la pérdida. La primera es una función del tiempo t que el sistema estaba abajo y la segunda es la suma global de dinero LI, que se pierde inmediatamente. Para el alcance de este documento se asume que la pérdida variable es una fracción del valor de los activos de información en juego, que se cita cada año.

La variable LT (pérdida total anual) se define de tal manera que:

$$L_T = L_I + I * t/365 \quad (3)$$

Donde LI es la pérdida instantánea, I es el valor de los activos de información en juego, t es el tiempo, en días, que el sistema no está disponible para el servicio.

Las organizaciones también pueden modelar la pérdida de forma diferente como A(t) (pérdida de disponibilidad), una función que describe la forma en que los ingresos de los activos de información en juego se pierden durante el período de tiempo t , durante el cual hay un corte.

$$L_T = L_I + A(t). \quad (4)$$

Con posterioridad al incidente y durante el tiempo que la información se pierde o nuevos ingresos no se materialicen, el personal de TI intentará reparar el sistema ya sea mediante la restauración de copias de seguridad, reemplazo de equipos o mediante la realización de cualquier operación para restaurar el sistema a el estado original. Cualquiera que sea el método elegido, hay un costo financiero para reconstruir R el sistema para una operación tal y por lo tanto la ecuación anterior se modifica para:

$$L_T = L_I + A(t) + R. \quad (5)$$

Con frecuencia, el costo laboral hora-hombre R será el costo dominante y por lo tanto la ecuación puede ser reescrita como:

$$L_T = L_I + A(t) + R(t), \quad (6)$$

Donde R(t) es una función que describe el dinero gastado anual para reconstruir pérdidas activos de TI durante el tiempo que el sistema estaba abajo. Con frecuencia, el tiempo durante el cual el sistema está abajo esta dictado por el acuerdo de nivel de servicio o SLA de la organización. Típicamente, para un tiempo t más bajo mayor es el costo del SLA.

El objetivo de cualquier programa de seguridad de la información es proteger los activos de información de una manera rentable. De las ecuaciones (1) y (6), el proyecto de seguridad es viable si:

$$E_S < L_T, \quad (7)$$

O alternativamente:

$$(F + B + M) < (L_T + A(t) + r(t)). \quad (8)$$

El análisis presentado hasta el momento se centró en las vulnerabilidades intrínsecas al sistema. La posibilidad de un ataque no fue un factor estudiado. Un sistema que no esté protegido por mecanismos de defensa y que tienen numerosas vulnerabilidades aún no está en peligro de ser dañado si no hay amenazas. Para completar el modelo se introduce la noción de amenazas.

La variable costo anual de brecha o CTB , se define de tal manera que:

$$CTB = C_D + C_V, \quad (9)$$

Donde C_D es el costo anual para entrar en los mecanismos de defensa y el C_V es el costo anual para explotar las vulnerabilidades en el sistema. Se aprecia que esta cifra es muy difícil de calcular.

El daño anual D realizado a los mecanismos de defensa por los ataques, es el que se produce en los mecanismos de defensa D_D y la infraestructura subyacente D_I que aloja los activos de información, pero no los propios activos de información. Este daño no necesariamente resulta en la pérdida de información, pero tendrá que ser reparado lo mismo. El costo de la reparación de este modo se denota por:

$$D = D_D + D_I. \quad (10)$$

De hecho DD y DI son funciones probabilísticas. La desigualdad dada en la ecuación (8) puede ser modificado de manera que la seguridad de la información del proyecto es viable si:

$$(F + B + M) < (L + A(t) + r(t) + D). \quad (11)$$

Se asume que un hacker u otro usuario malicioso no lograrán romper o abusar de un sistema a menos que gaste más de lo que cuesta construir los mecanismos de defensa. Así, los mecanismos de defensa deben ser construidos de tal manera que el costo de romperlos es más de lo que cuesta construirlos:

$$CTB > (F + B + M). \quad (12)$$

Del mismo modo, se espera que una entidad malintencionada está dispuesta a pagar cerca pero no más que la pérdida instantánea LI, si se tiene la intención de robar datos o posiblemente LI + A(t) si tiene la intención de dañar la reputación de una organización. El CTB se ve influenciado por la motivación de atacar el sistema:

$$CTB < (L_I + A(t)). \quad (13)$$

La percepción del valor de la información para el atacante puede ser de hecho mayor que la percepción de valor del propietario de la información, en cuyo caso la motivación puede seguir siendo alta incluso con un alto CTB.

El modelo ROISI, que se muestra en la figura 4-4 ilustra la relación entre las variables expuestas anteriormente y resalta la importancia de obtener estimaciones de las cantidades marcadas por "Viabilidad del gasto", "La motivación para ataque" y "efectividad de un ataque". Estos conceptos forman una tríada, representado por las diversas desigualdades que se presentaron.

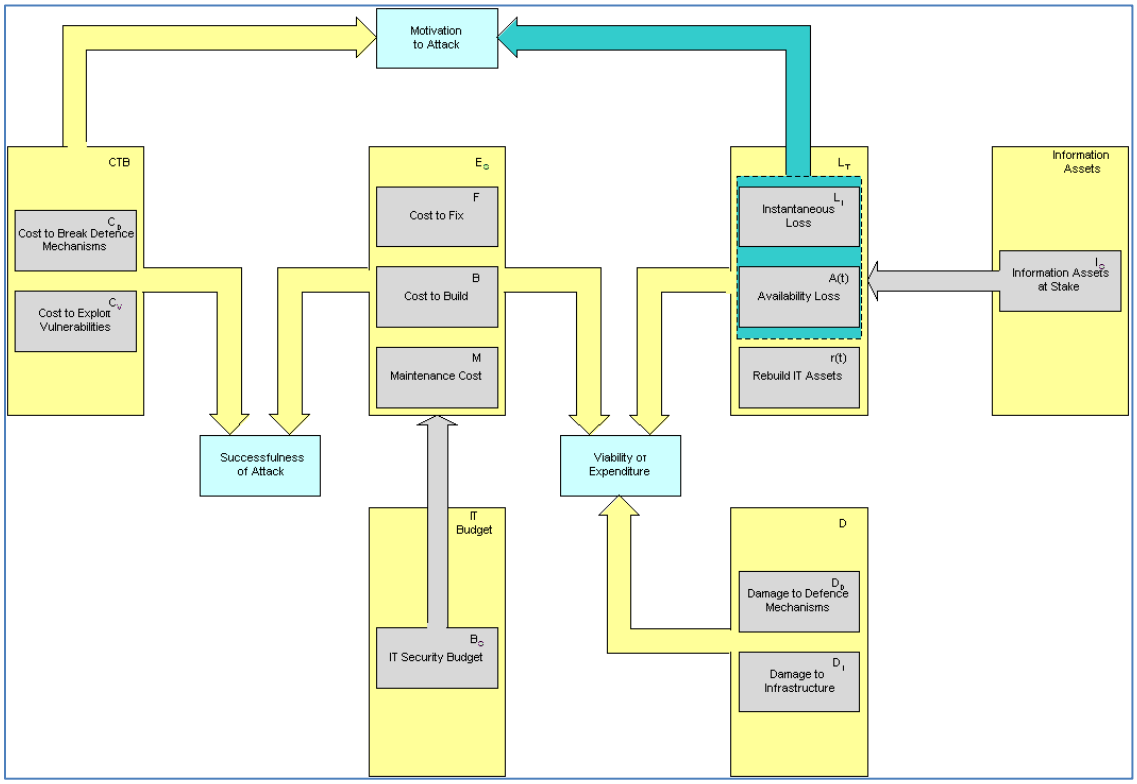

FIGURA 4-4 MODELO ROISI

FUENTE: MIZZI, 2010

4.5.6 CREMONINI

En este modelo, los autores sugieren que al evaluar inversiones en tecnología de seguridad, el índice de retorno de la inversión debe ir acompañado de un índice correspondiente destinado a medir la conveniencia de ataques. Se propone el indicador Return On Attack (ROA), especialmente aplicable en situaciones donde diferentes tecnologías se combinan o cuando una solución de seguridad degrada su eficiencia con el tiempo (Cremonini & Martini, 2005).

Los beneficios de la tecnología de seguridad dependen de la frecuencia esperada de un ataque, cual es el daño probable y la eficacia de la tecnología de seguridad es en la mitigación de los daños causados por los ataques. Para los autores, las evaluaciones basadas en rendimiento de la inversión sufren de muchas debilidades y son intrínsecamente incompletas.

El índice ROA refleja el impacto medio esperado de una solución de seguridad en el comportamiento de los atacantes. El objetivo es identificar la solución que mejor pueda disuadirlos en sus intentos de intrusión, un aspecto que el análisis del ROI estándar no identifica claramente.

En el análisis, se empieza con cálculo típico de un índice ROI, basado en la evaluación de la ALE, la eficiencia esperada de la adopción de la solución de seguridad y los costos correspondientes:

$$\text{ROI} = \frac{ALE_{beforeS} - ALE_{afterS}}{cost\ of\ security\ measure} = \frac{EFF * CI - CS}{CS} = \frac{EFF * CI}{CS} - 1$$

La relación se puede derivar a partir de una medida de seguridad S y la estimación de ALE antes de S, que representa los costos anuales relacionados con los incidentes de seguridad que la medida de seguridad S va a mitigar. Llamaremos CI a estos costos anuales, de modo que ALE antes de S es igual a CI. Estos costos pueden incluir las pérdidas tangibles e intangibles, tales como los costos de recuperación de datos, en el primer caso, o daños a la reputación, en el segundo.

El término ALE luego de S está compuesto por dos partes. La primera es el costo anual que la firma sufre de incidentes de seguridad que medida de seguridad S debería haber sido capaz de evitar, pero en realidad no lo hizo. Este término se calcula como la diferencia entre las pérdidas antes de la adopción de la medida de seguridad S, es decir ALE antes de S, y la fracción de estas pérdidas evitadas debido a la adopción de S. Esta fracción llamada EFF, con EFF incluido en [0, 1], representa la eficiencia de la medida

de seguridad S y el ahorro en las pérdidas son entonces representados por la EFF * ALE antes de S. La segunda parte es el costo de la medida de seguridad S, llamado CS.

La motivación de la hipótesis es que dicho índice, ofrece una caracterización parcial de las inversiones en tecnología de seguridad de la información, ya que carece de considerar explícitamente los intereses de los atacantes. Suponiendo que la pérdida de la organización es igual a la ganancia atacante, lo cual es una simplificación poco realista. Además, el costo de un ataque no puede estar directamente relacionado con el costo de la medida de seguridad.

El índice de retorno de la inversión debe ir acompañado de un índice correspondiente (ROA) destinado a medir cuales son los cambios de conveniencia del atacante con la adopción de la misma medida de seguridad S. Este índice es definido como la ganancia que el atacante espera a partir de un ataque exitoso sobre las pérdidas debido a la adopción de la medida de seguridad S. En esta definición del ROA, la ganancia esperada debido a un ataque exitoso es el término independiente que se supone que es constante. El término dependiente es el costo del ataque que puede variar.

Es importante destacar que el ROA es la evaluación que hace una organización acerca de la efectividad de una medida de seguridad para desalentar una cierta clase de intentos de intrusión asumiendo algunos perfiles de posibles atacantes. Esto significa que no se corresponde exactamente al ROI calculado por un atacante específico en la evaluación de su inversión. Las dos perspectivas no son necesariamente lo mismo, aunque ambas en gran medida están basadas en las percepciones acerca de los costos, las ganancias y eficiencia.

Al igual que en el cálculo del ROI, se llama GI a la ganancia esperada del incidente, CA el costo percibido por el atacante cuando tenga éxito y EFF la eficiencia del atacante violar las medidas de seguridad.

A continuación, se puede afirmar que:

$$\text{ROA} = \frac{gain\ from\ successful\ attack}{cost\ before\ S + loss\ caused\ by\ S} = \frac{GI}{CA_{beforeS} + (CA_{afterS} - CA_{beforeS})}$$

$$= \frac{GI}{\frac{CA}{EFF'_{beforeS}} + (\frac{CA}{EFF'_{afterS}} - \frac{CA}{EFF'_{beforeS}})} = \frac{GI}{\frac{CA}{EFF'_{afterS}}}$$

Se hace la siguiente hipótesis, la eficiencia del atacante para violar las medidas de seguridad corresponde a la incapacidad de las medidas de seguridad para impedir sus ataques. Por lo tanto, para que una medida de seguridad S con eficiencia EFF, la eficiencia del atacante EFF prima es igual a 1- EFF.

A continuación, se correlaciona ROA con la eficiencia EFF de S:

$$\text{ROA} = \frac{GI}{\frac{CA}{EFF'}} = \frac{GI}{\frac{CA}{1-EFF}} = \frac{GI}{CA} * (1 - EFF)$$

Desde el punto de vista del atacante, ROA debe aprovecharse al máximo. En consecuencia, desde el punto de vista de la defensa, con el objetivo de evaluar la mejor inversión en medidas de seguridad, el ROA debe ser minimizado.

4.5.7 BODIN

El autor propone el uso de la variante de AHP (Analytic Hierarchy Process) para determinar la asignación óptima de un presupuesto para mantener y mejorar la seguridad del sistema de información de una organización. El árbol AHP puede implicar costos y/o beneficios. (Bodin & Loeb, 2005).

Bajo el método de calificaciones, la organización enumera los criterios y subcriterios que deben utilizarse y emplea el AHP para determinar los pesos para cada uno de estos criterios y subcriterios. Posteriormente, la organización evalúa las propuestas alternativas para mantener y mejorar su seguridad de la información del sistema.

Estas alternativas se evalúan individualmente contra cada criterio y subcriterio utilizando niveles de intensidad (logro) que miden la capacidad de una alternativa de cumplir un criterio o subcriterio particular.

Una puntuación se determina para cada alternativa. La alternativa perfecta tiene una puntuación de 1,0. La puntuación de una alternativa siempre se encuentra entre 0 y 1,0 y cada puntuación se determina de forma independiente de las puntuaciones de las otras alternativas.

El método clasificaciones se lleva a cabo de la siguiente forma:

1. Se definen los criterios, subcriterios, y los niveles de intensidad para los criterios o subcriterios.
2. Se dibuja el árbol de AHP que contiene los criterios, subcriterios, y niveles de intensidad.
3. Se determinan los pesos que se utilizarán para los criterios, subcriterios, y los niveles de intensidad en cada nivel del árbol usando comparaciones por pares. Sea C (i,j) una comparación del par que el tomador de decisiones hace entre dos elementos i y j, que son hijos de un nodo en el árbol de AHP. Suponiendo que el elemento i se considera al menos tan preferible como elemento j. Cuanto mayor sea el valor de C (i, j), más el decisor prefiere elemento de i a j. C (i,j) = 1 significa que el tomador de decisiones considera a los elementos i y j como igualmente importantes. Cuando C (i, j) = 3, 5, 7 y 9, el tomador de decisiones que valora al elemento i de manera moderadamente preferido, fuertemente preferido, muy fuertemente preferido, etc., respectivamente con respecto al elemento j. Cada comparación puede interpretarse como una escala de proporción. Para los elementos i y j en el mismo nivel del árbol, C (i, j) se puede interpretar como sigue:

$$C(i,j) = \frac{\text{The weight the decision-maker would like to assign to element i}}{\text{The weight the decision-maker would like to assign to element j.}}$$

4. Se crea una hoja de cálculo que muestra la evaluación de cada alternativa usando los pesos para cada criterio, subcriterio, y la intensidad determinada en el paso anterior. La alternativa i se evalúa en la fila i de la hoja de cálculo. La Celda (i j) en la hoja de cálculo da el peso de cada criterio o subcriterio j con respecto a la alternativa i.
5. La puntuación para cada alternativa es la suma de los pesos de las distintas casillas de la línea I de la hoja de cálculo.

El árbol AHP puede implicar costos y/o beneficios. Si un criterio no tiene subcriterio, entonces la puntuación de un criterio es el siguiente:

$$\text{criterion score} = \frac{\text{(weight of the criterion) * (weight of the intensity)}}{\text{weight of the exceptionally high intensity for the criterion.}}$$

Si un criterio tiene un sub-criterio, entonces la puntuación para el sub-criterio es el siguiente:

$$\text{sub-criterion score} = \frac{\text{(weight of the criterion)* (weight of the sub-criterion)* (weight of the intensity)}}{\text{weight of the exceptionally high intensity for the criterion.}}$$

La metodología AHP es una herramienta útil para ayudar a una organización en la toma de decisiones de inversión de seguridad de la información, pero no pretende sustituir al tomador de decisiones. El decisor debe decidir sobre los criterios, sub-criterios e intensidades y hacer numerosas evaluaciones para obtener un ranking de las alternativas. El AHP ayuda a organizar los pensamientos del CISO y proporciona un

mecanismo de comparación. El AHP puede ser una herramienta valiosa utilizada por sí sola o combinada con otros enfoques analíticos.

4.5.8 WANG

En esta investigación se introduce el concepto value-at-risk (VaR) para medir el riesgo de pérdidas diarias se enfrenta a una organización debido a las fallas de seguridad y el uso de análisis de valores extremos para estimar cuantitativamente el valor en riesgo (Wang, Chaudhury, & Rao, 2008).

VaR se desarrolló originalmente como una herramienta para evaluar el riesgo de los activos financieros y es ampliamente utilizado en la ingeniería financiera y de seguros. Es una medida estadística de los riesgos asociados a una inversión o un conjunto de inversiones.

La teoría del valor extremo cuantifica el comportamiento estocástico de un proceso en niveles inusualmente grandes o pequeños. Se ocupa de las cuestiones probabilísticas y estadísticas relacionadas con los eventos extremadamente raros.

En este modelo, se utiliza VaR para medir el riesgo de seguridad de la información enfrentado por una empresa y el análisis de valor extremo para estimar el VaR de las pérdidas diarias.

Los decisores pueden utilizar esta metodología para tomar decisiones de inversión adecuadas en función de sus propias preferencias de riesgo en lugar de perseguir una solución que minimiza sólo el costo esperado.

Una situación de riesgo en un modelo teórico se caracteriza generalmente en términos del valor esperado de una variable estocástica, porque en la mayoría de aplicaciones el interés principal está en el centro de la distribución y no la cola.

En el modelo, se describe la situación en términos de su comportamiento extremo. Por ejemplo, una situación de riesgo posible se puede caracterizar como una pérdida diaria media de X dólares, mientras que en este enfoque se caracteriza por tener una probabilidad de Z % para que la pérdida diaria exceda Y dólares.

En algunas decisiones son los valores extremos los de interés primario, como en el caso de fallos de seguridad, que son eventos de baja probabilidad que pueden provocar enormes pérdidas.

Para este modelo tenemos las siguientes notaciones:

j	The type of incident, $j = 1, 2, \ldots, T$.
n_j	The daily number of incidents of type j.
X	The daily number of activities.
I	The security investment level.
$P_j(I)$	The occurrence probability of an activity resulting in an incident of type j at security investment level I.
$C_j(I)$	The cost caused by a successful exploit of type j at security investment level I.
L	The daily loss.
$F_L(z)$	The cumulative distribution function (CDF) of L.
z_p	The pth quantile of $F_L(z)$. p is a probability, such that $0 \leq p \leq 1$.

La pérdida diaria incluye todas las pérdidas causadas por diferentes incidentes en un día. Dado un nivel de inversión de seguridad I, la pérdida diaria L es entonces:

$$L = \sum_{j=1}^{T} n_j C_j(I) = X \sum_{j=1}^{T} P_j(I) \cdot C_j(I).$$

Se supone que los incidentes de diferentes tipos son independientes. Con la inversión de seguridad adecuada, esperamos que la pérdida diaria por encima de un determinado nivel tienda a una probabilidad deseada. Se denota la función de distribución acumulativa (CDF) de L por FL(z). Se define el valor en riesgo de la pérdida diaria con probabilidad p como:

$$p = \Pr[L \geq VaR] = 1 - \Pr[L \leq VaR] = 1 - F_L(VaR)$$

A partir de la definición, la probabilidad de que la organización se encuentre con una pérdida diaria que supera VaR es p. Como alternativa, se puede decir que con probabilidad 1 - p, la pérdida diaria encontrada por la organización es inferior o igual al valor en riesgo. La definición muestra que el VaR se ocupa de comportamiento de la cola de la CDF FL(z). Más específicamente, la cola derecha de FL(z). Dado un univariado CDF FL(z) y la probabilidad p ($0 \leq p \leq 1$) , el cuantil de FL(z) se define como:

$$z_p = \inf\{z \mid F_L(z) \geq p\},$$

Donde inf denota el número real más pequeño que satisface $FL(z) \geq p$. Si se conoce la CDF FL(z), a continuación el VaR es simplemente su (1 - p). Sin embargo no es posible conocer CDF en la práctica. Así, el estudio del valor en riesgo de la pérdida diaria se ocupa esencialmente de la estimación de la CDF FL(z) y su cuantil, especialmente el comportamiento de la cola de la CDF .

El tomador de decisiones puede utilizar esta información para tomar una decisión de inversión adecuada teniendo en cuenta su preferencia de riesgo. El enfoque por Wang se puede aplicar de dos maneras. En primer lugar de una manera no comparativa, es decir sólo una alternativa de inversión se evalúa, donde el VaR y los costes diarios esperados de la inversión, que consisten en la media pérdidas diarias y costes de la solución diarias, se comparan con la situación actual. En segundo lugar, en un análisis comparativo, en el que el VaR y los costes diarios esperados se calcularon y compararon para cada alternativa es la inversión. En ambos sentidos, el tomador de decisiones, elige cualquiera de las alternativas (o el estado actual) en función la disminución de los costos o VaR diario esperado.

4.5.9 ROYER

Denis Royer desarrollo un framework específico para evaluar el valor de las soluciones de identity management corporativas (Royer, 2007).

El autor propone los siguientes pasos a seguir para preparar un análisis:

1. Analizar el entorno de la organización a fin de obtener los objetivos estratégicos para la introducción de un sistema IAM.
2. Construir una vista integral de la organización sobre la base de los objetivos estratégicos, derivando a un plan global para la introducción de IAM.
3. Dividir el plan global en pequeños sub-proyectos.
4. Evaluar los sub-proyectos.
5. Determinar la secuencia de los sub-proyectos basados en su retorno para la posterior ejecución de los planes.

El proceso descrito se visualiza en la figura 4-5. Los circuitos de retroalimentación introducidos en los pasos 1 a 3 ayudan para mejorar los resultados del proceso en sí.

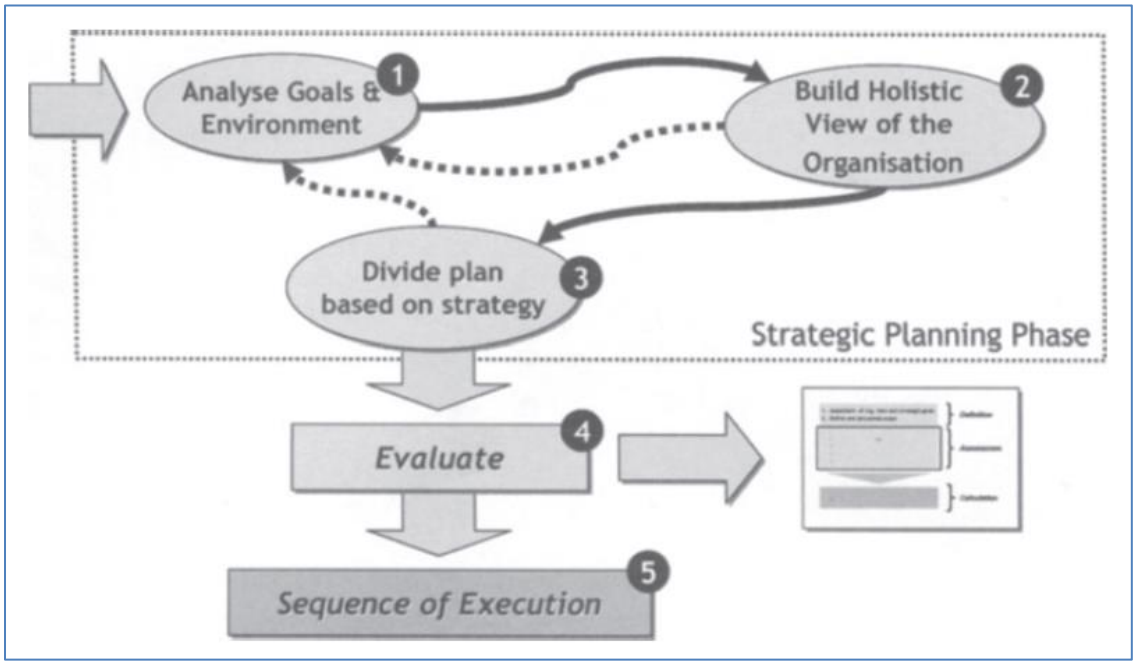

FIGURA 4-5 PROCESO DE PREPARACIÓN - ENFOQUE DE ROYER

FUENTE: ROYER, 2007

La estructura del proceso de evaluación propuesto se divide en 6 etapas:

- Paso 1, evaluación de la vista organizacional sobre IAM a fin de obtener los objetivos estratégicos para su introducción.
- Paso 2, definir y documentar el alcance del proyecto basado en los determinantes estratégicos fijados anteriormente.
- Paso 3, definir todos los costos del proyecto, incluyendo todas las inversiones en hardware y software, derechos de licencia, y mano de obra.
- Paso 4, documentar y estimar beneficios tangibles e intangibles potenciales. Para los beneficios tangibles, incluir ahorros directos e indirectos y las ganancias. Es importante analizar las interdependencias entre los beneficios tangibles e intangibles. En este caso, se necesitan métodos estandarizados para determinar los costos en consecuencia.

- Paso 5, documentar los posibles riesgos operativos tales como los recursos, el calendario, el personal y legal y determinar los impactos tangibles e intangibles asociados.
- Paso 6, cálculo del rendimiento potencial basado en los beneficios tangibles y los impactos potenciales de los riesgos. Por ejemplo, mediante el uso de métodos y modelos como el ROI o ROSI.

El proceso de evaluación propuesto se visualiza en la figura 4-6. En comparación con otros modelos, los potenciales riesgos operacionales asociados a IAM se incorporan. Esto es necesario, ya que las inversiones en seguridad ayudan a reducir o mitigar los riesgos potenciales. Como resultado se obtiene una visión más precisa de los beneficios que pueden derivarse de este tipo de tecnologías.

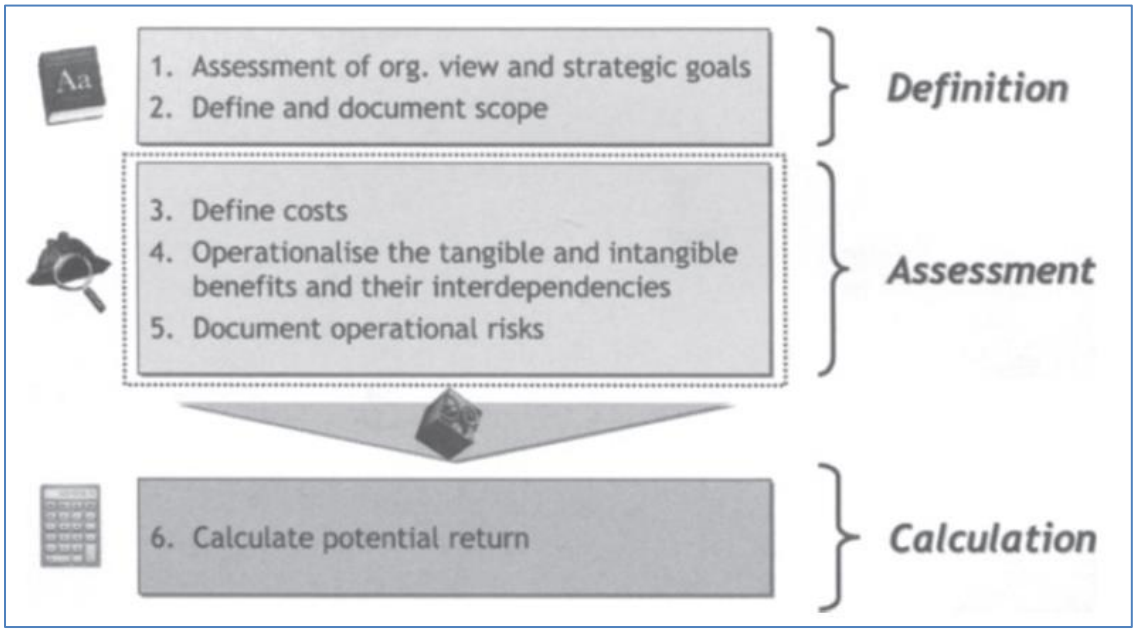

FIGURA 4-6 PROCESO DE EVALUACIÓN - ENFOQUE DE ROYER

FUENTE: ROYER, 2007

El proceso presentado en gran medida se basa en la documentación de los pasos

realizados y la evaluación de los riesgos relacionados con la operación, los beneficios y los costos. Esto ayuda a identificar las interdependencias entre estos aspectos más fácilmente y de una manera más consistente.

La documentación debe ser escrita de tal manera que todas las partes involucradas puedan entender la terminología y los conceptos utilizados. Las bases de conocimientos comunes y glosarios son útiles para cumplir con este requisito. En la opinión del autor, esto ayuda a las partes no involucradas en el proceso de evaluación para comprender y validar los resultados con mayor facilidad.

4.5.10 FLORES

Los autores proponen el método valor actual neto, también conocido como NPV o VAN, como la técnica de evaluación para determinar el valor futuro de inversiones de seguridad de la información. El documento demuestra por medio de esta técnica se puede evaluar el valor de las inversiones en el ámbito de la seguridad y la gobernabilidad (Flores, Sommestad, Holm, & Ekstedt, 2011).

El VAN una métrica financiera que ha demostrado eficacia en la evaluación de proyectos y comparación de proyectos. De esta forma la alternativa de inversión más beneficiosa se puede identificar y comunicar de una manera comprensible para el tomador de decisiones. El uso de VPN como una herramienta de evaluación para las inversiones de seguridad en fase de propuesta también ha sido sugerido por otros autores como Gordon, Loeb y Sonnenreich.

El punto de partida en el método VAN es el costo del capital para las inversiones, también conocido como el rendimiento requerido. El costo de capital es la cantidad que un inversor exige en compensación por el valor temporal del dinero invertido y por asumir el riesgo de la inversión. Por lo tanto, representa los costos para que tome la

alternativa de inversión y es la rentabilidad mínima que los inversores esperan para proporcionar capital a una inversión, estableciendo así un punto de referencia que la inversión tiene que cumplir. Para una inversión agregue valor, debe ganar más que el costo del capital.

Al calcular el VAN de una inversión se utiliza la siguiente fórmula:

$$NPV = \sum_{t=0}^{\infty} \frac{R_t}{(1+i)^t}$$

La tasa de costo de capital de (i) se utiliza como la tasa de descuento. Esta es la tasa de rendimiento que se puede ganar en una alternativa de inversión con un riesgo similar. R es el flujo neto de caja, es decir, la cantidad de dinero en efectivo, menos la entrada de flujo de salida, en el momento t. Para calcular el VAN de una inversión cada entrada de efectivo/flujo de salida asociada a ella se descuenta de nuevo a su valor actual. El VPN es la suma de todos los valores actuales de la serie temporal de los flujos de efectivo (Flores, Sommestad, Holm, & Ekstedt, 2011).

Si el VAN es mayor que cero, es beneficioso hacer la inversión y por lo tanto la inversión es una buena oportunidad de inversión real. Si el VAN es menor que cero no va a añadir valor. Aplicado a la seguridad, una oportunidad atractiva de inversión es aquella que genera valor futuro en términos de menor impacto de los incidentes de seguridad y proporciona un valor para el accionista (Flores, Sommestad, Holm, & Ekstedt, 2011).

Otro autor como Xiaomeng Su, propone mejorar el análisis con otra métrica comúnmente asociada como es la Tasa Interna de Retorno. También conocida como TIR o IRR, se calcula mediante el uso de un flujo de caja como el VAN (Su, 2006).

4.5.11 THOMAS

Como solución Russell Cameron Thomas propone un framework denominado “Total Cost of Security” o TCoS, que acorde al autor tiene las siguientes ventajas frente a otros comúnmente utilizados (Thomas, 2009):

- Es compatible con las Prácticas de Contabilidad Generalmente Aceptadas (PCGA) y paquetes ERP modernos.
- Es compatible con los marcos de gestión del riesgo empresarial (ERM).
- Es compatible con las teorías económicas de la empresa y la toma de decisiones racionales con información incierta e incompleta.
- Proporciona un marco general para la integración de una variedad de métricas de seguridad en una vista compuesta más relevante.
- Reduce significativamente la carga de recopilación de datos en comparación con otros enfoques como ALE.
- Esto hace que la mayor parte de la información esté disponible y evita muchos de los problemas de incertidumbre.
- Es robusto a los ambientes de amenazas cambiantes.
- Es compatible con una variedad de instrumentos de incentivo para los interesados tanto para una mejor gestión de riesgos, minimizar las externalidades y de revelar información relevante.
- Permite un análisis modular de las organizaciones complejas y redes tanto a nivel de componentes y en los distintos niveles de agregación.
- Se puede ampliar para incluir los riesgos relacionados tales como la privacidad, protección de la propiedad intelectual y los derechos digitales.
- Es aplicable a una amplia variedad de organizaciones, incluyendo fines de lucro, sin fines de lucro, gubernamentales y militares. Se escala bien a través de tamaño y estructuras de organización, incluidas las redes de organizaciones.

Este modelo logra armonizar las dos perspectivas de riesgo económico. La primera perspectiva es la del inversor racional que se centra en la rentabilidad a corto plazo y la volatilidad de los rendimientos. El rendimiento se define como retorno de la inversión y se determina por la "grasa de la curva", caracterizada por la media y la varianza de la distribución de rendimientos.

El segundo punto de vista es el actuario de seguros que se centra en la financiación a largo plazo de un grupo de riesgos. El rendimiento se define como evitar la "ruina" y se determina por la "cola de la curva". Caracterizada por los parámetros que cuantifican el espesor de la distribución de probabilidad a valores extremos.

A diferencia de los métodos anteriores, este es un marco de seguridad que armoniza estas dos perspectivas sobre el riesgo económico para apoyar la toma de decisiones racional.

Este marco se basa en el Modelo de Distribución de Pérdidas o LDA que se ha vuelto común en la gestión del riesgo empresarial, pionero en la industria de servicios financieros. La curva de la Figura 4-7 es una función de densidad de probabilidad de futuro para el costo total de la seguridad durante un período determinado.

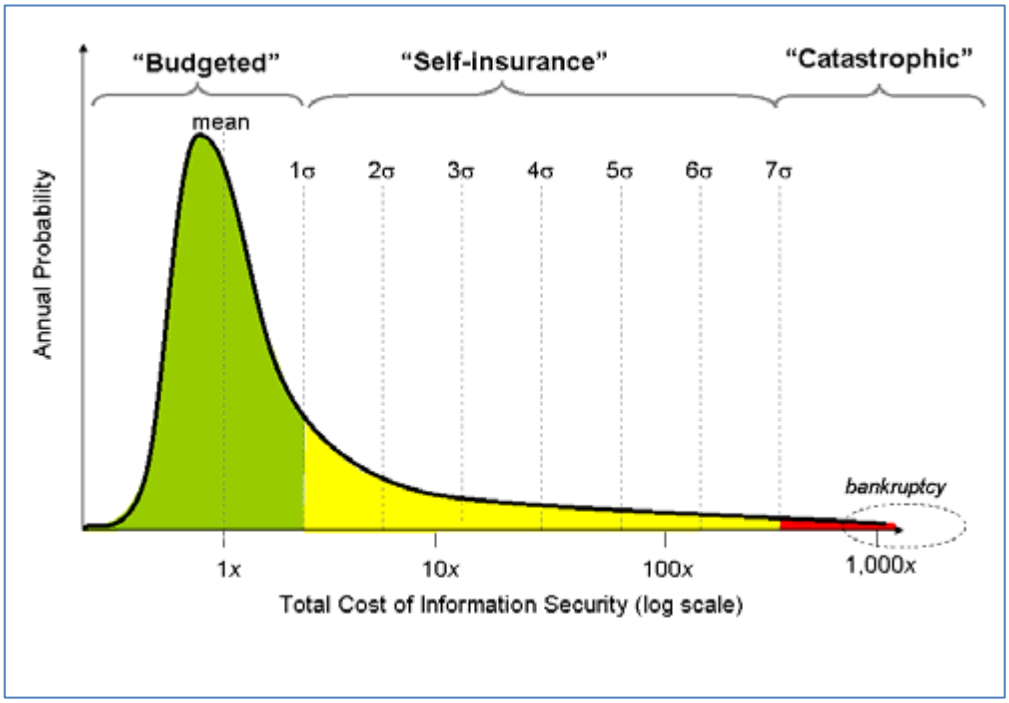

FIGURA 4-7 FUNCIÓN DE DENSIDAD DE PROBABILIDAD - ENFOQUE DE THOMAS

FUENTE: THOMAS, 2009

Se pretende que el marco sea amplio y podría incluir:

- Los costos directos de seguridad de la información (personal, gastos de explotación y de capital específicos de seguridad, servicios profesionales programas de formación y sensibilización de seguridad, los costos de medición y gestión de la seguridad, etc.).
- Los costos indirectos de seguridad de la información, asignados proporcionalmente (asistencia de TI, gestión de configuración, gestión de parches, etc.).
- Los costos directos de las violaciones de seguridad, intrusiones, las pérdidas y la recuperación (descubrimiento, control de daños, la respuesta de emergencia, la restauración del sistema, sanciones y / o multas, etc.).

- Los costos indirectos de las brechas de seguridad, intrusiones, las pérdidas y la recuperación, incluyendo impacto en los ingresos, daños a la reputación, etc.).

La primera innovación del enfoque es dividir los costos relacionados con la en tres categorías: "Presupuestado", "Auto-asegurado" y "Catastrófico". Básicamente, este enfoque divide la distribución de probabilidad costo agregado en tres secciones. La parte "grasa" de la curva cerca de la media es "Presupuestado". La sección de cola hasta un cierto umbral (95% o 99%) es "Auto-seguro". El extremo muy lejos de la cola es "catastrófico".

Por lo tanto, cualquier tipo de incidente dado podría contribuir a los costos en cualquiera o todas estas categorías:

- La región "Presupuestado" es la parte de "grasa" de la curva que incluye los costos que son predecibles y probablemente dentro del ejercicio presupuestario. Esto incluye todo el gasto directo en la seguridad, además de los costes indirectos, más el valor esperado de todas las pérdidas de alta frecuencia y una pequeña mezcla de las pérdidas de frecuencias más bajas. También incluye los costos de oportunidad.
- La región "Auto-asegurado" cubre magnitudes de pérdida que son potencialmente lo suficientemente grandes como para superar el presupuesto o podría conseguir la primera página de un periódico nacional, o incluso podría poner en peligro la calificación de crédito de la empresa, pero no necesariamente poner en peligro la supervivencia de la empresa. Estas pérdidas son de baja probabilidad, pero no cerca de cero.
- La región "Catastrófica" abarca los valores de pérdida más extremas que son muy poco probables o muy impredecibles, pero podría amenazar la supervivencia de las empresas.

La segunda innovación es el tratamiento de los costos indirectos, especialmente los costos indirectos de los incidentes de seguridad. El autor está a favor de un método

general de valoración denominado "Expected Cost of Recovery". Este es el costo anticipado de la restauración de los sistemas de información, datos, procesos de negocio y las relaciones de negocios a su nivel anterior de capacidad y rendimiento. Esta es más conservadora y fiable que otras medidas que tratan de estimar el valor de pérdidas del negocio debido a los incidentes de seguridad, incluyendo disminución de precios de las acciones y otras métricas de valor de las partes interesadas.

La fórmula general para TCoS se resume en la siguiente ecuación:

TCoS = B + SI + C, donde:

- **TCoS** es el costo total de la medida de seguridad.
- **B** son costos presupuestados de seguridad y pérdidas para el período, es decir los costos de la mediana o dentro de un margen de la mediana.
- **SI** es la prima de auto-seguro para cubrir las pérdidas de al impacto y baja probabilidad.
- **C** es el costo de la continuidad del negocio para escenarios catastróficos, asignados de acuerdo a las causas y efectos de seguridad de la información.

El resultado es un TCoS en dólares corrientes para el próximo período de tiempo. Un flujo de valores TCoS de varios periodos puede ser tratado como flujos de efectivo en el método de flujo de caja descontado (DCF) estándar. La tasa de descuento, un parámetro crítico, que en las firmas es el costo promedio ponderado del capital, o en otros contextos, la tasa libre de riesgo.

El criterio de decisión más general es "Minimizar las TCoS, mientras se cumplen otros objetivos de negocio".

También es posible la integración de las TCoS en cálculos de retorno de inversión para obtener una rentabilidad ajustada al riesgo de diversas oportunidades de negocio que tienen consecuencias para la seguridad de la información.

Por supuesto, el éxito de este o cualquier otro método de medición depende de nuestra capacidad para estimar las curvas de distribución de probabilidad correspondientes:

- La región "Presupuestado" pude ser estimada utilizando modelos de costos bastante convencionales y los datos extraídos de los sistemas de información contable.
- La región de "Auto-asegurado" se modela usando enfoques orden de magnitud, posiblemente la combinación de métodos estocásticos con el razonamiento inferencial.
- La región de "Catastrófica" se basa en utilizar análisis de escenarios y escalas ordinales o nominales. Aquí, la precisión de la estimación de costos es mucho menos importante de lo que es el valor cualitativo para guiar la estrategia y planificación de la continuidad del negocio.

4.6 COMPARACIÓN DE ENFOQUES

En esta sección se compara los enfoques descriptos anteriormente desde el punto de vista de IAM.

Los criterios y calificaciones fueron seleccionados por su relevancia en el análisis. La tabla comparativa fue confeccionada en base a la información relevada y la interpretación del autor de la misma.

El objetivo de la comparación identificar fortalezas y debilidades de los enfoques a la hora de evaluar soluciones IAM.

4.6.1 CRITERIOS

Los criterios seleccionados para la comparativa de enfoques son los siguientes

1. Objetivo: Especifica la finalidad y utilidad del enfoque propuesto para las organizaciones.
2. Métrica: Indicador/es especificado/s en el enfoque como herramienta de medición. Si el enfoque no establece ninguna métrica, este criterio será calificado como No Definido (ND).
3. Unidad: Unidad/es de valor que aplican a la/s métrica/s del enfoque. Si el enfoque no establece ninguna métrica, este criterio será calificado como No Definido (ND).
4. Reducción de riesgo: Este es uno de los drivers principales de una solución IAM, este criterio evalúa si el enfoque lo aborda y en tal caso si es de forma precisa o parcial según el juicio del autor.

5. Reducción de costos: Este es uno de los drivers principales de una solución IAM, este criterio evalúa si el enfoque lo aborda y en tal caso si es de forma precisa o parcial según el juicio del autor.
6. Eficiencia operacional: Este es uno de los drivers principales de una solución IAM, este criterio evalúa si el enfoque lo aborda y en tal caso si es de forma precisa o parcial según el juicio del autor.
7. Facilitación de negocios: Este es uno de los drivers principales de una solución IAM, este criterio evalúa si el enfoque lo aborda y en tal caso si es de forma precisa o parcial según el juicio del autor.
8. Cumplimiento regulatorio: Este es uno de los drivers principales de una solución IAM, este criterio evalúa si el enfoque lo aborda y en tal caso si es de forma precisa o parcial según el juicio del autor.

4.6.2 Calificaciones de cumplimiento de drivers

Para los criterios 4 al 8, se definen 3 calificaciones posibles

- Cumple (C): Esta calificación aplica si el enfoque aborda de forma precisa el criterio.
- No Cumple (NC): Esta calificación aplica si el enfoque no aborda el criterio.
- Cumple parcialmente (CP): Esta calificación aplica cuando el enfoque no se especifica en forma clara, da por supuesto o aborda parcialmente el criterio.

4.6.3 Tabla Comparativa

En la siguiente tabla se comparan los diferentes enfoques propuestos:

Enfoque	Objetivo	Métrica	Unidad	Reducción de Riesgo	Reducción de Costos	Eficiencia Operacional	Facilitación de Negocios	Cumplimiento Regulatorio
ENISA	Cuantificar retorno de inversión	ROSI	Porcentaje de retorno	C	NC	NC	NC	NC
Gordon	Cuantificar los beneficios esperados y el monto óptimo de inversión	EBIS ENBIS Z	Unidades monetarias	C	NC	NC	NC	NC
Butler	Comparar inversiones de seguridad considerando el riesgo	SAEM	Unidades monetarias	CP	NC	NC	NC	NC
Sonnenreich	Comparar inversiones de seguridad	ROSI	Porcentaje de retorno	C	NC	NC	NC	NC
Mizzi	Comparar inversiones de seguridad	ROISI	Porcentaje de retorno	C	NC	NC	NC	NC

Cremonini	Comparar inversiones de seguridad	ROI ROA	Porcentaje de retorno	C	NC	NC	NC	NC
Bodin	Comparar inversiones de seguridad	ND	ND	CP	CP	CP	CP	CP
Wang	Cuantificar el beneficio y/o comparar inversiones de seguridad	VaR	Unidades monetarias	C	NC	NC	NC	NC
Royer	Cuantificar los beneficios de una solución IAM	ND	ND	CP	CP	CP	CP	CP
Flores	Cuantificar los beneficios esperados	VAN TIR	Unidades monetarias Tasa de retorno	CP	CP	CP	CP	CP

Thomas	Minimizar costos de seguridad	TCoS	Unidades monetarias	CP	CP	CP	CP	CP

TABLA 4-3 TABLA COMPARATIVA DE ENFOQUES

FUENTE: ELABORACIÓN PROPIA

4.7 EJEMPLO DE APLICACIÓN

A continuación, se lleva a cabo un ejercicio de evaluación económica de un proyecto IAM de ejemplo considerando uno de los enfoques propuestos en este capítulo.

4.7.1 PREMISAS

4.7.1.1 METODOLOGÍA

Para el desarrollo del ejemplo de aplicación se utilizó la siguiente metodología de trabajo:

1. Se establecieron las premisas generales:
    a. Metodología.
    b. Enfoque.
    c. Contexto.
    d. Información técnica.
    e. Supuestos.
2. Se determinaron los costos del proyecto.
3. Se identificaron y cuantificaron los beneficios del proyecto por medio de un análisis de escenarios.
4. Se obtuvo el flujo de fondos del proyecto y los indicadores.
5. Se realizó un análisis de resultados y se obtuvo conclusiones.

4.7.1.2 ENFOQUE

La evaluación se llevó a cabo bajo la siguiente óptica:

- Se seleccionó un modelo tradicional de evaluación de proyectos con el fin de demostrar la viabilidad de su aplicación (enfoque de Flores).

- Se calcularon los siguientes indicadores:
  - Flujo de fondos.
  - VAN.
  - TIR.
- La unidad de medida seleccionada es el dólar estadounidense.
- El plazo de análisis es 5 años.
- Para la elaboración, se contó con la colaboración del staff de consultores de la empresa Assertiva S.A., que cuenta con una amplia experiencia en implementaciones IAM en Argentina y Chile.
- Los datos y parámetros utilizados en la evaluación son promedios o benchmarks de la industria, provistos por Assertiva S.A.

4.7.1.3 CONTEXTO

El caso se enmarca en el contexto que se define a continuación.

Con respecto a la empresa en estudio:

- Es una entidad financiera con fines de lucro con base en la República de Chile.
- Cuenta con aproximadamente 2.500 empleados y 500 contratistas.
- Tiene oficinas distribuidas en todo el territorio de Chile.
- Dispone de un datacenter principal ubicado en la ciudad de Santiago de Chile.
- La infraestructura tecnológica es amplia y heterogénea. Actualmente dispone de más de 50 aplicaciones activas. De estas 11 son consideradas críticas por el negocio.
- Debe cumplir con regulaciones de la Superintendencia de Bancos e Instituciones Financieras de Chile (SBIF), SOX y PCI-DSS.

Información del proyecto:

- Se requiere de servicios profesionales para la implementación de la solución IAM.
- Se espera que el proyecto abarque todas las aplicaciones críticas.
- El proyecto consta de 5 fases que se llevarán a cabo durante 5 años, en las cuales gradualmente se integrarán sistemas y automatizarán procesos de gestión de identidades a la solución.

4.7.1.4 INFORMACIÓN TÉCNICA

La evaluación tiene las siguientes premisas técnicas:

- La solución IAM a implementar es la suite completa de NetIQ Identity Manager en su versión 4.5, la misma pertenece al segmento IGA. Incluye los siguientes módulos:
    - Plataforma base (Identity Manager).
    - Módulo de gestión de roles y accesos (RBPM).
    - Metadirectorio de identidades (eDirectory).
    - Módulo de auditoría y reportería (Reporting Module)
    - Componentes de integración y aprovisionamiento con el sistema de RRHH y demás sistemas core del negocio (Drivers).
    - Módulo de flujos de trabajo automatizados (Workflows).
    - Portal de autoservicio de identidades (User Application y Dashboard).
    - Módulo de autogestión y sincronización de contraseñas (SSPR).
    - Módulo de administración (iManager).
- Toda la infraestructura base que soporta la solución es open source, por lo que no tiene costo adicional de licenciamiento.
- Software base:
    - Sistema operativo: Red Hat 6.5 (64-bit)
    - Servidor de aplicación: Apache Tomcat 7.0.55

  - Base de datos: PostgreSQL 9.3.4
- Hardware:
  - Capa de negocio
    - 16 GB RAM
    - 1.8 GHZ 4 Cores
    - 160 GB de Disco Duro
  - Capa de datos
    - 16 GB RAM o superior
    - 1.8 GHZ 4 Cores o Superior
    - 300 GB de Disco Duro
  - Auditoría y reportería
    - 16 GB RAM o superior
    - 1.8 GHZ 4 Cores o Superior
    - 500 GB de Disco Duro
- No se incluye alta disponibilidad.
- Todo el hardware está ubicado en el datacenter principal de la empresa.

4.7.1.5 SUPUESTOS

Para el cálculo de los indicadores se consideran distintos supuestos que se detallan a continuación.

Información sobre su gestión de identidades y accesos:

- En promedio los usuarios manejan 8 cuentas distintas.
- El sueldo promedio de la organización es 1.500 dólares mensuales.
- El sueldo promedio de un administrador de sistemas en la empresa es 2.300 dólares mensuales.
- Cantidad aproximada de nuevos empleados por año 300.

- Cantidad aproximada de desvinculaciones por año 170.
- Cantidad aproximada de cambios de responsabilidad por año 450.
- Tiempo promedio de resolución de ticket de ABM: 2 horas.
- Tiempo promedio de resolución de ticket por gestión de contraseñas: 30 minutos.
- Cantidad aproximada de solicitudes de ABM por año: 4000.
- Cantidad de solicitudes de cambio de contraseña por año: 3000.
- Cantidad de auditorías por año: 5.
- Cantidad de horas requeridas por auditoría: 90.

Otras variables:

- Cotización del dólar: 660 pesos chilenos por dólar. Fuente Banco Central de la República de Chile.
- Tasa libre de riesgo o tasa de descuento: Se tomará como referencia la tasa de interés mercado secundario de los bonos licitados por el Banco Central de Chile a 5 años que es aproximadamente 4%. Fuente Banco Central de la República de Chile.

4.7.2 ANÁLISIS DE COSTOS

Para la ejecución y mantenimiento del proyecto se identificaron los siguientes costos:

4.7.2.1 LICENCIAMIENTO DE SOFTWARE Y MANTENIMIENTO

Los costos de licenciamiento considerados en el estudio aplican solo a la solución IAM ya que el resto de la tecnología es open-source:

Concepto	**Cuantificación**
Licencia inicial de NetIQ Identity Manager (incluye costos de conectores)	60 dólares por usuario por única vez

Renovación de licencia de NetIQ Identity Manager	12 dólares por usuario anual
Cantidad total de usuarios a licenciar	3000
Cálculo	costo de licencia * cantidad de usuarios

TABLA 4-4 CÁLCULO LICENCIAMIENTO Y MANTENIMIENTO

FUENTE: ELABORACIÓN PROPIA, 2016

4.7.2.2 SERVICIOS PROFESIONALES

Todas las fases del proyecto requieren de servicios profesionales de implementación:

Concepto	**Cuantificación**
Costo por hora de recurso senior	30 dólares
Recursos Fase 1	3 dedicados
Recursos Fase 2 a 5	1 dedicado anual
Cálculo (por año)	número de recursos * horas anuales * costo por hora

TABLA 4-5 CÁLCULO SERVICIOS PROFESIONALES

FUENTE: ELABORACIÓN PROPIA, 2016

4.7.2.3 RECURSOS INTERNOS DE IMPLEMENTACIÓN

Todas las fases del proyecto requieren de apoyo interno de implementación:

Concepto	**Cuantificación**
Costo mensual recurso	2300 dólares
Recursos Fase 1 a 5	1 dedicado anual

Cálculo (por año)	número de recursos * costo anual del recurso

TABLA 4-6 CÁLCULO RECURSOS INTERNOS DE IMPLEMENTACIÓN

FUENTE: ELABORACIÓN PROPIA, 2016

4.7.2.4 RECURSOS INTERNOS DE ADMINISTRACIÓN, INGENIERÍA Y SOPORTE DE OPERACIONES

Todas las fases del proyecto requieren de apoyo interno de operaciones:

Concepto	**Cuantificación**
Costo mensual recurso	2300 dólares
Recursos Fase 1 a 5	1 dedicado anual
Cálculo (por año)	número de recursos * costo anual del recurso

TABLA 4-7 CÁLCULO RECURSOS INTERNOS DE OPERACIÓN

FUENTE: ELABORACIÓN PROPIA, 2016

4.7.2.5 HARDWARE Y SOFTWARE BASE

Se requiere la adquisición por unica vez de hardware y su correspondiente instalación. Esto incluye el software base:

Concepto	**Cuantificación**
Costo de promedio de compra e instalación completa por servidor	10.000 dólares
Cantidad de servidores	3
Cálculo	costo promedio servidor * cantidad de

	servidores

TABLA 4-8 CÁLCULO HW Y SW BASE

FUENTE: ELABORACIÓN PROPIA, 2016

4.7.2.6 COSTOS PROYECTADOS

La proyección de costos a 5 años esta valorizada en dólares:

Costos	0	1	2	3	4	5
Licenciamiento de software y mantenimiento	180,000.00	36,000.00	36,000.00	36,000.00	36,000.00	-
Servicios profesionales	172,800.00	57,600.00	57,600.00	57,600.00	57,600.00	-
Recursos internos de implementación	27,600.00	27,600.00	27,600.00	27,600.00	27,600.00	-
Recursos internos de operaciones	27,600.00	27,600.00	27,600.00	27,600.00	27,600.00	-
Hardware y software base	30,000.00	-	-	-	-	-
Inversión Anual	**438,000.00**	**148,800.00**	**148,800.00**	**148,800.00**	**148,800.00**	**-**
Inversión Acumulada	**438,000.00**	**586,800.00**	**735,600.00**	**884,400.00**	**1,033,200.00**	**1,033,200.00**

TABLA 4-9 COSTOS PROYECTADOS

FUENTE: ELABORACIÓN PROPIA, 2016

4.7.3 ANÁLISIS DE BENEFICIOS

Para el análisis de beneficios se plantea un análisis de escenarios, donde se compara la situación actual frente a los resultados producto de la implementación de la solución IAM. El diferencial positivo entre ambos escenarios representa el beneficio del proyecto.

En este ejemplo solo se cuantificaron algunos de los potenciales beneficios, además estos podrían variar de acuerdo con las características de cada organización.

4.7.3.1 AUMENTO DE LA PRODUCTIVIDAD DE LOS USUARIOS

Como resultado de la implementación de la solución IAM se esperan los siguientes resultados en cuanto al incremento de la productividad de los usuarios por efecto de la automatización:

- Reducción de tiempo promedio en el cual un nuevo empleado obtiene todos sus accesos (RN). Se espera disminuir de un promedio de 3 días hábiles a pocos minutos. RN = cantidad nuevos empleados * horas perdidas * costo por hora.
- Reducción de tiempo promedio en el cual un empleado obtiene todos sus accesos ante un cambio de función organizacional (RC). Se espera disminuir de un promedio de 3 días hábiles a pocos minutos. RC = cantidad cambios de rol * horas perdidas * costo por hora.
- Reducción en el tiempo ocioso de un usuario frente a la espera de una solicitud de accesos (RO). Se espera disminuir de un día hábil a pocos minutos. RO = cantidad cambios de solicitudes * horas perdidas * costo por hora.
- Cálculo ahorro por año: (RN0 – RN1) + (RC0 – RC1) + (RO0 – RO1), donde 0 es el escenario base y 1 el escenario proyectado. En la proyección se considera una mejora gradual como resultado de la integración de sistemas críticos en las diferentes fases del proyecto.

Escenario Actual	0	1	2	3	4	5
Costo tiempo promedio de altas	67,500.00	67,500.00	67,500.00	67,500.00	67,500.00	67,500.00
Costo tiempo promedio de cambios de rol	78,750.00	78,750.00	78,750.00	78,750.00	78,750.00	78,750.00
Costo tiempo promedio de solicitudes	112,500.00	112,500.00	112,500.00	112,500.00	112,500.00	112,500.00
Escenario Proyectado	**0**	**1**	**2**	**3**	**4**	**5**
Costo tiempo promedio de altas	67,500.00	20,250.00	13,500.00	10,125.00	3,375.00	3,375.00
Costo tiempo promedio de cambios de rol	78,750.00	23,625.00	15,750.00	11,812.50	3,937.50	3,937.50

Costo tiempo promedio de solicitudes	112,500.00	33,750.00	22,500.00	16,875.00	5,625.00	5,625.00
Total ahorro	**-**	**181,125.00**	**207,000.00**	**219,937.50**	**245,812.50**	**245,812.50**

TABLA 4-10 CÁLCULO AUMENTO DE PRODUCTIVIDAD

FUENTE: ELABORACIÓN PROPIA, 2016

4.7.3.2 REDUCCIÓN DE COSTOS LABORALES HELP DESK

Se estiman los siguientes resultados en cuanto a la reducción de costos de help desk:

- Reducción de tickets por altas, bajas o modificaciones de accesos (RT). Se espera disminuir el volumen de tickets hasta un 85% gradualmente (North, 2008). RT = número de tickets * horas necesarias de mesa de ayuda * costo hora.
- Reducción de tickets por solicitudes relacionadas a contraseñas. Se espera disminuir el volumen de tickets hasta un 85% gradualmente (North, 2008). RT = número de tickets * horas necesarias de mesa de ayuda * costo hora.
- Cálculo ahorro por año: (RT0 – RT1) + (RS0 – RS1), donde 0 es el escenario base y 1 el escenario proyectado. En la proyección se considera una mejora gradual como resultado de la integración de sistemas críticos en las diferentes fases del proyecto.

Escenario Actual	0	1	2	3	4	5
Tickets por ABM	115,000.00	115,000.00	115,000.00	115,000.00	115,000.00	115,000.00

Tickets por contraseñas	21,562.50	21,562.50	21,562.50	21,562.50	21,562.50	21,562.50
Escenario Proyectado	**0**	**1**	**2**	**3**	**4**	**5**
Tickets por ABM	115,000.00	40,250.00	28,750.00	23,000.00	17,250.00	17,250.00
Tickets por contraseñas	21,562.50	7,546.88	5,390.63	4,312.50	3,234.38	3,234.38
Total ahorro	**-**	**88,765.63**	**102,421.88**	**109,250.00**	**116,078.13**	**116,078.13**

TABLA 4-11 CÁLCULO REDUCCIÓN DE COSTOS DE HELP-DESK

FUENTE: ELABORACIÓN PROPIA, 2016

4.7.3.3 REDUCCIÓN DEL COSTO DE AUDITORÍAS INTERNAS Y EXTERNAS

La solución IAM tiene la capacidad de generar reportes y vistas en forma automatizada reduciendo costos auditorías:

- Reducción de tiempos de auditoría. Se espera disminuir en un 70% los tiempos de auditoría relacionados a accesos (North, 2008). RA = número de auditorías * cantidad de horas requeridas por auditoría * costo hora
- Cálculo ahorro por año: RA0 – RA1, donde 0 es el escenario base y 1 el escenario proyectado.

Escenario Actual	**0**	**1**	**2**	**3**	**4**	**5**
Tiempos auditoría	6,468.75	6,468.75	6,468.75	6,468.75	6,468.75	6,468.75
Escenario Proyectado	**0**	**1**	**2**	**3**	**4**	**5**
Tickets por ABM	6,468.75	1,940.63	1,940.63	1,940.63	1,940.63	1,940.63

Total ahorro	**-**	**4,528.13**	**4,528.13**	**4,528.13**	**4,528.13**	**4,528.13**

TABLA 4-12 CÁLCULO REDUCCIÓN DE COSTOS DE AUDITORÍA

FUENTE: ELABORACIÓN PROPIA, 2016

4.7.3.4 REDUCCIÓN DEL RIESGO

Por medio de una adecuada gestión de identidades se espera reducir la probabilidad de brechas. Tomando como base las características de la empresa y la información estadística de IBM "Data Breach Risk Calculator" se obtiene:

- Reducción de brechas de seguridad (RB). Se espera reducir al 20% los costos asociados a incidentes de seguridad de la información (North, 2008). RB = probabilidad de brecha * costo total de brecha
- Costo total de una brecha crítica de seguridad: 1.030.000 dólares.
- Probabilidad anual de una brecha de seguridad: 12.5 %.
- Cálculo ahorro por año: RB0 – RB1, donde 0 es el escenario base y 1 el escenario proyectado.

Escenario Actual	0	1	2	3	4	5
Incidentes de seguridad	128,750.00	128,750.00	128,750.00	128,750.00	128,750.00	128,750.00
Escenario Proyectado	**0**	**1**	**2**	**3**	**4**	**5**
Incidentes de seguridad	128,750.00	25,750.00	25,750.00	25,750.00	25,750.00	25,750.00

Total ahorro	**-**	**103,000.00**	**103,000.00**	**103,000.00**	**103,000.00**	**103,000.00**

TABLA 4-13 CÁLCULO REDUCCIÓN DE RIESGO

FUENTE: ELABORACIÓN PROPIA, 2016

4.7.3.5 REDUCCIÓN COSTOS DE SEGURIDAD

La implementación de una solución IAM es capaz de facilitar tareas y controles propias de áras de seguridad de la información:

- Reducción de tiempos de certificación anual de accesos. Se espera disminuir en un 50% el tiempo necesario (North, 2008). RR = cantidad de horas necesarias por usuario * cantidad de usuarios * costo hora
- Cálculo ahorro por año: RR0 – RR1, donde 0 es el escenario base y 1 el escenario proyectado.

Escenario Actual	**0**	**1**	**2**	**3**	**4**	**5**
Costo de recertificación de accesos	56,250.00	56,250.00	56,250.00	56,250.00	56,250.00	56,250.00
Escenario Proyectado	**0**	**1**	**2**	**3**	**4**	**5**
Costo de recertificación de accesos	56,250.00	28,125.00	28,125.00	28,125.00	28,125.00	28,125.00
Total ahorro	**-**	**28,125.00**	**28,125.00**	**28,125.00**	**28,125.00**	**28,125.00**

TABLA 4-14 CÁLCULO REDUCCIÓN DE COSTOS DE SEGURIDAD

FUENTE: ELABORACIÓN PROPIA, 2016

4.7.3.6 BENEFICIOS PROYECTADOS

La proyección de beneficios a 5 años esta valorizada en dólares:

Beneficios	0	1	2	3	4	5
Aumento de productividad	-	181,125.00	207,000.00	219,937.50	245,812.50	245,812.50
Reducción de costos de help-desk	-	88,765.63	102,421.88	109,250.00	116,078.13	116,078.13
Reducción de costos de auditorías	-	4,528.13	4,528.13	4,528.13	4,528.13	4,528.13
Reducción de brechas de seguridad	-	103,000.00	103,000.00	103,000.00	103,000.00	103,000.00
Reducción de costos de seguridad	-	28,125.00	28,125.00	28,125.00	28,125.00	28,125.00
Beneficio total	**-**	**405,543.75**	**445,075.00**	**464,840.63**	**497,543.75**	**497,543.75**
Beneficios acumulados	**-**	**405,543.75**	**850,618.75**	**1,315,459.38**	**1,813,003.13**	**2,310,546.88**

TABLA 4-15 BENEFICIOS PROYECTADOS

FUENTE: ELABORACIÓN PROPIA, 2016

4.7.4 FLUJO DE FONDOS E INDICADORES

Una vez cuantificados los costos y beneficios se procede a generar el flujo de fondos puro del proyecto:

Concepto	0	1	2	3	4	5
Beneficios	-	405,543.75	445,075.00	464,840.63	497,543.75	497,543.75
Costos	-	- 148,800.00	- 148,800.00	- 148,800.00	- 148,800.00	-
Amortización Bienes de Uso	-	- 3,000.00	- 3,000.00	- 3,000.00	- 3,000.00	- 3,000.00
Utilidad antes de impuesto	-	253,743.75	293,275.00	313,040.63	345,743.75	494,543.75
Impuesto a las Ganancias	-	- 48,211.31	- 55,722.25	- 59,477.72	- 65,691.31	- 93,963.31
Utilidad después de imp.	-	205,532.44	237,552.75	253,562.91	280,052.44	400,580.44
Amortización Bienes de Uso	-	3,000.00	3,000.00	3,000.00	3,000.00	3,000.00
Inversión Inicial	- 438,000.00	-	-	-	-	-
FLUJO DE FONDOS NETO	**- 438,000.00**	**208,532.44**	**240,552.75**	**256,562.91**	**283,052.44**	**403,580.44**

TABLA 4-16 FLUJO DE FONDOS DEL PROYECTO

FUENTE: ELABORACIÓN PROPIA, 2016

En base al cash flow se obtiene los siguientes indicadores:

Índices	0	1	2	3	4	5
Flujo de Fondos Acumulado	- 438,000.00	- 229,467.56	11,085.19	267,648.09	550,700.53	954,280.97
VAN Año	**- 438,000.00**	**200,511.96**	**222,404.54**	**228,083.49**	**241,954.41**	**331,713.70**
VAN Acumulado	**- 438,000.00**	**- 237,488.04**	**- 15,083.50**	**212,999.99**	**454,954.40**	**786,668.10**
TIR	**-100%**	**-52%**	**2%**	**27%**	**40%**	**49%**

TABLA 4-17 INDICADORES DEL PROYECTO

FUENTE: ELABORACIÓN PROPIA, 2016

4.7.5 RESULTADOS Y CONCLUSIONES

En esta sección se detallan y grafican los resultados del caso de ejemplo:

4.7.5.1 FLUJO DE FONDOS DEL PROYECTO

En el siguiente esquema se diagrama el flujo de fondos del proyecto por año:

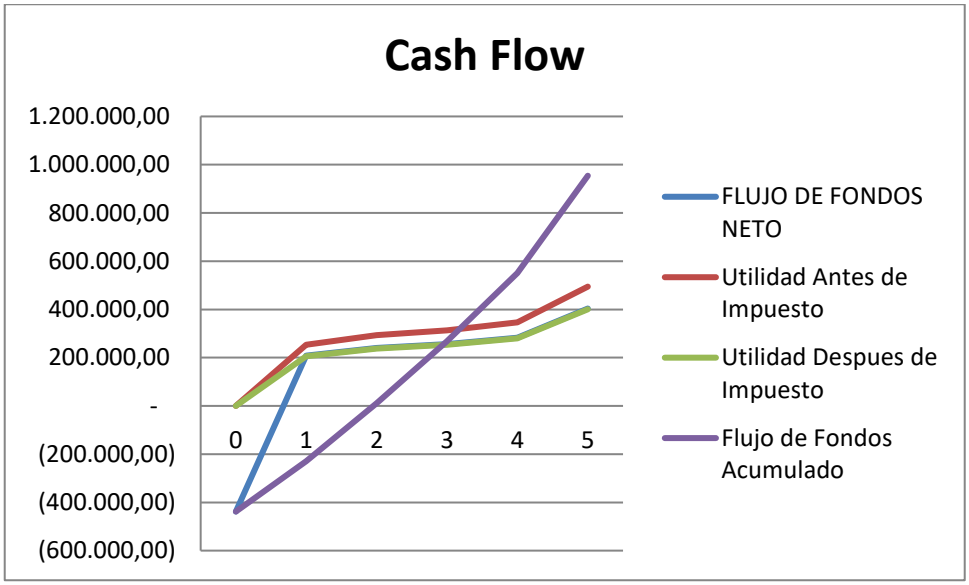

FIGURA 4-8 CASH FLOW DEL PROYECTO

FUENTE: ELABORACIÓN PROPIA, 2016

Como se puede observar, el flujo de fondos acumulado es positivo a partir del segundo y año. Además, mantiene esta tendencia hasta el último periodo en estudio.

4.7.5.2 TASA INTERNA DE RETORNO

En el siguiente diagrama se puede observar la evolución de la tasa interna de retorno del proyecto discriminada por anualmente:

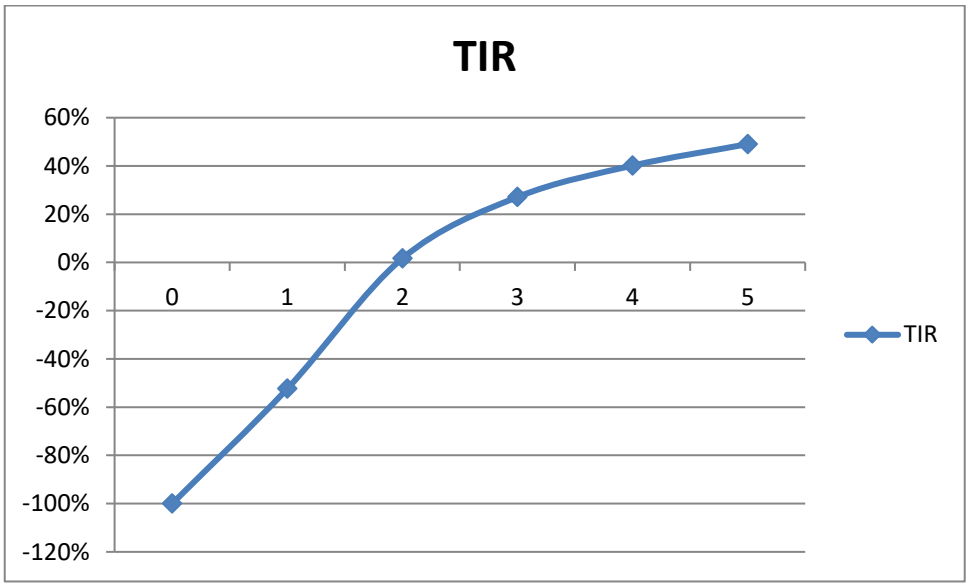

FIGURA 4-9 TIR DEL PROYECTO

FUENTE: ELABORACIÓN PROPIA, 2016

Este índice evidencia una tasa de retorno positiva del 49 % a 5 años.

4.7.5.3 VALOR ACTUAL NETO

En los esquemas a continuación se puede observar la evolución del VAN del proyecto por año:

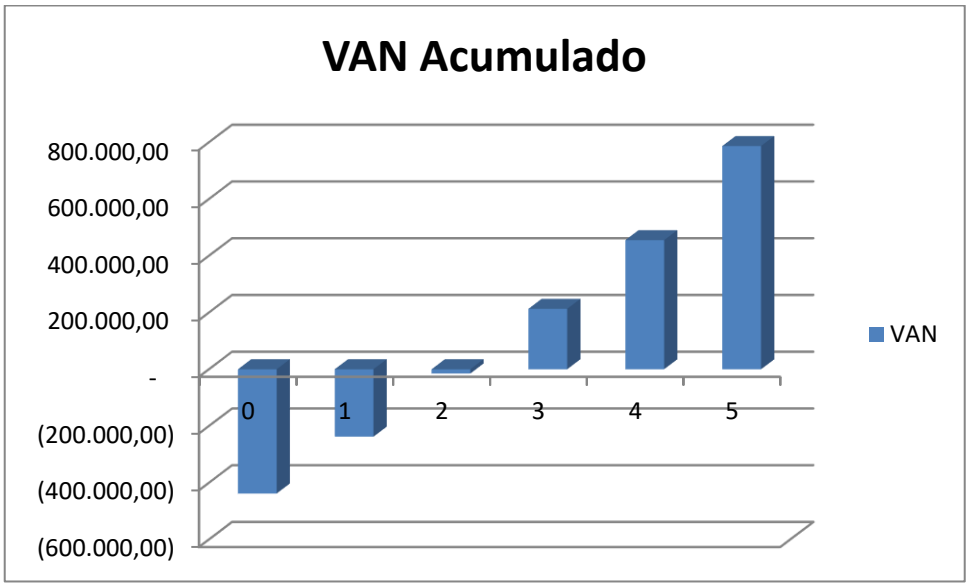

FIGURA 4-10 VAN ACUMULADO DEL PROYECTO

FUENTE: ELABORACIÓN PROPIA, 2016

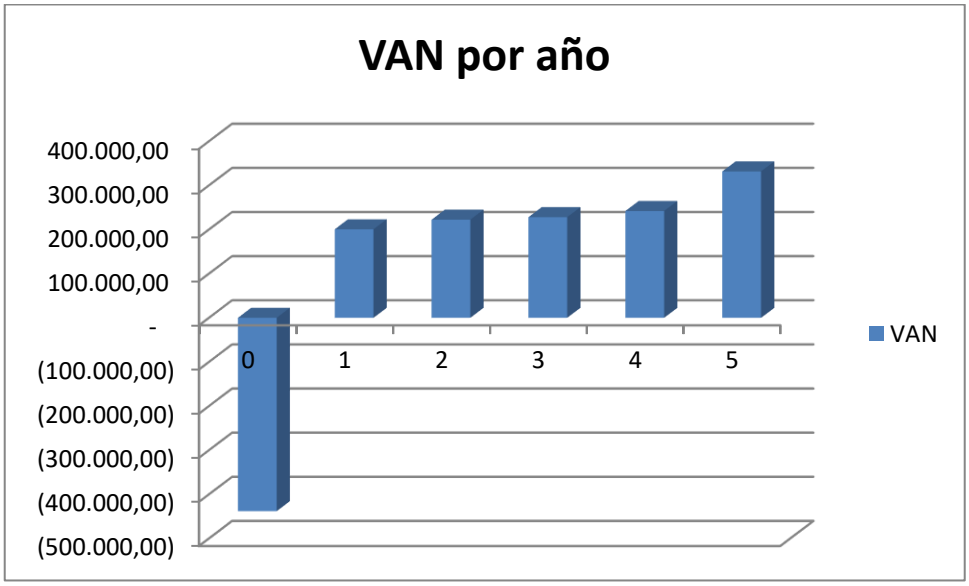

FIGURA 4-11 VAN POR AÑO

FUENTE: ELABORACIÓN PROPIA, 2016

Este indicador expone que el valor presente de los flujos de caja futuros generados por el proyecto en 5 años a valores actuales es $US 786,668.

Por lo tanto, concluimos que el proyecto es rentable y tiene la capacidad de aportar valor a la empresa.

5 CONCLUSIONES

5.1 HALLAZGOS DE LA COMPARATIVA DE ENFOQUES

Se puede observar de la descripción y comparación de los enfoques de evaluación de proyectos planteados en el capítulo anterior, que todos evidencian diversas fortalezas y debilidades desde la óptica de la gestión de identidades y accesos. Solo el modelo de Royer fue diseñado específicamente para IAM y el resto son modelos aplicables a todo tipo de proyectos de seguridad de tecnologías de la información.

Una primera clasificación propuesta por el presente trabajo para su mejor análisis es dividir los enfoques entre aquellos de tipo “framework” o “marco” y los enfoques de tipo “modelo” o “formales”.

Los enfoques de tipo marco, se caracterizan por presentar metodologías y/o lineamientos generales que deben adaptarse a cada estudio en particular y no precisan con detalle técnicas, métricas y componentes para la evaluación. Definen una estructura sobre la cual se debe llevar a cabo el estudio y la evaluación. En esta categoría se incluyen los enfoques de Butler, Bodin, Royer, Flores y Thomas.

Si se analizan mencionados enfoques, no establecen con precisión las variables involucradas. En contrapartida otorgan mayor libertad para definir todos los criterios que sean necesarios para el estudio, por lo tanto la inclusión de parámetros de IAM depende de quien realice la evaluación y el caso de estudio en particular. En algunos enfoques se incluyen métricas, sin embargo estas son incompletas y deben

perfeccionarse con las variables antes mencionadas. Estos frameworks pueden ser utilizados tanto para comparar proyectos como para sus cuantificar beneficios.

Por su parte los enfoques de tipo modelo, son aquellos que cuentan con un patrón expresado formalmente. Definen y detallan los elementos que lo componen y las relaciones entre ellos. Como resultado, son más precisos, pero acotan las posibilidades de implementación y los hace menos flexibles. En esta categoría se incluyen los enfoques de ENISA, Gordon, Sonnenreich, Mizzi, Cremonini y Wang.

En estos últimos modelos se observa un gran detalle y fundamento teórico de las variables y métricas, sin embargo solo se mide la reducción del riesgo dejando de lado los demás drivers de IAM. Estos enfoques pueden ser utilizados tanto para comparar proyectos como para cuantificar sus beneficios.

5.2 CONCLUSIONES DEL TRABAJO

El presente trabajo describe en primer lugar el marco teórico de la gestión de identidades y accesos. Se detallan definiciones básicas, se muestra el panorama general de los estándares relacionados y describe el Framework IAM.

A continuación, se analiza el contexto a nivel mundial. Se caracterizan los segmentos IGA e IDDAS y se identifica las principales tendencias en el mercado.

Por último, se estudia la evaluación económica de proyectos IAM, se listan y comparan los principales enfoques y modelos de evaluación de proyectos de seguridad y se lleva a cabo un ejemplo de aplicación.

Como resultado se llega a las siguientes conclusiones:

- IAM se refiere a los procesos, tecnologías y políticas para gestionar identidades digitales y controlar cómo las identidades pueden acceder y hacer uso de los recursos.
- IAM es un framework soportado por diversas tecnologías y estándares.
- Los proyectos de IAM tienen 5 drivers principales, la facilitación de negocios, la reducción de costos, la eficiencia operacional, la gestión de riesgos de TI y el cumplimiento regulatorio.
- Existen dos grandes mercados de gestión de identidades y accesos, uno más antiguo y maduro denominado IGA y otro emergente llamado IDAAS basado en la nube.
- Las principales tendencias de estos mercados apuntan a la integración con otras tecnologías de seguridad y la normalización respecto estándares mundiales.
- Existen diversos enfoques que pueden ser aplicados a la evaluación de proyectos de IAM y que son utilizados como soporte para la toma de decisiones.
- Uno de los puntos de partida para una correcta evaluación es la estructura misma del proyecto, especialmente en el caso de IAM que interviene a nivel de procesos organizacionales.
- Los enfoques pueden clasificarse en dos categorías, los de clase “framework” o “marco” y los enfoques de tipo “modelo” o “formales”.
- Se debe considerar que los métodos de evaluación estándares basados en medidas financieras no están bien adaptados para inversiones en seguridad, ya que no reflejan la amplia gama de beneficios potenciales, como los aspectos intangibles y la interconexión de los diferentes aspectos inherentes.
- Los modelos de evaluación de seguridad de la información clásica se enfocan principalmente en la reducción del riesgo dejando de lado diversos factores que deben considerarse desde la óptica de IAM.

- La mayoría de los métodos presentados no abordan el problema de la recolección de datos y la identificación de información relevante para el análisis. Además, la falta de datos empíricos como base para los análisis limita la significación.
- No es posible determinar todos los datos y variables con 100% de precisión en un plazo aceptable y con recursos limitados. Por lo tanto, los resultados sólo tienen que ser lo suficientemente precisos para la toma de decisiones.

Finalmente dado el análisis efectuado, puede arribarse a la confirmación de las hipótesis oportunamente planteadas. Queda demostrado que existen modelos en uso y aceptados por su rigor científico capaces de evaluar proyectos IAM con un grado de precisión razonable. Además, todos estos modelos fueron concebidos por sus respectivos autores para demostrar que bajo ciertas condiciones los proyectos pueden generar beneficios económicos.

Se espera que los conceptos discutidos en este documento fomenten una mayor investigación sobre la relación entre la productividad y la seguridad. Esta es una de las áreas más prometedoras para demostrar la sinergia entre la seguridad y el rendimiento financiero.

5.3 FUTURAS LÍNEAS DE INVESTIGACIÓN

Durante el desarrollo de la investigación se han detectado las siguientes líneas de trabajo y problemas abiertos:

- Investigar fuentes de información estadística relevantes y confiables para alimentar modelos de evaluación de proyectos.

- Profundizar en las técnicas de evaluación cuantitativa de los costos, beneficios y el riesgo.
- Estudiar enfoques alternativos como el de Royer y Meints que proponen un modelo basado en Balanced Scorecard (BSC). Este enfoque amplio promete ser una herramienta más completa para ayudar a ejecutivos a superar situaciones de toma de decisiones complejas. (Royer & Meints, 2009).

6 BIBLIOGRAFÍA

Al-Khouri, A. M. (2011). Optimizing Identity and Access Management (IAM) Frameworks. *International Journal of Engineering Research and Applications (IJERA), ISSN: 2248-9622. Vol. 1, Issue 3, pp.461-477*.

ANSI INCITS. (2004). *359 - Role Based Access Control.*

Bagchi, K., & Udo, G. (2003). An analysis of the growth of computer and Internet security breaches. *Commun. Assoc. Inf. Syst. 12, 684–700*.

Beaver, K. (2008). Making The Business Case For Information Security. *Security Technology and Design , 44-46.*

Belussi, A., Catania, B., Clementini, E., & Ferrari, E. (2007). Spatial Data on the Web: Modeling and Management. *Springer. p. 194. ISBN 978-3-540-69878-4.*

Bistarelli, S., Fioravanti, F., & Peretti, P. (2005). Defense trees for economic evaluation of security investments. *Availability, Reliability and Security.*

Bodin, L., & Loeb, M. P. (2005). Evaluating information security investments using the hierarchy.

Butler, S. A. (2002). Security Attribute Evaluation Method:. *Proceedings of the 24th International Conference on Software Engineering, 2002*.

Cheng, K. (2008). Return on Security Investment (ROSI).

Chong, F. (2004). Identity and Access Management". The Architecture Journal. Microsoft Corporation 2015. *The Architecture Journal. Microsoft Corporation 2015.*

Cisco Systems Inc. (2015). *2015 Annual Security Report.*

Cremonini, M., & Martini, P. (2005). Evaluating Information Security Investments from Attackers Perspective: the Return-On-Attack (ROA).

Demetz, L., & Bachlechner, D. (2013). To Invest or Not to Invest? Assessing the Economic Viability of a Policy and Security Configuration Management Tool. *The Economics of Information Security and Privacy*.

ENISA. (2012). *Introduction to Return on Security Investment.* European Network and Information Security Agency.

Ferraiolo, D., & Kuhn, D. (1992). Role Based Access Control. *15th National Computer Security Conf. Oct 13-16, 1992, pp. 554-563 the original paper that evolved into the NIST RBAC model. 43, no. 6 (June, 2010), pp. 79-81*.

Flores, W., Sommestad, T., Holm, H., & Ekstedt, M. (2011). Assessing Future Value of Investments in Security-Related IT Governance Control Objectives – Surveying IT Professionals. *Electronic Journal Information Systems Evaluation Volume 14 Issue 2*.

Forrester . (2011). *Twelve Recommendations For Your 2011 Security Strategy.* Forrester Research.

Forrester. (2011). *Identity Management Market Forecast: 2007 To 2014.* Forrester Research.

Forrester. (2015). *Navigate The Future Of Identity And Access.*

Forrester. (2015). *The Forrester Wave™: B2E Cloud IAM, Q2 2015.*

Forrester. (2016). *The Forrester Wave™: Identity And Access Management Suites, Q2 2016.*

Gartner. (2015). *Magic Quadrant for Identity and Access Management as a Service,.*

Gartner Inc. (2016). *Magic Quadrant for Identity Governance and Administration.*

Gordon, L., & Loeb, M. (2002). The Economics of Information.

Gordon, L., & Loeb, M. (2006). Economic aspects of information security: an emerging field of Research. *Inf. Syst. Front. 8(5), 335–337* .

ISO/IEC, 2.-1. (2011). Information technology -- Security techniques -- A framework for identity management -- Part 1: Terminology and concepts.

ITU. (2010). *X.1252 - Baseline identity management terms and.*

ITU. (2010). *X.1252 - Baseline identity management terms and definitions.*

Jackson, L., & Al-Hamdani, W. (2008). Economic acceptable risk assessment model. Proceedings of the 5th annual conference on Information security curriculum development.

KPMG. (2008). *KPMG's 2008 European Identity & Access Management Survey - Status and maturity of identity and access management projects in European organizations.*

Lewis, J. (2003). Enterprise Identity Management: It's About the Business. *The Burton Group Directory and Security Strategies Report.*

Magnusson, C., Molvidsson, J., & Zetterqvist, S. (2007). Value creation and Return On Security.

McQuaide, B. (2003). Identity and Access Management. Transforming E-security into a Catalyst for Competitive Advantage. *Information System Contro Journal, volumen 4.*

Mizzi, A. (2010). Return on information security investment: the viability of an anti-spam solution in a wireless environment. *Int. J. Netw. Secur. 10(1), 18–24.*

Mont, M. C., Beres, Y., & Pym, D. S. (2010). Economics of Identity and Access Management: Providing decision support for investments. *Network Operations and Management Symposium Workshops (NOMS Wksps)*.

North, J. (2008). The Total Economic Impact Of Identity Manager.

OASIS. (2005). *SAML V2.0 Executive Overview*.

Pato, J. (2005). Identity Management. *Encyclopedia of Cryptography and Security. Springer, pp. 282–285.*

Royer, D. (2007). Enterprise Identity Management – What's in for Organisations.

Royer, D., & Meints, M. (2009). Enterprise Identity Management Towards a Decision Support Framework Based.

Sandhu, R. S., Coyne, E., Feinstein, H., & Youman, C. (1996). Role-Based Access Control Models. *IEEE Computer 29(2): 38-47, IEEE Press, 1996.- proposed a framework for RBAC models.*

Sandhu, R., Ferraiolo, D., & Kuhn, R. (2000). The NIST Model for Role Based Access Control: Towards a Unified Standard. *Proceedings, 5th ACM Workshop on Role Based Access Control, July 26-27, 2000, Berlin,pp.47-63. - initial proposal for the current INCITS 359-2004*.

Solms, B. V., & Solms, R. V. (2004). The 10 deadly sins of information security Management. *Computers & Security, Vol.23 No 5 (ISSN 0167 -4048, 2004), pp. 371-376.*

Sonnenreich, W. (2006). Return On Security Investment (ROSI) - A Practical Quantitative Model. *Journal of Research and Practice in Information Technology, Vol. 38, No. 1.*

Su, X. (2006). An Overview of Economic Approaches to Information Security Management.

Theodosios, T. (2010). Information Security Expenditures: a Techno-Economic Analysis .

Thomas, R. C. (2009). Total Cost of Security – A Method for Managing Risks and Incentives Across the Extended Enterprise.

Wagner, R. (2010). *Identity and Access Management.* Gartner.

Wang, J., Chaudhury, A., & Rao, R. (2008). A Value-at-Risk Approach to Information Security Investment.

Willemson, J. (2006). On the Gordon & Loeb Model for Information Security Investment.

Windley, P. (2005). *Digital Identity.* OReilly.

Witty, R. J. (2003). *Five Business Drivers of Identity and Access.*

7 ANEXOS

A continuación, se listan los documentos anexos a este trabajo:

- Anexo 1 - Carta Assertiva: Carta de autorización de la consultora de seguridad informática Assertiva S.A. para obtener asesoramiento de su staff e información estadística.