COBIT 5.0 EN UNA ARQUITECTURA ORIENTADA A SERVICIOS: GESTIÓN Y TRATAMIENTO DE RIESGOS EN SERVICIOS WEB

Gaitán, Luis
lfernando.gaitanp@gmail.com
Universidad Piloto de Colombia

***Resumen* – En este documento se presenta un método de gestión y tratamiento de riesgos para servicios web en SOA (Arquitectura Orientada a Servicios), utilizando el marco de referencia COBIT 5.0, sus etapas más importantes en procesos de riesgo y los controles y medidas adecuadas en la preservación de la seguridad de la información. Se hace una reseña de las características y propiedades de la arquitectura orientada a servicios y las situaciones que implica el trabajo con servicios web, encontrando elementos que pueden ser integrados con COBIT 5.0, en un proceso de administración y gobernabilidad que propone el cuidado de las propiedades de la seguridad, tales como: Confidencialidad, integridad y disponibilidad, así como un método de atención a eventos, incidentes, amenazas y vulnerabilidades que impactan a las organizaciones que se encuentran trabajando bajo esquemas de servicios web y donde sus riesgos no son supervisados y gestionados.**

***Abstract* - This document presents a risk management and treatment method for web services in SOA (Service Oriented Architecture), using the COBIT 5.0 framework, its most important stages in risk processes, and adequate controls and measures in the preservation of information security. It outlines the characteristics and properties of the service-oriented architecture and the situations involved in working with web services, finding elements that can be integrated with COBIT 5.0, in a process of administration and governance that proposes the care of the properties security, such as: Confidentiality, integrity and availability, as well as a method of attending to events, incidents, threats and vulnerabilities that impact organizations that are working under web services schemes and where their risks are not supervised and managed.**

***Índice de Términos* – Framework, gobierno, riesgo, servicio, vulnerabilidad.**

***Keywords* – Framework, governance, risk, service, vulnerability.**

I. INTRODUCCIÓN

En las empresas, el activo a nivel de seguridad más importante es la información, caracterizada por su continuo movimiento e interacción con personas, sistemas y ambientes. Dentro de las actuales necesidades de tránsito y transformación que vive la era actual de la información, surge la implementación de sistemas, que más allá de ser un mecanismo de organización, constituyen un elemento fundamental y una oportunidad para fortalecer y aprovechas los tres pilares de la seguridad: Integridad, disponibilidad y confidencialidad, estas tres propiedades que a lo largo de la historia de la seguridad son preservadas ante usuarios inescrupulosos que pueden sustraer, modificar y borrar la información.

Uno de los objetivos del especialista en seguridad de la información se basa en escoger las mejores prácticas para proteger la triada en el mejor estado posible, reduciendo el daño y anulando las incidencias de los ataques a la información; estas razones acompañadas de varios elementos técnicos conducen a encontrar respuestas en las arquitecturas y frameworks de diversos tipos, pero en especial la orientada a servicios SOA.

Extraer elementos de SOA y COBIT, permite tener una herramienta integral que logra atender las necesidades de gestión y tratamiento de riesgos a un nivel organizacional, pero puntualmente en los servicios web creados dentro de la arquitectura SOA, siendo hoy por hoy un modelo de gobernabilidad y de éxito a nivel de desarrollo de software, que se puede articular con las empresas y servir como estándar para manejar sus procesos de forma eficiente, segura y recursiva.

Combinar una arquitectura y un framework implican una forma de hacer gestión de procesos de manera controlada, de tal manera que tanto el negocio como las tecnologías de la información logran disminuir los riesgos en la toma de decisiones cuando un cambio puede afectar la organización desde cualquiera de estos ejes.

SOA y COBIT, al estar enfocados en un camino similar, permiten un acercamiento a un aspecto muy importante en las organizaciones: La gobernabilidad como eje central de la gestión y tratamiento de riesgos, permite a un esquema bien definido, una convergencia entre procesos de negocio, factores externos y seguridad.

Gestionar y tratar riesgos, implica una alta comprensión de las necesidades y requisitos del negocio que dimensionan clara y transparentemente, a qué nivel de exposición se puede llegar y qué tanto se puede asumir dentro de las organizaciones, por consiguiente, se hace necesario cambiar la forma en que se

relacionan los procesos de negocio y las tecnologías, convirtiendo los procesos en esquemas definidos, articulados e implementados por quienes tienen el conocimiento para gestionar y promover su desarrollo en las compañías.

El modelo propuesto en este documento, parte de la gobernabilidad propuesta por SOA y se enfoca en riesgos netamente asociados a servicios REST y RAW, que bajo un marco de tratamiento COBIT, permiten mitigar estas situaciones mediante las mejores prácticas y a un costo bajo.

II. SOA: ARQUITECTURA ORIENTADA A SERVICIOS

El concepto de SOA, (Service Oriented Architecture - Arquitectura Orientada a Servicios), no es nuevo, ha sido promovido desde los años 80's y fue impulsado por las comunidades que dieron inicio al diseño de software a través de componentes, que en su momento fue conocido como la "Programación Orientada a Objetos" (OOP), por sus siglas en inglés Oriented Object Programming.

En 1983, la ISO (International Standards Organization) adoptó el modelo OSI (Open System Interconnect) como una referencia estándar para el desarrollo de patrones de comunicaciones de datos. A pesar del avance tecnológico y el cambio de capacidades que se han observado en cada capa del modelo OSI, la arquitectura permanece en el tiempo.

Al hacer una correlación de este concepto respecto a la funcionabilidad que debe presentar un servicio tecnológico, en la medida que las interfaces o relaciones entre servicios permanezcan estables y soportadas con estándares de industria, los servicios, en sí mismos, pueden ser cambiados fácilmente según las necesidades que vayan demandando los requerimientos de negocio.

Se denomina Arquitectura Orientada a Servicios, a un marco conceptual de arquitecturas informáticas de negocios, que se caracteriza por ofrecer las funcionalidades básicas de los sistemas de información de una empresa a través de servicios reutilizables.

El principal objetivo de SOA, es construir los distintos sistemas de información de una empresa, sobre un conjunto de estándares informáticos, con el objetivo de que todos ellos, incluso los realizados con distintas tecnologías, puedan operar de forma integrada y sin que existan dependencias entre los mismos.

En el contexto SOA, el gobierno es el proceso que asegura que todos los intereses de los participantes en la arquitectura sean tenidos en cuenta en la planeación, diseño y ejecución de una organización. En este sentido el gobierno SOA hace referencia a la organización, procesos, procedimientos, políticas y métricas requeridas para administrar SOA exitosamente, entendiendo como exitosa que conoce y promueve los objetivos del negocio durante todo el tiempo.

La seguridad SOA se presenta como un subconjunto de la función del gobierno SOA, siendo fundamental este aspecto en los servicios de seguridad, ya que la aplicación es vital para la integridad del ambiente o entorno en el que se implemente. Un marco para la estructura de gobierno y la toma de decisiones efectivas es necesario en la orientación del negocio. Las herramientas y tecnologías pueden ayudar a facilitar iniciativas de gobierno y evaluaciones de cumplimiento. Una seguridad eficaz dentro de un marco de gobierno implica establecer cadenas de responsabilidad, autoridad y comunicación que permitan capacitar a las personas para controlar eficazmente el sistema.

Debido a que SOA extiende las interacciones más allá de los límites de la empresa, la seguridad en la arquitectura debe interactuar con grupos similares de otras organizaciones para lograr un conjunto común de normas que permitan definir reglas y parámetros, tanto al interior como al exterior de las compañías.

La ausencia de gobierno para SOA puede provocar los siguientes problemas:

-El programa SOA entrega resultados inconsistentes.

-El crecimiento es caótico a nivel de infraestructura y servicios.

-Los servicios tienen funcionabilidad redundante.

-Se dispone de servicios que no se pueden reutilizar en la organización.

-Existe una inconsistencia en la identificación, diseño y uso de los servicios.

-No se definen métricas para cuantificar el éxito.

-Existe una ausencia de coordinación entre proyectos.

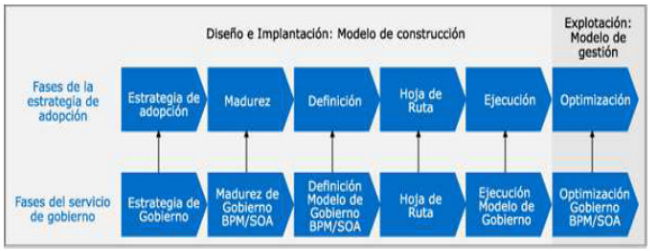

Fig. 1. Fases en el gobierno SOA [1]

En la figura 1 se muestran las fases del gobierno SOA, cada una de ellas pretende dotar de los mecanismos de control, procesos, procedimientos y métodos probados en la práctica para garantizar el orden en las decisiones que se tomen en una iniciativa, evitando el caos en cualquier proyecto SOA que se planteé, logrando la efectividad y agilidad esperada en la transición hacia SOA. [1]

A. Procesos de Gobierno SOA

Los procesos de Gobierno SOA, son esenciales para definir las acciones a realizar en diferentes áreas estratégicas y tácticas de la organización. Algunos de los procesos más cruciales en el Gobierno SOA son:

- Procesos para la gestión del portafolio de servicios, cuya finalidad es establecer e identificar el inventario de los servicios que se encuentran disponibles en la organización.

- Procesos del ciclo de vida de los servicios, aquí se establece la gestión en ciclo de vida de los servicios SOA; uno de los framework que apoyan dicho proceso es AUT SOA.

- Procesos de gestión del cambio, estos son realizados con el fin de establecer reglas, versiones, procedimientos y métodos en los servicios, que se encuentran expuestos en la organización.

B. Principio de seguridad en SOA

Los principios de seguridad generales que se aplican en cualquier entorno son: Identidad, autenticación, autorización, confidencialidad, integridad, auditoría y cumplimiento, gestión de políticas y disponibilidad.

La gestión de la seguridad es un tema transversal a todos los procesos de las compañías, en especial a los ciclos de vida de software y es un facilitador clave para lograr los objetivos de conectividad y flexibilidad. Conforme a los procesos ya mencionados se debe realizar un examen de los requisitos de alto nivel para la gestión de la seguridad en SOA, donde se destacan los siguientes aspectos:

- La seguridad, es un requisito comercial, no sólo tecnológico. Los arquitectos empresariales se preocupan por los desafíos de identidad y seguridad de SOA, porque tienen visibilidad del panorama general.

- La necesidad de identidades de usuarios y servicios y la propagación de estas identidades en toda la organización. Es poco probable que las identidades de usuario sean las mismas en todos los servicios, las cuales componen un flujo de procesos empresariales, toda vez que involucran varias organizaciones.

- La necesidad de conectarse perfectamente a otras organizaciones en tiempo real y transaccional. A nivel de servicios web existen varias formas de interacción entre organizaciones. Ejemplo: Se pueden integrar interfaces de usuario de servicios de diferentes dominios u organizaciones en una interfaz de portal. Otro ejemplo, es un servicio prestado por una organización que se invoca directamente desde un proceso de negocio, independientemente de la forma de la interacción, es necesario que la seguridad, la identidad, y las políticas de acceso se definan y se apliquen para todas las transacciones entrantes y salientes.

- El aseguramiento sobre todas las aplicaciones, donde todos los controles se promulguen para cada servicio y sus diferentes sub servicios. Por tanto, los Identity Services deberán validar la identidad del receptor y confirmar que estén autorizados para realizar la operación y mapear la identidad al servicio de destino, para que pueda entender y utilizar la transacción o solicitud.

- La protección de los datos en tránsito y en reposo. Los servicios de seguridad frontera son un punto de partida para las transacciones, debido a que son capaces de proporcionar una verificación a las solicitudes y establecen una relación de confianza entre las organizaciones, permitiendo la cooperación entre éstas. Esto implica establecer reglas alrededor de la interacción activa o pasiva, como la definición de información de identidad que debe propagarse entre las organizaciones, así como el establecimiento de las claves criptográficas para asegurar los mensajes.

- La definición de un estándar de cumplimiento de un conjunto de empresas, en la parte industrial y en las normas regulatorias.

- La seguridad SOA debe abarcar el ciclo completo de desarrollo a través de las fases de modelamiento, ensamblaje, implementación y administración de aplicaciones SOA, como se observa en la figura 2:

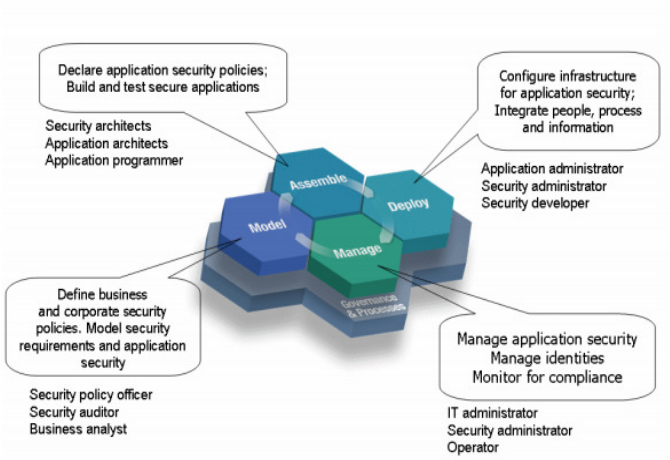

Fig. 2. Ciclo de vida en servicios desde una perspectiva de seguridad [1]

C. Principio de gestión de riesgos en SOA

La gestión de riesgos se ocupa inicialmente del proceso de evaluación sobre SOA, posteriormente se desarrollan estrategias para manejar el nivel de exposición. La administración del riesgo mediante un proceso de gestión se determina en función de los factores, tales como la probabilidad e impacto, que equilibran los riesgos con el costo.

Es necesario procesos y políticas empresariales para definir las funciones de la organización, las responsabilidades y la autoridad que debe existir en ella.

El riesgo más alto que contiene una arquitectura SOA, es pensar que es una tecnología. Teniendo en cuenta el concepto de varios expertos, SOA es un conjunto de dos niveles: Estratégico y organizacional; de éstos, no se puede desligar la tecnología, por cuanto los servicios y la implementación requieren de su ayuda.

III. COBIT 5.0 UN FRAMEWORK DE GOBIERNO Y GESTIÓN DE RIESGO

Una definición corta de COBIT 5 es que ayuda a las organizaciones a crear un valor óptimo a partir de las tecnologías de la información, al mantener un equilibrio entre

la obtención de beneficios y la optimización de los niveles de riesgo y utilización de los recursos.

COBIT 5 permite que las tecnologías de la información relacionadas se gobiernen y administren de una manera holística a nivel de toda la organización, incluyendo el alcance completo de todas las áreas de responsabilidad funcionales y de negocios, considerando los intereses relacionados de las partes interesadas internas y externas.

Los principios habilitadores de COBIT 5 son genéricos y útiles para las organizaciones de cualquier tamaño, bien sean comerciales, sin fines de lucro, o en el sector público.

COBIT (objetivos de control para tecnología de la información y tecnologías relacionadas). Por sus siglas en inglés, Control Objectives for Information Systems and related Technology, es el marco desarrollado por ISACA (Information Systems Audit and Control Association) para el gobierno de las TI, lanzado en 1996 y desde entonces ha cambiado las prácticas para el gobiernos de las TI, los procesos de negocio y las prácticas de control; este marco consolida en forma eficiente los estándares de fuentes globales, permitiendo de esta manera la integración y el control de las organizaciones en TI y demás áreas del negocio.

Desde el marco inicial de COBIT hasta el momento se pueden analizar diferentes versiones, en las cuales se presentan características diversas que han ido avanzando hasta llegar a la versión 5.0 (ISACA, 2012) con la cual contamos en la actualidad, situación que se aprecia en la figura 3.

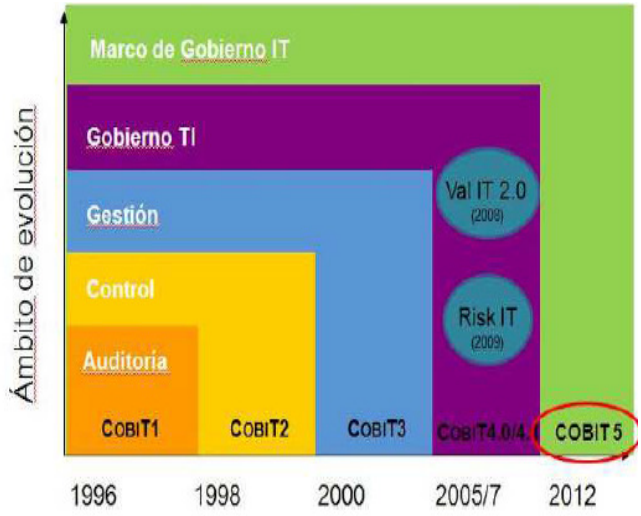

Fig. 3. Evolución de versiones COBIT [2]

Dentro de las diferentes versiones publicadas de COBIT, existe un factor común y es precisamente la unidad de las tecnologías de la información con las demás áreas de las organizaciones.

Por tanto, COBIT, se aplica a los sistemas de información, además de la gestión de la tecnología y la implementación de los procesos de gobierno de toda la organización; todo el modelo se basa en que los recursos de TI y demás procesos deben ser administrados por un conjunto de procesos naturalmente agrupados para proveer la información pertinente y confiable que requiera una organización, para lograr sus objetivos.

La estructura planteada por COBIT, propone un marco donde los diversos criterios de la información son analizados y evaluados, criterios tales como la seguridad, la calidad y demás variables en el desempeño de la organización, teniendo en cuenta, los recursos tanto físicos, como humanos, que entran en relación directa con la información y los procesos, elevando así el número de herramientas que contribuyan en una correcta evaluación.

El modelo de referencia de procesos de COBIT 5, divide los procesos de gobierno y de gestión de las TI empresarial en dos dominios principales:

- Gobierno: Contiene cinco procesos de gobierno; dentro de cada proceso se definen prácticas de evaluación, orientación y supervisión (EDM)

- Gestión: Contiene cuatro dominios, alineados con las áreas de responsabilidad y de actividades propias, tales como: Planificar, construir, ejecutar, supervisar y proporcionar la cobertura de extremo a extremo de las TI. [2]

Estos dominios son una evolución de la estructura de procesos y dominios de COBIT 4.1. Los nombres de estos dominios han sido elegidos, teniendo en cuenta las designaciones de áreas principales, pero contienen más verbos para describirlos:

-Alinear, Planificar y Organizar (Align, Plan and Organize, APO)

-Construir, Adquirir e Implementar (Build, Acquire and Implement, BAI)

-Entregar, dar servicio y Soporte (Deliver, Service and Support, DSS)

-Supervisar, Evaluar y Valorar (Monitor, Evaluate and Assess, MEA)

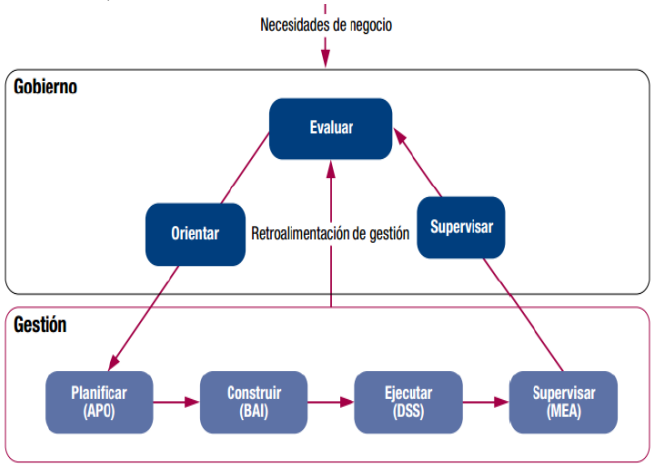

Fig. 4. Áreas claves de gobierno y gestión de COBIT 5 [2]

IV. COBIT 5.0 EN LA LINEA DE GOBERNABILIDAD SOA

Esta línea presenta un esquema de funcionamiento general de las fases de un modelo de gobernabilidad, aprovechando los elementos estratégicos de SOA y COBIT y resaltando que el dominio APO12 del modelo COBIT, puede ser incluido en un método para tratar los riesgos en servicios web. A continuación, se describen los pasos requeridos:

1. Definir un esquema de gestión de arquitectura de la organización, tomando elementos representativos de gestión, cooperación e integración, permite contribuir a las metas del negocio e inversión en TI. Así mismo se deben definir los objetivos, riesgos, costos y toda una estrategia administrativa que involucre los temas normativos y legales. Este esquema debe ser detallado, de tal manera que se lleve a cabo los planes tácticos acordes con las fases posteriores. En esta primera fase se debe tener en cuenta la exposición de servicios web seguros a los clientes, que, mediante la definición del esquema de gestión, se pueda analizar, si es viable reutilizar estos servicios, reconociendo y aceptando la necesidad de una iniciativa de implementación o mejora, lo que permitirá identificar los puntos débiles actuales, desencadenando y creando el ánimo de cambio a un nivel de dirección ejecutiva.

2. Determinar la arquitectura actual de la organización y los servicios e integraciones presentes, con el objetivo de generar un inventario y asegurar la infraestructura tecnológica, así como definir las necesidades de seguridad informática que requiere la fase de orientación, concentrándose en el alcance de la iniciativa de implementación o mejora, empleando el mapeo de COBIT de metas empresariales con metas de TI, a los procesos de TI asociados y considerando que los escenarios de riesgos podrían destacar los procesos claves de focalización. Los diagnósticos de alto nivel también pueden ser útiles para delimitar y entender áreas de alta prioridad en las que se hace necesario centrar la atención. Se lleva a cabo una evaluación del estado actual y se identifican los problemas y deficiencias mediante la ejecución de un proceso de revisión de capacidad. Se deben estructurar iniciativas de gran escala, como múltiples iteraciones del ciclo de vida, para cada iniciativa de implementación que exceda los seis meses, existe un riesgo de perder el impulso, el objetivo y el interés de las partes implicadas.

3. En la gestión por procesos se debe establecer y mantener un marco de trabajo financiero, para administrar las inversiones, los costos de los activos y los servicios. Todo esto garantiza la estabilidad financiera necesaria para dar cumplimiento con el respaldo a las propuestas de TI y permitir de esta manera, que los objetivos de negocio se definan clara y directa con los requerimientos de TI. La administración financiera se convierte en este caso, en uno de los esquemas fundamentales para el desarrollo de la organización, sin percances de último momento y evitando retrasos en el desarrollo de las metas de TI.

4. Definir los canales y puntos de comunicación efectivos, que permitan asegurar el entendimiento y conocimiento de los objetivos entre todas las partes interesadas

5. Definir planes que permitan establecer los marcos y modelos de trabajo para una adecuada transición, además de dar prioridades, especificar y acordar los planes de transiciones que conlleva una arquitectura orientada a servicios, que cubran el alcance completo de todas las iniciativas requeridas para lograr los resultados esperados de los programas de inversión en TI. Se establece un objetivo de mejora, seguido de un análisis más detallado aprovechando las directrices de COBIT para identificar diferencias y posibles soluciones. Algunas soluciones pueden ser beneficios inmediatos (quick wins) y otras actividades pueden ser más desafiantes y de largo plazo.

6. Definir una arquitectura de referencia: Para una adecuada gestión por proceso se debe establecer y mantener un modelo de información empresarial para SOA, que facilite el desarrollo de aplicaciones integrales y las actividades de soporte en la toma de decisiones, consistente con los planes de TI. El modelo debe facilitar la creación, uso y la posibilidad de compartir en forma óptima la información por parte del negocio, de tal manera que se mantenga la integridad, flexibilidad, funcionabilidad, seguridad y tolerancia en fallos.

7. Definir procesos, organización y relaciones: El marco de trabajo debe incluir estructura y relaciones de TI (administrando brechas y superposiciones de proceso), propiedad, medición de desempeño, mejoras, cumplimiento, metas de calidad y planes para alcanzarlas. El marco debe proporcionar integración entre los procesos que son específicamente de TI, administración del portafolio de la empresa, procesos de negocio y procesos de cambio de negocio. Planificar soluciones prácticas mediante la definición de proyectos apoyados por casos de negocios justificados. Además, se desarrolla un plan de cambios para la implementación. Un caso de negocio bien desarrollado asegura los beneficios del proyecto.

8. Implementar planes de transición: La gestión por procesos se deberá desarrollar con planes de transición en SOA, con base en el marco de trabajo, diseñado para reducir el impacto de una interrupción mayor de las funciones y de los procesos claves del negocio. Los planes deben considerar requerimientos de resistencia, procesamientos alternativos y capacidad de recuperación de todos los servicios críticos de la arquitectura orientada a servicios. Estos planes deben cubrir lineamientos de uso, roles, responsabilidades, procedimientos, procesos de transiciones de los servicios y un enfoque de pruebas.

9. Habilitar la operación y uso de los servicios: Garantizar un adecuado control de los servicios, que apoyen la gestión por procesos, dentro de un esquema por etapas: Definir, implementar, mantener y habilitar procedimientos estándar, para la operación de los servicios y garantizar que el personal

de operaciones esté familiarizado con todas las tareas de esta área.

10. Monitoreo y evaluación del rendimiento: Establecer un marco de trabajo de monitoreo general y un enfoque que defina el alcance, la metodología y el proceso a seguir, para medir la solución y la entrega de servicios SOA, donde éstos a su vez, permitan evaluar el rendimiento que tienen dichos servicios en la contribución que realiza TI al negocio. Además, es relevante el diseño de sistemas que evalúen constantemente los procesos y el enfoque de la organización, donde la aplicación de SOA genera un crecimiento y un apoyo constante a los requerimientos de TI en la organización. Se pueden definir las mediciones y establecer la supervisión, empleando las metas y métricas de COBIT para asegurar la consecución de alineación con el negocio, donde el rendimiento puede ser medido. El éxito requiere del compromiso y la decisión de la alta dirección, así como las partes involucradas con el negocio.

11. Administrar políticas de conformidad: Para lograr este objetivo se deben establecer políticas que permitan el trabajo integral, donde los aspectos de las diversas fases se integren de manera directa; además, es importante generar espacios para realizar las revisiones respectivas, que faciliten la consecución de objetivos comunes de las diversas áreas de la organización, en su integración a SOA. Se revisa el éxito global de la iniciativa, se identifican requisitos adicionales, para el gobierno o la gestión de la TI empresarial y se refuerza la necesidad de la mejora continua. [3]

A. Administración de Riesgos en COBIT 5 una referencia para SOA

El dominio de Gobierno contiene cinco procesos de gobierno, dos de los cuales se enfocan en el riesgo relacionado con los objetivos de los terceros interesados:

- *EDM03 - Asegurar la optimización de riesgos.* Asegurar que los riesgos relacionados con TI no superen la tolerancia al riesgo y el nivel de riesgo; el impacto de los riesgos de TI de valor de la empresa es identificado y manejado, y la posibilidad de fallas de cumplimiento es mínimo. El dominio de Gestión, Alinear, Planear y Organizar, contiene un proceso de riesgos relacionados: APO12 Gestionar el riesgo.

- *APO12 - Gestionar el riesgo.* Continuamente identificar, evaluar y reducir los riesgos relacionados con TI, dentro de los niveles de tolerancia establecidos por la dirección ejecutiva de la empresa. En este dominio de desarrollo del modelo de COBIT, se plantea generalmente una estrategia y un método a seguir, con el cual se busca identificar, en qué forma las tecnologías de la información logran de manera acertada contribuir al desarrollo y logro de los objetivos de las organizaciones, por tanto, se genera una visión estratégica que debe ser administrada y comunicada, para acoplar al modelo de negocio, buscando así, una mejor comprensión de las estrategias de negocio y su futura integración con las estrategias de TI (IT Governance Institute, 2007).

Este dominio cubre los siguientes cuestionamientos típicos de la gerencia:

-¿Están alineadas las estrategias de TI y del negocio?

- ¿La empresa está alcanzando el uso óptimo de sus recursos?

-¿Entienden todas las personas dentro de la organización los objetivos de TI?

-¿Se entienden y administran los riesgos de TI?

-¿Es apropiada la calidad de los sistemas de TI para las necesidades del negocio?

Las políticas deben estar alineadas con el umbral de riesgo de la empresa y son un componente clave de los sistemas de control interno en la empresa, cuyo propósito es gestionar y contener el riesgo. Como parte de las actividades de gobierno sobre los riesgos, se define la tolerancia de la empresa a los mismos y debe quedar reflejada en las políticas.

Una empresa propensa al riesgo tiene políticas más restrictivas que una empresa sólida. Las políticas necesitan ser revalidadas y/o actualizadas en intervalos regulares. El objetivo final del proceso es integrar la gestión de riesgos empresariales relacionados con la TI con el ERM en general, y equilibrar los costos y beneficios de la gestión de riesgos relacionados con TI de la empresa.

Todas las actividades de la empresa tienen una exposición de riesgos asociados, derivados de las amenazas ambientales que aprovechan las vulnerabilidades del factor habilitador.

Todos los demás procesos incluyen prácticas y actividades que son diseñadas para tratar el riesgo relacionado (evitar, reducir / mitigar / controlar/ compartir / transferir / aceptar). [4]

V. ESQUEMA DE TRATAMIENTO Y GESTIÓN DE RIESGOS EN SOA

Como se ha mencionado a lo largo de la especialización, los responsables de la seguridad deben estar en condiciones, de evitar o aceptar riesgos individuales, o reducir los riesgos a un nivel aceptable. La reducción de riesgos a un nivel aceptable supone adoptar las contramedidas apropiadas en la práctica. Todo lo anterior se une en varias etapas, según los expertos en implementación se recomienda que después de cada etapa, haya una reflexión conjunta para tomar oportunas decisiones. En esencia, los contenidos y objetivos de cada etapa son los que se resumen a continuación y se recogen en un modelo de administración de seguridad:

- Primera etapa: Identificar la naturaleza y ámbito del sistema, sujeto a revisión de sus componentes.

- Segunda etapa: Evaluar las amenazas y vulnerabilidades.

- Tercera etapa: Gestionar los riesgos identificados.

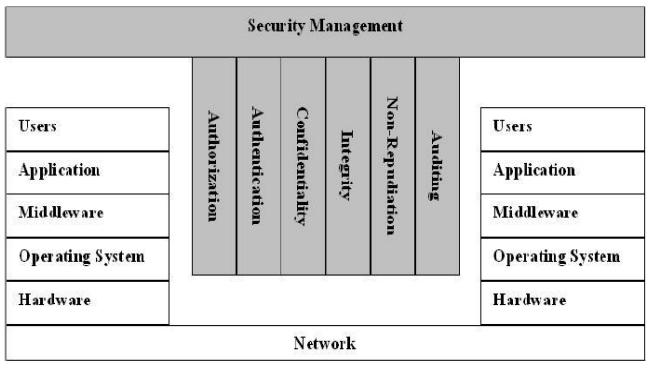

Fig. 5. Modelo UT para seguridad en SOA [8]

El proceso COBIT AP012 define una guía de medidas detalladas, teniendo en cuenta los riesgos determinados durante la etapa anterior, estableciendo un nivel de comparación con el nivel de seguridad, (un nivel de umbral asociado con cada contramedida) con el fin de identificar, si los riesgos son suficientemente grandes para justificar la instalación de un determinado control de mitigación

Las recomendaciones adaptadas al caso SOA – COBIT se definen de la siguiente manera:

1. APO12 Debe existir un perfil de riesgo actual y completo desarrollado por la función de aseguramiento para la tecnología, las aplicaciones, los procesos y la infraestructura dentro de la arquitectura. Este perfil debe ser medido por la existencia, puntualidad e integridad de los perfiles de riesgo.

2. De acuerdo con APO12.01, es necesario identificar y recopilar datos pertinentes para permitir el análisis y notificación de riesgos relacionados con las TI, garantizando el perfil de riesgo empresarial y las políticas y procedimientos de la función de aseguramiento. Este paso permitirá identificar y recopilar datos pertinentes en el análisis y notificación de riesgos para un aseguramiento efectivo.

3. APO12.02 Analizar el riesgo, extrayendo información útil para apoyar las decisiones, teniendo en cuenta la pertinencia de los factores de riesgo. La función de aseguramiento identifica los análisis y evalúa el riesgo dentro de la arquitectura.

4. APO12.03 Mantener un perfil de riesgo a través de un inventario que contenga los atributos de riesgo y riesgos conocidos (incluyendo la frecuencia esperada, el impacto potencial y las respuestas), de los recursos, capacidades y actividades de control actuales.

5. APO12.04 Proporcionar información sobre el estado actual de las exposiciones y oportunidades relacionadas con las TI, de manera oportuna a todas las partes interesadas necesarias para una respuesta adecuada. Definir e implementar estrategias de evaluación de riesgos.

6. APO12.05 Definir una serie de acciones de gestión de riesgos: Gestionar oportunidades para mitigar el riesgo a un nivel aceptable.

7. APO1206 Responder al riesgo de manera oportuna con medidas efectivas para limitar la magnitud de la pérdida de eventos relacionados con TI. Incluir los niveles de riesgo como insumo en la planificación del aseguramiento. [5]

El proceso de análisis y gestión de riesgos de un modelo de gobernabilidad SOA – COBIT se resume en la figura 5:

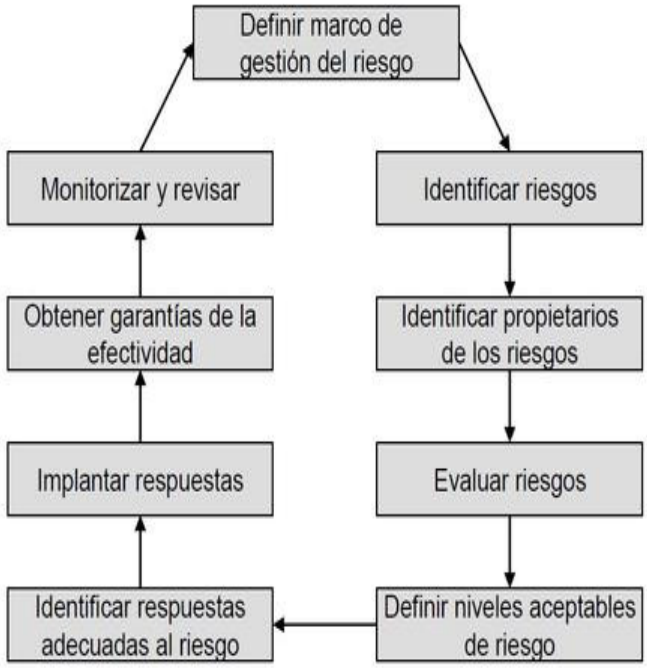

Fig. 6. Proceso de gestión de riesgo [4]

VI. RIESGOS Y VULNERABILIDADES EN SERVICIOS WEB

Los servicios web específicos para los proyectos globales soportan la operación total de las compañías, pero los riesgos y vulnerabilidades en seguridad no son medidos, ni tenidos en consideración, al inicio del proyecto, saltando esa premisa o mejor práctica previa a la implementación de seguridad en SOA, que menciona una fase de definición del proyecto integral, que a futuro permite intervenir los riesgos y mitigarlos de la manera más adecuada.

El riesgo puntual al que se ven enfrentados los servicios desarrollados en una arquitectura orientada a servicio es su deficiente seguridad y poca implementación de los estándares ya existentes. En conclusión, los proyectos de muchas compañías a nivel web delegan la seguridad a la protección de un firewall y el cifrado utilizado es de tipo https.

Los riesgos en servicios web sobre SOA se manifiestan en los siguientes aspectos:

- Alta exposición de aplicaciones que son críticas para el negocio.

- Los mecanismos como firewall y cifrados por protocolo actualmente no cubren servicios desarrollados en XML/SOAP.

- El backend termina siendo una puerta de entrada a conexión, con servicios propios de las compañías, debido a que el tráfico proveniente de esta parte no tiene un monitoreo constante y los ataques pueden ser encapsulados.

- El uso de XML en los servicios provee una carga natural al servidor de aplicación, debido a que la transformación y procesamiento de datos, consume recursos de hardware significativos afectando el rendimiento, razón por la cual, las empresas deshabilitan los dispositivos de validación y dejan una exposición importante de la arquitectura.

- Los incrementos de ataques basados en XML no están contemplados por los dispositivos de seguridad físicos y lógicos.

- Las vulnerabilidades conocidas, que, al materializarse en riesgos, pueden tener consecuencias a nivel de reputación, confidencialidad, disponibilidad e integridad son las siguientes:

-Escaneo en WSDL: La estructura del WSDL en un servicio Web, muestra las operaciones, parámetros y enlaces de red. Algunas de estas operaciones, deben ser utilizadas solamente por el proveedor de servicios. Por ejemplo, operaciones administrativas. El resto de las operaciones, pueden ser invocadas por cualquier consumidor de servicio. Gran parte de los datos vitales de un servicio Web están disponibles en el manifiesto WSDL. El atacante puede intentar adivinar el nombre de la operación interna e invocarla obteniendo datos de parámetros y operaciones internas.

-Suplantación de metadatos: Un atacante puede modificar los metadatos relacionados con los servicios Web, tales como el manifiesto WSDL asociado a WS-Security. Por ejemplo, el punto final del servicio Web puede modificarse para que el atacante establezca un ataque de "hombre en el medio" por espionaje o incluso peor, por paso de datos modificados a los servicios Web.

-Ataque de ofuscamiento: Los estándares XML Encryption y XML Signature se utilizan para proporcionar cifrado y servicios de firma digital para mensajes de servicio Web (como SOAP). Tal cifrado puede ser utilizado por un atacante para ocultar código malicioso que se ejecuta al momento de descifrar.

-Uso de criptografía de gran tamaño: La norma WS-Security no impone restricciones sobre qué partes de un encabezado de seguridad pueden ser cifradas, el mensaje SOAP puede ser cifrado o incluso el tamaño del mensaje. Esto significa que un atacante es capaz de causar una denegación de servicio mediante el envío de basura encriptada en el encabezado del mensaje del servicio web. Tales mensajes causan una alta carga en la CPU del servidor Web Hosting del servicio, al tratar de descifrar esos mensajes generando problemas de disponibilidad.

A nivel de capa de procesos empresariales

-Exploración de BPEL: Un proceso de negocio WS-BPEL (BPEL) en su manifiesto puede ser sometido a un "escaneo BPEL".

-Inundaciones de instanciación (directas e indirectas). Los motores BPEL instancian un nuevo proceso cuando reciben un mensaje de "recepción" entrante. Cuando se recibe un mensaje, el motor BPEL hace una pausa en su ejecución actual y continúa sólo después de que el mensaje entrante sea recibido completamente. Un atacante puede explotar los motores BPEL, al enviar repetidamente mensajes de recepción no válidos. Tales mensajes afectan gravemente al motor BPEL disminuyendo o incluso anulando su disponibilidad para mensajes. La inundación indirecta de los motores BPEL también es posible cuando el objetivo de ataque difiere, es decir, el atacante puede usar un proceso instanciado en un motor BPEL para causar una inundación a otro motor BPEL. Esto es posible si el atacante invoca un proceso desde el primer motor BPEL que interactúa con otro servicio Web o proceso de negocio en el segundo motor BPEL.

-Envenenamiento de esquemas: Se logra al modificar la información del esquema XML para atacar un sistema de destino. Un atacante puede interceptar un esquema XML antes de que llegue a un cliente (desde un servidor) y modificarlo. El envenenamiento de esquema puede causar un ataque DoS, ya que el analizador de XML puede colgar o llegar a un estado inconsistente y no tener información del esquema relevante para analizar el documento XML. Las modificaciones menores del esquema (como modificar tipos de datos) pueden enviar una respuesta inexacta al cliente.

Los servicios web en entornos bien implementados defienden la orquestación de servicio como un principio y una fortaleza, que bien aprovechada permite mejorar la interoperabilidad y el rendimiento de procesos de integración en las compañías, es por esto, que el estándar WS-Security se convierte en una alternativa de seguridad para las organizaciones.

Parte de la definición e implementación de la política, se basa en la forma de procesar los webs Services en múltiples subcapas por efecto de la granularidad de SOA, esto en términos técnicos significa que, mediante un analizador sintáctico con unas reglas definidas, permite validar la función de entrada, procesarla y llevarla a un esquema encriptado, teniendo en cuenta el escalamiento a la medida y que el compromiso de seguridad no debe verse afectado en ninguna de las fases. [5]

VII. MÉTODOS DE MITIGACIÓN DE RIESGOS SOBRE SERVICIOS WEB

El método describe un conjunto de normas y tecnologías de seguridad, destinadas a crear un enfoque unificador para seguridad en un mundo de servicios Web, es aquí donde parte

un punto de referencia para afrontar y mitigar los riesgos.

-El primer estándar por implementar dentro de la etapa tres del esquema de tratamiento de riesgos definido para servicios web es WS Security (construido en XML Signature, XML Encryption, SAML y otros estándares de seguridad), el cual será el pilar de otras normas. WS-Security describe las extensiones de SOAP para la mensajería segura. Es un mecanismo de propósito general para asociar tokens de seguridad con mensajes SOAP, creaciones de WS-Security En y es totalmente compatible con tecnologías de seguridad establecidas y maduras como SSL, IPSec13, XML Signature y XML Encryption. Está diseñado para garantizar la integridad, confidencialidad y autenticación de mensajes y la codificación de tokens de seguridad que viajan con los mensajes asegurados. [6]

-Mediante WS-Policy y ajustándonos al dominio COBIT debemos mostrar las capacidades y restricciones de la política de seguridad. WS-Policy permite a las organizaciones exponer los servicios web recolectando información y requisitos asociados con la privacidad o seguridad. Esto hace que WS-Policy sea el recipiente de información y análisis, dándole información a la arquitectura y detallando una especificación de alto nivel, proporcionando las bases necesarias para componer un lenguaje de política particular. Los complementos para generar las políticas requeridas son WS-Policy Assertions, que proporciona algunos aspectos a la política básica que se aplican a cualquier tipo de política, y la especificación WS-Policy Attachment, que proporciona orientación sobre cómo adjuntar una política a un recurso.

-Para mantener la relación de confianza mediante un perfil, existe WS-Trust, que describe el modelo básico de relacionamiento y se enfoca en los mecanismos de mensajería seguros de WS-Security, definiendo primitivas y extensiones adicionales para la emisión, intercambio y validación de operaciones de seguridad. WS-Trust también permite emisión y difusión de credenciales dentro de diferentes dominios de confianza. Para asegurar una comunicación entre dos partes, deben intercambiar credenciales de seguridad (directa o indirectamente). Sin embargo, cada parte debe determinar si puede "confiar" en las credenciales de la otra parte. Esta especificación define las extensiones de WS-Security para emisión e intercambio de características de seguridad y formas de establecer y acceder a relaciones de confianza. Utilizando estas extensiones, las aplicaciones pueden comprometerse en una comunicación segura diseñada para trabajar con la arquitectura general de servicios Web. [7]

-WS-Privacy: Esta especificación permitirá a los usuarios indicar las preferencias de privacidad y los servicios para establecer e implementar prácticas de privacidad.

-WS-Secure Conversation: Describe cómo administrar y autenticar mensajes entre las partes, incluido el intercambio de contextos de seguridad y el establecimiento de seguridad del protocolo de Internet. Proporciona seguridad de extremo a extremo en la capa de Internet del conjunto de TCP / IPS que deriva en claves de sesión.

-WS-Authorization: Esta especificación define los datos de autorización de servicios web y las políticas.

-WS-Auditing - Aún no existe un estándar para auditoría de servicios Web. Después de invocar un servicio, no hay forma de determinar quién ha utilizado el servicio y de dónde se originó la petición. Como resultado, no existe una pista de auditoría que pueda utilizarse más tarde para investigar posibles infracciones en la seguridad. No hay manera de determinar quién ha hecho qué y en qué hora. [8]

-El escaneado WSDL puede ser mitigado utilizando mecanismos de control de acceso como el empleo de un firewall XML sobre las operaciones internas o mediante el despliegue de operaciones internas en los servicios web.

-Para mitigar los ataques a los metadatos, los consumidores de servicios deben verificar cuidadosamente la autenticidad de los metadatos del servicio Web. Sin embargo, hay que tener en cuenta que no existen mecanismos estándares para verificar la autenticidad de los metadatos.

-Para mitigar los ataques de ofuscación, el contenido del esquema cifrado debe ser validado por la seguridad, después del descifrado, y no antes de descifrarlo.

-Los ataques de criptografía de gran tamaño se pueden mitigar al tener el servicio consumidor, alineado con la política de seguridad del servicio web.

-Los ataques de envenenamiento de esquemas pueden ser frustrados con protección de esquemas XML contra modificaciones no autorizadas. Muchas de las amenazas descritas se pueden mitigar haciendo uso de autenticación, confidencialidad, integridad y normas de autorización, como: (SAML), WS-Security y control de acceso eXtensible Markup Language (XACML), y comercial de la plataforma (COTS) soluciones como IBM Tivoli Identity Manager (TIM), IBM Tivoli Access Manager (TAM) y SOA de CA Security Manager para la autenticación y para la autorización.

VIII. CONCLUSIONES

La sencillez de estos dos modelos hace que el tratamiento y gestión de riesgos sea aplicable a cualquier proceso no sólo de servicios web y tecnología, sino de toda una arquitectura SOA, aprovechando las bondades y capacidades del framework de trabajo COBIT 5.0

Los beneficios son relevantes en tema de costos para las organizaciones, el ahorro es un factor fundamental y es algo que proporciona la arquitectura SOA, si desde el principio de la definición se estiman la mayoría de entradas y el tratamiento de los riesgos.

Los sistemas informáticos y los sistemas distribuidos, en particular, enfrentan varios riesgos de seguridad. Son vulnerables a ataques tanto activos como pasivos. Un sistema distribuido se compone de varias capas, incluyendo una red totalmente funcional, con nodos en esa red que se ejecutan en una pieza de hardware.

SOA es un tipo de sistema distribuido middleware y, por tanto, es vulnerable a los riesgos de seguridad que afectan a cada una de las capas en las que se compone, los WS-Security mencionados como confidencialidad, integridad, autenticación, control / autorización de acceso, no repudio y auditoría se utilizan para mitigar dichos riesgos de seguridad, a más bajo costo, en la aplicación del dominio de gestión de riesgo COBIT 5.0.

REFERENCIAS

[1] A. Buecker, P. Ashley, M. Borrett, M. L. Sridhar Muppidi Neil Readshaw Understanding SOA Security, pp 305-330, 2007.

[2] COBIT 5 for Assurance ISACA, Estados Unidos, 2013.

[3] C. M. Carmona. R., Modelo de Gobernabilidad basado en COBIT para la Gestión por Procesos Definida en un Espacio Multidimensional, Medellín, Colombia, pp 120-174, 2013.

[4] A. Ortiz. (2014, marzo). Metodología de evaluación de Riesgos Informáticos. [Online]. Disponible en: http://riesgosycontrolsegblog.blogspot.com.co/p/cramm.html.

[5] M. Jensen, et al., SOA and Web Services: New Technologies, New Standards - New Attacks. In: Fifth European Conference on Web Services (ECOWS), Halle (Saale), Germany, 2007.

[6] D. Sosnoski. (2009, Junio 16) Axis2 WS-Security signing and encryption. [Online]. Disponible en: https://www.ibm.com/developerworks/ssa/webservices/library/j-jws7/index.html.

[7] D. Sosnoski. (2011, agosto 5). Utilización Granular de WS-Security. [Online]. Disponible en: https://www.ibm.com/developerworks/java/library/j-jws5/index.html.

[8] S. Indrakanti, Service Oriented Architecture Security Risks and their Mitigation, Command, Control, Communications and Intelligence Division Defence Science and Technology Organisation, Commonwealth of Australia, 2012

[9] Cobit 5 ISACA Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa, Estados Unidos, 2012.

[10] M. J. Morales. Los 10 errores más frecuentes implantando una estrategia soa. [Online]. Disponible en: https://www.modusoperantic.com/es/los-10-errores-mas-frecuentes-implantando-una-estrategia-soa/

[11] A. Hevia. (2010, diciembre 12). Los riesgos en la implantación de SOA. [Online]. Disponible en: https://andreshevia.com/2010/12/12/los-riesgos-en-la-implantacion-de-soa/

Luis Fernando Gaitan Pinto Nació en Bogotá, Colombia en 1986. Se graduó en el año 2014 como Ingeniero de Sistemas de la Universidad Distrital Francisco José de Caldas. Actualmente se encuentra realizando la Especialización en Seguridad Informática en la Universidad Piloto de Colombia.