Integration proposal of enterprise architecture and security architecture

Andrés Felipe Díaz Palacios, Claudia Patricia Santiago Cely
Escuela Colombiana de Ingeniería Julio Garavito, Colombia, andres.diaz-p@mail.escuelaing,edu.co,
Claudia.santiago@mail.escuelaing.edu.co

Abstract*— This article presents a proposal of integrating enterprise architecture with a security architecture to provide a tool to the small- and medium-sized companies (SMEs) for optimally using their information technologies and mitigating the risk of their assets that increase the security of the information because the trends in the investments made by these companies are of technological nature. However, sometimes, these companies do consider the importance of security. Computer attacks are highly frequent on SMEs, the preferred victims. Consequently, these attacks enable unauthorized access to the private information of these companies and loss or unauthorized modification of data. In most critical cases, these attacks lead to denial of the IT services of SMEs. These attacks are also alarming the shortness of the shelf life of the investments so that the companies incur costs higher than those fixed in the budgets. This is due to the fact that SMEs do not have an enterprise architecture model within their organizational structure, which helps them to make technological investments that are aligned with the business strategy and consequently reduce the risk of future investments.

***Keywords*– Enterprise architecture, security architecture, small- and medium-sized companies, information security.**

Digital Object Identifier (DOI):
http://dx.doi.org/10.18687/LACCEI2017.1.1.171
ISBN: 978-0-9993443-0-9
ISSN: 2414-6390

Propuesta de integración de arquitectura empresarial y arquitectura de seguridad

Andrés Felipe Díaz Palacios, Claudia Patricia Santiago Cely
Escuela Colombiana de Ingeniería Julio Garavito, Colombia, andres.diaz-p@mail.escuelaing,edu.co,
Claudia.santiago@mail.escuelaing.edu.co

RESUMEN

El presente documento presenta una propuesta de arquitectura empresarial integrada con una arquitectura de seguridad con el objetivo de dar una herramienta a las PYMES (pequeñas y medianas empresas) de manera que puedan tener un mejor aprovechamiento de sus tecnologías de la información y a su vez puedan mitigar el riesgo de sus activos incrementado la seguridad de la información puesto que la tendencia en sus inversiones son de índole tecnológico pero en ocasiones no tienen en cuenta la importancia de la seguridad. Cada vez son más frecuentes los ataques informáticos en los que las víctimas preferidas son las PYMES, los cuales tienen como consecuencia acceso no autorizado a su información privada, pérdida o modificación no autorizada de datos y en los casos más críticos denegación de sus servicios en TI. También es alarmante lo corto de la vida útil de las inversiones realizadas, tanto así que incurren en costos superiores a los presupuestados, esto se debe a que no tiene dentro de su estructura organizacional un modelo de arquitectura empresarial que les ayude realizar inversiones tecnológicas alineadas con la estrategia del negocio y a su vez disminuir el riesgo de futuras inversiones.

Palabras Clave: Arquitectura empresarial, Arquitectura de Seguridad, PYMES, seguridad de la información.

I. INTRODUCCIÓN

En el mundo globalizado en el que vivimos, existe un recurso cuyo valor muchas veces no es tenido en cuenta como debería ser por las personas y empresas que lo poseen, este recurso es la información.

En el caso de las personas muchas de ellas no son conscientes del volumen de información que llegan a manejar. De igual manera las empresas, que claramente manejan un volumen de información muy superior la cual recibe un grado de clasificación de tipo confidencial, sensible o pública y es en este punto donde comienza la problemática de la seguridad de la información.

En general las empresas buscan tener una ventaja competitiva frente a su competencia, constantemente se están comparando con las empresas de su entorno con el fin hacer sus proyecciones y buscar elementos que agreguen valor a su modelo de negocio. una forma en que generalmente lo hacen es mediante la incorporación de herramientas que necesariamente implican una inversión tecnológica. El problema radica en que la decisión de realizar estas inversiones no tiene un análisis de fondo que indique que soluciones hay en el mercado, casos de éxito de implementación, costos, tiempos de implementación, entre otros, y muchas veces las soluciones a sus problemas se quedan cortos en su horizonte de planeamiento.

¿Cómo realizar inversiones tecnológicas que soporten la operación de un negocio en un horizonte de tiempo razonable?

¿Cómo se pueden prevenir ataques informáticos si las empresas no son conscientes de los activos de información que poseen?

La respuesta a estas preguntas será caso de estudio en el desarrollo de este artículo que evidencia los retos que tienen que afrontar los expertos en el tema. Para lo cual se revisará la problemática actual en cuanto a TI y seguridad de la información, se presentará el marco de referencia y luego se procederá a presentar la propuesta de integración entre ambas arquitecturas

II. PROBLEMÁTICA

La tecnología es una herramienta que usan las empresas para apalancarse y mejorar sus procesos de negocio todo con el fin de aumentar sus márgenes de utilidad. En numerosos casos no se tiene en cuenta el riesgo al que están expuestos los activos de información de las PYMES, por esto es importante tener en cuenta la seguridad de la información con el fin de que se tomen las medidas adecuadas y se mitigue el riesgo al que está expuesta la misma, cuando se pretende implementar un proyecto de TI.

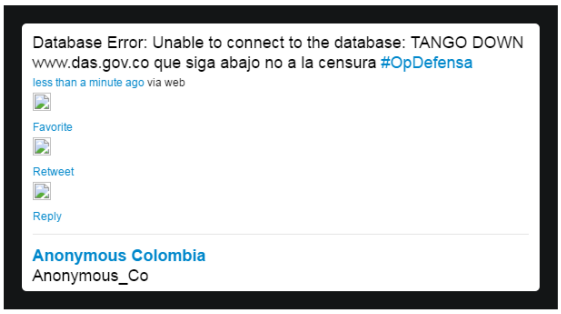
Cuando se habla de seguridad informática, existen dos tipos de incidentes (ataques) que se pueden presentar, están los incidentes públicos y los privados, estos incidentes pueden generar problemas relacionados con fraudes,

Digital Object Identifier (DOI): http://dx.doi.org/10.18687/LACCEI2017.1.1.171
ISBN: 978-0-9993443-0-9
ISSN: 2414-6390

sabotajes, pérdida, robo y modificación de información, ataques de denegación de servicio y Phishing (suplantación de información)

El Estado colombiano ha presentado un número de ataques informáticos públicos que ponen en alarma el estado de la seguridad de la información de la nación, varios de ellos realizados por el grupo de piratas informáticos denominado Anonymous en el año 2011 y 2012. El blanco de estos ataques fueron varios servidores de páginas web del Estado como lo son la página de la Policía nacional, la cual duro inhabilitada alrededor de 18 horas, de igual manera la página del Departamento Administrativo de Seguridad (DAS) fue derribada por motivo de una campaña de no a la censura.

Al digitar la dirección de la página salía el siguiente mensaje:



El mismo grupo hacktivista realizó dos ataques catalogados como privados, las víctimas fueron el presidente de la republica Juan Manuel Santos el cual tuvo un ataque en su perfil de Facebook y de igual manera el ex presidente Álvaro Uribe, este último en su cuenta de Twitter.

Pese a que los ataques mencionados anteriormente fueron realizados a páginas y funcionarios de un Estado, un informe realizado por Digiware en el año 2014 [1], primer integrador de seguridad informática de Latinoamérica, tuvo como resultado que Colombia fue el país que generó más ataques informáticos entre países de habla hispana, seguido de Argentina, Perú, México y Chile, estos ataques fueron realizados por personas del común, grupos criminales y en algunos casos entidades reconocidas como la Dijin.

Continuando con los resultados del informe de Digiware, se tiene que en Latinoamérica los ataques más frecuentes son los de denegación de servicio abarcando el 88,39% del total de ataques, seguido de los ataques exploit (comportamiento no deseado) con un 7,67% y finalmente los ataques que incurren en fuga de información con un 3,59%.

A nivel mundial Estados Unidos es el país con mayor generación de ataques en el mundo, los siguientes en la lista son China, Francia y Holanda.

El número de ataques y vulnerabilidades que presentan los sistemas de información y demás recursos de almacenamiento de la misma está implícito con el crecimiento de la población que usa internet, se percibe un crecimiento exponencial de la red más grande del mundo y esto genera nuevos retos para los expertos en seguridad de la información. Si bien es cierto que las empresas que lideran el mundo poseen los recursos para proteger sus activos, también presentan vulnerabilidades que son explotadas para la generación de ataques como el que recibió Apple en 2015, en el que también se vio perjudicado Amazon. El ataque fue realizado a la cuenta de iCloud de un ciudadano estadounidense que tuvo que sufrir la pérdida de la información contenida en su Macbook, Ipad y Iphone, y la denegación del acceso a sus cuentas de redes sociales. Ésta es una muestra de que los servicios que prestan compañías grandes también presentan vulnerabilidades. [1].

Los blancos típicos de estos ataques son los Gobiernos, el sector bancario y empresas con diferente razón social, vale la pena resaltar que, aunque generalmente los ataques informáticos empresariales más relevantes son hacia empresas y corporación de gran tamaño, puesto que manejan un volumen de información bastante alto, un tercio de los ataques son dirigidos a PYMES , es decir que cuentan con 250 o menos empleados.

La problemática que afrontan las PYMES se basa en el desconocimiento de los riesgos que poseen sus activos de información además que no cuentan con los recursos económicos suficientes para mitigar el riesgo al que están expuestas antes los piratas informáticos y peor aún piensan que al ser una empresa catalogada como PYME no son un blanco atractivo frente ataques de índole informático.

III. MARCO TEÓRICO

Si bien los hechos mencionados anteriormente fueron realizados a personas con un rol de poder con unos parámetros de seguridad de la información muy superiores al promedio de la población fueron insuficientes, es momento de señalar que no existe ningún sistema o activo de información que se pueda proteger al 100% pero si se puede disminuir el nivel de riesgo al que están expuestos constantemente mediante el uso e implementación de métodos y/o herramientas de seguridad.

Por tal motivo es importante que las empresas trabajen en la identificación y el fortalecimiento de la seguridad de la información sin dejar a un lado el objetivo primario que básicamente consiste en aumentar la productividad del negocio. Se considera que integrar marcos de trabajo de arquitectura de seguridad y arquitectura empresarial cumple los lineamientos anteriormente mencionados.

A continuación, encontramos los marcos de trabajos más relevantes en la actualidad.

a) ARQUITECTURA EMPRESARIAL

La arquitectura empresarial es una metodología que nos permite hacer una análisis de cómo se encuentra una empresa u organización actualmente con el fin de alinear procesos de negocio, datos, aplicaciones e infraestructura tecnológica de manera que apunten a los objetivos estratégicos del negocio y a la razón de ser de las empresas [2], para proponer una arquitectura objetivo de manera que el negocio obtenga un alineamiento de su estrategia y TI, permitiéndole incrementar su agilidad mediante el establecimiento de iniciativas que aporten a la visión futura de la empresa en general, para poder tomar decisiones acerca de posibles inversiones tecnológicas que satisfagan los objetivos estratégicos planteados por la empresa.

Los frameworks de trabajo más relevantes del mercado son los siguientes:

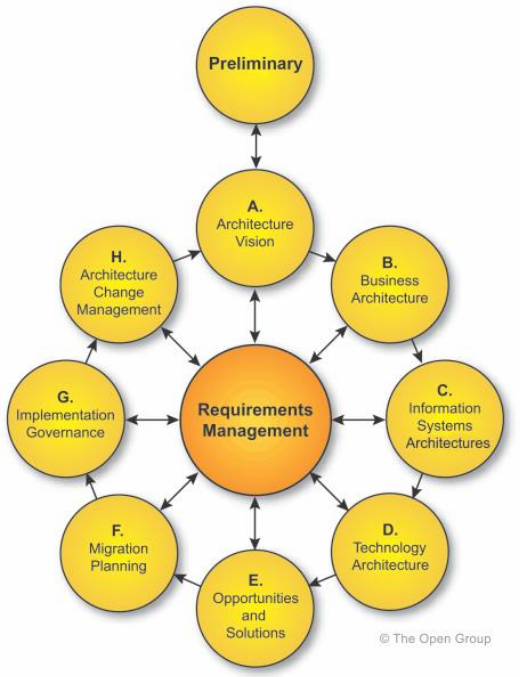
TOGAF:

Es una de las metodologías más populares existentes en el mercado para llevar a cabo el desarrollo de una arquitectura empresarial, ellos se definen de la siguiente manera:

"TOGAF es una herramienta para asistir en la aceptación, creación, uso, y mantenimiento de arquitecturas. Está basado en un modelo iterativo de procesos apoyado por las mejores prácticas y un conjunto reutilizable de activos arquitectónicos existentes" [4]

Desde su creación togaf ha tenido 10 versiones, y la versión actual es TOGAF V.9.1 Corrección de errores.

La siguiente imagen ilustra la estructura de una arquitectura empresarial.



[3] **Arquitectura Empresarial TOGAFF**

ZACHMAN

Creado en 1984 por John Zachman y publicado en 1987 en el IBM Systems Journal.

La metodología propuesta está resumida en una matriz de filas por columnas, compuesta en su primera fila con las preguntas ¿Qué?, ¿Cómo?, ¿Cuándo?, ¿Quién?, ¿Dónde? y ¿Por qué? Que tiene como finalidad describir las ideas más complejas respecto a la visión de la organización, representando sus procesos, datos, servicios, aplicaciones y los recursos de TI de una empresa.

Perspectivas de la primera fila:

La formulación de las preguntas conlleva al levantamiento de información de la empresa, tales como sus procesos de negocio, aplicaciones o módulos de aplicación existentes, numero de sedes con las que cuenta la empresa, descripción de los roles y objetivos estratégicos de la empresa.

Perspectiva de la primera columna:

Relaciona las preguntas de la primera fila con el fin de especificar los procesos de negocio de la organización, los sistemas necesarios para soportarlos, su especificación en detalle de la funcionalidad y sus limitaciones, y el funcionamiento de la empresa en general. [5]

b) ARQUITECTURA DE SEGURIDAD

Es una herramienta utilizada para describir el estado actual de una organización o empresa basada en los activos de información que posee, sistemas de información y personas que pertenecen a la empresa. Con el análisis realizado a la situación actual de seguridad, se pretende diseñar y documentar una arquitectura de seguridad objetiva, de manera que se minimicen los riesgos y vulnerabilidades que presentan actualmente sus activos mediante la implementación de herramientas de seguridad que protejan la información.

La arquitectura de seguridad tiene como objetivo minimizar el riesgo al que está expuesta la información y las personas, para esto, se debe realizar un análisis de riesgo que básicamente consiste en identificar los activos de información y recursos más relevantes para la empresa, con el fin de detectar todo tipo de amenazas a los que están expuestos. Estas amenazas pueden ser desde la intercepción de un recurso o hasta la interrupción del mismo, generando una denegación del servicio a los usuarios.

Los frameworks y estándares de trabajo más relevantes en la actualidad son los siguientes:

TOGAF

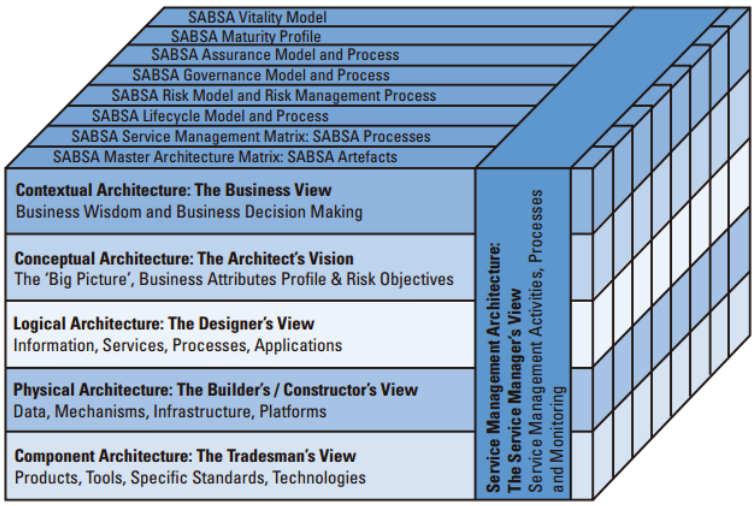
Para TOGAF la arquitectura de seguridad tiene un enfoque que se basa en la implementación de políticas de seguridad que una empresa u organización debe tener para proteger el recurso de la información. La estructura de su arquitectura está compuesta en ocho (8) fases, también llamadas arquitecturas, alienadas de principio a fin. [6]

Tienen como propósito proteger el valor de los sistemas de información y los bienes de la empresa, de manera que cumplan con los siguientes criterios de aceptación de autenticación, autorización, auditoria, aseguramiento, disponibilidad, protección de activos, administración y gestión del riesgo.

SABSA

Es un modelo y una metodología para desarrollar el manejo de riesgo en una arquitectura de seguridad empresarial, tiene como objetivo la entrega de soluciones de infraestructura de seguridad que soporten las iniciativas críticas para el negocio. La característica principal del modelo de SABSA consiste en que todo se deriva de un análisis de los requerimientos para seguridad del negocio, esencialmente en los que permite nuevas oportunidades de negocio que pueden ser desarrolladas y explotadas. [7]

El modelo SABSA esta comprendido por seis capas, negocio (business), arquitecto (The architect), diseñador (the designer), constructor (the builder), comerciante (the tradesman), gerente de instalaciones (the facilities manager), que tratan aspectos contextuales, conceptuales, lógicos, físicos, componentes y operacionales de la arquitectura de seguridad respetivamente, su estructura es muy similar a la propuesta por John A. Zachman en el modelo de arquitectura empresarial, pero ha sido adaptado buscando un enfoque en el tema de seguridad.



[8] **Arquitectura de Seguridad TOGAFF**

OSA Arquitectura de seguridad TI

OSA (Open Security Architecture) tiene una definición de arquitectura de seguridad compuesta por dos componentes fundamentales, Seguridad TI y Arquitectura TI (Diseño de artefactos que describen los compontes de la organización, sus interrelaciones, principios y directrices que gobiernan su diseño y evolución) [9].

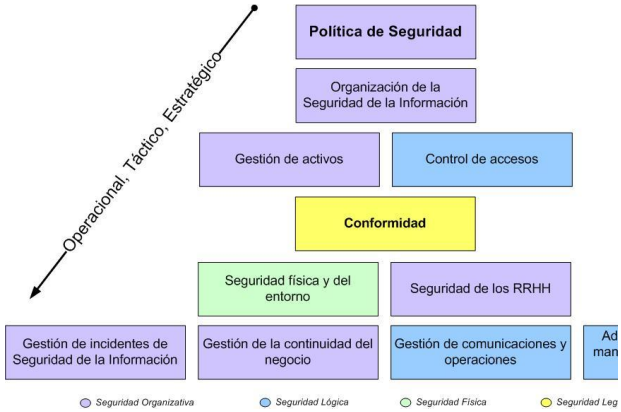
En esencia consiste en el diseño de herramientas o artefactos que describen cómo los controles de seguridad están posicionados y cómo se relacionan en general con la arquitectura TI, los controles tienen como propósito mantener los atributos de calidad del sistema tales como confidencialidad, integridad, disponibilidad, responsabilidad y seguridad. [10]

ISO 27000

La serie ISO (International Organization for Standarization) 27000 es un conjunto de estándares y normas que contiene las mejores prácticas en el tema de seguridad de la información, la norma permite desarrollar, implementar y mantener especificaciones para los sistemas de gestión de seguridad informática. [11]

Tiene la posibilidad de integrarse con otros sistemas de gestión como el ISO 9001, ISO 14001 entre otros, tiene una reducción de costos y mejora en los procesos de servicio y por último el aumento de la seguridad en base a la gestión de procesos en lugar de la compra sistemática de productos y tecnologías. [12]

ISO 27000 está centrado en el apoyo desde 14 dominios de riesgo presentados a continuación.



[13] **Estructura ISO 2700**

IV. PROPUESTA DE INTEGRACIÓN DE ARQUITECTURA EMPRESARIAL Y ARQUITECTURA DE SEGURIDAD

Luego de investigar acerca de los marcos de trabajo más relevantes en el ámbito empresarial y de seguridad de ambas arquitecturas, se decidió la selección de la metodología de TOGAF en arquitectura empresarial puesto que permite un alineamiento holístico por fases de las cuales se tiene un dominio del tema en cuanto a sus plantillas y demás recursos ofrecidos por el framework. Adicionalmente, se integraron estándares internacionales de seguridad como la norma ISO 27000 la cual incluye herramientas que permiten medir el estado de la seguridad de la información en las organizaciones que serán expuestos en la explicación de cada capa de la arquitectura.

La propuesta busca el alineamiento holístico entre los procesos de negocios y los recursos TI de las organizaciones, diseñando una estrategia de implementación basada en el estado actual de los procesos de negocio, los tipos de información que maneja, las aplicaciones involucradas en los procesos y los diferentes componentes tecnológicos que posee para poder plantear una arquitectura objetivo según los requerimientos suministrados por los stakeholders de la compañía, el problema radica en que en esta arquitectura no se maneja el concepto de gestión de riesgo, el cual es sumamente importante puesto que el principal recurso de las empresas es la información que manejan.

A continuación, para cada etapa definida por togaf se presentan las recomendaciones para formular la arquitectura empresarial de una empresa y luego las recomendaciones para implementar la arquitectura de seguridad a dicha fase.

- ✓ **Capa 1: Fase preliminar:**

Describe la lógica del negocio la cual incluye la misión y visión del mismo, también indica en qué sector de la economía se desempeña, lo anterior con el fin de identificar y describir sus actividades con base en la infraestructura de la compañía, los recursos humanos que posee, los componentes tecnológicos que soportan su operación, como la lleva acabo describiendo la logística interna y externa y por último cómo es el servicio al cliente.

Como complemento en seguridad se debe pensar en definir el concepto de plan de continuidad de negocio (Business Continuity Plan) el cual tiene parte de desarrollo en esta capa puesto que va ligada al análisis del entorno organizacional, identificando el tipo de empresa, y su estado deseado en un futuro, de con el fin de definir en la fase siguiente escenarios de falla y acciones correctivas que mitiguen la para en la operación de la empresa.

- ✓ **Capa 2: Visión de la Arquitectura**

Describen los objetivos estratégicos del negocio, generalmente son suministrados por las compañías puesto que son los que tiene clara la estrategia definida, aunque como la propuesta definida es enfocada a PYMES puede suceder que no tengan definidos sus objetivos, en este punto se debe iniciar con la alineación del negocio con TI para finalmente hacer las proyecciones de la estrategia. Posteriormente se hace un análisis interno y externo de las debilidades, fortalezas, amenazas y oportunidades que tiene el negocio que complementa definición de la estrategia planteada anteriormente, se definen principios de negocios suministrados por el framework que se acoplen al tipo de empresa y negocio, estos principios están enfocados al negocio, los datos, las aplicaciones y la tecnología.

En el tema de seguridad se definen los requisitos del sistema de gestión de la seguridad de la información, el cual busca proteger la información ante amenazas con el fin de minimizar daños, aumentar las oportunidades del negocio, mejorar el retorno a la inversión, garantizar la continuidad del negocio y finalmente crear una cultura de ética en la organización.

Se debe definir el alcance acompañado del objetivo de la seguridad de la información según el procesamiento de la misma para garantizar que existe un nivel de protección apropiado, posteriormente deben definirse un número considerable de políticas de seguridad de la información aplicables a la empresa que van ligadas a la aplicación de leyes, normas y regulaciones que pueden variar según la legislación del país donde la organización realiza su operación.

La implantación de la norma ISO 27001 conlleva a las organizaciones a realizar un análisis de riesgos para los activos de información que posee, para lo cual se debe hacer un listado de los activos definiendo, el propietario, el tipo, estos pueden ser de información o hardware, y por último su ubicación puesto que el activo puede prestar un servicio a través de un dispositivo en línea.

En el manual se encuentra una matriz con la estructura para realizar el análisis de riesgos con base en los criterios de disponibilidad, integridad y confidencialidad que generan las siguientes preguntas:

Disponibilidad

- Impacto si el activo esta indisponible 1 hora
- Impacto si el activo esta indisponible 1/2 día
- Impacto si el activo esta indisponible 1 día
- Impacto si el activo esta indisponible 1 semana

Integridad:

- El Activo es modificado parcialmente
- El Activo es modificado en su gran mayoría
- El Activo es modificado totalmente
- El Activo es eliminado

Confidencialidad

- El Activo es visto por un grupo pequeño no autorizado
- El Activo es visto por todos los funcionarios del área
- El Activo es visto por todos los funcionarios de la institución
- El Activo es visto por todo el mundo

Cada uno de los ítems puede ser puntuado de la siguiente manera:

5. Crítico: Genera pérdidas de alto costo, como sanciones, multas o demandas que impidan la ejecución normal de las tareas. Se impacta la imagen y se pierde la confianza con los usuarios de la entidad.

4. Alto: Podría generar pérdidas de alto costo, como sanciones, multas o demandas que impidan la ejecución normal de las tareas a corto plazo. Podría causar un impacto negativo en la imagen y confianza en los usuarios de la entidad.

3. Medio: Podría generar pérdidas de costo moderado, como sanciones, multas o demandas que impidan la ejecución normal de las tareas a mediano plazo. Podría impactar la imagen de la entidad negativamente, en áreas, servicios o sectores de usuarios.

2. Bajo: Podría generar pérdidas de costo bajo, como sanciones, multas o demandas que no afecte considerablemente la ejecución normal de las tareas. Podría generar un impacto poco considerable en áreas, servicios o sectores de usuarios de la SIC.

1. Insignificante: No genera costos significativos para la ejecución de las tareas. No afecta la imagen de la entidad.

Al final se pondera las puntuaciones por cada criterio.

- ✓ **Capa 3: Arquitectura de Negocio**

Describe y modela el estado actual de los procesos de negocio con el fin de desarrollar la arquitectura de Negocio actual y objetivo, en esta fase se analizan las capacidades que tiene el negocio, sus procesos y las personas involucradas en ellos. La comparación de la arquitectura objetivo (TO BE) con el estado actual (AS IS) permite la identificación de brechas y programas derivados que son producto de a dónde se quiere llegar.

Los programas derivados deben apuntar a los objetivos estratégicos definidos en la fase anterior (visión de la arquitectura) para lograr el alineamiento estratégico deseado.

En materia de seguridad se lleva a cabo la continuación de la fase 1 de plan de continuidad de negocios (BCP) relacionando los objetivos estratégicos de la primera parte con los procesos de negocio de la compañía, esto con el fin de catalogar los procesos y encontrar relación entre los mismos que apunten al cumplimiento de la estrategia de negocio, también se pueden identificar procesos críticos que en caso de que tengan una para afectan la operación de la compañía e incluso generar pérdidas económicas y permite en fases futuras definir acciones preventivas en caso de que esto ocurra.

- ✓ **Capa 4: Arquitectura de Datos**

En esta fase se definen los tipos y fuentes de información para dar soporte a los sistemas de información de la organización, no se busca llegar al nivel físico o lógico de los sistemas de almacenamiento de la empresa sino definir las entidades de información, sus atributos y las relaciones entre ellos para garantizar el correcto funcionamiento del sistema, que sea comprensible, completo consistente y estable, para esto hace uso del modelo entidad relación.

Se identifican las entidades de información que hacen parte de los procesos de negocio de la arquitectura de negocio para tener un alineamiento estratégico entre estas dos fases y como insumo para las futuras.

Como complemento del análisis de riesgo realizado en la fase preliminar, se procede a desarrollar la evaluación para ese análisis de riesgo, el cual tiene como propósito listar los principales activos de información que tengan un gran impacto en el negocio para analizar las vulnerabilidades y amenazas a los que están expuestos y así determinar el nivel de riesgo.

En el manual se incluye una matriz que permite realizar la evaluación. A continuación, presentamos algunos de los formatos que contiene la matriz:

No.	Proceso
1..N	Nombre proceso 1..N

Proceso	Activo	Propietario	Ubicación
1, 2, o N	Nombre activo 1...N	Nombre del propietario 1,,,N	Lugar

[14]

El propósito de la evaluación es identificar todas las posibles amenazas a las que están expuestos los activos de información, posteriormente determinar los eventos de las posibles amenazas incluyendo el actor que podría realizarla con el fin de determinar riesgo mediante una valoración regida por los siguientes puntajes:

VALORACION DEL RIESGO	
NIVEL DE RIESGO INHERENTE	CALIFICACION
EXTREMO	41 A 75
ALTO	21 A 40
MODERADO	11 A 20
BAJO	1 A 10

[15]

Con la información resultante de diligenciar la tabla se recomienda hacer gráficos de barras y pasteles que permiten la identificación de los riesgos de los activos de información más críticos dentro de la compañía y de esta manera se puede priorizar el tratamiento de las vulnerabilidades y amenazas encontradas en el proceso.

Capa 5: Arquitectura de aplicaciones

Reúne todas las aplicaciones del negocio con su respectiva funcionalidad y su evolución. Se definen y/o describen los requerimientos de las aplicaciones del negocio con el fin de soportar los procesos de negocio tratados en la arquitectura anterior, en este punto se ve reflejado el alineamiento estratégico requerido a través de las tres fases mencionadas hasta el momento.

En resumen, se espera que la arquitectura tenga las siguientes características:

- Aplicaciones para soportar los procesos de negocio
- Integración entre aplicaciones
- Integración de las aplicaciones
- Base de datos que almacenen la información

Para documentar la arquitectura de aplicaciones, inicialmente se debe tener un inventario de las mismas. Posteriormente se debe documentar la manera en que la aplicación almacena la información, que puede ser de manera física o a través de un software y finalmente se debe documentar de qué manera las aplicaciones soportan los procesos de negocio definidos anteriormente.

En relación con la seguridad se definen roles de usuario para otorgar permisos en las aplicaciones con base en el estándar triple A (Autenticación, Autorización y Registro), adicionalmente se identifican los proveedores y consumidores de información para determinar la veracidad y la calidad de los datos, por último, se continua con la fase 1 de plan de continuidad de negocios que tiene como parte final identificar las siguientes relaciones:

- Relación de los procesos de negocio con los sistemas de información

Se pretende identificar la dependencia de los procesos de negocio en los sistemas de información y que tan grave puede ser esto para el negocio, por ejemplo, si un sistema de información presenta fallas está implícita la para en el proceso de la empresa lo cual puede ocasionar perdidas económicas si no se tiene un plan de acción para los diferentes escenarios de falla del sistema.

- Relación sistemas de información, tecnología y actores involucrados

La seguridad de la información depende en gran medida de quienes hace uso de ella, por esta razón es de suma importancia identificar la relación que tienen los sistemas de con los usuarios finales, para definir buenas prácticas enfocadas al correcto uso de las aplicaciones, con el fin de disminuir el número de vulnerabilidades presentes en los sistemas de información y de más herramientas tecnológicas de las organizaciones.

✓ **Capa 6: Arquitectura de Tecnología**

Se reúnen todos los componentes tecnológicos, software y hardware de infraestructura, sus relaciones e interfaces y su evolución. Tiene como objetivo definir y describir la estructura de hardware, software y redes necesarios para soportar la implementación de las aplicaciones que soportan los procesos de negocio de la empresa, se deben tener en cuentas los entornos y la distribución geográfica (cantidad de sedes de la empresa).

En la parte de seguridad se lleva a cabo la fase de análisis el entorno tecnológico del plan de continuidad de negocio, la cual contiene una matriz que relaciona los activos tecnológicos de la organización e incluye una descripción del ambiente en el que están presentes, su localización, los componentes de aplicación que hacen uso del recurso tecnológico y las características tecnológicas que tiene por ejemplo la capacidad de memoria, base de datos que usa, etc.

Posteriormente se definen escenarios de falla, esto permite identificar las vulnerabilidades de los activos de la compañía, con las posibles de fallas se pueden definir acciones correctivas para garantizar la continuidad de

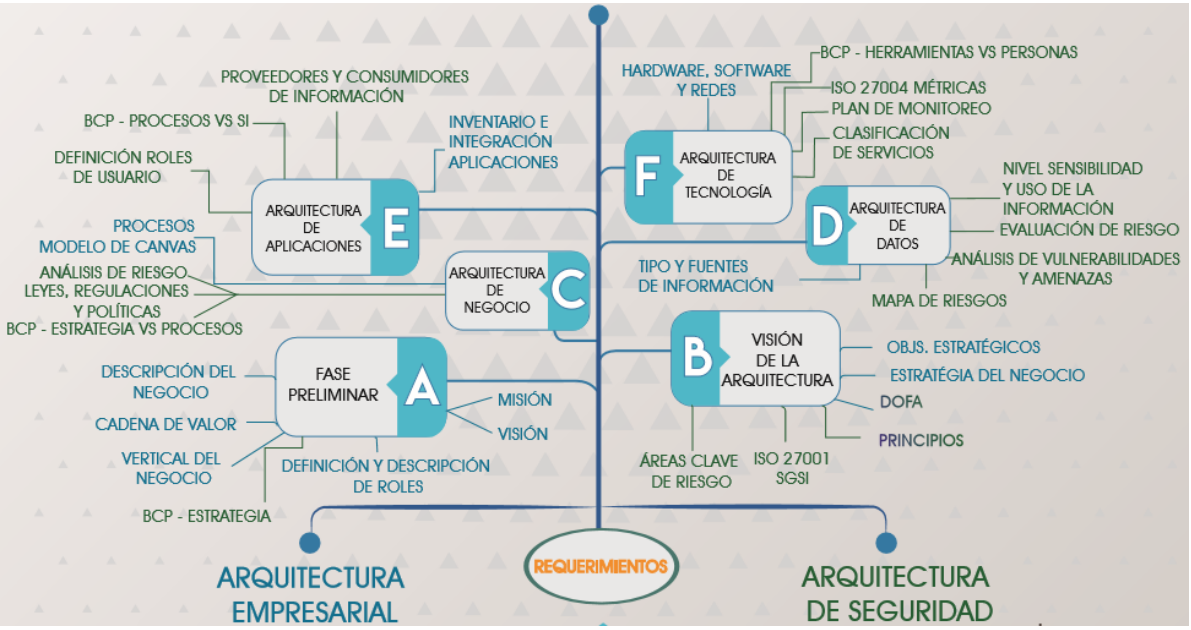
negocio. El siguiente formato para diligenciar esta información.

Código	Activo	Escenario	Descripción

[16]

El siguiente árbol ilustra gráficamente todos los componentes de la propuesta con los componentes empresariales y de seguridad integrados.

Componentes de la propuesta de integración de arquitectura empresarial y arquitectura de seguridad



IV. METODOLOGIA

Luego de la construcción del manual se seleccionó una empresa que sirvió como caso de estudio para la construcción de la arquitectura actual y la arquitectura objetivo, basada en el manual de usuario, el cual fue retroalimentado luego de llevar la teoría a la práctica. Se encontró que con la definición de la arquitectura la empresa obtuvo los siguientes beneficios:

- Alineamiento estratégico del negocio con TI (tecnologías de la información).
- Modelo de inversión predecible disminuyendo la probabilidad de futuras inversiones.
- Optimización de los procesos de negocio gracias al uso de herramientas tecnologías y soluciones de software.
- Identificación de vulnerabilidades y amenazas de los activos de información de la organización.
- Definición de controles de seguridad basados en los posibles eventos de amenazas identificados.
- Gestión del cambio organizacional.
- Definición de escenarios de falla.
- Definición de acciones correctivas.

Nombre de la empresa: Metadata Ingeniería Colombiana S.A.S

V. CONCLUSIONES Y TRABAJO FUTURO

En la actualidad las empresas buscan obtener una ventaja competitiva frente a sus competidores, esta ventaja se puede presentar con la adquisición de nuevas herramientas

tecnológicas, soluciones de software y demás tecnologías de la información, sin embargo la gran mayoría de las decisiones en cuanto a estas inversiones no tienen un análisis profundo por ende el alineamiento estratégico del negocio con TI no se ve reflejado cuando entran en operación, lo que trae problemas futuros como lo son islas de información, fallas en la integración de sistemas de información, y en el peor de los casos las soluciones adquiridas se vuelven insuficientes en un plazo de tiempo menor que el esperado.

La integración de metodologías de seguridad de la información disminuye la probabilidad de que se presente un ataque informático, sin embargo, se debe generar un cambio organizacional para crear conciencia sobre las amenazas que tiene los activos de información. Con esto queda evidenciado que la seguridad incluye a personas y a herramientas tecnológicas y que no hay ningún sistema 100% seguro pero si se puede mitigar el riesgo que lo rodea.

Como trabajo futuro queda implementar la propuesta en empresas de distintos sectores de la economía de manera que se valide la efectividad de la misma y a su vez se enriquezca la propuesta.

Bibliografía

[1] Diario El Espectador, «Colombia lidera lista de ataques informáticos en países de habla hispana,» 20 Octubre 2014. [En línea]. Available: http://www.elespectador.com/tecnologia/colombia-lidera-lista-de-ataques-informaticos-paises-de-articulo-523201. [Último acceso: 15 Noviembre 2016].

[2] A. Molano, «colombiadigital.net,» 27 Enereo 2015. [En línea]. Available: http://www.colombiadigital.net/actualidad/articulos-informativos/item/8123-que-es-arquitectura-empresarial.html. [Último acceso: 2016 Julio 09].

[3] The Open Group, «Introduction,» 2011. [En línea]. Available: http://pubs.opengroup.org/architecture/togaf9-doc/arch/chap05.html. [Último acceso: 19 Noviembre 2016].

[4] A. Molano, «¿Qué es TOGAF?,» 20 Febrero 2015. [En línea]. Available: https://colombiadigital.net/actualidad/articulos-informativos/item/8163-que-es-togaf.html. [Último acceso: 13 11 2016].

[5] G. M, «Marco de trabajo Zachman,» 17 Junio 2014. [En línea]. Available: https://prezi.com/2lputchj3lgt/marco-de-trabajo-zachman/. [Último acceso: 18 Noviembre 2016].

[6] The Open Group Security Forum and Members of The Open Group Architecture Forum, «Guide to Security Architecture in TOGAF ADM,» San Francisco, CA 94104 , 2005.

[7] A. C. D. L. John Sherwood, de *Enterprise Security Architecture a Business-Driven Approach* , Nueva York, CRC Press, 2005, p. 587.

[8] vanharen, 22 Agosto 2013. [En línea]. Available: http://www.vanharen.net/blog/enterprise-architecture/sabsa-in-3-minutes/. [Último acceso: 18 Noviembre 2016].

[9] OSA, «opensecurityarchitecture.org,» [En línea]. Available: http://www.opensecurityarchitecture.org/cms/definitions/it-architecture. [Último acceso: 29 Junio 2016].

[10] OSA, «opensecurityarchitecture.org,» [En línea]. Available: http://www.opensecurityarchitecture.org/cms/definitions/it-security-architecture. [Último acceso: 29 Junio 2016].

[11] International Organization for Standarization, «www.iso27000.es,» [En línea]. Available: http://www.iso27000.es/download/doc_iso27000_all.pdf. [Último acceso: 4 Junio 2016].

[12] International Organization for Standarization, «ISO 27000,» [En línea]. Available: http://www.iso27000.es/download/doc_iso27000_all.pdf.

[13] offencivestate, «Estándar de seguridad ISO 2700,» 15 Septiembre 2015. [En línea]. Available: http://blog.offensivestate.com/2015/09/estandar-de-seguridad-iso-2700-primera.html. [Último acceso: 20 Noviembre 2016].

[14] J. C. Naranjo, *Templates*, Bogota, 2015.

[15] C. Villalba, *Valoración de riesgo*, Bogotá, 2015.

[16] C. Villalba, *Matriz Activos de información*, Bogotá, 2015.

[17] Caratina udlap, «Herramenientas de seguridad Cap. 2,» [En línea]. Available: http://catarina.udlap.mx/u_dl_a/tales/documentos/lis/argueta_a_a/capitulo2.pdf. [Último acceso: 18 Noviembre 2016].