ESCUELA COLOMBIANA DE INGENIERÍA JULIO GARAVITO

DOCUMENTO FINAL PROPUESTA DE INTEGRACIÓN DE ARQUITECTURA DE EMPRESARIAL Y ARQUITECTURA DE SEGURIDAD METADATA INGENIERÍA COLOMBIANA S.A.S

INTEGRANTES
FELIPE DÍAZ PALACIOS

PRESENTADO A:

CLAUDIA PATRICIA SANTIAGO CELY

PROYECTO DE GRADO 1
ESCUELA COLOMBIANA DE INGENIERÍA JULIO GARAVITO
BOGOTÁ DICIEMBRE 2016

ESCUELA COLOMBIANA DE INGENIERÍA JULIO GARAVITO

Tabla de contenido

1. Formulación del Proyecto

A continuación, se encuentra los objetivos del proyecto, así como su justificación, los cronogramas de trabajo y un resumen ejecutivo que pone en contexto al lector.

1.1 Información general del proyecto de grado

Nombre	Integración de la Arquitectura Empresarial y Arquitectura de Seguridad para PYMES.
DIRECTOR	CLAUDIA SANTIAGO CELY
EQUIPO DE ESTUDIANTES	FELIPE DÍAZ PALACIOS

GRUPO DE INVESTIGACIÓN	Ciencia, Tecnología y Gestión - CTG-Informática
LÍNEA DE INVESTIGACIÓN	Informática y MIPYME
PROYECTO DE INVESTIGACIÓN AL QUE PERTENECE	Información que deberá ser suministrada por el director de proyecto
DURACIÓN (MESES)	8 meses

1.2 Resumen ejecutivo

El proyecto busca definir y documentar la propuesta de integración de las arquitecturas empresarial y de seguridad para una empresa determinada, haciendo una investigación acerca de los diferentes frameworks (marcos de trabajo) con el fin de seleccionar los más adecuados de manera que estén fuertemente acoplados garantizando la seguridad de la información de la empresa y la alineación de sus procesos de negocio con los recursos de TI.

1.3 Descripción del proyecto

A continuación, se presentas los componentes más relevantes del proyecto.

1.3.1 Planteamiento del problema

Actualmente las PYMES no cuentan con un alineamiento estratégico entre sus procesos de negocio y los recursos de TI que poseen, de manera que sus procesos claves en la mayoría de los casos se realizan de manera ineficiente. Teniendo en cuenta que el recurso principal y más importante de cualquier empresa u organización es la información, se parte del hecho de que en general las empresas cuenta con una infraestructura tecnológica para almacenar, tratar y modificar la información que poseen que da respaldo a su operación pero esta infraestructura tecnología compuesta en su mayoría de los casos por software no se encuentra alineada, es decir no se tiene un alineamiento holístico entra la visión y razón de ser la empresa, sus procesos de negocio, los datos (información) que soportan los procesos, las aplicaciones (software) y la tecnología, y lo que es más alarmante no se cuenta con las de herramientas de seguridad necesarias para proteger la información.

1.3.2 Justificación

Partiendo del hecho de que la mayoría de las empresas no cuentan con una arquitectura empresarial establecida, es decir no tiene un alineamiento holístico entre sus procesos críticos y sus recursos

de TI, el proyecto busca la documentación y definición de una arquitectura empresarial objetivo de una organización caso de estudio, integrándola con un framework de arquitectura de seguridad con el fin de cubrir las brechas que existen en el tema de seguridad que están pendientes en la arquitectura empresarial puesto que toda la plataforma de hardware y software puede ser objeto de amenazas y de intentos de violación, obteniendo como resultado un alineamiento estratégico con parámetros de seguridad que tenga mecanismos para su implantación de tal manera que las empresas puedan dar respuesta a las necesidades de seguridad y privacidad de la información que ellos gestionan.

1.3.3 Objetivos generales y específicos

General: Probar la integración de las metodologías de arquitectura de seguridad a la arquitectura empresarial mediante la aplicación a un caso específico en donde se parta de una arquitectura empresarial y de seguridad base y se llegue a la implantación de una arquitectura objetivo incluyendo la evaluación y puesta en operación de herramientas tecnológicas que aporten a la arquitectura de seguridad definidas.

Específicos:

- Realizar una evaluación de dos o tres metodologías actuales de arquitectura empresarial y arquitectura de seguridad revisando la integración entre ellas para proponer un framework integrado en la empresa caso de estudio
- Realizar la construcción de la AE y AS actuales y objetivo para una empresa seleccionada
- Definir los planes a seguir para llegar a la arquitectura objetivo y las herramientas de seguridad necesarias propuestas para dicha arquitectura.

1.3.4 Alcance del proyecto

El proyecto tiene como finalidad definir y documentar la arquitectura actual y futura de una empresa en particular, se abstiene de realizar la implementación puesto que es una decisión final de la empresa que involucra costos y un horizonte de planeamiento largo, sin embargo, con la realización del proyecto se suministran las directrices necesarias para que la empresa pueda hacer la inversión de las arquitecturas integradas si se ajusta a su presupuesto.

1.3.5 Metodología propuesta

- Reuniones semanales con la directora de proyecto para presentar los avances del proyecto, de igual manera reuniones del grupo de estudiantes y profesores de la línea de sistemas y organizaciones.

- Investigación acerca sobre que es una arquitectura empresarial y arquitectura de seguridad y frameworks.
- Integración de frameworks empresariales y de seguridad seleccionados
- Diseño y documentación de arquitectura de negocio, datos, aplicaciones y tecnología integrados con seguridad
- Evaluación de la propuesta de integración de las arquitecturas empresarial y de seguridad.

1.3.6 Área de aplicación del producto resultado del proyecto

La implementación de la propuesta se realizó en la empresa Metadata Ingeniería Colombiana S.A.S.

1.3.7 Cronogramas

1.3.8 Cronograma proyecto de grado 1

Integracion de Arquitectura Empresarial y arquitectura de seguridad para

Actividad	Fecha
Definicion estructura marco teórico	3 de Junio
Investigacion ¿Qué es arquitectura empesarial?	6 de Junio - 10 de Junio
Formulacion Proyecto de grado	11 de junio
Investigación frameworks arquitectura empesarial	11 de Junio - 13 de Junio
Investigación ¿Qué es arquitectura de seguridad?	14 de Junio - 17 de Junio
Investigación frameworks arquitectura de seguridad	18 de Junio - 20 de Junio
Vitrina académica - preparacion 1	21 de Junio
Registro versión inicial cartelera	21 de Junio
Relacion entre Arq. Empresarial - Arq. Seguridad	21 de Junio - 24 de Junio
Relación entre Frameworks seleccionados	27 de Junio - 1 de Julio
Presentacion Marco teórico	8 de julio
Diseño capa de negocio (Arq. Empresarial)	8 de julio - 22 de Julio
entrega cartelera	11 de Julio
Montaje vitrina académica	13de Julio
Vitrina académica	14 de Julio

1.3.8.1 Cronograma proyecto de grado 2

Actividad	Fecha
Arquitectura de Negocio	10 de agosto
Primera Reunion	19 de Agosto
Cronograma y metas	19 de Agosto
Formulación PGR2	19 de Agosto
Ajuste Propuesta de integración	22 de agosto
Tercera reunión Metadata Ingeniería Colombiana LTDA	25 de agosto
Inicio Arquitectura de Datos	25 de agosto
Fin Arquitectura de Datos	19 de septiembre
Cuarta reunión Metadata Ingeniería Colombiana LTDA	22 de septiembre
Inicio Arquitectura de Aplicaciones	20 de septiembre
Fin Arquitectura de Aplicaciones	19 de octubre
Quinta reunión Metadata Ingeniería Colombiana LTDA	26 de octubre
Inicio Arquitectura de Tecnología	24 de octubre
Registro versión inicial cartelera	15 de noviembre
Registro versión final Cartelera	16 de noviembre
Fin Arquitectura de Tecnología	20 de noviembre
Entrega física Cartelera	21 de noviembre
Montaje vitrina académica	23 de noviembre
Vitrina académica	23 de noviembre
Entrega Artículo técnico	2 de diciembre
Presentación Final	13 de diciembre
Entrega Productos	13 de diciembre

1.3.9 Criterios de aceptación

El proyecto debe contar la definición y documentación de las arquitecturas empresarial y de seguridad integradas, para ellos se debe presentar la propuesta de arquitectura objetivo de la empresa con las recomendaciones a seguir para que la empresa decida implementarla o no.

1.3.10 Evaluadores

- Ing. Oswaldo castillo Navetty
- Ing. Paula Uribe Vega-Lara
- Ing. Victoria Ospina Becerra
- Ing. Luis Daniel Díaz

2. Marco teórico y estado del arte

2.1. Arquitectura Empresarial

¿Qué es una 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 [1], 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. Es importante resaltar que la mayoría de empresas no cuenta con una arquitectura empresarial implementada en parte por el desconocimiento de la misma y porque no conocen los beneficios que lleva consigo.

La siguiente imagen ilustra los componentes que debe tener una arquitectura empresarial:

[2]

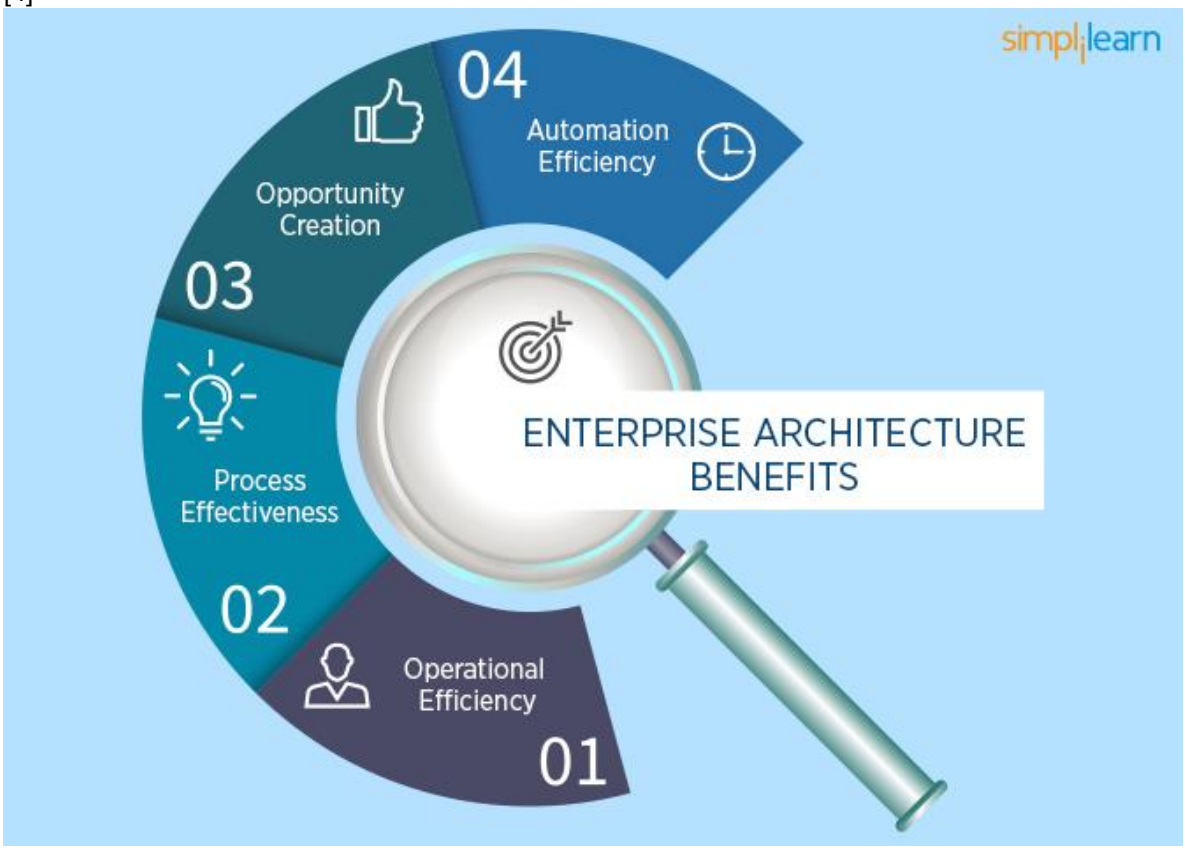
Fuente: Adaptación de Colombia Digital del gráfico desarrollado por Amazing Consultores

El objetivo general de la implementación de una arquitectura empresarial es garantizar la correcta alineación de los recursos tecnológicos y los procesos de negocio en una organización, con el propósito de alcanzar el cumplimiento de sus objetivos estratégicos.

[3]

Los beneficios de la arquitectura empresarial se ven reflejados en la parte operacional (negocio) mejorando el alineamiento del negocio con TI (Tecnologías de la información) de manera que los procesos se realizan de manera más eficiente y efectiva reduciendo los tiempos de producción, en la parte TI puesto que permite la implantación de plataformas y de más herramientas tecnológicas (software, hardware, redes, aplicaciones) de manera acoplada y automatizada, y finalmente en el entorno financiero mejorando el retorno en la inversión actual y minimizando el riesgo de futuras inversiones, ahorrado costos y creando nuevas oportunidades para el negocio a través de un modelo de inversión predecible. La siguiente grafica ilustra los beneficios mencionados anteriormente:

[4]



Algunas definiciones de Arquitectura Empresarial

TOGAF: La definición textual que TOGAF tiene de arquitectura empresarial "es la definición y representación de una vista de alto nivel de los procesos de negocio de una empresa y los sistemas de TI, sus interrelaciones, y el grado en que estos procesos y sistemas son compartidos por diferentes partes de la empresa"[1].

El centro de investigación de sistemas de información lo define MIT lo define como "la lógica de la organización y de los procesos de negocio e infraestructura de TI que refleja la integración y los requisitos de normalización de modelo de funcionamiento de la compañía"[2]

Para Gartner (empresa consultora y de investigación de las tecnologías de la información) la arquitectura empresarial "es una disciplina para liderar proactivamente y de manera integral una empresa, respondiendo a las fuerzas disruptivas mediante la identificación y el análisis de la ejecución del cambio hacia la visión y los resultados de negocio deseados. Ofrece valor mediante la presentación de los líderes de negocios y de TI con las recomendaciones de la firma para ajustar las políticas y proyectos y lograr resultados de negocio"[3].

[1] Traducción libre de **Fuente especificada no válida.**
[2] Traducción libre de **Fuente especificada no válida.**
[3] Traducción libre de **Fuente especificada no válida.**

ESCUELA
COLOMBIANA
DE INGENIERÍA
JULIO GARAVITO

FRAMEWOKS DE ARQUITECTURA EMPRESARIAL MÁS RELEVANTES

Framework TOGAF

La arquitectura empresarial tiene los siguientes componentes:

1. Visión de la arquitectura (Alineamiento estratégico)
2. Arquitectura de negocio (Procesos)
3. Arquitectura de datos (información)
4. Arquitectura de Aplicaciones
5. Arquitectura de tecnología.

Visión de la Arquitectura

También se conoce como fase preliminar, tiene como objetivo documentar los lineamientos estratégicos de la compañía con el fin de alinearlos, se deben identificar las partes interesadas (Stakeholders) y el plan de trabajo con las mismas, en este punto se documenta, crea o define la misión de la compañía (por qué existe la empresa), la visión (proyección de la empresa en un periodo de tiempo determinado) y la estrategia (cómo superar a la competencia). Para describir de manera más detallada el último ítem se deben documentar los objetivos estratégicos de la empresa, que son suministrados por la compañía.

Se debe definir el alcance de la arquitectura y principios de la arquitectura dependiendo de la vertical del negocio, las metas del negocio, sus limitaciones, resumir las necesidades de los clientes, sus requerimientos, las políticas y principios de la empresa.

Deben describirse los roles de la compañía para identificar su función dentro de la misma. Los principios de negocio tienen una razón de ser y unas implicaciones que deben se descritas, se deben documentar al menos dos principios por cada arquitectura (negocio. datos, aplicaciones y tecnología).

Arquitectura de Negocio

El objetivo de esta arquitectura es entender, describir y modelar el estado actual de los procesos de negocio con el fin de desarrollar la arquitectura de Negocio objetivo, en esta fase se pretende analizar 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. En este punto los programas derivados deben apuntar a los objetivos estratégicos definidos en la fase anterior (visión de la arquitectura) para lograr el alineamiento estratégico deseado.

Arquitectura de Datos

Tiene como misión definir los tipos y fuentes de información para dar soporte al sistema, 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 pretende identificar 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 las futuras.

Por último se debe describir el flujo de información de los procesos de negocio definidos en la capa anterior, para esto se propone el uso de un diagrama de flujo de datos por proceso, para eso se puede hacer uso de la herramienta Microsoft Visio.

Arquitectura de Aplicaciones

Es un marco de referencia que reúne todas las aplicaciones del negocio con su respectiva funcionalidad y su evolución. Tiene como objetivo definir y/o describir 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 y BD que almacenen la información

Para documentar la arquitectura de aplicaciones inicialmente se debe tener un inventario de las mismas de manera. 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.

Arquitectura de Tecnología

Es un marco de referencia que reúne 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).

Framework Zachman

Es un marco de referencia de arquitectura empresarial que tiene como características la descomposición de la complejidad de un negocio a través de la descripción de sus componentes. Fue creado en 1984 por John Zachman y publicado en 1987 en el IBM Systems Journal.

La metodología propuesta está plasmada 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. A continuación, se presenta en detalle la razón de ser de cada pregunta:

¿Qué? Entidades de información presentes en los procesos de negocio de la empresa que son representadas en estructuras de datos como tablas estructuradas y modelos relacionales.

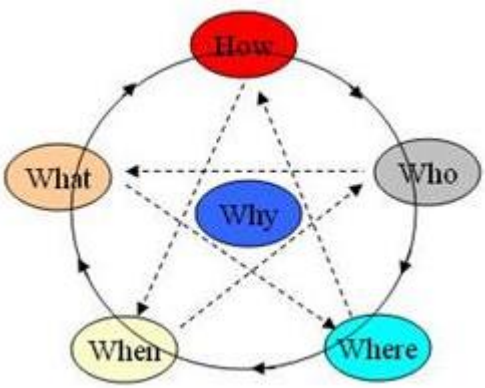
¿Cómo? Funciones de las aplicaciones, del hardware y las redes que dan soporte a los procesos de negocio.

¿Dónde? Distribución geográfica de la empresa.

¿Quién? Personas de la empresa, estructura de autoridad y delegación de trabajo.

¿Cuándo? Relación del tiempo con los recursos y criterios de rendimiento de los procesos de la empresa.

¿Por qué? Razón de los objetivos de la empresa. [5]



[6]

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. A continuación se presenta una descripción detallada de cada ítem de la primera columna:

Objetivo: resumen con una estimación del tamaño, el costo y la funcionalidad de un sistema específico. Tiene como objetivo controlar el entorno competitivo de la empresa, así como sus fuerzas

internas y externas que influyen en lo anterior, de manera que las especificaciones de sus objetivos a largo plazo sean claras.

Modelo de negocio: Contiene las entidades y los procesos de negocio haciendo énfasis en su interacción usando diagramas de procesos, de flujo de trabajo que reflejan la operación de la empresa.

Modelo de sistema: Tiene como finalidad determinar los componentes de datos y especificaciones de software que representan el modelo de negocio para su posterior análisis.

Modelo tecnológico: contempla las limitaciones que tienen los componentes y herramientas de tecnología. En este punto se construyen (definen) los sistemas de información teniendo en cuenta sus restricciones.

Representación detallada: tiene como finalidad la representación de los módulos que suplen las necesidades del negocio de manera individual.

Funcionamiento de la empresa: representa la operación de la empresa.

[7] Ilustración gráfica de la matriz Zachman

El marco de trabajo de Zachman	DATOS Qué (Cosas)	FUNCION Cómo (Proceso)	RED Dónde (Locación)	GENTE Quién (Gente)	TIEMPO Cuando (Tiempo)	MOTIVACION Porqué (Motivación)
MIRA (Contextual) Planificador						
MODELO DE NEGOCIO (Conceptual) Dueño						
MODELO DE SISTEMA (Lógico) Diseñador						
MODELO DE TECNOLOGIA (Físico) Constructor						
PRESENTACIONES DETALLADAS (Fuera de contexto) Subcontratista						
FUNCIONAMIENTO EMPRESA						

Selección framework de arquitectura para el desarrollo de la propuesta.

Luego de la investigación acerca de los frameworks de trabajo más relevantes sobre arquitectura empresarial, se toma la decisión de seguir la metodología propuesta por TOGAF, la razón se debe a que suministra un número de plantillas conocidas por los participantes del proyecto relativamente sencillas de documentar, mientras que el framework de Zachman presenta un tipo de documentación un poco pesado [8], esto se debe a uno de sus principios de arquitectura que dice que cada celda es independiente de la otra, teniendo en cuenta esto la figura anterior cuenta con 36 celdas que pueden ser modeladas por varios modelos (según el caso).

La metodología de Zachaman no tiene un orden establecido, al ser cada celda independiente se podría empezar desde un punto no definido y desarrollar la arquitectura desde ahí, esto puede tergiversar el enfoque que se busca en la arquitectura empresarial de buscar un alineamiento holístico desde el principio de la arquitectura, este alineamiento se puede llevar a cabo implementando la metodología propuesta por togaf.

2.2. Arquitectura de seguridad

¿Qué es una arquitectura de seguridad?

La 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 de las personas que pertenecen a la empresa en general. 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 presenta actualmente sus activos mediante la implementación de herramientas de seguridad que protejan la información.

Inicialmente la arquitectura de seguridad fue propuesta en primera instancia por Gartner Inc. Empresa especializada en el desarrollo de frameworks de trabajo para varios tipos de arquitecturas incluida la empresarial y de seguridad, pero existen varios modelos o marcos de trabajo que indican metodologías para la definición e implementación de la arquitectura de seguridad.

La arquitectura de seguridad tiene como objetivo minimizar el riesgo al que está expuesta la información y las personas que pertenecen a una empresa determinada, 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 al que están expuestos que pueden ir desde la intercepción de un recurso o hasta la interrupción del mismo, generando una denegación del servicio a los usuarios.

[9]

Inicialmente la arquitectura de seguridad utiliza herramientas que permiten evaluar y establecer políticas de seguridad que mitigan en gran porcentaje las vulnerabilidades que tiene los sistemas, se clasifican de la siguiente manera:

- Herramientas de monitoreo: analizan la confiabilidad de un sistema ofreciendo un grado mínimo de seguridad en la red. Entre ellas tenemos a SATAN, que busca y genera automáticamente reportes acerca de las vulnerabilidades de una red

- Herramientas de seguridad: Modifican los parámetros de un sistema con el fin de asegurarlo contra diversos ataques, entre los más comunes están los Firewalls

  (filtrar tráfico de información entre 2 redes), la criptografía que busca codificar los mensajes apara que no puedan ser interceptados por personas ajenas a ellos y Kerberos que está diseñado para procesos de autenticación permitiendo enviar su identificación a otros a través de redes de segura a través de un servidor de red seguro haciendo uso de la inscripción. [10]

Para que las herramientas mencionadas anteriormente tengan un impacto en la seguridad de la empresa se deben tener en cuenta las siguientes premisas:

- ¿Qué acciones comprometen la seguridad de la información de la organización?

- ¿Qué mecanismos se deben implantar para prevenir o recuperarse ante un ataque?
- ¿Qué servicios se deben ofrecer al usuario respecto a la transferencia de información en una red de datos?

Algunas definiciones de arquitectura de seguridad

Enterprice Security Architecture la define como "El arte y ciencia de diseñar y supervisar la construcción de sistemas del negocio, usualmente sistemas de información del negocio, los cuales son: libres de peligro, daño, etc. Libres de miedo, preocupaciones, etc. En un lugar seguro, que no suele fallar, capaz de responder a un ataque de forma segura".[4]

Open security architecture: "el diseño de artefactos que describe como los controles de seguridad están procesiones y como se relacionan con la arquitectura de. Estos controles tiene el propósito de mantener los atributos de calidad del sistema (confidencialidad, integridad, disponibilidad, responsabilidad y garantía"[5].

TOGAF Framework [11]

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.

[4] Traducción libre de [13]
[5] Traducción libre de **Fuente especificada no válida.**

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:

Autenticación: es fundamental contar con la identidad de las personas o entidades que tienen relación con algún sistema de la empresa.

Autorización: definición y ejecución de las capacidades permitidas para una persona o entidad.

Auditoria: capacidad de suministrar datos forenses que den constancia de que los sistemas se han utilizado de acuerdo con las políticas de seguridad establecidas.

Aseguramiento: demostrar que la arquitectura de la empresa tiene los atributos de seguridad necesarios para defender las políticas de seguridad establecidas.

Disponibilidad: garantiza que la empresa pueda operar sin la interrupción de los servicios prestados a pesar de eventos o ataques maliciosos.

Protección de activos: protección de los activos de información ante su pérdida o divulgación y los recursos de usos no autorizados o no esperados.

Administración: capacidad de modificar o añadir las políticas de seguridad, personas o entidades relacionadas con los sistemas de información.

Gestión del riesgo: tolerancia de la organización al riesgo.

La arquitectura debe incluir las reglas del negocio en cuanto al manejo de información, codificación de los datos, políticas de seguridad por escrito, documentación de análisis de riesgo y documentación de la clasificación de los datos.

Componentes de la arquitectura de seguridad [12]

1. Visión de la arquitectura.
2. Arquitectura de negocio
3. Arquitectura de sistemas de información
4. Arquitectura de tecnología

Fase preliminar

La fase preliminar busca definir el alcance y los principios de arquitectura con el fin de identificar las limitaciones y las libertades presentes en el desarrollo de la misma, posteriormente se deben definir un arquitecto de seguridad y/o un grupo de arquitectura de seguridad a los cuales se le indican las funciones y responsabilidades que deben cumplir y su lugar de ubicación dentro de la compañía.

Visión de la arquitectura

La visión de la arquitectura tiene como objetivo validar y definir los principios de negocio de la empresa de manera que estén acordes a su razón de ser, de igual manera busca definir los objetivos de la empresa a través de la identificación de los principales stakeholders (interesados) quienes expresan sus preocupaciones de modo que se pueden identificar los requerimientos clave de la empresa y empezar a plantear la estrategia de la organización.

En este punto se pretende identificar los procesos criticos de la compañía con el fin de identificar cuales podrian ser los posibles planes de continuidad de negocio y planes de recuperacion de desastres en caso de ser presentados, también se quiere llegar a la documentación de los entornos físicos del negocio ya sean ambientes comerciales, entornos móviles, lugares al aire libre, así como el entorno empresarial en el que trabajan las personas pertenecientes a la compañía.

Arquitectura de negocio

Tiene como objetivo desarrollar los objetivos de la arquitectura, para esto se debe describir la organización, las funciones y procesos, la información, los aspectos geográficos del entorno del negocio, basados en los principios y los objetivos estratégicos del negocio. Se debe realizar el análisis gap para definir la situación actual de la empresa y plasmar la arquitectura objetivo.

En este punto se deben identificar y documentar los activos de la compañía, así como los actores legítimos que pueden estar involucrados en el proceso, definiendo los diferentes roles existentes que usan los sistemas presentes en los procesos (Administradores, usuario y operarios). Posteriormente se debe evaluar la seguridad de estos procesos a través de la documentación de como los usuarios del sistema hacen uso del mismo. Se debe definir el nivel de aceptación mínimo en caso de que se presente un inconveniente para la utilización de las medidas de seguridad para que los intentos de

burlar estas medidas por los usuarios del sistema sean fallidos. Se debe determinar el costo de los activos perdidos en caso de alguna falla.

Arquitectura de sistemas de información

Tiene como objetivo definir y documentar el nivel de sensibilidad de la información almacenada en los sistemas de información determinando las obligaciones a las que el sistema y sus propietarios son sometidos, de tal manera que exista una responsabilidad por parte de los sistemas en el mantenimiento de la confidencialidad de los datos. De la misma manera se quiere identificar la relación del sistema con los planes de continuidad y planes de desastres existentes en el negocio, de esta manera se obtiene la situación actual y se puede plantear la arquitectura objetivo abordando los siguientes enfoques:

- Mitigación
- Aceptación
- Transferencia
- Evitar

Arquitectura de tecnología

El objetivo de la arquitectura de tecnología se basa en la creación de las especificaciones técnicas detalladas en los sistemas en los cuales se implementarán los requisitos de seguridad definidos en las arquitecturas anteriores, se debe identificar primero el estado actual de la seguridad en los sistemas específicos para definir la arquitectura objetivo, mediante la implementación de estándares, normas y directrices aplicables a la compañía.

Es aconsejable identificar el nivel de confianza de:

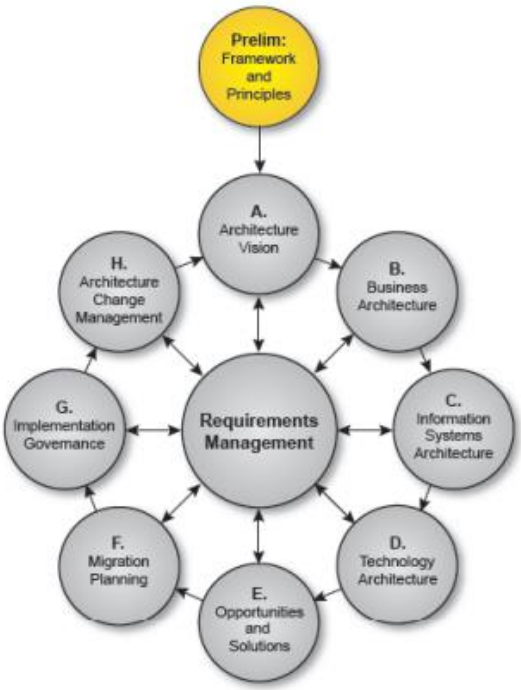
- Todos los usuarios del sistema
- Administradores del sistema
- Todos los sistemas de interconexión más allá del control del proyecto

Los compontes que tiene influencia en este punto van desde los requisitos reglamentarios, los niveles de clasificación de la información, las necesidades del negocio y los activos.

La arquitectura tiene como resultado para la organización lo siguiente:

- Lista de estándares de seguridad

- Plan de conservación de los recursos
- Planes de monitoreo y métricas de seguridad
- Políticas de autorización de usuarios
- Plan de gestión de riesgos



SABSA Framework [13]

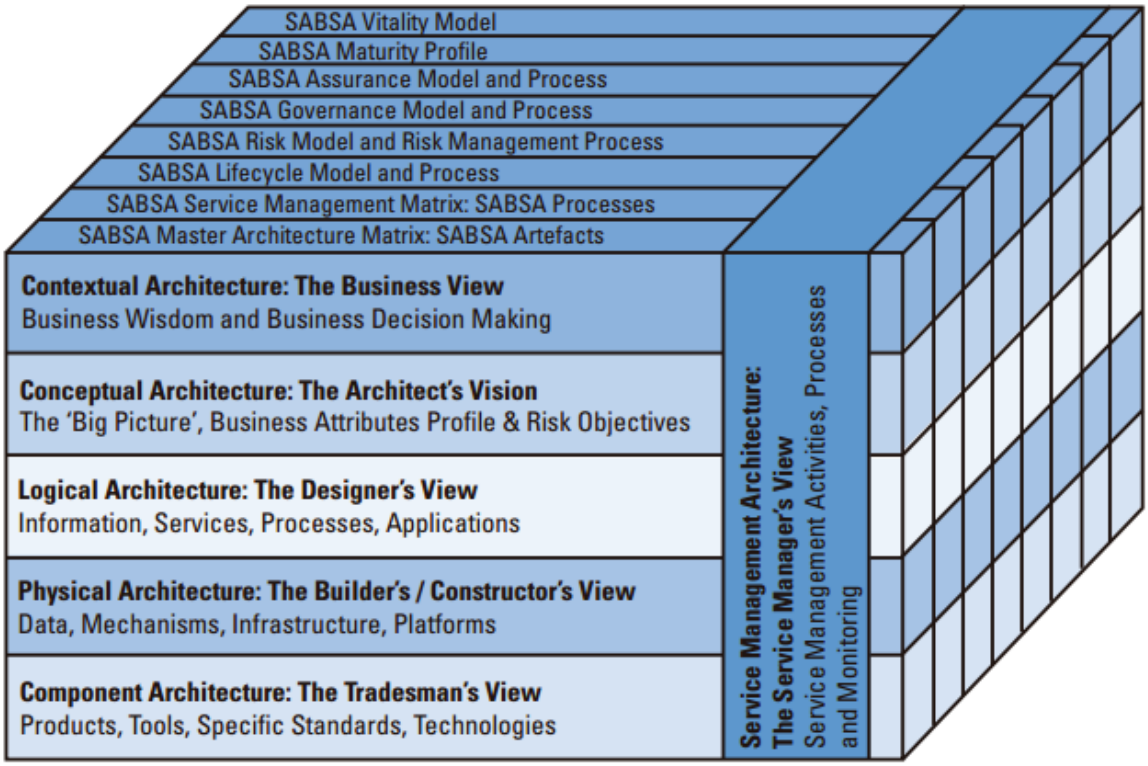
SABSA es un modelo y una metodología para desarrollar el manejo de riesgo en una arquitectura de seguridad empresarial, tiene como objetivo la entrega de soluciones de infraestructura de seguridad que soporten las iniciativas críticas para el negocio. La característica principal del modelo de SABSA consiste 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.

El proceso de análisis de los requerimientos de negocio permite la planeación de la estrategia, que posteriormente es diseñada e implementada a través de las fases del modelo teniendo como resultado indicadores o medidas que permiten determinar la preservación del negocio a lo largo del ciclo de vida del modelo. [14]

El modelo SABSA esta comprendido por seis (6) 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. Cada capa mencionada

anteriormente representa una vista dentro de los roles existentes en el proceso de especificación, diseño y construcción.

[15]



El modelo SABSA formula las mismas seis preguntas del framework de Zachman, que, por qué, cómo, dónde y cuándo para realizar el análisis a través de las seis capas.

Business view

Esta capa busca definir los requerimientos del negocio, los cuales se deben cumplir en la arquitectura, en este punto se le empieza a dar forma a la matriz de SABSA con la primera pregunta del modelo que representa la parte contextual de la arquitectura, teniendo como resultado una descripción del negocio y del contexto de como deber ser diseñando, construido y operado un sistema seguro.

Pregunta	Descripción	Ejemplo
What	Busca identificar los requerimientos que necesita el negocio para garantizar la seguridad de la información	Continuidad operacional y estabilidad del negocio
Why	Busca identificar los riesgos del negocio expresados a través de metas que tiene el negocio	Protección de la marca, prevención ante perdidas de información
How	Busca identificar los procesos de negocio de la organización más críticos que requieren seguridad	Transacciones, comunicaciones, etc.

Who	Busca identificar los componentes de las dependencias organizaciones que requieren seguridad dada su naturaleza	Cadena de suministro, out-sourcing
Where	Busca identificar el lugar geográfico donde se localiza el negocio	Estaciones de trabajo, puntos de venta, franquicias
When	Busca identificar los tiempos de dependencia del negocio	Tiempo de vida – Tiempos muertos

Architect view

En esta capa el arquitecto del negocio debe identificar los activos de la compañía que se deben proteger, teniendo en cuenta los requerimientos establecidos en la capa anterior que evidencia la razón por la cual deben ser protegidos. Se debe plantear la estrategia de seguridad en términos de alto nivel, definir quiénes están involucrados en el manejo de la seguridad y decidir cuándo es relevante la protección.

Designer view

Teniendo en cuenta que la información del negocio es una representación lógica del negocio real, esta capa busca representar la estructura lógica de la estrategia de seguridad de la arquitectura de seguridad conceptual definida en la capa anterior respondiendo las siguientes preguntas

Pregunta	Descripción
What	Que información necesita ser asegurada
Why	Especificación de políticas de seguridad
How	Especificación de los servicios de seguridad (autenticación, confidencialidad, integridad, etc)
Who	Especificación de las entidades (usuarios, administradores, auditores)
Where	Especificación de los dominios de seguridad (lógicos y físicos)
When	Especificación del ciclo de procesamiento de seguridad (Registro, certificación, login, etc.)

Builders view

La arquitectura de seguridad física se tiene como objetivo definir las siguientes especificaciones:

Pregunta	Descripción
What	Modelo de datos y la respectiva seguridad de las estructuras de datos (tablas, mensajes , certificados)
Why	Reglas , condiciones, practicas
How	Mecanismo de seguridad (encripción, control de acceso etc.)
Who	Aplicaciones que usan los usuarios y la seguridad de la interfaz de usuario
Where	Seguridad en la infraestructura tecnológica (hardware, software y líneas de comunicación)
When	Tiempo de dependencia en base a la ejecución de estructuras de control

Tradesman view

Tiene como objetivo detallar la estructura de los datos planteada en la capa anterior, con el fin de seleccionar estándares de seguridad e implementarlos a través de herramientas y productos de seguridad para que las funciones del sistema sean seguras para los usuarios de la compañía.

Facilities manager

Esta capa tiene como función supervisar la operación en general, de manera que los servicios prestados operen de la manera que deben operar de acuerdo a los requerimientos establecidos antes de la fase de construcción, en otras palabras busca garantizar la continuidad del negocio en términos de confidencialidad, integridad, disponibilidad, auditabilidad y responsabilidad a través de la administración segura de usuarios, la administración de los sistemas de seguridad, la realización constante de back ups y demás acciones que hayan sido consideradas en las fases anteriores.

[14]

The SABSA matrix

SABSA	Assets (WHAT)	Motivation (WHY)	Process (HOW)	People (WHO)	Location (WHERE)	Time (WHEN)
Contextual	The Business	Business Risk Model	Business Process Model	Business Organisation and Relationships	Business Geography	Business Time Dependencies
Conceptual	Business Attributes Profile	Control Objectives	Security Strategies and Architectural Layering	Security Entity Model and Trust Framework	Security Domain Model	Security-Related Lifetime and Deadlines
Logical	Business Information Model	Security Policies	Security Services	Entity Schema and Privilege Profiles	Security Domain Definitions and Associations	Security Processing Cycle
Physical	Business Data Model	Security Rules, Practices and Procedures	Security Mechanisms	Users, Applications and User Interface	Platform and Network Infrastructure	Control Structure Execution
Component	Detailed Data Structures	Security Standards	Security Products and Tools	Identities, Functions, Actions and ACLs	Processes, Nodes, Addresses and Protocols	Security Step Timing and Sequencing
Operational	Assurance of Operational Continuity	Operational Risk Management	Security Service Management and Support	Application and User Management and Support	Security of Sites and Platforms	Security Operations Schedule

Otros Frameworks, Estándares y controles

OSA Arquitectura de seguridad TI

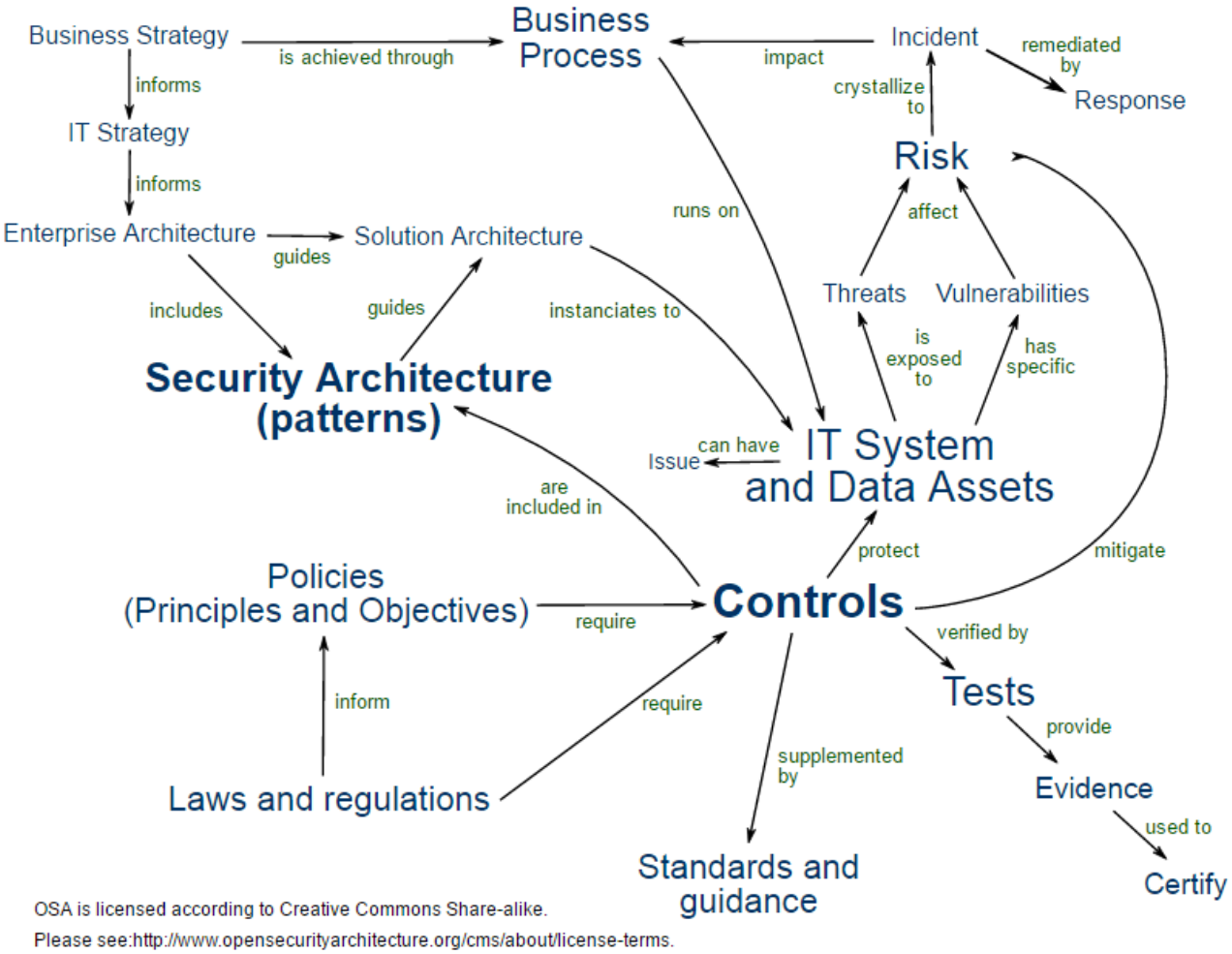
OSA (Open Security Architecture) tiene una definición de arquitectura de seguridad compuesta por dos componentes fundamentales, Seguridad TI y Arquitectura TI (Diseño de artefactos que describe la estructura de los compontes de la organización, sus interrelaciones, principios y directrices que gobiernan su diseño y evolución) [16]. En esencia consiste en el diseño de herramientas o artefactos que describen como los controles de seguridad están posicionados y como 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. [17]

La arquitectura de seguridad de OSA se centra en la identificación del riesgo al que están expuestos los sistemas de TI que dan soporte a los procesos de negocio de la organización, presenta un gran

acoplamiento a la arquitectura empresarial puesto que se ve involucrada la estrategia de negocio. Inicialmente se realiza un análisis de riesgo que tiene como objetivo identificar las vulnerabilidades a las que están expuestas los sistemas y medir el impacto que tiene en los procesos de negocio en caso de presentarse un incidente, busca mitigar estas vulnerabilidades con la implementación de controles, que básicamente definen un conjunto de políticas (principios y objetivos) que van ligados a las leyes y regulaciones que debe cumplir la empresa dependiendo de su razón de ser, el cumplimiento de estas leyes y regulación es soportado por estándares y directrices que son probadas y tienen como resultado la emisión de certificados.

La siguiente grafica describe detalladamente el flujo de procesos descrito anteriormente que el modelo OSA lleva a cabo en su modelo de arquitectura.

[18]



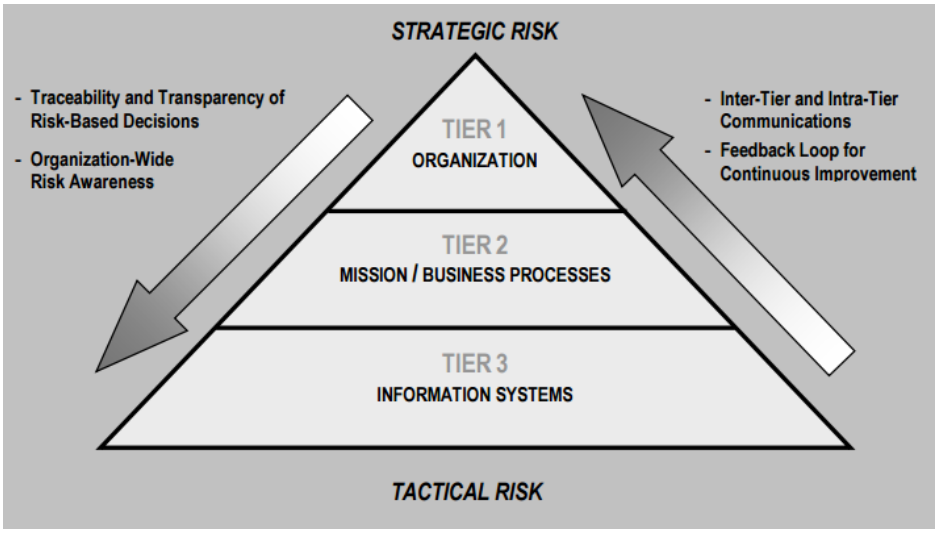
NIST (National Institute of standars an technology) publicación especial 800-53 [19]

El NIST es un instituto especializado en medidas y estándares tecnológicos regulado por la agencia del departamento de comercio de los Estados Unidos, en abril de 2013 realizo una publicación acerca de la seguridad y controles de privacidad que tiene las siguientes características:

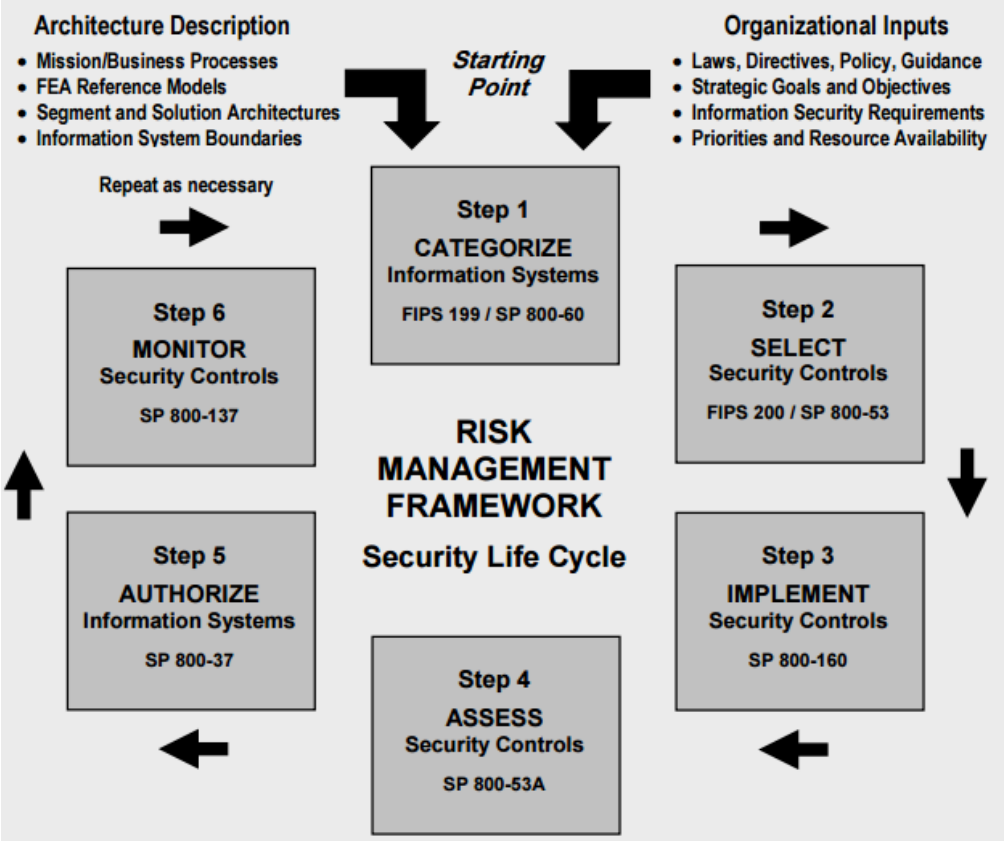
El manejo de riesgo está compuesto por la selección y la especificación de los controles de seguridad para un sistema de información, los controles pueden ser leyes federales, órdenes ejecutivas, directivas, políticas, regulaciones, estándares y directrices. Maneja tres niveles en particular:

- Nivel 1: organizacional
- Nivel 2: misión / procesos de negocio
- Nivel 3: sistemas de información

El nivel 1 proporciona las priorizaciones de la organización basadas en la misión y las funciones del negocio que giran en torno a la estrategia de inversión en soluciones en tecnologías de la información que sean consistentes con los objetivos estratégicos de la organización, El segundo nivel define los procesos de negocio necesarios para soportar la misión organizacional y las funciones del negocio, determina las categorías de seguridad de los sistemas de información necesarios, incorpora los requerimientos de seguridad de la información dentro de la misión y los procesos de negocio y por ultimo establece una arquitectura empresarial para facilitar la asignación de los controles de seguridad a los sistemas de información de la organización y el entorno en el que los sistemas operan.



El framework de trabajo propuesto en la publicación de NIST está compuesto de 6 pasos, el primero consiste en la categorización de los sistemas de información, el segundo se basa en seleccionar los controles de seguridad aplicables a los resultados de la categorización del paso 1, el tercero se encarga en la implementación de los controles de seguridad y la documentación del diseño y desarrollo de los mismos, el cuarto paso evalúa los controles de seguridad para determinar cuáles controles fueron implementados correctamente en base a los requerimientos de seguridad, el quinto paso consiste en la autorización de la operación de los sistemas de información y el sexto paso consiste en el monitoreo de los controles de seguridad implementados en los sistemas de información y en el ambiente de operación basados en los cambios en el sistema y/o en el ambiente según las leyes federales, órdenes ejecutivas, directivas, políticas, regulaciones, estándares y directrices.



A continuación se muestra una tabla con los controles de seguridad sugeridos en la publicación NIST 800-53:

ID	FAMILY	ID	FAMILY
AC	Access Control	MP	Media Protection
AT	Awareness and Training	PE	Physical and Environmental Protection
AU	Audit and Accountability	PL	Planning
CA	Security Assessment and Authorization	PS	Personnel Security
CM	Configuration Management	RA	Risk Assessment
CP	Contingency Planning	SA	System and Services Acquisition
IA	Identification and Authentication	SC	System and Communications Protection
IR	Incident Response	SI	System and Information Integrity
MA	Maintenance	PM	Program Management

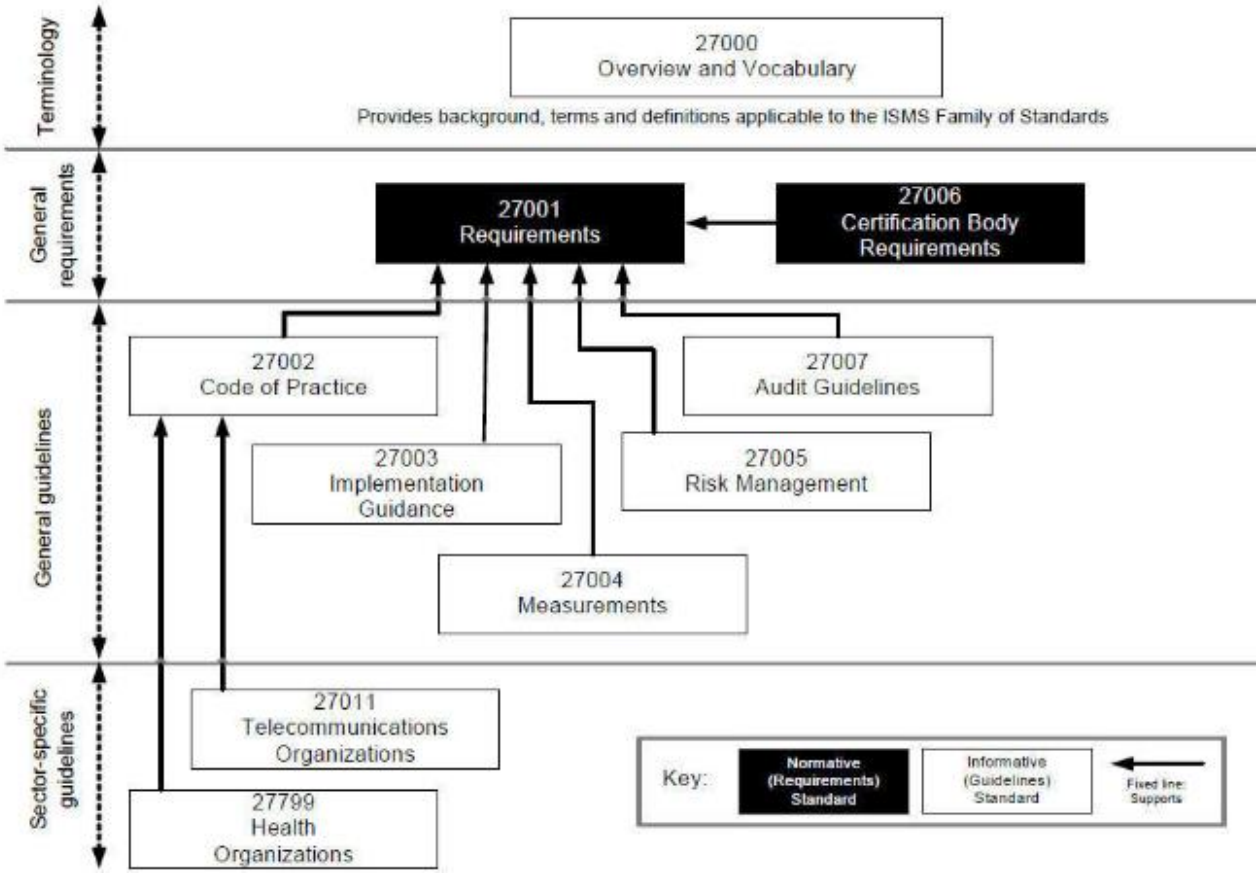
ISO 27000 [20]

La serio ISO (International Organization for Standarization) 27000 son 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.

La implementación de los estándares sugeridos en la estructura ISO 27000 tiene como beneficios el establecimiento de una metodología de gestión de la seguridad clara y estructurada, se reduce el riesgo de pérdida, robo o corrupción de información, los clientes tiene acceso a la información a través de medidas de seguridad, los riegos y sus controles son revisados continuamente, 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.

ISO 2700 tiene la siguiente estructura de normas aplicables al proyecto:

[21]



- **ISO/IEC 27000: Vocabulario (Abril de 2009)**

- **ISO/IEC 27001: ISMS – Requisitos para Sistema de Gestión de Seguridad de la Información (SGSI) (2005 y 2013)**

  Es un marco de políticas, prácticas y recursos desarrollado por la organización con el fin de implementar, mantener y mejorar la seguridad de sus activos de información, el sistema de gestión de seguridad informática (SGSI)es una herramienta que permite identificar, gestionar y minimizar los riesgos que pueden atentar contra la seguridad de la información de la empresa.

- **ISO/IEC 27002: Code of practice for information security management (2005 y 2013).**

  Es una guía de buenas prácticas en la cual se describen los objetivos y controles recomendables para garantizar la seguridad de la información. Contiene 39 objetivos de control y 133 controles agrupados en 11 dominios

- **ISO/IEC 27003: ISMS implementation guidance (Febrero de 2010). Directrices para alcanzar 27001**

- **ISO/IEC 27004: Information security management measurement (Diciembre de 2009). Cómo medir los controles generados.**

  Es una especificación de las métricas y técnicas de medida aplicables para determinar la eficacia de un SGSI y de los controles relacionados.

- **ISO/IEC 27005: Information security risk management (junio de 2008). Marco para la gestión del riesgo.**

  Establece las directrices para la gestión del riesgo de la seguridad informática. Es un apoyo para los conceptos de la norma ISO 27001 de manera que de soporte en la gestión de riesgos.

- **ISO/IEC 27006: Requirements for bodies providing audit and certification of information security management systems (febrero de 2007) – certificación de las certificadoras**

  Establece los requisitos para la acreditación de las entidades de certificación y auditoria de los sistemas de gestión de seguridad informática.

3. Propuesta de integración de arquitectura empresarial y arquitectura de seguridad

La investigación del estado del arte de la arquitectura empresarial y arquitectura de seguridad son la base para proponer la integración de los marcos de trabajo de TOGAF para ambas arquitecturas, la razón de la selección de estos frameworks se basa en que en la arquitectura empresarial maneja un 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 profundiza el concepto de gestión de riesgo, el cual es sumamente importante puesto que el principal recurso de las empresas es la información que manejan. Por otro lado, TOGAF tiene un marco de trabajo el cual maneja una estructura diseñada para el desarrollo del manejo de riesgo que no está integrado con el marco empresarial.

Los dos modelos de TOGAF están compuestos de 5 (vistas, arquitecturas, capas, etc.) en las cuales se realizan tareas similares, pero con diferentes énfasis que pueden ser integradas entre sí. A continuación, se encuentra la descripción de cada arquitectura indicando la manera como se propone llevar a cabo la integración entre las mismas. Para esto se presenta la propuesta de integración especificando como llenar las plantillas y matrices del marco de trabajo.

FASE PRELIMINAR

1. Introducción

Contiene la descripción de los temas que se van a encontrar más adelante en el desarrollo del documento de arquitectura asociado a la empresa que tomo la decisión de diseñar una arquitectura empresarial

1.1. Descripción del negocio

En primer lugar, se debe realizar una pequeña descripción del negocio en palabras con el fin de familiarizarse con el negocio y entender a qué se dedica la empresa.

1.2. Vertical del negocio

Se debe identificar la vertical del negocio para ver en qué sector de la economía se desempeña.

Nombre de la vertical	Justificación
Sector al que pertenece	Descripción de la justificación

Tabla 1 Vertical de negocio

1.3. Misión y visión

En segundo lugar, se debe describir la misión y visión, de la empresa con el fin de describir la razón de ser la misma y cómo se ve en un horizonte de tiempo no superior a 5 (cinco) años, de manera que se puedan plantear en fases posteriores la estrategia del negocio alienada a esta misión y visión.

1.4. Cadena de valor

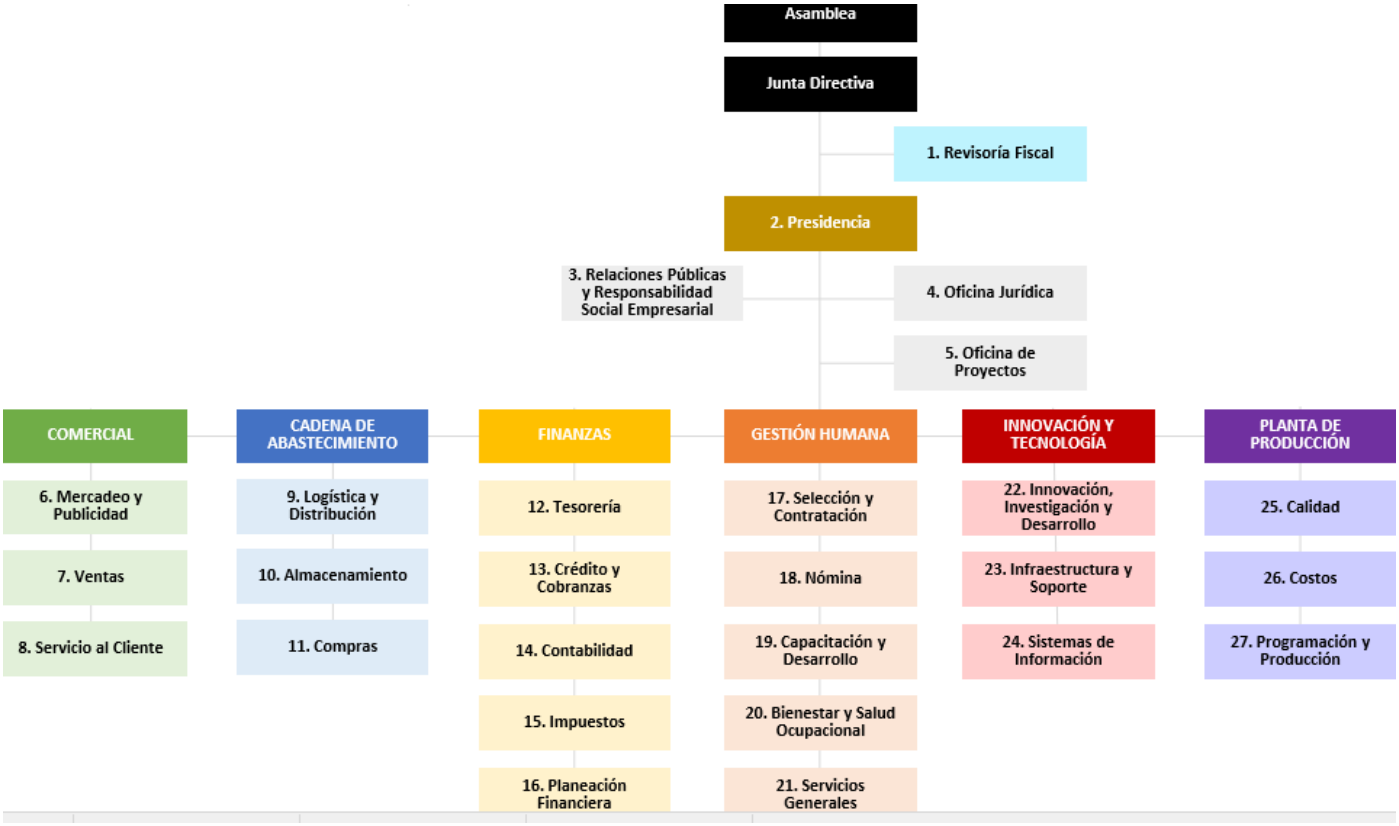
Para describir las actividades de la empresa se hace uso de la cadena de valor la cual permite describir la infraestructura, la gesrion de recursos humanos, su desarrollo tecnologico, su estructura

de compras, la logistica interna y externa, su opreacion, como realiza sus actividades de mercadeo y por último su interaccion con el cliente luego de la venta de sus productos y/o servicios. La cadena de valor tiene la sigiuente forma:

Ilustración 1 Diagrama de la cadena de valor

1.5. Organigrama de la empresa

Como complemento a la descripción de las actividades, es necesario incluir la estructura organizacional de la empresa, para esto se debe incluir el organigrama de la misma con todas sus dependencias. A continuación, se presenta un esquema de todas las dependencias que puede tener una empresa.



[22]

2. Organización del proyecto

En esta parte se describen los roles de las personas que harán parte del proyecto describiendo sus actividades y funciones.

2.1. Descripción de roles

Como complemento a la descripción de la estructura organizacional se debe realizar la descripción de los roles que están presentes en las dependencias de la empresa, para la cual se debe diligenciar la siguiente plantilla, que tiene el nombre y la función que desempeña dentro de la organización y/o proyecto:

Roles	Descripción

Tabla 2 y 3 Descripción de Roles y sus actividades

3. ESTRATEGIA DE LA ORGANIZACIÓN

En esta fase de la arquitectura se deben describir los objetivos estratégicos de la empresa, así como la estrategia para llegar al cumplimiento de los mismos, a continuación, se presenta los componentes de esta capa de la arquitectura.

3.1. Planes de continuidad de negocio (Business Continuity Plan)

Como inicio se empieza a trabajar en los planes de continuidad de negocio (Business continuity plan) describiendo la importancia del mismo muy brevemente con palabras. En este punto debe quedar reflejado la importancia que tienen los procesos de negocio, los recursos físicos y las personas. La metodología propuesta tiene un diseño Fast Track que incluye los siguientes componentes:

Personas: Describe la interacción de las personas con la empresa.

Infraestructura: describe los activos de la empresa para poder operar.

Planes: se definen luego de identificar posibles incidentes

Los planes de continuidad de negocio buscan analizar el entorno de la organización, analizar el entorno tecnológico y por último definir la estrategia de recuperación, estos componentes del plan se realizarán de manera alineada a las siguientes capas de la arquitectura.

3.2. Análisis DOFA

Continuando con el desarrollo de la arquitectura se hace uso de análisis DOFA para describir la estrategia de la organización, el cual hace un análisis interno y externo de la misma con base en las D: debilidades, O: oportunidades, F: fortalezas y A: amenazas presentes en su entorno y que tienen impacto en la organización, se debe hacer uso de la siguiente plantilla:

	Análisis DOFA
DEBILIDADES	
OPORTUNIDADES	
FORTALEZAS	
AMENAZAS	

Tabla 4 Análisis DOFA

3.3. Objetivo general y específicos

Como resultado del análisis DOFA, se pueden identificar los objetivos estratégicos de la empresa con base en las oportunidades y fortalezas que tiene, en caso de que no los tenga claros o no se hayan descrito anteriormente. Si la empresa ya tiene su estrategia definida son ellos quien deben suministrar estos objetivos y se pueden complementar con el resultado del análisis DOFA.

3.4. Objetivos estratégicos y BCP fase 1: Análisis del entorno organizacional

El siguiente formato permite documentar los objetivos de manera clara y con su respectivo indicador de cumplimiento:

Código Objetivo	Nombre Objetivo	Descripción del Objetivo	Indicador

Tabla 5 Objetivos Estratégicos

Con la plantilla diligenciada anteriormente también se completa la fase 1 del business continuity plan el cual tiene como propósito hacer un análisis del entorno organizacional.

3.5. Estrategia del negocio

Para representar la estrategia del negocio se hace uso de la siguiente plantilla que tiene una breve descripción de la estrategia y apunta que objetivo estratégico se puede cumplir con la estrategia:

Código Estrategia	Código Objetivo afectado	Descripción de la estrategia

Tabla 6 Estrategias de Negocio

4. Visión de la arquitectura

En la visión de la arquitectura se busca definir el alcance de la misma, es decir hasta donde va a llegar el proyecto, de igual manera busca describir los procesos de negocio de la compañía que dan soporte a su operación usando la siguiente plantilla por cada proceso de negocio:

Nombre	Gestión de Documentación
Referencia	
Descripción	

Tabla 7 Proceso de negocio 1

4.1. ISO 27001: Requisitos Sistema de Gestión de la Seguridad de la Información SGSI)

En este punto se deben definir los requisitos para el Sistema de Gestión de la Seguridad de la Información Estableciendo en principio el alcance del mismo para cada proceso de negocio, posteriormente se deben definir las políticas de la seguridad de la información dentro de la organización alineada a los activos de información presentes en la misma y en los procesos descritos anteriormente.

4.1.1. Alcance y objetivos

Se debe definir el alcance del SGSI para cada proceso de negocio con el fin de mitigar el riesgo al que están expuestos sus activos de información, así como el objetivo de la implantación del estándar en la organización.

4.1.2. Políticas de seguridad

La siguiente plantilla permite diligenciar las políticas de seguridad que se ajusten a las necesidades la empresa y su razón de ser, como se mencionó anteriormente, estas políticas deben estar alineadas a la preservación de los activos de información presentes en la compañía.

CODIGO POLITICA DE SEGURIDAD	DESCRIPCIÓN
PSI01… PS0N	

Tabla 9 Políticas de seguridad de la información

4.1.3. Leyes normas y regulaciones de la seguridad de la información

Se debe identificar la legislación de la seguridad de la información que aplique a la empresa para garantizar la protección de la misma, para esto se debe investigar como esta en materia de seguridad el país en el que se esté desarrollando la arquitectura y así poder aplicar esta normativa. El siguiente formato permite diligenciar el ente que emite la norma y los artículos que se apegan a la misma.

Norma	Artículos
Constitución política	- Art. 1 … - Art. N…

4.1.4. Metodología

Para hacer la evaluación del riesgo se deben listar todos los activos de información indicando el tipo (software, hardware) y su ubicación usando la siguiente plantilla:

Nombre del activo de información	Tipo de activo	Ubicación (Dispositivo / Servicio en Línea)

Tabla 10 Políticas de seguridad de la información

Cada activo de información deberá ser calificado en base los criterios de disponibilidad, integridad y confidencialidad con una puntuación de uno a 5 ponderada según las siguientes preguntas y con los siguientes criterios:

Puntaje	Criterio
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 de la SIC.
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.

Tabla 11 puntaje activos de información

DISPONIBLIDAD	PUNTAJE
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	
Impacto disponibilidad	Promedio puntaje

Tabla 12 Criterios de disponibilidad

INTEGRIDAD	PUNTAJE
El Activo es modificado parcialmente	
El Activo es modificado en su gran mayoría	
El Activo es modificado totalmente	
El Activo es eliminado	
Impacto integridad	Promedio puntaje

Tabla 13 Criterios de integridad

CONFIDENCIALIDAD	PUNTAJE
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	
Impacto Confidencialidad	Promedio puntaje

Tabla 14 Criterios de confidencialidad

4.1.5. Informe de análisis de riesgos

Luego de realizar la evaluación de los activos de información se recomienda hacer graficas de barras y de pasteles con el fin de hacer el análisis de riesgos que indicara las áreas y los activos más vulnerables para tratarlos cuanto antes con el fin de que los riesgos no se materialicen.

4.2. Principios de arquitectura

Por último, en esta fase de visión de la arquitectura, se deben especificar los principios de arquitectura (al menos dos para negocio, datos, aplicaciones y tecnología) usando la siguiente plantilla:

Nombre	
Referencia	
Descripción	
Razón	
Implicaciones	

Tabla 15 Criterios de confidencialidad

5. Arquitectura de negocio

La arquitectura de negocio busca describir el estado actual de los procesos de negocio de la compañía para definir una serie de iniciativas que definan una arquitectura objetivo.

5.1. Modelo de negocio

El modelo canvas es una herramienta que permite definir el modelo de negocio de la organización con base en los siguientes ítems:

- Socios (Key Partners): Aportan capital a la empresa, pueden ser inversionistas o estar involucrados en los procesos de negocio de la compañía.
- Actividades clave (Key Activities): Son aquellas actividades sin las que el negocio no puede funcionar, es decir si no está en esta lista el negocio no puede operar.

- Recursos clave (Key Resources): Son los recursos (hardware, software, personas) que la empresa necesita para realizar sus procesos de negocio.
- Propuesta de valor (Value Proposition): Es el diferenciador de la empresa frente a la competencia, se puede definir con la siguiente pregunta ¿Qué ofrece mi compañía que las demás no?
- Relación con el cliente (Customer Relationships): Busca definir la interacción que tengo con el cliente de manera que quede explicito como la empresa se comunica con él.
- Canales (chanels): Define la manera en que el producto o servicio es entregado a los clientes, es decir a través de que hago llegar mi producto y/o servicio.
- Segmento de clientes (Customer Segments): Es el pedacito de mercado al que quiero llegar, son los clientes potenciales de la empresa a los cuales voy a capturar para que consuman el producto y/o servicio.
- Estructura de costos (Cost Structure): Es el dinero que al empresa gasta para operar,dentro de ellos están los salarios de los empleados, servicios públicos, impuestos y cualquier otro costo derivado de la operación del negocio.
- Flujo de ingresos (Revenue Streams): Es la manera en la que la empresa recauda dinero, se deben incluir todas las fuentes de ingresos.

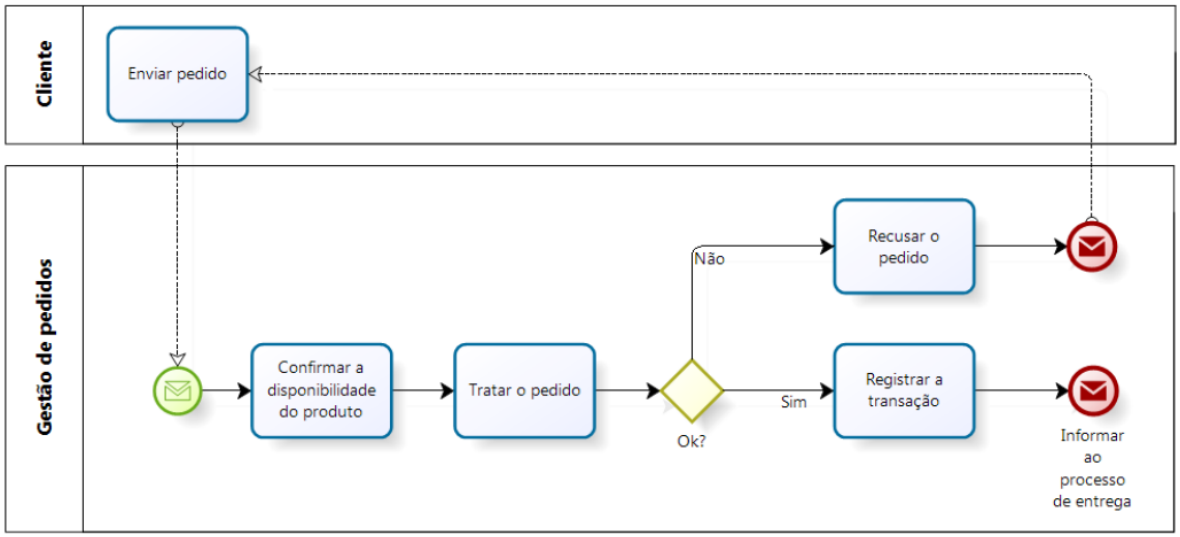
A continuación, se presenta la estructura del modelo canvas

[23]

5.2. Arquitectura AS-IS (Presente)

La arquitectura actual busca describir cómo están los procesos de negocio de la compañía, cómo y quién los lleva a cabo para esto se deben realizar los diagramas de procesos (BPMN). A continuación, se presenta un ejemplo de cómo es un diagrama de procesos

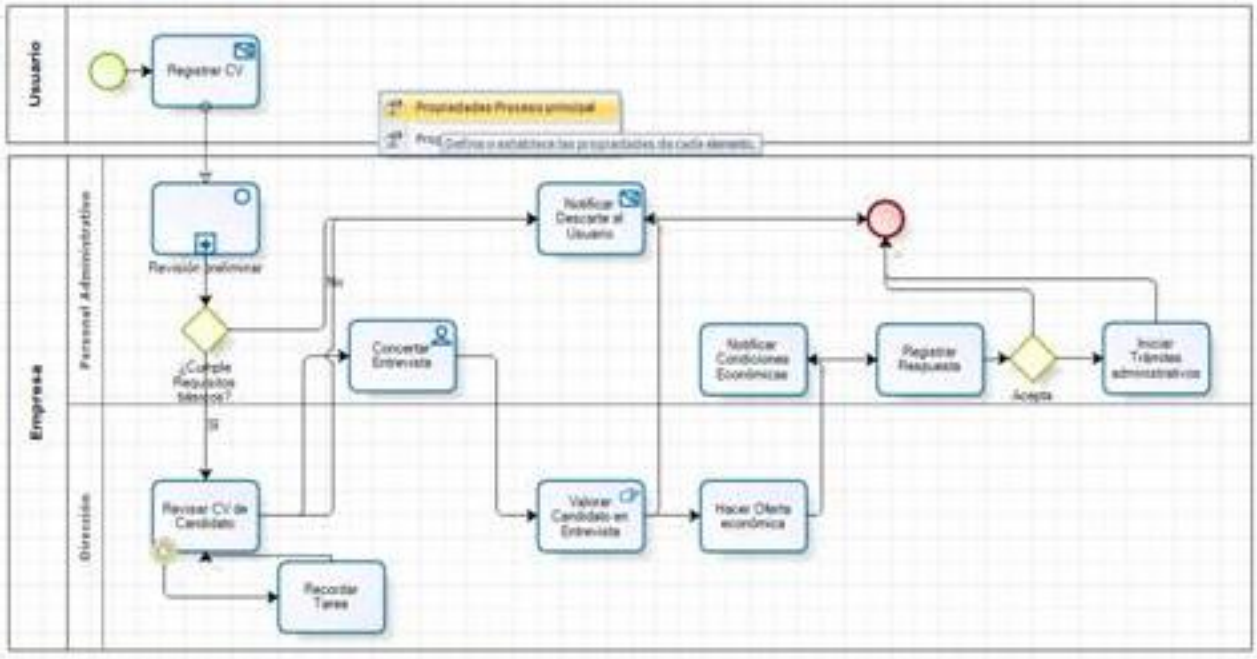
5.2.1. Proceso de negocio 1…N



5.3. Arquitectura TO-BE (Futura)

La arquitectura TO-BE describe como se deben realizar los procesos de negocio de manera más objetiva con el fin de aumentar la productividad del negocio, de la misma manera se deben hacer los diagramas de procesos (BPMN)

5.3.1. Proceso de negocio 1…N



5.4. BCP fase 1: Análisis del entrono organizacional

Relación de los objetivos estratégicos con los procesos de negocio

Busca identificar como procesos de negocios apalancan el cumplimiento de los objetivos estratégicos, de manera que se puedan identificar procesos críticos dentro de la compañía. La siguiente matriz permite detallar la relación de los objetivos y los procesos describiendo brevemente cómo interactúan, en caso de que no exista la relación se pone en la casilla no aplica:

Estrategia – procesos(AS-IS)			
	Proceso de negocio 1	**Proceso de negocio 2**	**Proceso de negocio N**
Objetivo estratégico 1	Relación del proceso con la meta	No aplica	No aplica
Objetivo estratégico 2	Relación del proceso con la meta	Relación del proceso con la meta	No aplica
Objetivo estratégico N	No aplica	Relación del proceso con la meta	No aplica

6. Arquitectura de datos

La arquitectura de datos tiene como objetivo identificar y analizar las entidades de información presentes en los procesos de negocio de la empresa con el fin de determinar su importancia clasificando el nivel de sensibilidad y el uso de la información que se maneja en la compañía.

6.1. Arquitectura AS-IS

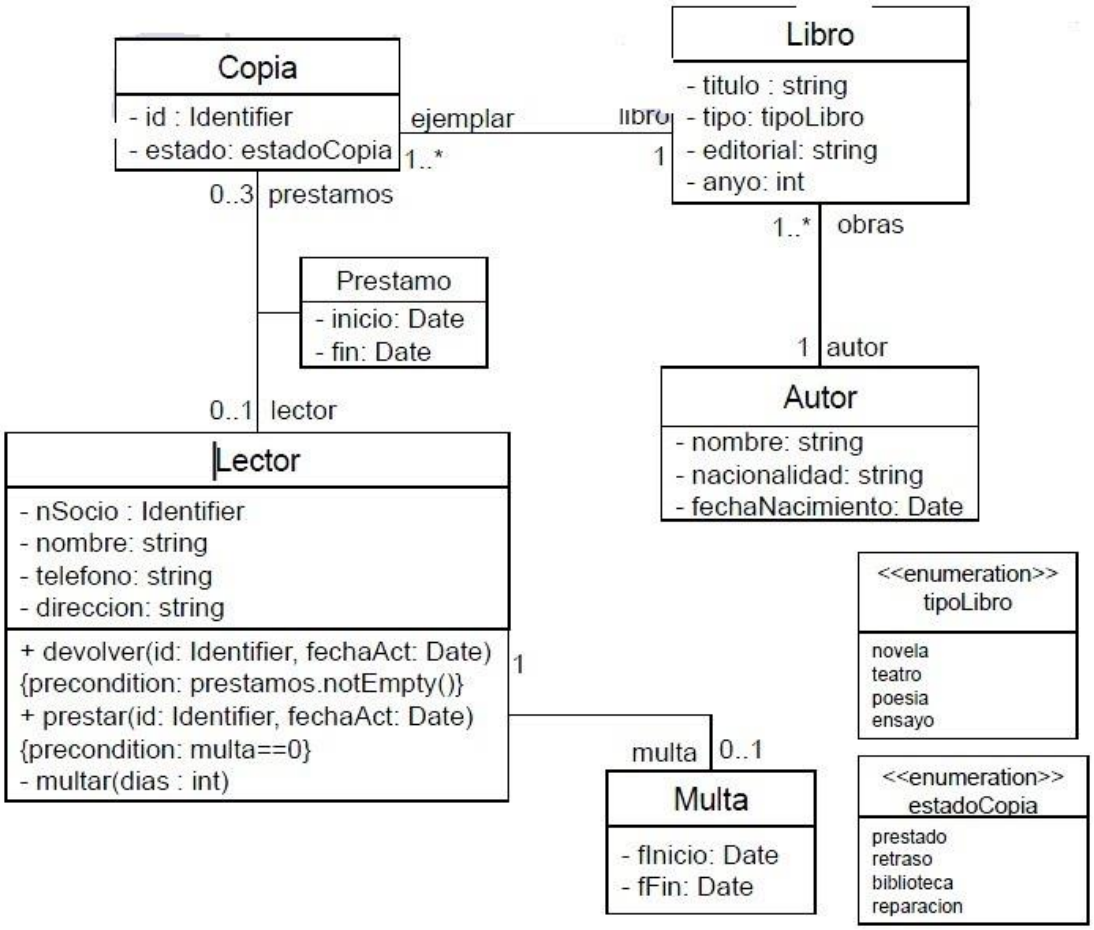
Por cada proceso de negocio se deben hacer los siguientes modelos y matrices

6.1.1. Proceso de negocio 1 …N

Modelo entidad relación

Permite identificar la relación entre las entidades de información presentes en el proceso, para esto primero de deben listar las entidades y hacer una breve descripción de las mismas con el siguiente formato:

Entidad	Descripción
Entidad 1 … N	

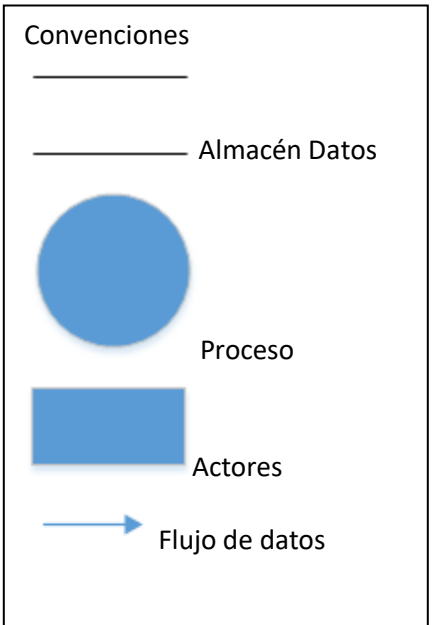


[24]

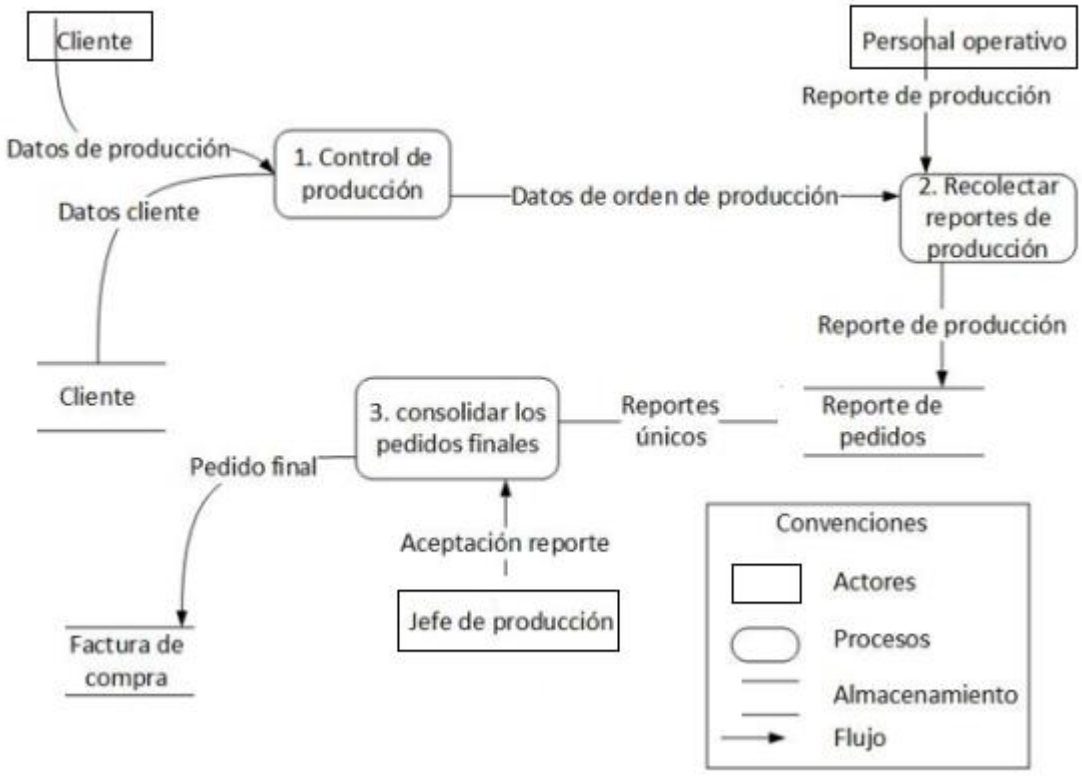
Diagrama de flujo de procesos

El diagrama de flujo de datos permite referenciar las entidades presentes en el proceso de negocio, así como el flujo de información que maneja cada entidad.

Convenciones



El diagrama presentado a continuación, es un ejemplo del flujo de información entre cada entidad y de cómo debe ser diligenciado



[25]

6.1.2. Matriz CRUD

Luego de definir las entidades de información se debe hacer un listado de todas, para identificar la participación que tiene en los procesos de negocios para eso se propone usar la matriz CRUD (c: crear, r: referenciar, u: actualizar, d: eliminar) que tiene la siguiente estructura en la cual en cada casilla vacía se debe indicar que tipo de acción lleva acabo la entidad de información que se está analizando:

PROCESOS DE NEGOCIO/ENTIDADES	PROCESO DE NEGOCIO 1	PROCESO DE NEGOCIO 2

Entidad 1		**No aplica**
Entidad 2		
Entidad N		

Tabla 16 Matriz CRUD

6.2. Arquitectura TO- BE

En la arquitectura futura se hace el mismo procedimiento, pero con los cambios que tienen los procesos de negocio establecidos en la arquitectura de negocio.

6.3. Evaluación de riesgo

Con el consolidado final de las entidades de información se procede a hacer la evaluación de riesgo de las que tienen un alto impacto según el análisis de riesgo realizado en la capa anterior. La evaluación se realiza con un archivo de Excel suministrado y se debe diligenciar de la siguiente manera:

Primero se deben listar los procesos de negocio con el siguiente formato:

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

Posteriormente se deben listar las entidades de información indicando el proceso de negocio al cual pertenecen, el propietario y la ubicación.

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

Para medir el nivel de sensibilidad de los activos se debe traer la información de la matriz de análisis de riesgo, la cual se diligencio anteriormente bajo los criterios de confiabilidad impacto y disponibilidad

	Sensibilidad de los activos					
Clasificación	Confidencialidad	Impacto	Disponibilidad	Total1	Valor1	Valor2
	Valor de 1.0 a 5.0	Valor de 1.0 a 5.0	Valor de 1.0 a 5.0	C+I+D	Alto	3
	Valor de 1.0 a 5.0	Valor de 1.0 a 5.0	Valor de 1.0 a 5.0	C+I+D	Medio	2

	Valor de 1.0 a 5.0	Valor de 1.0 a 5.0	Valor de 1.0 a 5.0	C+I+D	Bajo	1

El valor de la columna Total 1 es la suma de los valores de la confidencialidad, impacto disponibilidad de cada activo y esta formulado en el archivo .xls suministrado, de igual manera las columnas Valor 1 y Valor 2 están formuladas y pueden arrojar los valores alto, medio y bajo, y tiene los valores 3, 2 y 1 respectivamente que indican el valor de sensibilidad de los activos de manera gramatical y numérica.

Se debe hacer una descripción de lo impacto al negocio por cada activo según el siguiente criterio:

Valor	Descripción
1	**La brecha puede resultar en poca o nula pérdida o daño.**
2	**La brecha puede resultar en una pérdida o daño menor.**
3	**La brecha puede resultar en una pérdida o daño serio, y los procesos del negocio pueden verse afectados negativamente.**
4	**La brecha puede resultar en una pérdida o daño serio, y los procesos del negocio pueden fallar o interrumpirse.**
5	**La brecha puede resultar en altas pérdidas. Los procesos del negocio fallarán.**

Descripción de impactos al negocio

El siguiente paso consiste en listar las vulnerabilidades de cada activo y darle una puntación basada en los criterios de severidad y exposición, se debe diligenciar de la siguiente manera:

Criterios.

	Valor	
Severidad	1	Severidad Menor: Se requiere una cantidad significativa de recursos para explotar la vulnerabilidad y tiene poco potencial de pérdida o daño en el activo.
	2	Severidad Moderada: Se requiere una cantidad significativa de recursos para explotar la vulnerabilidad y tiene un potencial significativo de pérdida o daño en el activo; o se requieren

	3	pocos recursos para explotar la vulnerabilidad y tiene un potencial moderado de pérdida o daño en el activo. Severidad Alta: Se requieren pocos recursos para explotar la vulnerabilidad y tiene un potencial significativo de pérdida o daño en el activo.
Exposición	1	Exposición Menor: Los efectos de la vulnerabilidad son mínimos. No incrementa la probabilidad de que vulnerabilidades adicionales sean explotadas.
	2	Exposición Moderada: La vulnerabilidad puede afectar a más de un elemento o componente del sistema. La explotación de la vulnerabilidad aumenta la probabilidad de explotar vulnerabilidades adicionales.
	3	Exposición Alta: La vulnerabilidad afecta a la mayoría de los componentes del sistema. La explotación de la vulnerabilidad aumenta significativamente la probabilidad de explotar vulnerabilidades adicionales.

Análisis de vulnerabilidades

Igual que las vulnerabilidades las amenazas requieren un análisis y se realiza listando todos los eventos de cada amenaza para cada activo de información con su respectivo agente o persona que está en condición de realizarlo. A cada evento se le da una puntuación basada en los criterios de capacidad y motivación de la realización de la amenaza y se debe diligenciar de la siguiente manera:
Criterio

Análisis de vulnerabilidades			
Vulnerabilidad	Severidad	Exposición	Valor3
Vulnerabilidad 1 a N	1, 2 o 3	1, 2 o 3	S+E-1

Valor	Descripción

Capacidad	1	Poca o nula capacidad de realizar el ataque.
	2	Capacidad moderada. Se tiene el conocimiento y habilidades para realizar el ataque, pero pocos recursos. O, tiene suficientes recursos, pero conocimiento y habilidades limitadas.
	3	Altamente capaz. Se tienen los conocimientos, habilidades y recursos necesarios para realizar un ataque.
Motivación	1	Poca o nula motivación. No se está inclinado a actuar.
	2	Nivel moderado de motivación. Se actuará si se le pide o provoca.
	3	Altamente motivado. Casi seguro que intentará el ataque.

Análisis de amenazas

El siguiente paso consiste en determinar el nivel de riesgo residual, es decir la posibilidad de que las vulnerabilidades se conviertan en amenazas y las amenazas en riesgos latentes. La fórmula para calcular el riesgo es **Riesgo = Amenaza x Vulnerabilidad x Probabilidad x Impacto**, de la cual solo nos falta determinar la probabilidad de que el riesgo se materialice, la matriz se diligencia de la siguiente manera basado en el siguiente criterio:

Análisis de amenazas				
Agente	**Evento de amenaza**	**Capacidad**	**Motivación**	**Valor4**
Agente 1 …N	**Nombre evento 1…N**	**1, 2 o 3**	**1, 2 o 3**	**C+M-1**

	Valor	Descripción
Probabilidad	1	Baja, no hay historial y es raro que la amenaza ocurra.

	2	Media, se han presentado casos y puede ocurrir la amenaza.
	3	Alta, se han presentado suficientes casos y la amenaza seguramente ocurrirá.

Riesgo				
Amenaza	**Vulnerabilidad**	**Probabilidad**	**Impacto**	**Riesgo Total**
1 a 5	**1 a 5**	**1 a 3**		**A*V*O*I**

El valor de la amenaza es el valor4 traído de la tabla de análisis de amenazas, el valor de la vulnerabilidad es el valor 3 traído de la tabla de análisis de vulnerabilidades y el impacto el valor total1 y es traído de la tabla de clasificación de nivel de sensibilidad de los datos.

Si valor del riesgo total indica si la probabilidad de que se materialice el riesgo es alto bajo o medio y esta formulado en el archivo suministrado.

Finalmente se deben proponer controles para mitigar el riesgo al que están expuestos los activos de información, puntuándolo bajo los criterios de severidad y exposición.

Criterios

Descripción
Severidad Menor: Se requiere una cantidad significativa de recursos para explotar la vulnerabilidad y tiene poco potencial de pérdida o daño en el activo. **Severidad Moderada: Se requiere una cantidad significativa de recursos para explotar la vulnerabilidad y tiene un potencial significativo de pérdida o daño en el activo; o se requieren pocos recursos para explotar la vulnerabilidad y tiene un potencial moderado de pérdida o daño en el activo.** **Severidad Alta: Se requieren pocos recursos para explotar la vulnerabilidad y tiene un potencial significativo de pérdida o daño en el activo.**
Exposición Menor: Los efectos de la vulnerabilidad son mínimos. No incrementa la probabilidad de que vulnerabilidades adicionales sean explotadas.

Exposición Moderada: La vulnerabilidad puede afectar a más de un elemento o componente del sistema. La explotación de la vulnerabilidad aumenta la probabilidad de explotar vulnerabilidades adicionales. **Exposición Alta: La vulnerabilidad afecta a la mayoría de los componentes del sistema. La explotación de la vulnerabilidad aumenta significativamente la probabilidad de explotar vulnerabilidades adicionales.**

Valores severidad y exposición

Valor	Descripción
1	**Baja, no hay historial y es raro que la amenaza ocurra.**
2	**Media, se han presentado casos y puede ocurrir la amenaza.**
3	**Alta, se han presentado suficientes casos y la amenaza seguramente ocurrirá.**

Descripción del control	Severidad	Exposición	Valor
	1	**1**	**1**

Por último se debe realizar la administración de riesgos según el estándar ISO/IEC 27005 el cual indica que se debe reducir (reduction) retener (retention) evitar (avoidance) o transferir (transfer).

Administración de riesgos
Reducir, retener, evitar o transferir

Dentro de la evaluación de riesgo se debe realizar un mapa de riesgos en el cual se identifica el riesgo, se clasifica y se valora. El primer paso para realizar el mapa consiste en listar los riesgos identificados describiendo las causas y las consecuencias del mismo de la siguiente manera:

Identificación del riesgo			
Nº DE RIESGO	**RIESGO**	**CAUSAS**	**CONSECUENCIAS**
1…N			

ESCUELA COLOMBIANA DE INGENIERÍA JULIO GARAVITO

Para cada riesgo de debe determinar la probabilidad de ocurrencia, el impacto que tiene y con esta información se procede a calcular la evaluación y el nivel de riesgo inherente, el siguiente formato permite diligenciar y obtener esta información:

Calificación del riesgo			
PROBABILIDAD	**IMPACTO**	**EVALUACION DEL RIESGO**	**NIVEL DE RIESGO INHERENTE**
		P*I	

La probabilidad y el impacto se trae de la tabla de riesgos y el nivel de riesgo inherente se debe evaluar según el resultado de la evaluación de riesgo (impacto x probabilidad) y se clasifica de la siguiente manera:

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

Por último, se realiza la valoración del riesgo que consiste en listar los controles existentes para cada riesgo, se debe determinar su eficacia y puntuar la valoración del control para poder obtener el grado de exposición residual. El siguiente es el formato que se debe diligenciar:

Valoración del riesgo				
CONTROLES EXISTENTES	**EFICACIA CONTROL**	**VALORACION DEL CONTROL**	**GRADO DE EXPOSICION (RESIDUAL)**	**NIVEL DE RIESGO RESIDUAL**

La eficacia del control debe seguir los siguientes criterios:

EFICACIA DEL CONTROL

ALTO	**4**
MEDIO	**3**
BAJO	**2**
INEXISTENTE	**1**

La valoración del control debe seguir los siguientes criterios:

VALORACION CONTROL	
EXCELENTE	**5**
MEDIO	**4**
REGULAR	**3**
BAJO	**2**
NULO	**1**

El grado de exposición esta formulado en el archivo suministrado y es el resultado de dividir la evaluación del riesgo sobre la valoración del control. El nivel del riesgo residual se obtiene con los siguientes criterios:

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

6.3.1. Informe de evaluación de riesgo

Luego de realizar la evaluación de los activos de información se recomienda hacer graficas de barras y de pasteles con el fin de sacar conclusiones sobre la evaluación de riesgos que indicara las vulnerabilidades y los eventos de amenazas a los que se debe prestar más atención para que el riesgo no se materialice.

7. Arquitectura de aplicaciones

La arquitectura de aplicaciones hace uso de las entidades de información identificadas anteriormente mediante los sistemas de información y de más soluciones de software existentes en las organizaciones. Dentro del diseño de la arquitectura se debe realizar la gestión de información y de los usuarios, se debe realizar un inventario de aplicaciones, e indicar como almacenan su información, a continuación, se presenta la metodología para realizar el levantamiento de información mencionado.

7.1. Gestión de información

En este punto de la arquitectura se pretende identificar y definir los proveedores y consumidores de información que tiene la organización y que son parte fundamental en el ciclo de vida de los procesos del negocio puesto que su objetivo es realizar el procesamiento de la misma.

7.2. Definición de roles de usuario

La definición de roles de usuario consiste en identificar todas las personas que hacen uso de los sistemas de información de la organización con su respectivo cargo, para esto se debe diligenciar la siguiente plantilla la cual permite el registro de los roles con las funciones que tienen dentro del sistema.

Roles	
Nombre	**Funciones**
Rol de usuario	• Descripción función 1. • Descripción función N.

7.3. Proveedores de información

Los proveedores son parte importante de los sistemas de información puesto que son su materia prima, es importante definir quienes suministran información a las organizaciones y la siguiente matriz permite diligenciar esta información:

Proveedores

Nombre	Información
Proveedor 1… N	Descripción de la información que proporciona

7.4. Consumidores de información

Se deben describir los consumidores de la información que sale de los sistemas de información y de la empresa. La siguiente plantilla permite diligenciar esta información:

Consumidores	
Nombre	**Información**
Consumidor 1… N	Descripción de la información que consume

7.5. Arquitectura AS-IS

La arquitectura actual describe las aplicaciones con las que cuenta la empresa actualmente, los siguientes ítems ilustran la manera en que los sistemas de información interactúan con la organización.

7.5.1. Inventario de aplicaciones

Las aplicaciones con las que cuenta la organización deben ser inventariadas con la siguiente matriz:

Aplicaciones	
Nombre	**Descripción**
App 1	Descripción del funcionamiento de la aplicación

Tabla 17 Inventario aplicaciones

7.5.2. Matriz levantamiento de información de aplicaciones/datos

Posteriormente se debe indicar la manera en la que la aplicación almacena la información (física o software mediante la siguiente plantilla:

Aplicación – Almacenamiento (AS-IS)		
	Almacenamiento en Software	Almacenamiento Físico
App1	Registro almacenando en BD	No aplica

Tabla 18 almacenamiento aplicaciones

7.5.3. BCP fase 1: análisis del entorno organizacional y Matriz levantamiento de información aplicaciones/procesos de negocio

Relación de los procesos de negocio con los sistemas de información

Es importante definir como los procesos de negocio están soportados con los sistemas de información y demás aplicativos de la organización, con el fin de identificar dependencias de procesos y sistemas de manera de que si aplicativo deja de funcionar se puedan definir acciones correctivas para que el proceso no se detenga e incurran en pérdidas económicas a la organización.

La siguiente matriz permite diligenciar esta información e identificar estas dependencias:

Aplicación – Negocio (AS-IS)		
	Ventas	Producción
App 1	Descripción	descripción

7.6. Arquitectura TO-BE

La arquitectura futura tiene la misma estructura, pero tiene los cambios que tiene la organización con los sistemas de información y demás aplicativos propuestos que deben estar alineados a los cambios en la arquitectura de procesos futura todo en busca de aumentar la productividad del negocio.

8. Arquitectura de tecnología

La arquitectura de tecnología define la estructura de hardware, software y redes necesarios para la implementación de las aplicaciones que dan soporte a los procesos de negocio, pero no se establecen unos parámetros como lo son las reglas de seguridad, prácticas y procedimientos en el manejo de estas tecnologías como mecanismos de seguridad se permite la implementación de herramientas de monitoreo las cuales se clasifican de la siguiente manera:

- Herramientas de monitoreo: analizan la confiabilidad de un sistema ofreciendo un grado mínimo de seguridad en la red. Entre ellas tenemos a SATAN, que busca y genera automáticamente reportes acerca de las vulnerabilidades de una red,

- Herramientas de seguridad: Modifican los parámetros de un sistema con el fin de asegurarlo contra diversos ataques, entre los más comunes están los Firewalls (filtrar tráfico de información entre 2 redes), la criptografía que busca codificar los mensajes apara que no puedan ser interceptados por personas ajenas a ellos y Kerberos que está diseñado para procesos de autenticación permitiendo enviar su identificación a otros a través de redes de segura a través de un servidor de red seguro haciendo uso de la inscripción.

Esta es una medida que mitiga los ataques informáticos a los activos de información, y permite identificar amenazas y vulnerabilidades para que sean tratadas de manera adecuada.

8.1. BCP Fase 2: Análisis del entorno tecnológico

La fase 2 hace el cruce de información entre las plataformas tecnológicas y los sistemas de información, permitiendo definir escenarios de falla y acciones correctivas para los mismos, los siguientes ítems de la arquitectura tecnológica permiten identificar los componentes necesarios para soportar la operación de las aplicaciones y al mismo tiempo llevar a cabo la fase 2 del BCP

8.1.1. Definición escenarios de falla

Definir escenarios de falla 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. Se debe diligenciar la siguiente matriz indicando el activo que puede presentar la falla, el escenario (falla) y la descripción del escenario.

Código	Activo	Escenario	Descripción
EF01	Computador	Falla técnica	Falla de un componente físico que impida su correcto funcionamiento

8.1.2. Implementación de acciones correctivas

Las acciones correctivas son aquellas que se llevan a cabo para disminuir el impacto de un suceso que afecte la continuidad del negocio, a continuación, se presenta una tabla en la cual se deben diligenciar las acciones correctivas para de mitigar el riego de falla en los activos de la compañía.

Código	Nombre	Descripción
AC01	Aseguramiento del Harware	Adecuar las estaciones de trabajo de manera que cuando se presente un temblor o un incidente de fuerza mayor los equipos de cómputo y de más implementos físicos estén protegidos

8.2. Arquitectura AS – IS

La arquitectura actual describe los componentes que posee la empresa, se debe realizar un inventario de los mismos y describir su entorno. Los ítems siguientes permiten registrar y analizar esta información.

8.2.1. Continuación BCP Fase 2: matriz entorno de tecnología

En la matriz se describe el entorno y la tecnología con la que cuenta la empresa indicando el proceso de negocio en el que participa (ambiente) las aplicaciones y demás componentes tecnológicos necesarios para su correcto funcionamiento. La siguiente matriz permite diligenciar esta información:

Código	Ambiente	Localización	Componentes de aplicación	Componentes de tecnología

MT01	1. Proceso de negocio 1. 2. Proceso de negocio N	Calle 1 # 123	Software contable CRM	- Base de datos Oracle para en la cual se almacenan los documentos. - 1 equipo de cómputo.

8.2.2. Matriz componentes de red

Se deben identificar todas las redes y componentes de red presentes en la empresa y que están presentes en los procesos de negocio indicando si tienen un control de acceso y los requerimientos de banda ancha. La siguiente matriz permite diligenciar la información mencionada anteriormente:

Código	Plataforma tecnológica	Unidad de despliegue	Requerimientos de banda ancha	Control de acceso	Observaciones
MR01	Proceso de negocio 1, Proceso de negocio N	Servidor Internet Modem Etc.	10 MB	Password	Actualmente la empresa cuenta con un servidor interno que como función…

8.2.3. continuación BCP fase 2 e inventario de componentes de tecnología

Se deben listar los activos tecnológicos de la empresa con su descripción el tipo de activo (Sotfware, Hardware), el proveedor o marca la capacidad que tiene en gigabytes y los procesos de negocio en los que participa, para lo cual se tienen las siguientes convenciones:

Código	Descripción
PN01 … PN0N	Descripción del proceso de negocio

Luego se debe diligenciar la siguiente matriz con las especificaciones mencionadas anteriormente:

Código	Nombre	Descripción	Tipo de componente(SW, HW o servicio)	Proveedor	Fin del soporte	Capacidad total (GB)	Proceso que soporta
INTI1	Internet, computador	Provee a la empresa conexión a la	Servicio	ETB	A fin de cada mes	ilimitado	-PN01 -PN02 -PN03

	, modem, impresora	red de internet por 20 Mbps					

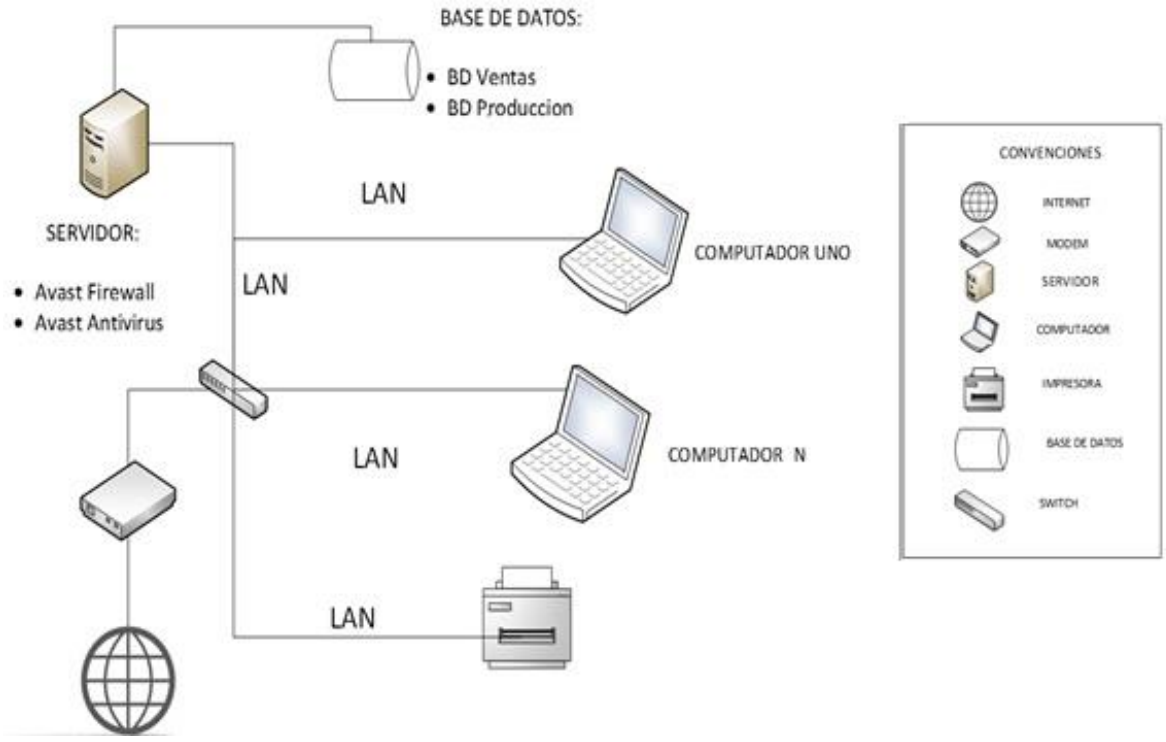
8.3. Arquitectura TO-BE

La arquitectura futura tiene la misma estructura, pero al igual que todas las arquitecturas futuras, se deben incluir los nuevos componentes tecnológicos para soportar las aplicaciones propuestas en la arquitectura de aplicaciones TO-BE.

8.4. Marco de referencia Físico

Es un modelo que ilustra de manera gráfica los componentes tecnológicos de la organización. para realizarlo se pueden usar la herramienta Microsoft Visio o cualquier otra que permita realizar el grafico.

Ejemplo marco de referencia:



Al final de todas las arquitecturas se debe realiza el análisis GAP que básicamente consiste en describir el cambio que tiene la organización con la propuesta de arquitectura objetivo. Tiene la siguiente estructura:

Código	PROCESO	AS- IS	TO- BE	PROGRAMAS DERIVADOS	OBJETIVO ESTRATEGICO
1	Proceso1	Sin sistema de información	Con sistema de información		

Tabla 20 análisis GAP Arquitecturas

De los programas derivados surgen las iniciativas que hacen parte del portafolio de proyectos resultante de la arquitectura, deben ser descritas y tener una prioridad para poder ser ejecutadas de manera correcta. Deben ser documentadas de la siguiente manera:

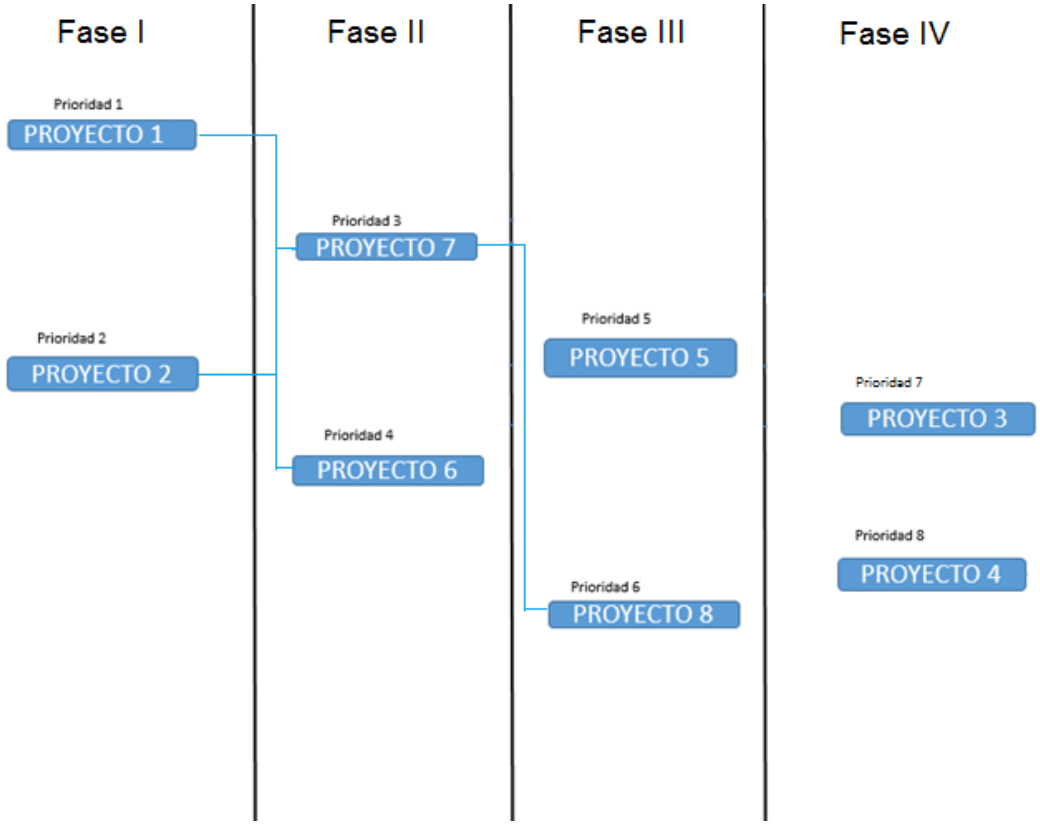
Código Iniciativa	Nombre Iniciativa	Descripción de Iniciativa	Prioridad	Código Objetivo Estratégico	Código GAP
IN1			1,2,3,..,N		

Como resultado del ejercicio obtenemos un portafolio de proyectos que nace de las iniciativas de cada arquitectura, para esto se deben listar los proyectos para alcanzar la arquitectura objetivo dándoles una prioridad de ejecución, la siguiente tabla permite listar los proyectos indicando de que capa de la arquitectura pertenecen, la descripción del gap que están cubriendo y el conjunto de actividades genéricas que son necesarias para realizar el proyecto, por último la prioridad que tiene según las necesidades de la organización.

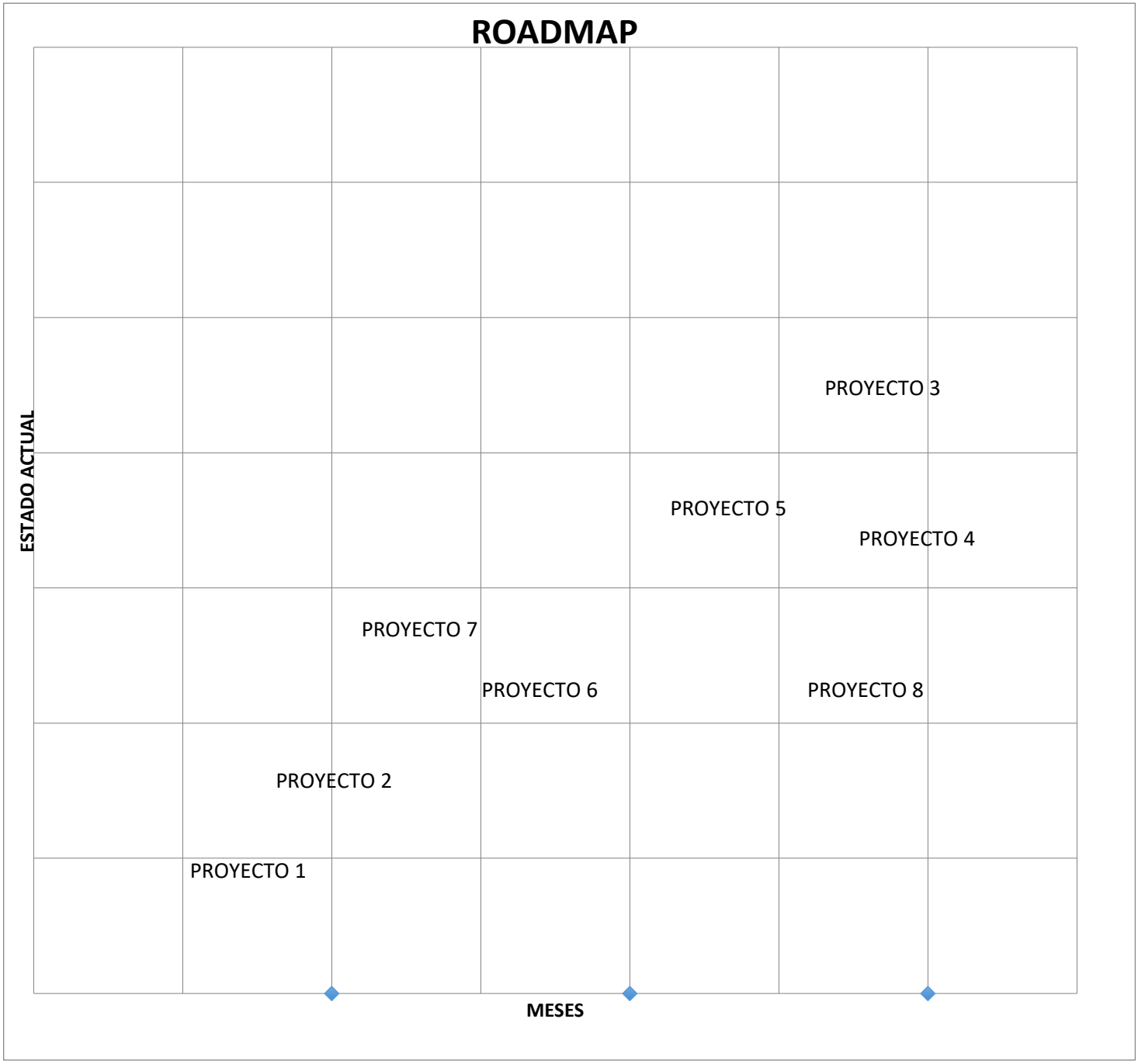
NO.	ARQUITECTURA	GAP	SOLUCIONES POTENCIALES	Prioridad
1	Negocio, datos, aplicación o tecnología	Descripción de la brecha que están cubriendo, ej: adquisición de un software contable	Actividades para realizar este proyecto	1…N

Para ilustrar gráficamente se debe realizar el Roadmap, también conocido como hoja de ruta donde se indica cómo se van a realizar los proyectos en el tiempo, acompañado de un diagrama por fases. Ambos tienen la siguiente estructura:

ESCUELA COLOMBIANA DE INGENIERÍA JULIO GARAVITO



Con la priorización de los proyectos se definen las fases de ejecución de los proyectos, queda por realizar que algunos proyectos dependen directamente de otros para su desarrollo, las líneas azules indican esa dependencia.

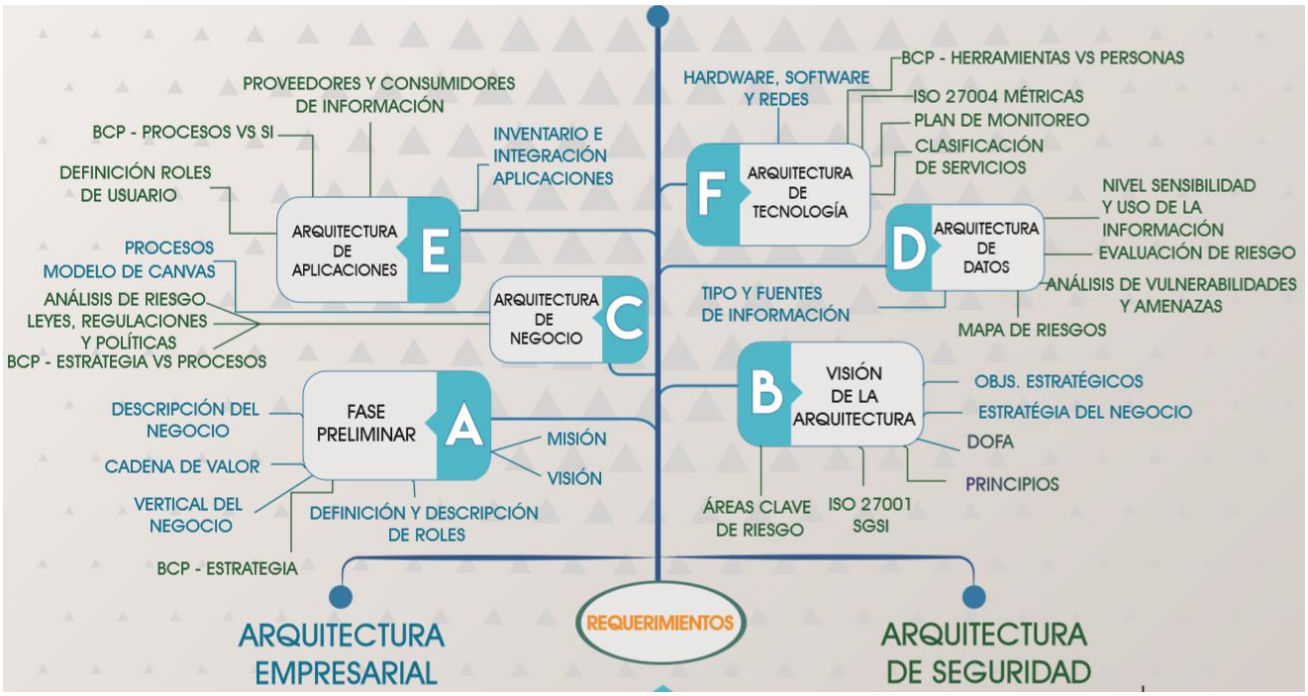


La estructura del roadmap tiene en el eje horizontal el tiempo de ejecución de los proyectos y en el eje vertical el estado actual con el fin de ilustrar las necesidades del negocio y los cambios que va teniendo para aumentar su productividad.

Con la integración de los marcos de trabajo de TOGAF la organización caso de estudio puede tomar la decisión de implementar la propuesta luego de realizar la documentación de la integración de

ambas arquitecturas, tendrá como beneficios el alineamiento holístico de sus procesos de negocio y recursos TI con la estrategia planteada en la arquitectura empresarial minimizando sus costos de operación y recuperando el retorno a la inversión (ROI) según los proyectos que surjan luego de la propuesta de arquitectura objetivo generando un plus frente a sus competidores, con el agregado del sistema de gestión de riesgos, de manera que la información que maneja cumplirá con estándares que mitigan las vulnerabilidades a las que está expuesta.

A continuación, se presenta el esquema de la propuesta de integración con todos sus componentes



4. Conclusiones y trabajo Final

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 quedan corta en un plazo de tiempo menor que el esperado.

El término arquitectura empresarial en las PYMES es desconocido, aunque con el paso del tiempo ha cogido fuerza por los beneficios que trae la implementación y definición de una arquitectura. Con

el manual suministrado las empresas podrán construir su arquitectura y al final hacer un análisis del dinero que dejan de ganar con su modelo de negocio actual de manera que puedan tomar una decisión de lanzar un proyecto de implementación el cual les generara un nuevo modelo de negocio enfocado a la optimización de sus procesos negocio basado en las tecnologías de la información y comunicación garantizando la seguridad de la de sus activos y personas y finalmente obteniendo la ventaja competitiva que han estado buscando.

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] A. Molano, "colombiadigital.net," 27 Enereo 2015. [Online]. Available: http://www.colombiadigital.net/actualidad/articulos-informativos/item/8123-que-es-arquitectura-empresarial.html. [Accessed 2016 Julio 09].

[2] A. d. C. D. d. g. d. p. A. Colombia, "colombiadigital.net," 27 enero 2015. [Online]. Available: http://www.colombiadigital.net/actualidad/articulos-informativos/item/8123-que-es-arquitectura-empresarial.html. [Accessed 2016 Junio 12].

[3] J. l. r. ayala, "docplayers.es," septiembre 2015. [Online]. Available: http://docplayer.es/2551429-La-arquitectura-empresarial-comenzo-inicialmente-para-hacer-frente-a-dos-problemas.html. [Accessed 5 Junio 2015].

[4] A. Monnappa, "simplilearn.com," 11 Diciembre 2015. [Online]. Available: http://www.simplilearn.com/how-to-successfully-plan-enterprise-architecture-article. [Accessed 10 Junio 2016].

[5] G. M, "prezi.com," 17 Junio 2014. [Online]. Available: https://prezi.com/2lputchj3lgt/marco-de-trabajo-zachman/. [Accessed 20 Junio 2016].

[6] "liteea.com," 2 Enero 2014. [Online]. Available: http://www.liteea.com/wordpress/eaframework/zachman-wu-xing/. [Accessed 16 Junio 2016].

[7] E. Architect, "sparxsystems.com.ar," [Online]. Available: http://www.sparxsystems.com.ar/download/Ayuda%20HTML%20EA%207.5/index.html?swimlanes_matrix.htm. [Accessed 11 Julio 2016].

[8] C. Collins, "ccollins.wordpress.com," 16 Febrero 2008. [Online]. Available: https://ccollins.wordpress.com/2008/02/16/introduction-to-the-zachman-framework/. [Accessed 11 Julio 2016].

[9] U. N. A. d. México, "redyseguridad.fi-p.unam.mx," [Online]. Available: http://redyseguridad.fi-p.unam.mx/proyectos/seguridad/EntornoPerfiles.php. [Accessed 19 Junio 2016].

[10] "cataria.udlap.mx," [Online]. Available: http://catarina.udlap.mx/u_dl_a/tales/documentos/lis/argueta_a_a/capitulo2.pdf. [Accessed 21 junio 2016].

[11] TOGAF, "pubs.opengroup.org," Noviembre 2005. [Online]. Available: http://pubs.opengroup.org/architecture/togaf9-doc/arch/chap21.html#tag_21_01. [Accessed 24 junio 2016].

[12] The Open Group Security Forum and , "http://pubs.opengroup.org/," Noviembre 2005. [Online]. Available: http://pubs.opengroup.org/onlinepubs/7699949499/toc.pdf. [Accessed 25 Junio 2016].

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

[14] handdrawnea, "handdrawnea.com," [Online]. Available: http://www.handdrawnea.com/SupportSystems/Security.html. [Accessed 29 Junio 2016].

[15] vanharen, "vanharen.net/," 22 Agosto 2013. [Online]. Available: http://www.vanharen.net/blog/enterprise-architecture/sabsa-in-3-minutes/. [Accessed 28 Junio 2016].

[16] OSA, "opensecurityarchitecture.org," [Online]. Available: http://www.opensecurityarchitecture.org/cms/definitions/it-architecture. [Accessed 29 Junio 2016].

[17] OSA, "opensecurityarchitecture.org," [Online]. Available: http://www.opensecurityarchitecture.org/cms/definitions/it-security-architecture. [Accessed 29 Junio 2016].

[18] OSA, "opensecurityarchitecture.org," [Online]. Available: http://www.opensecurityarchitecture.org/cms/foundations/osa-taxonomy. [Accessed 29 Junio 2016].

[19] NIST, "nvlpubs.nist.gov," Abril 2014. [Online]. Available: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf. [Accessed 29 Junio 2016].

[20] International Organization for Standarization, "www.iso27000.es," [Online]. Available: http://www.iso27000.es/download/doc_iso27000_all.pdf. [Accessed 4 Junio 2016].

[21] Otton consulting, "ottonconsulting.com," [Online]. Available: http://ottonconsulting.com/316-iso_27001.htm. [Accessed 2 Junio 2016].

[22] M. Martínez, "Estructura organizacional 2016," Bogotá, 2016.

[23] blogthingbig, "9 pasos para que tu negocio sea un exito a traves del modelo canvas," 4 septiembre 2013. [Online]. Available: http://blogthinkbig.com/modelo-canvas-9-pasos-exito-negocio/. [Accessed 30 Agosto 2016].

[24] J. Alguero, "Herramienta case o modelado - jossey alguero," 10 Octubre 2015. [Online]. Available: http://gruponextdiagramauml.blogspot.com.co/. [Accessed 31 Agosto 2016].

[25] F. D. Palacios, "Flujo de datos - produccion," Bogota, 2016.

[26] Espineria, Sheldon y asociados, "boletín de asesoría gerencial," 2008. [Online]. Available: http://www.pwc.com/ve/es/asesoria-gerencial/boletin/assets/boletin-advisory-edicion-09-2008.pdf. [Accessed Octube 2016].

[27] P. d. l. República, "http://es.presidencia.gov.co/," Diciembre 2014. [Online]. Available: http://es.presidencia.gov.co/dapre/DocumentosSIGEPRE/M-TI-01-Manual-Sistema-Seguridad-Informacion.pdf. [Accessed 1 Agosto 2016].