UNIVERSIDAD TÉCNICA PARTICULAR DE LOJA

La Universidad Católica de Loja

ÁREA TÉCNICA

TITULACIÓN DE INGENIERO EN SISTEMAS INFORMÁTICOS Y COMPUTACIÓN

Guía de ciberseguridad para arquitectura empresarial

TRABAJO DE FIN DE TITULACIÓN

AUTOR: Torres Villalta, Alfredo David

DIRECTOR: Jaramillo Hurtado, Danilo Rubén, Ing

LOJA – ECUADOR

2015

APROBACIÓN DEL DIRECTOR DEL TRABAJO DE FIN DE TITULACIÓN

Ingeniero.

Danilo Rubén Jaramillo Hurtado

DOCENTE DE LA TITULACIÓN

De mi consideración:

El presente trabajo de fin de titulación: *Guía de ciberseguridad para arquitectura empresarial* realizado por *Alfredo David Torres Villalta,* ha sido orientado y revisado durante su ejecución, por cuanto se aprueba la presentación del mismo.

Loja, abril de 2015

f) …..…….
Jaramillo Hurtado Danilo Rubén
1102917240

DECLARACIÓN DE AUTORÍA Y CESIÓN DE DERECHOS

Yo, *Alfredo David Torres Villalta* declaro ser autor del presente trabajo de fin de titulación: *Guía de ciberseguridad para arquitectura empresarial*, de la titulación de *Ingeniero en Sistemas Informáticos y Computacion*, siendo Danilo Ruben Jaramillo Hurtado director del presente trabajo; y eximo expresamente a la Universidad Técnica Particular de Loja y a sus representantes legales de posibles reclamos o acciones legales. Ademas certifico que las ideas, conceptos, procedimientos y resultados vertidos en el presente trabajo investigativo, son de mi exclusiva responsabilidad.

Adicionalmente declaro conocer y aceptar la disposición del Art. 88 del Estatuto Orgánico de la Universidad Técnica Particular de Loja que en su parte pertinente textualmente dice: "Forman parte del patrimonio de la Universidad la propiedad intelectual de investigaciones, trabajos científicos o técnicos y tesis de grado o trabajos de titulación que se realicen con el apoyo financiero, académico o institucional (operativo) de la Universidad"

f. …….
Alfredo David Torres Villalta
0705184604

DEDICATORIA

A Dios por permitirme alcanzar esta meta tan importante y darme la fortaleza para continuar día a día, mis padres Alfredo y Mary por ser el pilar de mi vida, darme su amor y apoyo incondicional, a mi familia y mi Pao por estar a mi lado en todo momento incentivándome para cumplir con mis objetivos, a mi querida hija Samantha que llego a mi vida para darme una razón más para seguir adelante, sin olvidar a mis amigos con quienes he compartido ideales y grandes momentos, junto a experiencias enriquecedoras tanto en lo profesional y personal.

AGRADECIMIENTO

Quisiera expresar mi mas sincero agradecimiento a Dios por permitirme culminar con este proyecto, a mis padres, hermanos, familia, amigos y de manera muy especial al Ing. Danilo Jaramillo por su guía a través del desarrollo de este trabajo, sobre todo por su apoyo, experiencia y paciencia para culminar con el mismo, de igual manera quisiera agradecer aquellos docentes de nuestra universidad que me impartieron sus conocimientos para formarme en el camino de la profesionalización.

ÍNDICE DE CONTENIDOS

RESUMEN

La ciberseguridad dentro de sus enfoques trata principalmente el cuidado y protección de la confidencialidad, integridad y disponibilidad de los sistemas de información, que implementada sobre una arquitectura empresarial (AE), ayuda a tener una visión general de los componentes que se deben fortalecer y priorizar.

La presente guía propone un conjunto de actividades agrupadas por cada fase del ADM (método de desarrollo de arquitectura) del marco de trabajo de TOGAF, que se especializa en la construcción y mantenimiento de AE, donde intervienen los principios de AE: arquitectura de negocio, arquitectura de datos, arquitectura de aplicaciones, y arquitectura tecnológica.

En cada fase de la guía intervienen actividades que proporcionan la información necesaria para su ejecución, junto a normas y marcos de trabajo como: ISO 27001, ISO 27032, COBIT 5 (Transformando la ciberseguridad usando COBIT 5) y NIST (Marco de trabajo para mejorar la ciberseguridad de infraestructuras críticas), y un grupo de plantillas por cada actividad para el levantamiento de información.

La guía se complementa con una aplicación web, que valida la implementación de actividades de ciberseguridad dentro de un ambiente empresarial.

Palabras claves: Ciberseguridad, Arquitectura Empresarial, TOGAF, SABSA

ABSTRACT

Cybersecurity within their approaches are mainly the care and protection of the confidentiality, integrity and availability of information systems that implemented on an enterprise architecture (EA), it helps to have an overview of the components to strengthen and prioritize .

This guide proposes a set of grouped for each phase of ADM (architecture domain model) the framework of TOGAF, specializing in the construction and maintenance of AE, where AE principles involved activities: business architecture, architecture data, application architecture, and technology architecture.

At each stage of the guide involved activities that provide the information necessary for execution, along with standards and frameworks such as ISO 27001, ISO 27032, COBIT 5 (Transforming cybersecurity using COBIT 5) and NIST (Framework for improving critical infrastructure cyber security), and a set of templates for each activity to the collection of information.

The guide is complimented by a web application, which validates the implementation of cybersecurity activities within a business environment.

KEYWORDS: Cybersecurity, Enterprise Architecture, TOGAF, SABSA

PALABRAS CLAVE

TOGAF:	The Open Group Architecture Framework
ADM:	Architecture Development Method (Metodo de desarrollo de arquitectura)
Zachaman Framework:	Marco de Trabajo Zachman
COBIT:	Control Objectives for Information and related Technology (Objetivos de Control para Información y Tecnologías Relacionadas)
ISO:	International Organization for Standardization (Organización Internacional de Normalización)
NIST:	National Institute of Standards and Technology (Instituto Nacional de Estándares y Tecnología)
COIP:	Codigo Orgánico Integral Penal
SABSA:	Sherwood Applied Business Security Architecture
AE:	Arquitectura Empresarial
CS:	Ciberseguridad
RM:	Requirements Management (Gestion de requerimientos)
PP:	Preliminar Phase (Fase preliminar)
AV:	Architecture Vision (Vision de arquitectura)
BA:	Business Architecture (Arquitectura del negocio)
ISA:	Information Systems Architectures (Arquitectura de sistemas de información)
TA:	Technology Architecture (Arquitectura tecnológica)
OS:	Opportunities and Solutions (Oportunidades y soluciones)
MP:	Migration Planning (Planificación de migración)
IG:	Implementation Governance (gobierno de la implementacion)
ACM:	Architecture Change Management (Gestión de cambios de la arquitectura)
BAPCS:	Atributos del perfil de Negocio para Ciberseguridad
SICSAE:	Sistema para validación de ciberseguridad en arquitectura empresarial

INTRODUCCIÓN

El ambiente empresarial, va cambiando conforme se adoptan nuevas tecnologías, donde se presentan oportunidades que las organizaciones deben aprovechar para alinear su estrategia y objetivos de negocio con tecnología de la información (TI), y servicios externos para almacenamiento, alojamiento y/o procesamiento, un claro ejemplo es la nube, en la cual se ha visto un incremento considerable de su uso, según Eset (Equipo de Investigación de ESET Latinoamérica, 2014) se espera que para el año 2016, un 36% de la información de los usuarios finales este almacenada en la nube, a partir de todos estos cambios que envuelve a las organizacioness, nace la necesidad de implementar procedimientos y controles, utilizando distintas normas y marcos de trabajo, para minimizar el riesgo de pérdida de información y caída de servicios críticos para las organizaciones.

Normalmente se invierten fuertes cantidades de dinero en tecnología con el objetivo de proporcionar mayor seguridad a los sistemas de información (SI)[1] sin un previo análisis de las necesidades reales, o también se puede dar el caso contrario, en donde no se mide eficazmente la criticidad de los SI y la seguridad que los mismo necesitan.

La ciberseguridad debe ser una de las partes fundamentales dentro del funcionamiento de una organización, donde se aproveche las capacidades ofrecidas por una arquitectura empresarial (AE) implementada formalmente, en donde altos directivos establezcan un compromiso colaborativo, para incluir y valorar muchas de las decisiones que se tomen, y así evitar riesgos potenciales que afecten a la ciberseguridad dentro de la organización que causen pérdidas económicas y de imagen.

La presente guía, tiene como principal objetivo orientar a través de una serie de actividades, en la aplicación de ciberseguridad para AE, esta guía está desarrollada en base a marcos de trabajo y normas que apoyan cada uno de los aspectos relacionados con AE y ciberseguridad, las misma está dividida de acuerdo a los cuatro principios de AE: arquitectura de negocio, arquitectura de información, arquitectura de aplicaciones y arquitectura tecnológica; a partir de estos cuatro principios se ha establecido una serie de actividades que deberán ser considerados de acuerdo a las necesidades requeridas por una organización.

[1] Sistemas de Información (SI): es un conjunto discreto de recursos de información organizada para la recolección, procesamiento, mantenimiento, uso, distribución, difusión, o disposición de la información.
Tomado y traducido de: http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

Para el proyecto de tesis, se ha realizado una investigación que está dividida en diferentes apartados, el primero corresponde al contexto de investigación, en donde se realiza un estudio previo sobre el tema de ciberseguridad y AE, determinando cual es la necesidad de la investigación e implementación de controles y procedimientos para esta área; en el segundo apartado se encuentra el estado del arte, donde se detalla cada uno de los conceptos de los temas que se abordan dentro de la guía, así mismo se realiza una investigación sobre la actualidad de los marcos de trabajo y normas que se van a utilizar en la guía, de los cuales se contrastará cada uno de ellos basados en los aspectos de ciberseguridad; el tercer apartado corresponde a la guía de ciberseguridad para AE, que consta de diferentes actividades, divididas dentro de las fases del ADM de TOGAF, cada actividad explica los procedimientos que se deben llevar a cabo a través de diferentes controles y procedimientos seleccionados de las normas y marcos de trabajo investigados; el cuarto apartado está dedicado al desarrollo de una aplicación web para el control de la implementación de ciberseguridad en AE, de igual forma se encuentra un estudio de herramientas como opciones de la aplicación desarrollada; El quinto y último apartado contiene la aplicación de la guía con sus respectivos resultados, conclusiones y recomendaciones.

CAPÍTULO I

CONTEXTO DE LA INVESTIGACIÓN

1.1. Tema.

Guía de ciberseguridad para arquitectura empresarial

1.2. Problemática.

Actualmente el rápido desarrollo de TI, SI, comunicaciones, y el entorno empresarial en constante cambio, presentan una serie de desafíos para las organizaciones que tienen la necesidad de gestionar su protección, en donde también intervienen factores como la migración hacia servicios externos, y la necesidad de comunicación con clientes, proveedores y personal, lo que está forzando a las organizaciones a implementar controles apropiados de seguridad en sus SI, para combatir y minimizar los riesgos de seguridad.

Los riesgos relacionados a ciberseguridad incluyen normalmente ataques informáticos hacia los SI, como accesos indebidos, denegación de servicios, malware, explotación de vulnerabilidades, robo de información, etc. Que se ejecutan desde fuera e incluso desde dentro de la misma organización, haciendo que peligre la confidencialidad, integridad y disponibilidad de los sistemas informáticos, este tipo de ataques impactan directamente en las organizaciones causando no solamente pérdidas económicas, sino también un daño en su imagen.

El inconveniente más grande surge al momento de buscar una solución para implementar y gestionar la ciberseguridad en una organización, debido a la complejidad que presenta el adaptar marcos de trabajo y normas de ciberseguridad y AE, dentro de un único marco de referencia.

Para enfrentar cada una de las dificultades mencionadas, es neceario obtener las características (procesos, controles, requerimientos, etc.) de cada marco de trabajo y norma de ciberseguridad y AE para desarrollar una guía que se adapte a la arquitectura empresarial de una organización, donde se gestione cada uno de sus componentes de forma clara y ordenada para controlar sus cambios y crecimiento tecnológico, para aprovechar las fortalezas que ofrece una AE para la implementación de ciberseguridad. La aplicación de ciberseguridad debe cubrir cada una de las fases y principios de AE de acuerdo a los requerimientos de las partes interesadas, a través de procedimientos que ayuden a tratar temas de: conectividad móvil, servicios externos (Cloud Computing), comunicaciones seguras, auditorias de seguridad, gestión de incidentes, etc.

Se importante destacar que muchas organizaciones no poseen una AE implementada, por tal motivo el panorama que ofrecen no es el más favorable en cuanto a la implementación de ciberseguridad a través de la presente guía, pero aun así pueden utilizar el mismo modelo de

la guía para implementar procedimientos a través de sus actividades y proteger sus SI dentro del área de ciberseguridad, aunque el trabajo a realizar seria mayor.

1.3. Justificación.

Debido a los aspectos que intervienen dentro de la implementación de seguridad en las organizaciones, además de la existencia de diferentes normas y marcos de trabajo que actúan sobre la ciberseguridad y AE, se ha planteado trabajar ambas áreas y así desarrollar una guía de ciberseguridad para AE, la misma que estará contrastada con los marcos de trabajo y normas antes mencionadas para establecer un conjunto de actividades orientadas por los principios y requerimientos de ciberseguridad; de esta forma se guiará al oficial o responsable de seguridad de una organización en el proceso de aplicación y gestión de ciberseguridad para AE.

1.4. Alcance.

El alcance definido para la implementación, de una guía de Ciberseguridad para arquitecturas empresariales involucra:

- Planificar:
    - Comparar y seleccionar marcos de trabajo para arquitectura empresarial.
    - Determinar normas y marcos de trabajo orientados a la ciberseguridad.
    - Definir los procesos base de arquitectura empresarial que se integren con los controles de ciberseguridad.
    - Definir las fases que categorizaran los controles, procesos y actividades de la guía.
- Hacer:
    - Implementar las fases dentro de la guía.
    - Implantar las actividades dentro de cada fase.
    - Implementar una herramienta o aplicación, que valide la implementacion de la guía de ciberseguridad para arquitectura empresarial.
- Verificar
    - Revisar las mejorar que se pueden aplicar a través de las actividades de la guía de ciberseguridad para arquitectura empresarial.
- Actuar
    - Evaluar los resultados de la validación de la guía de ciberseguridad para arquitectura empresarial.

1.5. Objetivos.

General

Elaborar una “guía de ciberseguridad para arquitectura empresarial” implementada a través de una herramienta que automatice el proceso de verificación de su implementación.

Específicos

- Contrastar los marcos de trabajo y normas que son la base de la ciberseguridad, para su aplicación dentro de la guía de ciberseguridad para arquitectura empresarial.
- Determinar los procesos y controles, dentro de cada uno de los componentes de la guía de ciberseguridad para arquitecturas empresariales.
- Implementar una herramienta o aplicación, que automatice el proceso de verificación de la aplicación de la guía de ciberseguridad para arquitectura empresarial.
- Validar la guía dentro de un entorno empresarial.

CAPÍTULO II

ESTADO DEL ARTE

2.1. Definición de conceptos.

2.1.1. Arquitectura empresarial (AE).

Se identifican varios conceptos sobre AE, para tener una idea clara de los mismos se citan tres de ellos a continuación:

De acuerdo a (Lankhorst, 2013), AE “es un conjunto coherente de principios, métodos, y modelos que se utilizan en el diseño y la realización de la estructura organizativa de una organización, negocios, procesos, sistemas de información, y la infraestructura”

De acuerdo al White Paper de (The Open Group and The SABSA Institute, 2011), AE “es utilizada como un término inclusivo para referirse a todos los tipos de vistas arquitectónicas - operativo, sistema, seguridad, etc.”

Según se cita en el artículo de (Niemi & Pekkola, 2013), AE “es un enfoque para la gestión de la complejidad de la estructura de la organización, la tecnología de información (TI) y el entorno empresarial, y facilitar la integración de estrategia, personal, negocio y TI hacia un objetivo común a través de la producción y el uso de modelos estructurados para proporcionar una visión holística de la organización”

De acuerdo a los tres conceptos citados, una AE engloba la gestión de una organización en cuanto a análisis, diseño, implementación y control de cada uno de sus componentes en la arquitectura del negocio, datos, aplicaciones, y tecnología, incluyendo la relación e interacción entre ellos; en consecuencia, el éxito de una organización se basa en tener una AE bien diseñada, para que cada uno de sus componente o áreas de trabajo, actúen conjuntamente y así conseguir que se cumplan las metas y objetivos del negocio.

Dentro del ambiente de una AE, debido a la constante evolución de la tecnología y el cambio de mercado, se debe priorizar un buen diseño e implementación de una AE para minimizar el riesgo de realizar cambios futuros dentro de los componentes de una organización; Como se menciona en el artículo de (Arango, Jesús, & Zapata, 2010), “las empresas tiene que manejar la complejidad de su información y la tecnología, y deben mantener activos los sistemas y el ambiente computacional que vienen operando desde años atrás”.

La AE es esencial para la mejora de los SI y las TI que los soportan, esto se logra en términos comerciales como por ejemplo: flujo de datos, misión de la empresa, funciones del negocio, información y entornos de sistemas; en los términos técnicos por ejemplo: software, hardware y comunicaciones; también incluye un plan de transición que va desde el entorno de la línea base a la meta de su ambiente, en donde es necesario tomar en consideracions las dimensiones de la AE que se muestran la Figura 1.

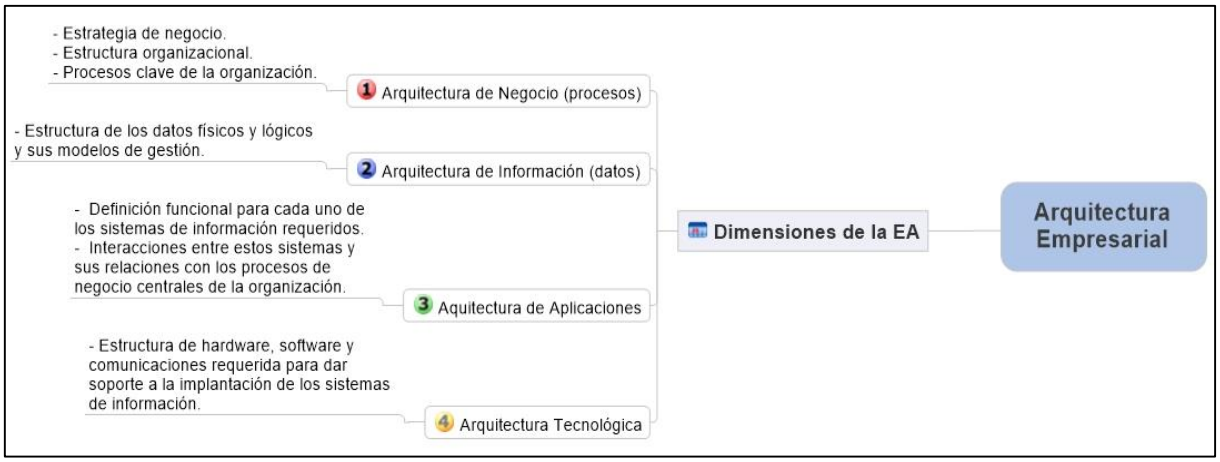

Figura 1: Dimensiones que cubre una AE

Fuente: (Autor, 2013)

2.1.2. Ciberseguridad.

Para comprender el concepto de ciberseguridad, a continuación se considera tres definiciones de la misma:

Según el artículo de (Herring, 2014), la ciberseguridad consiste en la "protección de la información mediante la prevención, detección y respuesta de ataques a los datos electrónicos"

De acuerdo a (ISACA, 2013), la ciberseguridad "abarca todo lo que protege a las organizaciones e individuos de ataques intencionales, violaciones e incidentes, así como las consecuencias. En la práctica, la ciberseguridad se ocupa principalmente de los tipos de ataques, violaciones o incidentes que están dirigidos, sofisticados y difíciles de detectar o gestionar"

Según (Information Secutiry Standars, 2012), define a ciberseguridad como la "preservación de la confidencialidad, integridad y disponibilidad de la información en el ciberespacio"

Según la conceptualización en las tres citas, la ciberseguridad se basa en la prevención y gestión adecuada de ataques y el tratamiento de los tres principios básicos: confidencialidad, integridad y disponibilidad.

- Confidencialidad: la información confidencial debe ser compartida o visible solo por los usuarios correspondientes.
- Integridad: la información debe conservar su integridad y no ser o haber sido alterada de su estado original.
- Disponibilidad: la información deben estar disponibles para aquellos que la necesitan cuando la necesitan.

Otro punto importante que cita en su artículo (Sommerville, 2013), es la división del alcance de la ciberseguridad, la cual se encuentra desglosada de la siguiente forma:

- Técnicas de las amenazas, análisis de ataques y mitigación.
- Protección y recuperación de tecnologías, procesos y procedimientos para los individuos y organizaciones.
- Políticas, leyes y reglamentos pertinentes para el uso de equipos e internet.

Para garantizar la ciberseguridad se requiere de esfuerzos coordinados en todas las áreas de los SI, además de implementar controles y dar seguimiento a riesgos que generen y puedan generar pérdidas en los sistemas de información, en la *Figura 2* se muestra una perspectiva general de la ciberseguridad.

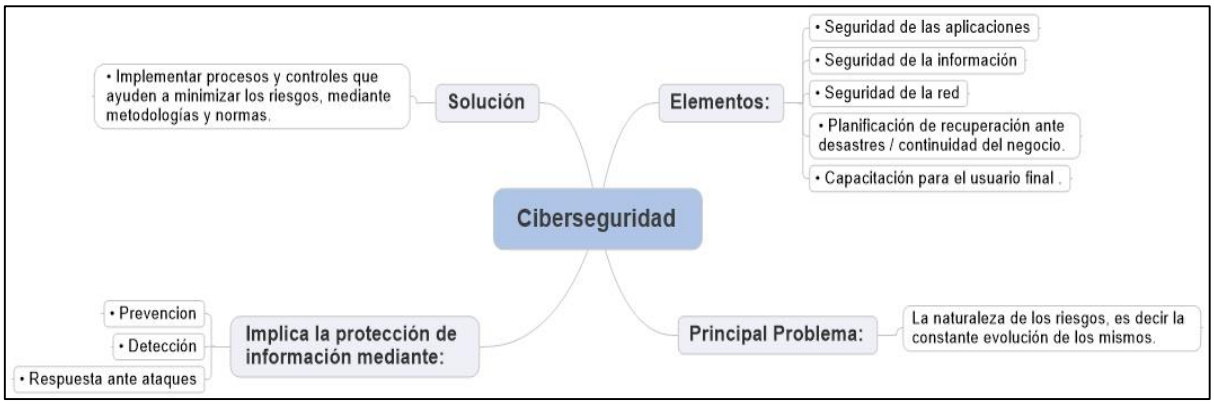

Figura 2: Perspectiva general de Ciberseguridad

Fuente: (Autor, 2013)

2.1.3. Ciberataques.

Un tema a tratar dentro de la ciberseguridad, son los ciberataques para lo cual se citan dos conceptos, en los cuales se define un ciberataque como:

De acuerdo al artículo de (Morenés, 2013), un ciberataque es una “acción producida en el ciberespacio que compromete la disponibilidad, integridad y confidencialidad de la información mediante el acceso no autorizado, la modificación, degradación o destrucción de los sistemas de información y telecomunicaciones o las infraestructuras que los soportan”

Según el artículo de (wiseGEEK, 2014), se define un ciberataque como un “intento de quebrantar o poner en peligro el funcionamiento de un sistema basado en computadoras, o intentar realizar un seguimiento de los movimientos en línea de las personas sin su permiso. Los ataques de este tipo pueden ser indetectables para el usuario final o el administrador de la red, o dar lugar a una interrupción total de la red para que ninguno de los usuarios puede realizar incluso la más rudimentaria de las tareas”

Como se menciona en los conceptos citados, un ciberataque, se basa en un conjunto de procedimientos que intentan afectar la confidencialidad, integridad, y disponibilidad de la información, haciendo que falle o vulnerando cada uno de los sistemas y controles involucrados en defender la misma dentro del internet.

2.1.4. Cibercrimen.

Para tener una visión general sobre cibercrimen, se consideran dos conceptos a continuación: Según se cita en (TechTerms.com, 2014), cibercrimen es el "robo de identidad, en el que los delincuentes utilizan el internet para robar información personal de otros usuarios, dos de las formas más comunes de hacer esto es a través de phishing y pharming, ambos métodos atraen a los usuarios a sitios web falsos, donde se les pide que introduzca información personal, esto incluye la información de inicio de sesión, como nombres de usuario y contraseñas, números de teléfono, direcciones, números de tarjetas de crédito, números de cuentas bancarias y otra información que criminales pueden usar para robar la identidad de otra persona"

De acuerdo a la (Interpol, 2013), el cibercrimen "es uno de los de más rápido crecimiento en ámbitos delictivos. Estos incluyen los ataques contra los datos y sistemas informáticos, el robo de identidad, la distribución de imágenes de abuso sexual infantil, el fraude de subastas en Internet, la penetración de los servicios financieros en línea, así como el despliegue de los virus, botnets, y varias estafas por correo electrónico, como el phishing"

Como se puede observar en los conceptos citados, el cibercrimen se basa en el uso de la tecnología y las técnicas que las mismas ofrecen, por parte de un atacante, para robar información y realizar otras actividades ilícitas, sin ser detectados antes de cumplir con sus objetivos, en donde un equipo desprotegido es una muy buena oportunidad para los atacantes, pues las amenazas de cibercrimen en la actualidad incluyen virus, gusanos, troyanos, phishing, etc. Que buscan acceder a equipos y robar dinero, datos confidenciales, códigos, etc.

2.1.5. Ciberespacio.

Se puede describir el ciberespacio de acuerdo a dos criterios que se citan a continuación:

Según el artículo de (Ministerio De Defensa De España, 2013), el ciberespacio es el "espacio virtual mundial que interconecta sistemas de información, dispositivos móviles y sistemas de control industrial. Está soportado por todo tipo de comunicaciones tales como internet y redes de telefonía móvil. La interconexión proporciona acceso en línea a información y servicios"

Según el artículo de (Benschop, 2013), el ciberespacio “es una ilusión, es una alucinación consensual de que no hay ningún sitio en nuestra realidad física, se trata de un no-lugar que sólo existe dentro de nuestra cabeza. El ciberespacio es algo que de ninguna manera puede ser demarcado en términos geográficos. Es una realidad que puede ser localizada 'en ninguna parte' y sin embargo, se siente su presencia en todas partes”

Conforme a las citas que describen el ciberespacio, se lo puede definir como un lugar no físico, sino lógico, soportado a través de una red de internet, donde se conecta e interactúa hardware y software, con el fin de establecer comunicaciones para actividades, desde las más simples hasta las más complejas que transmiten grandes cantidades de datos.

2.1.6. Tecnología de la Información.

En cuanto a seguridad, se mencionará muy seguido el término de tecnología de la información (TI), a continuación se citan dos conceptos:

Según (ISACA, 2012), tecnología de la Información es el “hardware, software, comunicación y otras habilidades utilizadas para introducir, almacenar, procesar, transmitir y salidas de datos en cualquiera de sus formas”

Según (NIST, 2013), la tecnología de la información trata sobre “informática, hardware de comunicaciones y/o componentes de software y recursos relacionados que se pueden recoger, almacenar, procesar, mantener, compartir, transmitir, o disponer de los datos. Los componentes de TI incluyen ordenadores y dispositivos periféricos asociados, sistemas operativos de computadoras, software de utilidad/soporte, y comunicaciones de hardware y software”

TI, es un conjunto de componentes tecnológicos (hardware y software), que interconectados establecen comunicación, para gestionar la información dentro de diferentes campos, como por ejemplo: científicos, tecnológicos, sociales, etc. El uso eficiente de TI supone una gran ayuda, así mismo ventajas competitivas para las organizaciones, aunque periódicamente se requieren nuevos conocimientos para su gestión.

2.1.7. Seguridad de la Información.

Existen varias definiciones de lo que es seguridad de la información, a continuación se consideran dos de ellos:

Según el artículo de (Ramos, 2009), la seguridad de la información “tiene como fin la protección de la información y de los sistemas de información de una amplia variedad de amenazas como por ejemplo: acceso, uso, divulgación, interrupción o destrucción no

autorizada. Su protección tiene como objeto asegurar la continuidad de negocio, minimizar los riesgos y maximizar el retorno de la inversión y las oportunidades de negocio”

De acuerdo a (Isaca, 2012), la seguridad de la Información “asegura que dentro de la organización, la información está protegida frente a usuarios no autorizados (confidencialidad), la modificación indebida (integridad) y el no acceso cuando sea necesario (disponibilidad)”

En los conceptos anteriormente citados se puede observar claramente lo que es seguridad de la información, pues la misma gestiona cada uno de los controles a seguir para minimizar los riesgos y amenazas que comprometan la información, ante ataques y accesos no autorizados.

2.2. Relación entre ciberseguridad y seguridad de la información.

Existe cierta confusión dentro de las áreas de trabajo y los fines a alcanzar mediante la aplicación de ciberseguridad y/o la seguridad de la información, de acuerdo a las definiciones antes mencionadas en los puntos 2.1.2 y 2.1.7, ambas actúan bajo los principios de proteger la confidencialidad, integridad y disponibilidad de la información; una diferencia que cita (Kosutic, 2012), es que “seguridad de la información, incluye la seguridad en medios no digitales (por ejemplo, papel), mientras que la ciberseguridad se enfoca solamente en la información en formato digital”, en la Figura 3 muestra la relación entre ciberseguridad y seguridad de la información:

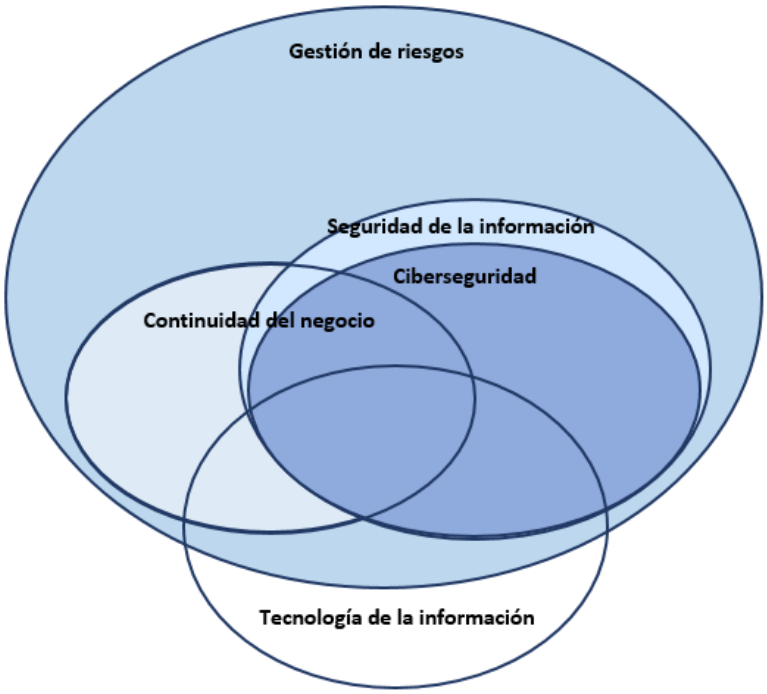

Figura 3: Relación entre Ciberseguridad y Seguridad de la Información

Fuente: (Kosutic, 2012)

Aunque los términos de seguridad de la información y ciberseguridad se los suele utilizar indistintamente, algunas investigaciones como lo cita (NoVa Infosec, 2014), sobre ambos términos, considera que “ciberseguridad trata especialmente los ataques relacionados dentro del campo cibernético y que la seguridad de la información implica la seguridad de los sistemas de información o la información” (ver Figura 4), independientemente de la esfera donde se presente, dado que todo lo que ocurre en el campo cibernético implica de alguna manera la protección de los sistemas de información, se puede concluir que la seguridad informática abarca un súper conjunto de la ciberseguridad que se especializa en la detección y defensa de los ataques informáticos.

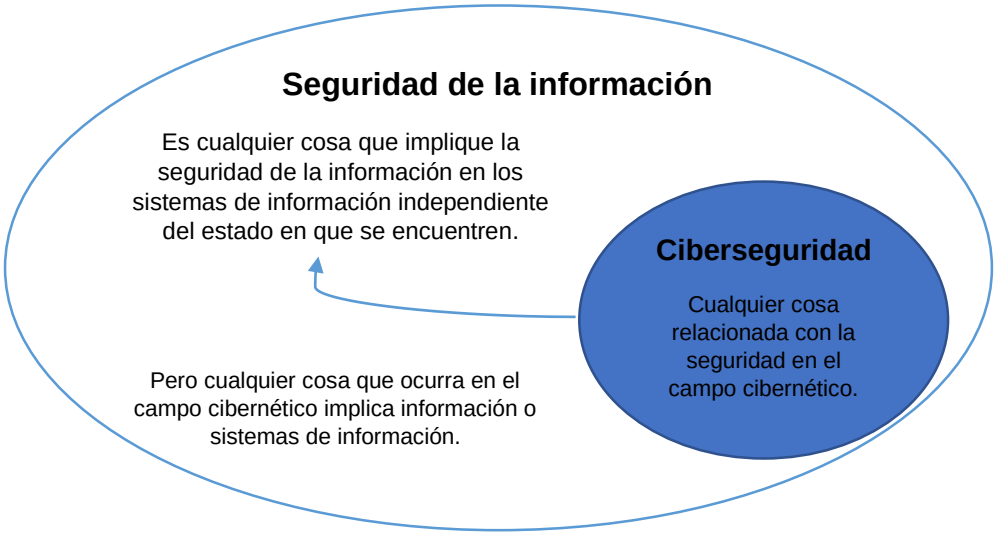

Figura 4: Área de trabajo de ciberseguridad y seguridad de la información

Fuente: tomado y traducido de (NoVa Infosec, 2014)

2.3. COBIT 5 – Un marco de negocio para el gobierno y la gestión de la empresa.

Previo a entrar en materia de AE y ciberseguridad, es necesario conocer a fondo, la importancia de la información como un recurso clave para todas las organizaciones, es por esto que se ha tomado “COBIT 5 un marco de negocio para el gobierno y la gestión de la empresa**”**, el cual se describe así mismo dentrol marco de negocio para el gobierno y la gestión de las ti de la empresa (ISACA, 2012), “como un marco de trabajo integral que ayuda a las organizaciones a alcanzar sus objetivos para el gobierno y la gestión de las TI corporativas. Dicho de una manera sencilla, ayuda a las organizaciones a crear el valor óptimo desde TI manteniendo el equilibrio entre la generación de beneficios y la optimización de los niveles de riesgo y el uso de recursos”

COBIT 5 se basa en cinco principios clave para el gobierno y la gestión de las TI empresariales, los cuales se citan en su marco (ISACA, 2012):

Principio 1: *satisfacer las necesidades de las partes interesadas*, provee todos los procesos necesarios y otros catalizadores para permitir la creación de valor del negocio mediante el uso de TI.

Principio 2: *cubrir la empresa extremo a extremo*, COBIT 5 integra el gobierno y la gestión de TI en el gobierno corporativo:

- Cubre todas las funciones y procesos dentro de la empresa; COBIT 5 trata la información y las tecnologías relacionadas como activos que deben ser tratados como cualquier otro activo por todos en la empresa.
- Considera que los catalizadores relacionados con TI para el gobierno y la gestión deben ser a nivel de toda la empresa y de principio a fin, es decir, incluyendo los que sean relevantes para el gobierno y la gestión de la información de la empresa y TI relacionadas.

Principio 3: *aplicar un marco de referencia único integrado*, COBIT 5 se alinea a alto nivel con otros estándares y marcos de trabajo relevantes, y de este modo puede hacer la función de marco de trabajo principal para el gobierno y la gestión de las Ti de la empresa.

Principio 4: *hacer posible un enfoque holístico*, COBIT 5 define un conjunto de catalizadores (enablers) para apoyar la implementación de un sistema de gobierno y gestión global para las TI de la empresa. Los catalizadores se definen en líneas generales como cualquier cosa que puede ayudar a conseguir las metas de la empresa.

Principio 5: *separar el gobierno de la gestión*, el marco de trabajo COBIT 5 establece una clara distinción entre gobierno y gestión. Estas dos disciplinas engloban diferentes tipos de actividades, requieren diferentes estructuras organizativas y sirven a diferentes propósitos.

Gobierno, de acuerdo a (ISACA, 2012), “contiene cinco procesos de gobierno, en los cuales se definen prácticas de evaluación, orientación y supervisión en cada uno de ellos”

Gestión, conforma a (ISACA, 2012), contiene cuatro dominios, “en conformidad con la áreas de responsabilidad de planificar, construir, ejecutar y supervisar, y proporciona cobertura extremo a extremo de las TI”. Los nombres de estos dominios han sido elegidos de acuerdo a las designaciones de las áreas principales, pero contienen más verbos para describirlos:

- Alinear, Planificar y Organizar
- Construir, Adquirir e Implementar
- Entregar, dar Servicio y Soporte
- Supervisar, Evaluar y Valorar

Otro punto importante por el cual se ha tomado este marco como punto de inicio es debido a su adaptación con otros marcos y normas tanto de seguridad y de AE, en la Figura 5, se puede ver la coincidencia entre sus áreas y dominios, de acuerdo a los cuatro dominios de gestión.

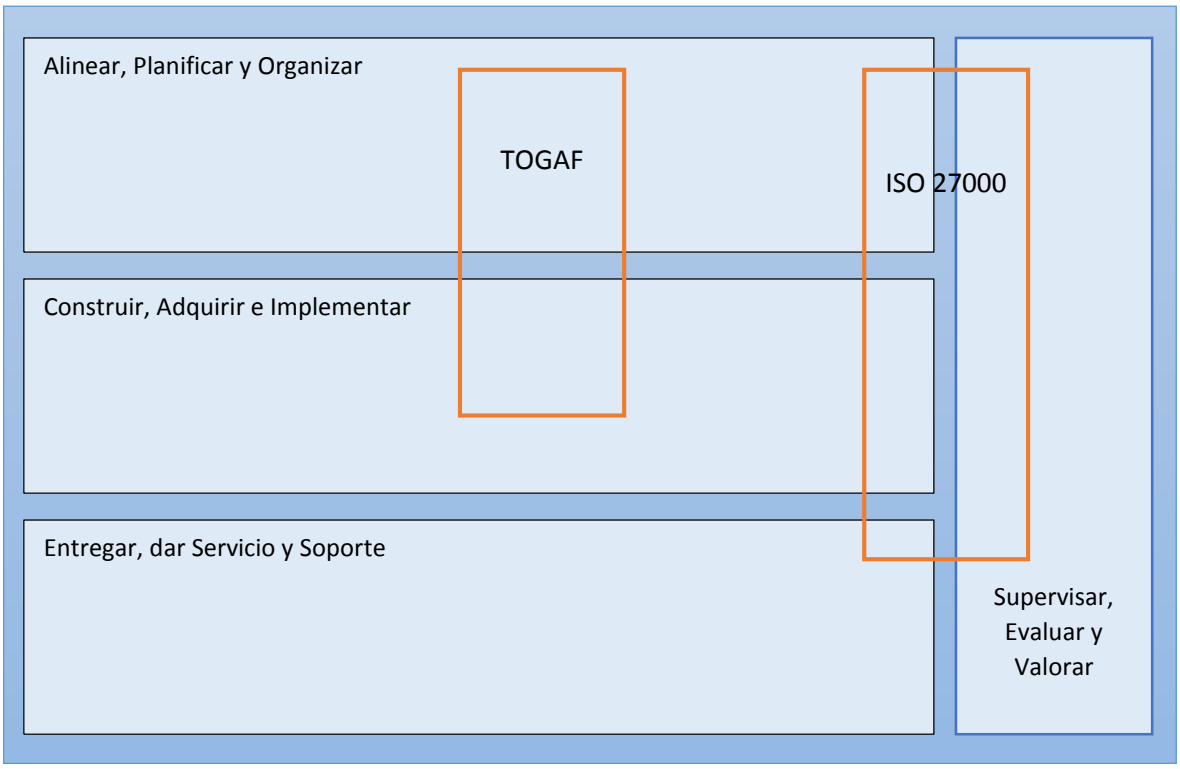

Figura 5: Cobertura de COBIT 5 con otros estándares y marcos de trabajo

Fuente: Tomado y adaptado de COBIT 5 [2]

2.4. Marcos de trabajo para arquitectura empresarial.

El uso de marcos de trabajo es un soporte fundamental para la implementación de una AE; según cita (Sessions, 2007) de acuerdo a los marcos de trabajo, “ninguno de los enfoques es realmente completo, cada uno tiene fortalezas en algunas áreas y debilidades en otras”. Debido a este enfoque se estudian dos marcos de trabajo, que serán objeto de análisis en el presente trabajo, para así determinar cuál se puede acoplar de mejor manera a la Ciberseguridad, estos dos marcos son TOGAF y Zachman Framework por ser los mas conocidos a nivel comercial y empresarial.

2.4.1. Zachman Framework.

De acuerdo a (Zachman, 2008), Zachman framework es una “ontología para describir la empresa, este marco de trabajo (ontología) es una estructura, mientras que una metodología

[2] COBIT 5 - *Un Marco de Negocio para el Gobierno y la Gestión de la Empresa,* http://www.isaca.org/COBIT/Documents/COBIT5-Framework-Spanish.pdf

es un proceso, una estructura no es un proceso, una estructura establece la definición, mientras que una metodología ofrece un proceso de transformación"

Zachman framework es más una taxonomía, con la cual se organiza, clasifica y analiza diferentes artefactos de la arquitectura y también se clasifica toda la estructura de una organización de manera inteligente y ordenada, la misma se encuentra compuesta por seis vistas, de acuerdo al artículo (Osorio, 2010), se describen estos dos componentes de la siguiente manera:

- Alcance: corresponde a un sumario ejecutivo para un planeador o inversionista que requiere una perspectiva general del sistema, cuánto costaría y como se relacionaría con el sistema general donde este operaria.
- Modelo empresarial: son los modelos de la empresa/negocio, los cuales constituyen los diseños del negocio y muestran las entidades del negocio y como se relacionan los procesos.
- Modelo de sistema de información: corresponden al modelo del sistema diseñado por un Analista el cual debe determinar los elementos de datos, el flujo de la lógica de los procesos y las funciones que representan entidades o procesos de negocios.
- Modelo tecnológico: corresponden a los modelos tecnológicos, los cuales se deben adaptar al modelo de sistemas de información, estos tienen en cuenta los lenguajes de programación, los dispositivos de I/O u otra tecnología de soporte.
- Especificación detallada: corresponde a las especificaciones detalladas que se le dan a los programadores que desarrollan modelos específicos sin tener en cuenta el contexto general.
- Empresa en funcionamiento: vista del sistema actual.

De acuerdo al análisis de realizado por (Sessions, 2007), Zachman framework se trata de una estructura lógica para la clasificación y organización de los artefactos de diseño de una organización, que son importantes para su gestión. Se basa en un sistema de clasificación que se encuentra en las disciplinas más maduras de la arquitectura/construcción e ingeniería/fabricación, utilizado para clasificar y organizar los artefactos de diseño relacionados con los productos físicos complejos. Existen varias versiones del diagrama donde se representa el marco de Zachman para la AE, la tabla 1 ha sido adaptada de una versión oficial que incluye detalles sobre los modelos de la célula que está disponible en (John Zachman, 2012).

Tabla 1. Componentes de Zachman Framework

Clasificación de nombres / Perspectivas de audiencia	*Que*	*Como*	*Donde*	*Quien*	*Cuando*	*Porque*	Clasificación de nombres / Modelo de nombres
Perspectiva ejecutiva ***(Contexto de negocio Planificadores)***	**Identificación de inventario** *Lista: tipos de inventario*	**Identificación de proceso** *Lista: tipos de proceso*	**Identificación de distribución** *Lista: tipos de distribución*	**Identificación de responsabilidades** *Lista: tipos de responsabilidades*	**Identificación de tiempos** *Lista: tipos de tiempo*	**Identificación de motivación** *Lista: tipos de motivación*	Contexto de alcance *(Identificación de alcance Listas)*
Perspectiva de gestión de negocio ***(conceptos de negocio Propietarios)***	**Definición de inventario** *Entidad de negocio Relación de negocio*	**Definición de proceso** *Transformar el negocio Entradas/Salidas del negocio*	**Definición de distribución** *Localización del negocio Conexiones del negocio*	**Definición de responsabilidades** *Rol del negocio Productos de trabajo del negocio*	**Definición de tiempos** *Intervalos de negocio Momento del negocio*	**Definición de motivación** *Fin del negocio Medios del negocio*	Conceptos de negocio *(Definición del negocio Modelos)*
Perspectiva de la arquitectura ***(lógica del negocio Diseñadores)***	**Representación de inventario** *Entidad del sistema Relación del sistema*	**Representación de proceso** *Transformar el sistema Entradas/Salidas del sistema*	**Representación de distribución** *Localización del sistema Conexiones del sistema*	**Representación de responsabilidades** *Rol del sistema Productos de trabajo del sistema*	**Representación de tiempos** *Intervalos de sistema Momento del sistema*	**Representación de motivación** *Fin del sistema Medios del sistema*	Lógica del sistema *(Sistema Representación de modelos)*
Perspectiva de ingeniero ***(Tecnología física del negocio Constructores)***	**Especificación de inventario** *Entidad tecnológica Relación tecnológica*	**Especificación de proceso** *Transformación tecnológica Entradas/Salidas de tecnología*	**Especificación de distribución** *Localización tecnológica Conexiones tecnológica*	**Especificación de responsabilidades** *Rol de la tecnología Productos de trabajo tecnológicos*	**Especificación de tiempos** *Intervalos de tecnología Momento de tecnología*	**Especificación de motivación** *Fin de la tecnología Medios de la tecnología*	Tecnología física *(Tecnología Especificación de modelos)*
Perspectiva técnica ***(Componentes del negocio Programadores)***	**Configuración de inventario** *Entidad de herramientas Relación de herramientas*	**Configuración de proceso** *Transformación de herramientas Entradas/Salidas de herramientas*	**Configuración de distribución** *Localización de herramientas Conexiones de herramientas*	**Configuración de responsabilidades** *Rol de herramientas Productos de trabajo de herramientas*	**Configuración de tiempos** *Intervalos de herramientas Momento de herramientas*	**Configuración de motivación** *Fin de las herramientas Medios de las herramientas*	Componentes de la herramienta *(Configuración de herramientas Modelos)*
Perspectiva empresarial ***(Usuarios)*** **La Empresa**	**Instanciaciones de inventario** *Operaciones de entidades Operaciones de relaciones*	**Instanciaciones de proceso** *Operaciones transformadas Entradas/Salidas de operaciones*	**Instanciaciones de distribución** *Localización de operaciones Conexión de operaciones*	**Instanciaciones de responsabilidades** *Rol de las operaciones Productos de trabajo de las operaciones*	**Instanciaciones de tiempos** *Intervalos de las operaciones Momento de operaciones*	**Instanciaciones de motivación** *Fin de las operaciones Medios de las operaciones*	Instancias de operación *(Implementación)* La Empresa
Perspectivas de audiencia / Nombres de la empresa	**Conjuntos de inventario**	**Flujos de procesos**	**Distribución de la redes**	**Asignaciones de responsabilidad**	**Ciclos de tiempo**	**Intensiones de motivación**	

Fuente: traducido y adaptado del sitio de ZachmanInternational (John Zachman, 2012)

Las columnas de la matriz se denominan nombres de clasificación y responden a las siguientes interrogantes:

- Que? – Conjunto de inventario: “describe las entidades involucradas en cada punto de vista de la empresa. Los ejemplos incluyen los objetos de negocio, datos del sistema, las tablas relacionales, las definiciones de campo” [3].
- Como? - Flujos de procesos: “muestra las funciones dentro de cada perspectiva. Incluyen procesos de negocio, la función de la aplicación de software, la función del hardware del equipo, y lazo de control del lenguaje” [4]
- Donde? - Distribución de la redes: “muestra las localizaciones y las interconexiones dentro de la empresa. Esto incluye lugares geográficos empresariales importantes, secciones separadas dentro de una red logística, la asignación de los nodos del sistema, o incluso las direcciones de memoria dentro del sistema” [5]
- Quien? - Asignaciones de responsabilidad: “representa las relaciones de las personas dentro de la empresa. El diseño de la organización empresarial tiene que ver con la asignación de trabajo y la estructura de autoridad y responsabilidad. La dimensión vertical representa la delegación de autoridad, y la horizontal representa la asignación de la responsabilidad” [6]
- Cuando? - Ciclos de tiempo: “representa el tiempo, o el caso de las relaciones que establecen los criterios de rendimiento y los niveles cuantitativos de los recursos de la empresa. Esto es útil para diseñar el programa maestro, la arquitectura de procesamiento, arquitectura de control, y dispositivos de sincronización” [7]
- Por que? - Intensiones de motivación: describe las motivaciones de la empresa. “esto pone de manifiesto los objetivos de la empresa y los objetivos, plan de negocios, la arquitectura del conocimiento, y el diseño de los conocimientos” [8]

Otras componentes impontantes de Zachman Framework son las diferentes perspectivas, resumidas de acuerdo al trabajo de (Ruiz Sanchez, 2014):

- Perspectiva ejecutiva: aquí se define el contexto del negocio junto con el alcance y límites de la empresa, esta perspectiva es un nivel de planificación, los planificadores de contexto del negocio describen qué, cómo, dónde, quién, cuándo y cómo se debe hacer. Los

[3] Alekseigil's SAP Warehouse Management: Descripcion Conceptual de Arquitecturas Empresariales [en linea] <https://alekseigil.wordpress.com/2011/07/22/arquitecturas_empresariales/> [citado el 28 de marzo de 2015]
[4] Ibíd. p. 1
[5] Ibíd. p. 1
[6] Ibíd. p. 1
[7] Ibíd. p. 1
[8] Ibíd. p. 1

contextos de alcance describen un alcance de los modelos, arquitecturas, y las descripciones de la organización.

- Perspectiva de gestión de negocio: describe modelos, arquitectura, requisitos de alto nivel para la empresa y descripciones que son utilizadas por los propietarios de los procesos de negocio.
- Perspectiva de la arquitectura: describe por medio de modelos, arquitecturas, y descripciones que son utilizadas por los diseñadores, ingenieros y arquitectos que están en busca de un compromiso entre lo que es deseable y lo que es técnicamente posible.
- Perspectiva del ingeniero: se basa en crear un diseño de la tecnología física mediante modelos, arquitecturas y descripciones que se utilizan para diseñar y crear un proyecto real.
- Perspectiva técnica: tiene que ver con la implementación, configuración de herramientas, la aplicación de herramientas y la conversión de los modelos físicos en realidad.
- Perspectiva empresarial: en esta perspectiva se observa la empresa en funcionamiento con todas las implementaciones de las perspectivas anteriores. Esta es la perspectiva del usuario final y cubre la ejecución real en sí muestra el objetivo del modelo.

“Este marco permite entender aspectos particulares de un sistema en cualquier punto de su desarrollo y puede ser útil para tomar decisiones acerca de cambios o extensiones” (Mendieta Matute, 2014)

Resolviendo cada una de las características de este marco se pueden obtener diferentes componentes que pueden fortalecer los procedimientos necesarios dentro de ciberseguridad, como las diferentes perspectivas que se asocian a los cuatro principios de AE, mas las interrogantes que permiten clasificar as tareas a realizar dentro de cada perspectiva, asegurando que todos los aspectos de una empresa estén en su lugar y que tengan relaciones claras para asegurar un trabajo completo sin que importe el orden en que se establecieron.

2.4.2. TOGAF (The Open Group Architecture Framework).

TOGAF (en español, el marco del grupo de arquitectura abierta), según la descripción de (The Open Group, 2013), TOGAF es una “metodología de arquitectura empresarial probada y la más utilizada por organizaciones líderes en el mundo para mejorar la eficiencia del negocio”

Otra descripción sobre TOGAF de acuerdo a (The Open Group and The SABSA Institute, 2011), es que TOGAF es un marco de trabajo que “proporciona los métodos y herramientas para ayudar en la aceptación, producción, uso y mantenimiento de una AE. Se basa en un modelo de procesos iterativo con el apoyo de las mejores prácticas y un conjunto reutilizable

de activos que existen”, según (Dominguez Reinaga, 2012) en su documento, TOGAF consta de tres partes principales:

- Método de desarrollo de arquitectura (ADM), que explica la forma de obtener una arquitectura específica de la arquitectura de la organización que se ocupa de los requerimientos del negocio.
- Empresa continuum, es un "repositorio virtual" de todos los activos de la arquitectura - modelos, patrones, las descripciones de la arquitectura
- La base de recursos TOGAF, es un conjunto de recursos, como directrices, plantillas, checklist para verificación y otros materiales, para ayudar a los arquitectos en el uso de las ADM.

La base de recursos no está incluido en la versión 9.1 de TOGAF, debido a que algunos elementos han quedado en desuso a partir de la especificación TOGAF, pero todavía estarán disponible en forma de libro blanco. Otros elementos de la base de recursos se han trasladado a otras zonas de la especificación.

De acuerdo a su documento TOGAF soporta 4 tipos de arquitectura:

- Arquitectura de negocio: define la estrategia de negocio, la estructura organizacional y los procesos clave de la organización
- Arquitectura de datos: la estructura de datos lógicos y físicos que posee una organización y sus recursos de gestión de datos.
- Arquitectura de aplicación: un plano de las aplicaciones individuales a implementar, sus interacciones y sus relaciones con los procesos de negocio principales de la organización.
- Arquitectura tecnológica: describe la capacidad de software y hardware que se requiere para apoyar la implementación de servicios de negocio, datos y aplicación, esto incluye infraestructura de TI, capa de mediación, redes, comunicaciones, procesamiento y estándares.

TOGAF proporciona una descripción de cada fase, en términos de objetivos, enfoque, entradas, pasos a seguir y salidas.

Una ventaja de TOGAF según cita (Josey, 2011) en su guía, es que se complementa, y se puede usar en conjunto con otros marcos de referencia que “se basan en entregables específicos, en sectores como por ejemplo gobierno, telecomunicaciones, manufactura, defensa y finanzas”
De acuerdo a la versión 9.1 de TOGAF (The open Group, 2011), existen siete partes principales en el documento de TOGAF:

Parte I: Introducción, esta parte proporciona una introducción de alto nivel a los conceptos clave de AE y, en particular, el enfoque de TOGAF. Contiene las definiciones de los términos utilizados en TOGAF y notas de publicación que detallan los cambios entre esta versión y la versión anterior de TOGAF.

Parte II: método de desarrollo de la arquitectura (ADM), esta parte es el núcleo de TOGAF. Describe el método de desarrollo de la arquitectura de TOGAF – un enfoque paso a paso para el desarrollo de una AE.

Parte III: guías y técnicas de ADM, esta parte contiene una colección de guías y técnicas disponibles para la aplicación de ADM.

Parte IV: marco de referencia del contenido arquitectónico, esta parte describe el marco de referencia del contenido de TOGAF, incluyendo un meta modelo estructurado para artefactos arquitectónicos, el uso de bloques de construcción de la arquitectura reutilizables, y una descripción de entregables típicos de arquitectura.

Parte V: continuum de la empresa y herramientas, esta parte trata de las taxonomías apropiadas y las herramientas para clasificar y almacenar los resultados de la actividad de arquitectura dentro de una organización.

Parte VI: modelos de referencia de TOGAF, esta parte proporciona una selección de modelos de referencia arquitectónicos, modelo de referencia técnico (TRM) de TOFAG, y el modelo de referencia para la Infraestructura de la información integrada (III-RM)

Parte VII: Marco de Referencia de la capacidad Arquitectónica, esta parte trata de la organización, procesos, habilidades, roles y responsabilidades requeridas para establecer y operar una función de la arquitectura dentro de una organización.

La parte principal, que permitirá desarrollar la guía de ciberseguridad para AE es el ADM, el mismo que se profundiza a continuación:

Método de desarrollo de arquitectura (ADM)

Una parte central en TOGAF es el método de desarrollo de arquitectura (ADM por sus siglas en ingles), la cual proporciona un proceso repetible para el desarrollo de arquitecturas, ADM es un método para obtener arquitecturas empresariales que son específicas para la organización en diferentes niveles (negocio, aplicaciones, datos y tecnología); según se cita (Josey, 2011), “ADM consiste en varias fases que se desplazan cíclicamente a través de una serie de dominios de Arquitectura que permiten asegurar que un conjunto complejo de requerimientos se aborden adecuadamente”, la estructura de ADM se muestra en la Figura 6.

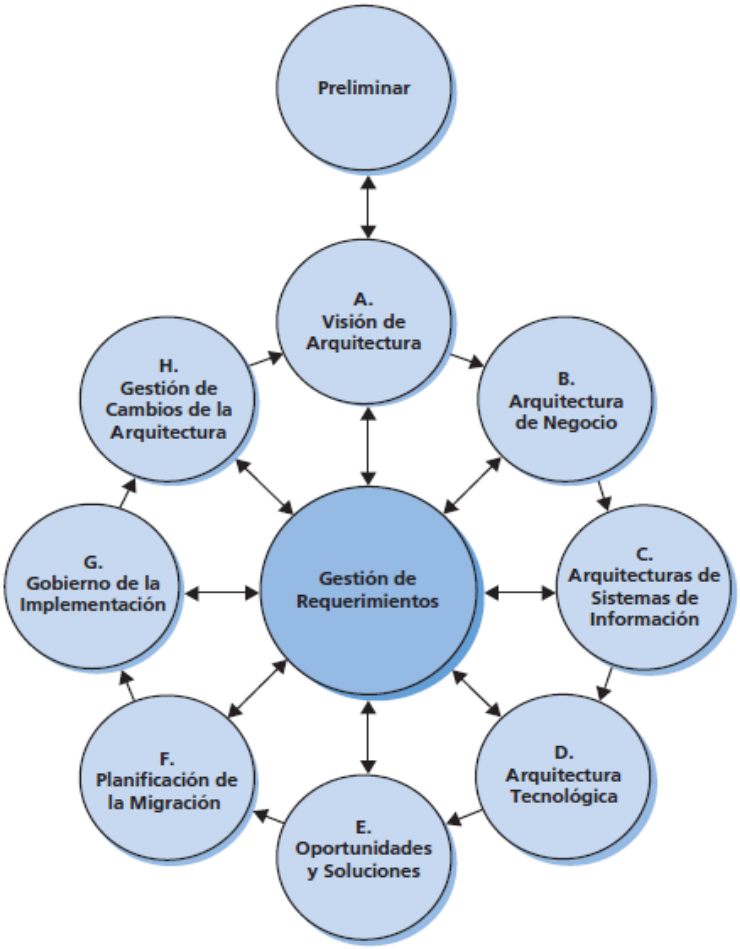

Figura 6: El ciclo del método de desarrollo de la Arquitectura (ADM)

Fuente: Traducido y adaptado de (The Open Group Architecture Forum, 2005)

Durante la etapa de ADM, se debe realizar una validación frecuente de los resultados respecto a los requerimientos originales, en la cual se reconsidera el alcance, el plan y los hitos; las fase que componen el ADM se detallan a continuación, de acuerdo al estudio de (Mendieta Matute, 2014):

Fase preliminar: Esta fase preparar a la organización para crear un plan exitoso de arquitectura; durante esta fase se puede:

- Entender el ambiente del negocio
- Comprender a la alta gerencia
- Alcanzar un acuerdo respecto al alcance
- Establecer principios arquitectónicos
- Establecer una estructura de gobernanza
- Llegar a un acuerdo respecto al método a ser adoptado.

Fase A: Visión de la arquitectura: Durante esta fase se inicia la iteración del proceso de arquitectura, donde se afianza el alcance, limitaciones y expectativas, junto a esto se crea la

visión de la arquitectura, se valida el contexto del negocio, y se construye una declaración del trabajo de la arquitectura.

Fase B: Arquitectura de negocio: En esta fase se analiza la organización fundamental del negocio, inciando por:

- Sus procesos y personal
- Sus relaciones, tanto entre ellos, como con el ambiente.
- Los principios que gobiernan su diseño y evolución, y
- La manera en que la organización alcanzara sus metas de negocios.

En esta fase se define:

- Estructura de la organización
- Objetivos de negocio y metas
- Funciones de megocio
- Servicios que ofrece el negocio y sus procesos.
- Roles en el negocio
- Correlación entre la organización y sus funciones

Fase C: Arquitectura de sistemas de información: En esta fase se definen los aspectos fundamentales en los sistemas de información de la empresa, estos están distribuidos de acuerdo a:

- Tipos de información de importancia para la empresa, junto a los sistemas de aplicación que los procesan.
- Relaciones entre cada sistema de aplicación y el ambiente, igualmente que los procesos que gobiernan su diseño y evolución.

Con esto se demuestra como los Sistemas de Información servirán para alcanzar los objetivos de la empresa.

Fase D: Arquitectura tecnológica: Durante esta fase se especifica como el o los SI recibirán soporte por medio de componentes, tanto basado en Hardware como en Software, al igual que la comunicación y relación con el negocio.

Fase E: Oportunidades y soluciones: En esta fase, se realizan las siguientes actividades:

- Planeación Inicial de implementación
- Identificar los proyectos más grandes en la implementación
- Agrupar proyectos en arquitecturas de transición
- Decidir una aproximación para:

- Construir / Comprar / Reusar
- Outsourcing
- COTS (Commercial on the shelf)
- Open Source
- Evaluar prioridades
- Identificar Dependencias.

Fase F: Planeación de migraciones: En esta fase se trabajan los proyectos identificados en la Fase E, mediante:

- Un análisis costo/beneficio
- Evaluación de riesgos
- Desarrollo detallado de un plan de implementación y migración.

Fase G: Implementación de la gobernanza: Durante esta fase se se provee una supervisión arquitectónica de la implementación, donde se definen las limitaciones existentes en los proyectos de implementación, contratos de arquitectura y se monitorea el trabajo de implementación.

Fase H: Gestión de la arquitectura de cambio: Esta fase provee monitoreo continuo, para:

- Asegurarse de que los cambios en la arquitectura se manejan de una manera cohesiva e inteligente.
- Establecer y brindar soporte a la arquitectura empresarial para proveer flexibilidad en los cambios que se presentan debido a cambios tecnológicos o en los negocios.
- Monitorear la capacidad administrativa del negocio.

TOGAF posee algunas características que son de gran ayuda para la construcción de una AE, las cuales alinean la parte tecnológica con el negocio en sí, estas características se mencionan en el artículo de (Arizabaleta & Ávila, 2012), las cuales se citan a continuación:

- Reducción de costos.
- Mejorar las relaciones de los departamentos
- Reducción del riesgo, TOGAF identifica las ineficiencias de cada uno de los actores y sus objetivos vs los del Negocio.
- Flexibilidad y adaptación, el manejo de los requisitos es el centro de la metodología ADM, quien se convierte en la clave para adaptar proyectos sin perder su objetivo inicial frente a las arquitecturas propuestas.

- Lenguaje común, TOGAF provee un repositorio de documentos y modelos que permiten adaptar la visión de la organización a los diferentes actores involucrados: de esta forma crea una relación entre los conceptos de negocio y tecnología.

Otro punto para valorar el marco de trabajo de TOGAF, de acuerdo a (The open Group, 2011), es que TOGAF proporciona la capacidad y el entorno de colaboración para la integración con otros marcos de trabajo (ITIL, CMMI, COBIT, PRINCE2, PMBOK, y MSP). Las organizaciones son capaces de utilizar plenamente los dominios verticales de negocios, áreas tecnológicas horizontales (como seguridad o capacidad de administración), o áreas de aplicación (por ejemplo, e-Commerce) para producir un marco de AE competitivo que maximiza sus oportunidades de negocio.

2.4.3. Comparación entre TOGAF y Zachman Framework.

Para construir una AE, se debe considerar un marco que trabaje sobre las cuatro dimensiones de una AE (arquitectura de negocio, arquitectura de información, arquitectura de aplicaciones y arquitectura tecnológica). Para su comparación se ha tomado en cuenta diferentes aspectos (Tabla 2), que pueden ayudar en el desarrollo de una AE robusta y que abarque cada dominio de interés que permita construir una arquitectura mas segura.

Tabla 2. Comparación entre TOGAF y Zachman Framework

Marcos de trabajo / Componentes	TOGAF	Zachman Framework
Aporta beneficios de TI	X	X
Basado en entregables	X	
Adaptable a las necesidades de una organización	X	X
Gestión de infraestructura	X	X
Centrado en las actividades del negocio	X	X
Organización y clasificación de artefactos	X	X
Gestión de requerimientos	X	
Gestión de alcance	X	X
Gestión de cambios	X	X
Gestión de riesgos	X	X
Adaptable a otros marcos de trabajo	X	
Reducción de costos	X	X
Identificación de oportunidades	X	X

Fuente: (Autor, 2013)

De acuerdo a las comparaciones entre estos dos marcos de trabajo, TOGAF es el idóneo para la construcción de una AE, aunque por otro lado Zachman framework puede ayudar en la clasificación de artefactos del diseño de una AE.

TOGAF es más general y da las bases desde donde construir una AE, pero en el caso de seguridad de la información es muy necesario apoyarse en otros marcos de trabajo y normas.

Zachman framework, es una forma de organizar una organización y asignar responsabilidades, a través de su modelo de interrogantes y puntos de vista.

De acuerdo a las observaciones del artículo de (Osorio, 2010), TOGAF es más práctico en los aspectos de creación de una arquitectura sólida.

2.5. Normas y marcos de trabajo de ciberseguridad.

A continuación se citan cuáles son los marcos de trabajo y normas en la implementación de ciberseguridad para AE:

2.5.1. ISO/IEC 27001.

Según el artículo (ISO 27000.es, 2005), ISO 27001 contiene los requisitos del sistema de gestión de seguridad de la información, de acuerdo a (27001 Academy), su objetivo es "proporcionar una metodología para la implementación un sistema de gestión de la seguridad de la información (SGSI) en una organización", además permite que una organización sea certificada.

Dentro de esta norma existen 4 fases que se deben implementar en forma constante para reducir al mínimo los riesgos sobre confidencialidad, integridad y disponibilidad de la información; estas 4 cuatro fases ayudan a reducir considerablemente los riesgos sobre confidencialidad, integridad y disponibilidad; las fases son las siguientes:

- La fase de planificación: planifica la organización básica y establecer los objetivos de la seguridad de la información para escoger los controles adecuados de seguridad.
- La fase de implementación: Implica la realización de todo lo planificado en la fase anterior.
- La fase de revisión: monitorea el funcionamiento del SGSI y verificar si los resultados cumplen los objetivos establecidos.
- La fase de mantenimiento y mejora: mejora todos los incumplimientos detectados en la fase anterior

Para complementar definiremos lo que es un SGSI (sistema de gestión de la seguridad de la información), en ingles conocido como ISMS (Information Security Management System), la seguridad de la información, según (ISO 27000.es, 2012), consiste en la "preservación de su

confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización”

Para garantizar que la seguridad de la información sea gestionada correctamente, se debe hacer uso de un proceso sistemático, documentado y conocido por toda la organización, desde un enfoque de riesgo empresarial. Este proceso es el que constituye un SGSI.

2.5.2. ISO/IEC 27032.

Según el artículo de (ISO, 2012), “proporciona directrices para mejorar el estado de la ciberseguridad, destacando aspectos únicos de dicha actividad y su dependencia de otros ámbitos de seguridad”

Esta norma proporciona un marco seguro para el intercambio de información, el manejo de incidentes y la coordinación para hacer más seguros los procesos según se cita (García, 2012), también “ofrece una visión general de ciberseguridad y ayuda a proteger de una manera fiable la privacidad de las personas. Con el fin prepararse, detectar, monitorizar y responder a los ataques”

De acuerdo a (ISO, 2012), esta norma extrae los aspectos individuales y dependencias de otros ámbitos de seguridad (ver Figura 7), en particular como:

- Seguridad de la información.
- Seguridad de redes.
- Seguridad del Internet, y
- La protección de la infraestructura crítica de información.

Figura 7 – Relación entre Ciberseguridad y otros dominios de seguridad

Fuente: Tomado y Traducido de (Klinburg & Hathaway, 2013)

De acuerdo a la relación con otros ámbitos, esta norma se basa en dos enfoques principales:

Primer Enfoque

Aborda problemas de ciberseguridad, que se concentra en reducir los diferentes vacíos en el ciberespacio, y proporciona una guía técnica para abordar riesgos de ciberseguridad comunes, incluyendo:

- Ataques de ingeniería social.
- el acceso secreto y no autorizado a sistemas informáticos (hacking)
- Proliferación de software malicioso (malware).
- Software espía (Spyware)
- Otros tipos de software potencialmente no deseado.

La guía técnica proporciona controles para hacer frente a estos riesgos, incluyendo controles para:

- Prepararse para ataques de, por ejemplo, software malicioso, delincuentes aislados u organizaciones criminales del Internet.
- detectar y monitorear ataques, y
- responder a los ataques.

Segundo enfoque

Se basa en la colaboración, puesto que existe la necesidad del compartir información de manera eficiente y efectiva, y de coordinación y gestión de incidentes entre las partes interesadas en el ciberespacio.

Además esta norma proporciona:

- Descripción general de la ciberseguridad.
- Explicación de la relación entre la ciberseguridad y otros tipos de seguridad.
- Definición de las partes interesadas y una descripción de su papel en la ciberseguridad.
- Orientación para abordar las cuestiones comunes de ciberseguridad, y
- Un marco que permitirá a los interesados colaborar en la resolución de cuestiones de ciberseguridad.

2.5.3. Transformando la ciberseguridad utilizando COBIT 5 (TCS).

De acuerdo a (ISACA, 2013), el presente marco de trabajo de ciberseguridad “examina el impacto del cibercrimen, la conectividad permanente, una sociedad cada vez más centrada en TI, un nuevo sistema de clasificación que identifica a la gente por habilidades tecnológicas y cómo administrar y transformar la seguridad usando COBIT 5, un marco de negocio para el

gobierno y la administración de la información empresarial y de tecnología". Junto con la publicación de la guía, ISACA también se anunció la conformación de una fuerza de tarea global de ciberseguridad.

Según (ISACA, 2013), existen 3 factores de cambio en la ciberseguridad, las cuales se tratan en la guía, que ofrecen el propósito y la oportunidad para las brechas de la ciberseguridad y las actividades criminales, especialmente las amenazas avanzadas persistentes (APT):

a. Conectividad permanente:
   - Los datos críticos y la información están agrupados en las nubes.
   - Están creciendo los hotspots Wi-Fi.
   - Es fácil tener acceso a los sistemas del trabajo en casa o en movimiento.
b. Negocio y sociedad centrados en TI.
   - Los sistemas en línea son las nuevas infraestructuras críticas.
   - La dependencia de la sociedad de "lo permanente" crea ventanas más amplias del tiempo de ataque.
   - No hay un plan alternativo en caso de emergencias.
c. Nuevo sistema de clases por habilidades tecnológicas
   - Las características de los dispositivos móviles siguen siendo un misterio para muchos.
   - Menos nativos digitales tienen habilidades de TI profundas.
   - Nuevas aplicaciones y sistemas operativos favorecen la conveniencia sobre el control de los usuarios.

2.5.4. NIST - Marco de trabajo para mejorar la ciberseguridad de infraestructuras críticas (CS-IC).

Es un marco de trabajo, publicado por NIST (National Institute of Standards and Technology), contiene un conjunto de directrices sobre ciberseguridad para ayudar a proteger infraestructuras críticas, y está basado en la gestión de riesgos para la ciberseguridad, el mismo se compone por tres partes según (NIST, 2014):

a. El núcleo del marco de trabajo, presenta estándares de la industria, directrices y prácticas que de una manera permiten la comunicación de las actividades de ciberseguridad y los resultados en toda la organización desde el nivel ejecutivo hasta el nivel de aplicación/operaciones. El núcleo del marco de trabajo consiste de cinco funciones principales: identificar, proteger, detectar, responder y recuperarse.
   - Identificar, implica obtener una comprensión de los recursos y los niveles de riesgo asociados a los activos.
   - Proteger y detectar, cubren temas tales como control de acceso y supervisión de la seguridad.

- Responder y recuperar, buscan la forma de reaccionar en caso de un incidente de seguridad.

b. Niveles de aplicación del marco de trabajo (Niveles), proporcionan un contexto de cómo una organización entiende por riesgo la ciberseguridad y los procesos para gestionar ese riesgo. Los niveles describen el grado en que las prácticas de gestión de riesgos de ciberseguridad de la organización presentan las características definidas en el marco de trabajo (por ejemplo, el riesgo y amenazas conscientes, repetible y adaptable). Los niveles caracterizan prácticas de una organización a través de una gama, desde parcial (Nivel 1) hasta adaptado (Nivel 4).

c. El perfil del marco de trabajo (Perfil), representa los resultados basados en las necesidades del negocio que una organización ha seleccionado de las categorías y subcategorías del Marco de trabajo. El perfil puede ser caracterizado como la alineación de las normas, directrices y prácticas para el núcleo del marco de trabajo en un escenario de implementación en particular. Los perfiles pueden ser utilizados para identificar las oportunidades, para mejorar la postura de ciberseguridad mediante la comparación de un perfil "Actual" (el "como es" el estado) con un perfil "Objetivo" (el "ser" del estado). Para desarrollar un perfil, una organización puede revisar todas las categorías y subcategorías y, basándose en los impulsores del negocio y una evaluación de los riesgos, determinar cuáles son los más importantes, ya que pueden añadir categorías y subcategorías, según sea necesario para hacer frente a los riesgos de la organización. El perfil actual puede entonces ser utilizado para apoyar el establecimiento de prioridades y la medición del progreso hacia el perfil objetivo, mientras que factorizando en otras necesidades de negocio, incluyendo la rentabilidad y la innovación. Los perfiles pueden ser utilizados para llevar a cabo autoevaluaciones y comunicarse dentro de una organización o entre organizaciones.

2.5.5. Comparación entre marcos de trabajo y normas de ciberseguridad.

Dentro de la implementación de ciberseguridad es necesario conocer los componentes que puedan ayudar a fortalecer la ciberseguridad en una AE, por esta razón en la *Tabla 3*, se identifican las ventajas que ofrece cada marco de trabajo y norma, para posteriormente implementarlas dentro de la guía de ciberseguridad para AE, cabe mencionar que las normas ISO 27001, se la utilizará en su versión 2013, considerando su mayor flexibilidad en cuanto a su implementación y lo más importante de acuerdo a (ISOTools - Excellence, 2013), las organizaciones cuentan con un tiempo definido para adaptarse a los cambios de la versión 2013, a partir del 2014.

Tabla 3. Comparativa del marcos de trabajo y normas de ciberseguridad

Normas y marcos de trabajo / Parámetros CS	ISO 27001	ISO 27032	COBIT 5 (TCS)	NIST (CS-IC)
Políticas de seguridad	x		x	x
Preservación de CID	x	x		x
Gestión de incidentes informáticos	x	x	x	x
Gestión de recursos	x			
Gestión de riesgos	x			x
Hacking		x		
Seguridad de internet	x	x	x	x
Mejora Continua	x	x	x	x
Software Malicioso	x	x		
Intercambio de Información	x	x	x	x
Cloud Computing			x	
Dispositivos Móviles	x		x	
Gestión de Infraestructura				x

Fuente: (Autor, 2014)

Cada uno de los aspectos comparados se pueden complementar con el marco de trabajo seleccionado, debido a su flexibilidad para adaptar otros marcos de trabajo, en este caso cada una de las normas y marcos de trabajo ofrecen distintas características que pueden ayudar a fortalecer la ciberseguridad de una AE.

2.6. Marcos de trabajo y guías de seguridad empresarial.

2.6.1. Guía para la arquitectura de seguridad en el ADM de TOGAF.

TOGAF proporciona una guía que trata la arquitectura de seguridad y el ADM, la cual tiene como objetivo explicar las consideraciones de seguridad que deben ser tratadas durante la aplicación del ADM, y una orientación de seguridad para los dominios de arquitectura, los cuales tiene como propósito fundamental proteger el valor de los sistemas y activos de información de la organización.

La arquitectura de seguridad tiene sus propios componentes, los cuales se deben interconectar con los sistemas de negocio de una manera equilibrada, con el fin de mantener las políticas de la organización, para no interferir con las operaciones del sistema y funciones.

A lo largo de la implementación de las fases de ADM, las decisiones de arquitectura, relacionadas con la seguridad, deben realizarse de conformidad a las decisiones empresariales, políticas y gestión de riesgos.

Las áreas de preocupación para la arquitectura de seguridad según (The open Group, 2011), son:

- Autenticación: comprobación de la identidad de una persona o entidad, verificando sus credenciales.
- Autorización: aplicación de capacidades permitidas para una persona o entidad cuya identidad ha sido establecida.
- Auditoría: capacidad de proporcionar datos forenses que consten que los sistemas se han utilizado de acuerdo a las políticas de seguridad establecidas.
- Garantía: capacidad de probar y demostrar que la arquitectura de la organización, tiene los atributos de seguridad necesarios para defender las políticas de seguridad establecidas.
- Disponibilidad: capacidad de la organización para funcionar sin interrupción a pesar de acontecimientos anormales o maliciosos.
- Protección de activos: protección de los activos de información la de pérdida o divulgación no intencional, y el uso no autorizado y no deseado de los recursos.
- Administración: capacidad de agregar y cambiar las políticas de seguridad, agregar o cambiar cómo se implementan las políticas en la organización, y añadir o cambiar las personas o entidades vinculadas a los sistemas.
- Gestión de riesgos: la actitud y la tolerancia al riesgo de la organización.

Para tratar la arquitectura de seguridad, según (Ertaul, Movasseghi, & Kumar, 2011), intervienen artefactos típicos, los cuales deben incluir:

- Reglas de negocio con respecto al manejo de activos (datos/información)
- Políticas de seguridad escritas y publicadas
- Codificación de datos/información y custodia de activos.
- Documentación del análisis de riesgos
- Documentación de políticas de clasificación de datos

Cada uno de estos artefactos, participan dentro de la gestión de la arquitectura de seguridad a través de las siguientes fases en la implementación de ADM:

Gestión de requisitos: esta fase impulsa continuamente el ADM, las políticas y normas de seguridad se convierten en parte del proceso de gestión de requisitos empresariales, las cuales se establecen desde un nivel ejecutivo y no se encuentran ligadas a ninguna tecnología en específico, estas políticas y normas pueden ser referidas como requisitos para todos los proyectos de la arquitectura; de acuerdo a (Ertaul, Movasseghi, & Kumar, 2011), un nuevo requisito de seguridad puede surgir a partir de: un nuevo mandato o una ley reglamentaria, una nueva amenaza, o una nueva iniciativa de la arquitectura de TI descubre nuevos interesado y/o nuevos requisitos.

Fase preliminar: en esta fase se define el alcance que va a tener la aplicación de la arquitectura de seguridad, en donde las políticas de seguridad de la organización deben estar en su logar por escrito. Para hacer cumplir y tratar con las políticas, debe existir un responsable de seguridad, con el objetivo de garantizar que se aborden todas las cuestiones y se resuelvan temas complicados que generen conflictos de intereses, haciendo cumplir las políticas de acuerdo a razones reglamentarias; otro punto que se debe considerar es la participación y relación con otras organizaciones, con las cuales se debe tratar las políticas, para desarrollar protocolos seguros de intercambio de información.

En la figura 8 se pueden ver las respectivas entradas y salidas de esta fase, donde se documentan y establecen los criterios necesarios para seguridad.

Figura 8. Entradas y Salidas de la Fase Preliminar
Fuente: Traducido y adaptado de (The open Group, 2011)

Fase A - Visión de arquitectura: de acuerdo a (The open Group, 2011) las etapas de esta fase, “son aplicables para garantizar que los requisitos de seguridad se abordan en la fases posteriores de ADM”, debido a que las consideraciones de seguridad tienen efecto en la organización, de este modo el desarrollo de la AE debe ser informada.

De acuerdo a (The Open Group Architecture Forum, 2005), en esta fase se determina todo lo relacionado a la aplicación de planes/requisitos para la recuperación de desastres y continuidad de negocio, el ambiente físico/regulador del negocio en donde se implementaran los sistemas, y la criticidad de sistemas valorados de acuerdo a los siguientes aspectos:

- Seguridad-critica, relacionada con los sistemas que se encuentran en peligro, en caso de fallo o mal funcionamiento.
- Misión-crítica, relacionada con sistemas que manejan dinero, cuota de mercado, o el capital en riesgo en caso de fallo.
- No-critico, relacionado con poca o ninguna consecuencia en caso de algún fallo.

En esta etapa intervienen las debidas entradas y salidas (ver Figura 9), las cuales aportan en el proceso del desarrollo de arquitectura de seguridad.

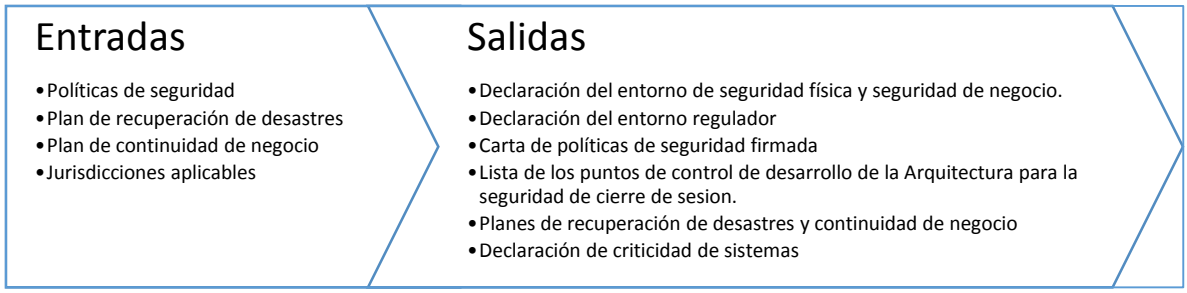

Figura 9. Entradas y Salidas de Fase A - Visión de Arquitectura

Fuente: Traducido y adaptado de (The open Group, 2011)

Fase B - Arquitectura de negocio: esta fase determina ampliamente los factores que interactúan con el producto, sistema o procesos; el conocimiento de esta fase según (The Open Group Architecture Forum, 2005) “es necesaria para trabajar con cualquiera de los dominios de arquitectura de negocio, aplicaciones y tecnología”

Dentro de esta fase se identifican las capacidades y características para las posteriores decisiones de autorización y los límites de operación para los administradores, operadores de sistemas y usuarios (pueden ser personas o software de aplicación)

De acuerdo a (Maganathin, 2010) se debe evaluar la línea base actual de los procesos específicos de seguridad del negocio, así mismo determinar cuánto es aceptable incomodar en la utilización de medidas de seguridad.

Para trabajar con las debidas entradas y salidas (ver Figura 10) de esta fase, de acuerdo a (The open Group, 2011), se debe identificar y documentar los sistemas de interconexión que están más allá del control del proyecto; también es necesario determinar los activos que se encuentran en riesgo; determinar el costo (tanto cualitativo como cuantitativo) de la pérdida e impacto de activos en caso de falla; identificar y documentar la propiedad de los activos; determinar y documentar los procesos forenses apropiados de seguridad; identificar la criticidad de la disponibilidad y el correcto funcionamiento de los servicios en general; revalorar y confirmar las decisiones de la visión de arquitectura; determinar y documentar cuanta seguridad (coste) se justifica por las amenazas y el valor del riesgo de activos; evaluar la alineación o conflicto de políticas de seguridad identificados con los objetivos empresariales; determinar e identificar las amenazas de alto nivel que influyan en el sistema y su probabilidad.

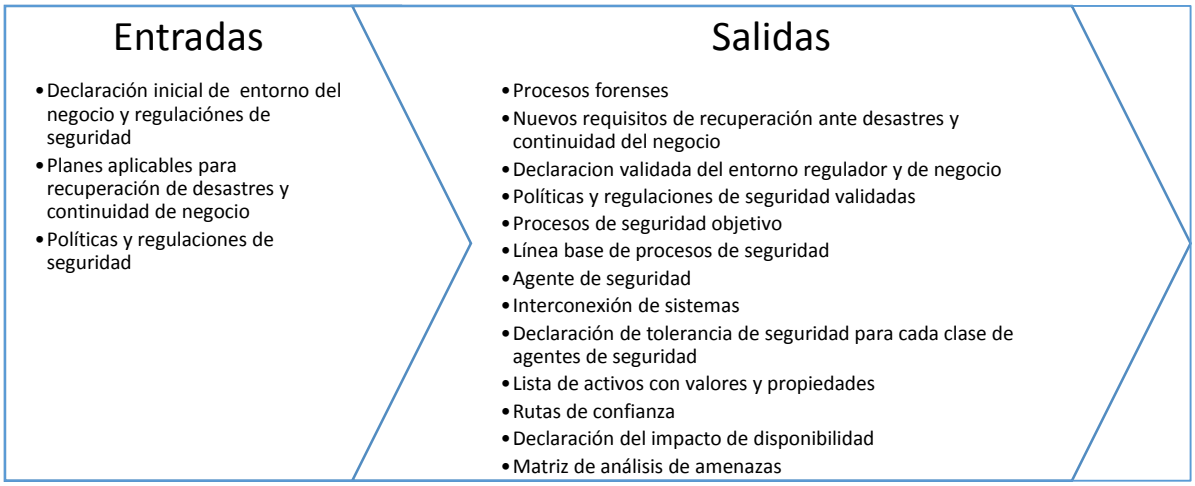

Figura 10. Entradas y Salidas de la Fase B - Arquitectura de Negocio

Fuente: Traducido y adaptado de (The open Group, 2011)

Fase C - Arquitectura de sistemas de información: esta fase abarca los dominios de arquitectura de datos y de aplicación, los cuales se pueden implementar no necesariamente en orden, pero se puede establecer mediante una metodología que adopte el arquitecto de seguridad.

En esta fase se trata principalmente los elementos específicos de seguridad de la arquitectura, acciones por defecto en caso de estados de fallo, directrices y normas aplicables, sistemas de interconexión, clasificación de información, planes de continuidad de negocio y de desastres, tiempo de vida de la información, logs para procesos forenses, la gestión de ataques y de riesgos; cada una de estas características se complementan por las entradas y salidas (ver Figura 11) que dispone esta fase.

Figura 11. Entradas y Salidas de la Fase C - Arquitectura de Sistemas de Información

Fuente: Traducido y adaptado de (The open Group, 2011)

Fase D - Arquitectura tecnológica: esta fase trata de las especificaciones técnicas detalladas para los sistemas, que llevan a cabo los requisitos de seguridad definidos en las fases anteriores.

Para obtener las respectivas entradas y salidas (ver Figura 12), hay que considerar las características de esta fase, de acuerdo a (The open Group, 2011), el Arquitecto de seguridad debe evaluar la línea base actual de las tecnologías específicas de seguridad, revisar las suposiciones relativas a los sistemas de interconexión más allá del control del proyecto, identificar y evaluar directrices y normas reconocidas, identificar los métodos para regular el consumo de recursos, diseñar un método por el cual se medirá la eficacia de las medidas de seguridad, y se identifica el nivel de confianza de los usuarios, los privilegios mínimos necesarios para que cualquier entidad logre un objetivo técnico o empresarial, e identificar las medidas de mitigación de seguridad.

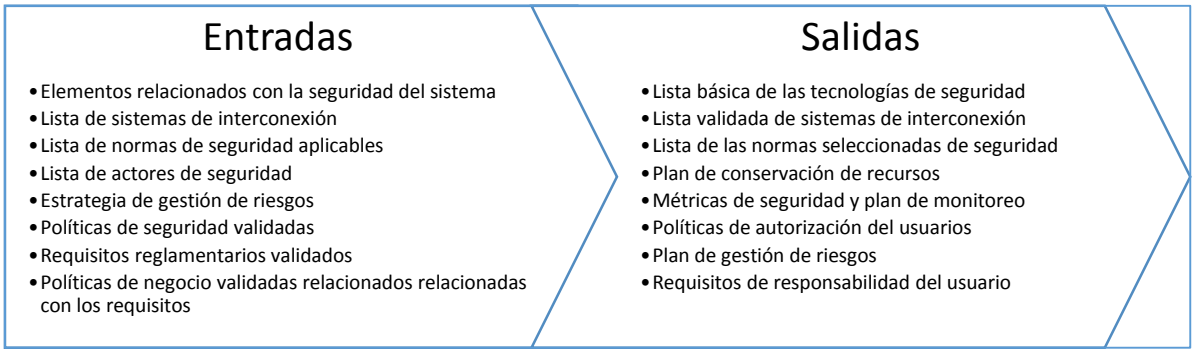

Figura 12. Entradas y Salidas de la Fase D - Arquitectura Tecnológica

Fuente: Traducido y adaptado de (The open Group, 2011)

Fase E - Oportunidades y soluciones: de acuerdo a (The open Group, 2011), durante esta fase se identifican los servicios disponibles de seguridad existentes para reutilización, las medidas de mitigación que el ingeniero aborda para los riesgos identificados, también se evalúa el software de seguridad que ha sido probado, que se puede reutilizar y los recursos de sistemas de seguridad, e identificar nuevos códigos/recursos/activos que son apropiados para la reutilización.

Fase F - Planificación de la migración: en esta fase se evalúa el impacto de las nuevas medidas de seguridad sobre otros componentes nuevos o sistemas existentes, se implementan métodos de supervisión mediante los cuales se medirá la eficacia de las medidas de seguridad, se identifican los parámetros correctos de instalación segura, y se implementan planes de recuperación ante desastres, continuidad de negocio y/o modificaciones.

Fase G - Gobernanza: esta fase establece artefactos de arquitectura, diseño, y revisiones de código y define los criterios de aceptación para una implementación exitosa de los hallazgos.

Otra característica que cita (Maganathin, 2010), es la implementación de los métodos y procedimientos para revisar las pruebas aportadas por el sistema las cuales reflejan la estabilidad operativa y la adherencia de las políticas de seguridad, también Implementa la capacitación necesaria para asegurar la correcta implementación, configuración y funcionamiento de los subsistemas y componentes relevantes para seguridad, además garantiza la formación de conciencia para todos los usuarios y operadores no privilegiados del sistema y/o sus componentes.

Fase H - Gestión de cambios de la arquitectura: esta fase gestiona los cambios que se producen en las normas o políticas de seguridad, conducidas por estatutos, regulaciones o porque algo se ha hecho mal; por lo general los cambios que surgen como consecuencia de un problema de seguridad o una nueva tecnología de seguridad, se incorporará en el proceso de gestión de requisitos.

2.6.2. SABSA – Seguridad de arquitectura empresarial.

De acuerdo a (Sherwood, Clark, & Lynas, 2009) SABSA, “es una metodología impulsada por el riesgo para el desarrollo de seguridad de la información empresarial, arquitecturas de seguridad de la información y para la entrega de soluciones de seguridad de infraestructuras que soportan y apoyan las iniciativas críticas del negocio“; otras características del marco de trabajo es la escalabilidad, independiente de proveedor, aplicable a cualquier sector empresarial o industrial, y permite integrarse con otras normas o marcos de trabajo (Ejemplo: TOGAF, ITIL)

Conforme se cita en (SABSA, 2013), SABSA “comprende una serie de marcos integrados, modelos, métodos y procesos, utilizados de forma independiente o como una solución empresarial integrada holística” para organizaciones de usuarios finales que utilizan la norma para el desarrollo e implementación de arquitecturas y soluciones empresariales, que incluyen diferentes marcos (ver Figura 13)

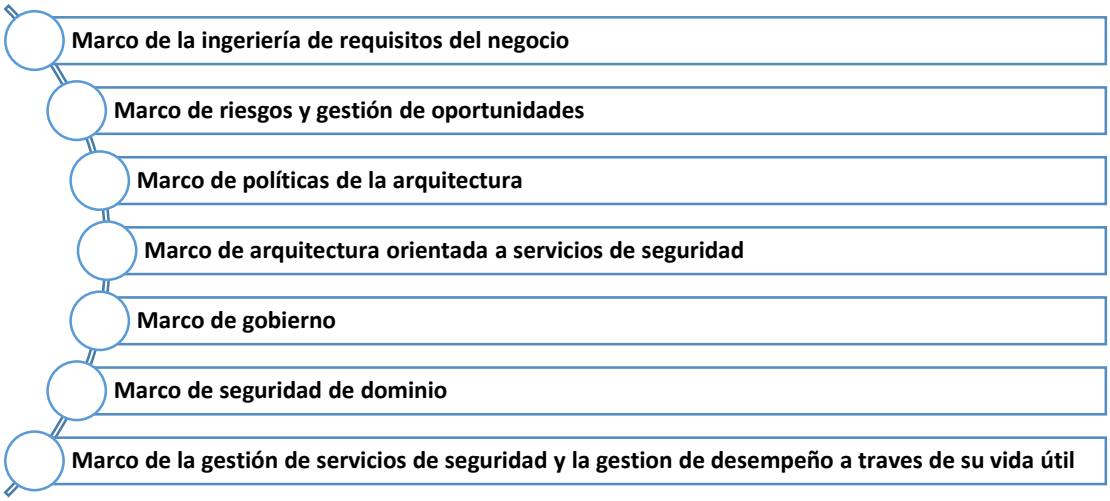

Figura 13 – Marcos Incluidos dentro de la aplicación de SABSA

Fuente: Adaptado y Traducido de (SABSA, 2013)

De acuerdo al artículo de (Sherwood, Clark, & Lynas, 2009), el modelo de SABSA consta de seis capas, resumida en la Figura 14 que se muestra a continuación:

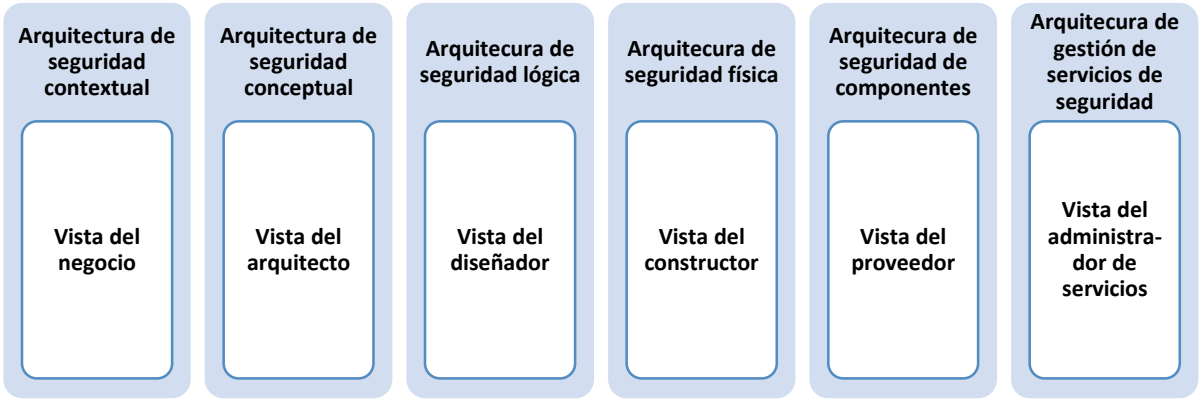

Figura 14 – Vista de la arquitectura en capas de SABSA

Fuente: Adaptado y Traducido de (Sherwood, Clark, & Lynas, 2009)

SABSA posee su modelo de ciclo de vida (ver Figura 15), el cual está formado por cuatro actividades, en donde las capas contextuales y conceptuales se agrupan dentro de la actividad de estrategia y planificación; las otras cuatro capas de arquitectura lógica, física, de componentes y de gestión de servicios se encuentran agrupadas dentro de la actividad de diseño, las otras dos actividades son implementación, y gestionar y medir

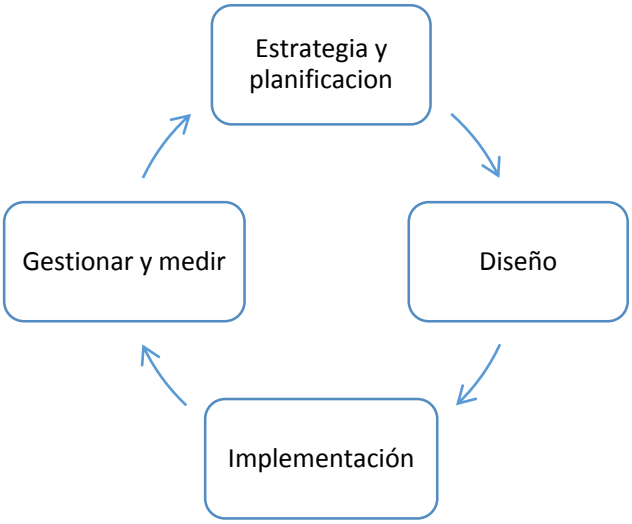

Figura 15 – Ciclo de vida de SABSA

Fuente: Adaptado y Traducido de (The Open Group and The SABSA Institute, 2011)

2.6.3. Integración de TOGAF y SABSA.

Como se ha visto en los apartados anteriores sobre el ADM de TOGAF como un método para obtener AE específicas para organizaciones, y sobre SABSA como un marco enfocado en el desarrollo de arquitecturas de seguridad empresarial, se encuentra desarrollado un documento por parte de The Open Group[9] y SABSA Institute[10], para la integración de ambos marcos de trabajo, tomando el ADM de TOGAF como el punto clave para integrar la arquitectura de seguridad, de esta forma se pude obtener el mapeo de las fases de ADM y el ciclo de vida de SABSA, como se muestra en la Figura 16.

De acuerdo al documento de (The Open Group and The SABSA Institute, 2011), la visión y propósito de la integración de ambos marcos de trabajo es “apoyar a los arquitectos empresariales que necesitan tomar en cuenta la gestión del riesgo operacional, proporcionando orientación, que describe cómo TOGAF y SABSA se pueden combinar de tal manera que el riesgo de negocio y el enfoque de la arquitectura de seguridad de SABSA, promovida por las oportunidades, se pueden integrar perfectamente en la estrategia de TOGAF impulsada por el negocio y enfocada para desarrollar una AE más completa y rica”

[9] http://opengroup.org
[10] http://www.sabsa.org/node/23

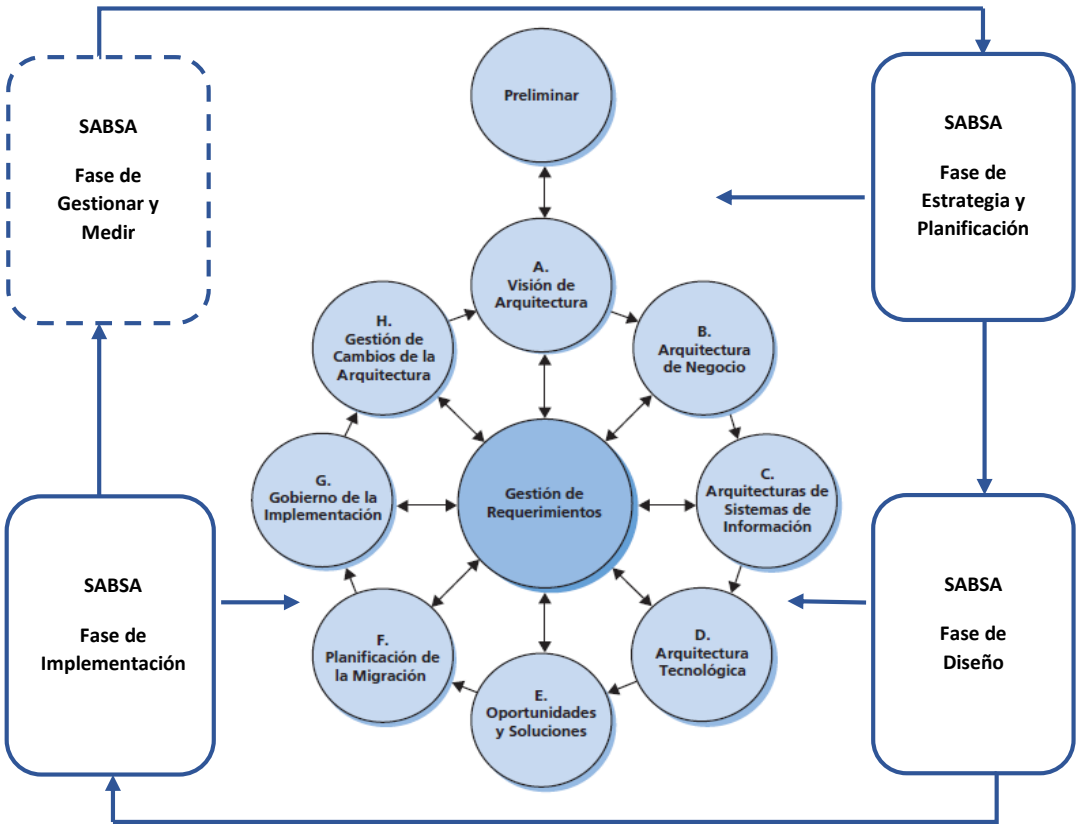

Figura 16 – Ciclo de vida de SABSA relacionado con las fases del ADM de TOGAF

Fuente: Traducido y adaptado de (The Open Group and The SABSA Institute, 2011)

SABSA Atributos del Perfil del Negocio

De acuerdo a (SABSA, 2013), el atributo del perfil del negocio "es la técnica de ingeniería de requerimientos que hace de SABSA verdaderamente único y proporciona el enlace entre los requerimientos del negocio y el diseño de la tecnología y/o procesos"

El atributo del perfil de negocio de SABSA, puede ser utilizada en el contexto del ADM de TOGAF, la alineación de los servicios a través de los atributos de negocio (ver Figura 17), se puede llevar a cabo utilizando los artefactos de TOGAF

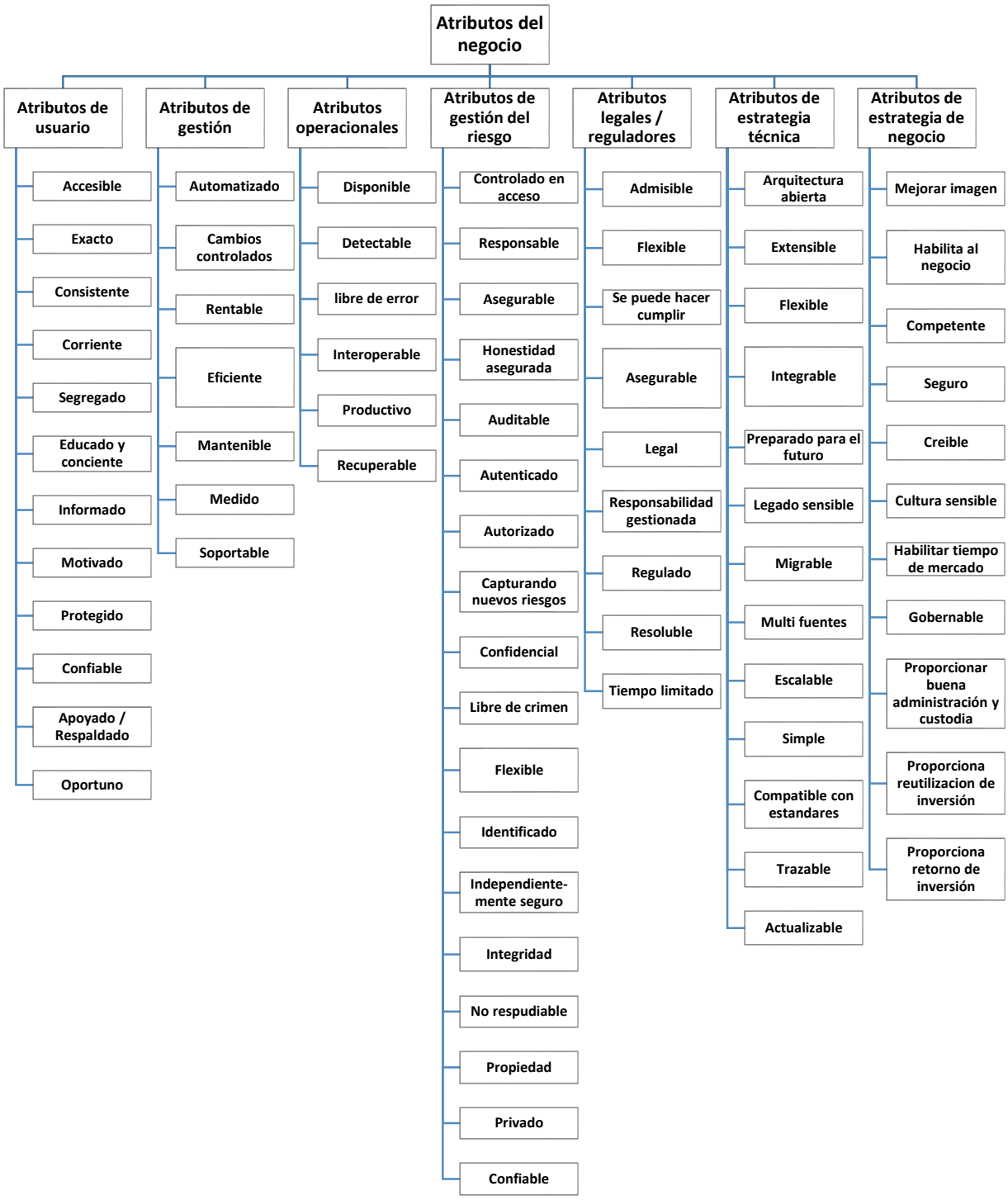

Figura 17 – Taxonomía SABSA - Atributos de negocio

Fuente: Traducido y adaptado de (The Open Group and The SABSA Institute, 2011)

Los atributos de negocio de acuerdo a (The Open Group and The SABSA Institute, 2011), son “una abstracción de los requisitos de negocio reales de los bienes encontrados previamente en varias organizaciones; la mayor parte fueron encontrados muchas veces, este ejemplo de taxonomía ha surgido de varios años de trabajo de consultoría, y proporciona definiciones genéricas para cada elemento de la taxonomía”, lo cual indica que el mismo no es solo un

ejemplo sino un marco de referencia que puede ayudar en la definición de requisitos de seguridad.

Artefactos que conforman una arquitectura de seguridad empresarial

TOGAF incorpora los componentes relevantes de SABSA en las fases de ADM, en donde se utiliza un conjunto de conceptos y artefactos; una descripción completa de los artefactos de SABSA dentro del ADM de TOGAF se puede ver en la Figura 18, en donde también se observa cuales se pueden utilizar para ciberseguridad.

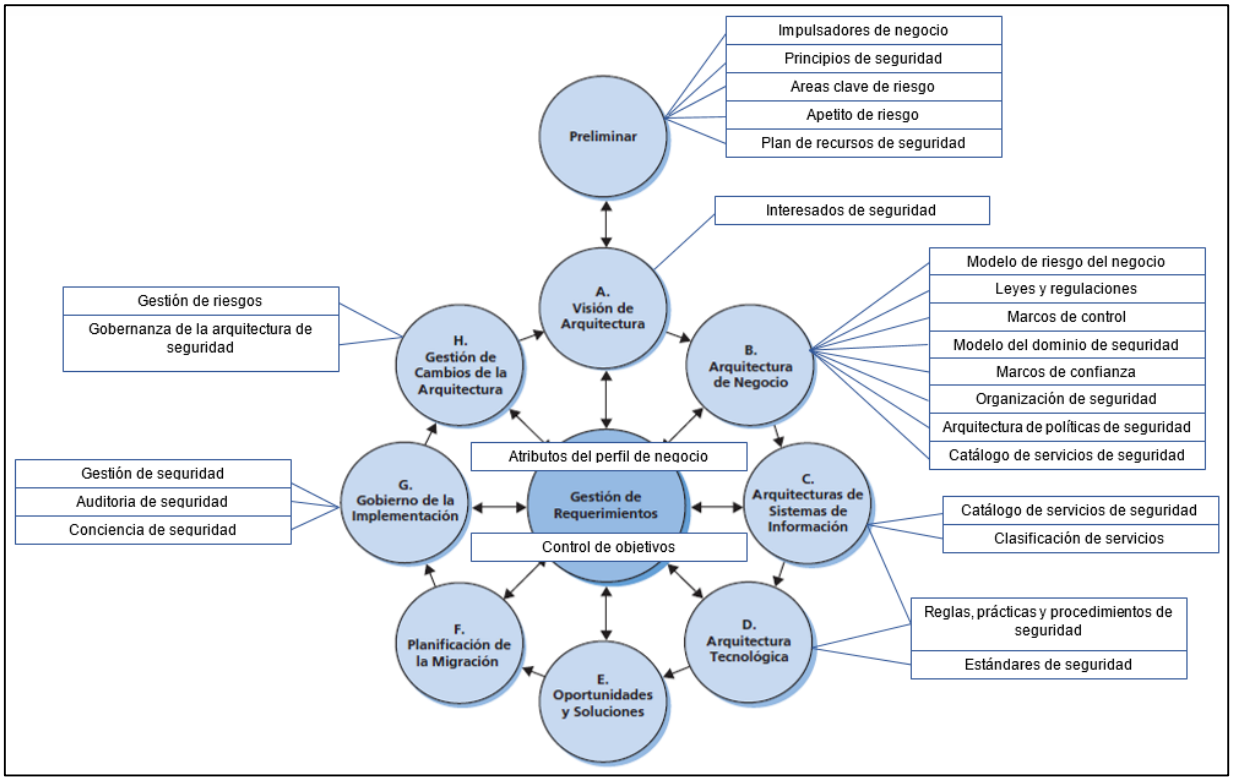

Figura 18 – Descripción de los artefactos relacionados con la seguridad en el ADM de TOGAF

Fuente: Tomado y Adaptado de (The Open Group and The SABSA Institute, 2011)

2.7. Marcos de trabajo y guías de riesgos de TI.

2.7.1. Marco de riesgos de TI.

Conforme se cita en el marco de riesgos de TI (ISACA, 2009), el marco de riesgos de TI "rellena la brecha entre los marcos genéricos de gestión de riesgos y los marcos detallados de gestión de riesgos de TI (principalmente relacionados con la seguridad). Proporciona una vista completa de extremo a extremo de todos los riesgos relacionados con el uso de TI y un tratamiento similar a fondo de la gestión del riesgo. En resumen, el marco permitirá a las organizaciones comprender y gestionar todos los tipos importantes de riesgo de TI, basándose en los componentes existentes de riesgo relacionados dentro de los marcos actuales de ISACA, es decir, COBIT y Val IT."

De acuerdo al marco de riesgos de TI (ISACA, 2009) y como se muestra en la Figura 19, “los riesgos de TI son un componente del universo de riesgos a los que está sometida una organización”

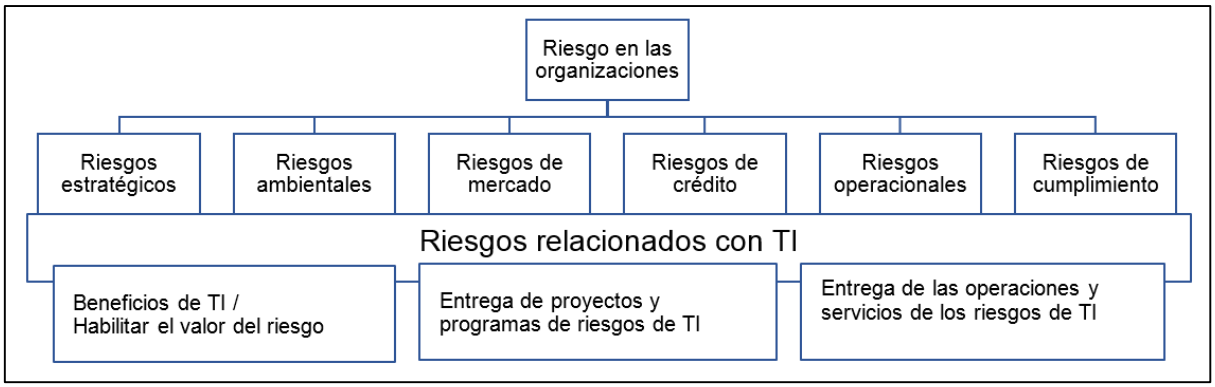

Figura 19 – Riesgos de TI en la jerarquía de riesgos

Fuente: Tomado y adaptado del marco de riesgos de TI (ISACA, 2009)

2.7.2. Guía profesional de riesgos de TI.

De acuerdo a (ISACA, 2009), la guía profesional de riesgos de TI (The Risk IT Practitioner Guide), “contiene una orientación práctica y detallada sobre cómo llevar a cabos algunas de las actividades principales que se describen en el modelo de proceso” del marco de riesgos de TI.

En este modelo de proceso de acuerdo a (ISACA, 2009), “se hacen múltiples referencias al análisis de riesgos, análisis de escenarios, responsabilidades, indicadores clave de riesgo y muchos otros términos relacionados con el riesgo”

2.8. Leyes y regulaciones.

Uno de los componentes para el control de la seguridad de la información y que también se puede aplicar dentro de la ciberseguridad son las leyes y regulaciones que rigen en cada país, dentro de Ecuador existe el código orgánico integral penal (COIP) que dispone de un conjunto de artículos y secciones que se deben tomar en consideración para su cumplimiento.

2.8.1. Código orgánico integral penal.

De acuerdo al (Ministerio de Justicia, Derechos Humanos y Cultos, 2014), el COIP, “tiene como finalidad normar el poder punitivo del Estado, tipificar las infracciones penales, establecer el procedimiento para el juzgamiento de las personas con estricta observancia del debido proceso, promover la rehabilitación social de las personas sentenciadas y la reparación integral de las víctimas”

La sección a la que se debe prestar mayor atención, es la SECCION TERCERA la cual corresponde a delitos contra la seguridad de los activos de los sistemas de información y

comunicación, en donde se pueden observar los siguientes artículos del COIP (Ministerio de Justicia, Derechos Humanos y Cultos, 2014):

- Art. 229.- Revelación ilegal de base de datos
- Art. 230.- Interceptación ilegal de datos.
- Art. 231.- Transferencia electrónica de activo patrimonial
- Art. 232.- Ataque a la integridad de sistemas informáticos
- Art. 233.- Delitos contra la información pública reservada legalmente.
- Art. 234.- Acceso no consentido a un sistema informático, telemático o de telecomunicaciones.

2.9. Contexto de aplicación de ciberseguridad para arquitectura empresarial.

La inclusión de ciberseguridad en una AE es un tema complejo dentro de una organización, pues el manejo de riesgos de seguridad, la continuidad del negocio, y la gestión de cambios son aspectos que intervienen al momento de alinear tecnología con los objetivos del negocio, de acuerdo al estudio realizado por (Bloomberg, 2013), “un axioma fundamental de la seguridad es que no podemos manejar el riesgo a cero, es decir el costo de la gestión de seguridad es alto y el presupuesto para responder a la seguridad se debe manejar de forma equilibrada”; debido a la naturaleza cambiante de los diferentes tipos de riesgos, se identifican y utilizan ciertos marcos de trabajos y normas que aportan controles y procedimientos que intervienen y colaboran dentro del contexto de ciberseguridad para AE (ver Figura 20)

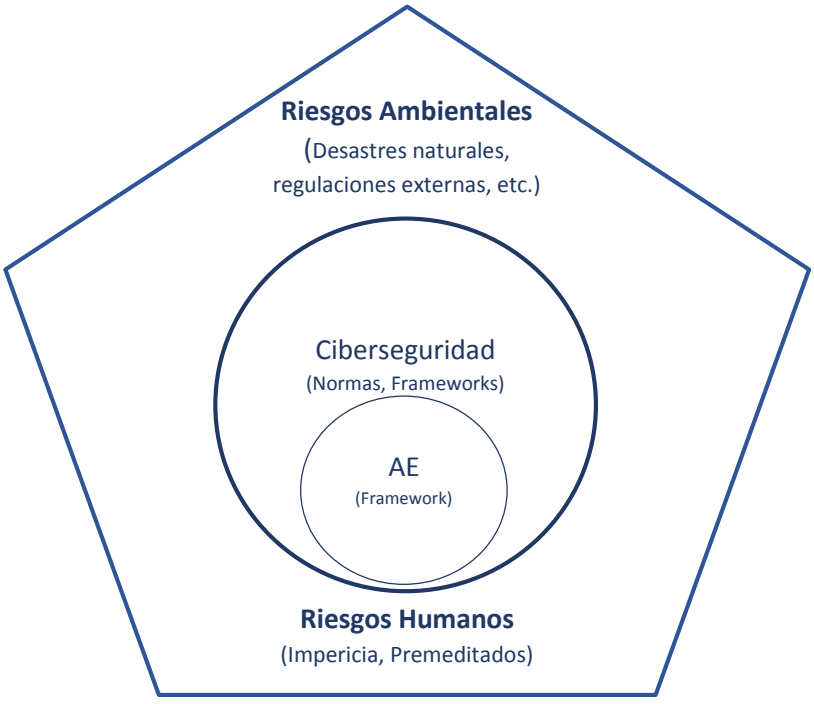

Figura 20 – Contexto de Ciberseguridad en AE

Fuente: (Autor, 2014)

Al momento de implementar ciberseguridad en una AE es necesario identificar los componentes disponibles, faltantes y los que se pueden mejorar, los cuales se traducen en los principios básicos de AE (arquitectura de negocio, arquitectura de información, arquitectura de aplicaciones y arquitectura tecnológica); de esta forma se pueden establecer los controles y procesos que fortalezcan cada uno de dichos componentes, reduciendo riesgos que afecten la continuidad del negocio.

Otro punto importante para tratar la ciberseguridad en la construcción de una AE clara es el uso de un marco de trabajo que ofrezca la posibilidad de adaptarse a otros para así enfrentar los cambios continuos que conllevan los avances tecnológicos y cambios de regulaciones, para este punto se ha optado por seleccionar el marco de trabajo de TOGAF.

En la implementacion de ciberseguridad para una AE, surgen otros aspectos que se deben tratar y es el, ¿qué va a suceder con las organizaciones que no tienen una AE definida formalmente para implementar ciberseguridad?, la respuesta a esta incógnita es que la guía implementará un modelo basado únicamente para AE de acuerdo al modelo del ADM de TOGAF a través de su proceso iterativo y de mejora para guiar a los interesados.

Es significativo tomar en cuenta que en la implementación de una AE, la ayuda de un marco de trabajo, fortalece los sistemas de información de la organización, y hace que sea fácil acoplar normas como las estudiadas en el presente documento (ISO 27001, ISO 27032, COBIT 5 y NIST), su aplicación aporta en que exista un funcionamiento adecuado, para satisfacer los requerimientos del negocio, reduciendo los riesgos a ciber-ataques y gestionar cada uno de ellos de la mejor manera; de acuerdo a (ISACA, 2013), en la gestión de la arquitectura de seguridad “los administradores de seguridad deben incluir los requisitos necesarios específicos para defenderse de los ataque y/o violaciones, e incluirlos en el repositorio de arquitectura, esto apoyado por las actividades estandarizadas dentro de la capacidad de servicio, como el inventario de activos, sistema de gestión de la configuración y servicios de descubrimiento de infraestructura. En la gestión de la ciberseguridad, estos elementos deben ser considerados como las capacidades existentes dentro de la organización. Esto incluye los atributos y objetivos más detallados de la capacidad de servicios basado en la arquitectura”

Un aspecto que no se debe dejar de lado, es la colaboración por parte de la dirección de la organización dentro de las decisiones referentes a ciberseguridad, haciendo cumplir e ir informando continuamente las políticas y normas que actúan dentro de la organización.

CAPÍTULO III

GUÍA DE CIBERSEGURIDAD PARA ARQUITECTURA EMPRESARIAL

3.1 Introducción.

Uno de los activos más importantes dentro de las organizaciones es la información, lo que lleva a identificar cada uno de los componentes o tecnologías que interactúan con ella, debido a esto se deben tomar las medidas necesarias para protegerlas, desde este enfoque se propone la presente guía bajo la necesidad de implementar ciberseguridad en una AE, la misma que consta de un proceso guiado a través de fases para planificar, diseñar, implementar y medir los controles o actividades en una organización, cada una de las fases posee sus actividades las mismas que trabajaran con determinados artefactos (plantillas) que permiten la gestión adecuada del alcance y los objetivos planteados por la organización.

3.2 ¿A quién va dirigida la guía?.

La guía va dirigida a aquellas organizaciones que tienen implementada una AE formalmente, debido a que la misma posee un conjunto de capacidades basadas en una estructura organizada y en constante mejora de sus componentes, que son un aspecto clave en la protección contra ciberataques hacia los sistemas de información.

Los arquitectos o directores de seguridad encargados de la ciberseguridad, deben utilizar esta guía apoyados por las capacidades arquitectonicas (p. ej. inventario de activos, sistema de gestión de la configuración (CMS)[11], partes interesadas, etc.) de la AE, para así evitar la duplicación de esfuerzos y que todo su trabajo este alineado con la arquitectura ya definida.

3.3 Beneficios de la guía.

- La guía considera la protección de la confidencialidad, integridad y disponibilidad de los sistemas de información contra ciberataques.
- Propone un conjunto de actividades por fases, para la mejora y gestión de los niveles de seguridad basada en el ADM de TOGAF, junto a los controles, procedimientos y actividades de ciberseguridad.
- Motiva a la organización para trabajar de una manera coordinada con los procesos y controles de ciberseguridad y AE.

3.4 Desarrollo de la guía de ciberseguridad en una arquitectura empresarial.

La guía está desarrollada bajo el ADM (método de desarrollo de arquitectura) de TOGAF integrada con el ciclo de vida de SABSA (ver Figura 21), en donde se utiliza un conjunto de actividades para cada una de las fases; dentro de las actividades se incluye la orientación

[11]ITIL, El CMS y usted - ¿Qué es un CMS?
http://documents.bmc.com/products/documents/26/59/92659/92659.pdf

necesaria para la implementación de ciberseguridad, y la gestión de los controles para la protección de los sistemas informáticos contra ciberataques.

La guía esta desarrollaba mediante una matriz (ver Tabla 4) que proporciona las actividades por cada fase del ADM de TOGAF, las cuales ayudan en el proceso del trabajo de ciberseguridad para AE; las actividades se encuentran referenciadas con los debidos controles y actividades de normas y marcos de trabajo, las cuales han sido investigados para el desarrollo de la guía.

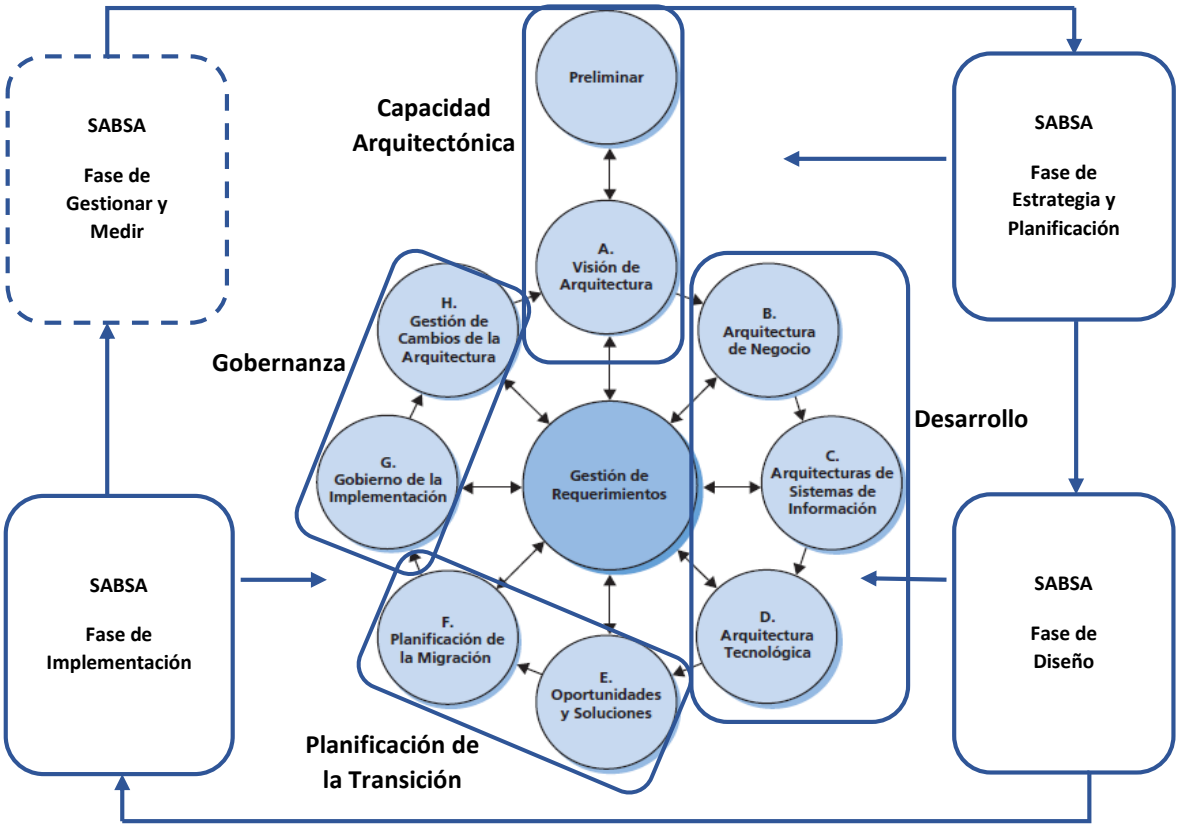

Figura 21 – Ciclo de trabajo del ADM de TOGAF y SABSA, e interacción entre fases

Fuente: Traducido y adaptado de (The Open Group and The SABSA Institute, 2011)

En cada una de las fases del ADM que se detallan a continuación, se han adaptado los conceptos y características que son necesarias en la implementación de ciberseguridad para la AE:

Gestión de requerimientos (RM): trabaja mediante un proceso dinámico en donde se gestiona los atributos del perfil de negocio y los requerimientos de ciberseguridad obtenidos de las partes interesadas, junto a la solución propuesta de dichos requerimientos para cada una de las fases del ADM.

Preliminar (PP): trabaja en la preparación de la organización para la implementación del trabajo de ciberseguridad, en donde se toma dos aspectos principales como los principios de

ciberseguridad y los marcos de trabajo que se van a utilizar incluyendo el de arquitectura, además se decide que artefactos de ciberseguridad son necesarios en la arquitectura y quien los creará.

A. Visión de arquitectura (AV): a través de esta fase se describe de forma inicial las fases B, C y D, por medio de la identificación de los requerimientos, e interesados, para determinar qué es lo que se desea realizar o alcanzar con la ciberseguridad.

B. Arquitectura del negocio (BA): determina los controles, leyes y marcos de confianza independientemente de Tecnologías de información que se encuentran dentro de la arquitectura.

C. Arquitectura de sistemas de información (ISA): esta fase comprende la arquitectura de datos y la arquitectura de aplicación, en donde se establece el estado actual y un estado objetivo, además de un análisis de brechas entre ambos estados; para datos se determina su estructura física y lógica, y para aplicación las interacciones entre sistemas y la relación con los procesos de negocio

D. Arquitectura tecnológica (TA): esta fase determina que estándares de seguridad son necesarios para la protección los componentes tecnológicos que soporta los SI.

E. Oportunidades y soluciones (OS): en esta fase se evalúa y determina la importancia de la implementación de los proyectos y procesos más significativos de ciberseguridad para la AE.

F. Planificación de la migración (MP): esta fase aborda los riesgos, beneficios, costos y controles asociados a la transición desde el estado actual al estado objetivo

G. Gobierno de la implementación (IG): asegura que la implementación del proyecto esté de acuerdo a lo planificado, y que se garantice que los procesos y sistemas se adhieran a la arquitectura de seguridad o seguridad de la información en general, evitando riesgos inaceptables

H. Gestión de cambios de la arquitectura (ACM): monitorea y controla continuamente que el trabajo de ciberseguridad responde a las necesidades de la organización, y que los cambios que ha surgido se gestionen de manera controlada para que no causen un impacto negativo dentro de la arquitectura

Los artefactos que trabajan con las actividades de cada fase, se respaldan en un conjunto de plantillas, cuyo modelo y diseño está desarrollado mediante las técnicas y conocimientos recopilados por el apoyo de marcos de trabajos y normas de ciberseguridad, los cuales fueron citados y estudiados previamente.

Tabla 4. Gestión y control de requerimientos – Guía de ciberseguridad para arquitectura empresarial

Fase	Actividad	Recomendación basada en Ciberseguridad
Gestión de requerimientos (RM)	**Identificar los atributos del perfil de negocio para ciberseguridad**	Identificar los atributos del perfil de negocio para Ciberseguridad, los mismos que ayudan a determinar el nivel de protección que es requerido en los sistemas de información (SI), y a controlar los límites y el alcance del trabajo de ciberseguridad. Para determinar estos atributos utilice como referencia la taxonomía de atributos de negocio de SABSA que se explica en la Figura 17, estos atributos determinaran las expectativas y objetivos de calidad en cada una de las fases del ADM para el trabajo de ciberseguridad. Se debe obtener como salida de esta actividad una lista de los atributos del perfil de negocio para ciberseguridad, que ayudará como una referencia y punto de control de la fase de gestión de requerimientos. Para recopilar los atributos del perfil de negocio identificados, utilizar la **plantilla de la actividad de atributos del perfil de negocio para ciberseguridad**
	Control de requerimientos	Tener en claro los requerimientos de ciberseguridad, para determinar el alcance de su trabajo para la AE, esta actividad va ligada a los requerimientos de ciberseguridad que se definen desde la fase de visión de arquitectura a través de las partes interesadas, y que continua a lo largo de todo el proceso del ADM. El control de los requerimientos es necesario debido a que los mismos están sujetos a cambios que pueden surgir durante las actividades de las fases del ciclo del ADM. El entendimiento de estos requerimientos hace que el trabajo de ciberseguridad sea claro y específico, para que su implementación no se salga de control. En el marcos de trabajo de TOGAF 9.1, dentro del capítulo 17 de Gestión de requerimientos de arquitectura (ADM Architecture Requirements Management) se puede encontrar información sobre los mismos (p. ej. Objetivos, enfoque, entradas, pasos y salidas), que ayudan en la gestión de requerimientos para la AE, los cuales se los puede destinar para controlar los requerimientos de ciberseguridad. Utilizar la **plantilla de la actividad de control de requerimientos**, para realizar el respectivo control de requerimientos al momento de generarse un cambio, ya sea por alguna nueva petición, o debido a que se pasó por alto algún requerimiento, los mismos deben ser evaluados por las partes interesadas para no sobrecargar el trabajo de ciberseguridad.

Fuente: (Autor, 2014)

Capacidad Arquitectónica.

Tabla 5. Iteración de capacidad arquitectónica – Guía de ciberseguridad para arquitectura empresarial

Fase	Actividad	Recomendación basada en Ciberseguridad
Preliminar (PP)	**Identificar los principios de ciberseguridad**	Identificar los principios de ciberseguridad, para tener una idea clara sobre el trabajo de la misma y dar respuesta a los ataques y/o violaciones dentro del dominio de ciberseguridad (ciberataques), estos principios de ciberseguridad se encuentran relacionados con la tolerancia al riesgo por parte de la organización. Para identificar los principios de ciberseguridad utilizar como modelo COBIT 5 (Transformando la ciberseguridad usando COBIT 5), en el apartado de principios de seguridad de la información, el cual posee un conjunto genérico de principios de ciberseguridad, que han sido traducidos con el objetivo de especializarlos dentro del área de ciberseguridad. Otro documento importante, que es necesario utilizar como modelo para determinar los principios de ciberseguridad es el marcos de trabajo de TOGAF 9.1, a través del capítulo 23 de principios de arquitectura, el cual proporciona ayuda basada en las características, componentes, desarrollo y aplicación de principios a ser desarrollados en la AE. La salida de esta actividad es una lista de los principios de ciberseguridad, la cual se puede diseñar de acuerdo a los componentes sugeridos por TOGAF 9.1 o basada en COBIT 5. Utilizar la **plantilla de la actividad de principios de ciberseguridad**, para los principios de ciberseguridad identificados.
	Definir el equipo de ciberseguridad	Definir el equipo de ciberseguridad con sus debidos roles y responsabilidades, quienes son requeridos para el trabajo de ciberseguridad. Se puede determinar el equipo, basado en el número de recursos requeridos, el perfil profesional y otros requisitos técnicos que son necesarios para las actividades de ciberseguridad. El documento obtenido como resultado tangible de este proceso se lo puede elaborar a través del White Paper de la integración de SABSA y TOGAF en el apartado del plan de recursos de seguridad (Security Resource Plan), que proporciona un conjunto de preguntas que se pueden utilizar como pasos para determinar los recursos de ciberseguridad, además basarse en el proceso (APO01.02) de COBIT 5 (TCS)

		dentro de la figura del mapeo de procesos APO, para establecer los roles y responsabilidades de ciberseguridad. Utilizar la **plantilla de la actividad del equipo de ciberseguridad**, para definir el equipo de ciberseguridad
	Determinar los marcos de referencia para ciberseguridad	Determinar los marcos de referencia que son necesarios y que mejor satisfacen las necesidades del trabajo de ciberseguridad en la AE. Se define a TOGAF 9.1 como el marco principal de arquitectura, y COBIT 5 como marco de ciberseguridad, ambos se encuentran relacionados con SABSA el cual interviene en la seguridad de AE, si es necesario se deben incluir otros marcos que faciliten el trabajo de ciberseguridad, los cuales generan como salida una lista de marcos de referencia para ciberseguridad, con el detalle de sus características de trabajo. Dentro del marco de trabajo de TOGAF 9.1 en el apartado de utilizando TOGAF con otros marcos (2.10 Using TOGAF with other frameworks) y en el White Paper de la integración de SABSA y TOGAF en el apartado de marcos de control (Control Frameworks) se pueden encontrar los puntos a considerar sobre la adaptación con otros marcos de referencia a utilizar dentro de la implementación de ciberseguridad en la AE. Utilizar la **plantilla de la actividad de marcos de referencia para ciberseguridad**, para la adaptación de marcos de referencia para ciberseguridad.
	Identificar las áreas de riesgo	Identificar las áreas de riesgo, estas son las que determinan el alcance del trabajo de ciberseguridad, y que se encuentran relacionadas con las oportunidades de negocio. Las áreas de riesgo son una de las causas para implementar ciberseguridad sobre los Sistemas de Información (SI), que se encuentran dentro del área de trabajo de AE. Para determinar cuáles son las áreas de riesgo, se debe identificar el conjunto de servicios que interactúan dentro del ciberespacio, en donde se transfiere información que es considerada crítica, lo que conlleva a definir el nivel de criticidad que tienen dichos servicios. Durante esta actividad se debe generar el documento de las áreas de riesgo, para lo se sugiere utilizar el marco de riesgos de TI de ISACA (RG1.1) junto a la guía para el especialista (The Risk IT Practitioner Guide) donde se identifican un conjunto de conceptos y prácticas (p. ej. RG1.1 desarrolla en una empresa el marco específico de gestión de riesgos TI) para la gestión de riesgos, o también puede basarse el modelo de riesgos que posee la organización. Utilizar la **plantilla de la actividad de áreas de riesgo**, para la identificar las áreas de riesgos.

Visión de arquitectura (AV)	**Identificar las partes interesadas de ciberseguridad**	Identificar las partes interesadas de ciberseguridad de las cuales se obtienen los requisitos necesarios para su implementación sobre la AE. Así mismo es importante identificar los interesados del negocio, quienes deben tener claros los beneficios y los principios de ciberseguridad, debido a que proveen el presupuesto para implementar de todo lo referente a ciberseguridad, lo cual está relacionado con la protección de los SI de la organización. Para determinar los interesados y desarrollar el documento de los mismos, utilizar el marco de trabajo de TOGAF 9.1 basado en el capítulo de gestión de interesados (24. Stakeholder Management), donde existen las técnicas para identificarlos. Normalmente para determinar a las partes interesadas de ciberseguridad se debe tomar en cuenta el nivel de influencia y poder de los mismos, así como las distintas necesidades de protección en el día a día que pueden requerir, del proyecto de ciberseguridad. Utilizar la **plantilla de la actividad de las partes interesadas de ciberseguridad**, para identificar a las partes interesadas
	Definir los requerimientos de ciberseguridad	(Esta actividad se encuentra relacionada con las partes interesadas de ciberseguridad AV:CSS y el Control de requerimientos RM:RC) Obtener los requerimientos de las partes interesadas para determinar el alcance del trabajo de ciberseguridad sobre la AE, en donde se realiza un análisis sobre dichos requerimientos y se los establece de forma clara, para poder basarse en ellos sin que generen confusión que afecten el trabajo de ciberseguridad. El proceso de identificación de requerimientos de ciberseguridad es necesario para saber qué servicios requieren protección de ataques informáticos o ciberataques, el levantamiento de los mismo se los puede realizar a través de entrevistas, prototipos, modelado (p. ej. UML), etc. Utilizar COBIT 5 (TCS) a través de la sección de Gobernanza de ciberseguridad, en el dominio de EDM para determinar las actividades y requerimientos de ciberseguridad (EDM05.01, EDM02.01), y el proceso mapeado DSS (DSS01.02) Se sugiere utilizar TOGAG 9.1, conforme se explica en la sección de desarrollo de requerimientos (17.2.2 Requirements Development) como técnica, para definir los requisitos, aunque este marco de trabajo está especializado en requerimientos de arquitectura, ofrece una guía para obtener requisitos que se pueden orientar a ciberseguridad.

		Utilizar la **plantilla de la actividad de requerimientos de ciberseguridad**, para identificar los requerimientos de ciberseguridad.
	Adaptar el marco de referencia de ciberseguridad	(Esta actividad se encuentra relacionada con los marcos de referencia de ciberseguridad PP:CSF) Determinar los marcos de referencia que mejor satisfacen las necesidades de ciberseguridad y AE durante toda esta fase y con los cuales se va a trabajar, por tal motivo es importante entender y conocer que actividades intervienen en la Visión de Arquitectura. Se define a TOGAF 9.1 como el marco principal de arquitectura, y COBIT 5 como marco de ciberseguridad y riesgos, ambos se encuentran relacionados con SABSA el cual interviene en la seguridad de AE, si es necesario se deben incluir otros marcos que faciliten el trabajo de ciberseguridad, los cuales generan como salida una lista de marcos de referencia para ciberseguridad, con el detalle de sus características de trabajo. Dentro del marco de trabajo de TOGAF 9.1 en el apartado de utilizando TOGAF con otros marcos (2.10 Using TOGAF with other frameworks) y en el White Paper de la integración de SABSA y TOGAF en el apartado de marcos de control (Control Frameworks) se pueden encontrar los puntos a considerar sobre la adaptación con otros marcos de referencia, para utilizar dentro de la implementación de ciberseguridad en la AE. Utilizar la **plantilla de la actividad de marco de referencia de ciberseguridad adaptado**, para la adaptación de marcos de referencia para ciberseguridad

Fuente: (Autor, 2014)

Desarrollo.

Tabla 6. Iteración de desarrollo – Guía de ciberseguridad para arquitectura empresarial

Fase	Actividad	Recomendación basada en Ciberseguridad
Arquitectura del negocio (BA)	**Establecer el modelo de riesgo de negocio**	Establecer o identificar el modelo de riesgos que utiliza el negocio, para determinar cuál es el costo de la perdida/impacto en caso de que ocurra algún evento (ataque/falla) de ciberseguridad. El modelo de riesgo organizacional es una herramienta útil, manejada como estrategia para la evaluación de riesgos, basado en amenazas identificadas, las probabilidades de materializarse y el impacto que puede causar un incidente. Se sugiere el uso del marco de riesgos de TI que contiene un repertorio de dominios y procesos ligados al gobierno de riesgos corporativos, basarse en el apartado del panorama del modelo de proceso del marco de riesgo de ti, el cual proporciona una visión general de los procesos de negocio a través de los riesgos de TI de acuerdo a tres ámbitos: gobernanza del riesgo, evaluación de riesgos y el riesgo de respuesta. Utilizar junto al marco de riesgos de TI, la Guía para el especialista de ISACA (The Risk IT Practitioner Guide), que contiene las indicaciones prácticas y detalladas (p. ej. Enterprise IT Risk Assessment Form) de cómo realizar las actividades del marco de riesgos de TI. El modelo de riesgos de negocio se deberá utilizar para la gestión eficaz de los riesgos de TI, la clasificación de la información con el objetivo de determinar el riesgo que la organización está dispuesta a aceptar, y determinar el propietario de dicha información quien es el que decide las medidas de mitigación para su información, como por ejemplo: aceptar, transferir, evitar, reducir o mitigar. Utilizar la **plantilla de la actividad de modelo de riesgos de negocio**, para establecer el modelo de riesgos de negocio.

	Identificar leyes y regulaciones ligadas a ciberseguridad	Identificar que leyes o regulaciones influyen dentro del ámbito de la ciberseguridad o que se encuentran ligadas hacia la misma, dentro de la legislación Ecuatoriana estas leyes o regulaciones pueden favorecer o restringir ciertas actividades por parte de los usuarios (personas, aplicaciones), en el caso de Ecuador se puede observar como ejemplo el Código Orgánico Integral Penal (EC) - SECCIÓN TERCERA - Delitos contra la seguridad de los activos de los sistemas de información y comunicación. Para determinar la información necesaria de esta actividad y generar una salida tangible (documento), se debe identificar la ley, o regulación y determinar dentro de las mismas la sección y el/los artículo(s) correspondiente(s) que están asociados o que se pueden asociar a la ciberseguridad. Utilizar la **plantilla de la actividad de leyes y regulaciones ligadas a ciberseguridad**, para identificar las leyes y regulaciones de ciberseguridad
	Adaptar el marco de referencia para ciberseguridad	(Esta actividad se encuentra relacionada con los marcos de referencia de ciberseguridad) Determinar con que marcos de referencia se va a trabajar durante esta fase, por este motivo, es importante entender y conocer que actividades intervienen dentro de la Arquitectura del negocio. Una vez que se establece lo que se va a hacer, se pueden listar los marcos de referencia con los que se va a trabajar y así adaptar el marco de referencia para ciberseguridad. Dentro del marco de trabajo de TOGAF 9.1 en el apartado de utilizando TOGAF con otros marcos (2.10 Using TOGAF with other frameworks) y en el White Paper de la integración de SABSA y TOGAF en el apartado de marcos de control (Control Frameworks) se pueden encontrar los puntos a considerar sobre la adaptación con otros marcos de referencia, para utilizar dentro de la implementación de ciberseguridad en la AE. Utilizar la **plantilla de la actividad de marcos de referencia para ciberseguridad**, para la adaptación de marcos de referencia para ciberseguridad
	Determinar el modelo del dominio de ciberseguridad	Determinar el modelo del dominio de ciberseguridad, para obtener una descripción grafica de la relación entre los distintos dominios, partes y actores, además del detalle de dichas relaciones y dominios, que se encuentran dentro del ámbito de la ciberseguridad y que están alineados con el modelo de negocio. La definición del modelo de dominio de ciberseguridad ayuda a identificar las áreas de responsabilidad, y los niveles de seguridad que requieren las mismas, dentro del White Paper de la integración de SABSA y

		TOGAF, en el apartado del modelo del dominio de seguridad (Security Domain Model) también se enfatiza sobre la definición de este modelo para el trabajo de seguridad sobre la AE. Para el diseño del modelo de dominio es necesario conocer la relación entre los Sistemas de Información, tanto internamente como externamente, y definir el tipo de seguridad que utilizan estas relaciones junto a su criticidad, para de esta forma sugerir un mejor modelo o mantener el mismo si es el adecuado. La salida tangible de esta actividad es el modelo del dominio de ciberseguridad con el detalle técnico de cada una de sus entidades, relaciones y dominios que se mencionan en un principio. Utilizar la **plantilla de la actividad de modelo del dominio de ciberseguridad**, para determinar el modelo de dominio de ciberseguridad
	Identificar los protocolos de confianza	(Esta actividad está relacionada con el modelo de dominio de ciberseguridad BA:CSDM) Identificar los protocolos de confianza que son utilizados en la relación con entidades externas, los mismo que deben estar apoyados por acuerdos legales, contratos y/o políticas de ciberseguridad Las relaciones de confianza pueden ser: unidireccional, bidireccional o inexistente. Para determinar los protocolos de confianza se debe saber que entidades están relacionadas y de qué forma se está protegiendo el enlace (descripción técnica) que conecta a una entidad con la otra. Utilizar los controles (A.13.1.1, A.13.1.2, A.13.2.1) de la norma ISO 27001:2013 y las categorías y subcategorías (ID.AM-3) del marco de trabajo de NIST (CS-IC), estos documentos proporcionan controles y actividades (subcategorías) para la protección de los protocolos de confianza, en cuanto a la protección de telecomunicaciones y flujo de datos. La salida de esta actividad se basa en un documento donde se detalle las relaciones de confianza entre entidades y sobre que protocolos de confianza (p. ej. SLAs[12]) existen las mismas. Utilizar la **plantilla de la actividad de los protocolos de confianza,** para identificar los protocolos de confianza aplicados a ciberseguridad.
	Determinar la organización de ciberseguridad	La organización de ciberseguridad determina los procesos para la gestión de riesgos que afectan a la seguridad de la información, en donde se establece la propiedad de los riesgos, responsabilidades y el proceso de gestión de ciberseguridad.

[12] service-level agreement (SLA): acuerdo a nivel de servicio (SLA), es un contrato entre un proveedor de servicios de red y un cliente, que especifica por lo general en términos mensurables los servicios que el proveedor de servicios de red proporcionará. http://searchitchannel.techtarget.com/definition/service-level-agreement

		En el proceso de gestión de ciberseguridad incluye: - Evaluación de riesgos - Definición de objetivos de control - Medidas de ciberseguridad - Informes del estado de ciberseguridad y - Gestión de incidentes. Esta actividad de organización de ciberseguridad, se la puede manejar a través de un plan de gestión de ciberseguridad o un plan de gestión de incidentes, en donde se estructuren procedimientos para cada uno de los temas del proceso de gestión de ciberseguridad antes mencionados, asignando responsabilidades mediante roles y propiedades (dueños) de los riesgos. Utilizar los controles (p. ej. A.12.2.1, A.16.1.1, A.16.1.2, A.16.1.3, A.16.1.4, A.16.1.5, A.16.1.6, A.16.1.7) de la norma ISO 27001:2013 y las categorías y subcategorías (p. ej. PR.IP-9, RS.AN-2, RS.AN-4, RS.MI-1, RS.MI-2, RS.MI-3) del marco de trabajo de NIST (CS-IC) que proporcionan una serie de controles y actividades (subcategorías) para la gestión de incidentes que se apegan a la organización de ciberseguridad. Utilizar la **plantilla de la actividad de organización de ciberseguridad**, para determinar la organización de ciberseguridad.
	Determinar la arquitectura de las políticas de ciberseguridad	Una práctica ya conocida de seguridad dentro de las organizaciones, es el uso de políticas de seguridad de la información, debido a que corrige la alineación de la gestión de riesgo operacional. La creación de políticas de ciberseguridad, traduce los principios de seguridad de la información, en elementos más manejables y entendibles sin excederse con detalles técnicos; el propósito de este documento es expresar claramente las metas y objetivos, así como los límites para la gestión y soluciones de seguridad, para lo cual se debe tomar en cuenta el tamaño de la organización y los riesgos a ciberataques, mientras más pequeña o si son menores los riesgos, menos extensas y complejas serán las políticas de ciberseguridad. Para desarrollar las políticas de ciberseguridad, hacer uso de los controles (p. ej. A.5.1.1, A.5.1.2, A.18.2.2) de la norma ISO 27001:2013, y de las categorías y subcategorías (p. ej. PR.IP-9, RS.AN-2, RS.AN-4, RS.MI-1, RS.MI-2, RS.MI-3) de NIST, cuanto a la estructura y cada una de las políticas utilizar COBIT 5 (TCS), que dentro del apartado de políticas de ciberseguridad (Cybersecurity Policy) se encuentran definidas un conjunto

		de políticas, categorizadas por área y referenciadas por las políticas de seguridad, aunque el contenido y profundidad del documento de políticas de ciberseguridad dependerá del tamaño de la organización se recomienda como modelo la estructura de políticas que se encuentra dentro del mismo apartado, la misma que es reconocida internacionalmente y se asemeja a la estructura de la norma ISO. Utilizar y adaptar la **plantilla de la actividad de la arquitectura de las políticas de ciberseguridad**, para determinar la arquitectura de las políticas de ciberseguridad.
Arquitectura de sistemas de información (ISA)	**Elaborar el catálogo de servicios de ciberseguridad**	Tener actualizado el catálogo de servicios del negocio proporciona que la identificación de los servicios de ciberseguridad sea más ágil. Los servicios de ciberseguridad dentro del catálogo, aunque sean algo intangible son aquellos que proporcionan confidencialidad, integridad y disponibilidad para los diferentes servicios del negocio, los cuales pueden ser: protección contra malware, encriptado de información, u otros. A cada uno de los servicios dentro del catálogo, se los puede detallar con un nombre que los identifique, el objetivo que cumple el servicio, el detalle técnico de la funcionalidad del servicio, y el tipo de criticidad o importancia que tiene el servicio de ciberseguridad para la organización. Se sugiere utilizar la taxonomía de aplicaciones de la plataforma (43.4 Application Platform — Taxonomy) y el detalle de la taxonomía de la plataforma (43.5 Detailed Platform Taxonomy) de TOGAF 9.1 como referencia para desarrollar la lista del catálogo de servicios de ciberseguridad que es el documento objetivo que se debe generar como salida de esta actividad. Utilizar la **plantilla de la actividad de catálogo de servicios de ciberseguridad**, para elaborar el catálogo de servicios de ciberseguridad.

	Realizar la clasificación de servicios de ciberseguridad	(Actividad relacionada con el catálogo de servicios de ciberseguridad) Realizar la clasificación de los servicios de ciberseguridad, la cual se puede basar en el esquema de clasificación organizacional o puede estar basado en el tipo de información que almacena o gestiona el servicio. La clasificación de los servicios de ciberseguridad, puede ser una tarea que se suele obviar si la cantidad de servicios no es muy grande, aunque esto quedaría a consideración del responsable de seguridad debido a que la misma criticidad de los servicios requiere una clasificación. Utilizar los controles (p. ej. A.8.2.1, A.8.2.2) de la norma ISO 27001:2013, los mismos que asisten en la clasificación de información. Utilizar la **plantilla de la actividad de clasificación de servicios de ciberseguridad**, para realizar la clasificación de servicios de ciberseguridad.
	Adaptar el marco de referencia para ciberseguridad	(Esta actividad se encuentra relacionada con los marcos de referencia de ciberseguridad) Determinar con que marcos de referencia se va a trabajar durante esta fase, para esto es importante entender y conocer que actividades intervienen en la Arquitectura de sistemas de información Una vez que se determina lo que se va a hacer o como se va a trabajar, se puede adaptar el marco de referencia para ciberseguridad como una salida tangible (documento) de esta actividad. Dentro del marco de trabajo de TOGAF 9.1 en el apartado de utilizando TOGAF con otros marcos (2.10 Using TOGAF with other frameworks) y en el White Paper de la integración de SABSA y TOGAF en el apartado de marcos de control (Control Frameworks), se pueden encontrar los puntos a considerar para la adaptación del trabajo de arquitectura con otros marcos de referencia, guiarse por esta información dentro de la implementación de ciberseguridad para la AE. Utilizar la **plantilla de la actividad del marco de referencia para ciberseguridad,** para adaptar el marco de referencia de ciberseguridad.
	Realizar un análisis de brechas	(Actividad relacionad con el Catálogo de servicios de ciberseguridad) Una vez que se han identificado los servicios, es necesario determinar el cumplimiento mínimo de prácticas y controles de ciberseguridad para la protección de los sistemas de información. El análisis de brechas en esta fase, es necesario para determinar qué medidas se deben tomar en relación al estado actual y a un estado objetivo.

		Utilizar los controles de la norma ISO 27001:2013, el marco de NIST (CS-IC), y COBIT 5 (TCS), para determinar los procesos a seguir y así alcanzar un estado objetivo, hay que tener en cuenta que los controles y/o prácticas a implementar dependen del tamaño de la organización y las características de los sistemas de información que se desea proteger, para no extenderse en prácticas que pueden generar un esfuerzo mayor al necesario. Conforme a expuesto durante esta actividad se pueden seleccionar: - Controles de la norma ISO 27001 necesarios (p. ej. 10.1.1 Política de uso de los controles criptográficos, 12.2.1 Controles contra el código malicioso., 12.6.2 Restricciones en la instalación de software, etc.) - Subcategorías de NIST (p. ej. ID.AM-4: catálogo de sistemas de información externos, PR.AC-3: gestión de acceso remoto, etc.) - Información, técnicas y actividades de COBIT 5 (p. ej. APO02.04 llevar a cabo un análisis de brechas, APO02.05 Definir el plan estratégico y hoja de ruta, etc.) Utilizar la **plantilla de la acividad de análisis de brechas,** para realizar el análisis de brechas.
	Determinar la reglas, prácticas y procedimientos de ciberseguridad	(Actividad relacionada con el análisis de brechas Se debe determinar las reglas, prácticas y procedimientos a nivel de solución que son necesarios de acuerdo a las normas y marcos de trabajo que se han seleccionado para resolver los problemas que afectan a la ciberseguridad de la arquitectura de sistemas de información (datos, aplicaciones) Como se mencionó anteriormente esta actividad va relacionada con el análisis de brechas, donde ya se identifican los controles, actividades y procedimientos necesarios, los cuales se listan dentro del documento generado como salida de esta actividad, en el cual se detallan las reglas, prácticas y procedimientos de ciberseguridad de ISO 27001:2013, COBIT 5 (TCS) y NIST (CS-IC) Utilizar la **plantilla de la actividad de reglas, prácticas y procedimientos de ciberseguridad**, para determinar las reglas, prácticas y procedimientos de ciberseguridad.
Arquitectura tecnológica (TA)	**Identificar los estándares de Ciberseguridad**	Identificar los estándares de ciberseguridad para la protección de la arquitectura tecnológica, estos estándares suministran protección a las tecnologías de comunicaciones (p. ej. estándares de protección para tecnologías que gestionan la transferencia de datos).

		Se debe exigir el uso de técnicas o estándares como buenas prácticas que garanticen la seguridad a través del acceso público (p. ej. TLS, SAML, etc.), estos estándares pueden ser identificados dependiendo de las necesidades tecnológicas de cada organización para sus sistemas de información. La salida de esta actividad se basa en una lista de los estándares de ciberseguridad, con una descripción técnica de los mismos. Utilizar la **plantilla de la actividad de estándares de ciberseguridad**, para identificar los estándares de ciberseguridad
	Determinar las reglas, prácticas y procedimientos de ciberseguridad	(Actividad relacionada con los estándares de ciberseguridad) Determinar que controles o procedimientos a nivel de solución son necesarios, de acuerdo a los estándares que se han seleccionado para resolver los problemas que afectan a la ciberseguridad. Utilizar los controles de la norma ISO 27001:2013 como buenas prácticas (p. ej. A.14.1.2) y las subcategorías del marco de trabajo de NIST (p. ej. PR.AC-5, PR.DS-2, etc.), los mismo que engloban y respaldar los estándares de ciberseguridad seleccionados para la mejora de la arquitectura tecnológica. Utilizar la **plantilla de la actividad de reglas, prácticas y procedimientos de ciberseguridad**, para determinar las reglas, prácticas y procedimientos de ciberseguridad
	Adaptar el marco de referencia para ciberseguridad (TA:CSF)	(Esta actividad se encuentra relacionada con los marcos de referencia de ciberseguridad) Determinar con que marcos de referencia se va a trabajar durante esta fase, por este motivo es importante entender y conocer que actividades intervienen dentro de la Arquitectura tecnológica. Una vez que se establece lo que se va a hacer, se pueden adaptar los marcos de referencia necesarios para generar el documento de marco de referencia para ciberseguridad. Dentro del marco de trabajo de TOGAF 9.1 en el apartado de utilizando TOGAF con otros marcos (2.10 Using TOGAF with other frameworks) y en el White Paper de la integración de SABSA y TOGAF en el apartado de marcos de control (Control Frameworks), se pueden encontrar los puntos a considerar para la adaptación del trabajo de arquitectura tecnológica con otros marcos de referencia, guiarse por esta información dentro de la implementación de ciberseguridad para la AE. Utilizar la **plantilla de la actividad del marco de referencia para ciberseguridad**, para adaptar el marco de referencia de ciberseguridad.

Fuente: (Autor, 2014)

Planificación de la Transición.

Tabla 7. Iteración de planificación de la transición – Guía de ciberseguridad para arquitectura empresarial

Fase	Actividad	Recomendación basada en Ciberseguridad
Oportunidades y soluciones (OS)	**Análisis de los procedimientos para el control de oportunidades y soluciones**	Esta es una actividad orientada al control de procedimientos, donde se verifican los procesos y soluciones propuestas, y también se mide la eficacia de los servicios de ciberseguridad existentes. Verificar los controles destinados para su reutilización, para asegurar que el estado final contiene las medidas de ciberseguridad que funcionan y se integrar bien, caso contrario decidir si se incluye la remediación en el plan de migración o se reitera desde las fases B a la D para incluir nuevos controles y componentes. Considerar el marco de trabajo de TOGAF 9.1 en la fase de oportunidades y soluciones (Phase E: Opportunities and Solutions) para gestionar esta fase. Utilizar como apoyo a COBIT 5 (TCS), el cual engloba todo el universo de ciberseguridad para identificar las oportunidades y soluciones de la protección de los SI de negocios, y apoyarse en la **plantilla de análisis de procedimientos para el control de oportunidades y soluciones**.
Planificación de la migración (MP)	**Control de migración**	Asegurarse que se identifican todos los riesgos asociados, y los controles apropiados, para la implementación del trabajo de ciberseguridad y la ejecución de sus proyectos, los estos riesgos y controles se obtienen de los documentos generados como salida durante el desarrollo de las actividades de las fases B a la D del ADM. Tomar el White Paper de la integración de SABSA y TOGA, a través de la fase de planificación de la migración (Phase F: Migration Planning) de la cual se ha obtenido y especializado esta actividad de ciberseguridad para la AE. Utilizar la **plantilla de la actividad de control de migración**, para priorizar los proyectos, controles o procedimietos que son necesarios y que generen valor para el negocio a través de la implementacion de ciberseguridad.

Fuente: (Autor, 2014)

Gobernanza

Tabla 8. Iteración de gobernanza – Guía de ciberseguridad para arquitectura empresarial

Fase	Actividad	Recomendación basada en Ciberseguridad
Gobierno de la implementación (IG)	**Gestión de ciberseguridad**	Para mantener el control de todo lo que implica ciberseguridad es importante realizar una debida gestión sobre la misma, donde es necesario realizar una definición detallada de los roles y responsabilidades de ciberseguridad. Otro punto importante es la implementación de gobernanza de ciberseguridad, que va desde el plano preventivo al correctivo en cuanto a eventos causados por ciberataques, cuyo objetivo es definir cómo se va a proceder (p. ej. inteligencia contra amenazas, canales de comunicación, proactividad ante incidentes, flexibilidad, etc.) Además se deben definir los indicadores clave de desempeño y de riesgos de ciberataques, que justifican la aplicación de ciberseguridad en la AE, estos indicadores de riesgo determinan que tan posible es que se dé un evento, y los indicadores de desempeño son aquellos que se basan en la mitigación de los riesgos de ciberseguridad. Utilizar COBIT 5 (TCS) para: - Gestión de ciberseguridad (Cybersecurity Management) - Controles de seguridad existentes (Existing Security Controls) - Procesos de aplicación de ciberseguridad (COBIT 5 Processes Applying to Cybersecurity) Utilizar la **plantilla de la actividad de gestión de ciberseguridad**, para la gestión de ciberseguridad.

	Realizar auditoría de ciberseguridad	Realizar auditorías de ciberseguridad como una prueba de la importancia de implementar ciberseguridad dentro de la organización, donde se deben realizar informes que incluyan la revisión de seguridad de las configuraciones, controles y políticas implementadas, también del código desarrollado en contra de requerimientos y estándares seguros, y pruebas de penetración. Para las diferentes auditorias utilizar estándares o marcos de trabajos, en el caso de pruebas técnicas utilizar la guía de pruebas de OWASP, para el cumplimiento de auditorías basarse en los controles (p. ej. A.5.1.2, A.18.2.2), de ISO 27001:2013, y para abordar el universo de auditorías de ciberseguridad utilizar COBIT 5 (TCS) a través de la sección de auditoria y revisión de la ciberseguridad, que dispone de un conjunto metas de ciberseguridad relacionadas con los objetivos de la auditoria. Utilizar la **plantilla de la actividad de auditoría de ciberseguridad,** para auditorías de ciberseguridad.
	Implementar una conciencia de ciberseguridad	Es recomendable que se garantice la formación de conciencia de todos los usuarios y operadores de sistemas en cuanto a ciberseguridad. La formación de conciencia de ciberseguridad realizada de manera adecuada debe documentarse como una buena práctica que demuestre la debida diligencia para justificar las medidas correctivas en casos donde se explote o se comprometan los servicios afectando al negocio. Esta actividad se puede realizar a través de un plan de capacitación o se la puede incluir dentro de las políticas de ciberseguridad, donde se determinen las capacitaciones para el área de ciberseguridad y personal operativo, de acuerdo a los roles y responsabilidades asignadas dentro de la organización, estos temas de capacitación pueden darse durante periodos de tiempos definidos o de acuerdo a ciertas necesidades de seguridad. Para apoyar esta actividad, utilizar el apartado de conciencia de seguridad de COBIT 5 (TCS), donde se abordan temas sobre capacitación del personal contra ataques o violaciones potenciales y reales, y la preparación de materiales relacionados con la sensibilización y concienciación de seguridad de la información. Utilizar la **plantilla de la actividad de conciencia de ciberseguridad,** para implementar la conciencia de ciberseguridad.

	Gobernanza	Asegurar la conformidad con la arquitectura definida por los proyectos de ciberseguridad, ayuda a que no se pierda el rumbo hacia los objetivos planteados, mientras las actividades estan siendo implementadas y desplegadas, garantizando que el trabajo de ciberseguridad cumpla con las especificaciones, reglas, políticas y directrices, de forma que generen valor para la organización. Una herramienta recomendada para llevar a cado esta actividad es un checklist de donde se evalue el cumplimiento de las tareas, objetivos o proyectos que forman parte de la implementacion de la ciberseguridad. Tomar el marco de trabajo de TOGAF 9.1, a través de la fase de planificación de migración (Phase F: Migration Planning) junto al capitulo 50 de gobernanza de arquitectura. Utilizar la **plantilla de la actividad gobernanza**, para verificar el cumpliento de los proyectos planificados.
Gestión de cambios de la arquitectura (ACM)	**Gestión de cambios**	Identificar qué cambios se han originado dentro de las fases del ciclo del ADM, en donde se determina cual es el impacto de los mismos, y que acciones correctivas se deberían tomar o como se los va a gestionar, de forma que no se generen problemas dentro de la arquitectura. Los cambios existentes se los debe listar dentro de un documento que se genera como salida de esta actividad, donde se incluye el detalle de cada cambio, como por ejemplo el nombre del cambio, descripción, origen, impacto y la acción correctiva que se va a tomar sobre el mismo. Utilizar el marco de trabajo de TOGAF 9.1, a través del proceso de gestión de cambios de la AE (16.2.2 Enterprise Architecture Change Management Process), para determinar cómo deben ser gestionados los cambios, que técnicas se deben aplicar y además que metodologías pueden ser utilizadas. Utilizar la **plantilla de la actividad de gestión de cambios,** para la gestión de cambios de ciberseguridad.
	Gestión de riesgos	Evaluar los procesos de gestión de ciberseguridad en la arquitectura existente con respecto a las amenazas de ciberseguridad. Si basado en los resultados de este proceso, la arquitectura actual se considera inadecuada para mitigar los riesgos modificados o nuevos, o si se restringe demasiado el negocio en la explotación de nuevas oportunidades, debe tomarse una decisión sobre el cambio de los controles o procedimientos de ciberseguridad para la arquitectura. Las decisiones sobre esta actividad van incluidas en la plantilla de gestión de cambios

	Gobernanza de la arquitectura de ciberseguridad	(Actividad que se encuentra relacionada con la gestión de cambios) Esta actividad se basa en la toma de decisiones sobre los cambios existentes en los controles y procesos que son necesarios para hacer frente a incidentes causados por ataques o violaciones de seguridad, ya sean estos por cambios menores durante la iteración actual o por medio de una nueva iteración. Normalmente esta actividad no genera una salida tangible o un entregable, pero ayuda a determinar los cambios que son necesarios. Utilizar COBIT 5 (TCS), como guía para trabajar la gobernanza de la ciberseguridad, cuya información se detalla dentro los apartados de: - Objetivos de gobernanza de ciberseguridad - Gobernanza de ciberseguridad en el dominio EDM - Gobernanza de ciberseguridad en el dominio APO Utilizar la **plantilla de la actividad de gobernanza de la arquitectura de ciberseguridad**

Fuente: (Autor, 2014)

La tabla 9 muestra la relación entre los entregables propuestos por la guía de ciberseguridad, los artefactos de TOGAF, y los entregables del documento de la integración de TOGAF y SABSA:

Tabla 9. Matriz de controles de la guía de ciberseguridad

Fases	**Entregables**			
	TOGAF		**Integracion de TOGAF y SABSA**	**Guia de ciberseguridad para AE**
	Entregables	**Artefactos**	**Entregables**	**Entregables**
Gestion de requerimientos			Atributos del perfil de negocio	Atributos del perfil de negocio para ciberseguridad
		Catálogo de requerimientos	Control de objetivos	Control de requerimientos
Fase preliminar	Principios, metas, e impulsores de negocio		Impulsores de negocio	
		Catálogo de principios	Principios de ciberseguridad	Principios de ciberseguridad
			Areas clave de riesgo	Áreas de riesgo
			Apetito de riesgo	
	Modelo organizacional para la arquitectura empresarial		Plan de recurso de seguridad	Equipo de ciberseguridad
	Marco de arquitectura adaptado			Marcos de referencia para ciberseguridad
Fase A Vision de arquitectura	Plan de comunicación	Matriz del mapa de interesados	Interesados de seguridad	Partes interesadas de ciberseguridad
	Visión de arquitectura			Requerimientos de ciberseguridad
	Marco de arquitectura adaptado			Marco de referencia de ciberseguridad

Fase B Arquitectura de negocio	Marco de arquitectura adaptado		Marcos de control	Marco de referencia de ciberseguridad
	Documento de definición de arquitectura		Leyes y regulaciones	Leyes y regulaciones ligadas a ciberseguridad
			Modelo de riesgo del negocio	Modelo de riesgo de negocio
			Modelo del dominio de seguridad	Modelo del dominio de ciberseguridad
			Marcos de confianza	Protocolos de confianza
			Organización de seguridad	Organización de ciberseguridad
			Arquitectura de políticas de seguridad	Arquitectura de las políticas de ciberseguridad
		Catálogo de servicios de negocio/función	Catálogo de servicios de seguridad	
Fase C Arquitectura de sistemas de información		Catálogo del portafolio de aplicaciones	Cataálogo de servicios de seguridad	Catálogo de servicios de ciberseguridad
		Matriz de aplicación/ organización	Clasificacion de servicios	Clasificación de servicios de ciberseguridad
	Marco de arquitectura adaptado		Reglas, practicas y procedimientos de seguridad	Reglas, practicas y procedimientos de ciberseguridad
				Marco de referencia de ciberseguridad
			<Ninguno>	Análisis de brechas
Fase D Arquitectura tecnológica	Marco de arquitectura adaptado		Reglas, practicas y procedimientos de seguridad	Reglas, practicas y procedimientos de ciberseguridad
				Adaptar el marco de referencia de ciberseguridad
		Catálogo de estándares de tecnología.	Estandares de seguridad	Estándares de Ciberseguridad

Fase E Oportunidades y soluciones	Plan de implementación y migración	Diagrama de beneficios		Análisis de los procedimientos para el control de oportunidades y soluciones
Fase F Planificación de migración	Modelo de gobierno de la implementación			Control de migración
Fase G Gobierno de la implementación			Gestion de seguridad	Gestión de ciberseguridad
			Conciencia de seguridad	Conciencia de ciberseguridad
	Evaluacion de cumplimiento		Auditoria de seguridad	Auditoría de ciberseguridad
				Gobernanza
Fase H Gestión de cambios de la arquitectura	Evaluacion de impacto de requerimientos		Gestion de riesgos	Gestion de riesgos
			Gobernanza de la arquitectura de seguridad.	Gobernanza de la arquitectura de ciberseguridad
	Solicitud de cambios en la arquitectura.			Gestión de cambios

Fuente: (Autor, 2015)

Con el objetivo de apoyar y mejorar los controles de ciberseguridad, en la Tabla 9, se plantean varias soluciones que están referenciadas por la norma ISO 27001:2013 y los marcos de ciberseguridad de COBIT 5 (Transformando la ciberseguridad usando COBIT 5), y NIST (Marco para mejorar la ciberseguridad en infraestructuras críticas), orientadas al entorno de trabajo de ciberseguridad, que se pueden implementar de acuerdo a las necesidades organizacionales.

Si bien desde las tablas 4 hasta la 8, correspondientes a las actividades de implementación de la guía de ciberseguridad para AE, se encuentran diferentes referencias hacia marcos de trabajos, normas y guías, en la siguiente Tabla 10 se proporciona un conjunto de buenas prácticas y controles de ciberseguridad.

Tabla 10. Matriz de controles de la guía de ciberseguridad

Categoría	Subcategoría	Referencia	Categoría(s) relacionada(s)
Políticas	**POL-01: Políticas de ciberseguridad:** se deben establecer políticas de seguridad, estas políticas deben estar aprobadas y apoyadas por la dirección, las mismas tendrán en cuenta los requisitos de negocio, los contractuales y los legales y estatutarios que sean aplicables.	• ISO/IEC 27001:2013 A.5.1.1 • NIST CF ID.GV-1 • Transforming Cybersecurity - Using Cobit 5: Components of the Cybersecurity Policy - Figure 29	Ninguna
	POL-02: Cumplimiento Legal: controles y procedimientos para el cumplimiento de la legislación vigente aplicable a la organización, para así evitar infracciones hacia la misma.	• ISO/IEC 27001:2013 A.18.1.1, A.18.1.4 • Transforming Cybersecurity: Using Cobit 5: MEA Process Mapping - Figure 63 - MEA03.01 (Cybersegurity)	Ninguna
	POL-03: Servicio de Mensajería Electrónica: controles para garantizar el uso correcto y responsable del servicio, sobre todo en el envío de información crítica o confidencial.	• ISO/IEC 27001:2013 A.13.2.3 • NIST CF PR.DS-2	Personas
	POL-04: Regulación de Controles criptográficos: determinar los controles criptográficos sujetos a leyes y regulaciones, o los mismos pueden ser objeto de acuerdos con otras organizaciones, los cuales deben tener procedimientos para su uso adecuado.	• ISO/IEC 27001:2013 A.18.1.5	Ninguna
	POL-05: Cumplimiento de Políticas: garantizar que se cumplan las políticas y normas de seguridad, así como los requisitos legales, por parte del personal y de los sistemas de la organización, de ser posible realizar una revisión por a través de una entidad auditora externa especializada en el tema sobre la gestión y la implementación de los controles, políticas y procedimientos.	• ISO/IEC 27001:2013 A.18.2.1, A.18.2.2 • Transforming Cybersecurity - Using Cobit 5: Components of the Cybersecurity Policy - Figure 29	Personas Seguridad de la información

	POL-06: Uso de Dispositivos Móviles: controles destinados al uso responsable de los dispositivos móviles otorgados por parte de la organización.	• ISO/IEC 27001:2013 A.6.2.1	Personas
	POL-07: Acceso Remoto: determinar los controles para proteger la información que se accede, procesa y almacena de forma remota.	• ISO/IEC 27001:2013 A.6.2.2 • NIST CF PR.AC-3	Personas Seguridad de la información
	POL-08: Gestión de Contraseñas: control para el diseño de contraseñas, estas deberían depender de la criticidad de la información, para lo cual deben tener mayor complejidad (mesclar: caracteres, números, letras y símbolos)	• ISO/IEC 27001:2013 A.9.4.3 • NIST CF PR.AC-1	Personas
	POL-09: Seguridad Operativa y segregación de tareas: documentar las tareas que se deben afrontar, para lo cual se debe asignar responsables que cubran todas las actividades fundamentales dentro de la organización.	• ISO/IEC 27001:2013 A.6.1.2, A.12.1.1	Personas
	POL-10: Políticas para control de accesos: redactar las normas y políticas de seguridad para el control de accesos a redes, servicios de red, e información, de acuerdo a las necesidades del negocio o de acuerdo a la clasificación de la información conforme a su criticidad.	• ISO/IEC 27001:2013 A.9.1.1, A.9.1.2	Tecnología
	POL-11: Registro y gestión de usuarios: establecer procedimientos para registrar las altas y bajas de los permisos de acceso de los usuarios donde se garantizan o cancelan los mismos hacia los sistemas y/o servicios, en donde también se deben registrar los derechos de acceso privilegiado de manera controlada y limitada.	• ISO/IEC 27001:2013 A.9.2.1, A.9.2.2, A.9.2.3 • NIST CF PR.AC-1	Datos
	POL-12: Revisión de derechos de acceso: revisar regularmente los derechos de acceso concedidos y actualizarlos de ser necesario.	• ISO/IEC 27001:2013 A.9.2.5	Personas
	POL-13: Control para cambio o retirada de derechos de acceso: controles aplicados para la retirada de los derechos de acceso cuando	• ISO/IEC 27001:2013 A.9.2.6	Personas

	concluye el empleo o contrato de un empleado o contratista, o también para la adaptación de los permisos si es necesario en caso de cambio de puesto del empleado.		Aplicaciones
	POL-14: Revisión de estabilidad operativa: determinar los controles necesarios para verificar el cumplimiento de políticas y procedimientos los cuales podrían generar la implementación de nuevas normas de acuerdo a los hallazgos.	• ISO/IEC 27001:2013 A.18.2.1, A.18.2.3 • NIST CF ID.RA-1	Personas
	POL-15: Gestión de Cambios de Políticas: gestión de las normas o políticas de seguridad, debido a nuevas tecnologías, regulaciones o fallos de seguridad..	• ISO/IEC 27001:2013 A.5.1.2	Ninguna
Personas	**PER-01: Responsable(s) de Ciberseguridad:** asignación de responsabilidades para ciberseguridad.	• ISO/IEC 27001:2013 A.6.1.1 • NIST CF ID.AM-6	Políticas
	PER-02: Responsabilidades del usuario: el usuario debe mantener y seguir responsablemente los controles y procedimientos para el uso de contraseñas, como mantener su confidencialidad, no compartirla, no dejarla en un lugar de fácil acceso, etc.	• ISO/IEC 27001:2013 A.9.3.1 • NIST CF PR.AC-1	Políticas
	PER-03: Capacitación: proporcionar formación adecuada hacia el personal de la organización para un mejor rendimiento en sus tareas y conocimientos en materia de seguridad de la información.	• ISO/IEC 27001:2013 A.6.1.1 A.7.2.2 • NIST CF PR.AT-1, PR.AT-2 • Transforming Cybersecurity - Using Cobit 5: Cybersecurity Management Processes - Figure 32 - APO07, Sample Training Structure Program -Figure 44	Políticas
Seguridad de la Información (Datos, Tecnología)	**SEGINF-01: Protección de información organizacional:** controles asociados a la protección de documentos importantes dentro de la organización debido a motivos internos, contra la perdida, destrucción y falsificación de los mismos.	• ISO/IEC 27001:2013 A.18.1.3	Políticas

	SEGINF-02: Acuerdos para intercambio de información: requerir políticas y procedimientos para la protección de la información y de los recursos que se utilizan para su intercambio, además incluir las responsabilidades de las partes ante incidentes, para tratamiento de la información sensible, software, etc.	• ISO/IEC 27001:2013 A.13.2.1, A.13.2.2 • NIST CF PR.PT-4	Políticas
	SEGINF-03: Acuerdos de confidencialidad: determinar los procedimientos y controles para proteger adecuadamente la información critica de la organización, y realizar una revisión periódica de cuándo y quien tiene o debe firmar estos acuerdos	• ISO/IEC 27001:2013 A.13.2.4 • NIST CF PD.DS-5	Políticas
	SEGINF-04: Inventario de activos: realizar un inventario de activos, determinando sus características y quien es o son los responsables del mismo.	• ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 • NIST CF ID.AM-1	Tecnología
	SEGINF-05: Inventario de software y aplicaciones: realizar un inventario de las aplicaciones, que se encuentran dentro de la organización para establecer prioridades en su protección.	• ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 • NIST CF ID.AM-2	Tecnología
	SEGINF-06: Administración y uso de activos: determinar y documentar las normas para el uso adecuado de la información y de los activos que tienen por objetivo el tratamiento de la información.	• ISO/IEC 27001:2013 A.8.1.3	Políticas
	SEGINF-07: Cifrado: establecer controles criptográficos para proteger claves e información importante de acuerdo a las necesidades empresariales y criticidad de información.	• ISO/IEC 27001:2013 A.10.1.1, A.10.1.2	Políticas
	SEGINF-08: Clasificación de Información: se debe determinar la criticidad y sensibilidad de la información, así mismo debe ser tratada de acuerdo con el sistema de clasificación adoptado por la organización.	• ISO/IEC 27001:2013 A.8.2.1, A.8.2.2, A.8.2.3 • NIST CF PR.PT-2	Políticas
	SEGINF-09: Copias de Seguridad: deberán realizarse y probarse periódicamente los respaldos de información y software, además de	• ISO/IEC 27001:2013 A.12.3.1 • NIST CF PR.IP-4	Políticas

	imágenes de sistemas, de acuerdo a las políticas o prioridades de la organización.		
	SEGINF-10: Seguridad de Redes: procedimientos y controles para protección de la infraestructura y los servicios de red (internos o externos) a través de la segregación de la red, responsabilidades operativas, cifrado, autenticación, uso de logs, etc.	• ISO/IEC 27001:2013 A.13.1.1, A.13.1.2, A.13.1.3 • NIST CF PR.AC-5	Tecnología
Tecnología	**TEC-01: Inventario de dispositivos físicos:** determinar que activos, que soportan la infraestructura tecnológica forman parte de la organización.	• ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 • NIST CF ID.AM-1	Ninguna
	TEC-02: Control de acceso físico: determinar los controles para garantizar el acceso únicamente a personal autorizado, de acuerdo a sus respectivas responsabilidades.	• ISO/IEC 27001:2013 A.11.1.2 • NIST CF PR.AC-2	Políticas
	TEC-03: Criticidad de infraestructura y tolerancia al riesgo: determinar la criticidad de la Infraestructura clave dentro de la organización, para priorizar su continua operatividad con una medida tolerancia hacia el riesgo.	• NIST CF ID.RM-3	Ninguna
	TEC-04: Requisitos Tecnológicos para Seguridad: analizar y especificar el hardware o software que se va a adquirir.	• ISO/IEC 27001:2013 A.14.1.1	Ninguna
	TEC-05: Gestión de Cambios Tecnológicos: control para la aprobación y debida planificación de cambios.	• ISO/IEC 27001:2013 A.12.1.2 • NIST CF PR.IP-1	Eventos y amenazas de seguridad
	TEC-06: Controles para accesos a sistemas y aplicaciones: establecer los controles necesarios para el uso de procedimientos seguros de inicio de sesión, dentro de los cuales se permitirá el acceso	• ISO/IEC 27001:2013 A.9.4.1, A.9.4.2 • NIST CF PR.AC-4	Seguridad de la Información

	únicamente a usuarios autorizados conforme a las políticas para el control de accesos.		
	TEC-07: Instalación segura de Equipos: determinar los controles para la ubicación y funcionamiento de los equipos, además la protección del cableado de energía y telecomunicaciones para evitar fallos o interceptaciones de información.	• ISO/IEC 27001:2013 A.11.2.1, A.11.2.2, A.11.2.3 • NIST CF PR.IP-5	Políticas
	TEC-08: Mantenimiento de Equipos: control para mantenimiento preventivo y correctivo de los equipos para prolongar su correcto funcionamiento.	• ISO/IEC 27001:2013 A.11.2.4 • NIST CF PR.MA-1	Políticas
Eventos y amenazas de seguridad	**EAS-01: Impacto de Disponibilidad:** determinar el impacto causado por la falta de disponibilidad de las operaciones en el negocio.	• NIST CF ID.RA-4	Seguridad de la Información
	EAS-02: Gestión de la continuidad del negocio: desarrollar el plan de continuidad de negocio, en donde se identifiquen plenamente los protocolos y procedimientos a seguir, y determinar en qué momento se deben ejecutar y por quienes se deben llevar a cabo.	• ISO/IEC 27001:2013 A.17.1.1, A.17.1.2 • NIST CF PR.IP-9 • Transforming Cybersecurity - Using Cobit 5: DSS Process Mapping - Figure 62 - DSS04.01, DSS04.03)	Políticas
	EAS-03: Gestión de recuperación de desastres: desarrollar un plan para la recuperación de desastres, en donde se establezcan los procedimientos para una respuesta rápida y efectiva contra incidentes de seguridad.	• ISO/IEC 27001:2013 A.16.1.1 • NIST CF PR.IP-9 • Transforming Cybersecurity - Using Cobit 5: Components of the Cybersecurity Policy - Figure 29	Políticas
	EAS-04: Evaluación y verificación de los planes de continuidad del negocio y recuperación de desastres: es necesario probar regularmente los planes de continuidad del negocio para garantizar su eficacia, y que cubre cada todos los activos que se consideran importante dentro de la organización.	• ISO/IEC 27001:2013 A.17.1.3 • NIST CF PR.IP-10	Políticas

	EAS-05: Medidas seguras ante amenazas externas y ambientales: determinar los controles en cuanto a la legislación, y daños causados por fuego, inundaciones y otros desastres ya sean causados, involuntarios o naturales.	• ISO/IEC 27001:2013 A.11.1.4 • NIST CF PR.AC-2	Políticas
	EAS-06: Registro de Actividades: recopilar información de actividades como evidencia en caso de incidentes, como registro de fallos y de incidentes para análisis e investigaciones futuras.	• ISO/IEC 27001:2013 A.12.4.1 • NIST CF PR.PT-1	Políticas
	EAS-07: Control para protección de registros: determinar que controles y procedimientos se deben seguir para evitar accesos no autorizados hacia los registros y evitar manipulaciones indebidas.	• ISO/IEC 27001:2013 A.12.4.2 • NIST CF PR.PT-1	Políticas
	EAS-08: Gestión de los registros de actividad de administración: control para comprobar el cumplimiento de las actividades del sistema y de la red por parte del administrador u operador del sistema.	• ISO/IEC 27001:2013 A.12.4.3 • NIST CF PR.PT-1	Seguridad de la Información
	EAS-09: Análisis de Amenazas: realizar una matriz de acuerdo al análisis de riesgos de las amenazas internas y externas.	• NIST CF ID.RA-3, ID.RA-5:	Ninguna
	EAS-10: Procesos Forenses: recopilar y documentar información como evidencia en caso de acciones legales tras incidentes.	• ISO/IEC 27001:2013 A.16.1.7 • NIST CF RS.AN-3 • Transforming Cybersecurity - Using Cobit 5: Investigation and Forensics Phases - Figure 71	Políticas
	EAS-11: Gestión de Vulnerabilidades Tecnológicas: controles para gestionar las actualizaciones o parches en los Sistemas Operativos o Software.	• ISO/IEC 27001:2013 A.12.6.1 • NIST CF PR.IP-12	Seguridad de la Información
	EAS-12: Gestión de Incidentes de seguridad: determinar los controles para la evaluación y clasificación de los incidentes de seguridad.	• ISO/IEC 27001:2013 A.16.1.4 • NIST CF RS.AN-4	Ninguna

	EAS-13: Respuesta a Incidentes de seguridad: controles y procedimientos para dar una rápida respuesta a los incidentes de seguridad, conforme lo indica el plan de respuesta a incidentes.	• ISO/IEC 27001:2013 A.12.2.1 A.16.1.5 • NIST CF RS.RP-1, RS.MI-1, RS.MI-2, RC.RP-1	Ninguna
	EAS-14: Aprendizaje Continuo: controles para el aprendizaje y mejora continua, mediante información recopilada de incidentes registrados para así tomar decisiones en cuanto a la mejora de controles o para añadir otros.	• ISO/IEC 27001:2013 A.16.1.6 • NIST CF RS.AN-2	Políticas

Fuente: (Autor, 2014)

3.5 Plantillas para implementación de la guía de ciberseguridad para arquitectura empresarial

En cuanto a las actividades de cada fase, se diseña una plantilla básica donde se requiere información relevante de acuerdo a los marcos de trabajos seleccionados de seguridad de AE y AE para cumplir con el área de ciberseguridad.

3.5.1 Estructura de las plantillas.

La información que es requerida en cada fase se generaliza con el modelo de la siguiente plantilla (Ver tabla 10)

Tabla 10. Plantilla general para la implementación de ciberseguridad en arquitectura empresarial

Información del documento	
Fase	<nombre de la fase>
Documento	<nombre del documento>
Elaborado por	<persona o equipo que elaboro el documento>
Aprobado por	<persona responsable que aprueba el documento con sus procedimiento>
Versión	<versión actual del documento>
Fecha	<fecha de aprobación del documento>
Desarrollo del documento	
Propósito	<propósito específico del documento>
Actividades	<actividades y/o requisitos del documento de acuerdo a la fase correspondiente> - <actividad 1> - < actividad 2> - …

Fuente: (Autor, 2014)

Cada una de las secciones de la plantilla se detalla de la siguiente manera:

1. **Fase:** corresponde al nombre de la fase a la cual pertenece el documento las mismas que pueden observar en la figura 19.
2. **Documento:** corresponde al nombre del documento que se va a utilizar para obtener la información respectiva de acuerdo a la fase actual, ejemplo:
    a. Atributos del perfil del negocio (Gestión de Requerimientos)
    b. Principios de seguridad (Fase preliminar)
    c. Interesados de seguridad (Fase A. Visión de arquitectura)
3. **Elaborado por:** persona o equipo que durante esta fase elaboro el documento, en este caso puede ser el arquitecto de seguridad o también el arquitecto de AE
4. **Aprobado por:** responsable(s) de aprobar el documento de ciberseguridad para la AE

5. **Versión:** versión actual del documento, requerido para el respectivo control de las interacciones del ciclo de ADM
6. **Fecha:** fecha en que se aprobó el documento por parte de los responsables o interesados
7. **Propósito:** determinar la intención del documento de acuerdo a la fase donde actúa.
8. **Actividades o cuerpo de la plantilla:** determinar y subdividir según sean necesarias las actividades dentro del documento de cada actividad que lo requiere; en los siguientes gráficos se muestra de forma general que puntos se deben tomar en cuenta, para obtener la información relevante en cada fase.

3.5.2 Desarrollo de las plantillas.

A continuación se encuentran detalladas las plantillas de ciberseguridad para AE, ordenadas de acuerdo al ciclo del ADM de TOGAF.

Gestión de requerimientos

Plantilla de la actividad de gestión de atributos del perfil de negocio para ciberseguridad

Información del documento	
Fase	Gestión de requerimientos
Documento	Atributos del perfil de negocio para ciberseguridad
Elaborado por	<persona o equipo que elaboro el documento>
Aprobado por	<persona responsable que aprueba el documento con sus procedimientos>
Versión	0.1
Fecha	<fecha de aprobación del documento>
Desarrollo del documento	
Propósito	El atributo del perfil de negocio, es creado para definir los atributos del negocio, con los cuales se determina el alcance que va a cubrir la guía de ciberseguridad (activos que necesitan protección)
Actividades	
Código	<código del atributo>
Tipo	<tipo de atributo>
Atributo de negocio	<nombre del atributo de negocio>
Descripción	<características sobe el atributo>
Ejemplos	
Código	ATTR-01
Tipo	Atributos de usuario
Atributo de negocio	Exacto
Descripción	La información facilitada a los usuarios debe ser exacta, dentro de un rango que ha sido previamente acordado.

Plantilla para la actividad de control de requerimientos

Información del documento	
Fase	Gestión de requerimientos
Documento	Control de requerimientos
Elaborado por	<persona o equipo que elaboro el documento>
Aprobado por	<persona responsable que aprueba el documento con sus procedimientos>

Versión	0.1
Fecha	<fecha de aprobación del documento>
Desarrollo del documento	
Propósito	El control de requerimientos, se gestiona a través de la creación de un catálogo de requerimientos para determinar cuáles son los requisitos o controles específicos de ciberseguridad requeridos por la organización para proteger sus sistemas de información de ataques informáticos
Actividades	
Código	<código/id del requerimiento>
Requerimiento	<nombre del requerimiento>
Descripción	<descripción del requerimiento >
Prioridad	<determinar el nivel de prioridad, ya sea: alta, media, baja>
Fecha	<fecha en que se registró o acepto el requisito>
Origen	<quien pide el requisito>
Dependencia	<dependencia o relación con otros requerimientos>
Ejemplo	
Código	REQ-01
Requerimiento	Control de acceso
Descripción	Control de acceso hacia los sistemas, basado en logs para el control de actividades
Prioridad	Alta
Fecha	22/06/2014
Origen	Oficial de seguridad
Dependencia	Ninguna

Evaluación de capacidad empresarial

Fase preliminar

Plantilla para la actividad de principios de ciberseguridad

Información del documento	
Fase	Fase preliminar
Documento	Principios de Ciberseguridad
Elaborado por	<persona o equipo que elaboro el documento>
Aprobado por	<persona responsable que aprueba el documento con sus procedimientos>
Versión	0.1
Fecha	<fecha de aprobación del documento>
Desarrollo del documento	
Propósito	Los principios de ciberseguridad, se determinan para proporcionar una orientación en la toma de decisiones del negocio, llevadas a cabo por el apetito de riesgo de la organización.
Actividades	
Código	<código del principio de ciberseguridad>
Principio	<nombre del principio de ciberseguridad>
Descripción	<descripción del principio de ciberseguridad>
Ejemplo	
Código	CSP-01
Principio	Enfocarse en el negocio
Descripción	Analizar el riesgo de ataques/violaciones a los procesos de negocio y dar prioridad en consecuencia a la ciberseguridad

Plantilla para la actividad del equipo de ciberseguridad

Información del documento	
Fase	Fase preliminar
Documento	Equipo de ciberseguridad
Elaborado por	<persona o equipo que elaboro el documento>
Aprobado por	<persona responsable que aprueba el documento con sus procedimientos>
Versión	0.1
Fecha	<fecha de aprobación del documento>
Desarrollo del documento	
Propósito	El plan de recursos de ciberseguridad se determina con el fin de cubrir las necesidades de protección de las tecnologías de la información en la AE específicamente en el área de ciberseguridad, donde se determina la cantidad de recursos necesarios de acuerdo a los perfil profesional y experiencia, también se verifica si los recursos de seguridad de la arquitectura pueden formar parte del equipo de ciberseguridad o como apoyo hacia el mismo
Requisitos	
Código	<identificador del recurso de ciberseguridad de ciberseguridad>
Nombre	<nombre del recurso de ciberseguridad>
Tipo	<tipo de recurso, se determina si es un recurso *permanente* del equipo o de *apoyo* hacia el equipo>
Perfil	<habilidades técnicas requeridas de ciberseguridad>
Rol	<tipo de función que cumplirá el recurso>
Responsabilidades	<responsabilidades asignadas dentro del área de ciberseguridad>

Plantilla para la actividad de marcos de referencia para ciberseguridad

Información del documento	
Fase	Fase preliminar
Documento	Marcos de referencia para ciberseguridad
Elaborado por	<persona o equipo que elaboro el documento>
Aprobado por	<persona responsable que aprueba el documento con sus procedimientos>
Versión	0.1
Fecha	<fecha de aprobación del documento>
Desarrollo del documento	
Propósito	Identificar los marcos de referencia necesarios para el trabajo de ciberseguridad
Actividades	
Código	<código del marco de referencia>
Marco	<nombre del marco de referencia>
Descripción	<descripción del marco de referencia>
Ejemplo	
Código	FCS-01
Marco	Transforming Cybersecurity Using Cobit 5
Descripción	Marco trabajo de ciberseguridad

Plantilla para la actividad de áreas de riesgo

Información del documento	
Fase	Fase preliminar
Documento	Áreas de riesgo
Elaborado por	<persona o equipo que elaboro el documento>
Aprobado por	<persona responsable que aprueba el documento con sus procedimientos>
Versión	0.1

Fecha	<fecha de aprobación del documento>
Desarrollo del documento	
Propósito	Identificar las áreas clave de riesgo que permiten, mediante el apetito por el riesgo obtener un balance frente a las oportunidades.
Actividades	
Código	<código del riesgo>
Riesgo	<nombre del área clave del riesgo >
Descripción	<descripción del área clave del riesgo>
Probabilidad	<posibilidad de que se active un determinado riesgo>
Impacto	<grado del impacto en caso de ocurrir un riesgo>
Tipo de riesgo	<determinar el tipo del riesgo, ya sea este un riego operativo, riesgo de TI, etc.>
Ejemplo	
Código	KRA-01
Riesgo	Hacking – intrusión no autorizada
Descripción	Acceso hacia los sistemas de información
Probabilidad	Media
Impacto	Alto
Tipo de riesgo	Riesgo de TI

Fase A: Visión de Arquitectura

Plantilla para la actividad de partes interesadas de ciberseguridad

Información del documento	
Fase	Fase A: Visión de arquitectura
Documento	Partes Interesadas de ciberseguridad
Elaborado por	<persona o equipo que elaboro el documento>
Aprobado por	<persona responsable que aprueba el documento con sus procedimientos>
Versión	0.1
Fecha	<fecha de aprobación del documento>
Desarrollo del documento	
Propósito	El documento de interesados en ciberseguridad (stakeholders) es necesario, para determinar quienes intervienen en la validación del estado final de la implementación de ciberseguridad, también es muy importante identificar los interesados del negocio, quienes controlan el presupuesto y facilitan el apoyo hacia la ciberseguridad
Actividades	
Código	<código del interesado>
Interesado	<nombre del interesado>
Tipo	<tipo de interesado, el mismo que puede ser: de seguridad o de negocio; se pueden definir otros tipos conforme se considere por el arquitecto de seguridad de la AE>
Capacidad para alterar cambios	<Nivel de capacidad para alterar los cambios hacia la seguridad de la AE, como por ejemplo: alto, medio, bajo >
Entendimiento actual	<Nivel de entendimiento actual del interesado hacia la seguridad de la AE, como por ejemplo: alto, medio, bajo >
Entendimiento requerido	<Nivel de entendimiento requerido por el interesado hacia la seguridad de la AE, como por ejemplo: alto, medio, bajo >
Compromiso actual	<Nivel de compromiso actual del interesado hacia la seguridad de la AE, como por ejemplo: alto, medio, bajo >
Compromiso requerido	<Nivel de compromiso requerido por el interesado hacia la seguridad de la AE, como por ejemplo: alto, medio, bajo >
Apoyo necesario	<Nivel de apoyo requerido por parte del interesado hacia la seguridad de la AE, como por ejemplo: alto, medio, bajo >

Ejemplo	
Código	STKH-01
Interesado	Bill Cowell
Tipo	De seguridad
Capacidad para alterar cambios	Alto
Entendimiento actual	Medio
Entendimiento requerido	Alto
Compromiso actual	Bajo
Compromiso requerido	Medio
Apoyo necesario	Alto

Plantilla para la actividad de requerimientos de ciberseguridad

Información del documento	
Fase	Fase A: Visión de arquitectura
Documento	Requerimientos de ciberseguridad
Elaborado por	<persona o equipo que elaboro el documento>
Aprobado por	<persona responsable que aprueba el documento con sus procedimientos>
Versión	0.1
Fecha	<fecha de aprobación del documento>
Desarrollo del documento	
Propósito	Los requerimientos de ciberseguridad, determinan las preocupación de los interesados, los mismos que establecen el límite del trabajo de ciberseguridad
Actividades	
Código	<código del requerimiento>
Requerimiento	<nombre del requerimiento>
Tipo	<tipo de requerimiento, el mismo que puede ser: implantación u operativo; se pueden definir otros tipos conforme se considere necesario>
Origen	<quien pide el requerimiento de ciberseguridad >
Criticidad	<Nivel de importancia del requerimiento, como por ejemplo: alto, medio, bajo>
Ejemplo	
Código	RQ-01
Requerimiento	Control de tráfico malicioso
Tipo	Operativo
Origen	Oficial de seguridad de la información
Criticidad	Alto

Plantilla para la actividad de marco de referencia de ciberseguridad adaptado

Información del documento	
Fase	Fase A: Visión de arquitectura
Documento	Marco de referencia de ciberseguridad adaptado
Elaborado por	<persona o equipo que elaboro el documento>
Aprobado por	<persona responsable que aprueba el documento con sus procedimientos>
Versión	0.1
Fecha	<fecha de aprobación del documento>
Desarrollo del documento	
Propósito	Identificar los marcos de referencia necesarios para el trabajo de ciberseguridad

Actividades	
Código	<código del marco de referencia>
Marco	<nombre del marco de referencia>
Descripción	<descripción del marco de referencia>
Ejemplo	
Código	FCS-01
Marco	Transforming Cybersecurity Using Cobit5
Descripción	Marco trabajo de ciberseguridad

Desarrollo

Fase B: Arquitectura de negocio

Plantilla para la actividad de modelo de riesgos de negocio

Información del documento	
Fase	Fase B: Arquitectura de negocio
Documento	Modelo de riesgos de negocio
Elaborado por	<persona o equipo que elaboro el documento>
Aprobado por	<persona responsable que aprueba el documento con sus procedimientos>
Versión	0.1
Fecha	<fecha de aprobación del documento>
Desarrollo del documento	
Propósito	El documento del modelo de riesgos de negocio, determina la estrategia de la organización frente a los riesgos, el mismo que es desarrollado de manera interna de acuerdo a las necesidades del ambiente empresarial
Actividades	

Modelo de riesgos de negocio	<Para determinar el modelo de riesgos de negocio se pueden considerar los siguientes puntos para su identificación y clasificación:
	- Identificar los riesgos
	- Evaluar y clasificar los riesgos
	  o Criticidad
	  o Impacto
	  o Probabilidad
	- Definir estrategias/medidas de respuesta
	  o Aceptar
	  o Transferir
	  o Evitar
	  o Reducir
	  o Mitigar
	- Supervisar y controlar>

Plantilla para la actividad de actividad de leyes y regulaciones

Información del documento	
Fase	Fase B: Arquitectura de negocio
Documento	Leyes y regulaciones
Elaborado por	<persona o equipo que elaboro el documento>
Aprobado por	<persona responsable que aprueba el documento con sus procedimientos>
Versión	0.1
Fecha	<fecha de aprobación del documento>
Desarrollo del documento	
Propósito	El documento de leyes y regulaciones, determina el alcance de la implementación de ciberseguridad en la AE para la gestión de información
Actividades	

Código	<código de la ley o regulación>
Ley	<nombre de la ley o regulación que la organización debe adoptar>
Artículos relevantes	<Artículos a considerar por parte de la organización>
Descripción	<Descripción del artículo>
Ejemplo	
Código	LR-01
Ley	Código orgánico integral penal
Artículos	Artículo 230
Descripción	Conforme cita la (Ministerio de Justicia, Derechos Humanos y Cultos, 2014), "Será sancionada con pena privativa de libertad de tres a cinco años: 1. La persona que sin orden judicial previa, en provecho propio o de un tercero, intercepte, escuche, desvíe, grabe u observe, en cualquier forma un dato informático en su origen, destino o en el interior de un sistema informático, una señal o una transmisión de datos o señales con la finalidad de obtener información registrada o disponible. 2. La persona que diseñe, desarrolle, venda, ejecute, programe o envíe mensajes, certificados de seguridad o páginas electrónicas, enlaces o ventanas emergentes o modifique el sistema de resolución de nombres de dominio de un servicio financiero o pago electrónico u otro sitio personal o de confianza, de tal manera que induzca a una persona a ingresar a una dirección o sitio de internet diferente a la que quiere acceder. 3. La persona que a través de cualquier medio copie, clone o comercialice información contenida en las bandas magnéticas, chips u otro dispositivo electrónico que esté soportada en las tarjetas de crédito, débito, pago o similares. 4. La persona que produzca, fabrique, distribuya, posea o facilite materiales, dispositivos electrónicos o sistemas informáticos destinados a la comisión del delito descrito en el inciso anterior."

Plantilla para la actividad de marco de referencia de ciberseguridad adaptado

Información del documento	
Fase	Fase B: Arquitectura de negocio
Documento	Marco de referencia de ciberseguridad adaptado
Elaborado por	<persona o equipo que elaboro el documento>
Aprobado por	<persona responsable que aprueba el documento con sus procedimientos>
Versión	0.1
Fecha	<fecha de aprobación del documento>
Desarrollo del documento	
Propósito	Identificar los marcos de referencia necesarios para el trabajo de ciberseguridad
Actividades	
Código	<código del marco de referencia>
Marco	<nombre del marco de referencia>
Descripción	<descripción del marco de referencia>
Ejemplo	
Código	FCS-01
Marco	TOGAF-SABSA Integration
Descripción	Seguridad para AE

Plantilla para la actividad de modelo de dominio de ciberseguridad

Información del documento	
Fase	Fase B: Arquitectura de Negocio
Documento	Modelo de dominio de ciberseguridad

Elaborado por	<persona o equipo que elaboro el documento>
Aprobado por	<persona responsable que aprueba el documento con sus procedimientos>
Versión	0.1
Fecha	<fecha de aprobación del documento>
Desarrollo del documento	
Propósito	El modelo de dominio de ciberseguridad, describe las interacciones entre los distintos dominios, partes y actores, en donde se definen las áreas de responsabilidad entre las zonas de diferentes niveles de seguridad
Actividades	
Código	<código del dominio de ciberseguridad>
Nombre	<nombre del modelo de dominio de ciberseguridad>
Modelo de dominio de ciberseguridad	<Modelo del dominio de ciberseguridad, se puede utilizar para su representación: casos de uso, diagramas de actividad o diagramas de carril>
Detalle del modelo de dominio	<Definir cada uno de los componentes dentro del modelo de dominio de ciberseguridad: - Dominio: nombre del dominio - Autoridad: cargo de las personas que intervienen dentro de las actividades del dominio - Procesos: nombre de los procesos que actúa dentro del dominio - Relación: nombre/id de la relación relaciones existentes dentro del dominio>
Ejemplo	
Código	CSDM-01
Nombre	Modelo del dominio empresarial
Modelo de dominio de ciberseguridad	<Modelo del dominio de ciberseguridad, mediante casos>
Detalle del modelo de dominio	Dominio: Unidad organizacional
	Autoridad: CIO (Chief Information Officer)
	Proceso: Ventas
	Relación: DR1

Plantilla para la actividad de protocolos de confianza

Información del documento	
Fase	Fase B: Arquitectura de negocio
Documento	Protocolos de confianza
Elaborado por	<persona o equipo que elaboro el documento>
Aprobado por	<persona responsable que aprueba el documento con sus procedimientos>
Versión	0.1
Fecha	<fecha de aprobación del documento>
Desarrollo del documento	
Propósito	Este marco de confianza se basa en describir las relaciones de confianza entre las distintas entidades del modelo de dominio de ciberseguridad y sobre que objeto se encuentra basada esa confianza existente
Actividades	
Relación	<nombre/id de la relación>
Descripción de los limites	<descripción de la relación entre las entidades >
Control de limites	<controles legales y técnicos, sobre los que se basan las relaciones de confianza>
Ejemplo	
Relación	DR1
Descripción de los limites	**Organizacional** con **Clientes**

	Controles legales	Controles técnicos
Control de limites	- Políticas internas - Contratos - Regulaciones	- Firewall / ACLs - Roles de la cuenta de usuario

Plantilla para la actividad de organización de ciberseguridad

Información del documento	
Fase	Fase B: Arquitectura de negocio
Documento	Organización de ciberseguridad
Elaborado por	<persona o equipo que elaboro el documento>
Aprobado por	<persona responsable que aprueba el documento con sus procedimientos>
Versión	0.1
Fecha	<fecha de aprobación del documento>
Desarrollo del documento	
Propósito	El propósito de este documento es organizar la ciberseguridad dentro de la organización, mediante un conjunto de procesos de gestión para ciberseguridad
Actividades	
Procesos de gestión de la ciberseguridad	<Determinar los procesos para la gestión de ciberseguridad, en base a las responsabilidades asignadas para cumplir con las actividades correspondientes de ciberseguridad>
Ejemplo	
Procesos de gestión de la ciberseguridad	**Responsabilidades:** personas encargadas de velar por la ciberseguridad dentro de la organización como por ejemplo: oficial de seguridad de la información, propietarios de la información, administradores de sistemas, etc. **Propietarios de riesgos:** sobre quien recae la responsabilidad de determinados procesos de ciberseguridad **Evaluación de riesgos:** responsabilidad asignada a un recurso de la organización, normalmente se asigna a un oficial de seguridad de la información **Objetivos de control:** controles asociados a las necesidades y requerimientos del negocio **Medidas de ciberseguridad:** medidas tomadas para ciberseguridad de acuerdo a determinados objetivos de control **Informes del estado actual de la ciberseguridad:** establecido como responsabilidad de acuerdo a los roles asignados, para la presentación de informes en un intervalo de tiempo definido o en casos especiales o concretos. **Gestión de incidentes:** conjunto de actividades a seguir que son propuestas por parte de un comité de seguridad de la información como respuesta a incidentes de ciberseguridad

Plantilla para la actividad de políticas de ciberseguridad

Información del documento	
Fase	Fase B: Arquitectura de negocio
Documento	Políticas de ciberseguridad
Marco de Referencia	TOGAF-SABSA Integration, ISO 27001, ISO 27002, Framework for Improving Critical Infrastructure Cybersecurity
Elaborado por	<persona o equipo que elaboro el documento>

Aprobado por	<persona responsable que aprueba el documento con sus procedimientos>
Versión	0.1
Fecha	<fecha de aprobación del documento>
Desarrollo del documento	
Propósito	La arquitectura de políticas de ciberseguridad, corrige la alineación de la gestión de riesgo operacional, en los diversos aspectos de ciberseguridad, como lo es la seguridad de la información, gestión de eventos informáticos, continuidad del negocio, etc.; donde se pueden utilizar ciertos principios de la seguridad de la información y transformarlos en elementos más manejables y concisos expresando las metas y objetivos sin excederse con detalles técnicos
Estructura estándar reconocida internacionalmente para políticas de seguridad, de acuerdo a (ISACA, 2013)	
Sección introductoria	<editorial, encabezado corporativo, exenciones de responsabilidad, control de versiones, etc.>
Propósito de documento	<establecer el ámbito de "ciberseguridad" en el contexto de seguridad de la información; exponer el caso de negocio que se sirve del documento>
Aplicabilidad	<definir el alcance de la ciberseguridad tal como se define y entiende dentro de la organización, distinguiendo claramente de otros campos de la seguridad de la información>
Referencias normativas	<vincular las política de ciberseguridad a otras políticas y normas vigentes, e incluir referencias definitivas a todas las normas, regulaciones externas y otras ataduras vinculantes tal como se define por la organización>
Metas y objetivos	<establecer claramente los objetivos de ciberseguridad, según lo acordado y firmado con la alta dirección>
Área de temáticas	<incluir el área de temáticas (por ejemplo, estrategia, operaciones, etc.), agrupándolos de acuerdo con el enfoque de gestión de seguridad de la información>
Roles y responsabilidades	Definir gráficos RACI para ciberseguridad
Presentación de informes	<Definir los requisitos para la presentación de informes de ciberseguridad>
Mejora continua	<Establecer el ciclo de vida, niveles de madurez y el proceso de transformación al más alto nivel>

Fase C: Arquitectura de Sistemas de Información

Plantilla para la actividad de catálogo de servicios de ciberseguridad

Información del documento	
Fase	Fase C: Arquitectura de sistemas de información
Documento	Catálogo de servicios de ciberseguridad
Elaborado por	<persona o equipo que elaboro el documento>
Aprobado por	<persona responsable que aprueba el documento con sus procedimientos>
Versión	0.1
Fecha	<fecha de aprobación del documento>
Desarrollo del documento	
Propósito	El catálogo de servicios de ciberseguridad, lista los servicios de negocio que proporcionan funcionalidad específica de ciberseguridad como parte de la arquitectura
Actividades	
Código	<código del servicio de negocio>
Nombre	<nombre breve del servicio de negocio>
Objetivos	<determinar qué objetivos funcionales debe cumplir el servicio como atributos de calidad, ej. Tiempo mínimo en que debe restablecerse un determinado servicio dentro de la organización>

Detalle técnico	<detalle técnico de las medidas de seguridad aplicadas sobre el servicio >
Criticidad	<grado de criticidad del servicio de ciberseguridad>
Ejemplo	
Código	CSS-01
Nombre	Servidor LDAP
Objetivos	- Mantenerse activo durante el horario de trabajo
Detalle técnico	- Transferencia cifrada de datos - Cifrar la sesión entre el cliente y el servidor LDAP
Criticidad	Alto

Plantilla para la actividad de clasificación de servicios de ciberseguridad

Información del documento	
Fase	Fase C: Arquitectura de sistemas de información
Documento	Clasificación de servicios de ciberseguridad
Elaborado por	<persona o equipo que elaboro el documento>
Aprobado por	<persona responsable que aprueba el documento con sus procedimientos>
Versión	0.1
Fecha	<fecha de aprobación del documento>
Desarrollo del documento	
Propósito	Este documento establece los parámetros para la clasificación de los servicios disponibles, de acuerdo al esquema interno de clasificación de la organización
Actividades	
Código	<código del servicio>
Servicio	<nombre del servicio>
Tipo	<tipo de servicio, ejemplo: control de acceso, herramientas de monitoreo, etc.>
Criticidad	<nivel de criticidad del sistema, ejemplo: alto, medio, bajo>
Responsable	<persona responsable del sistema>
Ejemplo	
Código	CS-01
Servicio	Control de acceso lógico
Tipo	Control de acceso
Criticidad	Alta
Responsable	Oficial de seguridad de la información

Plantilla para la actividad de marco de referencia de ciberseguridad adaptado

Información del documento	
Fase	Fase C: Arquitectura de sistemas de información
Documento	Marco de referencia de ciberseguridad adaptado
Elaborado por	<persona o equipo que elaboro el documento>
Aprobado por	<persona responsable que aprueba el documento con sus procedimientos>
Versión	0.1
Fecha	<fecha de aprobación del documento>
Desarrollo del documento	
Propósito	Identificar los marcos de referencia necesarios para el trabajo de ciberseguridad en los sistemas de información
Actividades	
Código	<código del marco de referencia>
Marco	<nombre del marco de referencia>
Descripción	<descripción del marco de referencia>
Ejemplo	
Código	FCS-01

Marco	TOGAF-SABSA Integration
Descripción	Seguridad para AE

Plantilla para la actividad de análisis de brechas

Información del documento	
Fase	Fase C: Arquitectura de sistemas de información
Documento	Análisis de brechas
Elaborado por	<persona o equipo que elaboro el documento>
Aprobado por	<persona responsable que aprueba el documento con sus procedimientos>
Versión	0.1
Fecha	<fecha de aprobación del documento>
Desarrollo del documento	
Propósito	El documento de análisis de brechas permite determinar el estado actual y objetivo de ciberseguridad para establecer las mejoras a efectuar
Actividades	
Código	<código del servicio de negocio>
AS-IS	<estado actual del servicio o proyecto>
TO-BE	<estado objetivo del servicio o proyecto>
Mitigación	<proyecto a desarrollar para llegar al estado objetivo>
Ejemplo	
Código	CSS-01
AS-IS	Control de ingreso débil hacia los sistemas de la organización
TO-BE	Debe existir un control de ingreso robusto, para evitar el robo de credenciales
Mitigación	Desarrollar o adquirir un algoritmo de encriptado robusto

Plantilla para la actividad de reglas, prácticas y procedimientos de ciberseguridad

Información del documento	
Fase	Fase C: Arquitectura de sistemas de información
Documento	Reglas, prácticas y procedimientos de ciberseguridad
Elaborado por	<persona o equipo que elaboro el documento>
Aprobado por	<persona responsable que aprueba el documento con sus procedimientos>
Versión	0.1
Fecha	<fecha de aprobación del documento>
Desarrollo del documento	
Propósito	Este documento lista las reglas, prácticas y procedimientos a nivel de solución para la protección de datos y aplicaciones
Actividades	
Código	<código de la norma>
Norma	<nombre de la norma>
Control	<tipo de control, definido por el modelo de clasificación de la organización para una determinada norma>
Procedimiento	<procedimiento que se lleva a cabo por la norma>
Referencias	<norma referencia por un determinado estándar si este es requerido>
Ejemplo	
Código	CSRPP-01
Norma/regla	Control de acceso a sistemas y aplicaciones
Control	Gestión de contraseñas de usuarios
Procedimiento	Control para asegurar el manejo seguro de credenciales (contraseñas)
Referencias	ISO 27001 A.9.4.3

Fase D: Arquitectura Tecnológica

Plantilla para la actividad de estándares de ciberseguridad

Información del documento	
Fase	Fase D: Arquitectura Tecnológica
Documento	Estándares de ciberseguridad
Elaborado por	<persona o equipo que elaboro el documento>
Aprobado por	<persona responsable que aprueba el documento con sus procedimientos>
Versión	0.1
Fecha	<fecha de aprobación del documento>
Desarrollo del documento	
Propósito	Este documento lista los estándares, técnicas o garantías de ciberseguridad para la protección de la arquitectura tecnológica
Actividades	
Código	<código del estándar>
Estándar	<nombre del estándar que se va a aplicar, ejemplo: Common Criteria, TLS, SAML, etc.>
Servicio	<servicio sobre el cual utiliza el estándar>
Descripción	<descripción sobre el uso del estándar dentro del servicio>
Ejemplo	
Código	CSS-01
Estándar	SAML 2.0
Servicio	Gestión de accesos
Descripción	Permite crear una misma autenticación eficiente de usuarios de forma nativa, sin la necesidad de tener una misma tecnología o modelo de seguridad.

Plantilla para la actividad de reglas, practicas y procedimientos de ciberseguridad

Información del documento	
Fase	Fase D: Arquitectura Tecnológica
Documento	Reglas, prácticas y procedimientos de ciberseguridad
Elaborado por	<persona o equipo que elaboro el documento>
Aprobado por	<persona responsable que aprueba el documento con sus procedimientos>
Versión	0.1
Fecha	<fecha de aprobación del documento>
Desarrollo del documento	
Propósito	Este documento lista las reglas, prácticas y procedimientos a nivel de solución para la protección de la arquitectura tecnológica
Actividades	
Código	<código de la norma>
Norma	<nombre de la norma>
Control	<tipo de control, definido por el modelo de clasificación de la organización para una determinada norma>
Procedimiento	<procedimiento que se lleva a cabo por la norma>
Referencias	<norma referencia por un determinado estándar si este es requerido>
Ejemplo	
Código	CSRPPT-01
Norma/regla	Gestión de seguridad en redes
Control	Controles de red
Procedimiento	Gestionar y controlar la red, bajo responsabilidades bien definidas y uso de logs con información para detectar fallos
Referencias	ISO 27001 A.13.1.1

Plantilla para la actividad de marco de referencia de ciberseguridad adaptado

Información del documento	
Fase	Fase D: Arquitectura tecnológica
Documento	Marco de referencia de ciberseguridad adaptado
Elaborado por	<persona o equipo que elaboro el documento>
Aprobado por	<persona responsable que aprueba el documento con sus procedimientos>
Versión	0.1
Fecha	<fecha de aprobación del documento>
Desarrollo del documento	
Propósito	Identificar los marcos de referencia necesarios para el trabajo de ciberseguridad en la arquitectura tecnológica
Actividades	
Código	<código del marco de referencia>
Marco	<nombre del marco de referencia>
Descripción	<descripción del marco de referencia>
Ejemplo	
Código	FCS-01
Marco	TOGAF-SABSA Integration
Descripción	Seguridad para AE

Planificacion de la transición

Fase E: Oportunidades y soluciones

Plantilla para la actividad del análisis de los procedimientos para el control de oportunidades y soluciones

Información del documento	
Fase	Fase E: Oportunidades y soluciones
Documento	Análisis de los procedimientos para el control de oportunidades y soluciones
Elaborado por	<persona o equipo que elaboro el documento>
Aprobado por	<persona responsable que aprueba el documento con sus procedimientos>
Versión	0.1
Fecha	<fecha de aprobación del documento>
Desarrollo del documento	
Propósito	Identificar, verificar y priorizar los procesos y soluciones propuestas en las etapas anteriores para asegurar que estado objetivo se integre bien a la arquitectura de la organización.
Actividades	
Código	<código del marco de referencia>
Proyecto	<nombre del proyecto o paquete de trabajo a implementar>
Descripción	<descripción del proyecto o paquete de trabajo a implementar >
Prioridad	<determinar la prioridad del proyecto (crítica, alta, media, baja)>
Propietario	<interesado que tiene el proyecto bajo su responsabilidad>
Ejemplo	
Código	PROY-01
Proyecto	Implementación de controles de sesión de usuario.
Descripción	Implementar controles de sesión de usuario para las funcionalidades críticas, consideradas como no públicas.
Prioridad	Alta
Propietario	Arquitecto de seguridad

Fase F: Planificación de la migración

Gobernanza

Plantilla para la actividad de control de migración

Información del documento	
Fase	Fase F: Planificación de la migración
Documento	Control de migración
Elaborado por	<persona o equipo que elaboro el documento>
Aprobado por	<persona responsable que aprueba el documento con sus procedimientos>
Versión	0.1
Fecha	<fecha de aprobación del documento>
Desarrollo del documento	
Propósito	Realizar una evaluación coste beneficio de los proyectos a implementar ademas de identificar y evaluar los riesgos asociados al mismo, para priorizar los proyectos, normas o procedimientos que generen valor al negocio a través de la implementacion de ciberseguridad
Actividades	
Código	<código del marco de referencia>
Proyecto, controles o procedimientos	<nombre del proyecto, control o procedimiento a implementar>
Riesgo	<Nivel de riesgo, asociado a la implementacion dentro de la arquitectura>
Costo	<Costo de la implementacion del proyecto, frente al beneficio proporcionado por el mismo>
Beneficio	<Determinar beneficio (p. ej. Alto, Medio, Bajo)>

Fase G: Gobierno de la implementación

Plantilla para la actividad de gestión de la ciberseguridad

Información del documento	
Fase	Fase G: Gobierno de la implementación
Documento	Gestión de la ciberseguridad
Elaborado por	<persona o equipo que elaboro el documento>
Aprobado por	<persona responsable que aprueba el documento con sus procedimientos>
Versión	0.1
Fecha	<fecha de aprobación del documento>
Desarrollo del documento	
Propósito	La gestión de la ciberseguridad define los roles y responsabilidades de ciberseguridad, implementación de gobernanza y rendimiento de ciberseguridad, indicadores de riesgo, y todos los puntos que intervienen dentro del proceso de implementación de ciberseguridad para la AE
Actividades	
Roles	<establecer los roles y responsabilidades para la implementación de ciberseguridad>
Gobernanza de ciberseguridad	<determinar que procesos y procedimientos serían necesarios para hacer frente a incidentes causados por un ataque o violación hacia los sistemas de información>
Definición del rendimiento de ciberseguridad	<definición del rendimiento de ciberseguridad como punto clave para la protección de los sistemas de información>
Indicadores de riesgo	<determinar los indicadores de riesgo dentro de la implementación de ciberseguridad para cada dominio de la AE>

Ejemplo	
Roles	Oficial de seguridad de la información
Gobernanza de ciberseguridad	**Inteligencia impulsada por la amenaza** Integrar e interiorizar las nuevas vulnerabilidades, amenazas y riesgos de implementar elementos adaptables, y alinear el riesgo con las necesidades del negocio. **Funciones de ciberseguridad integradas.** Integrar plenamente las funciones de ciberseguridad con las funciones de negocio, implementar el intercambio de información obligatoria y canales de comunicación bien definidos. **Proactiva y basada en la anticipación.** Anticiparse a los ataques y al comportamiento atacante, evite el minimalismo en la estrategia de ciberseguridad, implementar un ciclo de vida de seguridad sistémica. **Flexible, adaptable y resistente.** Adaptación de los cambios a implementar y autorreflexión operacional, aprendizaje organizacional y mejora, incluyen la continuidad del negocio y el pensamiento de la continuidad de servicios de TI **Servicios orientados hacia el negocio** Definir e implementar la ciberseguridad como un servicio a la organización.
Rendimiento clave de ciberseguridad	Prevención, detección, respuesta y seguimiento hacia los incidentes de ciberseguridad
Indicadores de riesgo	Determinar la probabilidad de que un evento ocurra y que afecte los sistemas de información

Plantilla para la actividad de auditoria de ciberseguridad

Información del documento	
Fase	Fase G: Gobierno de la implementación
Documento	Auditoria de ciberseguridad
Elaborado por	<persona o equipo que elaboro el documento>
Aprobado por	<persona responsable que aprueba el documento con sus procedimientos>
Versión	0.1
Fecha	<fecha de aprobación del documento>
Desarrollo del documento	
Propósito	Este documento que incluye las revisiones de ciberseguridad hacia los procesos implementados, diseños técnicos y código desarrollado contra las políticas, además de pruebas de seguridad y penetración
Actividades	
Proceso de auditoria	<determinar un proceso de auditoria como control interno para asegurar el funcionamiento y cumplimiento de la planificación, en donde se pueden ejercer los siguientes métodos: - Revisión de configuraciones - Auditoria de controles y operaciones - Pruebas técnicas de ciberseguridad o pruebas de penetración>
Estructura básica de un informe	
Código	<código del informe de pruebas>
Servicio auditado	<servicio objeto de las revisiones>
Pruebas	<pruebas realizadas hacia el servicio>
Hallazgos	<hallazgos encontrados en las pruebas>
Recomendaciones	<recomendaciones para corregir los errores encontrados>
Herramientas	<conjunto de herramientas utilizadas dentro de la auditoria>

Plantilla para la actividad de conciencia de ciberseguridad

Información del documento	
Fase	Fase G: Gobierno de la implementación
Documento	Conciencia de ciberseguridad
Elaborado por	<persona o equipo que elaboro el documento>
Aprobado por	<persona responsable que aprueba el documento con sus procedimientos>
Versión	0.1
Fecha	<fecha de aprobación del documento>
Desarrollo del documento	
Propósito	Este documento cita los puntos para la implementación de capacitación necesaria para asegurar la correcta implementación, configuración y funcionamiento de sistemas y componentes para ciberseguridad
Actividades	
Temas de Capacitación	<nombre de los temas de capacitación necesaria>
Roles	<roles que necesitan capacitación>
Periodo para capacitación	<intervalo de tiempo recomendable para capacitar>
Ejemplo	
Temas de Capacitación	Ingeniería social
Roles	Secretarias y operadores de sistemas
Periodo para capacitación	Recomendable 2 veces por año, y 1 vez mínimo

Plantilla para la actividad de gobernanza

Información del documento	
Fase	Fase G: Gobierno de la implementación
Documento	Gobernanza
Elaborado por	<persona o equipo que elaboro el documento>
Aprobado por	<persona responsable que aprueba el documento con sus procedimientos>
Versión	0.1
Fecha	<fecha de aprobación del documento>
Desarrollo del documento	
Propósito	Este documento cita los puntos evaluados para validar el cumplimiento de los proyectos planificados de ciberseguridad dentro de la arquitectura empresarial.
Actividades	
Objetivo	<Objetivo a cumplir dentro de un proyecto de ciberseguridad>
Descripción	<Descripcion del objetivo a cumplir dentro del o los proyectos de ciberseguridad>
Cumplimiento	<Porcentaje de cumplimiento del o los proyectos de ciberseguridad>
Responsable	<Responsable del o los proyectos de ciberseguridad>>
Ejemplo	
Objetivo	Actualizar políticas de ciberseguridad
Descripción	Determinar la complejidad de las contraseñas dentro de la institución
Cumplimiento	50%
Responsable	Oficial de seguridad

Fase H: Gestión de cambios de la arquitectura

Plantilla para la actividad de gestión de cambios

Información del documento	
Fase	Fase H: Gestión de cambios de la arquitectura
Documento	Gestión de cambios
Elaborado por	<persona o equipo que elaboro el documento>
Aprobado por	<persona responsable que aprueba el documento con sus procedimientos>
Versión	0.1
Fecha	<fecha de aprobación del documento>
Desarrollo del documento	
Propósito	Este documento cita los puntos para la implementación de capacitación necesaria para asegurar la correcta implementación, configuración y funcionamiento de sistemas y componentes para ciberseguridad
Actividades	
Código	<código del cambio requerido>
Item	<nombre del cambio solicitado o requerido>
Descripción	<descripción textual del cambio requerido>
Origen	<causa que originó el cambio, tanto técnico, debido a una solicitud, etc.>
Impacto	<nivel de impacto que puede generar el cambio, ejemplo: alto, medio, bajo>
Acción correctiva	<acción o acciones a seguir para controlar debidamente el cambio>
Ejemplo	
Código	CM-01
Item	Cambio en las políticas
Descripción	Adaptar las políticas de ciberseguridad para establecer estrategias ante ataques informáticos
Origen	Falta de una referencia en cuanto a ciberseguridad para el personal técnico
Impacto	Medio
Acción correctiva	Modificar las políticas de seguridad de la información con un apartado para políticas de ciberseguridad, o Elaborar un documento de políticas de ciberseguridad

Plantilla para la actividad de gobernanza de la arquitectura de ciberseguridad

Información del documento	
Fase	Fase H: Gestión de cambios de la arquitectura
Documento	Gobernanza de la arquitectura de ciberseguridad
Elaborado por	<persona o equipo que elaboro el documento>
Aprobado por	<persona responsable que aprueba el documento con sus procedimientos>
Versión	0.1
Fecha	<fecha de aprobación del documento>
Desarrollo del documento	
Propósito	Este documento recoge los cambios que requeridos, debido a fallas en los controles o procedimientos implementandos, para así planificar una nueva iteración
Actividades	
Código	<código del cambio requerido>
Cambio	<nombre del cambio solicitado o requerido>
Control	<tipo del control que será afectado >
Origen	<causa que originó el cambio, tanto técnico, debido a una solicitud, etc.>
Impacto	<nivel de impacto que puede generar el cambio, ejemplo: alto, medio, bajo>
Ejemplo	

Código	CSAG-01
Cambio	Cambio en los controles de validación de sesiones de usuario
Control	Control de sesiones de usuario.
Origen	Vulnerabilidad en la validación de sesiones de usuario.
Impacto	Medio

CAPÍTULO IV

HERRAMIENTA PARA LA VALIDACIÓN DE IMPLEMENTACIÓN DE LA GUÍA DE CIBERSEGURIDAD PARA ARQUITECTURA EMPRESARIAL

4.1. Introducción.

Dentro de los objetivos del desarrollo de la *guía de ciberseguridad para arquitectura empresarial*, se encuentra la implementación de una herramienta, la cual permita validar la implementación de las actividades de ciberseguridad en una AE.

4.2. Investigación de herramientas para implementación de ciberseguridad.

4.2.1. Herramienta de ciberseguridad.

The Cyber Security Modeling Language (CySeMol)

Es una herramienta que utiliza un lenguaje para el modelado de arquitecturas de sistemas a nivel de la organización, trabaja junto a un motor de inferencia probabilística y de acuerdo a un meta-modelo que utiliza redes bayesianas.

Si los sistemas informáticos de una organización se modelan con CySeMoL (Figura 23), este motor de inferencia puede evaluar la probabilidad de que un ataque tenga éxito contra los sistemas de información. La teoría utilizada para los cálculos de probabilidad de ataque en CySeMoL, de basan en una compilación de resultados de investigación, sobre una serie de dominios de seguridad que cubre una amplia gama de ataques y contramedidas, basados en el conocimiento obtenido por expertos en el dominio del tema.

En este trabajo, la teoría también se valida a nivel del sistema. Un ensayo indica que la razonabilidad y la corrección de las evaluaciones CySeMoL se comparan con la razonabilidad y la exactitud de las evaluaciones de un profesional de la seguridad. Otro aspecto que posee esta herramienta es posibilidad de adaptar sus modelos a las necesidades del arquitecto o el usuario que lo utilice.

Entre otras cosas la herramienta ofrece la capacidad para evaluar la ciberseguridad de las arquitecturas de TI existentes o virtuales, sin necesidad de contar con expertos en ciberseguridad.

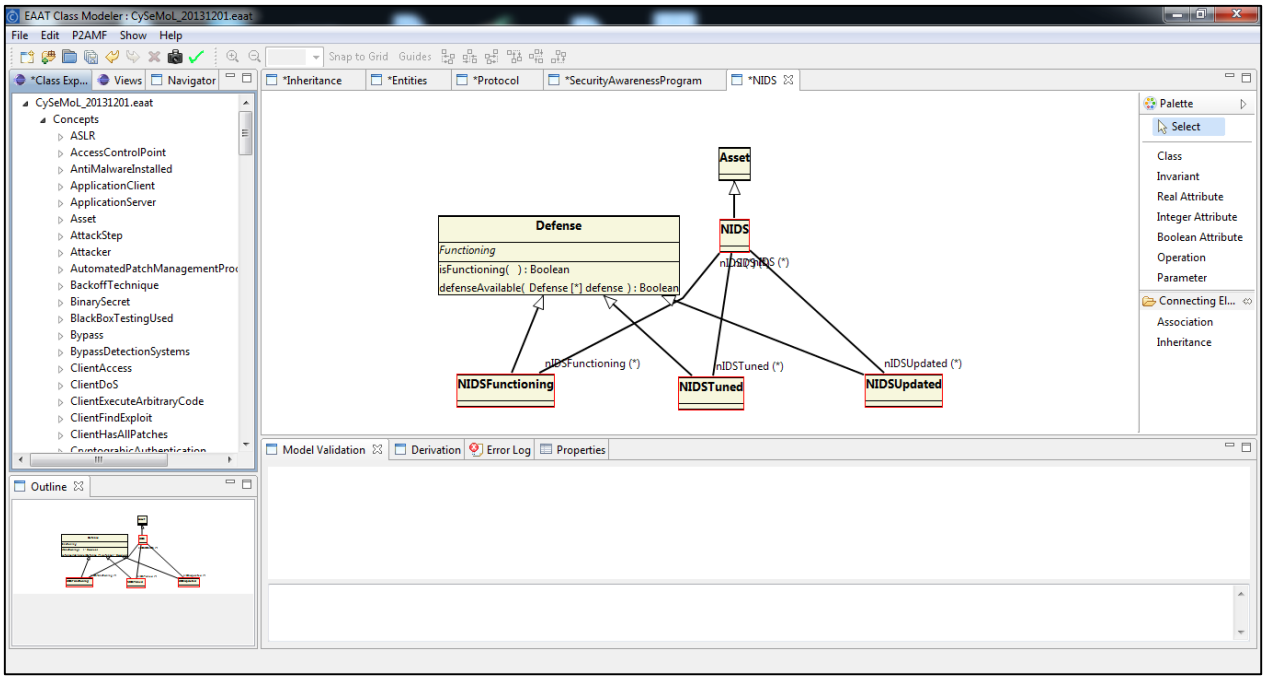

Figura 23 – Interfaz de CySeMol

Fuente: (Autor, 2014)

4.2.2. Herramientas de modelado de architectura empresarial.

En la gestión de procesos y controles de ciberseguridad que se pueden trabajar dentro de AE, se han investigado dos de las principales herramientas de AE, que ademas de sus características de modelado, se podría asociar como una solución dentro de la labor de validación y/o control de la implementacion de las actividades de la guía de ciberseguridad para AE:

Enterprise Architect.

Proporciona modelado completo del ciclo de vida para:

- Sistemas empresariales y de TI
- Software e Ingeniería de Sistemas
- Desarrollo en tiempo real e integrado

Con las capacidades de gestión de requisitos integrado, Enterprise Architect (Figura 24) ayuda a rastrear especificaciones de alto nivel para análisis, diseño, implementación, prueba y mantenimiento de modelos utilizando UML[13], SysML[14], BPMN[15] y otros estándares abiertos.

Enterprise Architect es un multi-usuario, una herramienta gráfica diseñada para ayudar a sus equipos a construir sistemas robustos y fáciles de mantener.

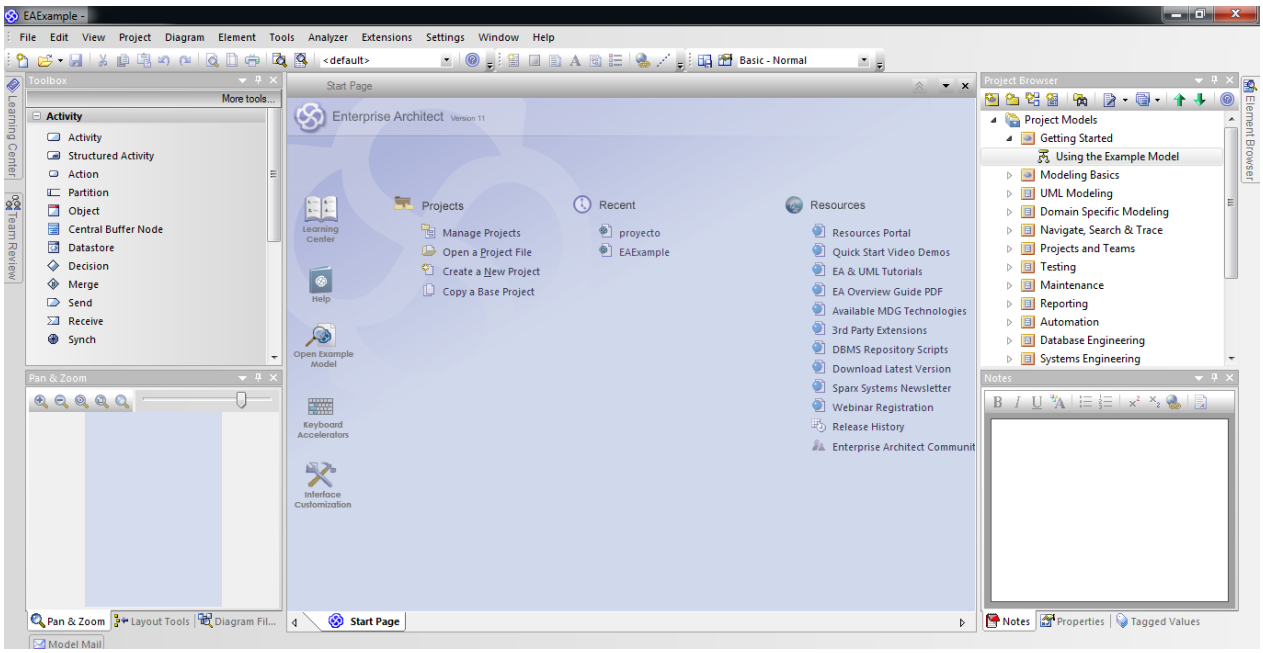

Figura 24 – Enterprise Architect

Fuente: (Autor, 2014)

ArchiMate.

De acuerdo a (Archi, 2013), ArchiMate (Ver Figura 25) "es un estándar abierto e independiente de AE que apoya la descripción, análisis y visualización de la arquitectura dentro y a través de los dominios de negocio. ArchiMate es uno de los estándares abiertos organizados por The Open Group y está totalmente alineada con TOGAF. ArchiMate ayudas los interesados en la evaluación del impacto de las opciones de diseño y cambios"

[13] UML: "Es un lenguaje gráfico para visualizar, especificar y documentar cada una de las partes que comprende el desarrollo de software". http://users.dcc.uchile.cl/~psalinas/uml/introduccion.html

[14] SysML: "Proporcionar técnicas de modelado de una gran variedad de sistemas, entre los que se encuentran contemplados sistemas hardware, software, datos, personas, procedimientos e instalaciones". https://sites.google.com/site/julianandresf/sysml

[15] BPMN: "Es una notación gráfica que describe la lógica de los pasos de un proceso de Negocio. http://www.bizagi.com/esp/descargas/BPMNbyExample.pdf?token=1.3.0.0 "

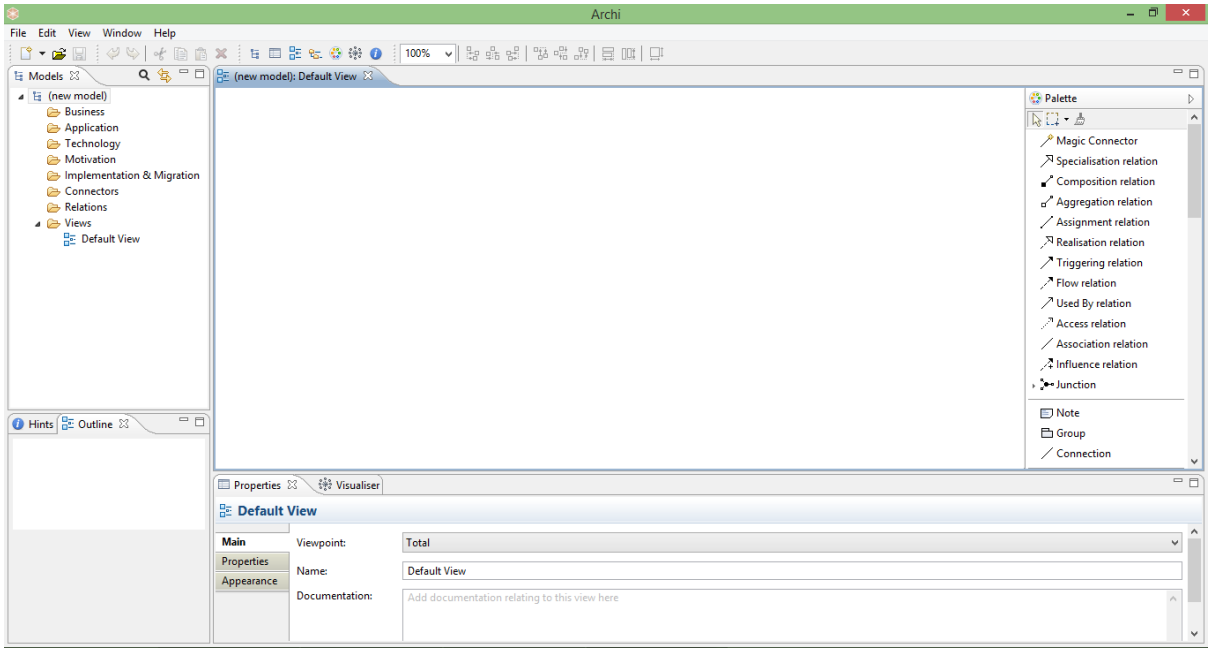

Figura 25 – Enterprise Architect

Fuente: (Autor, 2014)

4.2.3. Resultados basados en las herramientas investigadas.

Luego de investigar sobre las herramientas que permitan validar la implementación de ciberseguridad, se ha concluido que las mismas no cuentan con las características requeridas, estas herramientas se orientan solamente al modelado de procesos de una organización, y no hacia la validación de controles o procesos que se encuentran dentro del trabajo de la ciberseguridad, por tal motivo se ha propuesto desarrollar una aplicación, cuyo objetivo sea validar el cumplimiento de las actividades de la guía de ciberseguridad para AE.

4.3. Sistema validación de implementación de ciberseguridad para arquitectura empresarial.

4.3.1. Modelo de la aplicación.

Considerando el uso de tecnología de la información y la difusión masiva de su contenido, se ha decido implementar una aplicación web como herramienta, para permitir la conexión de usuarios desde varios puntos a través del internet y compartir las actividades desarrolladas dentro de la guía para validar la implementación de ciberseguridad en una AE.

4.3.2. Desarrollo de la aplicación.

Como parte del desarrollo de la aplicación se presentan los siguientes entregables basados en la metodología RUP (Rational Unified Process) que contribuye en el desarrollo eficiente y eficaz del sistema, estos entregables estan divididos de acuerdo a las fases de RUP:

Fase de Inicio: define y acuerda el alcance del proyecto, identifica los riesgos asociados al proyecto, propone una visión general de la arquitectura de software y produce el plan de fases y de iteraciones posteriores.

- Documento de visión (Anexo B)
- Documento de especificación de requerimientos (Anexo C)

Fase de Elaboración: selecciona los casos de uso que permite definir la arquitectura base del sistema, donde se diseña la solución preliminar.

- Diagrama de clases (Anexo D)
- Diagrama de casos de uso (Anexo E)

Fase de construcción: conpleta las funcionalidades del sistema, donde se clarifican los requerimientos pendientes, se administran los cambios de acuerdo a las evaluaciones realizadas y se realizan las mejoras del proyecto.

- Diagrama de secuencia (Anexo F)
- Diagrama de actividades (Anexo G)

Fase de cierre: asegura que el sistema o software este disponible para los usuarios finales, se ajustan errores y defectos encontrados en las pruebas de aceptación.

- Manual de usuario (Anexo H)

4.3.3. Objetivos técnicos de la aplicación.

- El acceso a las propiedades del sistema solo será posible para usuarios registrados en el mismo.
- Asignación de roles (Administrador, Cliente) a nivel de aplicación.
- La aplicación tiene la capacidad de soportar el flujo de usuarios activos, realizando las operaciones para las cuales fue desarrollada.
- El sistema permitirá generar un reporte en formato pdf sobre los items cumplidos por el usuario, mas las recomendaciones por las actividades que aun no se han cumplido.

4.3.3.1. Herramientas para el desarrollo de la aplicación.

- **Java:** es un lenguaje de programación orientado a objetos, de plataforma independiente, en la cual se pueden realizar distintos aplicativos.
- **JSP**: JSP (JavaServer Pages) es una tecnología que permite desarrollar páginas web dinámicas basadas en HTML y XML; utiliza Java como lenguaje de programación, y está construida sobre la base de servlet.

- **Java Script:** es un lenguaje de programación interpretado, orientado a páginas web y trabaja del lado del servidor, el cual se utiliza para la creación de páginas web dinámicas incorporando efectos y ejecutando funciones a través de opciones (p. ej. botones).
- **Netbeans:** es un entorno de desarrollo integrado libre y gratuito, el cual trabaja principalmente con el lenguaje de programación Java.
- **MySQL:** es un sistema para la gestión de bases de datos relacionales, multihilo y multiusuario, además de ser multiplataforma.
- **Apache Tomcat:** es un software multiplataforma desarrollado con Java que sirve como servidor web con soporte de servlets y JSPs.

4.3.3.2. Resultados esperados.

Los resultados deseados a través de la aplicación es la validación de la guía de ciberseguridad para arquitectura empresarial a través de un conjunto de items, que verifiquen el cumplimientos de las actividad de cada fase de la guía propuesta.

4.3.3.3. Construcción del sistema.

El sistema será construido en base a una arquitectura tres capas y un nivel, como se puede ver en la figura 26.

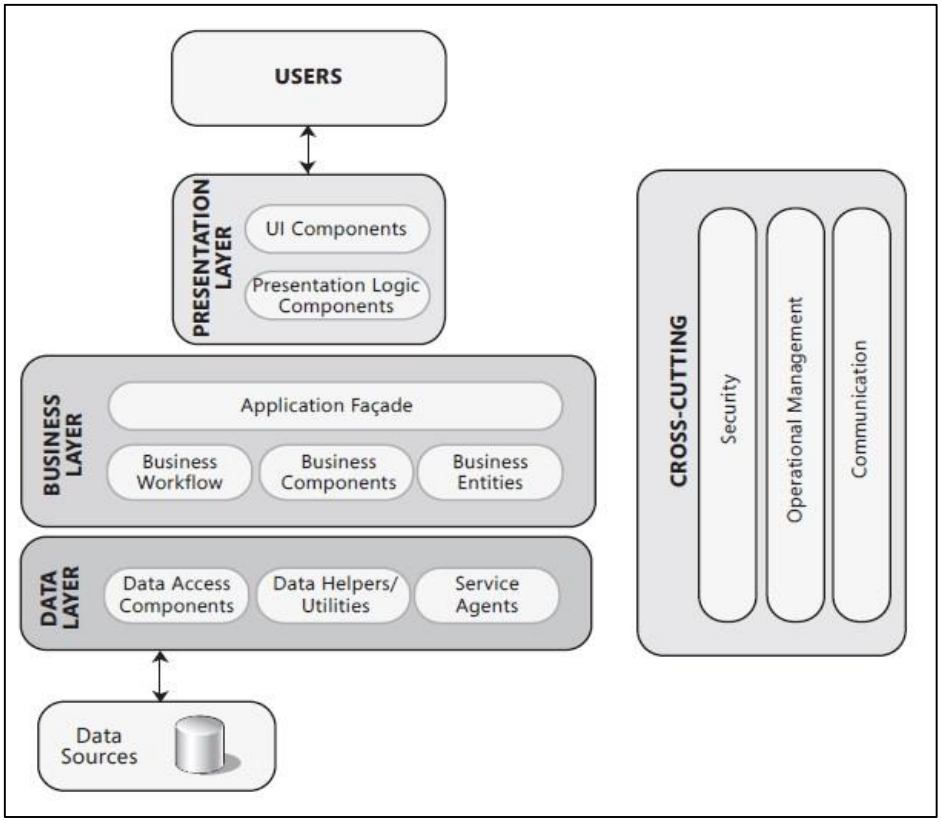

Figura 26. Arquitectura tres capas

Fuente: Tomado y adaptado de Microsoft Aplication Architecture Guide (Microsoft, 2009)

4.3.3.4. Carga de datos del sistema.

Dentro de la base de datos se almacena toda la información que requiere el sistema, como: usuarios, empresas, items, actividades, fases, etc. Dentro de la figura 27 se puede observar el modelo de la base de datos relacional que utilizará el sistema.

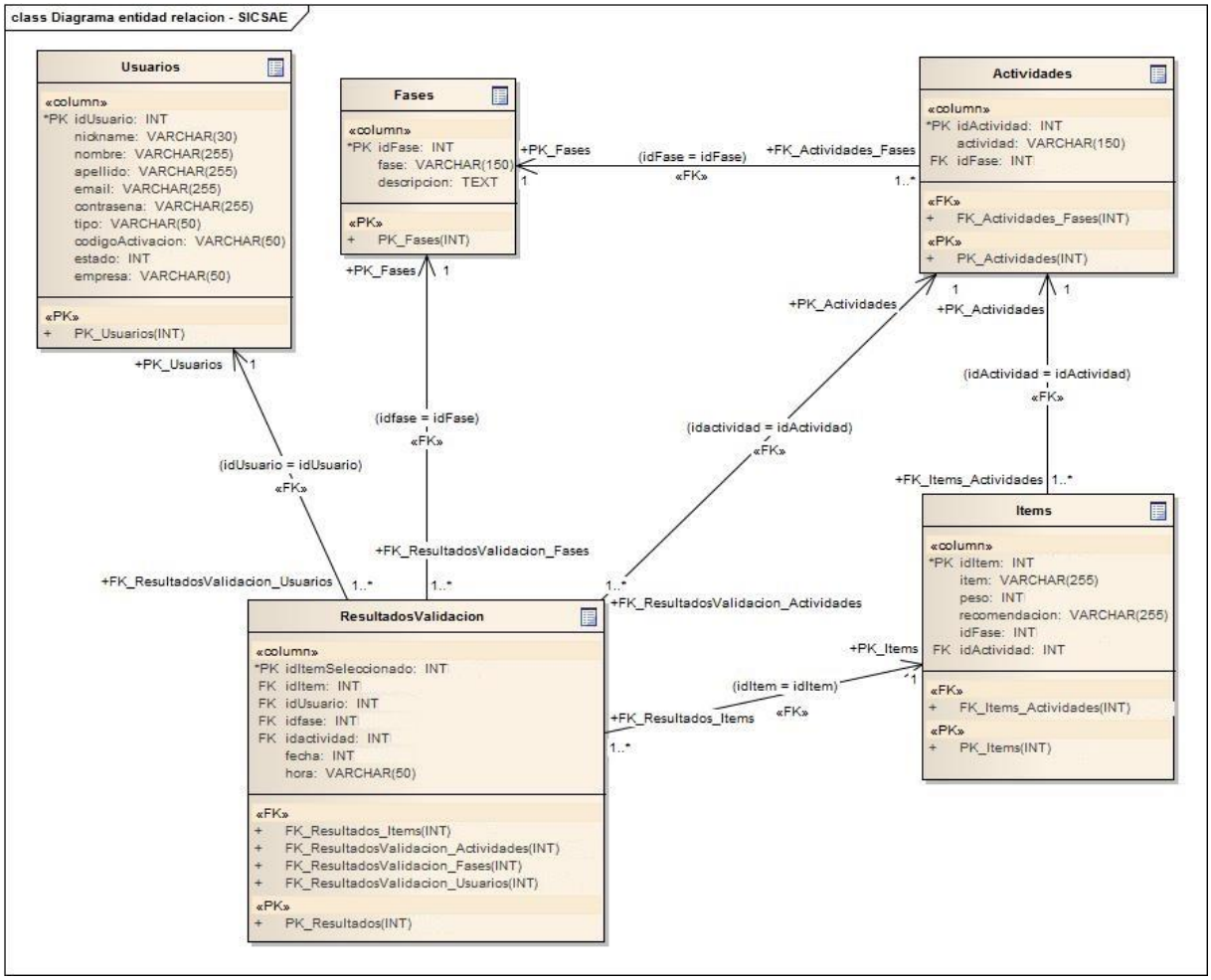

Figura 27. Modelo relacional de la base de datos de SICSAE

Fuente: (Autor, 2014)

4.3.3.5. Control de acceso al sistema.

Es sistema mendiante un formulario de autenticación, solicitará al administrador o cliente registrado, ingresar su usuario y contraseña.

4.3.3.6. Presentar datos.

Esta operación permitirá listar usuarios, items, recomendaciones, fases y actividades, de acuerdo a las necesidades que tenga el usuario.

4.3.3.7. Guardar datos.

Se guardará la información del registro de un nuevo usuario, así mismo como nuevos items y recomendaciones, ademas se guardaran los items de las operaciones de validación realizadas por un usuario tipo clientes dentro del sistema.

4.3.3.8. Calcular datos.

De acuerdo a la información guardada por el usuario de tipo cliente, se realizan cálculos para determinar con el peso de un item el porcentaje cumplido en cada actividad de la guía de ciberseguridad para AE, y así proporcionar un informe al usuario.

CAPÍTULO V
PRUEBAS DE VALIDACIÓN DE LA GUÍA DE CIBERSEGURIDAD PARA ARQUITECTURA EMPRESARIAL

5.1. Pruebas de validación de la guía de ciberseguridad para arquitectura empresarial.

Para el proceso de validación de la guía de ciberseguridad, se ha tomado como caso de estudio a la empresa Lunyxtec, donde se ha ido comprobando cada una de las actividades de las fases de la guía para asi verificar el nivel de ciberseguridad existente de acuerdo a un conjunto de items elaborados acorde a cada actividad de las fases del ADM.

5.2. Evaluación de Resultados.

De acuerdo a las pruebas de verificación de ciberseguridad, en la figura 28 se puede observar el porcentaje de cumplimiento en cada una de sus fases, donde se puede ver que existe un nivel de cumplimiento que escasamente promedia el 50%.

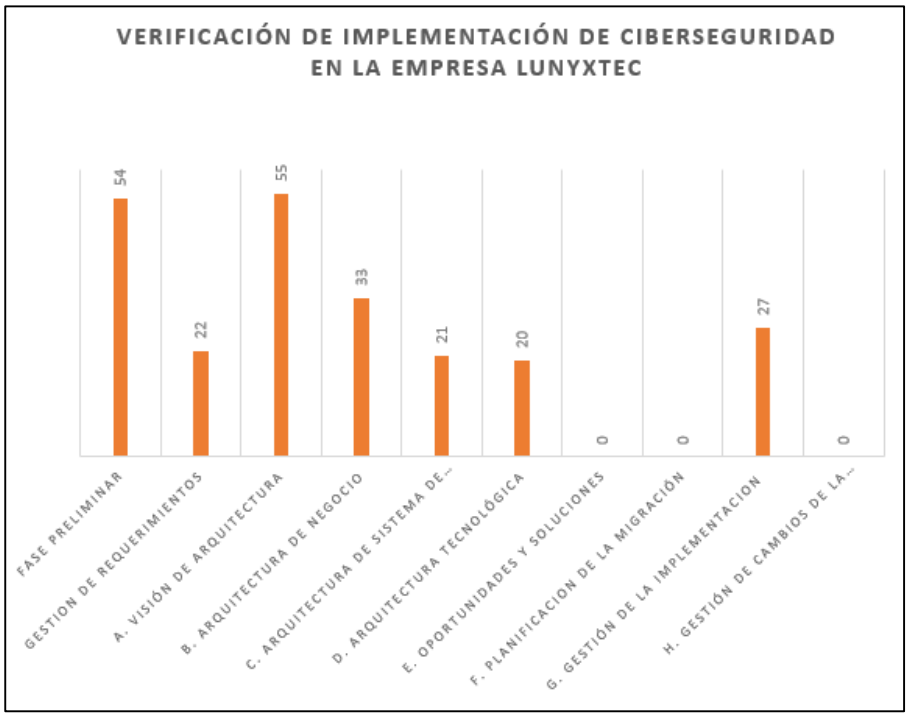

Figura 28 – porcentaje de cumplimiento de ciberseguridad de acuerdo a cada fase de la guía

Fuente: (Autor, 2014)

Como se puede observar en la figura 28, no existe una debida gestión de ciberseguridad dentro del caso evaluado, para sus procedimientos, políticas, principios, auditoria y uso de buenas prácticas en cuando a normas y marcos de trabajo.

En la figura 29, se puede ver la cantidad de items cumplidos y los que aún no se han cumplido por parte de la empresa evaluada, para así alcanzar un nivel aceptable en la gestión de ciberseguridad.

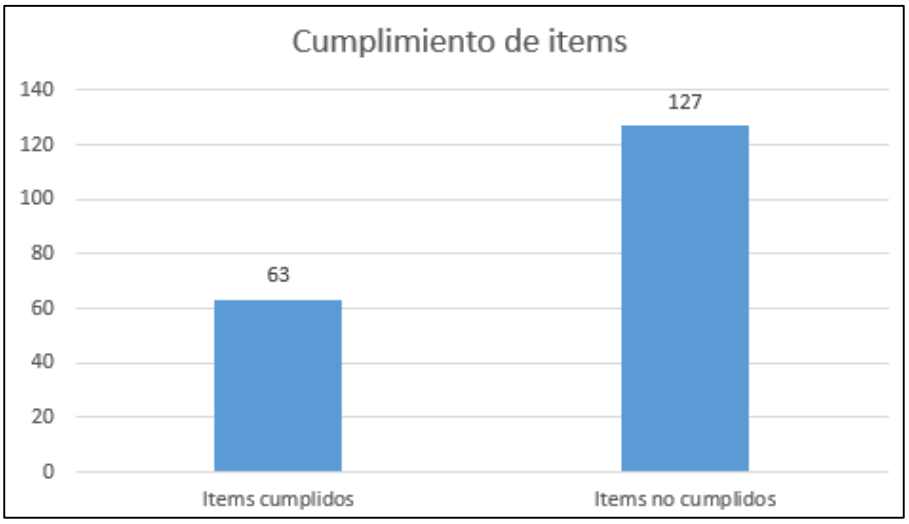

Figura 29 – Items cumplidos y no cumplidos en la organización evaluada

Fuente: (Autor, 2014)

En los siguientes gráficos se puede observar con mayor detalle los items que han sido cumplidos y los que aún no han sido cumplidos en cada actividad, para validar el trabajo necesario de ciberseguridad.

En el figura 30, se puede ver la fase de gestión de requerimientos, la cual controla los requerimientos de cada una de las fases dentro de las iteraciones del ADM; dentro de esta fase existen las actividades de control de requerimientos y la de atributos del perfil de negocio para ciberseguridad que se resumen en la tabla 11, la figura 30 muestra que ambas actividades destinadas a la gestión y control de requerimientos no se cumple ni en un 50%, lo que causa un deficiencia en el control de las actividades de las fases del ADM, ya que solo se llega a un 22% de cumplimiento.

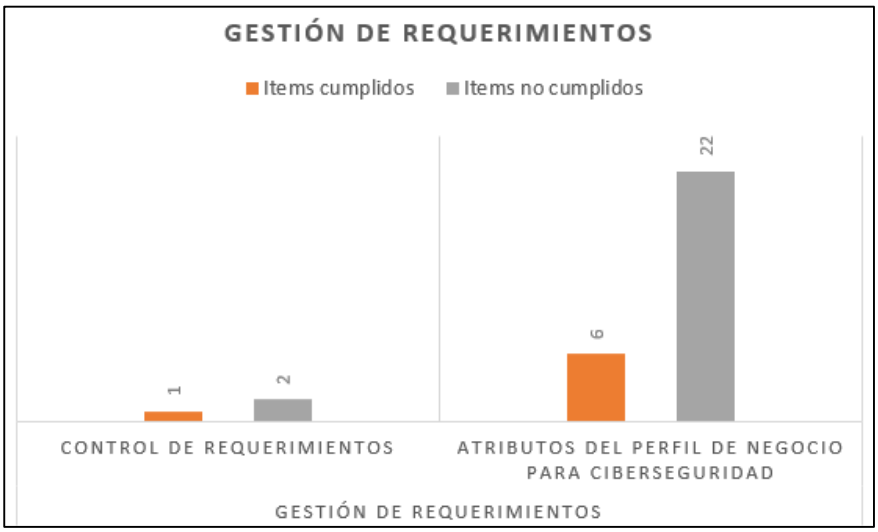

Figura 30 – Items cumplidos y no cumplidos dentro de la fase de gestión de requerimientos

Fuente: (Autor, 2014)

Tabla 11. Cumplimiento de items en la fase de gestión de requerimientos

Fase	Actividad	Total items	Items cumplidos	Items no cumplidos
Gestión de requerimientos	Control de requerimientos	3	1	2
	Atributos del perfil de negocio para ciberseguridad	28	6	22

Fuente: (Autor, 2014)

En la figura 31, se puede observar el resultado de los items validados en la iteración de evaluación de capacidad arquitectónica, donde se validaron las actividades de la fase preliminar y de visión de arquitectura, las mismas que se resumen en la tabla 12, los resultados de esta validación muestran que dentro de la fase preliminar se alcanza un 54% de cumplimiento, lo que representa que el equipo de ciberseguridad, las áreas de riesgo y los principios de ciberseguridad no se han identificado completamente, esto causa que existan vacios dentro de la planificación inicial, que resultaría en una perspectiva poco clara del trabajo necesario de ciberseguridad; en la fase de visión de arquitectura se alcanza un 55% de cumplimiento, basado en este porcentaje se determina que en las actividades de requerimientos y marcos de trabajo de ciberseguridad no se ha obtenido la totalmente la información requerida para refinar el trabajo de ciberseguridad.

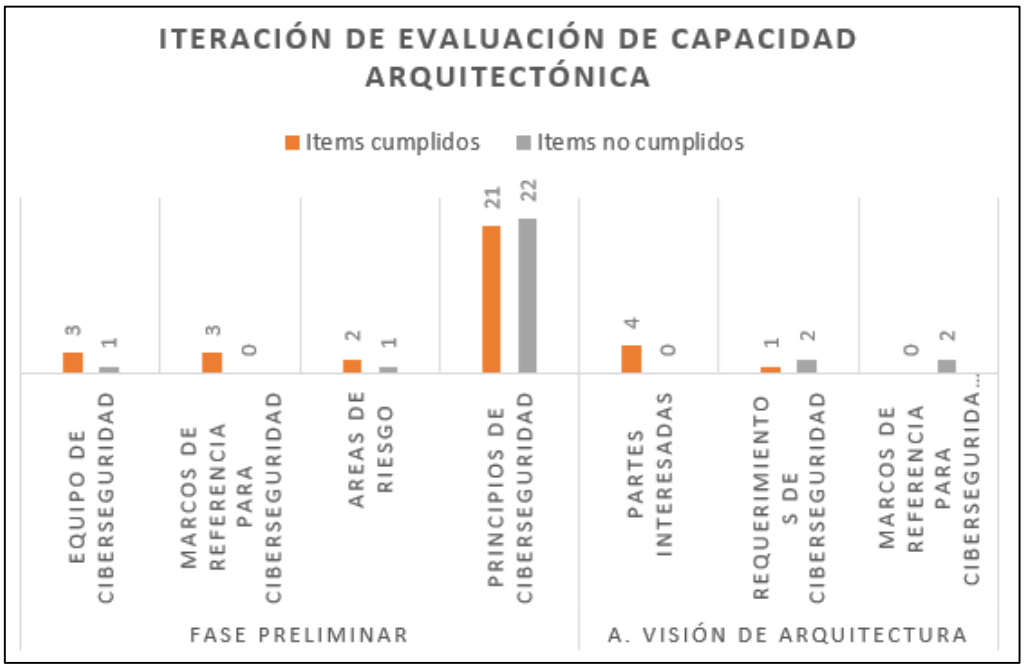

Figura 31 – Items cumplidos y no cumplidos en la iteración de evaluación de capacidad arquitectónica

Fuente: (Autor, 2014)

Tabla 12. Cumplimiento de items en la iteración de evaluación de capacidades

Fase	Actividad	Total items	Items cumplidos	Items no cumplidos
Fase preliminar	Equipo de ciberseguridad	4	3	1
	Marcos de referencia para ciberseguridad	3	3	0
	Areas de riesgo	3	2	1
	Principios de ciberseguridad	43	21	22
Gestión de requerimientos	Control de requerimientos	3	1	2
	Atributos del perfil de negocio para ciberseguridad	28	6	22
A. Visión de arquitectura	Partes interesadas	4	4	0
	Requerimientos de ciberseguridad	3	1	2
	Marcos de referencia para ciberseguridad adaptado	2	0	2

Fuente: (Autor, 2014)

En la figura 32 se muestran los resultados de la validación en la iteración de desarrollo, donde se encuentran las fases de arquitectura de negocio, arquitectura de SI, y arquitectura tecnológica, con sus respectivas actividades; en la tabla 13 se puede observar el resumen de las fases evaluadas, que indican que no se han implementado o definido, políticas de ciberseguridad, servicios, y estándares o normas de ciberseguridad, además de una débil implementación de controles de ciberseguridad dentro de los sistemas de información y arquitectura tecnológica.

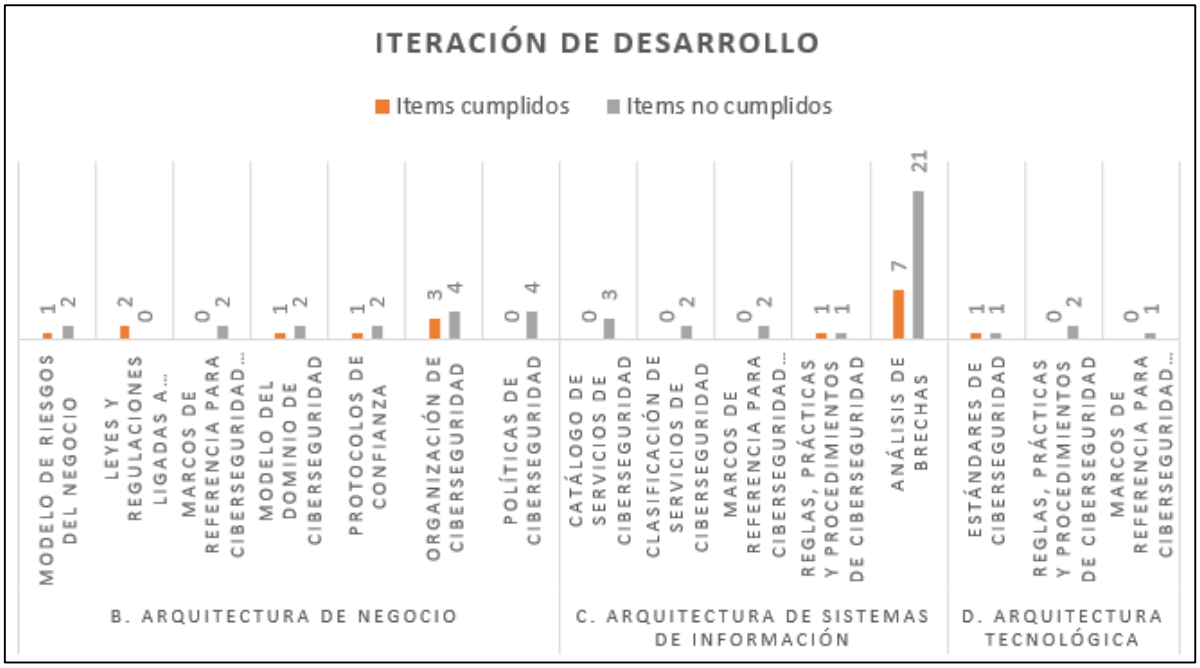

Figura 32 – Items cumplidos y no cumplidos en la iteración de desarrollo

Fuente: (Autor, 2014)

Tabla 13. Cumplimiento de items en la iteración de desarrollo

Fase	Actividad	Total items	Items cumplidos	Items no cumplidos
B. Arquitectura de negocio	Modelo de riesgos del negocio	3	1	2
	Leyes y regulaciones ligadas a ciberseguridad	2	2	0
	Marcos de referencia para ciberseguridad adaptado	2	0	2
	Modelo del dominio de ciberseguridad	3	1	2
	Protocolos de confianza	3	1	2
	Organización de ciberseguridad	7	3	4
	Políticas de ciberseguridad	4	0	4
C. Arquitectura de sistemas de información	Catálogo de servicios de ciberseguridad	3	0	3
	Clasificación de servicios de ciberseguridad	2	0	2
	Marcos de referencia para ciberseguridad adaptado	2	0	2
	Reglas, prácticas y procedimientos de ciberseguridad	2	1	1
	Análisis de brechas	28	7	21
D. Arquitectura tecnológica	Estándares de ciberseguridad	2	1	1
	Reglas, prácticas y procedimientos de ciberseguridad	2	0	2
	Marcos de referencia para ciberseguridad adaptado	1	0	1

Fuente: (Autor, 2014)

En la figura 33, se puede ver el resultado de la iteración de transición, donde interviene la fase de oportunidades y soluciones, y la fase de planificación de la migración, en la tabla 14 se puede ver el resumen de los items evaluados, que revelan una participación nula en las actividades evaluadas, lo que representa un bajo control para las soluciones o procedimientos propuestos durante la iteración de desarrollo, esto podría causar que no se consideren los riesgos de la integración de nuevos procedimientos dentro de la arquitectura de SI o TI.

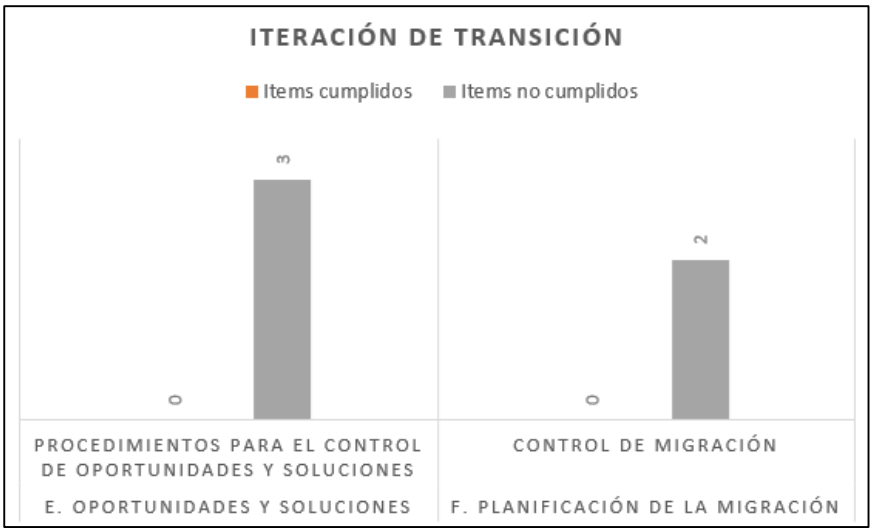

Figura 33 – Items cumplidos y no cumplidos en la iteración de transición

Fuente: (Autor, 2014)

Tabla 14. Cumplimiento de items en la iteración de transición

Fase	Actividad	Total items	Items cumplidos	Items no cumplidos
E. Oportunidades y soluciones	Procedimientos para el control de oportunidades y soluciones	3	0	3
F. Planificación de la migración	Control de migración	2	0	2

Fuente: (Autor, 2014)

Dentro de la figura 34, se puede observar la iteración de gobernanza, donde se encuentra la fase de gobierno de la implementación y la fase de gestión de cambios de la arquitectura con sus respectivas actividades; en la tabla 15 se puede observar el resumen de items validados, donde se puede ver, que en la fase de gobierno de la implementacion existe un bajo cumplimiento de las auditorias de ciberseguridad de los sistemas y procedimientos que se han ido desarrollando, ademas de un nulo cumplimiento para la gestión de una debida conciencia de ciberseguridad, también se puede observar que en las actividades de la fase de gestión de cambios no existe el debido cumplimiento, lo que genera que los cambios que aparecen durante las iteraciones no se gestionen de la mejor manera, y que no se verifique que el trabajo realizado se este cumpliendo conforme a los requerimientos iniciales, haciendo que se genere inestabilidad en las fases trabajadas dentro del ADM, que luego afecten a la AE.

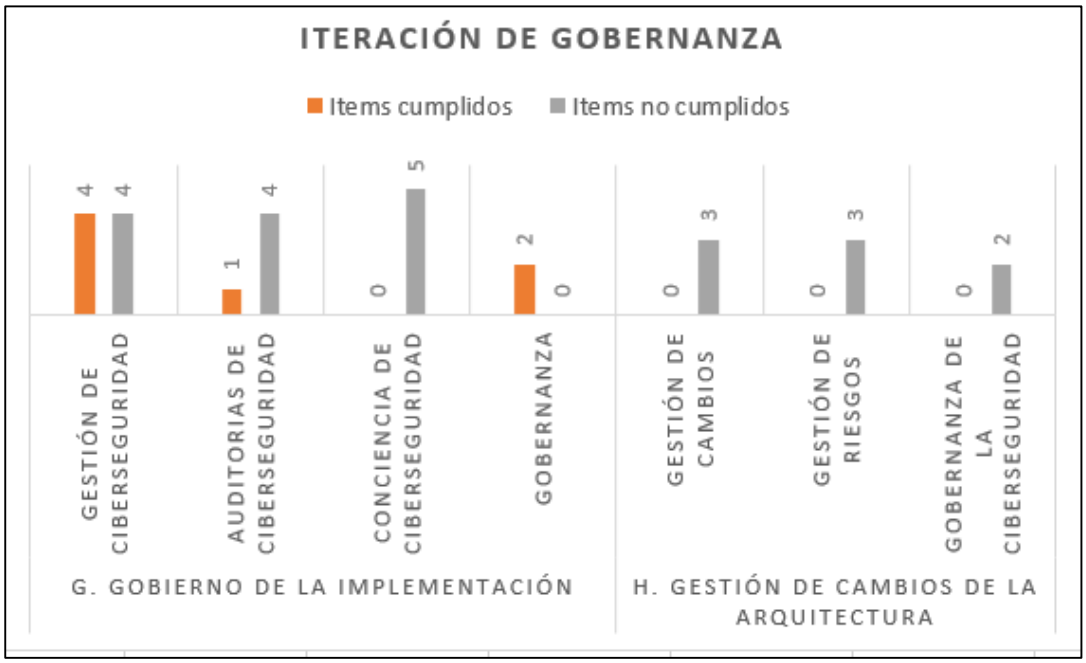

Figura 34 – Items cumplidos y no cumplidos en la iteración de gobernanza

Fuente: (Autor, 2014)

Tabla 15. Cumplimiento de items en la iteración de gobernanza

Fase	Actividad	Total items	Items cumplidos	Items no cumplidos
G. Gobierno de la implementación	Gestión de ciberseguridad	8	4	4
	Auditorias de ciberseguridad	5	1	4
	Conciencia de ciberseguridad	5	0	5
	Gobernanza	2	0	2
H. Gestión de cambios de la arquitectura	Gestión de cambios	3	0	3
	Gestión de riesgos	3	0	3
	Gobernanza de la ciberseguridad	2	0	2

Fuente: (Autor, 2014)

Es significativo destacar, que dentro de la implementación de ciberseguridad, es importante tomar en consideración el alcance del trabajo de ciberseguridad de acuerdo SI, tamaño de la empresa, TI y otros factores como leyes y regulaciones, para determinar el total de las actividades que se pueden utilizar de la presente guía.

CONCLUSIONES

A través del trabajo desarrollado, en la elaboración de la guía de ciberseguridad para arquitectura empresarial se ha concluido que:

- Una organización que cuente con una AE formalmente definida, facilita la integración de ciberseguridad dentro de la misma, debido a que se aprovechan los procesos trabajados dentro de ella. De acuerdo al caso de estudio, se observa que si los procesos de AE no han sido trabajados formalmente, afecta a cada una de las fases y se refleja en el nivel de la ciberseguridad.
- La flexibilidad proporcionada por el ADM-TOGAF y su capacidad para trabajar con otras normas y marcos de trabajo, permiten adaptar las actividades requeridas de ciberseguridad en cada una de sus fases. Los controles, técnicas y procesos de estas normas y marcos de trabajo de COBIT 5, ISO 27001, ISO 27032 y NIST, permitieron elaborar un marco de referencia de ciberseguridad para trabajar dentro del entorno de una AE; en donde cada actividad que se validó en el caso de estudio, y que no haya sido cumplida de acuerdo a las normas y marcos de trabajo propuestos, representan un punto bajo dentro de la fase a la que pertenecen y por consiguiente en la ciberseguridad de la AE.
- La evaluación que se realiza mediante el análisis de brechas, durante la fase de Arquitectura de SI para identificar el estado actual y así definir un estado objetivo, debe ser una prioridad para mejorar la seguridad en los controles de los SI, más los puntos elaborados dentro de las políticas de ciberseguridad de la fase de Arquitectura de Negocio, que determinan el horizonte a alcanzar con la ciberseguridad.
- La importancia que se dé al trabajo y gestión de ciberseguridad, es un tema que debe ser considerado desde el nivel más alto de la cadena de mando hasta el más bajo, donde se lleve una comunicación fluida para actuar ágilmente ante el riesgo de ataques informáticos y así mismo resolverlos, esta importancia va ligada desde los principios y requerimientos de ciberseguridad, para así tener claro el trabajo de la ciberseguridad y lo que se tratara de resolver con la misma.
- Los marcos de trabajo, normas y guías de seguridad de la información y ciberseguridad en una AE, no cubren la totalidad de los procesos de seguridad a través de una primera iteración, por tal motivo se debe priorizar los elementos críticos, para fortalecerlos e ir incorporando controles y procedimientos que mejoren continuamente los mecanismos de ciberseguridad.

- Identificar los activos, servicios y procesos que se desean proteger, permiten alcanzar mayor efectividad, para obtener una mejor protección y agilidad en la gestión del trabajo de ciberseguridad.
- Las actividades proporcionadas dentro de la guía, no implica obligatoriedad en su cumplimiento, las mismas se pueden ir desarrollando de acuerdo a las necesidades de la organización, que necesite de ciberseguridad.
- Para identificar y determinar las actividades necesarias para cada fase del ADM relacionadas a la ciberseguridad, fue importante el uso del modelo proporcionado por libro blanco de la integración de TOGAF y SABSA, debido a los entregables que trabajan dentro de cada fase.
- Los controles de la norma ISO-27001, proporcionan un enfoque altamente útil para el trabajo de ciberseguridad, especialmente en la protección de SI, y gestión de incidentes, así mismo como buenas prácticas dentro de políticas de seguridad.
- Dentro de las herramientas investigadas, no se han encontrado aplicaciones que validen el uso de ciberseguridad para una AE, estas aplicaciones solo cubren una parte de los procesos de TI, o el modelado de los mismos en una organización.

RECOMENDACIONES

Una ves concluido el trabajo de tesis de la guía de ciberseguridad para AE, se sugiere tomar en consideración las siguientes recomendaciones:

- Para implementar controles, normas y procedimientos de ciberseguriadad en una organización, se debe tomar en consideración que la AE es la clave del negocio y de las tecnologías y sistemas de informacion.
- Para utilizar o desarrollar actividades que permitan trabajar la ciberseguridad dentro de un entorno empresarial, se debe tomar en cuenta que cada empresa requiere un trabajo diferente, de acuerdo a sus servicios y tipo de tecnología, por tal motivo es idóneo plantear un marco genérico que se pueda adaptar a las necesidades del negocio para alinearlo a la parte tecnológica.
- Aprovechar las capacidades que ofrece una AE, para integrar el trabajo de ciberseguridad de manera que fortalezca la seguridad de SI dentro del internet.
- Utilizar normas y marcos de trabajo basados en ciberseguridad, seguridad de la información y riesgos, los cuales proveen un conjunto de procesos, controles y diversos dominios que se pueden aprovechar para la construcción de un único marco de referencia destinado para la gestión de ciberseguridad dentro de una organización.
- Para no caer en el incumplimiento y posterior sanción debido a leyes y reglamentaciones estipuladas constitucionalmente, es necesario investigarlas, estudiarlas y apegarse a ellas, de forma que se las pueda utilizar del lado de la organización que se desea implementar el trabajo de ciberseguridad.
- El uso de nuevas técnicas, marcos de trabajo y normas de ciberseguridad pueden ayudar a reforzar las actividades desarrolladas en cada fase, para asi trabajar la ciberseguridad de forma continua.
- Dentro de las actividades de las fases de arquitectura de SI y arquitectura tecnológica, se sugiere complementar el trabajo con técnicas y/o herramientas que sean de preferencia de los ingenieros o técnicos de la organización, para los aspectos de mejora de seguridad.
- Para utilizar esta guía como referencia de un trabajo futuro, se recomienda trabajar el conjunto de las fases por iteración, de modo que se puedan gestionar los componentes tecnológicos de una organización con las técnicas requeridas por cada actividad de la guía, mas técnicas o controles que permitan la mejora de la ciberseguridad en la AE.
- Se debe tener en cuenta que en la primera iteraccion del ADM, especialmente la de desarrollo, permite definir el estado actual de la arquitectura del negocio, SI, y tecnológica, y la segunda iteración permite determinar el estado objetivo de la AE.

BIBLIOGRAFÍA

27001 Academy. (s.f.). *27001 Academy.* Recuperado el 5 de Noviembre de 2013, de http://www.iso27001standard.com/es/que-es-la-norma-iso-27001

Arango, M., Jesús, L., & Zapata, J. (2010). Arquitectura Empresarial - Una Visión General. *Revista Ingenierias Universidad de Medellin, IX*(103), 101-111.

Archi. (2013). ArchiMate. Recuperado el 7 de Julio de 2014, de http://www.archimatetool.com/

Arizabaleta, A., & Ávila, G. (Marzo de 2012). *Universidad EAN.* Recuperado el 12 de Febrero de 2014, de http://repository.ean.edu.co/bitstream/10882/1622/4/AvilaGiovanny2012.pdf

Benschop, A. (13 de Septiembre de 2013). *Sociosite.* Recuperado el 14 de Enero de 2014, de http://www.sociosite.org/index_en.php

Bloomberg, J. (1 de Octubre de 2013). *Zapthink - A Dovel Technologies Company*. Recuperado el 4 de Noviembre de 2013, de http://www.zapthink.com/2013/10/01/enterprise-architecture-the-key-to-cybersecurity/

Dominguez Reinaga, A. (2012). *swindustria - Estudio de la industria mundial del software.* Recuperado el 10 de Febrero de 2014, de http://swindustria.zxq.net/PDFS/UnidadV.pdf

Equipo de Investigación de ESET Latinoamérica. (2014). Pérdida de privacidad y mecanismos para proteger la información en Internet. *Tendencias 2014: El desafío de la privacidad en internet(4)*. Recuperado el 2 de 09 de 2014, de ESET Latinoamérica: http://www.eset-la.com/pdf/tendencias_2014_el_desafio_de_la_privacidad_en_internet.pdf

Ertaul, L., Movasseghi, A., & Kumar, S. (2011). Enterprise Security Planning with TOGAF-9. (Autor, Trad.) Recuperado el 25 de Marzo de 2014, de http://www.mcs.csueastbay.edu/~lertaul/Enterprise%20Security%20Planining%20with%20TOGAF.pdf

García, A. (17 de Octubre de 2012). *CSO España*. Recuperado el 5 de Noviembre de 2013, de http://www.csospain.es/Norma-ISO-%7C-IEC-27032,-nuevo-estandar-de-ciberseguridad/seccion-actualidad/noticia-126991

Herring, M. (2014). *Virginia Attorney General - Computer Crime Section.* Recuperado el 21 de Octubre de 2013, de http://www.ag.virginia.gov/CCSWeb/Reports/Introduction_to_Cyber_Security.pdf

Information Secutiry Standars. (2012). *iso 27001 security.* Recuperado el 7 de Diciembre de 2013, de http://www.iso27001security.com/html/27032.html

Interpol. (2013). *Interpol*. (Cybercrime) Recuperado el 14 de Enero de 2014, de http://www.interpol.int/Crime-areas/Cybercrime/Cybercrime

ISACA. (2009). Marco de riesgos de TI. *RISK IT*. Rolling Meadows, Illinois, Estados Unidos. Recuperado el 2 de Julio de 2014, de http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/The-Risk-IT-Framework.aspx

ISACA. (2009). The Risk IT Practitioner Guide. Rolling Meadows, illinois, Estados Unidos. Recuperado el 12 de Julio de 2014, de http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/The-Risk-IT-Practitioner-Guide.aspx

Isaca. (2012). *Cobit 5 for Information Security.* Recuperado el 15 de Enero de 2014, de http://www.isaca.org/COBIT/Documents/COBIT-5-for-Information-Security-Introduction.pdf

ISACA. (2012). Glossary of Terms English-Spanish. Estados Unidos. Obtenido de http://www.isaca.org/About-ISACA/History/Documents/ISACA-Glossary-English-Spanish.pdf

ISACA. (2012). Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa. Rolling Meadows, Estados Unidos. Obtenido de http://www.isaca.org/COBIT/Documents/COBIT5-Framework-Spanish.pdf

ISACA. (19 de Junio de 2013). New COBIT 5 Guide Identifies Top Three Cybersecurity Game Changers . Recuperado el 22 de Octubre de 2013, de http://www.isaca.org/About-ISACA/Press-room/News-Releases/2013/Pages/New-COBIT-5-Guide-Identifies-Top-Three-Cybersecurity-Game-Changers.aspx

ISACA. (2013). Transforming Cybersecurity. *Transforming Cybersecurity: Using Cobit 5*. (E. autor, Trad.) Rolling Meadows, Illinois, Estados Unidos. Recuperado el 14 de Mayo de 2014, de http://www.isaca.org/KNOWLEDGE-CENTER/RESEARCH/RESEARCHDELIVERABLES/Pages/Transforming-Cybersecurity-Using-COBIT-5.aspx

ISO. (2012). ISO/IEC 27032:2012. *Information technology -- Security techniques -- Guidelines for cybersecurity*. Recuperado el 30 de Octubre de 2013, de http://www.iso.org/iso/catalogue_detail?csnumber=44375

ISO 27000.es. (2005). *iso27000.es - EL PORTAL DE ISO 27001 EN ESPAÑOL*. (ISO/IEC 27001) Recuperado el 30 de Octubre de 2013, de http://www.iso27000.es/iso27000.html#section3c

ISO 27000.es. (2012). *ISO 27000.es*. Obtenido de El portal de ISO 27001 en Español: http://www.iso27000.es/sgsi.html

ISOTools - Excellence. (14 de Noviembre de 2013). ISO 27001:2013. Cambios relevantes en la nueva versión. Recuperado el 25 de Abril de 2014, de http://www.pmg-ssi.com/2013/11/iso-270012013-cambios-relevantes-en-la-nueva-version/

John Zachman. (29 de Abril de 2012). The Zachman Framework is a schema. Recuperado el 11 de Febrero de 2014, de http://www.zachman.com/about-the-zachman-framework

Josey, A. (Abril de 2011). *Van Haren Publishing.* Recuperado el 8 de Febrero de 2014, de http://www.vanharen.net/Samplefiles/9789087537104SMPL.pdf

Klinburg, A., & Hathaway, M. (18 de Marzo de 2013). National Cyber Security Framework Manual. *Information, ICT, and Cyber Security*. (Autor, Trad.) Estados Unidos. Recuperado el 12 de Abril de 2014, de http://belfercenter.hks.harvard.edu/files/hathaway-klimburg-nato-manual-ch-1.pdf

Kosutic, D. (2012). Ciberseguridad en 9 pasos. Zagreb, Croacia: EPPS Services Ltd. Recuperado el 1 de Marzo de 2014

Lankhorst, M. (2013). *Enterprise Architecture at Work.* New York: Springer.

Maganathin, V. (25 de Agosto de 2010). TOGAF 9 - Security Architecture. (Autor, Trad.) Recuperado el 26 de Marzo de 2014, de http://www.slideshare.net/MVeeraragaloo/togaf-9-security-architecture-ver1-0-5053593

Mendieta Matute, M. I. (2014). Propuesta de framework de arquitectura empresarial para pymes basado en un análisis comparativo de los frameworks Zachman y Togaf. 25. Obtenido de http://dspace.ucuenca.edu.ec/bitstream/123456789/5105/1/TESIS.pdf

Microsoft. (Septiembre de 2009). Microsoft Application Architecture Guide. *2nd*. Recuperado el 18 de Marzo de 2015

Ministerio De Defensa De España. (Abril de 2013). Recuperado el 14 de Enero de 2014, de http://www.defensa.gob.es/ceseden/Galerias/ealede/cursos/curDefNacional/ficheros/Ciberseguridad_nuevo_reto_del_siglo_XXI_Guerra_cibernetica_aspectos_organizativos.pdf

Ministerio de Justicia, Derechos Humanos y Cultos. (3 de Febrero de 2014). Código Orgánico Penal. Quito, Pichincha, Ecuador. Recuperado el 20 de Junio de 2014, de http://www.justicia.gob.ec/wp-content/uploads/2014/05/c%C3%B3digo_org%C3%A1nico_integral_penal_-_coip_ed._sdn-mjdhc.pdf

Morenés, P. (2013 de Febrero de 2013). Ciberataque. (4154), 4154-4156.

Niemi, E., & Pekkola, S. (2013). *IEEE Computer Society*. Recuperado el 6 de Diciembre de 2013, de http://www.computer.org/csdl/proceedings/hicss/2013/4892/00/4892d878.pdf

NIST. (2013). Information Technology Security Training Requirements. *Information Technology*. Recuperado el 25 de Febrero de 2014, de http://csrc.nist.gov/publications/nistpubs/800-16/AppendixA-D.pdf

NIST. (12 de Febrero de 2014). *NIST.* Obtenido de NIST - National Institute of Standards and Technology: http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

NoVa Infosec. (5 de Mayo de 2014). Cyber Security versus Information Security. Recuperado el 27 de Junio de 2014, de https://www.novainfosec.com/2014/05/05/cyber-security-versus-information-security/

Osorio, J. (2010). Togaf y Zachman Framework. Manizales. Obtenido de http://ucvvirtual.edu.pe/campus/HDVirtual/700425872/Semana%2004/7000001661/TOGAF-ZACHMAN.pdf

Ramos, L. (6 de Noviembre de 2009). Normas ISO 27000. *Seguridad de la Información*, págs. 1-16. Obtenido de http://www.cpciba.org.ar/archivos/adjuntos/seguridad.pdf

Ruiz Sanchez, D. F. (2014). Diseño de arquitectura empresarial en el sector educativo colombiano: caso colegio privado Bogotá. 41-43. Obtenido de http://repository.ucatolica.edu.co:8080/jspui/bitstream/10983/1691/1/Trabajo%20de%20Grado%20Arquitectura%20Empresarial.pdf

SABSA. (2013). (Autor, Trad., & A. Torres, Recopilador) Recuperado el 4 de Junio de 2014, de http://www.sabsa.org/

Sessions, R. (Mayo de 2007). *Microsoft Developer Network.* Recuperado el 8 de Febrero de 2014, de http://msdn.microsoft.com/en-us/library/bb466232.aspx

Sherwood, J., Clark, A., & Lynas, D. (2009). Enterprise Security Architecture. 1-25. (Autor, Trad., & A. Torres, Recopilador) Estados Unidos. Recuperado el 4 de Junio de 2014, de http://www.sabsa.org/white_paper

Sommerville, I. (2013). *Cybersecurity 1. intro to cybersecurity.* Recuperado el 21 de Octubre de 2013, de http://www.slideshare.net/sommerville-videos/cybersecurity-1-intro-to-cybersecurity

TechTerms.com. (2014). *TechTerms.com*. (Cybercrime) Recuperado el 14 de Enero de 2014, de http://www.techterms.com/definition/cybercrime

The open Group. (2011). *The open Group.* Recuperado el 11 de Febrero de 2014, de http://pubs.opengroup.org/architecture/togaf9-doc/arch/index.html

The Open Group. (2013). *The Open Group*. Recuperado el 18 de Octubre de 2013, de http://www.opengroup.org/togaf/

The Open Group and The SABSA Institute. (2011). TOGAF and SAMSA Integration. Recuperado el 4 de Junio de 2014, de http://www.pinkacademy.nl/wp-content/uploads/2013/04/TOGAF-and-SABSA-Integration.pdf

The Open Group Architecture Forum. (Noviembre de 2005). *Guide to Security Architecture in TOGAF ADM.* Recuperado el 26 de Marzo de 2014, de http://pubs.opengroup.org/onlinepubs/7699949499/toc.pdf

wiseGEEK. (2014). *wiseGEEK.* Recuperado el 14 de Enero de 2014, de http://www.wisegeek.com/what-is-a-cyberattack.htm

Zachman, J. (2008). (The Zachman Framework: The Official Concise Definition) Recuperado el 14 de Octubre de 2013, de http://www.zachmaninternational.com/index.php/the-zachman-framework

ANEXOS

Anexo A: Implementación de la guía

Gestión de requerimientos

Atributos del perfil de negocio para ciberseguridad

Información del documento			
Fase	Gestión de requerimientos		
Documento	Atributos del perfil de negocio para ciberseguridad		
Elaborado por	David Torres		
Aprobado por	Ing. Andrea Jaramillo		
Versión	0.1		
Fecha	20/10/2014		
Desarrollo del documento			
Propósito	El atributo del perfil de negocio, es creado para definir los atributos del negocio, con los cuales se determina el alcance que va a cubrir la guía de ciberseguridad (activos que necesitan protección)		
Actividades			
Código	**Tipo**	**Atributo de negocio**	**Descripción**
ATTR-01	Atributo de usuario	Exactitud	La información facilitada a los usuarios debe ser exacta, dentro de un rango que ha sido previamente acordado.
ATTR-02	Atributo de usuario	Informado	El mismo debe estar informado sobre todo los correspondiente a actividades y reglamentaciones de ciberseguridad que se crean convenientes.
ATTR-03	Atributo de usuario	Protección	Debe estar protegida su información personal, la cual posee la organización.
ATTR-04	Atributo de usuario	Confiabilidad	El usuario debe ser confiable y apegarse a las normas y reglamentaciones que rigen dentro de la organización.
ATTR-05	Atributo de gestión	Automatizado	La gestión debe ser automatizada para agilizar el trato de incidentes de seguridad, con la ayuda de herramientas para cada caso a la cual corresponda
ATTR-06	Atributo de gestión	Eficiencia	Basados en la eficiencia de los sistemas de gestión de incidentes y operaciones dentro de la organización.
ATTR-07	Atributo de gestión	Mantenibilidad	Los sistemas de gestión deben ser mantenibles, para facilitar su continuidad.

ATTR-08	Atributo operativo	Disponibilidad	Continúa disponibilidad de los sistemas de información especialmente los de criticidad alta.
ATTR-09	Atributo operativo	Libre de errores	Los Sistemas de información deben ser libres de errores o acercarse a este estado óptimo.
ATTR-10	Atributo operativo	Recuperabilidad	Los Sistemas de información deben ser recuperables dentro del menor tiempo posible.
ATTR-11	Atributo de gestión de riesgos	Responsabilidad	Para la gestión de riesgos es primordial basarse en la responsabilidad, para el cumplimiento de normas y procedimientos.
ATTR-12	Atributo de gestión de riesgos	Autenticación	Los cuales deben tomar en cuenta la autenticación de usuarios (personas y aplicaciones)
ATTR-13	Atributo de gestión de riesgos	Identificación	Identificar nuevos riesgos de forma temprana.
ATTR-14	Atributo de gestión de riesgos	Propiedad	Establezca la propiedad de los riesgos identificados.
ATTR-15	Atributos legales/regul adores	Ejecutables	Estos atributos deben ser ejecutables dentro del entorno de la organización.
ATTR-16	Atributo de estrategia técnica	Flexibles/ Adaptables	Los mismos deben ser flexibles/adaptables sin que afecten la estabilidad del negocio
ATTR-17	Atributo de estrategia técnica	Migración	Se debe considerar la capacidad de migración de los sistemas de información.
ATTR-18	Atributo de estrategia técnica	Estandarización	Se debe ser compatibles con estándares de calidad.
ATTR-19	Atributo de estrategia técnica	Actualizable	Los sistemas de información deben tener la ventaja de ser actualizables.
ATTR-20	Atributo de estrategia de negocio	Administración/ Gestión	Proporcionar buena administración y custodia de los sistemas de información.

Control de requerimientos

Información del documento	
Fase	Gestión de requerimientos para ciberseguridad
Documento	Control de requerimientos
Elaborado por	David Torres
Aprobado por	Ing. Andrea Jaramillo
Versión	0.1
Fecha	24/10/2014

Desarrollo del documento	
Propósito	El control de requerimientos, se gestiona a través de la creación de un catálogo de requerimientos para determinar cuáles son los requisitos o controles específicos de ciberseguridad requeridos por la organización para proteger sus sistemas de información de ataques informáticos
Actividades	
Código	REQ-01
Requerimiento	Buenas prácticas en el uso de contraseñas
Descripción	Técnicas sugeridas para el diseño de contraseñas robustas de los usuarios.
Prioridad	Media
Fecha	24/10/2014
Origen	Oficial de seguridad
Dependencia	Ninguna

Fase preliminar

Principios de ciberseguridad

Información del documento		
Fase	Fase preliminar	
Documento	Principios de Ciberseguridad	
Elaborado por	David Torres	
Aprobado por	Ing. Andrea Jaramillo	
Versión	0.1	
Fecha	27/10/2014	
Desarrollo del documento		
Propósito	Los principios de ciberseguridad, se determinan con el objetivo de proporcionar una orientación en la toma de decisiones del negocio, llevadas a cabo y guiadas por el apetito de riesgo de la organización.	
Actividades		
Código	**Principio**	**Descripción**
CSP-01	Enfocarse en el negocio	- Analizar el riesgo de ataques/violaciones hacia los procesos de negocio y dar prioridad en consecuencia de la ciberseguridad - Establecer un nivel tolerable de ataques e infracciones, visto desde una perspectiva empresarial.
CSP-02	Entregar calidad y valor a las partes interesadas	- Realizar un análisis de las partes interesadas (internas y externas) y derivar los requisitos para ciberseguridad. - Realizar un análisis de los requerimientos de negocio y obtener los requisitos específicos para ciberseguridad. - Definir los objetivos de alto nivel de ciberseguridad y obtener la aprobación de la alta dirección.

CSP-03	Cumplir con los requerimientos legales y regulatorios	- Identificar leyes, regulaciones y normas de gobierno para ciberseguridad, y definir los requisitos.
CSP-04	Proporcionar información oportuna y precisa sobre el desempeño de la ciberseguridad.	- Establecer indicadores clave de rendimiento (KPI) e informes periódicos de ciberseguridad. - Establecer indicadores clave de riesgo (KRI) y presentación de informes periódicos ciberseguridad
CSP-05	Evaluar las amenazas actuales y futuras	- Identificar las amenazas para las partes críticas de la organización. - Anticiparse a las amenazas futuras a través de la ciberdelincuencia y la ciberguerra. - Recopilar datos y pruebas sobre los incidentes, ataques y violaciones de ciberseguridad - Aprovechar la experiencia externa, según corresponda.
CSP-06	Promover la mejora continua en ciberseguridad	- Establecer un proceso de mejora continua, basado en la experiencia de tendencias pasadas y futuras. - Establecer un proceso de tolerancia a fallos/errores de ciberseguridad. - Fomentar una cultura que promueva la mejora y adaptación del pensamiento de ciberseguridad.
CSP-07	Adoptar un enfoque basado en el riesgo	- Definir un proceso adecuado de identificación y evaluación del riesgo. - Alinear el riesgo con el modelo de gobernanza global seleccionado. - Incluir los incidentes del pasado y aprendizajes técnicos/organizacional. - Identificar y evaluar los nuevos riesgos derivados de la ciberdelincuencia y ciberguerra.
CSP-08	Proteger información clasificada	- Incluir el almacenamiento y servicios basados en la nube, además de datos que residen o que fluyen a través de dispositivos móviles o públicos. - Proporcionar información relacionada con la ciberseguridad para la gestión general de identidad y acceso.
CSP-09	Concentrase en aplicaciones críticas del negocio	- Identificar las aplicaciones críticas de negocio, mediante la realización de un análisis de impacto en el negocio (BIA) con una perspectiva de ciberseguridad. - Realizar un análisis de dependencia en profundidad de la capa de aplicación, para identificar los puntos de entrada potencialmente vulnerables. - Centrarse en el "eslabón más débil de la cadena" de ciberseguridad y alinear al BIA en general. - Asignar recursos y financiamiento, alineados con las amenazas reales de ciberdelincuencia y

		ciberguerra, y considerar los tipos de ataques indirectos y enfoques de ataque.
CSP-10	Desarrollar sistemas de manera segura	- Establecer controles para el ciclo de vida de software, en el desarrollo propio y personalizado de aplicaciones. - Definir un proceso incorporado de ciberseguridad para aplicaciones y sistemas potencialmente críticos. - Participar con los proveedores para lograr definir los controles de ciberseguridad.
CSP-11	Actuar de una manera profesional y ética.	- Aplicar la gobernanza de las políticas, normas y procedimientos operativos clave (Kops) de ciberseguridad - Dar a conocer las rutinas de autoevaluación y evaluación por pares para el personal expuesto (aseguramiento de la integridad). - Lleve a cabo verificaciones de antecedentes (sobre una base opt-in) para el personal de ciberseguridad. - Definir e implementar los controles y verificaciones pertinentes para los nuevos empleados en puestos sensibles. - Definir e implementar procedimientos adecuados para la terminación de responsabilidades o contrato. - Garantizar el reconocimiento del personal de ciberseguridad por incentivos y reconocimientos apropiados.
CSP-12	Fomentar una cultura positiva hacia la ciberseguridad	- Definir la orientación/gobernanza conductual de ciberseguridad. - Promover el conocimiento sobre ciberseguridad y delitos cibernéticos. - Proporcionar ejemplos prácticos y casos de ataques/infracciones. - Resaltar el impacto de ataques/infracciones en el negocio

Equipo de ciberseguridad

Información del documento	
Fase	Fase preliminar
Documento	Equipo de ciberseguridad
Elaborado por	David Torres
Aprobado por	Ing. Andrea Jaramillo
Versión	0.1
Fecha	29/10/2014
Desarrollo del documento	
Propósito	El plan de recursos de ciberseguridad se determina con el fin de cubrir las necesidades de protección de las tecnologías de la información en la AE específicamente en el área de ciberseguridad, donde se determina

	la cantidad de recursos necesarios de acuerdo a los perfil profesional y experiencia, también se verifica si los recursos de seguridad de la arquitectura pueden formar parte del equipo de ciberseguridad o como apoyo hacia el mismo

Requisitos				
Código	**Nombre**	**Tipo**	**Rol**	**Responsabilidad**
EQCS-01	David Torres	Temporal	Analista de seguridad	Gestionar la implementación de ciberseguridad en la organización
EQCS-02	Andrea Jaramillo	Permanente	CEO	Controlar que se realicen las actividades planificadas en la implementación de ciberseguridad

Marcos de referencia para ciberseguridad

Información del documento		
Fase	Fase preliminar	
Documento	Marcos de referencia para ciberseguridad	
Elaborado por	David Torres	
Aprobado por	Ing. Andrea Jaramillo	
Versión	0.1	
Fecha	29/10/2014	
Desarrollo del documento		
Propósito	Identificar los marcos de referencia necesarios para el trabajo de ciberseguridad	
Actividades		
Código	**Marco**	**Descripción**
FCS-01	Transformando la Ciberseguridad utilizando Cobit 5	Marco trabajo de ciberseguridad
FCS-02	Integración de TOGAF y SABSA	Marcos de trabajo para la implementación de seguridad en AE
FCS-03	Marco de trabajo TOGAF	Marco de trabajo para AE
FCS-04	Marco de riesgos de TI	Marco de riesgos basado en tecnologías de la información
FCS-05	Guía para el especialista de riesgos de TI	Guía Práctica que trabaja junto al marco de riesgos de TI.

Áreas de riesgo

Información del documento	
Fase	Fase preliminar
Documento	Áreas de riesgo
Elaborado por	David Torres

Aprobado por	Ing. Andrea Jaramillo				
Versión	0.1				
Fecha	31/10/2014				
Desarrollo del documento					
Propósito	Identificar las áreas clave de riesgo que permiten, mediante el apetito por el riesgo obtener un balance frente a las oportunidades.				
Actividades					
Código	**Riesgo**	**Descripción**	**Probabilidad**	**Impacto**	**Tipo de riesgo**
KRA-01	Hacking – intrusión no autorizada	Acceso hacia los sistemas de información	Medio	Alto	Riesgo de TI
KRA-02	Denegación de servicios	Caída de los Sistemas de Información	Medio	Alto	Riesgo de TI
KRA-03	Robo de contraseñas	Obtención de credenciales de los usuarios registrados en los sistemas de información	Medio	Alto	Riesgo de TI

Partes interesadas de ciberseguridad

Información del documento								
Fase	Fase A: Visión de arquitectura							
Documento	Partes Interesadas de ciberseguridad							
Elaborado por	David Torres							
Aprobado por	Ing. Andrea Jaramillo							
Versión	0.1							
Fecha	31/10/2014							
Desarrollo del documento								
Propósito	El documento de interesados en ciberseguridad (stakeholders) es necesario, para determinar quienes intervienen en la validación del estado final de la implementación de ciberseguridad, también es muy importante identificar los interesados del negocio, quienes controlan el presupuesto y facilitan el apoyo hacia la ciberseguridad							
Actividades								
Código	**Interesado**	**Tipo**	**Capacidad para alterar cambios**	**Entendimiento actual**	**Entendimiento requerido**	**Compromiso actual**	**Compromiso requerido**	**Apoyo necesario**
STKH-01	Andrea Jaramillo	Seguridad	Alto	Medio	Alto	Medio	Alto	Alto
STKH-02	Vicente Merino	Negocio	Medio	Medio	Medio	Medio	Alto	Alto
STKH-02	David Torres	Seguridad	Medio	Alto	Alto	Alto	Alto	Alto

Requerimientos de ciberseguridad

Información del documento				
Fase	Fase A: Visión de arquitectura			
Documento	Requerimientos de ciberseguridad			
Elaborado por	David Torres			
Aprobado por	Ing. Andrea Jaramillo			
Versión	0.1			
Fecha	31/10/2014			
Desarrollo del documento				
Propósito	Los requerimientos de ciberseguridad, determinan las preocupación de los interesados, los mismos que establecen el límite del trabajo de ciberseguridad			
Actividades				
Código	**Requerimiento**	**Tipo**	**Origen**	**Criticidad**
RQ-01	Disponibilidad en los sistemas de información de alta criticidad	Operativo	Analista de TI	Alta
RQ-02	Gestión de procedimientos para el manejo de los sistemas de información	Operativo	Analista de TI	Alta
RQ-03	Control de tráfico malicioso	Operativo	Oficial de seguridad de la información	Alta
RQ-04	Diseño de controles para la protección de datos o información personal	Implantación	Oficial de seguridad de la información	Alta
RQ-05	Gestión de incidentes de seguridad originados dentro de los sistemas de información de la organización	Operativo	Analista de TI	Alta

Marco de referencia de ciberseguridad adaptado

Información del documento		
Fase	Fase A: Visión de arquitectura	
Documento	Marco de referencia de ciberseguridad adaptado	
Elaborado por	David Torres	
Aprobado por	Ing. Andrea Jaramillo	
Versión	0.1	
Fecha	21/11/2014	
Desarrollo del documento		
Propósito	Identificar los marcos de referencia necesarios para el trabajo de ciberseguridad	
Actividades		
Código	**Marco**	**Descripción**
FCS-01	Transforming Cybersecurity Using Cobit5	Marco de trabajo de ciberseguridad
FCS-02	TOGAF	Marco de trabajo para AE

Anexo B: Documento de visión

SICSAE - Sistema para validación de ciberseguridad en arquitectura empresarial

Documento de visión

Historial de revisiones

Fecha	Versión	Descripción	Autor
29-Agosto-2014	1.0	Creación del documento de visión	Alfredo Torres
31-Agosto-2014	1.0	Corrección del documento de visión	Alfredo Torres
28-Marzo-2015	1.1	Corrección del documento de visión	Alfredo Torres

1. Introducción

1.1. Propósito

El propósito de este documento es recoger, analizar y definir las diferentes necesidades de alto nivel y las características del "Sistema para validación de ciberseguridad en arquitectura empresarial (SICSAE)", de la guía de ciberseguridad para arquitectura empresarial. El presente documento se centra en las funcionalidades requeridas por los participantes en el proyecto y los usuarios finales, con el objetivo de evaluar los ítems de las actividades de la guía de ciberseguridad para arquitectura empresarial (AE).

El detalle de cómo el sistema SICSAE cubre los requerimientos se pueden observar en la especificación de los casos de uso y otros documentos adicionales.

1.2. Alcance

Este documento de visión se ocupa del "Sistema para validación de ciberseguridad en arquitectura empresarial", el sistema permitirá a un usuario registrarse con el rol de cliente, para poder evaluar por ítems, y el cumplimiento de las actividades de cada fase de la guía de ciberseguridad para arquitectura empresarial, donde podrá al final obtener como resultado un informe, donde se listan las recomendaciones asociadas a los ítems que no ha cumplido y gráficas que representen el porcentaje del cumplimiento general por fase de la guía de ciberseguridad para AE.

El sistema también permitirá al administrador, gestionar a usuarios de tipo cliente, por medio de las opciones de editar y eliminar, además de gestionar los ítems con sus recomendaciones a través de las opciones de insertar, editar y eliminar.

Dentro del sistema, las actividades así como las fases a las que pertenecen, se encuentran predefinidas dentro del mismo y estas no cambian o eliminan, debido a que corresponden a la guía de ciberseguridad para AE.

1.3. Definiciones, siglas y abreviaturas

- RUP: (Rational Unified Process), metodología aplicada para la descripción del proceso de desarrollo de software.
- AE: Arquitectura empresarial.
- TOGAF: (The Open Group Architecture Framework), marco de trabajo para arquitectura de The Open Group.
- ADM: (Architecture Development Method), método de desarrollo de arquitectura.
- SABSA: (Sherwood Applied Business Security Architecture), marco de arquitectura de seguridad empresarial.
- COBIT: (Control Objectives for Information and related Technology), Objetivos de control para información y tecnologías relacionadas.
- ISO 27001: Estándar para la seguridad de la información.
- SICSAE: Sistema para validación de ciberseguridad en arquitectura empresarial.

2. Posicionamiento

2.1. Oportunidad de negocio

El sistema SICSAE permitirá validar el cumplimiento de actividades por cada una de las fases del ADM, en la implementación de ciberseguridad para AE.

El sistema estará desarrollado en web, a través de una interfaz gráfica amigable y de fácil percepción, en donde también se puedan visualizar rápidamente los resultados que proporciona la herramienta de acuerdo al avance de sus actividades.

2.2. Definición del problema

El problema	Llevar de forma manual el proceso de validación y análisis de resultados de las actividades de la guía de ciberseguridad para AE.
Afecta	Al cliente o usuario que utilice la guía de ciberseguridad para AE, que desee validar si se estan cumpliento las actividades propuestas dentro de la misma.
Impacto	Conocer si las empresas que estan utilizando la guía de ciberseguridad para AE, estan cumpliendo con las actividades propuestas dentro de la misma.
La solución adecuada	Desarrollar un sistema web, basado en un conjunto de ítems que validen el cumplimiento de las actividades de cada fase, propuestas dentro de la guía de ciberseguridad para AE, que ademas permita obtener un informe sobre el estado actual de la validación de cada fase, con las debidas recomendaciones por cada item no validado.

3. Descripción de los interesados y usuarios

3.1. Resumen de interesados

Rol	Descripción	Responsabilidad
Director del proyecto	Determina los lineamientos generales para el desarrollo del proyecto.	Dirigir el proyecto. Analizar el avance del proyecto.
Analista y desarrollador del sistema	Desarrolla el diseño del sistema y artefactos clave para el desarrollo del software de aplicación, y la parte de la programación del sistema de aplicación.	Analizar y describir las necesidades que el sistema debe cumplir a través de su funcionalidad. Realizar la codificación de acuerdo a los requerimientos.
Cliente	Utilizará la aplicación.	Utilizar e interactuar con el sistema.

3.2. Resumen de los usuarios

Los usuarios son aquellos que estarán directamente relacionados con el uso del sistema SICSAE, los mismos se detallan a continuación:

Rol	Descripción	Responsabilidad
Administrador	Persona encargada de administrar el sistema.	- Administrar y gestionar a los usuarios e ítems de las actividades.
Cliente	Persona que utilizará el sistema.	- Registrarse en el sistema. - Validar el registro de su cuenta. - Responder a los ítems de cada actividad, para controlar el avance de la implementación de ciberseguridad - Consultar los resultados del avance de ciberseguridad

3.3. Entorno del usuario tipo cliente

El cliente podrá ingresar al sistema a través de cualquier navegador, como requisito previo a su utilización es necesario registrar y posteriormente activar la cuenta a través de una url enviada al correo electrónico proporcionado por el usuario.

El sistema es de fácil uso, donde el usuario puede navegar a través de las opciones que corresponden a las fases del ADM de TOGAF para responder a los ítems propuestos y luego obtener el informe para controlar el avance de la implementación de ciberseguridad en la AE.

3.4. Perfiles de los interesados

3.4.1. Director del proyecto.

Representante	**Ing. Danilo Jaramillo**
Descripción	Director del proyecto
Tipo	Director
Responsabilidades	Determinar los lineamientos generales para la construcción y desarrollo del proyecto.
Criterio de éxito	Verificar el cumplimiento del cronograma del proyecto.
Implicación	Líder del proyecto.
Entregable	N/A
Comentarios	Mantener comunicación constante con el desarrollo del proyecto para brindar apoyo gerencial cuando sea necesario.

3.4.2. Analista del proyecto.

Representante	**Alfredo David Torres**
Descripción	Analista y desarrollador del sistema
Tipo	Desarrollo del proyecto
Responsabilidades	Analizar y determinar las funcionalidades que el sistema debe cumplir. Codificar el proyecto de acuerdo a los requerimientos especificados.
Criterio de éxito	Determinar las soluciones apropiadas para cubrir las necesidades del sistema
Implicación	Stakeholder
Entregable	Documento de visión Especificación de requisitos Casos de uso Aplicación desarrollada Manual de usuario
Comentarios	Tener una perspectiva clara sobre las soluciones hacia los requerimientos del proyecto

3.4.3. Cliente.

Representante	Lunyxtec
Descripción	Usuario de la aplicación
Tipo	Pruebas del sistema
Responsabilidades	Interactuar con el sistema
Criterio de éxito	Informe final sobre la evaluación del proyecto
Implicación	Stakeholder
Entregable	Pruebas
Comentarios	Coordinar las pruebas del sistema desarrollado

3.5. Perfiles de usuario

3.5.1. Administrador del sistema.

Representante	Alfredo David Torres
Descripción	Administrador del sistema
Tipo	Administrador
Responsabilidades	Administrar el sistema: gestión de usuarios (editar, eliminar) y gestión de items (insertar, editar, y eliminar)
Criterio de éxito	Mantener el buen funcionamiento del sistema, de acuerdo a las actividades de la guía.
Implicación	Desarrollar entregables e implementar el sistema.
Entregable	Ninguno
Comentarios	Mantener relación con los usuarios e items dentro del sistema.

3.5.2. Cliente del sistema.

Representante	Cliente
Descripción	Cliente del sistema.
Tipo	Cliente
Responsabilidades	Utilizar las opciones y procesos del sistema
Criterio de éxito	Obtener un sistema amigable que cumpla con las necesidades del cliente
Implicación	Ninguna
Entregable	Ninguno
Comentarios	Ninguno

3.6. Necesidades de los interesados

Necesidades	Prioridad	Inquietudes	Solución actual	Solución Propuesta
Control de acceso al sistema por usuario y contraseña	Alta	Verificar que las credenciales correspondan al usuario correcto	No existe	Desarrollar el control de acceso en base a roles de usuario
Gestionar dos tipos de perfil de usuario	Alta	Restringir las operaciones de los usuarios para gestionar la información	No existe	Gestionar dos roles, uno de administrador con total de privilegios y de otro para usuario (cliente) con permisos de lectura sobre los items
Gestionar información de clientes e items	Alta	Editar y borrar información de usuarios e insertar, borrar y editar items	No existe	Implementar funciones para eliminar y actualizar información de clientes y funciones de insertar, eliminar y editar items.
Gestionar información válida de clientes	Alta	Se debe gestionar la información del usuario de forma correcta a través de la validación de su cuenta	No existe	Implementar una función de registro de clientes a través de la validación de la cuenta por medio de un mail que contiene una url para su activación.
Guardar información de items	Alta	Guardar la información de los items seleccionados como cumplidos	No existe	Almacenar la información de los items seleccionados dentro de una base de datos MySQL

		para generar el informe del control de implementación de ciberseguridad en la AE		
Informar sobre el estado de la implementación de ciberseguridad en la AE	Alta	Tomar los resultados de la base de datos para generar un informe por fase y general de la implementación de ciberseguridad en la AE	No existe	Desarrollar funciones para obtener la información almacenada de los items del usuario logeado para generar un informe de la implementación de ciberseguridad en la AE
Recomendaciones para el cliente sobre la validación de la implementación de ciberseguridad	Alta	Comprobar cuáles han sido los items seleccionados por el cliente dentro de su cuenta para proporcionar recomendaciones	No existe	Desarrollar una función para obtener una lista de recomendaciones por cada una de sus actividades y fases que aún no se han cumplido
El sistema debe ser amigable para el usuario	Alta	El sistema debe cumplir con los requisitos del cliente	No existe	Desarrollar una interfaz amigable tomando en consideración los requisitos para facilitar la interoperabilidad del sistema

4. Descripción del producto

4.1. Perspectiva del producto

El producto a desarrollar será un sistema web para validar la implementación de ciberseguridad de una AE, basado en las actividades proporcionadas por la guía de

ciberseguridad para AE, en donde participan dos perfiles de usuarios, uno administrador y otro usuario:

Módulo de	Descripción
Registro de usuarios	Permite registrar a un nuevo usuario tipo cliente y validar su registro a través de un email enviado a su correo electrónico, mediante una url especialmente diseña.
Inicio de sesión	Permite a un usuario de tipo cliente o administrador ingresar a su cuenta utilizar las funcionalidades del sistema dependiendo de su rol, este modulo también incluye un control de seguridad a través de captcha, para evitar varios intentos de ingreso a una cuenta de usuario.
Recuperar contraseña	Permite a un usuario tipo cliente recuperar su usuario y contraseña, atraves de un email enviado a su correo registrado.
Gestión de clientes	Incluye modificación, listado y eliminación de clientes, quienes deben obtener su cuenta antes de utilizar cualquier funcionalidad del sistema; este modulo solo se aplica para el usuario con rol de administrador.
Gestón de items	Incluye inserción, modificación, y eliminación de items, además de listarlos mediante opciones de filtrado por fase y actividad; este modulo solo se aplica para el usuario con rol de administrador.
Gestión de recomendaciones	Incluye inserción, modificación, y eliminación de recomendaciones, además de listarlos mediante opciones de filtrado por fase y actividad; este modulo solo se aplica para el usuario con rol de administrador
Generar reporte	Permite a un usuario tipo cliente, generar un reporte en formato pdf, con recomendaciones y gráficas sobre el estado de la validación de la guía ciberseguridad para AE.

4.2. Resumen de capacidades

Capacidad	Beneficio para el beneficios
Autenticación basada en el perfil de administrador y cliente	La sistema permitirá el acceso de usuarios desde cualquier punto a través del internet.
El administrador puede gestionar a usuarios registrados	El sistema gestionará a los usuarios registrados a través de las opciones de editar y eliminar.

El administrador puede gestionar a los ítems de cada actividad	El sistema permite la gestión de los ítems dentro del sistema, con la posibilidad de poder eliminar, actualizar o insertar uno nuevo.
El administrador puede gestionar a las recomendaciones de cada actividad	El sistema permite la gestión de las recomendación dentro del sistema, con la posibilidad de poder eliminar, actualizar o insertar una nueva.
Los clientes pueden llevar el control de la implementación de ciberseguridad en la AE	El sistema permitirá a un usuario registrado llevar el control de la implementación de ciberseguridad en la AE, a través de la selección de ítems que se han cumplido por actividad
Reporte de la implementación de ciberseguridad en la AE	Dentro del sistema, el usuario registrado podrá obtener un resultado a través de un informe, en donde se detalla el avance por fase, un avance general y la cantidad de ítems cumplidos y faltantes por fase.

4.3. Características del producto

Característica	Detalle
Facilidad para registrarse en el sistema	Para el uso del sistema un usuario de tipo cliente completará un registro básico de datos personales, este registro requiere la activación de la nueva cuenta a través de un email enviado al correo electrónico registrado, mediante una url de activación.
Fácil acceso al sistema	Para el acceso al sistema el usuario y administrador deberán ingresar sus credenciales (usuario, contraseña). Un usuario normal deberá registrarse previamente en el sistema para ingresar.
Facilidad para editar información	El administrador podrá editar la información ya sea de un usuario, ítem y recomendación seleccionada previamente.
Facilidad para insertar datos	El administrador podrá registrar nuevos ítems en el sistema categorizados por fase y actividad, también un usuario normal podrá registrar los items seleccionados para el control de la implementación de ciberseguridad.
Facilidad para consultar o listar información	El sistema permitirá al cliente y al administrador visualizar usuarios, items y recomendaciones de acuerdo al rol que posean.

Facilidad para eliminar información	El administrador podrá eliminar la cuenta de clientes o items seleccionados previamente, en el caso de eliminar un cliente, como medida de control de auditorias posteriores, se ha optado por deshabilitar al cliente e items, utilizados para el control de la implementación de ciberseguridad.
Facilidad para generar reporte de estado de implementacion de ciberseguridad	Basado en las respuestas del cliente a los items de cada fase y actividad, se podrá generar un reporte en PDF con el porcentaje de avance en la implementación de ciberseguridad para una AE, de acuerdo al peso correspondiente a cada item.

4.4. Rangos de calidad

Eficiencia

El tiempo en el cual el sistema debe dar una respuesta a alguna transacción CRUD, no debe superar los 10 segundos.

Usabilidad

La herramienta deberá ser comprensible para todos y cada uno de los usuarios de tal manera que la encuentren útil dentro del proceso de control de la implementación de ciberseguridad.

Portabilidad

La herramienta deberá funcionar en diferentes entornos, es decir independientemente del sistema operativo y navegador web (Mozilla, Internet Explorer, Chrome, Safari, Opera)

Funcionalidad

El sistema debe poder establecer comunicación, de manera confiable, con la base de datos que va a utilizar.

Mantenibilidad

- El sistema debe soportar la modificación de componentes sin afectar los demás componentes.
- El sistema debe proporcionar interfaces adecuadas para facilitar la administración del sistema.

4.5. Precedencia y prioridad

Tomando en consideración las necesidades de los interesados y tomando en cuenta que todas las funcionalidades son importantes, se han ordenado las necesidades descritas, considerando el orden de precedencia.

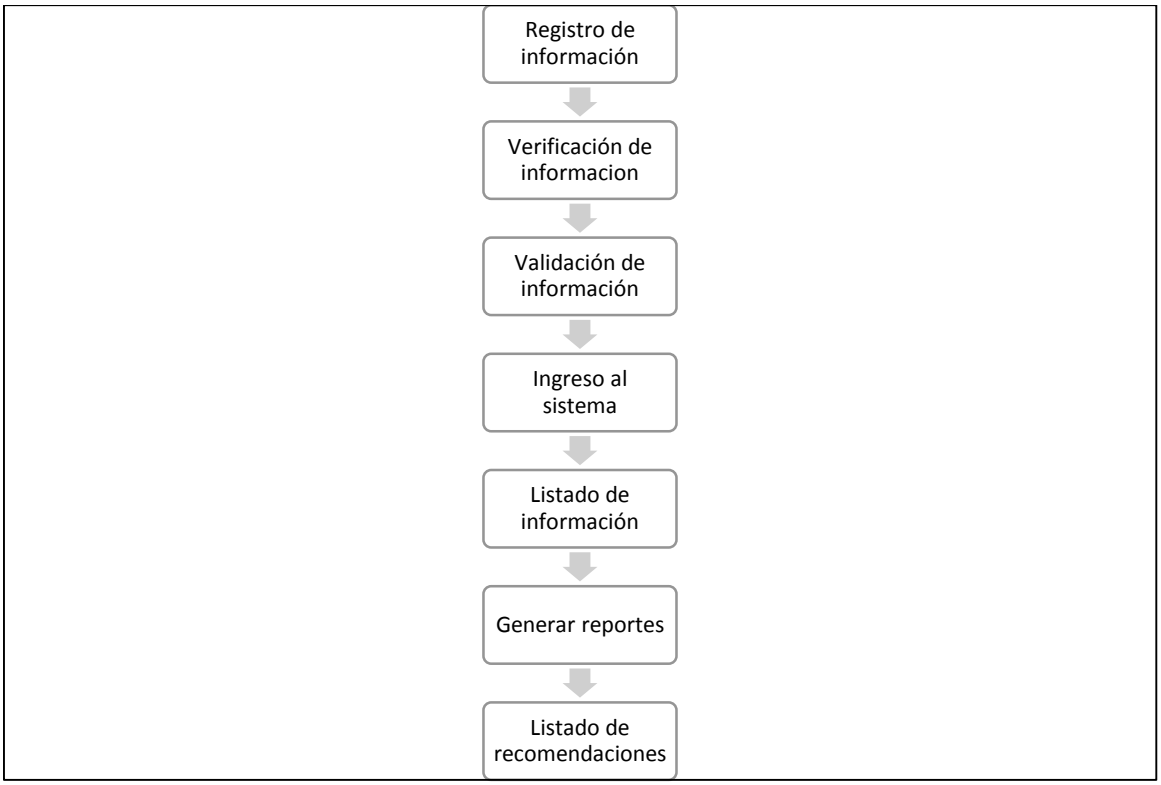

Figura 35. Precedencia y prioridad

Fuente: (Autor, 2014)

4.6. Conclusiones y recomendaciones

- Para la comprensión ideal de cada ítem, es necesario haber estudiado previamente la guía de ciberseguridad para AE.
- El reporte generado está basado en el peso de cada items seleccionado por el cliente.
- La información de clientes, items, fases, actividades y recomendaciones son almacenadas en una base de datos relacional.

4.7. Requerimientos de documentación

- Especificación de requerimientos (Anexo C)
- Casos de uso (Anexo D)
- Especificacion de casos de uso (Anexo E)
- Diagrama de clases (Anexo F)
- Diagrama de secuencia (Anexo G)
- Diagrama de actividades (Anexo H)
- Manual de usuario (Anexo I)

Anexo C: Especificación de requerimientos

SICSAE - Sistema para validación de ciberseguridad en arquitectura empresarial

Documento de especificación de requerimientos de software

Historial de revisiones

Fecha	Versión	Descripción	Autor
04/09/2014	1.0	Especificación de requerimientos de software	Alfredo Torres
29/03/2015	1.0	Especificación de requerimientos de software	Alfredo Torres

1. Introducción

El presente documento detalla la especificación de requerimientos de software (ERS), para el sistema de control de la implementación de ciberseguridad en una arquitectura empresarial (AE)

Esta especificación se ha estructurado conforme a las directrices proporcionadas por el estándar IEEE de Especificaciones de Requisitos de Software ANSI/IEEE 830, 1998.

1.1. Propósito

Este documento tiene como propósito definir las especificaciones funcionales y no funcionales para el desarrollo de un sistema de información web que permitirá llevar el control de la implementación de ciberseguridad en una AE. Éste será utilizado por el administrador del sitio y por usuarios registrados que tenga la necesidad de llevar a cabo el control de las actividades de ciberseguridad.

1.2. Alcance

Esta especificación de requisitos está dirigida hacia los usuarios que necesitan validar la implementación de las actividades de la guía de ciberseguridad para AE.

1.3. Personal involucrado

Nombre	Ing. Danilo Jaramillo
Rol	Director del proyecto
Responsabilidad	Determinar los lineamientos generales para la construcción y desarrollo del proyecto.
Información de contacto	djaramillo@utpl.edu.ec

Nombre	Alfredo Torres
Rol	Analista, diseñador y programador
Responsabilidad	Análisis de información, diseño y programación del SICSAE
Información de contacto	adtorres@utpl.edu.ec

1.4. Definiciones, acrónimos y abreviaturas

Nombre	Descripción
Administrador	Persona que administrara el contenido (Usuario, Items) de la aplicación
Usuario	Persona que usará el sistema para gestionar procesos
Item	Lineamiento considerado para el cumplimiento de una actividad
SICSAE	Sistema para validación de ciberseguridad en arquitectura empresarial
ERS	Especificación de Requisitos Software
RF	Requerimiento Funcional
RNF	Requerimiento No Funcional
AE	Arquitectura Empresarial

1.5. Referencias.

Título del Documento	Referencia
Standard IEEE 830 - 1998	IEEE

1.6. Resumen

Este documento consta de tres secciones, en la primera sección se realiza una introducción al mismo y se provee una visión general a través del propósito y alcance de la aplicación de software.

En la segunda sección del documento se realiza una descripción general del sistema, con el objetivo de identificar las funciones principales que éste debe realizar, y los datos asociados, además de las restricciones, supuestos y dependencias que afectan al desarrollo.

Por último, en la tercera sección se define detalladamente los requisitos que debe satisfacer el sistema.

2. Descripción general

El sistema será desarrollado para trabajar en entornos web, con una distribución lógica de tres capas (presentación, lógica de negocio y datos), a traves de Java como lenguaje de programación, y MySQL como gestor de base de datos para almacenar los registro requeridos por el sistema.

La aplicación debe ser intuitiva y fácil de usar por los usuarios, quienes deben tener una idea clara sobre las actividades de cada una de las fases de la guía.

2.1. Perspectiva del producto

El sistema SICSAE será diseñado para trabajar en un entorno WEB, lo que permitirá el fácil acceso y utilización de del mismo, de forma rápida y eficaz por parte del usuario.

2.2. Funcionalidad del producto

El sistema SICSAE dispondrá de funciones y opciones diferentes para el perfil de tipo administrador y el de tipo usuario, lo cual dará flexibilidad en la gestión de usuarios e ítems.

2.2.1. Interfaces de usuario

La interfaz del usuario dependerá del perfil del mismo, ya sea este de tipo administrador o cliente.

- El administrador, tendrá las opciones para la gestión de usuarios (listar, editar, eliminar) e ítems (listar, insertar, editar, eliminar)
- El cliente, podrá seleccionar los ítems que ha cumplido en cada fase, de acuerdo a su actividad.

2.2.2. Interfaces con hardware

El equipo del usuario final o cliente deberá estar en buen estado con las siguientes características:

- Adaptador de red
- Procesador de 2.00GHz o superior.
- Memoria mínima de 4,00 GB.
- Mouse.
- Teclado.

2.2.3. Interfaces con software

Debido a que el sistema es una aplicación web no existe dependencia con el sistema operativo que tenga el usuario final.

- Navegador web (Chrome, Mozilla, Explorer, Opera o Safari)

2.2.4. Interfaces de comunicación

Los servidores, clientes y aplicaciones se comunicarán entre sí, a través de protocolos de internet. Por ejemplo, para el logeo de usuario deberá utilizarse el protocolo (HTTPS u otros convenientes).

2.3. Características de los usuarios

Tipo de usuario	Administrador
Habilidad	Analista de seguridad
Formación	Conocimiento de las actividades de la guía de ciberseguridad para AE

Actividades	Gestión del sistema en general

Tipo de usuario	Cliente
Habilidad	analista de seguridad, Oficial de seguridad, arquitecto de seguridad
Formación	Conocimiento de las actividades de la guía de ciberseguridad para AE
Actividades	Interactuar con las opciones (ítems y fases) del sistema

2.4. Restricciones

- La aplicación debe ser usada con internet.
- Lenguajes y tecnologías en uso: JAVA, HTML, JavaScript, MySQL
- La aplicación debe tener la capacidad de atender varios usuarios.
- Los servidores deben tener la capacidad de atender consultas concurrentemente.
- El sistema será desarrollado bajo una arquitectura tres capas.
- El sistema deberá ser independiente de plataforma.

2.5. Suposiciones y dependencias

- El usuario deberá haber leído la guía de ciberseguridad para AE, para poder entender cada uno de los ítems de cada actividad.
- Se supone que los requisitos aquí descritos son estables
- El usuario que desee acceder a la aplicación debe cumplir con los requisitos antes indicados para garantizar una ejecución correcta de la misma.

3. Requisitos específicos

3.1. Requerimientos funcionales

REQUERIMIENTOS FUNCIONALES		
Iniciar sesión	RF001	Autenticación de usuario
Registro de cliente	RF002	Registrar nuevo cliente
	RF003	Activar cuenta
Gestión de clientes	RF004	Editar cliente
	RF005	Eliminar cliente
Gestión de Ítems	RF006	Insertar ítem
	RF007	Listar ítems
	RF008	Editar ítem
	RF009	Eliminar ítem
Gestión de recomendaciones	RF010	Editar recomendaciones

Validación de implementación de ciberseguridad	RF011	Guardar ítems seleccionados
	RF012	Listar ítems
	RF013	Listar recomendaciones
	RF014	Generar informe

Iniciar sesión

3.1.1. Requerimiento funcional 1

Identificación del requerimiento:	**RF01**
Nombre del Requerimiento:	Autentificación de usuario.
Descripción del requerimiento:	El sistema comprobará las credenciales (usuario y contraseña) del usuario para poder permitir el ingreso hacia el área correspondiente del mismo, ya sea este de tipo administrador o de tipo cliente.
Entrada	Llenar formulario de login

Proceso	- Ingresar datos:
	  o Usuario y
	  o Contraseña
	- Confirmar los datos ingresados.
	- Determinar tipo(cliente o administrador) de usuario.
	- Verificar si mail y contraseña son correctos

Salida	Ingreso del usuario al área correspondiente de cuardo al tipo de usuario: Administrador: Area de: - Gestión de clientes - Gestión de items - Gestión de recomendaciones. Cliente: Area de validación de implementación de ciberseguridad para una AE.
Prioridad del requerimiento:	Alta

Registro de cliente

3.1.2. Requerimiento funcional 2

Identificación del requerimiento:	**RF02**
Nombre del Requerimiento:	Registrar nuevo cliente

Descripción del requerimiento:	El sistema permitirá el registro de un nuevo cliente a través de un formulario
Entrada	Llenar formulario de registro

Proceso	- Ingresar datos:
	  o Usuario (Nickname)
	  o Nombre
	  o Apellido
	  o Mail y
	  o Contraseña
	  o Empresa
	- Confirmar los datos ingresados.
	- Verificar que no queden campos vacíos
	- Verificar si el mail suministrado es válido

Salida	Cliente registrado en el sistema
Prioridad del requerimiento:	Alta

3.1.3. Requerimiento funcional 3

Identificación del requerimiento:	**RF03**
Nombre del Requerimiento:	Activar cuenta
Descripción del requerimiento:	El sistema validará si la dirección de mail que utilizó el cliente es correcta, enviándole un mail con los datos de registro u una dirección URL para validad (activar) su cuenta
Entrada	Obtener la dirección URL que se envió al mail utilizado para el registro de usuario
Proceso	- Copiar o hacer clic en la URL que se envió al correo del cliente - Esperar un momento mientras se activa la cuenta del cliente
Salida	Cuenta del cliente activada para ingresar al sistema
Prioridad del requerimiento:	Alta

Gestión de clientes

3.1.4. Requerimiento funcional 4

Identificación del requerimiento:	**RF04**
Nombre del Requerimiento:	Editar cliente

Descripción del requerimiento:	El sistema permitirá al administrador dentro de la opción de gestión de clientes, editar la información del mismo.
Entrada	Administrador logeado en el sistema
Proceso	- Ir a la opción de Gestión de Clientes - Utilizar la opción de editar, del cliente en deseado - Editar información - Confirmar cambios (Aceptar)
Salida	Cliente actualizado en el sistema
Prioridad del requerimiento:	Alta

3.1.5. Requerimiento funcional 5

Identificación del requerimiento:	**RF05**
Nombre del Requerimiento:	Eliminar cliente
Descripción del requerimiento:	El sistema permitirá al administrador dentro de la opción de gestión de clientes, eliminar a un cliente determinado.
Entrada	Administrador logeado en el sistema
Proceso	- Ir a la opción de Gestión de clientes - Utilizar la opción de eliminar, del cliente en deseado
Salida	Cliente eliminado del sistema
Prioridad del requerimiento:	Alta

Gestión de Ítems

3.1.6. Requerimiento funcional 6

Identificación del requerimiento:	**RF06**
Nombre del Requerimiento:	Insertar ítem
Descripción del requerimiento:	El sistema permitirá al administrador insertar un nuevo ítem en el sistema, dentro de la opción de gestión de items.
Entrada	Administrador logeado en el sistema

Proceso	- Seleccionar la opción de insertar pregunta
	- Llenar los campos:
	  o Ingresar item
	  o Seleccionar fase
	  o Seleccionar actividad

	○ Seleccionar el peso - Confirmar los datos ingresados
Salida	Ítem insertado en el sistema
Prioridad del requerimiento:	Alta

3.1.7. Requerimiento funcional 7

Identificación del requerimiento:	**RF07**
Nombre del Requerimiento:	Listar ítems
Descripción del requerimiento:	El sistema permitirá al administrador listar los ítems de acuerdo a la fase y actividad seleccionada.
Entrada	Administrador logeado en el sistema
Proceso	- Ir a la opción gestión de items. - Seleccionar la fase. - Seleccionar actividad. - Confirmar la opción seleccionada para obtener la lista de ítems
Salida	Lista de ítems junto a las actividades donde pertenecen
Prioridad del requerimiento:	Alta

3.1.8. Requerimiento funcional 8

Identificación del requerimiento:	**RF08**
Nombre del Requerimiento:	Editar ítem
Descripción del requerimiento:	El sistema permitirá al administrador editar los ítems que se encuentran registrados en el sistema.
Entrada	Administrador logeado en el sistema Ítems listados
Proceso	- Seleccionar la opción editar del respectivo ítem - Confirmar la opción de editar - Editar ítem - Confirmar cambios (Aceptar)
Salida	Ítem actualizado en el sistema
Prioridad del requerimiento:	Alta

3.1.9. Requerimiento funcional 9

Identificación del requerimiento:	**RF09**
Nombre del Requerimiento:	Eliminar ítem
Descripción del requerimiento:	El sistema permitirá al administrador eliminar los ítems que se encuentran registrados en el sistema
Entrada	Administrador logeado en el sistema Ítems Listados
Proceso	- Seleccionar la opción eliminar del respectivo ítem - Confirmar la opción de eliminar
Salida	Ítem eliminado del sistema
Prioridad del requerimiento:	Alta

Gestión de recomendaciones

3.1.10. Requerimiento funcional 10

Identificación del requerimiento:	**RF10**
Nombre del Requerimiento:	Editar recomendaciones
Descripción del requerimiento:	El sistema permitirá al administrador editar las recomendaciones de acuerdo a la fase y actividad seleccionada.
Entrada	Administrador logeado en el sistema
Proceso	- Ir a la opción gestión de recomendaciones. - Seleccionar la fase. - Seleccionar actividad. - Seleccionar la opción editar de la recomendación - Editar recomendación - Confirmar cambios (Aceptar)
Salida	Recomendación actualizada en el sistema
Prioridad del requerimiento:	Alta

Validación de implementación de ciberseguridad

3.1.11. Requerimiento funcional 11

Identificación del requerimiento:	**RF11**
Nombre del Requerimiento:	Guardar ítems
Descripción del requerimiento:	El sistema permitirá al usuario guardar los ítems seleccionados para poder utilizar la misma información mas adelante y poder generar un informe sobre el estado actual de la implementación de ciberseguridad.
Entrada	Cliente registrado
Proceso	- Acceder en el sistema (login) - Filtrar items por fase y actividad - Seleccionar los ítems considerador por el usuario - Guardar información
Salida	Ítem guardados en el sistema
Prioridad del requerimiento:	Alta

3.1.12. Requerimiento funcional 12

Identificación del requerimiento:	**RF12**
Nombre del Requerimiento:	Listar ítems
Descripción del requerimiento:	El sistema permitirá al cliente observar inmediatamente, apenas ingresado a su cuenta, los ítems guardados en la sesión anterior para poder continuar con las actividades de validación de la implementación de ciberseguridad
Entrada	Cliente registrado
Proceso	- Acceder en el sistema (login)
Salida	Ítem cargados en el perfil del cliente
Prioridad del requerimiento:	Alta

3.1.13. Requerimiento funcional 13

Identificación del requerimiento:	**RF13**
Nombre del Requerimiento:	Listar recomendaciones

Descripción del requerimiento:	El sistema permitirá al cliente observar una lista de recomendaciones categorizadas por actividad y fase correspondiente, estas recomendaciones se basan en los items que aún no se han cumplido y que se sugiere implementar por parte del cliente.
Entrada	Cliente registrado
Proceso	- Acceder en el sistema (login) - Ir a la opción de recomendaciones
Salida	Lista de recomendaciones para la implementación de ciberseguridad en una AE.
Prioridad del requerimiento:	Alta

3.1.14. Requerimiento funcional 14

Identificación del requerimiento:	**RF14**
Nombre del Requerimiento:	Generar informe
Descripción del requerimiento:	El sistema permitirá al usuario observar el avance de la implementación de ciberseguridad en una AE, conforme a los ítems seleccionados en cada una de las fases del sistema a través de un reporte en PDF.
Entrada	Cliente registrado
Proceso	- Acceder en el sistema (login) - Ir a la opción de reporte (ícono reporte)
Salida	Resultados generados del avance de la implementación de ciberseguridad en una AE
Prioridad del requerimiento:	Alta

3.2. Requerimientos no funcionales

3.2.1. Requisitos de rendimiento

RNF01: Garantizar que el diseño de las consultas y de la base de datos no afecte el desempeño de la misma.

3.2.2. Seguridad

RNF02: Garantizar la confiabilidad, la seguridad y el desempeño del sistema hacia los usuarios. En el sentido de que la información almacenada podrá ser consultada permanente y simultáneamente, sin que se afecte el tiempo de respuesta.

RNF03: Garantizar la seguridad de la información y datos que se manejan en el sistema como información personal (Nombre, Apellido, Mail, Contraseña) e Ítems guardados correspondientes al estado de ciberseguridad de una organización.

RNF04: Controles para permitir el acceso hacia la información, únicamente por usuarios autorizados a través de Internet.

3.2.3. Fiabilidad

RNF05: El sistema debe tener una interfaz intuitiva y sencilla

RNF06: La interfaz de usuario debe ajustarse a las características de la web de la institución, en la cual estará incorporado el área de control de implementación de ciberseguridad en una AE.

3.2.4. Disponibilidad

RNF07: La disponibilidad del sistema debe ser continua (7 días por 24 horas) para los usuarios, garantizando un esquema que permita la detección de posibles fallas en cualquiera de sus componentes.

3.2.5. Mantenibilidad

RNF08: El sistema debe disponer de documentación entendible y actualizable que permita realizar operaciones de mantenimiento fácilmente.

3.2.6. Portabilidad

RNF09: El sistema será implantado bajo la plataforma de Windows.

4. Requerimientos de documentación

4.1. Manual de usuario

Se debe elaborar y facilitar un manual de usuario sobre el uso correcto del sistema.

Anexo D: Diagrama de casos de uso

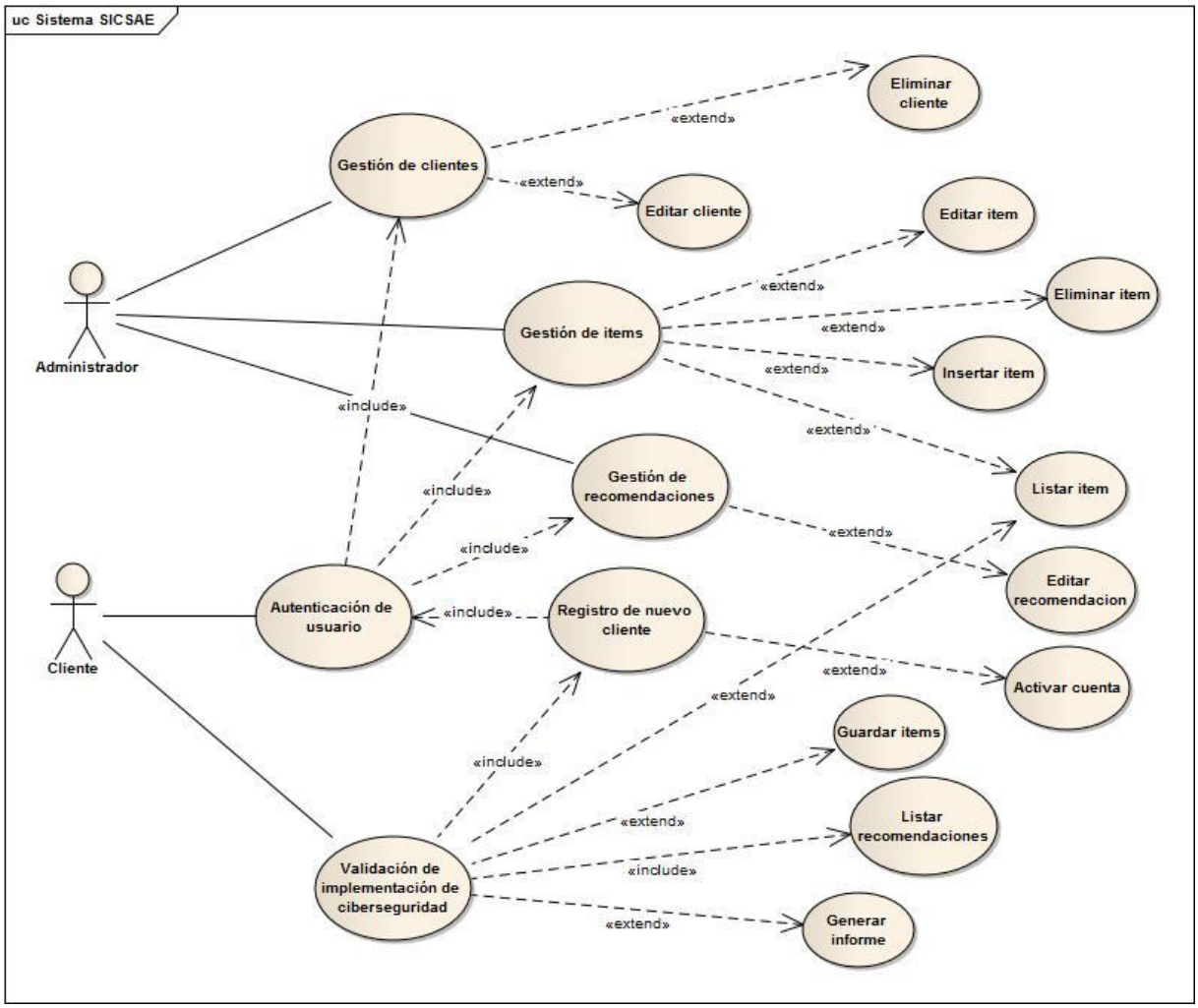

Figura 36. Diagrama de caso de uso del sistema

Fuente: (Autor, 2014)

Anexo E: Especificacion de casos de uso

SICSAE - Sistema para validación de ciberseguridad en arquitectura empresarial

Especificacion de caso de uso 01: Autenticación de usuario

Version 1.0

Nombre:	Autenticacion de usuario	
Actores:	Cliente, Administrador	
Descripción:	Su función es permitir el acceso hacia las funciones del sistema, en caso que el usuario no esté registrado, se solicitará que se registre y confirme la creación de su cuenta vía e-mail.	
Precondiciones:	El usuario debe estar registrado en el Sistema.	
Flujo Normal:	**Actor:**	**Sistema:**
	1. Solicita acceso hacia las funciones del sistema. 3. El usuario puede escoger: a. Ingresar usuario y contraseña, ó. b. Registrarse como nuevo cliente en el sistema.	2. Presentar formularios: a. Formulario para el ingreso de usuario y contraseña. b. Formulario para el registro de nuevo cliente. (SF1) 4. Validar ingreso de datos: a. Si los datos ingresados son correctos, se da acceso al sistema. b. Si los datos son incorrectos, regresa al paso 2 del flujo normal. c. Si el cliente olvido su usuario y/o contraseña; permitir su recuperación. 5. Fin del caso de uso.

<table>
<tr><td rowspan="5">Sub Flujos</td><td colspan="2">SF 1 Registro de nuevo cliente</td></tr>
<tr><td>Actor:</td><td>Sistema:</td></tr>
<tr><td>1. Solicita registrarse en el sistema.

3. Ingresa datos solicitados.</td><td>2. Visualizar formulario de registro.

4. Validar datos:
a. Si todos los datos son correctos, continúa con paso 5 del sub flujo 1 actual.
b. Si los datos son incorrectos o falta ingresar datos, retorna al paso 2 del sub flujo 1 actual.
5. Enviar e-mail de confirmación de registro.
6. Retorna al paso 2 del flujo normal.</td></tr>
<tr><td colspan="2">SF 1 Recuperar usuario y contraseña.</td></tr>
<tr><td>Actor:</td><td>Sistema:</td></tr>
<tr><td></td><td>1. Solicita recuperar su usuario y contraseña olvidada.

3. Ingresa e-mail y captcha.</td><td>2. Solicita ingrese e-mail y captcha.

4. Validar e-mail:
a. Si el e-mail no es válido, retorna al paso 2 del sub flujo 2 actual.
b. Si e-mail es válido, enviar un e-mail con los datos del usuario recuperados.</td></tr>
</table>

		5. Retornar al paso 2 del Flujo normal.
Flujo Alternativo:	**FA 1: Datos requeridos no han sido ingresados** Esto sucede cuando el cliente no ha ingresado los datos que son obligatorios y muestra un mensaje indicando el campo requerido que debe llenar y regresa al paso anterior del flujo que lo invocó.	
	FA 2: datos incorrectos <e-mail> incorrecto si los e-mail que se ingresan no corresponden a e-mails validos se presentara el siguiente mensaje de error: “El e-mail no es valido”	
Excepciones:	Si un cliente desea ingresar en el sistema sin antes haberse registrado, se le pedirá que se registre obligatoriamente. Mientras el cliente no confirme su registro en el sistema, el estado de activación permanecerá inactivo.	
Prioridad:	Alta	
Requerimientos Especiales:	Existe la posibilidad que el cliente olvide su contraseña, caso para el cual se le debe dar la facilidad de recordarla vía e-mail. Que el proceso de registro o ingreso de datos sea sencillo o corto para los usuarios.	
Notas adicionales:	Si el cliente realiza tres intentos fallidos aparecerá un captcha como control de seguridad del sistema, mas la opción de recuperar contraseña si el usuario la olvido.	

SICSAE - Sistema para validación de ciberseguridad en arquitectura empresarial

Especificacion de caso de uso 01: Gestión de clientes

Version 1.0

Nombre:	Gestión de clientes	
Actor:	Administrador	
Descripción:	Su función es administrar las opciones de editar y eliminar los clientes que se encuentran registrados en el sistema.	
Precondiciones:	El usuario debe estar registrado en el sistema y tener el rol de administrador	
Flujo Normal:	**Actor:**	**Sistema:**
	1. El administrador se autentica en el sistema. 3. El administrador selecciona la opción gestión de clientes. 5. El administrador cierra sesión.	2. El sistema presenta las opciones de: a. Gestión de clientes. b. Gestión de items c. Gestión de recomendaciones. 4. Presentar automáticamente la lista de clientes, junto a las opciones de editar y eliminar cliente: a. Opcion de eliminar cliente, borra todos los datos de un cliente registrado en el sistema. b. Opcion de editar cliente. (SF1) 6. Fin del caso de uso.

<table>
<tr><td rowspan="2">Sub Flujos</td><td colspan="2">SF1 Editar cliente</td></tr>
<tr><td>Actor:</td><td>Sistema:</td></tr>
<tr><td></td><td>1. Opcion editar cliente.

3. Editar los datos pertinentes (p. ej. nombre, apellido, etc.)
4. Seleccionar aceptar</td><td>2. Visualizar formulario con los datos del cliente, seleccionado para editar.

5. Validar datos:
a. Si todos los datos son correctos, continúa con el paso 6 del sub flujo 1 actual.
b. Si los datos son incorrectos o falta ingresar datos, retorna al paso 2 del sub flujo 1 actual.
6. Retorna al paso 3 del flujo normal.</td></tr>
<tr><td>Flujo Alternativo:</td><td colspan="2">FA 3: Datos requeridos no han sido ingresados

Esto sucede cuando el usuario no ha ingresado los datos que son obligatorios y muestra un mensaje indicando el campo requerido que debe llenar y regresa al paso anterior del flujo que lo invocó.</td></tr>
<tr><td></td><td colspan="2">FA 4: datos incorrectos

<u><usuario> incorrecto</u>

Si el cliente editado cambia su nombre de usuario por uno que ya se encuentra registrado, se presentara el siguiente mensaje de error: “El nombre de usuario ya esta en uso”</td></tr>
<tr><td>Excepciones:</td><td colspan="2">El usuario podrá únicamente visualizar estas opciones si su rol es de administrador.</td></tr>
<tr><td>Prioridad:</td><td colspan="2">Alta</td></tr>
</table>

Requerimientos Especiales:	Existe la posibilidad que el cliente olvide su contraseña, caso para el cual se le debe dar la facilidad de recordarla vía e-mail.
Notas adicionales:	Si el cliente realiza tres intentos fallidos aparecerá un captcha como control de seguridad del sistema, mas la opción de recuperar contraseña si el usuario la olvido.

SICSAE - Sistema para validación de ciberseguridad en arquitectura empresarial

Especificacion de caso de uso 01: Gestión de items

Version 1.0

Nombre:	Gestión de items	
Actor:	Administrador	
Descripción:	Su función es administrar las opciones de insertan, editar y eliminar items dentro del sistema.	
Precondiciones:	El usuario debe estar registrado en el sistema y tener el rol de administrador	
Flujo Normal:	**Actor:**	**Sistema:**
	1. El administrador se autentica en el sistema. 3. El administrador selecciona la opción gestión de items 6. El usuario cierra sesión.	2. El sistema presenta las opciones de: a. Gestión de clientes. b. Gestión de items c. Gestión de recomendaciones. 4. Presentar las opciones para filtrar los items por fase y actividades 5. lista los items, junto a las opciones de editar, eliminar e insertar items: a. Opcion de eliminar item, borra el item almacenado en el sistema. b. Opcion de editar item. (SF1) c. Opcion de insertar item. (SF2) 7. Fin del caso de uso.

<table>
<tr><td rowspan="6">Sub Flujos</td><td colspan="2">SF1 Editar item</td></tr>
<tr><td>Actor:</td><td>Sistema:</td></tr>
<tr><td>1. Opcion editar item.

3. Editar los datos pertinentes del item

4. Seleccionar aceptar</td><td>2. Visualizar formulario con los datos del item para editar.

6. Validar datos.

El sistema opcionalmente:
a. Si todos los datos son correctos, continúa con el paso 6 del sub flujo 1 actual.

b. Si los datos son incorrectos o falta ingresar datos, retorna al paso 2 del sub flujo 1 actual.

7. Retorna al paso 3 del flujo normal.</td></tr>
<tr><td colspan="2">SF2 Editar item</td></tr>
<tr><td>Actor:</td><td>Sistema:</td></tr>
<tr><td>1. Opcion insertar item.

3. Ingresa datos del item.</td><td>2. Visualizar formulario de ingreso de item.

4. Validar datos.

El sistema opcionalmente:
a. Si todos los datos son correctos, continúa con paso 6 del sub flujo 1 actual.

b. Si los datos son incorrectos o falta ingresar datos, retorna al paso 2 del sub flujo 1 actual.</td></tr>
</table>

		Retorna al paso 2 del Flujo normal.
Flujo Alternativo:	**FA 5: Datos requeridos no han sido ingresados** Esto sucede cuando el usuario no ha ingresado los datos que son obligatorios y muestra un mensaje indicando el campo requerido que debe llenar y regresa al paso anterior del flujo que lo invocó.	
Excepciones:	El usuario podrá únicamente visualizar estas opciones si su rol es de administrador.	
Prioridad:	Alta	
Requerimientos Especiales:	Existe la posibilidad que el usuario olvide su contraseña, caso para el cual se le debe dar la facilidad de recordarla vía e-mail.	
Notas adicionales:	Si el usuario realiza tres intentos fallidos aparecerá un captcha como control de seguridad del sistema, mas la opción de recuperar contraseña si el usuario la olvido.	

SICSAE - Sistema para validación de ciberseguridad en arquitectura empresarial

Especificacion de caso de uso 01: Gestión de recomendaciones

Version 1.0

Nombre:	Gestión de recomendaciones	
Actor:	Administrador	
Descripción:	Su función es administrar las opciones de editar recomendaciones dentro del sistema.	
Precondiciones:	El usuario debe estar registrado en el sistema y tener el rol de administrador	
Flujo Normal:	**Actor:**	**Sistema:**
	1. El usuario se autentica en el sistema. 3. El usuario (Administrador) selecciona la opción gestión de recomendaciones 6. El usuario cierra sesión.	2. El sistema presenta las opciones de: a. Gestión de clientes. b. Gestión de items c. Gestión de recomendaciones. 4. Presentar las opciones para filtrar las recomendaciones por fase y actividades 5. listar las recomendaciones junto a la opción de editar, recomendación: a. Opcion de editar item. (SF1) 7. Fin del caso de uso.

<table>
<tr><td rowspan="3">Sub Flujos</td><td colspan="2">SF1 Editar recomendación</td></tr>
<tr><td>Actor:</td><td>Sistema:</td></tr>
<tr><td>1. Opcion editar recomendación.

3. Editar los datos pertinentes del item

4. Seleccionar aceptar</td><td>2. Visualizar formulario con los datos de la recomendación seleccionada para editar.

5. Validar datos.

El sistema opcionalmente:
a. Si todos los datos son correctos, continúa con el paso 6 del sub flujo 1 actual.

b. Si los datos son incorrectos o falta ingresar datos, retorna al paso 2 del sub flujo 1 actual.

6. Retorna al paso 3 del Flujo normal.</td></tr>
<tr><td>Flujo Alternativo:</td><td colspan="2">FA 6: Datos requeridos no han sido ingresados

Esto sucede cuando el usuario no ha ingresado los datos que son obligatorios y muestra un mensaje indicando el campo requerido que debe llenar y regresa al paso anterior del flujo que lo invocó.</td></tr>
<tr><td>Excepciones:</td><td colspan="2">El usuario podrá únicamente visualizar estas opciones si su rol es de administrador.</td></tr>
<tr><td>Prioridad:</td><td colspan="2">Alta</td></tr>
<tr><td>Requerimientos Especiales:</td><td colspan="2">Existe la posibilidad que el usuario olvide su contraseña, caso para el cual se le debe dar la facilidad de recordarla vía e-mail.</td></tr>
<tr><td>Notas adicionales:</td><td colspan="2">Si el usuario realiza tres intentos fallidos aparecerá un captcha como control de seguridad del sistema, mas la opción de recuperar contraseña si el usuario la olvido.</td></tr>
</table>

SICSAE - Sistema para validación de ciberseguridad en arquitectura empresarial

Especificacion de caso de uso 01: Control de implementacion de ciberseguridad

Version 1.0

Nombre:	Control de implementacion de ciberseguridad	
Actor:	Cliente	
Descripción:	Su función es manipular las opciones y seleccionar los items cumplidos dentro de las actividades de ciberseguridad para arquitectura empresarial dentro del sistema.	
Precondiciones:	El usuario debe estar registrado en el sistema y tener la cuenta activa a través de la url enviada a través de e-mail.	
Flujo Normal:	**Actor:**	**Sistema:**
	1. El cliente se autentica en el sistema. 3. El cliente filtra los items por fase y actividad. 5. Seleccionar los .items que se consideran cumplidos por el usuario. 6. Seleccionada la opción guardar. 8. El cliente cierra sesión.	2. El sistema presenta las opciones para filtrar los items, por fase y actividad. 4. Presentar los items correspondientes a la acividad de la fase seleccionada en el paso 2 del flujo normal. 7. Proporcionar las opciones de: a. Listar recomendaciones b. Generar reporte (pdf) (SF1) 9. Fin del caso de uso.
Sub Flujos	**SF1 Generar reporte (pdf)**	
	Actor:	**Sistema:**

	1. Opcion generar reporte	2. Visualizar reporte en pdf con las estadísticas de la validación del cumplimiento de las actividades de ciberseguridad para arquitectura empresarial, junto a un listado de recomendaciones para ciberseguridad. 3. Retorna al paso 3 del flujo normal.
Flujo Alternativo:		
Excepciones:	El cliente podrá únicamente visualizar estas opciones si se encuentra registrado y su cuenta esta activa.	
Prioridad:	Alta	
Requerimientos Especiales:	Existe la posibilidad que el usuario olvide su contraseña, caso para el cual se le debe dar la facilidad de recordarla vía e-mail.	
Notas adicionales:	Si el cliente realiza tres intentos fallidos aparecerá un captcha como control de seguridad del sistema, mas la opción de recuperar contraseña si el usuario la olvido.	

Anexo F: Diagrama de clases

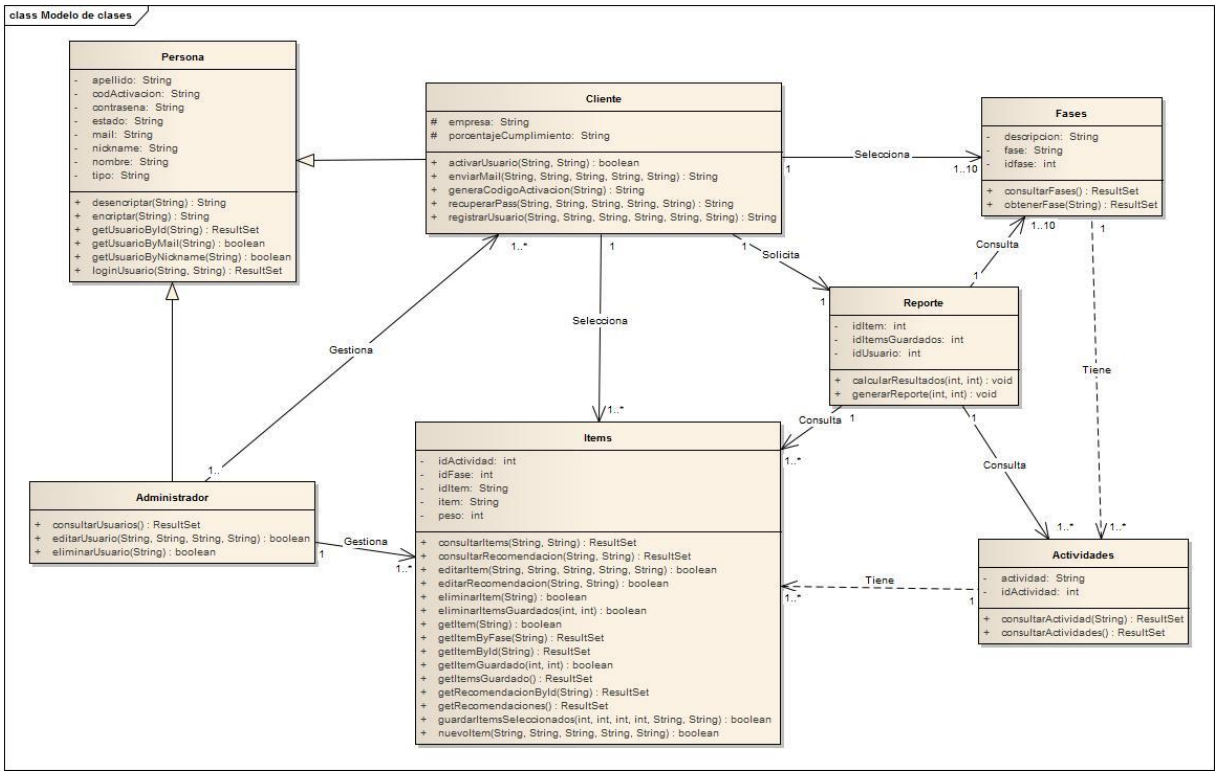

Figura 37. Diagrama de clases

Fuente: (Autor, 2014)

Anexo G: Diagramas de secuencia

Iniciar Sesión

Autenticación de usuario

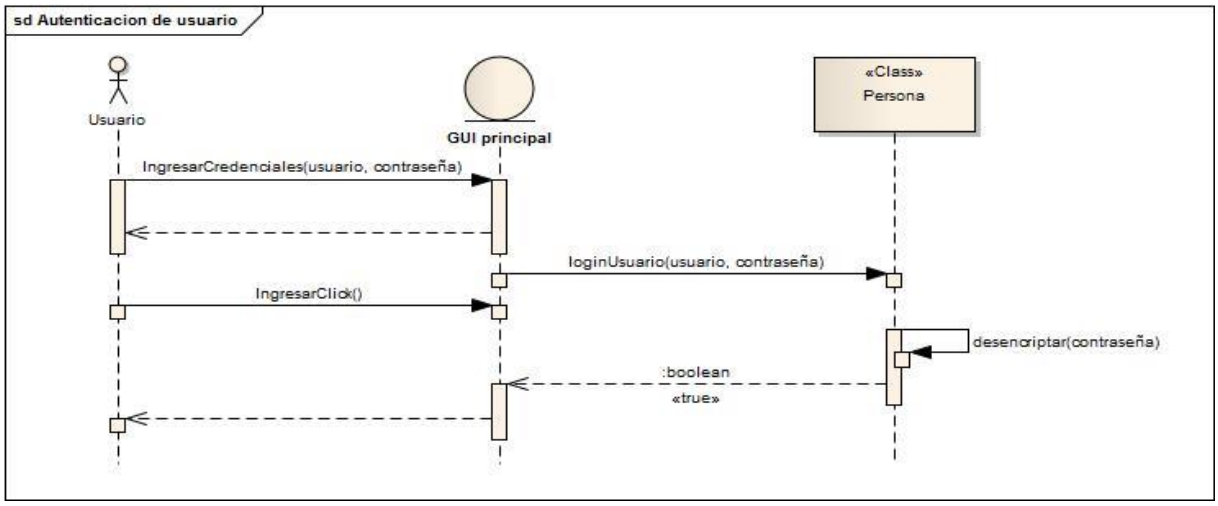

Figura 38. Autenticar usuario

Fuente: (Autor, 2014)

Registro de Cliente

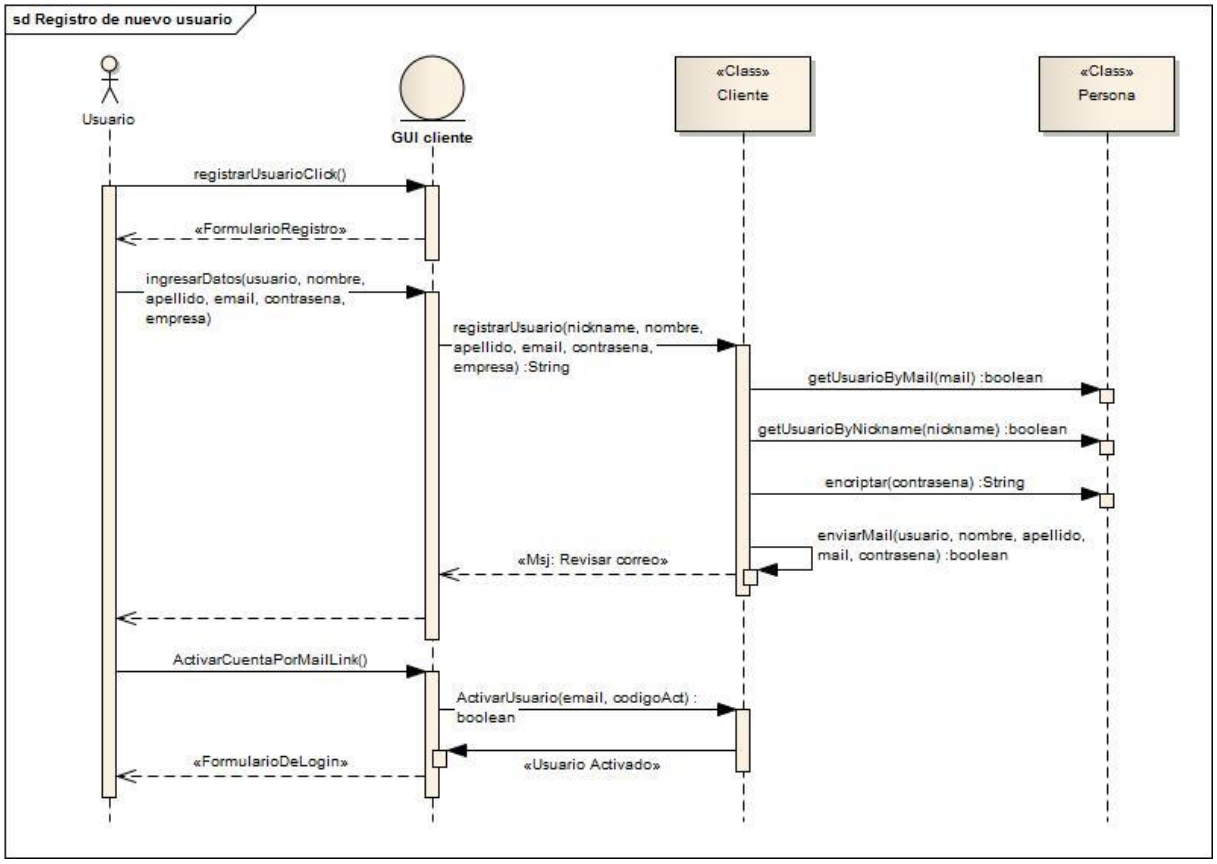

Figura 39. Registrar usuario

Fuente: (Autor, 2014)

Gestión de clientes

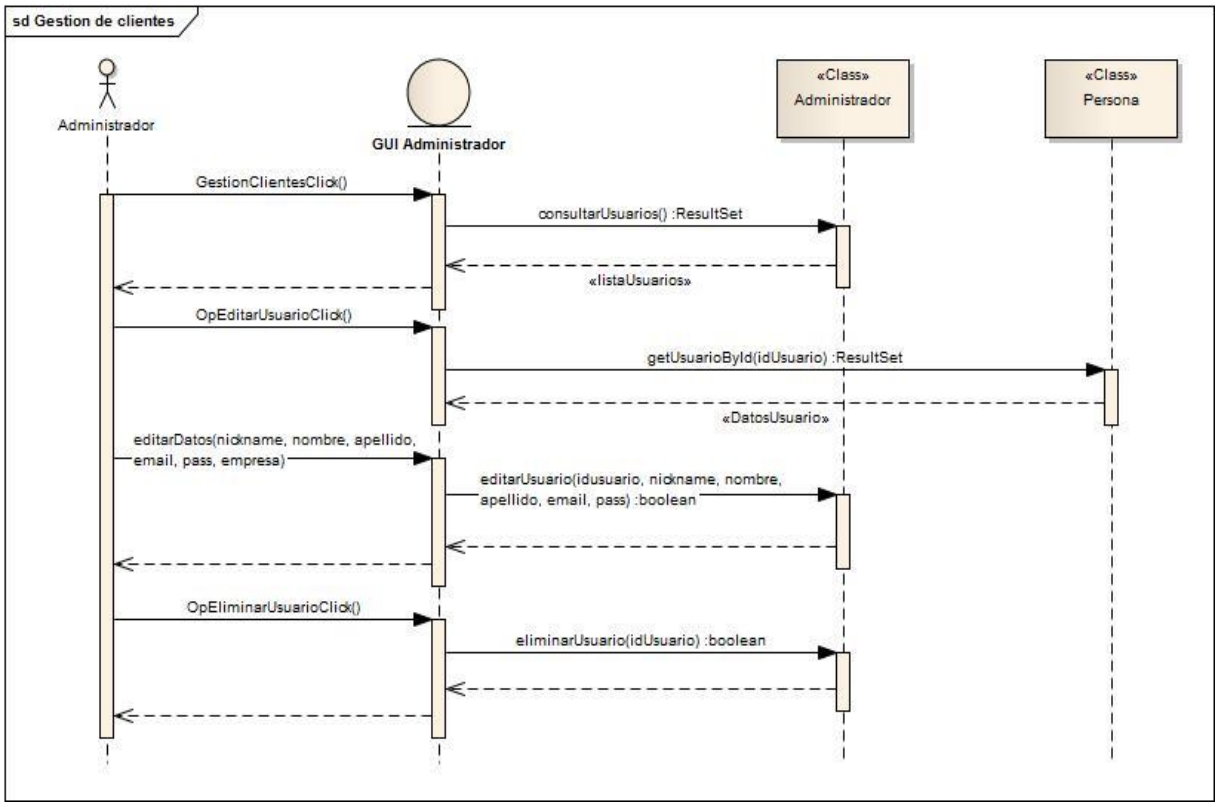

Figura 40. Gestión de clientes

Fuente: (Autor, 2014)

Gestión de items

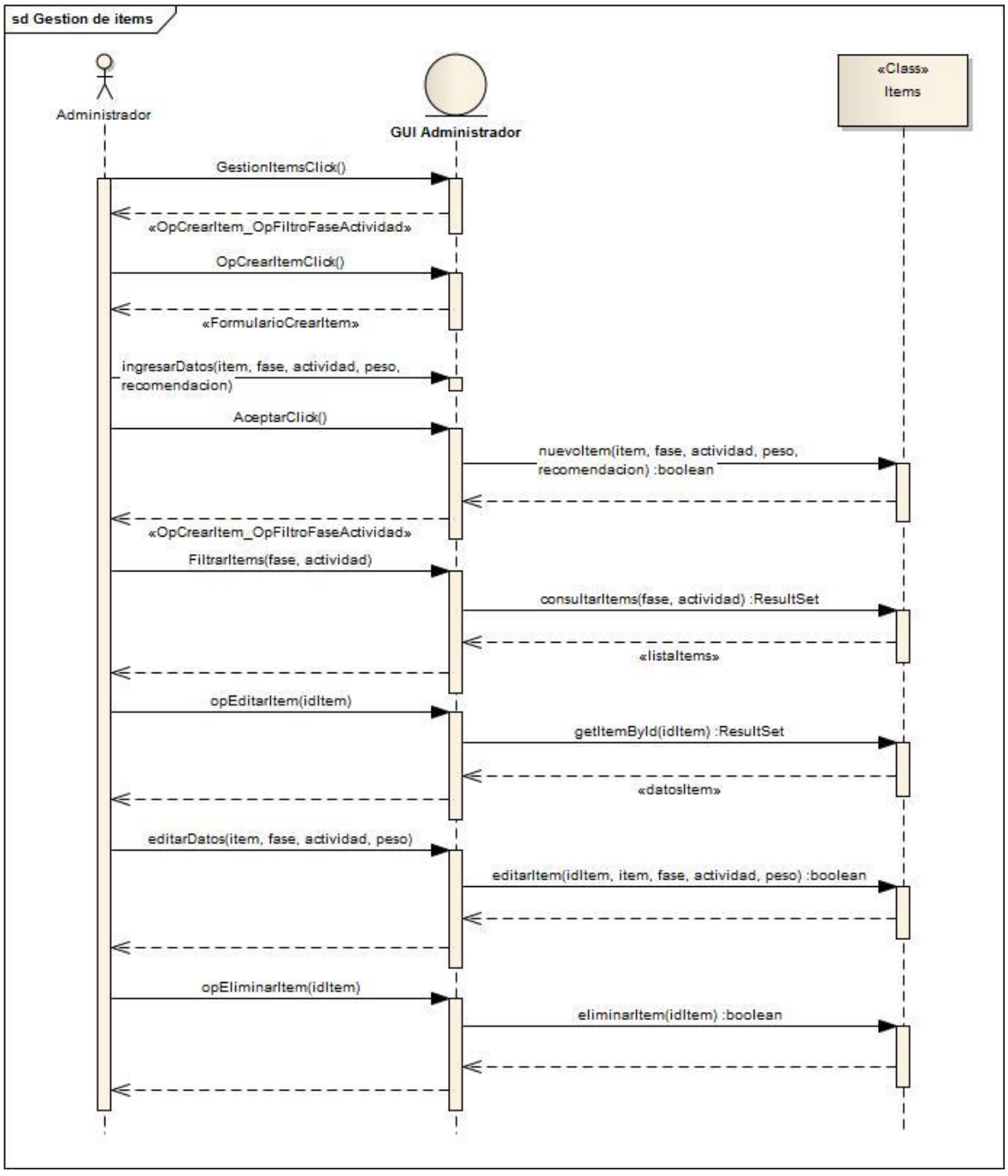

Figura 41. Gestión de items

Fuente: (Autor, 2014)

Gestión de recomendaciones

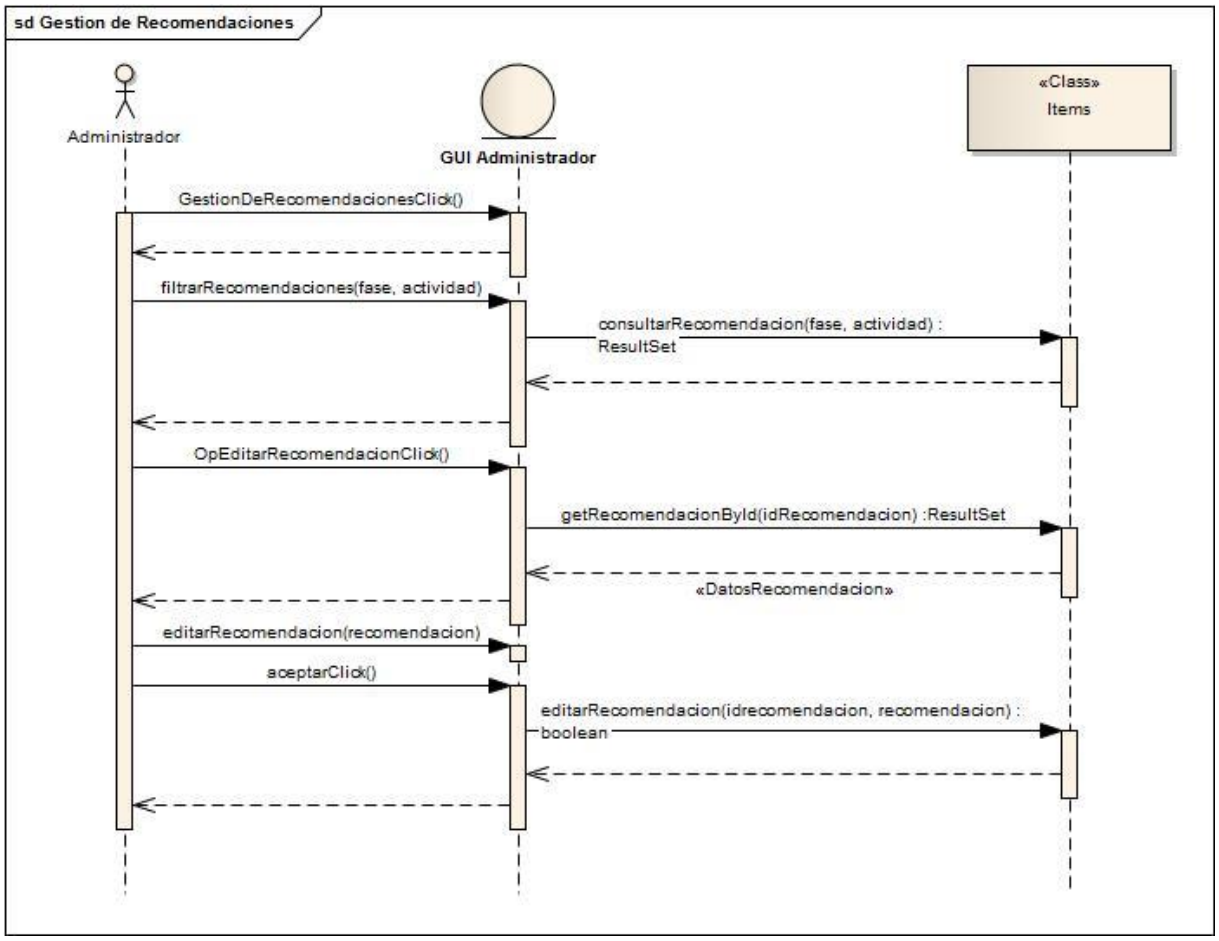

Figura 42. Gestión de recomendaciones

Fuente: (Autor, 2014)

Validación de implementacion de ciberseguridad

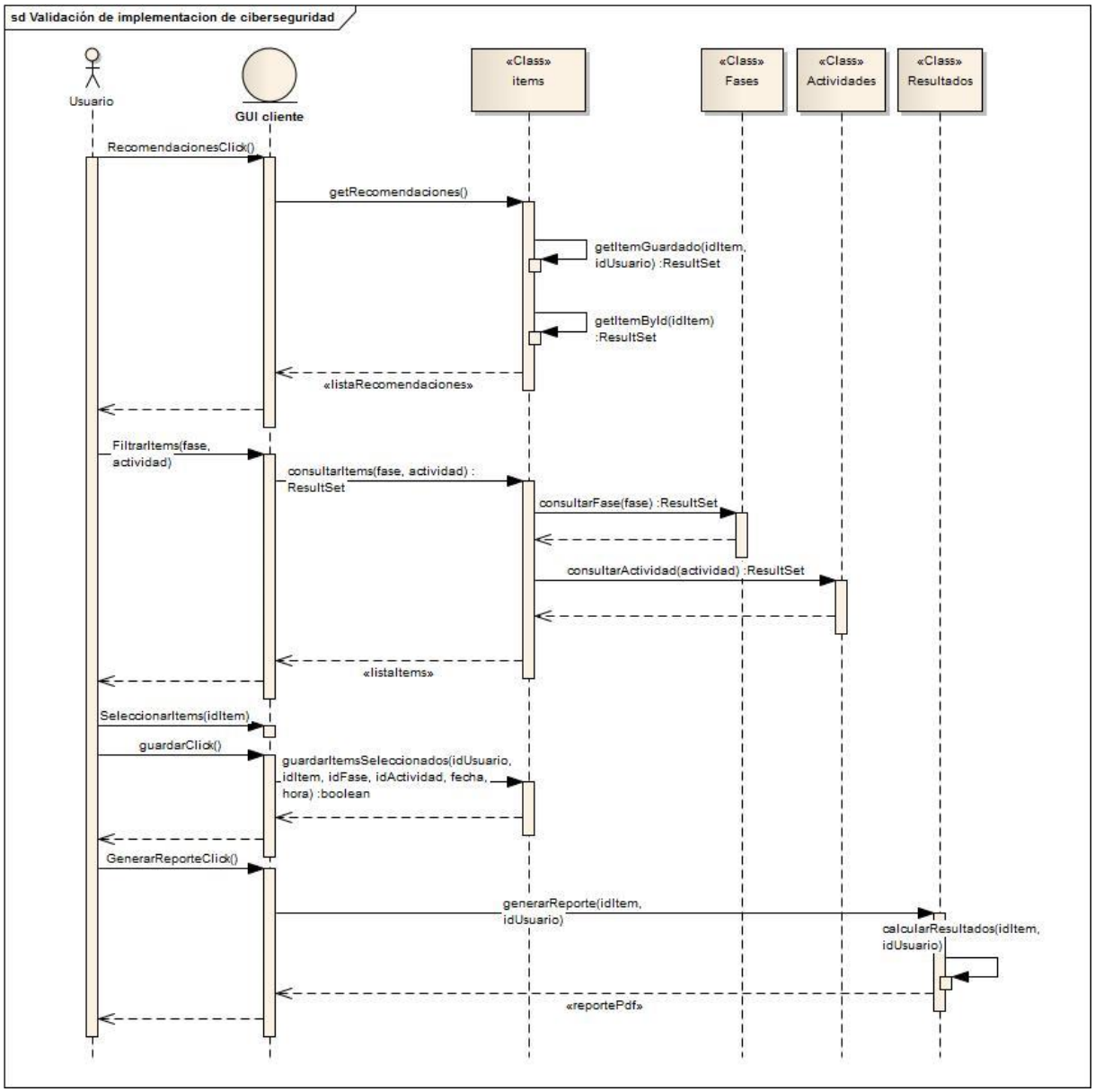

Figura 43. Validación de implementación de ciberseguridad

Fuente: (Autor, 2014)

Anexo H: Diagramas de actividades

Cliente

Logear Usuario

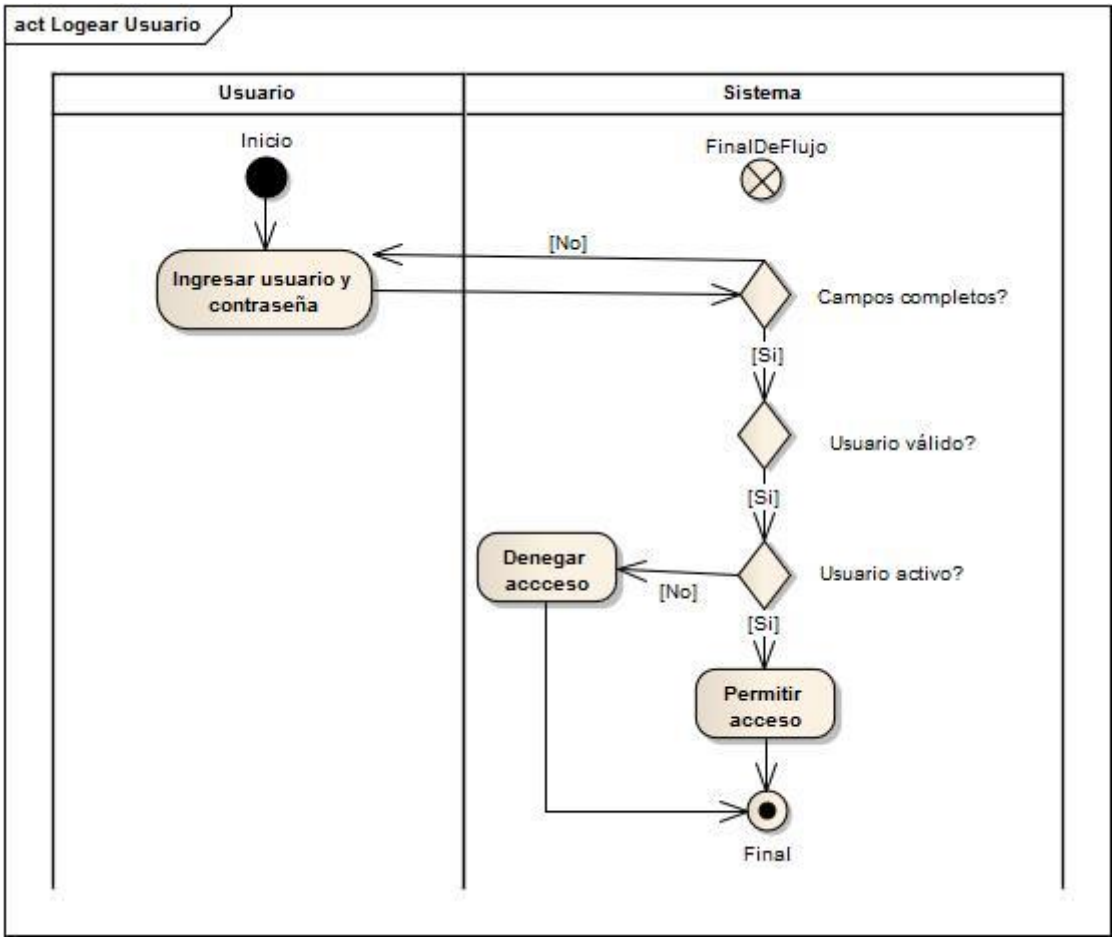

Figura 44. Logear Usuario

Fuente: (Autor, 2014)

Registrar nuevo cliente

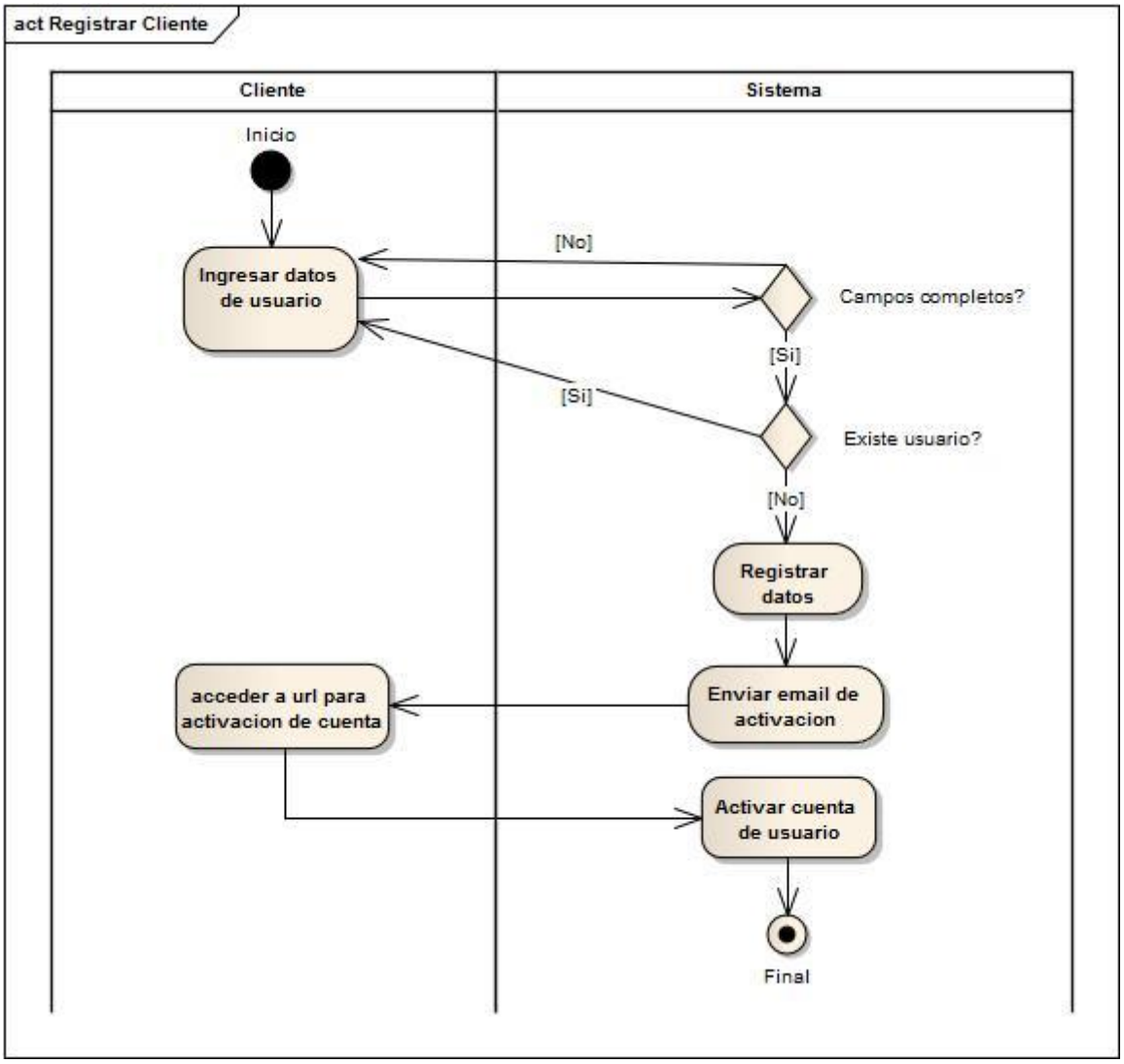

Figura 45. Registrar nuevo cliente

Fuente: (Autor, 2014)

Gestión de clientes

Editar cliente

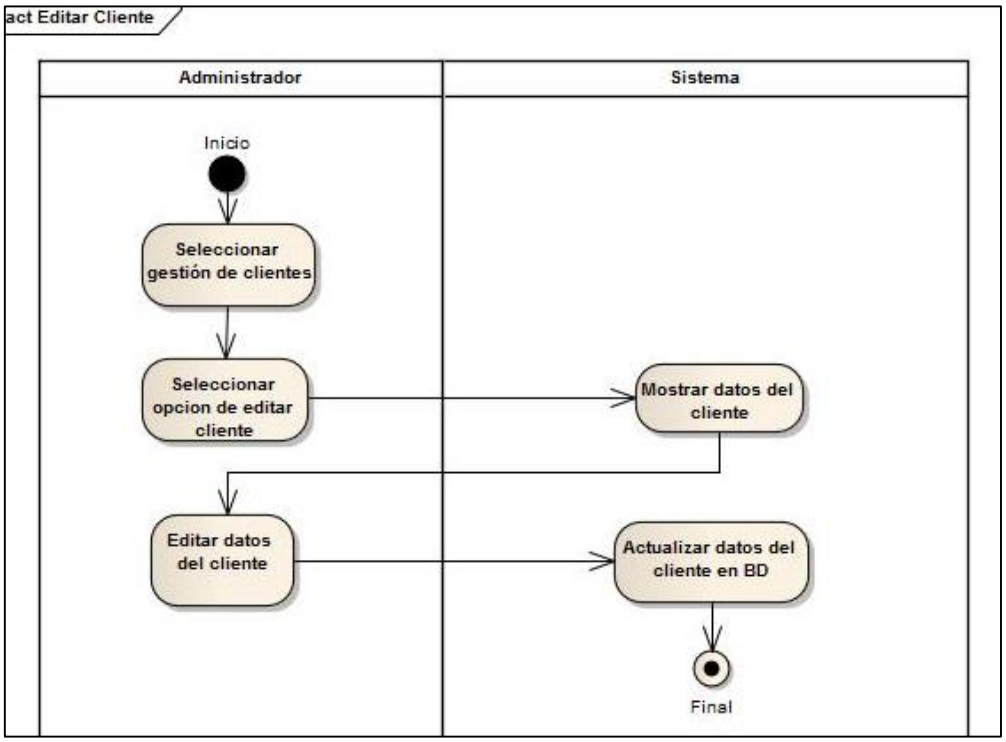

Figura 46. Editar datos del cliente

Fuente: (Autor, 2014)

Eliminar cliente

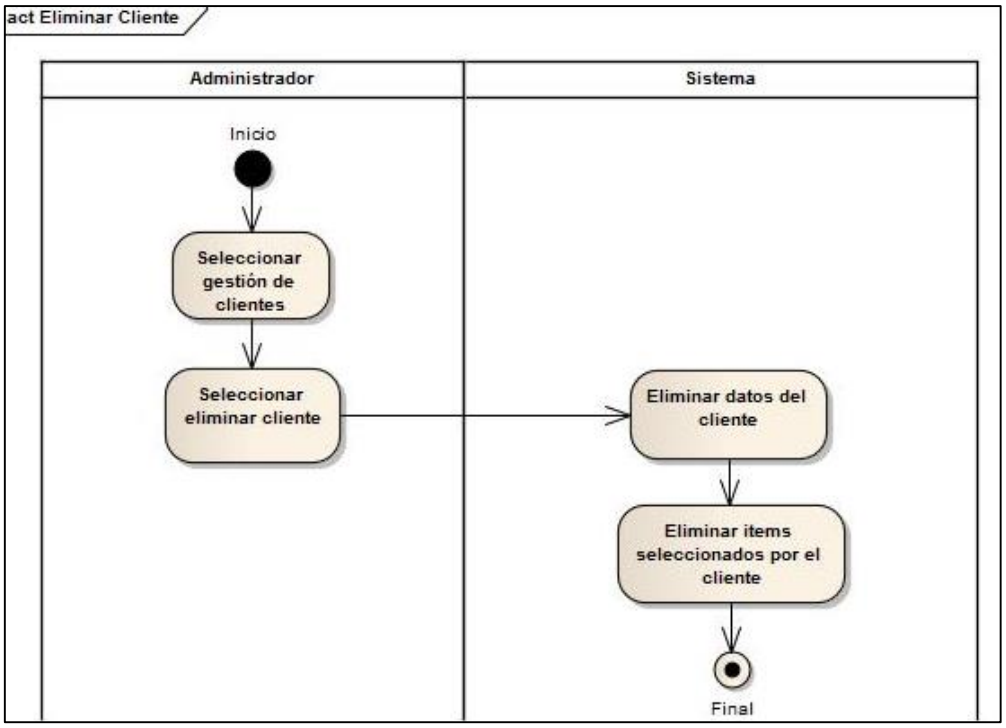

Figura 47. Eliminar cliente

Fuente: (Autor, 2014)

Gestion de items

Insertar ítem

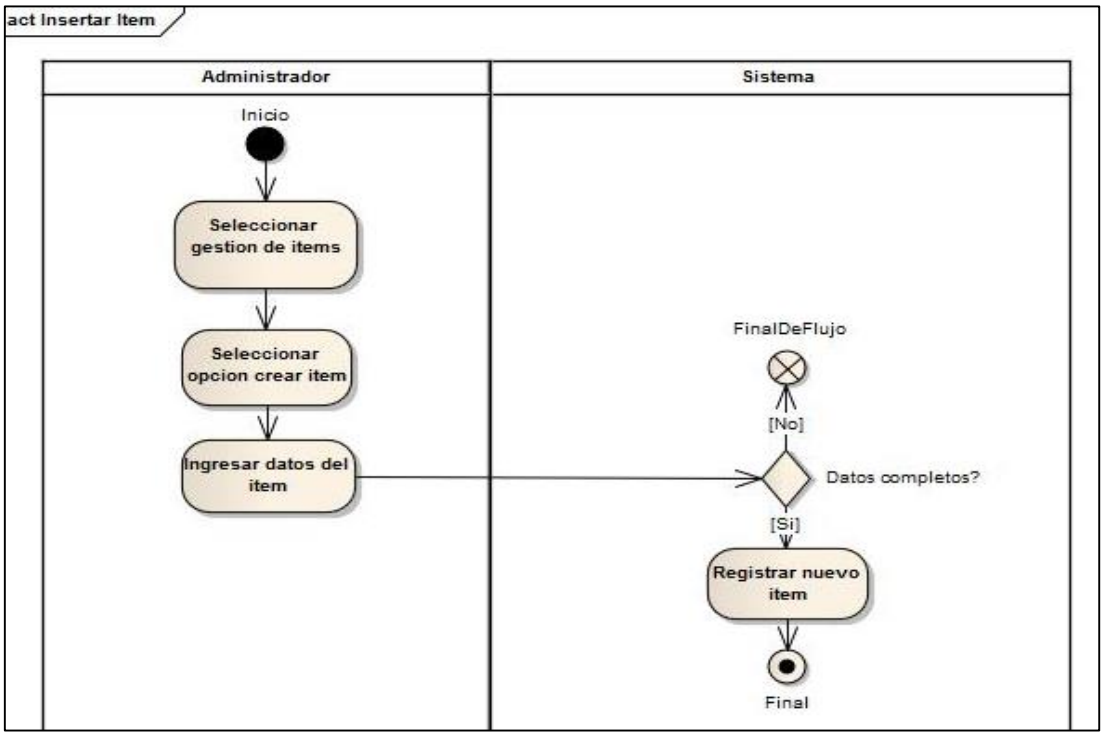

Figura 48. Insertar ítems

Fuente: (Autor, 2014)

Listar Ítems

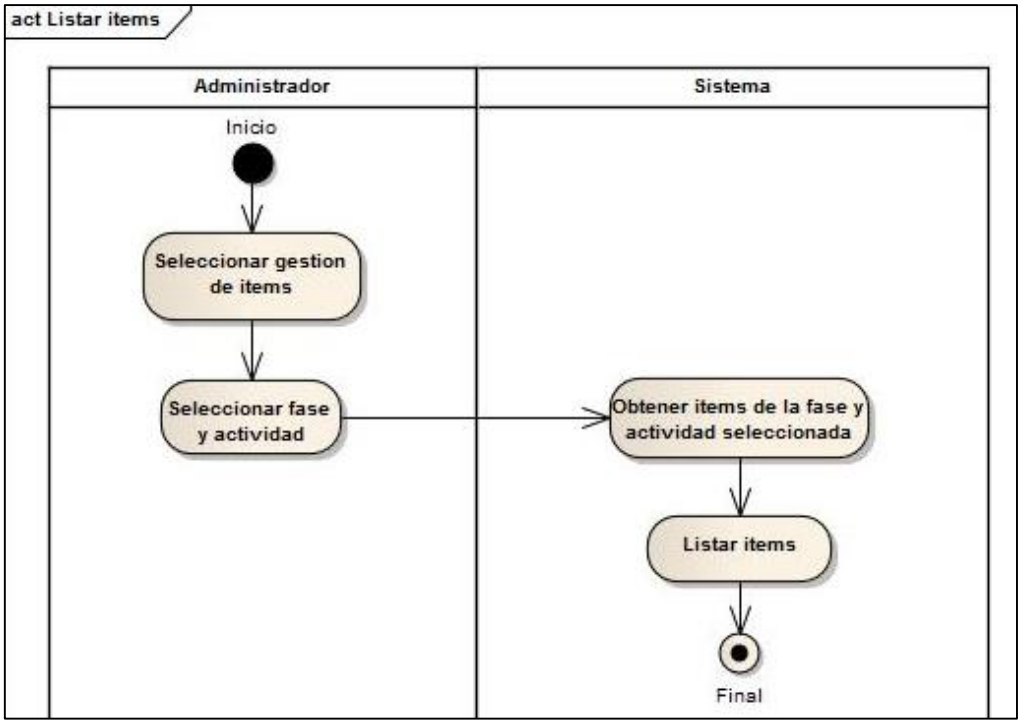

Figura 49. Listar ítems

Fuente: (Autor, 2014)

Editar ítem

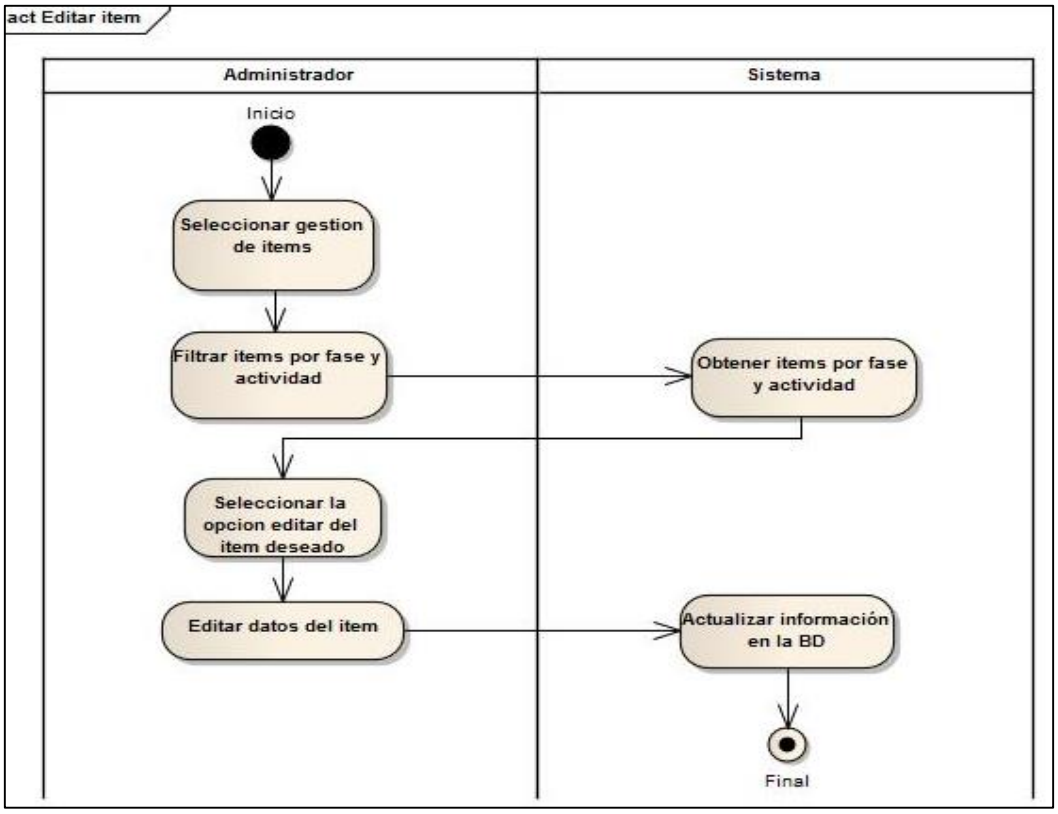

Figura 50. Editar ítem

Fuente: (Autor, 2014)

Eliminar ítem

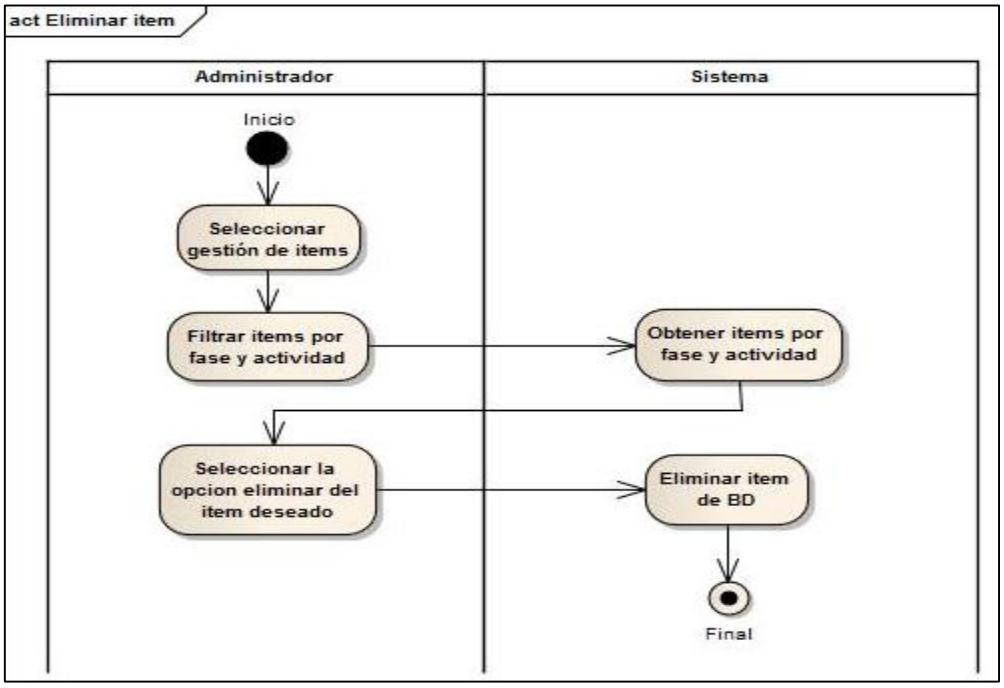

Figura 51. Eliminar ítems

Fuente: (Autor, 2014)

Gestión de items

Editar Recomendación

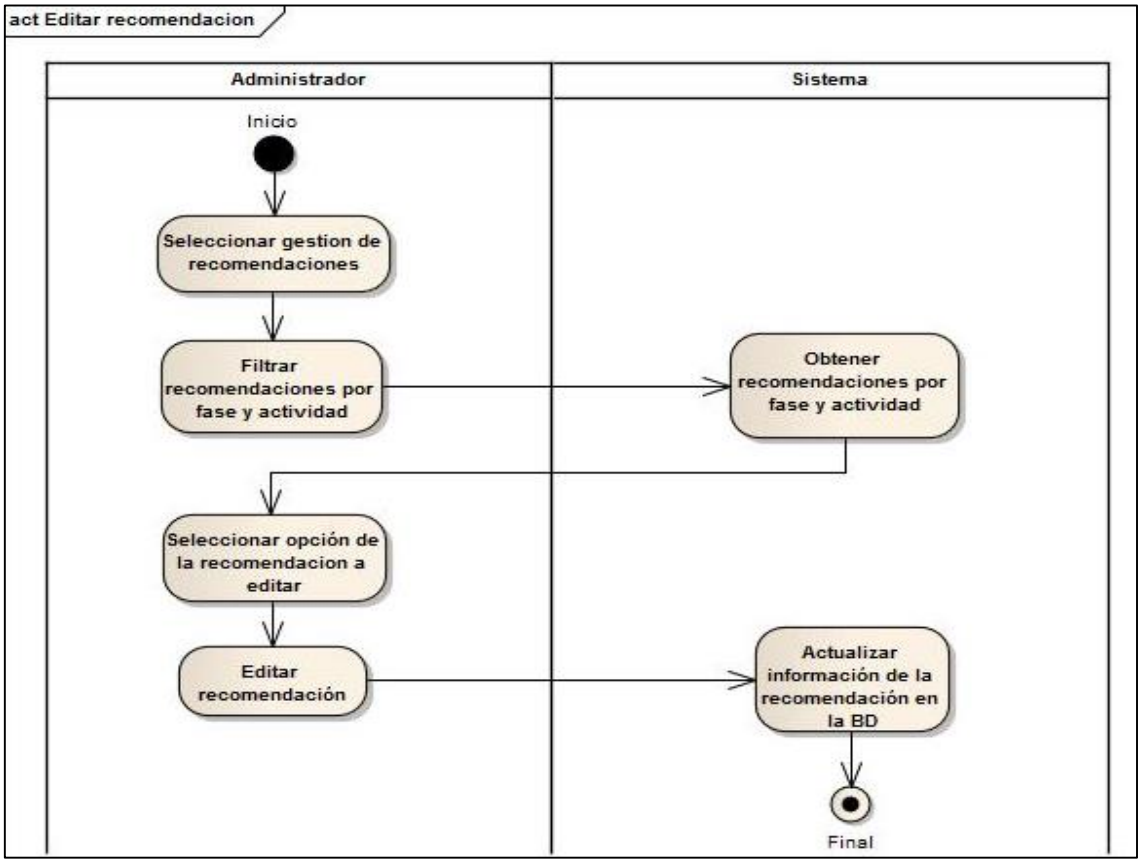

Figura 52. Editar Recomendación

Fuente: (Autor, 2014)

Validación de implementacion de ciberseguridad

Listar recomendaciones

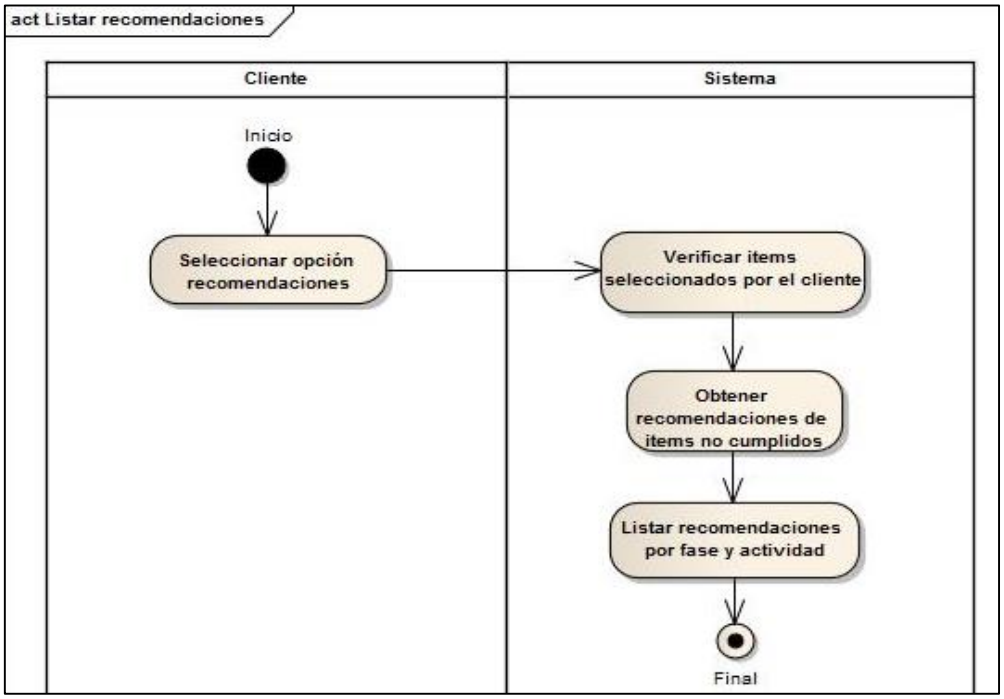

Figura 53. Listar recomendaciones

Fuente: (Autor, 2014)

Guardar ítems

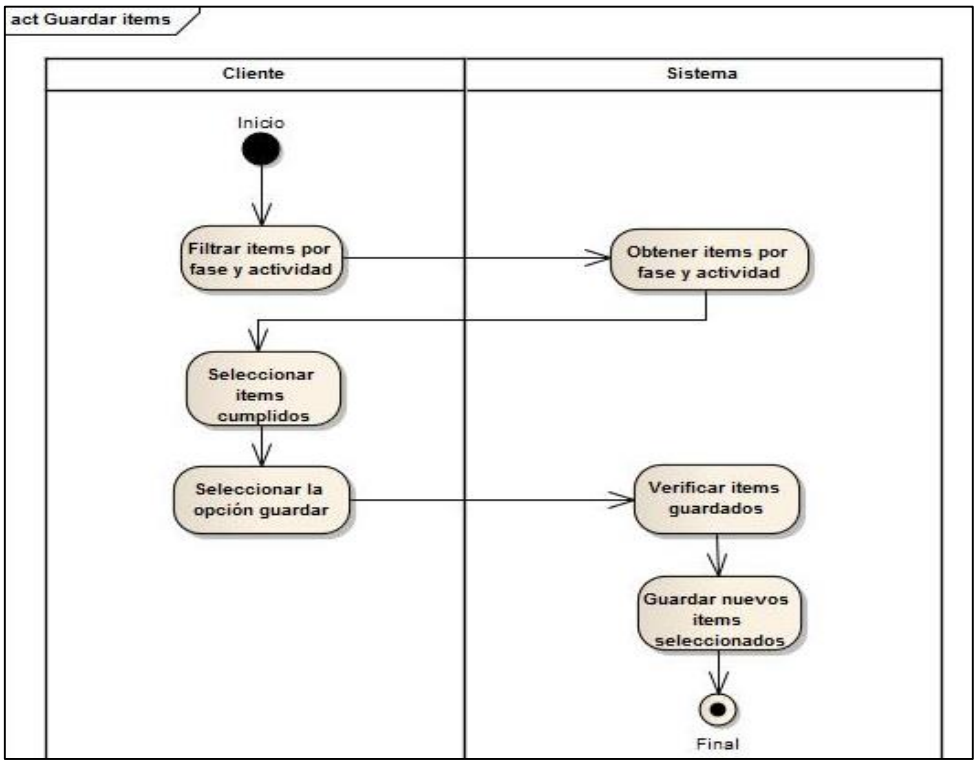

Figura 54. Guardar ítems seleccionados

Fuente: (Autor, 2014)

Generar reporte

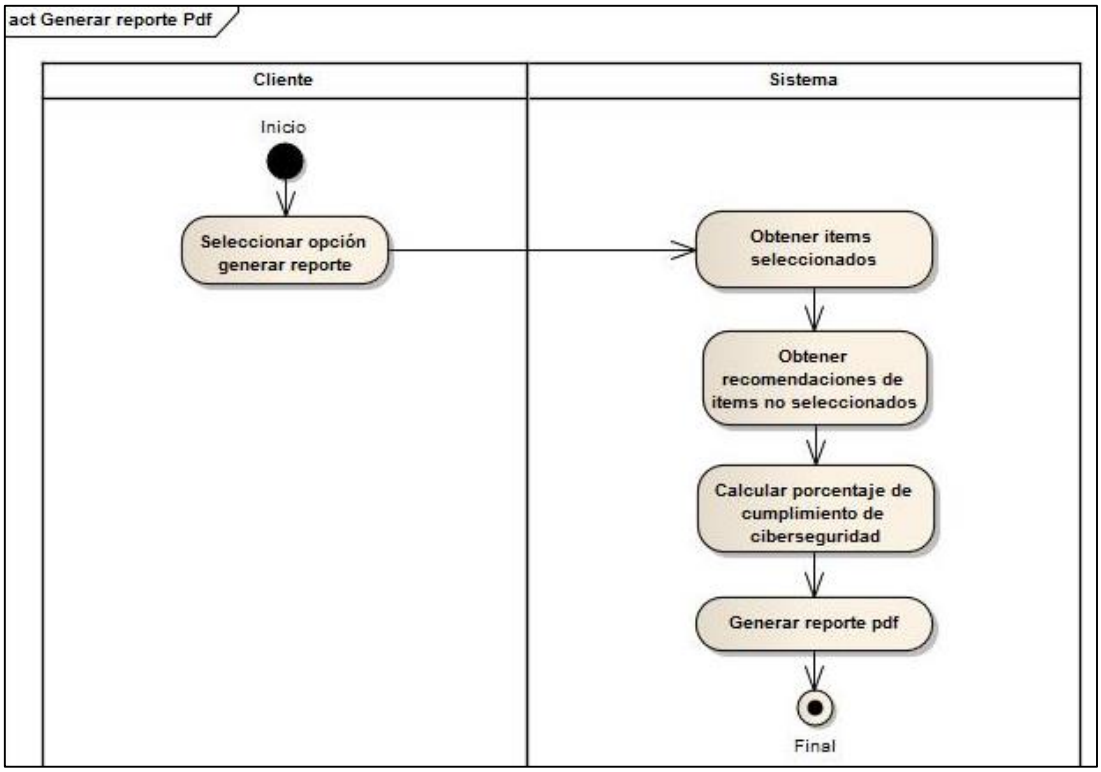

Figura 55. Generar reporte del control de la implementación de ciberseguridad

Fuente: (Autor, 2014)

Anexo I: Manuales

Manual de Usuario

Introducción

SICSAE permite a un usuario registrarse y poder llevar el control de la implementación de la guía de ciberseguridad para AE, a través de un conjunto de ítems clasificados por actividades de acuerdo a cada fase del ADM.

Sistema SICSAE

El sistema dispone de una ventana principal (ver Figura 56) donde se pide ingresar el mail y la contraseña del usuario, en caso de no estar registrado, se puede realizar el registro del nuevo usuario a través del link del mensaje que se encuentra debajo del botón ingresar.

Figura 56. Interfaz principal de SICSAE

Fuente: (Autor, 2014)

Cliente

Registro de nuevo cliente

En la Figura 57 se puede observar la ventana de registro, para un nuevo cliente, el cual deberá ingresar los datos requeridos (Username, Nombre, Apellido, Mail, Contraseña). El mail debe ser válido para poder enviar una URL de activación de la cuenta del nuevo cliente (ver Figura 58).

Figura 57. Interfaz para registro de nuevo cliente

Fuente: (Autor, 2014)

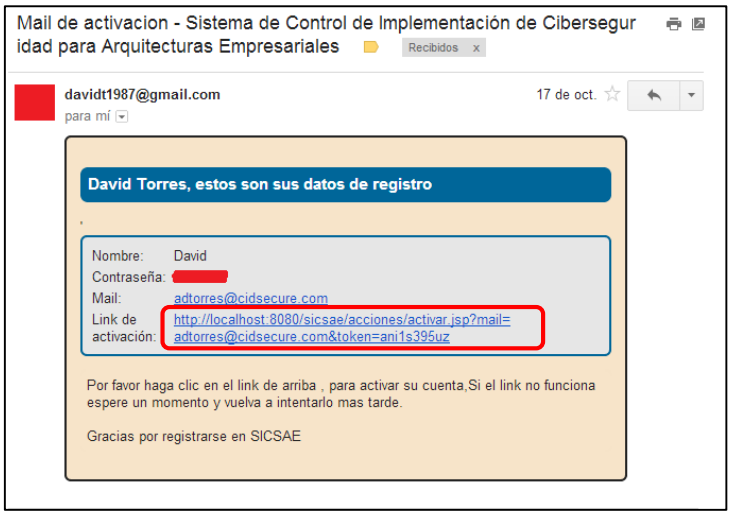

Figura 58. Mail de activación de nuevo cliente

Fuente: (Autor, 2014)

Recuperar contraseña

En caso de que el usuario realice tres intentos fallidos (ver Figura 59), se presentara una nueva ventana (ver Figura 60), donde se debe ingresar usuario, contraseña y el texto de la imagen catcha, esto como un método de seguridad para evidar multiples intentos de credenciales erróneas.

Figura 59. Mensaje de error, por usuario y contraseña incorrectos

Fuente: (Autor, 2014)

Si el cliente no recuerda su usuario y contraseña puede dar clic en la opción para recuperar contraseña (ver Figura 60)

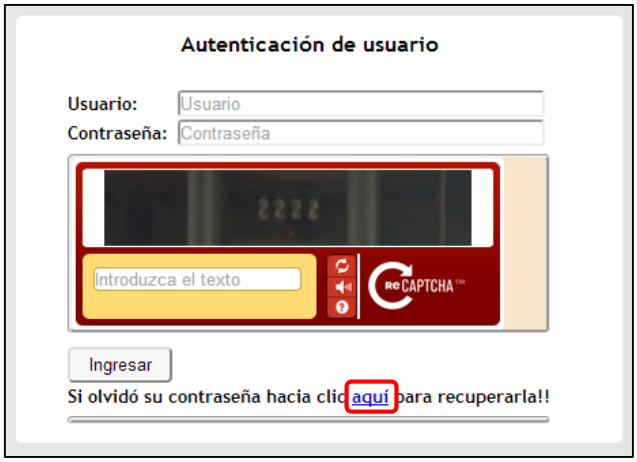

Figura 60. Opcion de ingreso de captcha, mas usuario y contraseña

Fuente: (Autor, 2014)

Una ves que el usuario haga clic en la opción para recuperar contraseña, será rederigido a una pagina (ver Figura 61) donde debe ingresar su email, mas el texto del captcha para poder recuperarla.

Figura 61. Recuperar usuario y contraseña

Fuente: (Autor, 2014)

Cuando el cliente haya ingresado el correo y el texto del captcha, deberá revisar su correo electrónico para ver los datos de su cuenta (ver Figura 62)

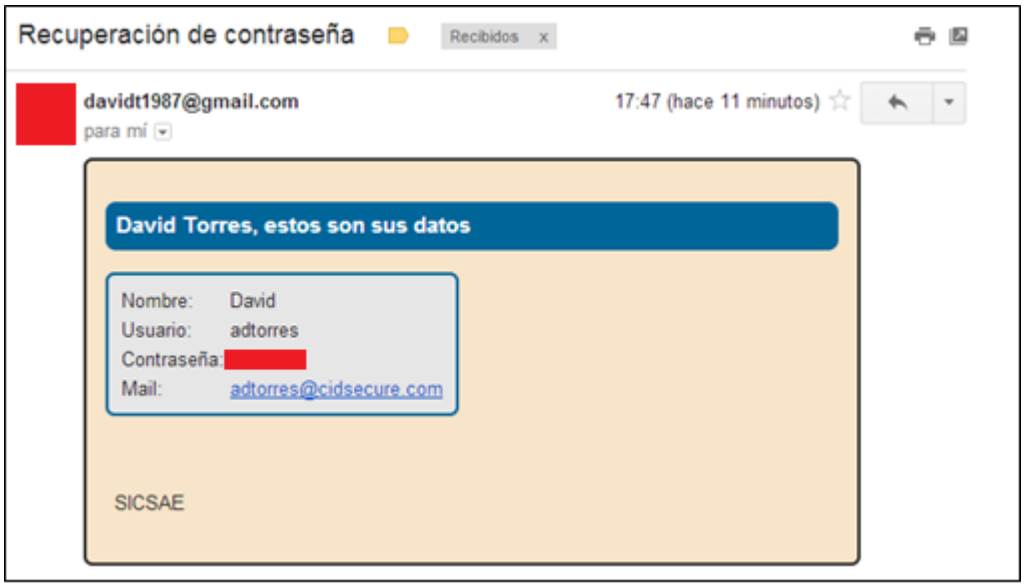

Figura 62. Mensaje de recuperación de usuario y contraseña

Fuente: (Autor, 2014)

Área de validación de implementación de ciberseguridad para AE

Dentro del área de validación de implementación de la guía, se pueden filtrar los items a través de las opciones de fase y actividad, que el usuario desee evaluar. (ver Figura 63).

Figura 63. Interfaz de validación de implementación de ciberseguridad para AE

Fuente: (Autor, 2014)

Una ver seleccionada la fase y la actividad se puede ver una ventana (ver Figura 64) donde se encuentran los items respectivos, que el cliente puede seleccionar y guardar para validar y ver el avance de la implementación de ciberseguridad.

Figura 64. Interfaz de validación de implementación de ciberseguridad para AE

Fuente: (Autor, 2014)

Reporte

Como se puede ver en la Figura 65, existe un ícono, el cual sirve para generar reporte (ver Figura 66), de la validación de implementación de ciberseguridad, además existe la opcion de recomendaciones, esta opción muestra una lista de recomendaciones (ver Figura 67) necesarias que provee el sistema SICSAE que se deben considerar dentro del trabajo de cada actividad de ciberseguridad.

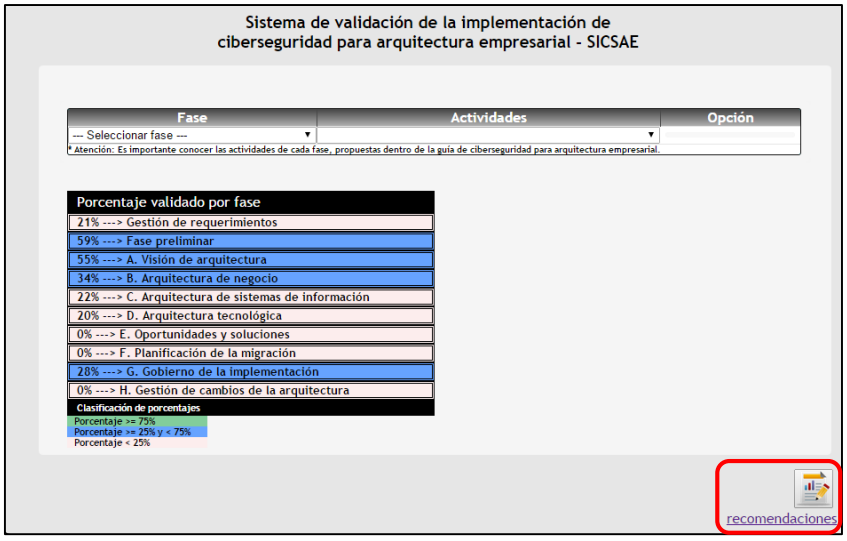

Figura 65. Opción de reporte y recomendaciones del sistema SICSAE

Fuente: (Autor, 2014)

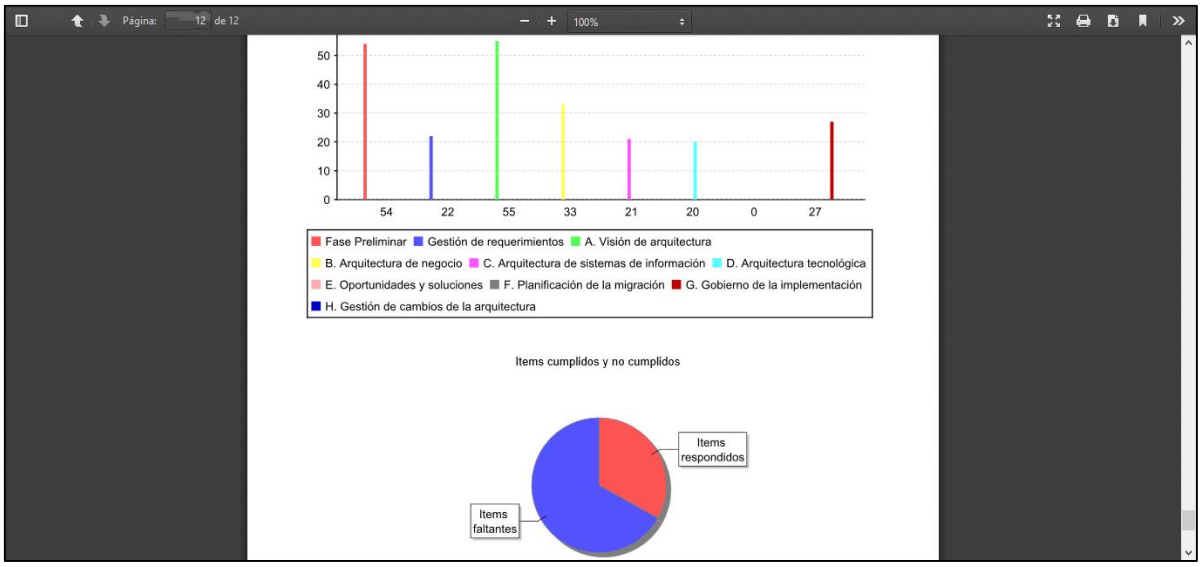

Figura 66. Reporte del sistema SICSAE

Fuente: (Autor, 2014)

Figura 67. Recomendaciones del sistema SICSAE

Fuente: (Autor, 2014)

Administrador

Como se puede observar en la Figura 68, para el perfil de administrador, existe un área de gestión de usuarios, gestión de ítems, y gestión de recomendaciones.

Figura 68. Área del administrador

Fuente: (Autor, 2014)

Gestión de usuarios

Para la gestión de usuario existen dos opciones por usuario registrado: editar y eliminar usuario (ver Figura 68)

Editar cliente

Si el administrador selecciona la acción de editar, ya puede proceder a editar la información (ver Figura 69), una vez realizada la operación, ya puede guardar los cambios realizados

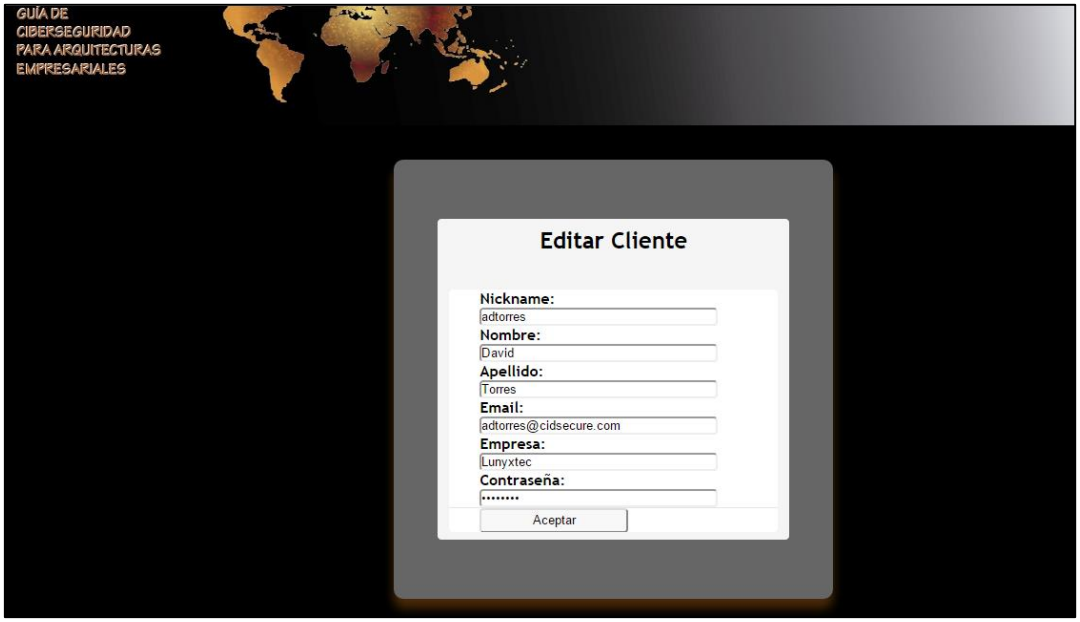

Figura 69. Gestión de clientes - Editar

Fuente: (Autor, 2014)

Borrar cliente

En la figura 68 se puede observar la opción de borrar, una vez seleccionada esta opción, el usuario se eliminará.

Gestión de items

Para gestionar los ítems, se puede filtrar las opciones de fase y actividad (Ver figura 70)

Figura 70. Gestión de items

Fuente: (Autor, 2014)

Una vez que se selecciona la fase y la actividad se puede observar una lista de ítems (ver Figura 71), con las opciones de editar y eliminar, para poder gestionarlos.

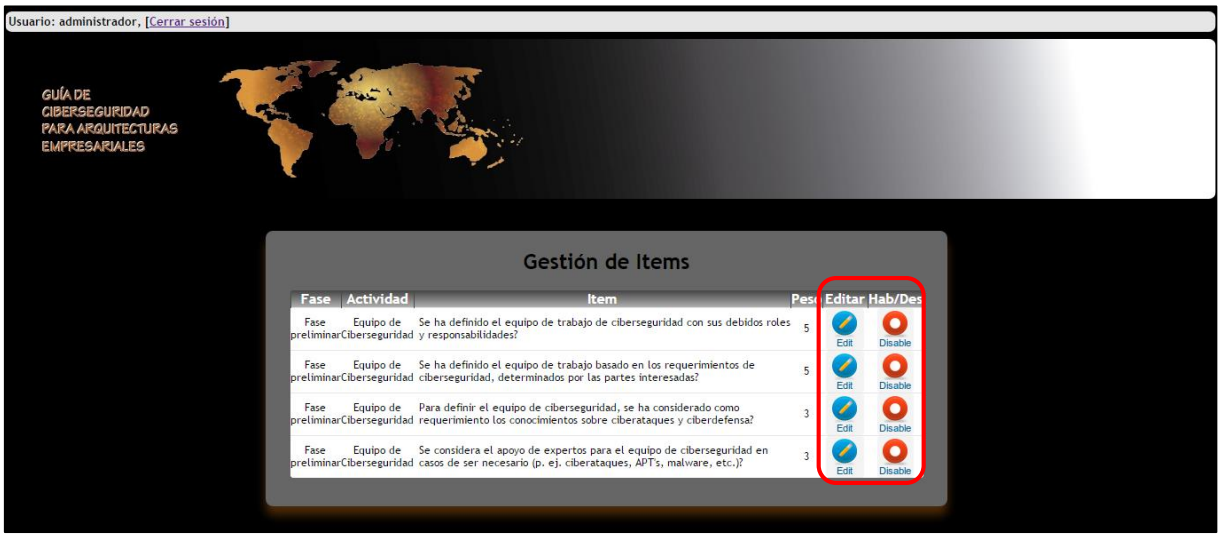

Figura 71. Lista de ítems por fase y actividad

Fuente: (Autor, 2014)

Editar Ítem

Ya que se ha seleccionado el ítem a editar, aparece un formulario con la información del ítem a editar (ver Figura 72), una vez terminado el procedimiento se puede dar clic en el botón aceptar

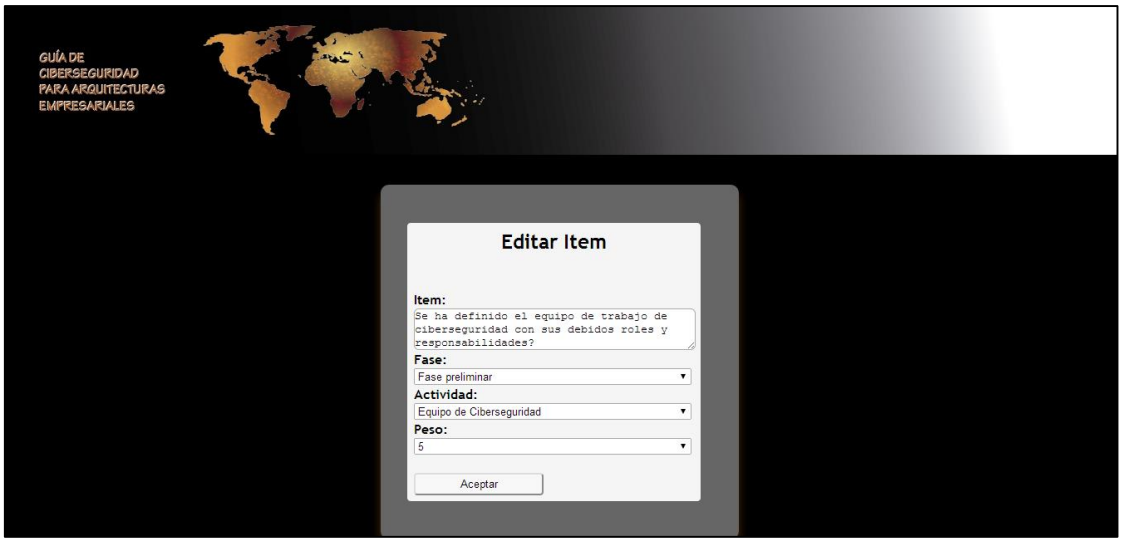

Figura 72. Editar ítem

Fuente: (Autor, 2014)

Eliminar Ítem

Una vez seleccionada la opción de delete ítem (ver Figura 71), este se eliminara

Insertar Ítems

En la figura 70 se puede ver la opción *crear ítems*, una ves seleccionada esta opción, se puede observar un formulario (ver Figura 73) para registrar un nuevo ítem en el sistema, como su respectiva recomendación, una vez llenados los campos, se debe dar clic en aceptar para insertar el nuevo ítem.

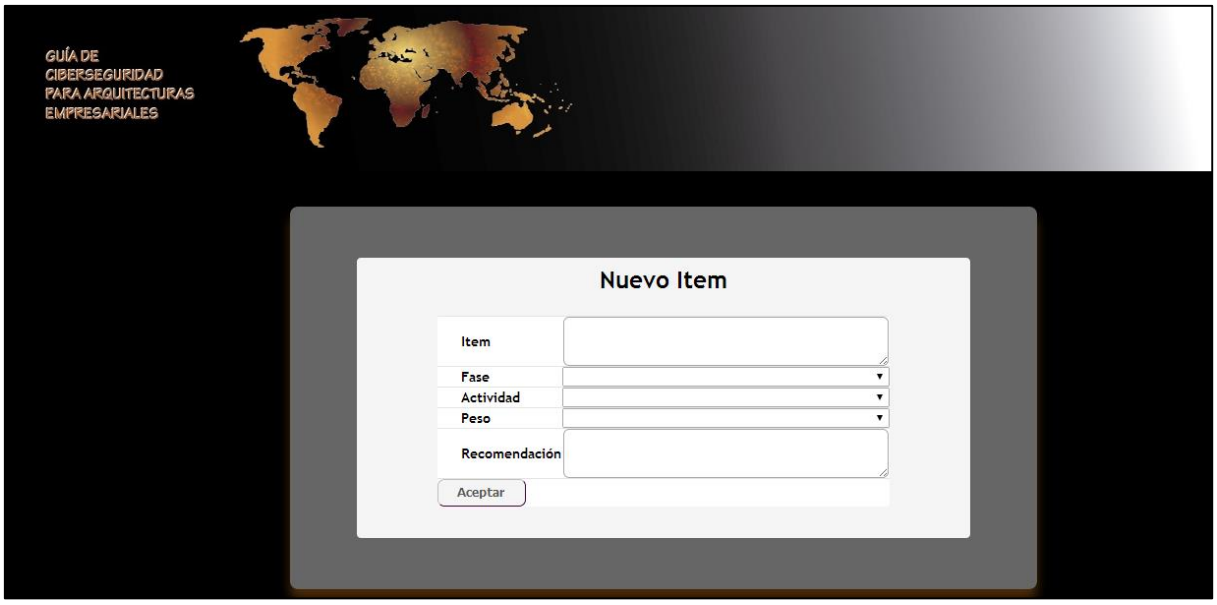

Figura 73. Insertar ítem

Fuente: (Autor, 2014)

Gestión de recomendaciones

Para la gestión de recomendaciones, se pueden filtrar las mismas de acuerdo a su fase y actividad (ver Figura 74)

Figura 74. Gestión de recomendaciones

Fuente: (Autor, 2014)

Editar Recomendación

Una vez que se ha seleccionado la fase y la actividad se despliegan los items correspondientes, en donde se puede observar la opción de editar para cada recomendación (ver Figura 75)

Figura 75. Gestión de recomendaciones

Fuente: (Autor, 2014)

Al momento de seleccionar la opción editar de la recomendación deseada se puede observar la información correspondientes para editarla (ver Figura 76)

Figura 76. Gestión de recomendaciones

Fuente: (Autor, 2014)

Anexo J: Items para validación de la implementacion de ciberseguridad

Para la validación de ciberseguridad dentro de la AE de una organización, se han desarrollado un conjunto de items, basados en el cumplimiento de las actividades por cada fase del ADM de la guía desarrollada, estos items

Tabla 16. Items para la validación de ciberseguridad en una AE

Item	Actividades	Fases
Se ha definido el equipo de trabajo de ciberseguridad con sus debidos roles y responsabilidades?	Equipo de Ciberseguridad	Fase preliminar
Se ha definido el equipo de trabajo basado en los requerimientos de ciberseguridad, determinados por las partes interesadas?		
Para definir el equipo de ciberseguridad, se ha considerado como requerimiento los conocimientos sobre ciberataques y ciberdefensa?		
Se considera el apoyo de expertos para el equipo de ciberseguridad en casos de ser necesario (p. ej. ciberataques, APT's, malware, etc.)?		
Se han identificado y definido previamente los marcos de trabajo necesarios para la implementación de ciberseguridad como SABSA y COBIT 5?	Marcos de referencia para ciberseguridad	
Se han considerado marcos de riesgos de TI dentro del trabajo de ciberseguridad?		
Se encuentra adaptado para la implementación de ciberseguridad el marco de TOGAF como el núcleo de la arquitectura empresarial?		
Se han identificado las áreas de riesgos, las cuales están propensas a ataques que afectarían al negocio?	Areas de riesgo	
Las áreas de riesgos son analizadas de acuerdo a los marcos de riesgos de TI seleccionados?		
Se ha establecido un nivel de criticidad para tratar las áreas de riesgos identificadas?		
Analizar el riesgo de los ataques/violaciones hacia los procesos de negocio y dar prioridad en consecuencia de la ciberseguridad	Principios de ciberseguridad	
Establecer un nivel tolerable de ataques e infracciones, visto desde una perspectiva empresarial.		
Realizar un análisis de las partes interesadas (internas y externas) y derivar los requisitos para ciberseguridad.		
Realizar un análisis de los requerimientos de negocio y obtener los requisitos específicos para ciberseguridad		
Definir los objetivos de alto nivel de ciberseguridad y obtener la aprobación de la alta dirección		
Identificar leyes, regulaciones y normas de gobierno para ciberseguridad, y definir los requisitos para su cumplimiento		
Cumplir con el mandato de los requerimientos de las leyes y regulaciones para el sistema global de ciberseguridad y sus componentes		

Establecer indicadores clave de rendimiento (KPI) e informes periódicos de ciberseguridad.		
Establecer indicadores clave de riesgo (KRI) y presentar informes periódicos de ciberseguridad		
Identificar las amenazas para todos los componentes de los Sistemas de Información de la empresa		
Anticiparse a las amenazas futuras ocasionadas por la ciberdelincuencia y la ciberguerra		
Recopilar datos y pruebas sobre los incidentes, ataques y violaciones de ciberseguridad		
Aprovechar la experiencia externa para la gestión de amenazas, según corresponda		
Establecer un proceso de mejora continua, basado en la experiencia de tendencias pasadas y futuras		
Establecer un proceso de tolerancia a fallos/errores de ciberseguridad.		
Fomentar una cultura que promueva la mejora y adaptación del pensamiento de ciberseguridad		
Definir un proceso adecuado de identificación y evaluación del riesgo		
Validar las opciones para el tratamiento de riesgos en la ciberseguridad		
Alinear el riesgo con el modelo de gobernanza global seleccionado		
Incluir los incidentes del pasado y aprendizajes técnicos/organizacionales		
Identificar y evaluar los nuevos riesgos, derivados de la ciberdelincuencia y ciberguerra		
Proteger la informacion, clasificando los datos en peligro por la ciberdelincuencia		
Proteger la información, mediante la clasificación de datos con respecto a la que se encuentra expuesta a la ciberguerra		
Proteger la información clasificada inclyendo la que se encuentra almacenada en servicios basados en la nube, además de datos que residen o que fluyen a través de dispositivos móviles o públicos		
Proteger la información relacionada con la ciberseguridad para la gestión de identidad y accesos en general		
Identificar las aplicaciones críticas del negocio, mediante la realización de un análisis de impacto en el negocio (BIA) con una perspectiva de ciberseguridad		
Realizar un análisis de dependencia en profundidad de la capa critica de aplicación, para identificar los puntos de entrada potencialmente vulnerables		
Centrarse en el "eslabón más débil de la cadena" de ciberseguridad y alinear al BIA en general		
Asignar recursos y financiamiento, alineados con las amenazas reales de ciberdelincuencia y ciberguerra, y considerar los tipos de ataques indirectos y enfoques de ataque		

Adoptar la mentalidad del atacante - mayores estragos con menos esfuerzo		
Establecer controles para el ciclo de vida de software, en el desarrollo propio y personalizado de aplicaciones		
Definir un proceso incorporado de ciberseguridad para aplicaciones y sistemas potencialmente críticos		
Participar con los proveedores para lograr definir los controles de ciberseguridad necesarios		
Participar con los proveedores para gestionar las vulnerabilidades de día cero y puntos de entrada		
Aplicar la gobernanza de las políticas, normas y procedimientos operativos clave (Kops) de ciberseguridad		
Dar a conocer las rutinas de autoevaluación y evaluación por pares para el personal expuesto (aseguramiento de la integridad)		
Llevar a cabo la verificaciones de antecedentes (sobre una base opt-in) para el personal de ciberseguridad		
Definir e implementar los controles y verificaciones pertinentes para los nuevos empleados asignados a puestos sensibles		
Definir e implementar procedimientos adecuados para la terminación de responsabilidades o contrato		
Garantizar el reconocimiento del personal de ciberseguridad por incentivos y reconocimientos apropiados		
Promover el conocimiento adecuado sobre ciberseguridad y delitos cibernéticos		
Proporcionar ejemplos prácticos y casos de ataques/infracciones.		
Resaltar el impacto de ataques/infracciones en el negocio		
Se realiza el respectivo control de cambios en los requerimientos de cada fase del ADM?	Control de requerimientos	Gestión de requerimientos
Se aprueban los cambios en los requerimientos de ciberseguridad bajo el respectivo control de los mismos?		
Existe la participación de las partes interesadas para la actividad de control de requerimientos de ciberseguridad?		
Atributos de usuario, el mismo debe estar informado sobre todo los correspondiente a actividades y reglamentaciones de ciberseguridad que se crean convenientes	Atributos del perfil de negocio para ciberseguridad	
Atributos de usuario, se debe incluir la debida motivación para su trabajo y optimo rendimiento		
Atributos de usuario, debe estar protegida su información personal, la cual posee la organización		
Atributos de usuario, el mismo debe ser confiable y apegarse a las normas y reglamentaciones que rigen dentro de la organización		
Atributos de gestión, los mismos deben ser automatizados para agilizar el trato de incidentes de seguridad		
Atributos de gestión, basados en la eficiencia de los sistemas de gestión de incidentes y operaciones dentro de la organzación		

Atributos de gestión, los mismos que deben ser mantenibles para facilitar su continuidad		
Atributos operativos, basados en la disponibilidad de los sistemas de información especialmente los de alta criticidad		
Atributos operativos, los cuales deben ser libres de errores o acercarse a este estado optimo		
Atributos operativos, deben ser recuperables en el menor tiempo posible		
Atributos de gestión de riesgos, los mismos que deben basarse en la responsabilidad		
Atributos de gestión de riesgos, se debe facilidar los procesos auditables		
Atributos de gestión de riesgos, los cuales deben tomar en cuenta la autenticación de usuarios (personas y aplicaciones)		
Atributos de gestión de riesgos, los mismo que deben manejar la debida autorización de usuarios (personas y aplicaciones)		
Atributos de gestión de riesgos, donde se identifiquen nuevos riesgos de forma temprana		
Atributos de gestión de riesgos, en donde se maneje la confidencialidad de la información		
Atributos de gestión de riesgos, donde se establezca la propiedad de los mismos		
Atributos legales/reguladores, los mismos que deben ser ejecutables dentro de la organización		
Atributos legales/reguladores, los cuales deben ser de carácter legal para su aplicación		
Atributos legales/reguladores, los cuales deben ser regulados		
Atributos de estrategia técnica, los cuales deben ser Flexibles/Adaptables		
Atributos de estrategia técnica, en donde se deben considerar la capacidad de migración de los sistemas de información		
Atributos de estrategia técnica, los mismos que deben contar con una capacidad escalable		
Atributos de estrategia técnica, quienes deben ser compatibles con estandares		
Atributos de estrategia técnica, los cuales deben ser actualizables		
Atributos de estrategia de negocio, quienes deben manejarse de manera segura		
Atributos de estrategia de negocio, los cuales deben basarse en un aspecto de gobernabilidad del negocio		
Atributos de estrategia de negocio - Proporcionar buena administración y custodia de los sistemas de información		
Se han identificado los roles que intervienen en el campo de seguridad de los SI, para determinar las partes interesadas?	Partes interesadas	A. Visión de arquitectura
Se utilizan técnicas (p. ej. encuestas, visitas de campo) para identificar a las partes interesadas?		

Se identifican las partes interesadas de ciberseguridad y del negocio?		
Se encuentran definido el nivel de participación e influencia de las partes interesadas?		
Se utilizan herramientas (p. ej. entrevistas, prototipos, modelado), para la recolección de requerimientos?	Requerimientos de ciberseguridad	
Se encuentran definidos los requerimientos (funcionales y no funcionales)?		
Se encuentran aprobados los requerimientos a través de las partes interesadas?		
Se han identificado los marcos de ciberseguridad que van a trabajar durante esta fase de Visión de Arquitectura?	Marcos de referencia para ciberseguridad adaptado	
Esta considerado el marco de trabajo de transformando a la ciberseguridad usando COBIT 5 durante esta fase?		
Se encuentra definido un modelo de riesgos propio del negocio?	Modelo de riesgos del negocio	B. Arquitectura de negocio
El modelo de riesgos del negocio definido, abarca a los SI?		
El modelo de riesgos definido, se lo puede aplicar hacia las amenazas identificadas, probabilidades de materializarse y el impacto que puede causar un incidente?		
Se han identificado las leyes y regulaciones de SI, que están ligadas hacia la ciberseguridad?	Leyes y regulaciones ligadas a ciberseguridad	
Se han identificado los artículos de las leyes y regulaciones que intervienen en el control y gestión de la ciberseguridad?		
Se han identificado los marcos de ciberseguridad que se utilizaran dentro de esta fase de Arquitectura de Negocio?	Marcos de referencia para ciberseguridad adaptado	
Para definir los marcos de referencia se han tomado en consideración a marcos de riesgos de TI e ISO 27001 para políticas de seguridad?		
Se han identificado a los dominios tanto internos y externos del negocio que requieren protección?	Modelo del dominio de ciberseguridad	
Se ha determinado la criticidad de la relación entre los dominios (servicios, aplicaciones) de ciberseguridad?		
Se ha identificado el tipo de seguridad requerida para las relaciones establecidas entre dominios?		
Los protocolos de confianza se encuentran definidos de acuerdo a las buenas prácticas de NIST (marco para mejorar la ciberseguridad en las infraestructuras críticas) e ISO 27001?	Protocolos de confianza	
Los protocolos de confianza están apoyados por documentos legales (p. ej. contratos, SLAs)?		
Se ha realizado un detalle técnico de los protocolos de confianza que existen entre dominios (internos y externos)?		
Se encuentran definidas las responsabilidades para la gestión de ciberseguridad?	Organización de ciberseguridad	
Se encuentra establecida la propiedad (responsable) de los riesgos de ciberseguridad?		
Existe un proceso definido para la gestión de riesgos de seguridad?		
Se han definido los objetivos de control (p. ej. Protección contra código malicioso, Gestión de incidentes de seguridad		

de la información y mejoras, etc.) para el proceso de gestión de ciberseguridad?		
Se encuentran definidas las medidas a tomar para la gestión de ciberseguridad ante incidentes informáticos?		
Se realizan Informes del estado actual de la ciberseguridad de forma periódica?		
Existes un proceso definido para la gestión de incidentes?		
Existen políticas definidas de seguridad de la información dentro de la organización?	Políticas de ciberseguridad	
Se han desarrollado políticas de ciberseguridad tomando en consideración las buenas practicas de ISO 27001, NIST y COBIT 5?		
Se han desarrollado las políticas de ciberseguridad de acuerdo a sus principios y requerimientos de las partes interesadas?		
Se encuentran definidas las políticas de forma clara y precisa para la protección contra fallos/ataques?		
Se encuentra actualizado el catálogo de los servicios de negocio de la organización?	Catálogo de servicios de ciberseguridad	C. Arquitectura de sistemas de información
Están definidos los servicios de ciberseguridad dentro del catálogo de servicios de la organización?		
Se encuentra definida la criticidad de cada uno de los servicios definidos dentro del catálogo?		
La organización cuenta con un esquema de clasificación que se aplique hacia los servicios de negocio y por consiguiente a los servicios de ciberseguridad?	Clasificación de servicios de ciberseguridad	
Se han utilizado normas (p. ej. ISO 27001) como buenas prácticas para la clasificación de servicios?		
Durante esta fase se han identificado los marcos de trabajo necesarios para la implementación de ciberseguridad en la arquitectura empresarial?	Marcos de referencia para ciberseguridad adaptado	
Se ha identificado a la norma ISO 27001 como un recurso que se adapte a TOGAF en el trabajo de implementación y mejora de la ciberseguridad?		
Se identificaron la reglas, prácticas y procedimientos de ciberseguridad de acuerdo al análisis de brechas?	Reglas, prácticas y procedimientos de ciberseguridad	
Se identificaron los marcos y normas (COBIT, ISO 27001, NIST) para referenciar el trabajo de ciberseguridad?		
Se realiza copias de respaldo de información y software, y se prueba regularmente?	Análisis de brechas	
Se asegura que el código móvil autorizado, opere de acuerdo a las políticas de seguridad?		
La documentación de los sistemas es protegida del acceso no autorizado?		
Se dispone de procedimiento para la gestión de contraseñas?		
Los usuarios solo tienen acceso a los servicios que están autorizados?		
Se utiliza mecanismos apropiados de autenticación para acceso de usuarios externos?		

Se segrega en la red, los usuarios y sistemas de información?		
Se controla el acceso al SO en las estaciones o terminales?		
Se restringe el uso de utilidades (software) no autorizadas, que podrán eludir las medidas de control del sistema?		
Se dispone de una política de uso de controles criptograficos para proteger la información?		
Se realiza gestión de claves para dar soporte al uso de las técnicas criptográficas?		
Se dispone de procedimientos para la instalación de software?		
Se controla el acceso al código fuente de los sistema de información?		
Se procura minimizar las vulnerabilidades que se podráan explotar de los sistemas de información?		
Se mantiene un inventario de activos de información?		
Todo activo de información tiene asignado un responsable (propietario)?		
Se dispone de una normativa para el uso de los activos de información?		
La información está clasificada según su valor, sensibilidad y criticidad?		
Se aplica seguridad a los equipos fuera del local?		
Todo equipo requiere autorización para ser retirado de la organización?		
Se encuentran separados los recursos de desarrollo, prueba y producción?		
Se encuentran establecidos criterios de aceptación de sistemas y se realizan las pruebas antes de su aceptación?		
Se validan los datos de entrada hacia las aplicaciones para asegurar que esta sea correcta y apropiada?		
Existen procedimientos y controles para protección de la infraestructura y los servicios de red a través de la segregación de la red, responsabilidades operativas, cifrado, autenticación y uso de logs?		
Se realizan pruebas periódicamente de los respaldos de información y software?		
Se protege la información de las transacciones en línea: De transmisión incompleta, pérdida de rutas, alteración, divulgación y duplicidad?		
Utiliza actualmente software la detección temprana de ataques informáticos?		
Existe acuerdos de confidencialidad, previos al conocimiento de áreas, activos o procesos críticos de la organización?		
Se han identificado los SI que necesitan protección y mejora en sus controles y procedimientos contra ciberataques?	Estándares de ciberseguridad	D. Arquitectura tecnológica
Se han identificado los estándares para la protección del flujo de información entre las TI?		
Se han determinado las reglas, prácticas y procedimientos de acuerdo a los estándares de ciberseguridad requeridos para esta fase?	Reglas, prácticas y procedimientos	

Se identificaron las buenas prácticas y controles de marcos y normas (ISO 27001 y NIST) para la implementación de ciberseguridad en la arquitectura tecnológica?	de ciberseguridad	
Se han identificado los marcos de ciberseguridad necesarios para su implementación durante esta fase?	Marcos de referencia para ciberseguridad adaptado	
Se han verificado los procesos y las soluciones propuestas en las fases B, C y D?	Procedimientos para el control de oportunidades y soluciones	E. Oportunidades y soluciones
Se ha medido la eficacia de los servicios de ciberseguridad existentes dentro de la arquitectura empresarial?		
Se han verificado los controles de ciberseguridad a reutilizar dentro de la arquitectura empresarial?		
Se han identificado todos los riesgos asociados en la implementación de ciberseguridad?	Control de migración	F. Planificación de la migración
Se han priorizado los controles más importantes para la implementación de ciberseguridad?		
Se han definido y afianzado los roles y responsabilidades de ciberseguridad para su implementación y gestión?	Gestión de ciberseguridad	G. Gobierno de la implementación
Se ha determinado un proceso de gestión e inteligencia contra amenazas?		
Se han integrado las funciones de ciberseguridad con las funciones del negocio?		
Se ha implementado un proceso de intercambio de información y canales de comunicación bien definidos?		
Se ha definido un proceso pro-activo para anticiparse a ataques y al comportamiento del atacante?		
Se ha determinado un proceso flexible y adaptable para aprendizaje y mejora organizacional de ciberseguridad?		
Existe un proceso (prevención, detección, respuesta y seguimiento de incidentes) para gestionar el rendimiento clave de ciberseguridad?		
Se han determinado los indicadores de riesgo que afecten a los sistemas de información?		
Se tiene establecido un proceso para auditoria de controles y políticas de ciberseguridad?	Auditorias de ciberseguridad	
Se lleva un proceso de pruebas o test de penetración hacia los SI?		
Se lleva un proceso para auditorias técnicas y de controles, apoyado por marcos de trabajo y normas de seguridad?		
Se lleva un proceso para la revisión de configuraciones de SI y TI?		
Se ha establecido un proceso para auditoria de código desarrollado en contra de requerimientos y estándares de seguridad?		
Se ha establecido un proceso para la concientización de ciberseguridad en los usuarios?	Conciencia de ciberseguridad	
Se encuentra establecido un periodo de tiempo para la capacitación contra ataques informáticos (ciberataques)?		
Se lleva un proceso para la capacitación de usuarios de acuerdo a ciertas necesidades técnicas y roles?		

Dentro de la conciencia de ciberseguridad se identifica la capacitación contra ataques y/o violaciones potenciales y reales?		
La concientización de ciberseguridad es llevada a cabo en la organización desde las políticas de ciberseguridad?		
Se evalúan los componentes priorizados para su implementacion, de manera que se asegure el trabajo planificado de ciberseguridad?	Gobernanza	
Se identifica dentro de cada iteración del ADM que los componentes y proyectos planeados se hayan cumplido de forma que generen valor hacia la arquitectura empresarial de la organización?		
Se ha verificado la existencia de cambios relevantes que han sido originados en las fases del ADM?	Gestión de cambios	H. Gestión de cambios de la arquitectura
Se ha determinado que acciones se van a llevar a cabo en la gestión de los cambios originados?		
Se ha generado el documento de cambios estableciendo la criticidad, origen e impacto de los mismos?		
Se ha realizado una evaluación del trabajo actual de ciberseguridad, para verificar sus ventajas?		
Se ha determinado si existen controles de ciberseguridad dentro de la arquitectura actual que son considerados inadecuados para mitigar los riesgos modificados o nuevos?		
Se ha abordado totalmente el proceso de toma de decisiones, sobre los cambio en los controles o procedimientos de ciberseguridad para la AE?		
Se realiza el control sobre los cambios existentes en los procesos, para hacer frente a incidentes causados por ataques o violaciones de seguridad?	Gobernanza de la ciberseguridad	
Se decide si los cambios a efectuar, se realizaran a través de la iteración actual o por medio de una nueva iteración?		

Fuente: (Autor, 2014)