METODOLOGÍA PARA LA IMPLEMENTACIÓN DEL MODELO DE ARQUITECTURA DE SEGURIDAD DE LA INFORMACIÓN (MASI)

JULY ASTRID CALVO SÁNCHEZ

DIEGO JAVIER PARADA SERRANO

UNIVERSIDAD PONTIFICIA BOLIVARIANA
ESCUELA DE INGENIERÍA
FACULTAD DE INGENIERÍA INFORMÁTICA
BUCARAMANGA
2010

METODOLOGÍA PARA LA IMPLEMENTACIÓN DEL MODELO DE ARQUITECTURA DE SEGURIDAD DE LA INFORMACIÓN (MASI)

JULY ASTRID CALVO SÁNCHEZ
ID: 69197

DIEGO JAVIER PARADA SERRANO
ID: 69530

Proyecto de grado para optar el título de Especialista en Seguridad Informática

DIRECTORA

ANGÉLICA FLOREZ ABRIL, MSc

UNIVERSIDAD PONTIFICIA BOLIVARIANA
ESCUELA DE INGENIERÍA
FACULTAD DE INGENIERÍA INFORMÁTICA
BUCARAMANGA
2010

Bucaramanga, 19 de 10 de 2010

Nota de aceptación:

Firma del presidente del jurado

Firma del jurado

Firma del jurado

AGRADECIMIENTOS

July Astrid Calvo Sánchez

Gracias a Dios porque por Él he logrado el equilibrio espiritual en mi vida, el cual me ha permitido desarrollar con éxito los proyectos y metas que me he trazado; Él me ha permitido a través de su bendición obtener de mis padres respaldo incondicional en todas las etapas de mi vida.

Gracias a mis padres y mi hermana por su comprensión y apoyo, en especial a mi Madre pues es ella el motor de mi vida y a quien debo todo lo que soy, debido a que con sus sacrificios y dedicación logró forjar mi carácter y enseñarme el valor de todo lo que Dios dispone para nosotros.

Gracias a mi abuelo Fidel Q.E.P.D. debido a que fue un apoyo incondicional, durante todas las etapas de mi vida y ahora como mi Ángel de la guarda, me enseño que con trabajo duro y dedicación se pueden cumplir los sueños, y que las cosas más valiosas son aquellas que nos cuestan trabajo.

A mi amigo y compañero de proyecto Diego Parada, por todos los años de amistad que me ha ofrecido y por todo lo que he podido aprender a su lado, por los sueños que hemos podido cumplir juntos, por su aporte a mi enriquecimiento personal y profesional, muchas gracias.

A toda mi familia en especial a mis primos Milton, Leidy y a sus padres, por su apoyo incondicional en los proyectos que he emprendido.

A mis compañeros de trabajo en NewNet S.A por todo lo que he podido aprender y lo que me han enseñado durante el tiempo que he trabajado con ellos.

Y por ultimo pero no menos importante a nuestra directora de proyecto y amiga Angélica por todos sus aportes y revisiones a este proyecto, porque cada día nos da herramientas para ser mejores personas y profesionales, por su visión crítica y objetiva y por el tiempo que nos ha dedicado desde el momento en que empezó hacer parte de nuestra vida como docente.

Diego Javier Parada Serrano

Este ha sido un trabajo en el cual se ha invertido tiempo y dedicación por parte de quienes lo desarrollamos, por ello primero deseo darle las gracias a July Calvo quien me ha permitido nuevamente trabajar y aprender de esa gran experiencia como persona y como profesional, además porque con este trabajo se ha afianzado la amistad que desde el pregr o estamos compartiendo.

Sin lugar a dudas, no podía pasar inadvertida la persona que con su toque de perfección y crítica constructiva, guio la formalización de este trabajo, a mi maestra, jefe y amiga Angélica Flórez gracias por su tiempo de dedicación y los buenos consejos, con los cuales mi formación personal y profesional se ha enriquecido positivamente.

Gracias también a las personas que estuvieron allí acompañando con sus oraciones, buenos deseos y energía positiva para que se llegara el día de hoy cuando se culminó este trabajo, a mi novia Leidy Calvo, por la paciencia, entendimiento y apoyo por hacerme un mejor profesional; a mis padres Javier Parada y Maritza Serrano, mis hermanos Sergio y Liliana Parada por su oración constante, por su acompañamiento y apoyo desinteresado y sobre todo por creer en mí.

Y por último y más lo más importante y a quienes sin su ayuda no habría podido ser esto, gracias Dios Padre, Hijo y Espíritu Santo y Santísima Virgen María, por habernos colmado a July y a mí con la prudencia, la sabiduría y la inteligencia de apropiarnos del conocimiento y formalizar el trabajo que nos hará merecedores del título de Especialistas en Seguridad Informática; una etapa más culminada que personalmente me deja las puertas abiertas para un nuevo sueño por realizar, una nueva etapa que iniciar como lo son los estudios en una Maestría, que con la Poderosísima Sangre de Cristo de mi lado sé que podré lograr.

GLOSARIO

Arquitecto de Seguridad de la Información: encargado de alinear los objetivos del negocio con los objetivos de Seguridad de la Información, de tal manera que ésta sea entendida como un apoyo para los procesos de negocio.

Ataque: acción que tiene como finalidad causar daño a un sistema o recurso informático en forma no autorizada.

Auditoria informática: análisis realizado por una persona o un grupo de personas que permite evaluar y generar un juicio de valor con respecto a la planificación, el control, la eficacia, la eficiencia, la efectividad, la seguridad, la economía y la adecuación de la infraestructura informática de la empresa.

Autenticación: esquema de administración en donde se requiere que un actor se identifique con un nombre de usuario y una contraseña ante un servicio informático.

Centro de Datos: espacio físico en el cual se encuentran ubicados los servidores, los equipos de comunicaciones y otros que forman parte de la infraestructura de la red.

CIO: por sus siglas en inglés CIO (*Chief Information Officer*) que en castellano se define como Director Ejecutivo de Tecnologías de Información (TI) o como Director Ejecutivo de Informática.

Clave, Contraseña (*Password)*: palabra o combinación secreta que autentica a los usuarios ante un servicio informático.

Cobit: guía para la administración, gestión y auditoria de los procesos de negocio relacionados con el manejo de la información. Definido por ISACA (*Information Systems Audit and Control Association*).

Copia de Respaldo (*Backup*): duplicación de la información en medios de almacenamiento alternos con el fin de que sea un medio de contingencia para recuperarla en caso de desastre.

Gobierno de Seguridad de la Información: esquema de seguridad de la información que representa las intenciones de la Alta Gerencia en la formalización de un programa de seguridad de la información.

Hardware: según el Diccionario de la Lengua Española (http://www.rae.es/) "Conjunto de los componentes que integran la parte material de una computadora".

Incidente: evento que puede o pone en riesgo la seguridad de uno o varios activos del negocio.

Modelo: según el Diccionario de la Lengua Española (http://www.rae.es/) "Esquema teórico, generalmente en forma matemática, de un sistema o de una realidad compleja, como la evolución económica de un país, que se elabora para facilitar su comprensión y el estudio de su comportamiento."

Nombre de usuario (ID o *Login)*: nombre o número que identifica a los usuarios para autenticarse ante los servicios informáticos de la red.

NTC-ISO/IEC 27001: norma internacional publicada por la *International Organization for Standardization* y por la *International Electrotechnical Commission*, la cual establece los lineamientos para el establecimiento, implementación, monitorización y revisión, mantenimiento y mejora del Sistema de Gestión de Seguridad de la Información (SGSI).

NTC-ISO/IEC 27002: norma internacional publicada por la *International Organization for Standardization* y por la *International Electrotechnical Commission*, es un anexo de la ISO/IEC 27001 donde se describen las buenas prácticas para la seguridad de la información.

Política: según el Diccionario de la Lengua Española (http://www.rae.es/): "Orientaciones o directrices que rigen la actuación de una persona o entidad en un asunto o campo determinado".

Seguridad de la Información (SI): proceso continuo para salvaguardar la confidencialidad, integridad y disponibilidad de la información, al igual que las características de la información como la autenticidad, no repudio, entre otras.

Sistema de Gestión de Seguridad de la información(SGSI): conjunto de actividades enfocadas a establecer, implementar, operar, hacer seguimiento, revisar, mantener, y mejorar la seguridad de la información en las organizaciones.

Software: según el Diccionario de la Lengua Española (http://www.rae.es/) “Conjunto de programas, instrucciones y reglas informáticas para ejecutar ciertas tareas en una computadora”.

TABLA DE CONTENIDO

Pág.

Pág.

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE TABLAS

Pág.

ANEXOS

Pág.

METODOLOGÍA PARA LA IMPLEMENTACIÓN DEL MODELO DE ARQUITECTURA DE SEGURIDAD DE LA INFORMACIÓN (MASI)

AUTOR(ES): JULY ASTRID CALVO SANCHEZ
DIEGO JAVIER PARADA SERRANO

DIRECTOR(A): ANGÉLICA FLÓREZ ABRIL

RESUMEN

En este documento se detalla el Modelo de Arquitectura de Seguridad de la Información (MASI) el cual se encuentra enmarcado en la descripción de los elementos que lo conforman que son: Negocio, Gestión de la Arquitectura de Seguridad de la Información, Marco Normativo de la Seguridad de la Información, Acuerdos e Infraestructura de Seguridad de la Información, los cuales fueron definidos teniendo en cuenta modelos de Arquitecturas de Seguridad de autores reconocidos como son: Bala Iyer y Richard Gottlieb, Jan Killmeyer, George Farah y Jeimy Cano; además otro referente que se tuvo en cuenta en el desarrollo del modelo fue el de normas internacionales como la ISO 27001:2006 y 27002:2007, además del framework de trabajo de ISACA: COBIT 4.1.

Identificados los elementos que conforman MASI, se describen y definen los aspectos que se deben tener en cuenta en la formalización de cada elemento, es decir, las consideraciones claves que se deben cumplir en la implementación de cada elemento para asumir que éste exista. Se establece el paso a paso que permitirá la formalización de las actividades y tareas que deben estar cubiertas en la concepción de cada elemento del MASI para el negocio.

Finalmente, se describen las competencias (formación, conocimientos y habilidades) que deben ser apropiadas por el encargado de llevar a cabo la implementación de la metodología del MASI, ésta responsabilidad recae directamente sobre el Arquitecto de Seguridad de la Información.

PALABRAS CLAVES: Modelo, Arquitectura, Diseño, Seguridad de la Información, Diagrama de Flujo.

V° B° DIRECTOR DE TRABAJO DE GRADO

METHODOLOGY FOR THE IMPLEMENTATION OF THE MODEL OF INFORMATION SECURITY ARCHITECTURE (MASI)

AUTHOR(S): JULY ASTRID CALVO SANCHEZ
DIEGO JAVIER PARADA SERRANO

DIRECTOR: ANGÉLICA FLÓREZ ABRIL

ABSTRACT

This paper shows in detail the Model of Information Security Architecture (MASI) which is framed in the description of the elements that make it up: Business, Management of Information Security Architecture, Information Security Normative Framework, Agreements and Infrastructure of Information Security. Such elements were defined according to the models of security and enterprise architectures proposed by recognized authors like Bala Iyer and Richard Gottlieb, Jan Killmeyer, George Farah and Jeimy Cano. Besides, another referent taken account during the development of the model was the international standards such as ISO 27001:2006 and 27002:2007, besides ISACA's work framework: COBIT 4.1.

Once the elements that make MASI up are identified, there is a description and a definition of the aspects importants for the formalization of each element, that is, the keys considerations that must be accomplished during the implementation of each element to assume that it exists. Afterwards, the steps to allow the formalization of activities and tasks are established, so that they are covered in the conception of each MASI element for business.

Finally, there is a description of competences (qualification, knowledge and skills) which must be appropriate for the person in charge of carrying out the implementation of MASI methodology. It responsibility depends directly on the Information Security Architect.

KEY WORDS: Model, Architecture, Design, Security of Information, Flow Diagram.

V° B° DIRECTOR OF GRADUATE WORK

INTRODUCCIÓN

La seguridad de la información es un proceso que busca establecer mecanismos para conservar en primera instancia la confidencialidad, integridad y disponibilidad las cuales son las características básicas de la información, teniendo en cuenta que ésta es considerada como un activo con valor para las organizaciones, los mecanismos definidos deben la existencia de diferentes técnicas como son: *phising*, *spoofing*, ingeniería social, troyanos, *rootkits*, *pharming*, entre otros ataques informáticos que buscan vulnerar sistemas de información con el fin de robar, destruir, secuestrar o alterar la información y con ello afectar el cumplimiento de las metas del negocio.

Dentro de los mecanismos definidos para la protección de la información de pueden establecer: políticas se seguridad, técnicas de monitorización y aseguramiento de la infraestructura tecnológica, entre otras actividades asociadas, sin obviar que es importante que se establezca un marco que permita brindar un orden y orientar los esfuerzos que se hagan en materia de seguridad de la información propendiendo por que estos de apoyen el desarrollo de los procesos de negocio y no de entorpecerlos.

El desarrollo de este proyecto de grado está orientado en la definición del Modelo de Arquitectura de Seguridad de la Información (MASI) como el elemento orientador dentro del proceso inherente a la seguridad de la información, además de la guía metodológica que permitirá su formalización y las competencias del encargado de orientar su implementación.

¿Por qué MASI?. Con base en la Arquitectura de Seguridad de la Información (ASI) es posible el establecimiento de la administración de la seguridad de la información, ya que se encarga de alinear los elementos del negocio con los elementos de seguridad y su contexto. Un modelo define un patrón claro con elementos genéricos a cualquier negocio que permiten su aplicación, dichas consideraciones son tenidas en cuenta en la definición de MASI y en los elementos que lo conforman.

Para la implementación de la ASI en las organizaciones, MASI establece la existencia de un líder el cual será responsable de orientar la ejecución de la guía metodológica en coordinación con la Alta Gerencia, en razón de cumplir con los requerimientos del negocio. Como apoyo a dicho ideal, MASI define las competencias requeridas por dicho líder enmarcado en el concepto del Arquitecto de Seguridad de la Información.

El Modelo de Arquitectura de Seguridad de la Información (MASI) propuesto en el presente documento, busca definir mecanismos que promuevan la incorporación de la Seguridad de la Información en el negocio (Recurso Humano, Procesos, Tecnologías de la Información). Referente a las tecnologías de la información, vela porque su incorporación esté alienada con las estrategias del negocio; así mismo, provee elementos que facilitan la gestión de la seguridad de la información en el negocio, añadiendo en las acciones de los actores (usuarios, proveedores, Alta Gerencia, clientes, entre otros) pautas, reglas o lineamientos que regulen sus actividades en el cumplimiento sus funciones; referente a los procesos de negocio, MASI es un facilitador mediante la definición de mecanismos que permitan que éstos fluyan o se desarrollen con total normalidad.

1 DESCRIPCIÓN DEL PROBLEMA

Actualmente en el contexto de la seguridad de la información es común encontrarse con un gran número de conceptos como: Gobierno de la Seguridad de la Información, Arquitectura de Seguridad de la Información, Seguridad Informática, Seguridad de la Información, Análisis de Riesgos, entre otros; cada uno de ellos enfocado en un saber o campo de acción específico frente a la protección de la información como aquel proceso inherente a la idea de negocio.

Teniendo en cuenta la importancia que toma dentro el negocio definir un marco de trabajo referente a la seguridad de la información, surge el siguiente cuestionamiento: ¿cómo desarrollar una guía metodológica para definir un modelo de administración de la seguridad de la información? Ésta guía metodológica se debe soportar en un proceso lógico y sistemático que permita alinear los procesos de negocio con los procesos de seguridad de la información, teniendo en cuenta los conceptos mencionados en el párrafo anterior, además de establecer el canal de comunicación por medio de un lenguaje transparente y comprensible por la Alta Gerencia y los encargados de gestionar la seguridad de la información, el cual debe ser aprovechado para manifestar el nivel de compromiso de ambas partes frente a la seguridad de la información.

En el año 2008 se desarrolló el proyecto: "Diseño de la Arquitectura de Seguridad de la Red de la Universidad Pontificia Bolivariana Seccional Bucaramanga"[1]. Con la experiencia lograda en la ejecución de este proyecto se concluyó que la respuesta para la administración de la seguridad de la información está dada por lo que se conoce como Arquitectura de Seguridad de la Información, pero se observó que encontrar una guía metodológica para su formalización no es algo sencillo, debido a que la información disponible presenta modelos complejos y poco explícitos. Por lo anterior, se plantea este proyecto como alternativa para estructurar no solo un modelo que contiene componentes genéricos y adaptables a las necesidades del negocio, sino también la metodología, es decir, el paso a paso para la implantación de un modelo de este tipo.

Para concluir, se considera importante que las organizaciones cuenten con un modelo de seguridad de la información que permita su administración dentro de un marco de trabajo, logrando un orden a las actividades de seguridad que se realicen como apoyo al funcionamiento de los procesos de negocio.

[1] Realizado también por los autores de éste documento como proyecto de grado de Ingeniería Informática de la Universidad Pontificia Bolivariana.

2 JUSTIFICACIÓN

Hoy en día existen documentos relacionados con la seguridad de la información que tocan temas como códigos de buenas prácticas de seguridad (NTC-ISO/IEC 27002), gestión de Tecnologías de la Información (ITIL, COBIT), gestión de riesgos (NTC-ISO/IEC 27005, BS 7799-3:2006), entre otros. Cada uno de ellos brinda pautas que permiten estructurar los requerimientos de seguridad de la información que, a consideración de los autores, deberían cumplirse en el contexto del negocio. Esto, aunque es de gran ayuda, define el qué pero no describe procedimientos para su implementación.

Con base en lo anterior, se define este proyecto para proveer en el negocio un marco de trabajo de la seguridad de la información que pueda ser incorporado en el negocio. También se requiere que dicho marco de trabajo permita alinear la seguridad de la información con la estrategia del negocio, intención que se refleja en la definición de cada uno de los elementos de la metodología, mediante la descripción de actividades y tareas que acompañan y facilitan el entendimiento sobre cómo lograr la formalización de la administración de la seguridad de la información.

3 OBJETIVOS

3.1 OBJETIVO GENERAL

- Desarrollar una guía metodológica que permita la implementación del modelo de arquitectura de seguridad de la información MASI el cual apoye la incorporación de la seguridad de la información en los procesos de negocio.

3.2 OBJETIVOS ESPECÍFICOS

- Definir los elementos que conforman el Modelo de Arquitectura de Seguridad de la Información MASI mediante la revisión del estado del arte de modelos existentes.

- Establecer los procedimientos y formatos que guíen la ejecución, el registro y la documentación de las actividades establecidas en el modelo para facilitar la implementación del MASI en las organizaciones.

- Definir el rol del Arquitecto de Seguridad de la Información y las competencias inherentes a su trabajo, de tal manera que se entienda como el encargado de orquestar los objetivos del negocio con los objetivos de seguridad de la información.

4 MARCO TEÓRICO

4.1 ARQUITECTURA DE SEGURIDAD DE LA INFORMACIÓN

El término de arquitectura se encuentra intrínsecamente relacionado con verbos como: diseñar, planear y construir; hecho que se reafirma revisando sus raíces etimológicas.

Etimología del término arquitectura [1]:

- Arquitectura ⟶ del latín *architectūra* (técnica de diseñar y construir)
- Arquitecto ⟶ del griego *ἀρχιτέκτων* (Arkhitekton)
  - *ἀρχ* (Arkhi) ⟶ jefe
  - *ιτέκτων* (tekton) ⟶ constructor

Arquitectura hace referencia a diseñar; dependiendo del contexto, se pueden encontrar diseños de tipo eléctrico, electrónico, de red de datos, diseño de máquinas, diseño industrial, diseño de redes de acueducto, entre otros. El proceso de diseño permite la definición de un esquema en el cual se vislumbre la armonía entre cada uno de los componentes del mismo y la forma como estos interactúan para proporcionar la funcionalidad dentro del sistema a construir.

En la norma ISO/IEC 27002 se define Seguridad de la Información como el "*proceso de proteger la información contra una gama amplia de amenazas, busca asegurar la continuidad del negocio, disminuir los posibles daños y maximizar el retorno de inversión"* [2]. Realizando un contraste entre la definición de arquitectura y de seguridad de la información, no se evidencia una relación directa entre las mismas, entonces, ¿por qué hablar de arquitectura de seguridad de la información?.

Si se da una mirada a las implicaciones que demanda la definición de SI, básicamente es encontrarse de cara a una serie de procesos complejos para su formalización, por ende se vislumbra la necesidad de darle una estructura, que refleje un orden y armonía, faciliten su implementación, gestión y administración;

dicha estructura se enmarca en la definición de un diseño lógico (arquitectura) que apoye tal fin.

En [1], Jeimy Cano, quien ha desarrollado investigación en el contexto de la SI, establece que una arquitectura de seguridad es: *"la organización lógica para los procesos, estructuras y acuerdos de una corporación que reflejan la integración y regulación de los requerimientos del modelo operacional de la misma"*. Esta definición permite observar otro punto de vista sobre el concepto de arquitectura de seguridad el cual converge con el de los autores del presente proyecto en el hecho en el cual refleja la necesidad de una estructura que permita orientar, integrar y regular el negocio.

Se puede concluir que la arquitectura de seguridad de la información es la correlación de los elementos que permiten diseñar y construir un esquema gerencial que: organice, administre y gestione los procesos de la organización bajo los fundamentos de las buenas prácticas de la SI alineados con las expectativas de la Alta Gerencia.

La alineación de procesos de seguridad y expectativas del negocio se puede manifestar a través de la comunicación clara, precisa y concreta que se establece entre el encargado de la seguridad y la Alta Gerencia del negocio. Dicha comunicación es posible mediante la Arquitectura de Seguridad de la Información la cual maneja un lenguaje estratégico, táctico y operacional:

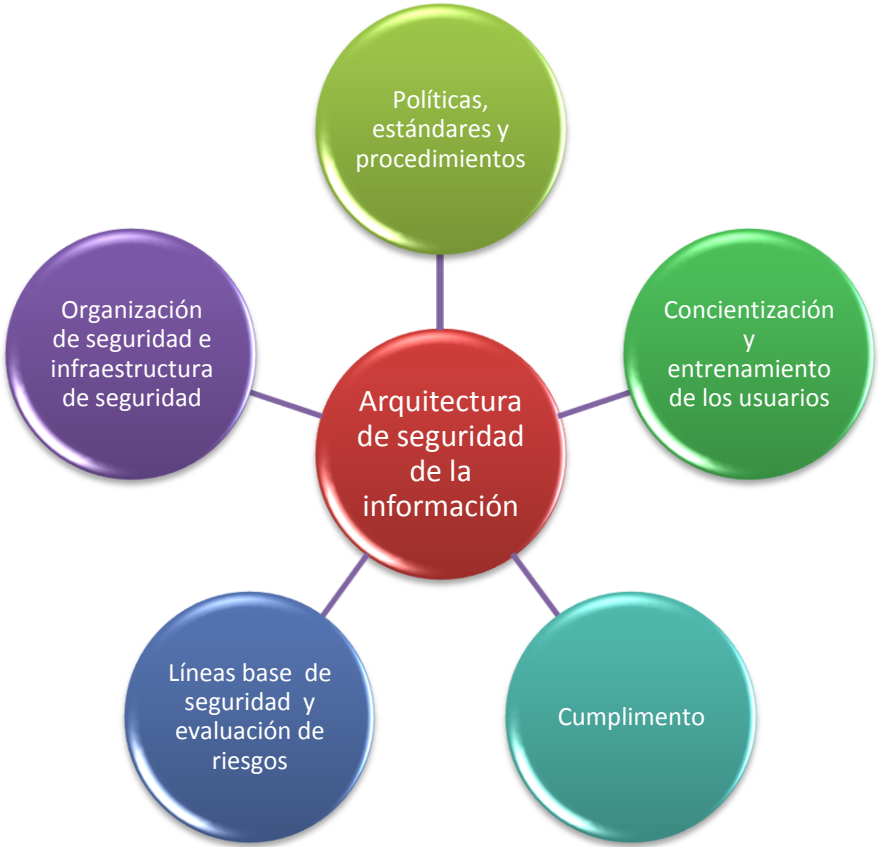
- Estratégico: formulación de la expectativas del negocio, esto es, los lineamientos generales de la ASI.
- Táctico: instrumentalización de la ASI a través de estándares y normas.
- Operacional: definición del comportamiento de los actores del negocio (usuarios, alta gerencia, clientes, proveedores, entre otros) en la ejecución de sus funciones, detallando el cómo se realizan los procesos definidos en la ASI.

4.2 MODELOS PARA LA DEFINICIÓN DE ARQUITECTURAS DE SEGURIDAD DE LA INFORMACIÓN

4.2.1 Arquitectura de seguridad de la información según Jan Killmeyer

Este modelo se encuentra documentado en el libro "Information Security Architecture an Integrated Approach to Security in the Organization" (ver Figura 2) escrito por Jan Killmeyer [3], en el cual se describen los elementos que a su consideración deben ser parte de una Arquitectura de Seguridad de la Información; el modelo contiene los siguientes elementos:

Figura 1. Componentes de la Arquitectura de Seguridad de la Información de Jan Killmeyer.



Fuente: Basado en [3]

- Organización de Seguridad e Infraestructura

Dicho elemento declara la existencia de una actividad principal en el negocio que permite el cumplimiento de los objetivos organizacionales. Para que las metas de la organización no se vean comprometidas en su normal funcionamiento, se incorpora la seguridad de la información como apoyo y facilitador de las mismas. Se designa una persona responsable de la gestión del área de seguridad el cual debe hacer parte de los organismos colegiados de la organización y éste mismo es asesorado por el Comité de Seguridad de la Información.

La Alta Gerencia es fundamental en éste elemento por su conocimiento del negocio, de las necesidades del mismo y de la capacidad de inversión dentro de la organización a nivel de: dispositivos tecnológicos, recurso humano, entrenamiento, entre otros, necesarios para el buen funcionamiento de la Arquitectura de Seguridad de la Información; además, es quien define y aprueba las competencias de la persona responsable de la gestión en seguridad.

A continuación se detallan algunos objetivos del componente: “Organización de Seguridad e Infraestructura”[3]:

- Comprender los principales involucrados (usuarios, contratistas, proveedores, clientes, entre otros) dentro de la estructura de seguridad de la empresa.
- Entender las funciones de seguridad de cada individuo en la organización de seguridad.
- Entender los desafíos de desarrollo de un eficaz funcionamiento y organización de la seguridad.
- Entender el Plan Estratégico de TI y cómo la arquitectura de seguridad debe ser identificada dentro de éste.

- Políticas, estándares y Procedimientos

Según Jan Killmeyer, la política de seguridad de la información describe los objetivos de SI que han sido definidos por la Alta Gerencia, es decir, las expectativas y necesidades que se han identificado respecto a la seguridad de la información en la organización, establece las directrices que deben seguir los usuarios para el cumplimiento de los objetivos de seguridad definidos, por lo tanto, ésta debe ser fácilmente entendible por todo el personal y debe estar incluida en el plan de concienciación y entrenamiento.

Los estándares son un conjunto de normas y procedimientos que han sido definidos para establecer lineamientos que permitan unificar el actuar de los usuarios. Estos son elaborados con base en buenas prácticas de seguridad de la información.

Los procedimientos están definidos de acuerdo a las buenas prácticas y a la experiencia adquirida en el desarrollo de las actividades en la organización, y reflejan la forma en la cual los usuarios deben desarrollar una función, esto permite mitigar las desviaciones en los resultados obtenidos por las diferentes personas que efectúan una misma labor.

- Líneas base de seguridad y la valoración del riesgo:

Los sistemas de información que soportan las actividades del negocio están expuestas a vulnerabilidades como: puertas traseras (*backdoors*), huecos de seguridad (*loopholes*), entre otros. El hecho de verificar estos problemas sobre cierto número de servidores demanda tiempo y dinero, por ello se hace necesario establecer un programa que gestione el riesgo, y este es el objetivo principal de este elemento que conforma la Arquitectura de Seguridad de la Información.

Básicamente el autor recomienda tres procesos para la gestión del riesgo: la creación de líneas base para mejorar la configuración del sistema, la educación a los administradores y usuarios del sistema, y la evaluación de los controles implementados, todo ello aplicado bajo el marco de un ciclo dinámico con el cual se realice realimentación sobre el trabajo que se hace en pro de realizar procesos de mejora continua.

- Capacitación y entrenamiento de los usuarios

La capacitación y entrenamiento apoyan al negocio en el entendimiento de los usuarios sobre la importancia de la SI como mecanismo de protección. El autor define que es imprescindible que los usuarios asuman su responsabilidad en cuanto a salvaguardar la información y la identificación de potenciales amenazas o violaciones sobre los recursos y sistemas de información. El negocio debe contar con los recursos necesarios para la realización de las capacitaciones, no debe escatimar esfuerzos en la definición de campañas creativas y eficaces para la formación de su recurso humano.

El proceso de capacitación debe tener en cuenta la definición y el desarrollo de un cronograma que permita llegar a todo el recurso humano y que facilite la interiorización de la política de seguridad, los procedimientos y las líneas base, así como los mecanismos establecidos por la organización para gestionar los incidentes identificados.

- Cumplimiento

El objetivo de éste componente radica en la medición continua de la eficacia de los objetivos de seguridad propuestos. Teniendo en cuenta que el contexto del negocio se encuentra en constante cambio, hay que medir si los involucrados están comprometidos o no con las expectativas del negocio en cuanto a la seguridad de la información.

4.2.2 Modelo de Arquitectura de Seguridad de la Información de Jeimy Cano

El modelo “Arquitectura de Seguridad Informática – Entre la Administración y el Gobierno de la Seguridad de la Información –”, define tres elementos (ver Figura 2) [1]:

- Estructuras: Pilares del Negocio y la Seguridad Informática.
- Procesos: ISO 27002.
- Acuerdos: Relación expectativas de la Alta Gerencia y Seguridad Informática.

Figura 2. Modelo de Arquitectura de Seguridad de Jeimy Cano[2]

Fuente: Basado en [1]

El modelo define los siguientes componentes:

- Estructuras: conformadas por:
    - Información: reconocida como un activo dentro el inventario de activos del negocio, sobre el cual se deben aplicar los mecanismos necesarios para su aseguramiento.
    - Estrategias de negocio: conocimiento de la misión, la visión y el plan de desarrollo de la empresa.
    - Fundamentos de Seguridad Informática: velar por salvaguardar la confidencialidad, integridad y disponibilidad como los requerimientos mínimos inherentes a la información.
    - Administración de Riesgos: implementación de una metodología de Análisis de Riesgos (CRAMM, Magerit, Octave, entre otras), que permita reconocer los puntos débiles (vulnerabilidades) del sistema de información.

[2] La consulta y referencia de este modelo fue expresamente autorizado por su autor.

- Procesos: incorporación de la norma ISO 27002 en los procesos de la organización, de tal forma que se establezcan directrices con base en buenas prácticas, que favorezcan el adecuado uso y manejo de la información en todos los niveles de la organización: estratégico, táctico y operacional.

- Acuerdos: buscan la integración del área de seguridad de la información (Procesos de SI) con la Alta Gerencia (expectativas del negocio), con el fin de alinear los esfuerzos estratégicos, tácticos y operacionales del negocio, teniendo en cuenta:

    - El establecimiento de prioridades con la Alta Gerencia: con base en el análisis de riesgos, priorizar los procesos críticos que necesitan atención inmediata e inversión, además del nivel del riesgo aceptado por el negocio.

    - Las competencias y habilidades requeridas en el área de seguridad informática: de acuerdo a las necesidades del negocio, establecer los conocimientos mínimos del personal que se dedicará a la atención y el tratamiento de las prioridades definidas por la Alta Gerencia.

    - El establecimiento y materialización del nivel de compromiso entre Alta Gerencia y el área de seguridad informática: esta recomendación está enfocada en la definición de tareas conjuntas entre la Alta Gerencia y el área de seguridad de informática, de tal forma que se haga el mayor esfuerzo para cumplir con los compromisos organizacionales y de seguridad. Si la Alta Gerencia se compromete a invertir en el área de seguridad de la información, ésta debería maximizar los recursos y cumplir con la ejecución presupuestal de acuerdo a las proyecciones realizadas según el nivel de prioridad. Por otro lado, que cada proyecto ejecutado y sus implementaciones se encuentren alineados con el negocio, de tal manera que trascienda a cada uno de los actores en la organización.

    - La definición y operacionalización de los acuerdos de nivel de servicio: definir los roles y las responsabilidades de cada uno de los usuarios con respecto a los requerimientos de seguridad del negocio.

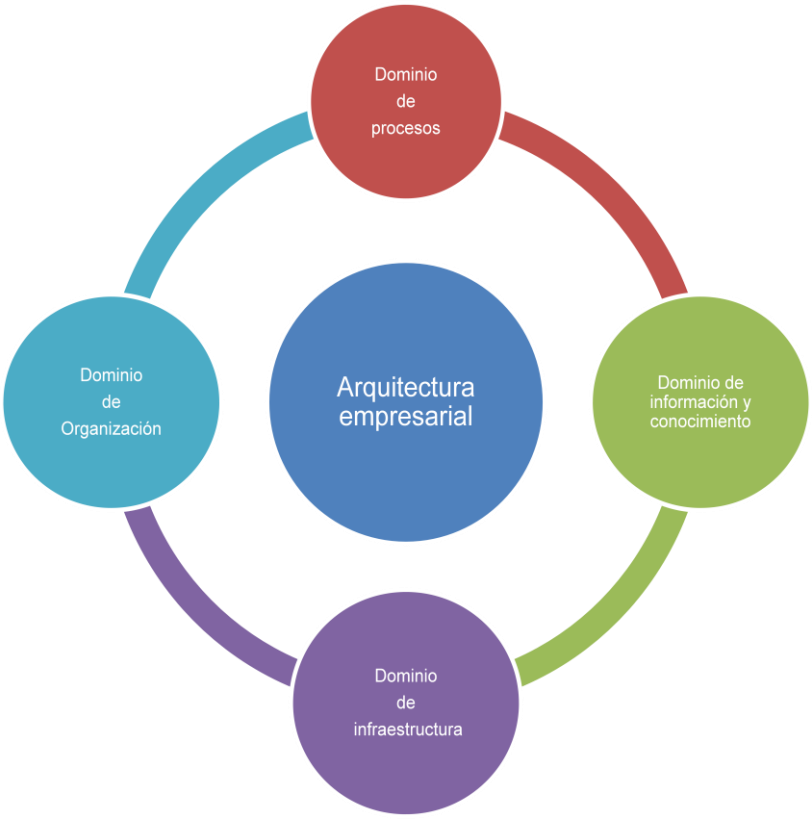
    - Los niveles de inversión en infraestructura de Seguridad Informática: incluir dentro de la programación presupuestal un rubro destinado a la inversión de la Alta Gerencia para sus compromisos en el tema de SI.

    - Compartir y alinear la agenda interna de la Alta Gerencia con la agenda interna del área de SI: considerar el incluir el tema de la SI dentro de las distintas reuniones que realiza la Alta Gerencia, de esta forma se mantiene al tanto del trabajo desarrollado en el Área de SI, verificando así el cumplimiento de la agenda de seguridad.

4.2.3 Arquitectura Empresarial

Las organizaciones se encuentran en continuo crecimiento, lo que trae consigo problemas en su capacidad para resolver los problemas que se van presentando; por esta razón, se considera la posibilidad de dividir la organización en áreas y se establece un elemento integrador que proporcione las herramientas para la interacción entre las diversas áreas. Como respuesta a ello surge la Arquitectura Empresarial (ver Figura 3), la cual integra los procesos de negocio, información (bases de datos, base de conocimiento), el conocimiento y los elementos relacionados con la infraestructura tecnológica de la organización [4].

Figura 3. Modelo de Arquitectura Empresarial.



Fuente: Basado en [4]

- Dominio de procesos

Dentro de este dominio se incluyen los procedimientos, las herramientas y las reglas que apoyan la ejecución de las actividades en la organización.

- Dominio de información y conocimiento

Este dominio incluye todo tipo de datos e información que tenga la organización tanto digital como física (documentos impresos).

- Dominio de infraestructura

Este dominio incluye las plataformas tecnológicas (hardware, los servicios, software) y de comunicaciones (redes y conectividad) de la organización, los cuales sirven de apoyo para la ejecución de las actividades de los otros dominios.

- Dominio de organización

Este dominio incluye los roles y responsabilidades del personal de la organización, así como las relaciones con clientes, proveedores y demás involucrados con la organización.

4.2.4 COBIT (Control OBjectives for Information and related Technology)

COBIT es un marco de referencia aceptado internacionalmente que ha sido desarrollado para la aplicación de buenas prácticas en la administración de los procesos que hacen parte del área TI. COBIT permite alinear las metas de negocio con las metas de TI, brindando métricas y modelos de madurez para medir los logros, e identificando las responsabilidades asociadas a los encargados de los procesos de negocio y de TI [5].

Los treinta y cuatro (34) procesos de TI de COBIT se encuentran organizados en los siguientes cuatro dominios:

- **Planear y Organizar (PO):**

Este dominio apoya la identificación de los elementos que van a permitir que TI contribuya con el logro de las metas de la organización, para lo cual se plantean los siguientes cuestionamientos:

• ¿Las estrategias de TI se encuentran alineadas con las de la organización?
• ¿La empresa esta optimizando el uso de los recursos?
• ¿Los colaboradores de la organización entienden los objetivos de TI?
• ¿Se entienden y administran los riesgos de TI?
• ¿La calidad de los sistemas de TI es apropiada para las necesidades del negocio?

- **Adquirir e implementar (AI)**

Mediante la aplicación de este dominio se identifican, desarrollan o adquieren los servicios de TI requeridos por la organización; además se provee el soporte o mejoramiento de los servicios ya existentes.

- **Entregar y dar soporte (DS)**

Este dominio cubre la entrega por parte de TI de los servicios requeridos y la continuidad de los mismos, así como la administración de la seguridad de la información (integridad, disponibilidad y confidencialidad). Este dominio satisface los siguientes cuestionamientos:

• ¿Los servicios se están entregando de acuerdo con las prioridades del negocio?
• ¿Los costos de TI se están optimizando?
• ¿La fuerza de trabajo es capaz de utilizar los sistemas de información de manera productiva y segura?
• ¿Están implantadas de forma adecuada la confidencialidad, integridad y disponibilidad en los servicios de TI?

- **Monitorear y evaluar (ME)**

Los procesos de TI deben cumplir con los objetivos propuestos, para ello se establece que estos serán evaluados de forma regular. Este dominio tiene en cuenta la administración del desempeño, la monitorización del control interno, el cumplimiento regulatorio y la aplicación del gobierno de TI.

4.2.5 NTC-ISO/IEC 27001:2006

Esta norma adopta el modelo de procesos *Deming* “Planificar-Hacer-Verificar-Actuar” para establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar el Sistema de Gestión de Seguridad de la Información (SGSI) en las compañías. ISO 27001 puede ser empleada en cualquier tipo de organización independiente de las características de la misma.

Se debe tener en cuenta que los numerales 4, 5, 6,7 y 8 de la norma ISO 27001 son requisitos no excluibles cuando una organización declara conformidad con la norma. Las exclusiones permitidas están enmarcadas en los controles descritos en el anexo A de la norma, sin embargo, estas deberán ser justificadas [6].

4.2.6 NTC-ISO/IEC 27002:2007

Esta norma está compuesta por 11 dominios los cuales contienen los objetivos de control y los controles; en total consta de 133 controles que pueden ser empleados para la mitigación de los riesgos identificados [2].

Dominios descritos en la norma:

- Política de seguridad de la información
- Organización de seguridad de la información
- Gestión de activos
- Seguridad de los recursos humanos
- Seguridad física y del entorno
- Gestión de operaciones y comunicaciones
- Control de acceso
- Adquisición, desarrollo y mantenimiento de sistemas de información.
- Gestión de los incidentes de seguridad de la información
- Gestión de la continuidad del negocio
- Cumplimiento

4.2.7 Arquitectura de seguridad de sistemas de información por el *SANS Institute*

SANS Institute, institución con buen prestigio a nivel mundial en el área de seguridad de la información, definió el documento denominado "*Information Systems Security Architecture: A Novel Approach to Layered Protection*", desarrollado por George Farah, experto en el tema de seguridad. Este documento explica cómo se desarrolla una arquitectura de seguridad de la información en un entorno complejo donde existen pocas medidas de seguridad. La propuesta define que para la definición de la arquitectura se deben tener en cuenta cinco fases (ver Figura 4):

- **Fase 1:** Realización de evaluaciones de la seguridad. En esta fase se pretende encontrar las vulnerabilidades inherentes a los datos, las aplicaciones y la infraestructura del sistema de información, al igual que los controles que se hayan aplicado. Para realizar ésta fase se recomienda:

    1. Realizar entrevistas con los responsables de los procesos para obtener información de la operación de los mismos.

    2. Definir el inventario de activos críticos y no críticos (*firewalls*, *IDS*, *proxy*, aplicaciones, bases de datos, entre otros).

3. Diseñar un modelo para las evaluaciones de seguridad de todos los componentes identificados, basado en un análisis del impacto empresarial (BIA) que permita determinar los controles adecuados tanto técnicos como administrativos que se aplicarán sobre los activos.

4. Identificación de amenazas, vulnerabilidades y problemas de seguridad en el inventario de activos.

5. Realización del análisis de riesgos de seguridad.

Figura 4. Fases del Modelo de Arquitectura de seguridad de sistemas de información por el *SANS Institute*

Fuente: Basado en [7]

- **Fase 2:** Formulación del Diseño de los Objetivos de la Arquitectura de Seguridad. La definición de los objetivos de la arquitectura se hace necesaria debido a que esto establece todos los elementos que van hacer parte de la misma; para ello se toma como referencia los resultados y recomendaciones de la fase 1, las cuales pueden ser usadas para realizar cambios sobre la

infraestructura de TI, las políticas, o definir nuevos controles de seguridad. Existen dos diseños a tener en cuenta en la arquitectura de seguridad.

1. El diseño de la arquitectura lógica de los componentes de TI: debe incorporar procesos, tecnología y usuarios; ésta debe definir además un perímetro de seguridad, un equipo de respuesta a incidentes, la política de antivirus, administración de seguridad, un Plan de Recuperación de Desastres (DRP), el análisis de riesgos, la seguridad de los datos, la seguridad de las aplicaciones, y la seguridad de la infraestructura.

2. El diseño de la arquitectura física: incluye el diagrama de la red ilustrando todos los dispositivos existentes, entre ellos: *firewalls*, *mail gateways*, servidores *proxy*, *modem pools*, VLAN, *DeMiliterized Zone* (DMZ), las conexiones internas y externas, además se recomienda identificar las direcciones IP de los dispositivos.

Fase 3: Construcción de Políticas y Procedimientos. George Farah recomienda que con el cumplimiento la fase 1 y 2 se puede dar inicio a la fase 3. En esta fase el autor establece la definición de las políticas y procedimientos teniendo en cuenta: la definición de una política corporativa, la definición de políticas departamentales y la definición de políticas específicas, todas estas relacionan lo que tiene que ser protegido y todos los sistemas de información que conforman la arquitectura de seguridad.

En [7] King, Dalton, y Osmanoglu definen como principio fundamental de las políticas de seguridad el "equilibrio entre la seguridad y la capacidad de hacer negocios", es decir, que el hecho de realizar esfuerzos en la creación de políticas de seguridad no debe entorpecer el negocio, por el contrario la seguridad debe ser un facilitador en la ejecución de los procesos de negocio.

- **Fase 4:** Implementación del Diseño de los Objetivos de la Arquitectura de Seguridad. Esta fase se lleva a cabo una vez se cumplan las fases 1, 2 y 3 en las cuales se desarrollan los estudios previos para la implementación de la arquitectura, teniendo en cuenta los plazos, la financiación y los recursos necesarios.

- **Fase 5:** Integración de las prácticas de seguridad para mantener el estado de seguridad. En esta fase se deben definir los roles y asignar las responsabilidades respecto a: la evaluación de los cambios en el diseño de los sistemas de información y la actualización de la estructura de la red, logrando mantener las medidas de seguridad día a día. Se definen dos procesos dentro de ésta fase:

1. La Gestión del cambio de los diferentes elementos o dispositivos que conforman la arquitectura.

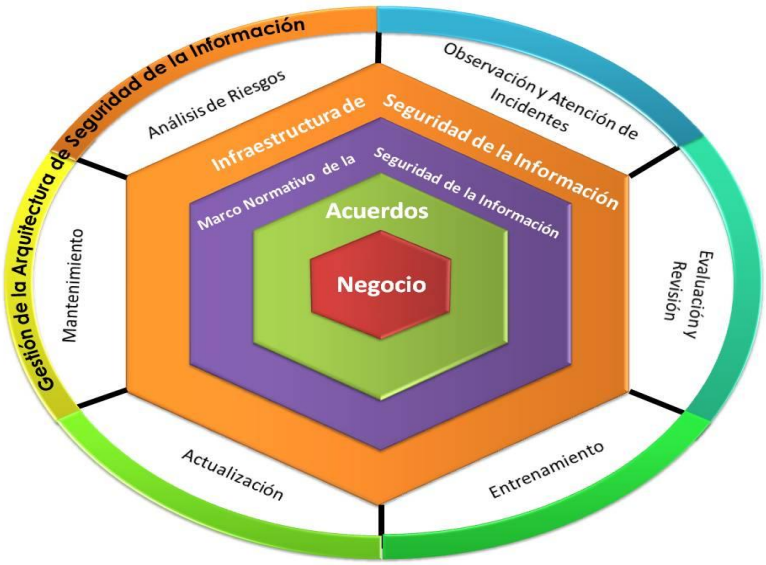
2. El desarrollo de una metodología que paute las directrices en la gestión de proyectos de tecnología, de tal manera que sea clara la definición de los requisitos y etapas en la ejecución de proyectos que realimenten el estado de la arquitectura y su actualización. El Arquitecto de Seguridad es el responsable de esta actividad.

5 ELEMENTOS DEL MODELO DE ARQUITECTURA DE SEGURIDAD DE LA INFORMACIÓN – MASI –

Para definir los elementos que conforman MASI se tomará como referencia el proyecto de grado: “Diseño de la Arquitectura de Seguridad de la red de la Universidad Pontificia Bolivariana seccional Bucaramanga” [8], donde se plantea una Arquitectura de Seguridad de la Información (ASI) conformada por cinco elementos: Acuerdos, Negocio, Políticas de Seguridad, Gestión de Seguridad e Infraestructura de Seguridad, los cuales dentro de dicho proyecto se definen pero no se especifica una metodología para su implantación, además de los modelos de ASI referenciados en el capitulo anterior.

Para puntualizar MASI (ver Figura 5) está constituido por cinco elementos: Negocio (lo que el negocio saber hacer[3]), Marco Normativo de Seguridad de la Información (pautas, reglas, lineamientos para los actores), Gestión de la Arquitectura de Seguridad de la Información (mejora continua), Acuerdos (alineación entre seguridad de la información y expectativas de la Alta Gerencia), Infraestructura de Seguridad de la Información (seguridad informática).

Figura 5 Elementos del MASI - Modelo de Arquitectura de Seguridad de la Información



[3] *Know How*

MASI incorpora un ciclo de mejora continua el cual permite que la Arquitectura de Seguridad de la Información (ASI) se encuentre adaptada a los cambios de la organización

5.1 DESCRIPCIÓN DE LOS ELEMENTOS DEL MASI

5.1.1 NEGOCIO

Este elemento está enmarcado en el conocimiento de los aspectos estratégicos de la organización, en evaluar cada uno de los componentes inmersos en el desarrollo de la misma. Con el conocimiento del negocio se pueden identificar sus necesidades en cuanto a SI, de tal manera que se logre suplir las mismas a través de la ASI.

A través del conocimiento del negocio se podrá establecer el tipo de organización y el cuadro de mando de la misma, lo cual facilitará la definición de estrategias de comunicación con la Alta Gerencia.

Para la obtención de este conocimiento MASI plantea el reconocimiento y estudio de los siguientes documentos, y de no existir se propone su formalización:

a. **Misión de la organización**: el entendimiento de la misión permitirá establecer la razón de ser de la organización [9].

b. **Visión de la organización**: brinda información relacionada con los planes futuros de la misma, es decir, proyección del negocio que tiene la Alta Gerencia en un tiempo determinado [9].

c. **Metas de la organización:** la evaluación de la metas de la organización permite conocer las expectativas del negocio.

d. ***Balanced Scorecard (BSC)*** **(Cuadro de Mando Integral):** es un sistema de planeación y gestión estratégica empleado por las organizaciones para alinear todas las actividades que desarrolla con la visión y estrategia de la misma, así mismo sugiere que las organizaciones sean analizadas desde cuatro perspectivas: financiera (rentabilidad del negocio), del cliente (cómo lograr su satisfacción), interna (lograr la competitividad del personal) y de innovación y aprendizaje (cómo lograr ser competitivos en el mercado). El BSC no sólo proporciona mediciones de rentabilidad económica sino de todos los ámbitos del negocio que finalmente repercuten en el desempeño de la organización.

e. **Plan de desarrollo**: herramienta que permite gestionar las directrices, pautas o acciones que ayudan a cumplir los objetivos, la misión y la visión del negocio mediante la definición de indicadores del cumplimiento de las metas trazadas [10].

Además de los aspectos descritos anteriormente, se debe revisar todo tipo de información disponible en la organización que conlleve a entender la operación de la misma, como por ejemplo la estructura organizacional, el mapa de procesos, entre otros.

El conocimiento y entendimiento de la definición del negocio es el punto de partida para alinear la Arquitectura de Seguridad de la Información con las estrategias del negocio.

5.1.2 Marco Normativo

El marco normativo (Ver Figura 6) es el elemento que establece los lineamientos de comportamiento y responsabilidades de los actores respecto a la protección de la información. Éste involucra la política, directrices, normas y procedimientos, además de la normativa corporativa que pueda apoyar el cumplimiento de los requerimientos de seguridad por parte de los actores como lo es el código de ética, reglamento interno de trabajo, normativa antifraude, reglamento disciplinario, entre otros.

Figura 6. Marco Normativo

Normativa de seguridad de la información

La normativa de seguridad de la información se define teniendo en cuenta las tres perspectivas en el negocio (ver Figura 7): los lineamientos generales con respecto

a la SI (nivel estratégico), la instrumentalización de los lineamientos generales, definidos mediante estándares y normas de SI (nivel táctico) y la definición de los procedimientos que detallan los pasos a seguir para el cumplimiento de las normas de SI (nivel operacional).

Figura 7. Normativa de seguridad de la información.

- Política de Seguridad de la Información

La política de seguridad de la información es la declaración de la importancia de la información en la organizaciones, de tal manera que refleje las intenciones de la Alta Gerencia por cumplir con los objetivos de seguridad del negocio, de acuerdo a su misión y visión e incorporando además la legislación vigente en materia de seguridad aplicable al negocio. La política de SI define las pautas en el comportamiento de los actores respecto a la protección de uno de los activos importantes dentro de la organización, la información. Se recomienda redactar la política de SI y sus directrices con un lenguaje apropiado que permita el fácil entendimiento a los usuarios.

- Directrices de seguridad de la información

Las directrices de seguridad de la información detallan los lineamientos estratégicos de la política de seguridad de la información.

- Normas de seguridad de la información.

Teniendo en cuenta que la política y las directrices de SI son un marco estratégico para cumplir con los objetivos del negocio, existe la necesidad de clarificar qué se busca proteger (activos, procesos, personas, entre otros) y el nivel de protección que se quiere brindar, especificando de forma general los ítems o requisitos necesarios para dar cumplimiento a la política desde un punto de vista táctico, en este sentido las normas establecen la instrumentalización de los lineamientos definidos en la política y las directrices de seguridad de la información [11] [12] [13].

- Procedimientos de seguridad de la información

Los procedimientos contienen el marco operativo y se encuentran encaminados en el cumplimiento de las normas de SI, por tal razón, en éstos se detallan cada una de las actividades basadas en buenas prácticas que deben ser desarrolladas por los actores. También en los procedimientos se especifican las tareas que determinan el cómo deben ser ejecutadas la actividades y los responsables de su ejecución [11] [12] [13].

Normativa corporativa

- Código de ética

Dentro del código de ética se encuentran documentados los principales valores y lineamientos éticos que la organización espera sean atendidos e interiorizados por todos los actores del negocio, esto evita que su actuar este únicamente encaminado hacia el concepto de lo que es correcto o incorrecto desde su perspectiva personal. Si bien el código de ética no garantiza que los empleados tengan un comportamiento adecuado, si provee elementos que apoyan la toma de decisiones en el ámbito del comportamiento humano y en su accionar en la organización [14] [15].

- Reglamento interno de trabajo

El reglamento interno de trabajo contiene las disposiciones que deben ser acatadas por los empleados y el empleador, para actuar de conformidad a las expectativas del negocio [16]. En el Código Sustantivo del Trabajo[4] se encuentran definidas las regulaciones del reglamento interno de trabajo en Colombia.

[4] "*La finalidad primordial de este código es la de lograr la justicia en las relaciones que surgen entre empleadores y trabajadores, dentro de un espíritu de coordinación económica y equilibrio social*." Tomado de Código Sustantivo del Trabajo.

- Normativa Antifraude

El fraude es toda acción negligente que va en contra de lo establecido en el código de ética. La motivación del autor del hecho identificado como fraude es obtener una ganancia, la cual en la mayoría de las veces es dinero, basando su accionar en el manejo de intereses particulares, engaños, sabotajes, chantajes, entre otras conductas. La normativa antifraude es aquella que permite llevar a cabo procesos contra los individuos cuyo comportamiento va en contravía del código de ética organizacional, amparado en el reglamento interno y a la legislación vigente que corresponda [17].

5.1.3 Gestión de la Arquitectura de Seguridad

La gestión contiene los elementos necesarios para el mantenimiento, la administración y continuo crecimiento de la Arquitectura de Seguridad de la Información. Los elementos que componen la Gestión de la ASI se encuentran en la Figura 8 [8]:

Figura 8**. Gestión de la Arquitectura de Seguridad.**

- Análisis de Riesgos

Los activos de las organizaciones se ven expuestos a amenazas debido a la variedad de usuarios que interactúan en estos, por lo tanto se debe realizar el análisis de riesgos que permita medir los riesgos en los que se ven expuestos los activos ante la existencia de amenazas y vulnerabilidades inherentes a los mismos, al igual que el impacto que tendrían al materializarse.

Para el desarrollo del Análisis de Riesgos existen diversas metodologías como MAGERIT, OCTAVE, AS/NZS 4360:2004, ISO 27005 entre otras, las cuales pueden ser adaptadas de acuerdo a las necesidades del negocio.

- Observación y Atención de incidentes

La gestión de incidentes permite identificar los eventos que pueden llegar a afectar los activos de información o los eventos que los han afectado, de tal manera que se logre reducir los impactos de la materialización de las amenazas, y a su vez establecer medidas para reducir su probabilidad de ocurrencia. Los resultados de la atención de incidentes pueden ser utilizados como insumos para las actividades de revisión y evaluación, actualización y mantenimiento.

- Revisión y Evaluación

La revisión y evaluación de la ASI permite verificar si ésta contribuye o no a la incorporación de la seguridad en los procesos de negocio. Para ello se toma como insumo los resultados del análisis de riesgos, además de los incidentes reportados. Teniendo en cuenta que la SI es un proceso dinámico, la revisión y evaluación permite identificar factores que puedan ocasionar problemas y por ende realizar las respectivas acciones para su corrección. Dentro de los aspectos a evaluar y revisar se tiene:

  - Los elementos de la Arquitectura de Seguridad de la Información
  - Los actores del negocio
  - La infraestructura tecnológica (revisión técnica)

Para las evaluaciones al recurso humano (los actores) se podrá emplear una encuesta de conocimiento en SI además de estrategias de observación que permitan identificar su comportamiento. Para evaluar la infraestructura se realizan pruebas de vulnerabilidades. La evaluación de los elementos de la ASI se logra mediante la revisión y verificación continua de cada elemento y sus interacciones.

Para definir la periodicidad del proceso de revisión y evaluación en las organizaciones se debe considerar la regulación aplicable al negocio, los ciclos de auditoría establecidos, entre otros factores que pueden influir; MASI propone sea:

- Cada seis meses para el recurso humano y la infraestructura tecnológica
- Cada año para los elementos de la ASI

- Entrenamiento

La ASI requiere que los actores que interactúan en la organización estén en capacidad de comprender los cambios que se generen en el desarrollo de las actividades y procesos tras la incorporación de la SI, y su compromiso frente al cumplimiento de los objetivos de SI. Para lograr este compromiso se requiere de la gestión de recursos que permitan el entrenamiento de los usuarios.

- Actualización

Para lograr la actualización de los elementos del modelo se requiere del análisis de los resultados obtenidos en el proceso de revisión y evaluación, los cuales permiten identificar las oportunidades de mejora a nivel de: los elementos de la ASI, las vulnerabilidades que deben ser actualizadas en el análisis de riesgos con sus respectivas salvaguardas, nuevos activos que deben ser protegidos y recurso humano que requiere ser capacitado. Es conveniente realizar un proceso continuo de actualización que realimente el funcionamiento de la ASI de tal forma que ésta crezca y se renueve a la par del desarrollo organizacional.

- Mantenimiento

Este elemento en la Gestión de la ASI define la implementación de las actualizaciones aprobadas en cualquier nivel de la ASI, con el fin garantizar su adaptación a los procesos del negocio. El mantenimiento permite aumentar la vida útil y la disponibilidad de los elementos que conforman la ASI y una mejora continua del modelo. Esta actividad tiene en cuenta que día a día cambian los requerimientos del negocio, aparecen nuevas amenazas y se generan nuevos procesos de mejora ante las amenazas existentes.

5.1.4 Acuerdos

La concepción de la ASI establece la necesidad de buscar el canal de comunicación que garantice la integración del área de seguridad de la información (procesos de seguridad) y la Alta Gerencia (expectativas del negocio), a fin de alinear los esfuerzos estratégicos, tácticos y operacionales del negocio. Tomando

como referencia el modelo de ASI definido por Jeimy Cano, los ***Acuerdos*** brindarán apoyo a las necesidades de inversión, para llevar a cabo los proyectos en el contexto de la implementación, administración y mantenimiento de la ASI.

De acuerdo a lo definido por Jeimy Cano, se propone tener en cuenta en el elemento Acuerdos:

- El establecimiento de prioridades con la Alta Gerencia
- La definición de las competencias y habilidades requeridas en el Área de Seguridad Informática
- El establecimiento y la materialización del nivel de compromiso entre la Alta Gerencia y el Área de Seguridad
- La definición y operacionalización de los acuerdos de nivel de servicio
- Los niveles de inversión en infraestructura de seguridad informática
- El compartir y alinear la agenda interna de la Alta Gerencia, con la agenda interna del Área de seguridad de la información

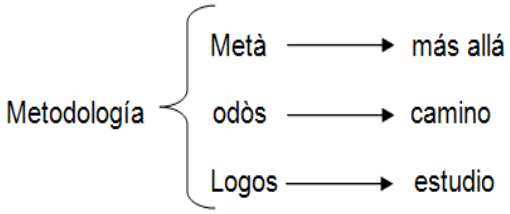
5.1.5 Infraestructura de seguridad de la información

Está compuesta por los elementos como: *firewalls*, *VNP, IDS, IPS,* entre otros, requeridos por la organización para la mitigación de los riesgos relacionados con la seguridad lógica de la información (confidencialidad, integridad y disponibilidad), es decir, de toda aquella información que se encuentra almacenada en un dispositivo electrónico como: servidores, computadores, dispositivos móviles, entre otros [18].

6 METODOLOGÍA DEL MODELO DE ARQUITECTURA DE SEGURIDAD DE LA INFORMACIÓN

Antes de iniciar con la estructuración de las actividades a desarrollar para la implementación del modelo, se definirá el concepto de metodología el cual contextualizará el desarrollo de esta etapa del proyecto.

Etimológicamente el concepto de metodología tiene sus raíces en tres vocablos griegos los cuales serán descritos a continuación:



Se puede definir la metodología como una serie de pasos ordenados que van a permitir seguir un camino para lograr determinado fin [19].

6.1 MÉTODO DEL MODELO DE ARQUITECTURA DE SEGURIDAD DE LA INFORMACIÓN

Los elementos del MASI pueden ser ejecutados en el siguiente orden.

- Conocer el Negocio: la ejecución de las actividades dispuestas en este elemento del MASI, permitirán obtener el conocimiento detallado de las expectativas del negocio respecto a la SI, además de interiorizar los objetivos del negocio y establecer la forma como la arquitectura apoyará el cumplimiento de los mismos.

- Definir el Marco Normativo de SI: la elaboración del Marco Normativo permite plasmar en documentos las expectativas de la Alta Gerencia, así como los compromisos que deberán ser adquiridos por los actores para dar cumplimiento a éstas. El cumplimiento de las medidas dispuestas para salvaguardar la información de la compañía por parte de los actores

- establece un punto crucial para el buen funcionamiento y regulación del MASI.

- Gestión de la Arquitectura: la gestión del MASI permite identificar las oportunidades de mejora de la ASI, es decir, evaluar si la ASI está alineada con los elementos del MASI, los actores y los procesos de negocio, de tal manera que se realicen correcciones asertivas que conlleven al mejoramiento de la ASI mediante un ciclo de mejora continua.

- Definir los acuerdos: conlleva a establecer las estrategias de comunicación entre el Área de seguridad de la información y la Alta Gerencia.

- Establecer la Infraestructura de Seguridad: las medidas de protección existentes en las tecnologías de la información implantadas en los diferentes sistemas de información de la organización, permitiendo mitigar los riesgos relacionados con la confidencialidad, integridad y disponibilidad de la información.

6.2 DEFINICIÓN DE LA METODOLOGÍA PARA LA IMPLEMENTACIÓN DE LA ARQUITECTURA DE SEGURIDAD

Para la estructuración de la metodología del MASI se definirá por cada elemento un diagrama de flujo que permitirá organizar las actividades a desarrollar en cada etapa de la implementación de la ASI. La explicación de cada actividad, el flujo de los procesos y de la información se representa en el procedimiento de ejecución de cada elemento del MASI.

6.3 MASI VS. SGSI

MASI es un modelo para la administración de la seguridad entendiéndose como un proceso para la planificación, organización, dirección y control en la formalización de la seguridad de la información. El SGSI (Sistema de Gestión de la Seguridad de la Información) se entiende como un sistema global para establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información con enfoques similares pero teniendo en cuenta que MASI se realiza especial énfasis en la alineación de las estrategias de seguridad con el negocio y especifica dentro de procedimientos o propuestas la forma como el modelo puede ser empleado en las organizaciones. A continuación se realiza un contraste mediante el cual se identifican puntos en común entre MASI y SGSI.

Tabla 1. Comparativo entre SGSI y MASI

SGSI	MASI
Precisa un proceso para definir la política de seguridad.	Dentro del Marco Normativo se encuentra el marco de seguridad en el cual se define la política de seguridad de la información.
SGSI define un proceso para la identificación, valoración y tratamiento de los riesgos.	Dentro del elemento Gestión de la Arquitectura de Seguridad de la Información establece un proceso de análisis de riesgos en el cual se realiza un inventario de activos, definición de amenazas y vulnerabilidades, valoración del riesgo intrínseco y efectivo o residual, definición de controles y el mapa de riesgos.
Define un proceso para el seguimiento y revisión de controles.	Dentro del elemento de Gestión de la ASI, declara un proceso para evaluar y revisar la relación de los elementos del MASI y de los elementos del negocio.
Define un proceso de mantenimiento y mejora.	Dentro de la Gestión de la ASI, define un proceso de Actualización y Mantenimiento, los cuales permiten corregir y mejorar los elementos, procesos, actividades y tareas del MASI.
Define un proceso de documentación.	Existen anexos que permiten la documentación y registro de las actividades inmersas, en los elementos y los procesos que lo conforman.
Define un proceso que declara el compromiso, la responsabilidad y revisión por parte de la Dirección.	Define el elemento Acuerdos con el cual declara a la Alta Gerencia como un actor comprometido y responsable en la definición, formalización y dirección de la SI.
Define la Gestión de Recursos (aprobación de recursos, formación, toma de conciencia y competencia).	Los Acuerdos definen las prioridades e inversión y en la Gestión de la ASI define la actividad de entrenamiento encargada de la concienciación.
Define Auditorías Internas.	Dentro del elemento de Gestión de la ASI define un proceso de Revisión y Evaluación el cual es una aproximación a las Auditorías Internas planteadas por el SGSI.
Plantea la revisión del SGSI por parte de la Dirección.	Todos los elementos tienen asociado el acompañamiento formal de la Alta Gerencia, pues el diseño de un proceso es definido, revisado, modificado (de ser necesario) y aprobado en consenso con el Arquitecto de Seguridad de la Información.
Plantea un proceso de mejora del SGSI (mejora continua, acciones correctivas, acciones preventivas).	El elemento de Gestión de la ASI define todos los procesos necesarios (análisis de riesgo, entrenamiento, observación y atención de incidente, revisión y evaluación, actualización y mantenimiento) que permiten la mejora continua de la ASI alineado con el contexto de negocio.

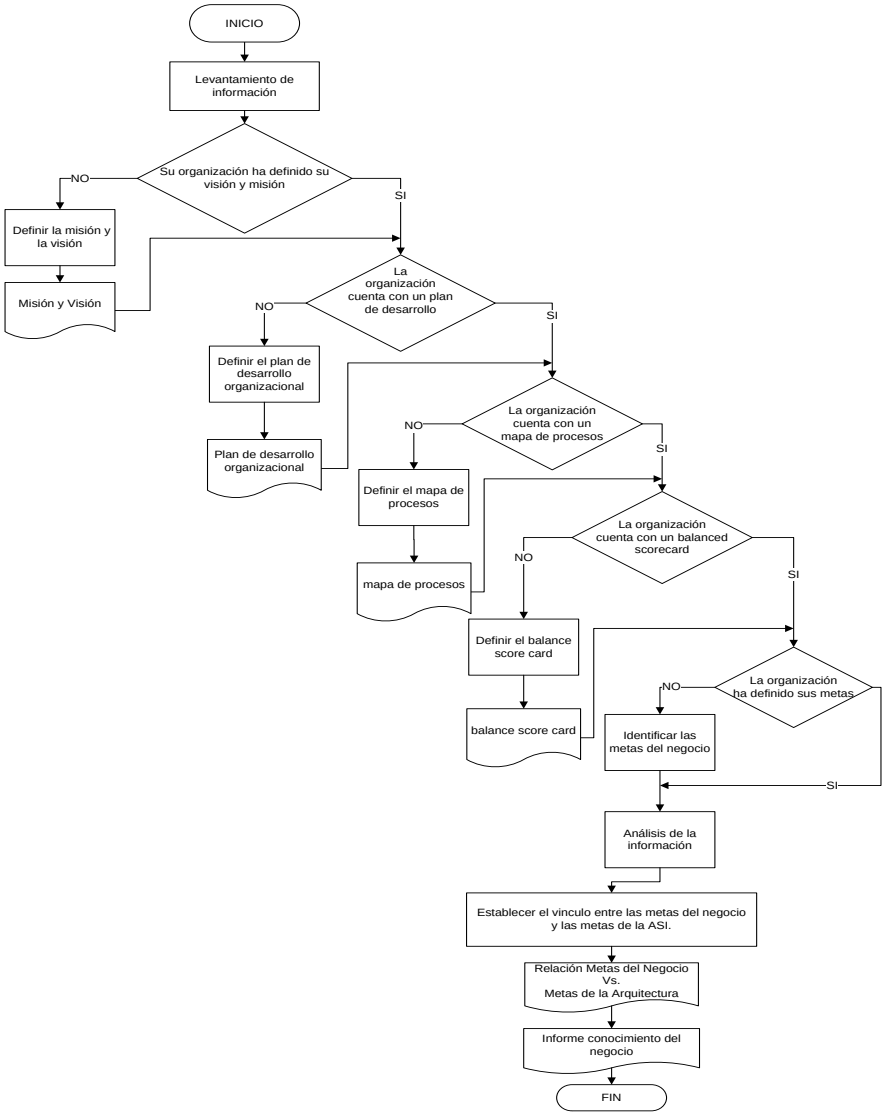
En conclusión, MASI, aunque formalmente no declara la implementación de un SGSI, tiene intrínsecamente inmersos procesos asociados con el SGSI.

6.4 NEGOCIO

6.4.1 Diagrama de flujo

A continuación se presenta el diagrama de flujo (ver Figura 9) representa el proceso para la formalización del elemento Negocio dentro del MASI, en el cual se hace hincapié que ante la no existencia de un documento se propone la formalización del mismo y seguido a ello se explicara el procedimiento detallado.

Figura 9. Diagrama de Flujo de Negocio



Procedimiento

- Levantamiento de información: recolectar toda la información requerida tomando como base el numeral 5.1.1 y el formato levantamiento de información del negocio (ver Anexo A).

    - Análisis de la Información: el análisis es la etapa mediante la cual el Arquitecto de SI interioriza cada uno de los documentos referenciados y entiende las expectativas del negocio.

    - Para lograr el entendimiento requerido se recomienda que se realicen reuniones con la Alta Gerencia y con las áreas encargadas de la definición de los planes estratégicos.

- Definición de documentos que identifican el negocio: en caso que la organización no cuente con alguno de los documentos o información referenciada en el formato de levantamiento de información del negocio, la Alta Gerencia deberá realizar las reuniones respectivas de tal forma que estos elementos sean estructurados, y así se puedan identificar los requerimientos de SI del negocio y estos puedan ser resueltos mediante la implementación de la Arquitectura de Seguridad de la Información.

- Relación de las metas del negocio con las metas de la arquitectura: la revisión periódica de la ASI permite establecer qué factores en los elementos de la misma deberán ser actualizados o mejorados con miras a optimizar el funcionamiento de la misma; de las revisiones desarrolladas pueden surgir cambios tanto a nivel normativo como de infraestructura que requieran nuevos acuerdos entre las partes, además los cambios en las organizaciones deben estar revisándose para que el conocimiento del negocio no se pierda con el tiempo. En la Tabla 1 se establece la relación entre las metas del negocio[5] y las metas de la ASI, las cuales están enfocadas en dar repuesta a los siguientes interrogantes:

    - ¿Cómo establecer el Marco Normativo de Seguridad de la Información en la organización?

    - ¿Qué elementos debe contener la Gestión de la ASI en la organización?

    - ¿Cómo se identifican los requerimientos técnicos de SI?

[5] Las metas de negocio definidas en la tabla 1 son un ejemplo, cada organización debe definir las metas de acuerdo a su negocio.

- ¿Cómo establecer un canal de comunicación en el cual converjan las expectativas seguridad y los procesos del negocio?

Para el análisis de la tabla 2 se debe tener en cuenta que las equis (X) representan los puntos en los cuales la arquitectura apoya el cumplimiento de las metas organizacionales.

Tabla 2 Relación Metas del Negocio Vs. Metas de la Arquitectura.

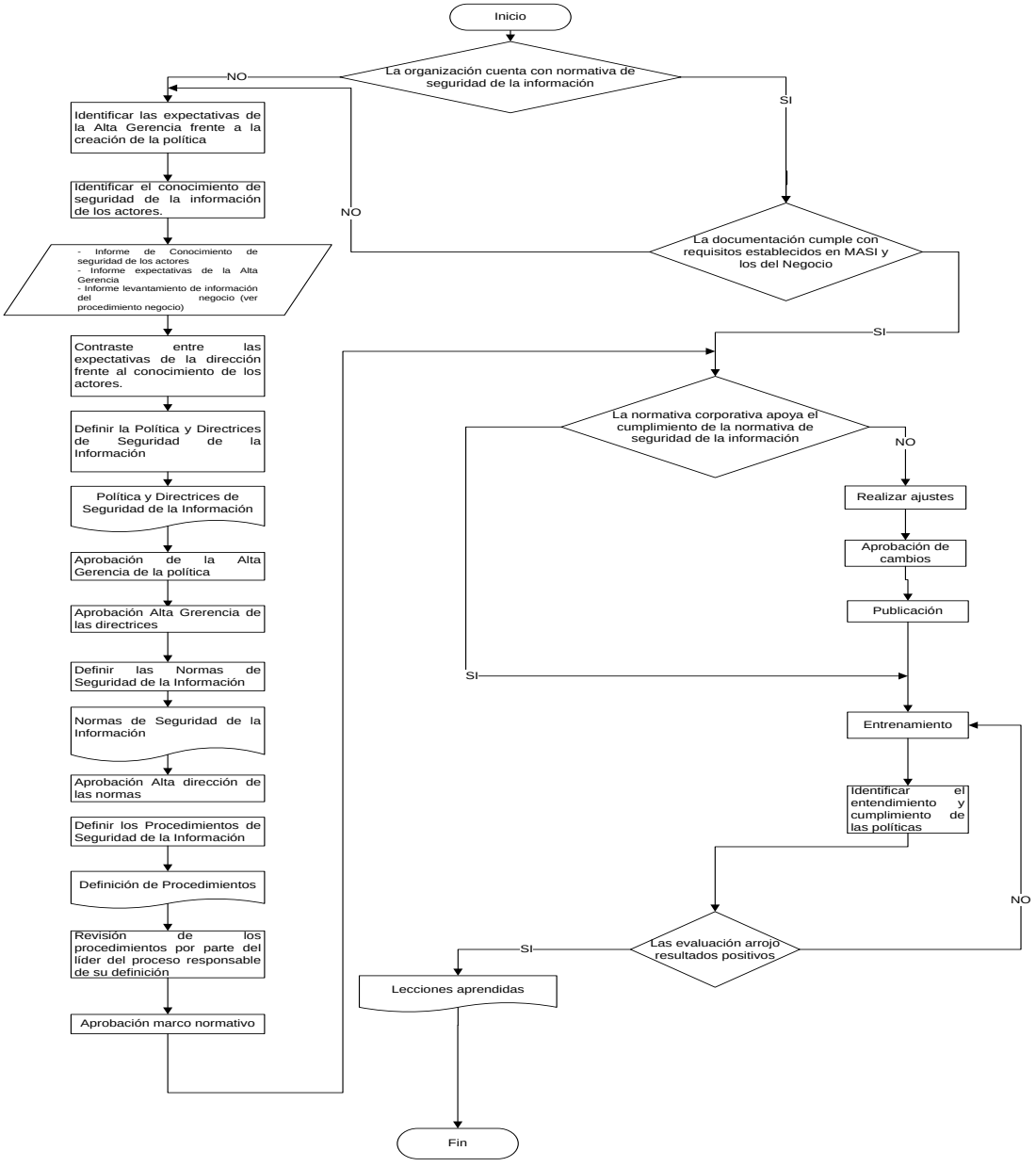
Metas de la Arquitectura / Metas del Negocio	Proveer los lineamientos para la organización de la seguridad en las empresas	Gestionar la arquitectura de seguridad de la información	Identificar e implementar los requerimientos técnicos de seguridad	Establecer el marco de comunicación entre el área de seguridad y la alta gerencia	Identificar y cumplir los requerimientos de seguridad del negocio
Proveer información oportuna a sus clientes	**X**	**X**			
Cumplimiento del margen de utilidad definido	**X**		**X**		**X**
Posicionamiento en el mercado	**X**	**X**			
Gestión de Recursos		**X**			
Competitividad		**X**			
Diferenciadores en el mercado	**X**	**X**	**X**	**X**	**X**
Entrega eficaz de productos o servicios	**X**	**X**	**X**	**X**	**X**
Mejorar los procesos del negocio	**X**	**X**	**X**	**X**	**X**
Contar con información veraz para la toma de decisiones	**X**	**X**		**X**	**X**
Cumplimiento de normatividad interna y requisitos de ley	**X**				
Comunicación entre los procesos de la compañía	**X**			**X**	**X**

6.5 MARCO NORMATIVO

6.5.1 Diagrama de flujo

La Figura 10 representa el flujo de actividades propuestas para el desarrollo del Marco Normativo, en este se puede observar la interacción entre la Normativa Organizacional y la Normativa de SI y cómo desde la primera se apoya el cumplimento de la normativa de seguridad.

Figura 10. Diagrama de Flujo Marco Normativo



6.5.2 Procedimiento[6]

Premisa: la Política de Seguridad de la información debe estar inmersa en un proceso de mejora continua.

- Reconocimiento de Normativa de Seguridad: en este punto se deberá analizar si el negocio cuenta con un marco normativo de seguridad de la información.

- Si el negocio cuenta con un marco normativo de seguridad de la información se deberá:

    - Convocar una reunión con el equipo de trabajo para la definición del marco normativo (TI, área de seguridad física, cultura, gestión humana), a fin de evaluar que la documentación existente cuenta con el nivel de detalle definido en MASI (política, directrices, normas y procedimientos), y si además, es suficiente para la organización.

    - Si se logra establecer que la normativa existente cumple con los requerimientos, se procederá a:

        - Realizar un entrenamiento a los actores sobre el marco normativo de seguridad usando el procedimiento de entrenamiento.

        - Identificar el entendimiento y cumplimiento del marco normativo, esto se desarrollará mediante una evaluación y visitas de campo; en caso que esta fase no arroje resultados positivos se realizará nuevamente las actividades de entrenamiento.

- Si el negocio no cuenta con normativa en cuanto a la SI, o esta no cumple con los requisitos, tanto del negocio, como del MASI se debe:

    - Identificar las expectativas de la Alta gerencia: para esto se deberá convocar una reunión con la Alta Gerencia para conocer las expectativas de la misma en cuanto a la normativa de seguridad de la información.

    - Identificar el conocimiento de seguridad de la información de los actores: para esto se recomienda desarrollar una encuesta que permita identificar prácticas de los actores respecto a la SI, ésta permitirá establecer que prácticas requieren ser replanteadas debido a que podrían ocasionar la materialización de riesgos sobre los activos de

[6] En el Anexo B se encuentra disponible un ejemplo que puede ser tomado como guía para la definición de la política, directrices, normas y procedimientos de seguridad de la información.

información, además de aquellos que puedan ser ejemplarizados y empleados en las estrategias de sensibilización.

- Contraste entre las expectativas de la Alta Gerencia y el conocimiento de los actores: Identificar el nivel de entendimiento de los actores frente a la seguridad de la información con relación a las expectativas del negocio, con el fin establecer qué elementos deberán ser reforzados.

- Luego se deberá convocar una reunión con el equipo de trabajo para la definición del Marco Normativo (TI, área de seguridad física, cultura, gestión humana), y así analizar la información obtenida en la reunión con la Alta Gerencia, las conclusiones que se tengan de la fase de entendimiento del negocio y la encuesta de conocimiento en seguridad de la información.

- Una vez se ha analizado toda la información, se procede a definir la Política de Seguridad de la Información, para ello se debe tener en cuenta que ésta debe contener al menos los siguientes ítems [2]:

  - Los objetivos de la Política de SI.

  - El alcance de la Política de SI.

  - Declaración por parte de la Alta Gerencia de la conformidad de la política con las estrategias y objetivos del negocio

  - Inclusión del marco de cumplimiento dentro de la política, esto encierra los requisitos legales del negocio, requisitos de educación, formación y toma de conciencia además de las consecuencias por las violaciones de la política y los mecanismos de verificación de su cumplimiento.

  - Desarrollo de las directrices, se debe tener en cuenta que las directrices de seguridad de la información son requisitos de seguridad de segundo nivel que estarán alineados con la política de seguridad y así facilite el cumplimiento de la política de seguridad; para ello se puede tomar como base los dominios de seguridad descritos en la norma ISO/IEC 27002, el análisis de la información de las entrevistas desarrolladas para conocer las expectativas del negocio y los resultados del estudio del negocio.

- Con el documento de la Política y las Directrices de Seguridad de la Información definido, el equipo de trabajo de definición de marco normativo deberá realizar una presentación a la Alta Gerencia, en aras de establecer si el documento cumple con la expectativas del negocio, si no cumple se deberá reunir nuevamente el equipo de trabajo, analizar las recomendaciones dadas por la Alta Gerencia y establecer las correcciones pertinentes. Luego de ello si

cumple con los requerimientos se deberá realizar la aprobación de la política y las directrices.

- Tomando como referencia el documento de la política de seguridad aprobado se procede a definir las normas y procedimientos asociados.

- Definición de normas de seguridad de la información: las normas establecen de manera general las actividades o elementos que apoyan el cumplimiento e implantación de las directrices de seguridad de la información. Las normas deberán ser avaladas por la Alta Gerencia.

- Definición del procedimiento de seguridad de la información: los procedimientos establecen el flujo de tareas que deberán ser ejecutadas para implantar una norma o grupo de normas en el negocio. Los procedimientos serán avalados por el líder del proceso responsable de su definición y los lideres de gestión documental al interior de las organizaciones

- Aprobación del Marco Normativo: Una vez definido los documentos que hacen parte del marco normativo se realiza la aprobación definitiva del mismo.

- Luego se procede a evaluar si la normativa corporativa apoya el cumplimiento de la normativa de seguridad.

- Si la normativa corporativa no apoya el cumplimiento de la normativa de seguridad, se procede realizar los cambios pertinentes; si por el contrario, la normativa corporativa apoya el cumplimiento de la normativa de seguridad, se proceden a publicar el marco normativo de seguridad y a desarrollar las siguientes actividades:

    - Realizar un entrenamiento a los actores sobre el marco normativo de seguridad usando el proceso de entrenamiento.

    - Identificar el entendimiento y cumplimiento del marco normativo, esto se desarrollará mediante una evaluación y visitas de campo; en caso que esta fase no arroje resultados positivos se realizará nuevamente las actividades de entrenamiento.

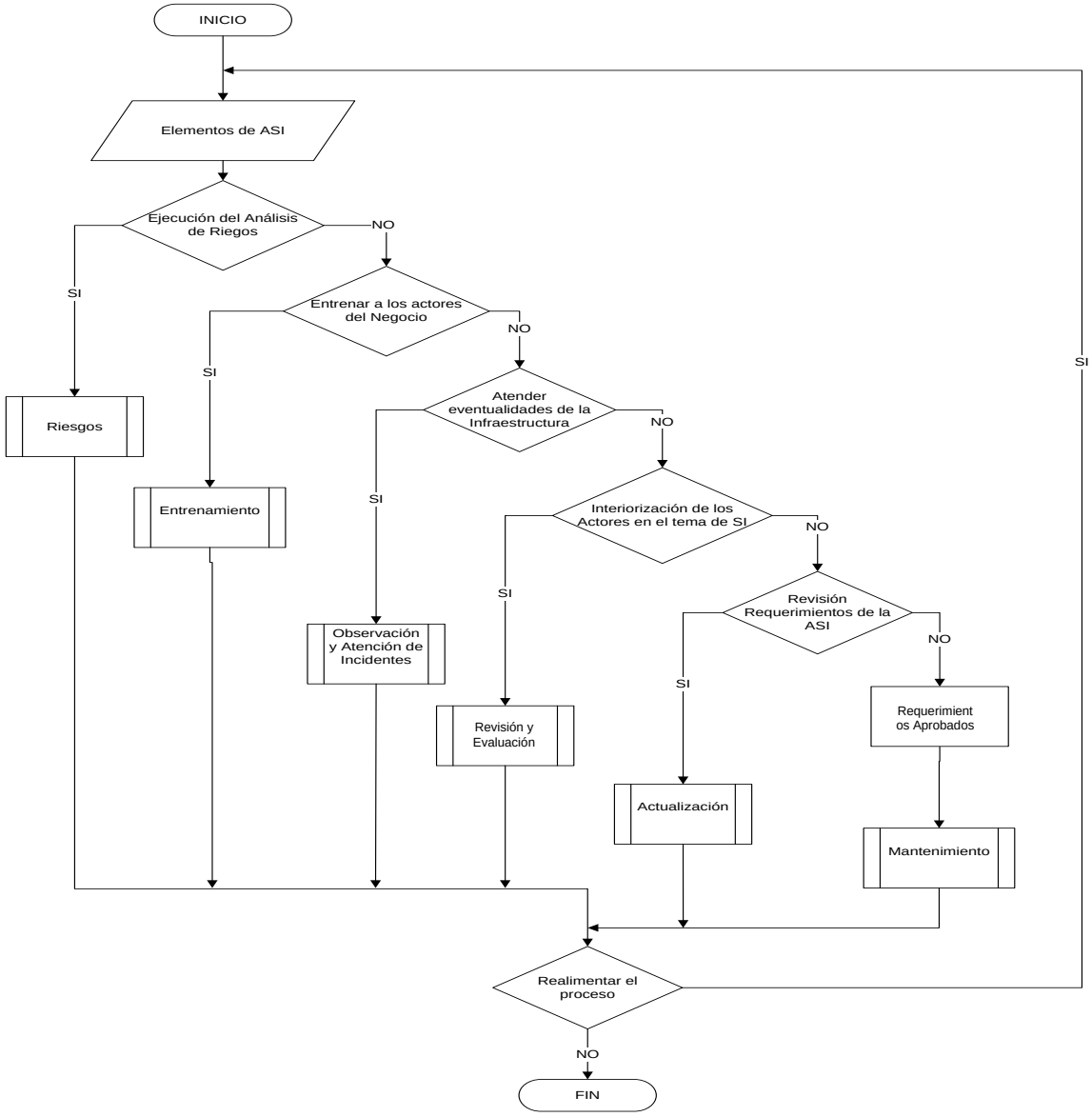
- Lecciones aprendidas: consiste en la elaboración de un documento donde se detallen todos los elementos que facilitaron o entorpecieron el proceso de entrenamiento.

6.6 GESTIÓN DE LA ARQUITECTURA DE SEGURIDAD DE LA INFORMACIÓN

La Figura 11 muestra el proceso general de la Gestión de la Arquitectura de Seguridad de la Información, sus componentes y su ciclo de mejora continua.

Algo que vale pena tener en cuenta para el proceso es el hecho que el encargado de su ejecución pueda acceder específicamente a un componente, esto dependiendo de lo que éste necesite hacer, además puede darse que los productos un componente sean la entrada para la ejecución de otro.

Figura 11 Diagrama de Flujo Gestión de la Arquitectura de Seguridad



6.6.1 Procedimiento Para la Gestión de la Arquitectura de Seguridad de la Información.

Las Figuras 12, 13, 14, 15 y 16 muestran el proceso de cada uno de los elementos definidos en el marco de trabajo de Gestión de la Arquitectura de Seguridad de la información, los cuales permiten la formalización de la mejora continua de sus procesos y por ende de los elementos del MASI.

6.6.2 Análisis de Riesgos

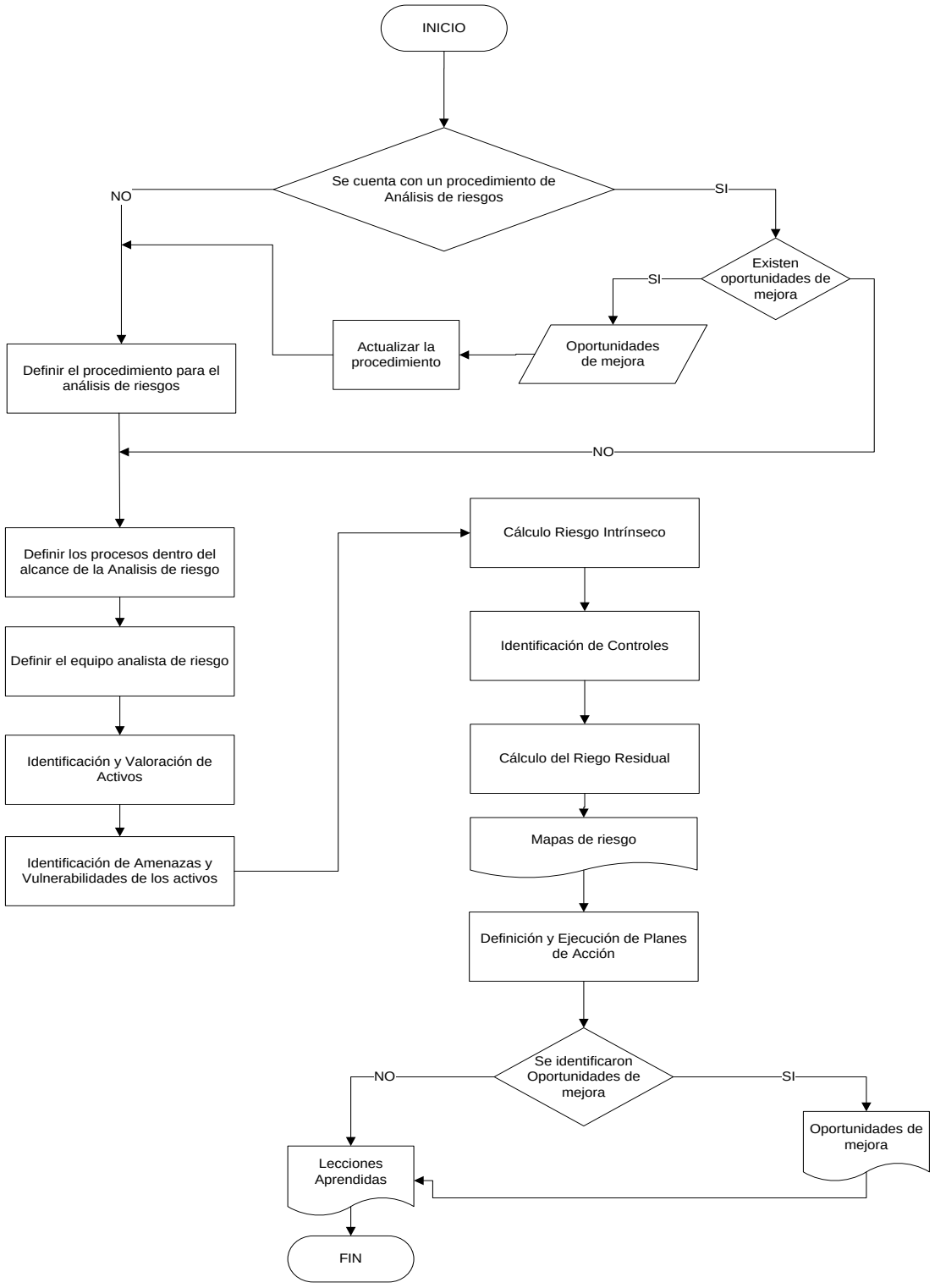
Antes de iniciar el proceso de análisis de riesgos se debe definir como requisitos mínimos:

- La metodología que se va a emplear y el tipo de reporte que se quiera presentar (cuantitativo o cualitativo)
- La definición de las tablas de valoración de activos, tablas de valoración del impacto y probabilidad de materialización de los riesgos, el nivel aceptable de riesgo, tablas de disminución de impacto y probabilidad luego de la aplicación de controles; como valor agregado, se definen los demás factores que se crean pertinentes, teniendo en cuenta que estos deberán estar aprobados por la Alta Gerencia.

6.6.2.1 Diagrama de Flujo Análisis de Riesgos

La Figura 12 muestra el proceso definido que se recomienda para llevar a cabo el análisis de riesgos, que permitirá identificar el nivel de inseguridad al que están expuestos de los elementos del Negocio (Recurso Humano, Procesos de Negocio, TI) en su contexto tanto interno como externo.

Figura 12 Diagrama de Flujo Análisis de Riesgos.



6.6.2.2 Desarrollo del procedimiento de Análisis de Riesgos

Para la documentación de la información relacionada con las actividades de: Identificación de Amenazas y Vulnerabilidades de los Activos, Cálculo del Riesgo Intrínseco, Identificación de Controles, Cálculo del Riesgo Efectivo o Residual, Mapa de Riesgos, Definición y Ejecución de Planes de Acción referenciadas en el procedimiento de análisis de riesgos se puede emplear el documento referenciado en el Anexo G.3 y su instructivo establecido en el Anexo H.

- Si la Organización no cuenta con un procedimiento de análisis de riesgos de activos de información deberá seguir los siguientes pasos para su definición:

    - Manifiesto de importancia del análisis de riesgos: realizar una reunión para dar a conocer la importancia del análisis de riesgos, esta debe estar precedida por los actores o partes interesadas, es decir, la Alta Gerencia con el Arquitecto de Seguridad, donde éste último expondrá al detalle el por qué, el para qué y el cómo se realizará el análisis de riesgos y la forma como se reportarán los resultados.

    - Definición de la Metodología para el Análisis de Riesgos: para lograr resultados repetibles es necesario definir el flujo de actividades que guiará el desarrollo del análisis de riesgos sobre los activos de información del negocio. Para ello se debe tener en cuenta que existen diferentes metodologías para implementar un Análisis de Riesgos, dentro de las cuales de las encuentran: OCTAVE, CRAMM, MAGERIT, AS/NZS 4360:2004, ISO NTC 5254, NTC-ISO-IEC 27005, entre otras, cuyo propósito es brindar las pautas mínimas que se deben cumplir antes, durante y después de la ejecución de dicho proceso.

    - Definir el alcance del análisis de riesgos: la Alta Gerencia es quien define y aprueba el alcance del análisis de riesgos, es decir, los procesos considerados críticos donde se hará mayor énfasis y análisis.

    - Definir el equipo analista de riesgo: teniendo claro el alcance aprobado por la Alta Gerencia, el Arquitecto de Seguridad debe disponer de personal experto en quien pueda delegar la ejecución de pruebas de: (análisis de puertos, servicios de red, ingeniería social, entre otras), las cuales permitirán encontrar las fallas, los puntos débiles, las vulnerabilidades de tipo físicas y lógicas inherentes al sistema de información del negocio.

- Identificación y valoración de activos: para ello se deben tener en cuenta los siguientes aspectos:

- Identificar los procesos del negocio tomando como base la documentación del Sistema de Gestión de Calidad en caso que cuente con uno, de lo contrario se deberán efectuar reuniones con los directivos para identificarlos.

- Cada uno de los actores de los procesos deberán seleccionar al equipo de trabajo encargado de la realización del Análisis de Riesgos, para ello se debe tener en cuenta que este equipo debe ser conformado por las personas que tengan un mayor conocimiento del funcionamiento del proceso. El encargado del proceso hará las veces de líder de equipo.

- Realizar una reunión informativa con los equipos de trabajo para contextualizar cada una de las actividades que se van a realizar. En esta reunión se deberá exponer la metodología de trabajo. Se recomienda que quien convoque a esta reunión sea el líder del equipo.

- Desarrollar el plan de entrevistas para ejecutar el análisis de riesgos con cada equipo de trabajo el cual debe ser cumplido a cabalidad para lograr la eficacia en cada una de las actividades que se deben desarrollar.

- Realizar pruebas piloto del diligenciamiento del Formato de Inventarío de Activos del Anexo C siguiendo el paso a paso y los conceptos contenidos en el Anexo D; esto con el fin de que el formato sea entendido por los dueños de los procesos y estos realicen las respectivas preguntas sobre el diligenciamiento del mismo, con ello se podrá tener un alto grado de confiabilidad en cuanto a la información que será proporcionada en la ejecución de las entrevistas.

- Ejecución del plan de entrevistas a los dueños de procesos.

  - Diligenciar el Formato de Inventarío de Activos del Anexo C siguiendo el paso a paso y los conceptos contenidos en el Anexo D.
  - Organización del Formato de Inventarío de Activos del Anexo C el cual fue diligenciado en el paso anterior.
  - El líder de equipo deberá revisar la información contenida Formato de Inventarío de Activos para verificar que éste se encuentre con todos sus campos diligenciados.
  - Consolidar los activos identificados en cada proceso, como resultado de esta actividad deberá surgir el documento final del inventario de activos de información el cual es el Formato de Inventarío de Activos del Anexo C totalmente organizado y diligenciado
  - El documento del inventario de activos de información deberá ser dado a conocer al dueño del proceso para su respectiva realimentación.

- Tratamiento de los activos

  - Se deben definir medidas de protección para los activos de información teniendo en cuenta la clasificación de los mismos.
  - Las medidas de protección definidas para los activos deben ser dadas a conocer a los integrantes de cada proceso.

- Identificación de Amenazas y Vulnerabilidades de los Activos

  - Identificación de vulnerabilidades de cada uno de los activos: las vulnerabilidades son todos aquellos factores inherentes a los activos que pueden permitir que éstos se vean comprometidos por los diversos factores presentes en su entorno del negocio. Para el desarrollo de ésta actividad se recomienda revisar el Anexo F, donde se condensa un catálogo de vulnerabilidades.

  - Identificación de amenazas de cada uno de los activos: las amenazas son los diferentes factores presentes en el entorno del negocio que pueden aprovecharse de las vulnerabilidades de los activos. Para el desarrollo de ésta actividad se puede tener en cuenta las amenazas descritas en el Anexo E.

- Cálculo del Riesgo Intrínseco

  - El cálculo del riesgo intrínseco de los activos se realiza sin tener en cuenta los controles existentes para la mitigación de los mismos. Se debe tener en cuenta que este valor no es fácil de identificar, debido a que las organizaciones intrínsecamente han implementado controles que complican el hecho que los equipos de trabajo definan valores de probabilidad y de impacto sin tener en cuenta dichos controles.

  - La identificación de la probabilidad de materialización de la Vulnerabilidad vs. la Amenaza: consiste en la definición de la probabilidad de que la amenaza aproveche la vulnerabilidad y se materialice el riesgo sobre el activo. Para ello se puede emplear la tabla disponible en el Anexo G; para la selección de este valor no se debe tener en cuenta los controles existentes.

  - La identificación del impacto de la materialización de la Vulnerabilidad vs. la Amenaza: consiste en la definición del nivel de afectación del negocio en caso que la amenaza aproveche la vulnerabilidad y materialicen el riesgo sobre el activo; para ello se puede emplear la tabla disponible en el

Anexo G. Para la selección de este valor no se deben tener en cuenta los controles existentes.

- La criticidad del riesgo se determina teniendo en cuenta la relación impacto-probabilidad.

- Identificación de Controles

  - La identificación de los controles se realiza teniendo en cuenta la relación que existe entre el activo y el par “amenaza vs. Vulnerabilidad”, lo cuales ayudan a mitigar tanto la probabilidad (posibilidad de que la amenaza se aproveche de la vulnerabilidad) como el impacto (consecuencia de la materialización de los riesgos).

- Cálculo del Riesgo Efectivo o Residual

  - Se debe identificar la probabilidad para cada par amenaza vs. vulnerabilidad, esto corresponde a la posibilidad de que la amenaza aproveche la vulnerabilidad y se materialice el riesgo sobre el activo, para ello se puede emplear la tabla disponible en el Anexo G. Para la selección de este valor se deben tener en cuenta los controles existentes.

  - Se debe identificar el Impacto para cada par amenaza vs. vulnerabilidad, lo que corresponde a identificar el nivel de afectación del negocio en caso que la amenaza aproveche la vulnerabilidad y se materialice el riesgo sobre el activo, para ello se puede emplear la tabla disponible en el Anexo G. Para la selección de este valor se deben tener en cuenta los controles existentes.

  - La criticidad del riesgo se determina teniendo en cuenta la relación impacto-probabilidad.

- Mapa de Riesgos

  Es el resultado del análisis de riesgos en el cual se pueden identificar las necesidades de inversión en seguridad, mediante el análisis por parte de la Alta Gerencia; estas necesidades pueden ser estructuradas en planes de tratamiento de riesgo para aquellos que se encuentren sobre el umbral de riesgos aceptable definido por el negocio.

- Definición y Ejecución de Planes de Acción

    - Teniendo en cuenta el nivel aceptable de riesgos se deben definir los planes de tratamiento de riesgo para aquellos que se encuentren sobre el umbral de riesgos aceptable.

    - Implementar los planes de tratamiento de riesgos definidos, para ello se requiere del apoyo económico del negocio.

    - Realizar nuevamente el proceso de Análisis de Riesgos teniendo en cuenta que los proyectos implementados pasan a ser controles. Se espera que el resultado del riesgo residual sea menor luego de aplicados los controles.

- Si la organización cuenta con un procedimiento de análisis de riesgos deberá verificar sí existen oportunidades de mejora, de tal manera que si el proceso de Análisis de Riesgos se ha ejecutado al menos una vez, se realimente en aras de identificar:

    - Nuevos Activos
    - Nuevas Amenazas y Vulnerabilidades
    - Recalcular el Riesgo Intrínseco
    - Nuevos Controles
    - Recalcular el Riesgo Residual
    - Redefinir el Mapa de Riesgos
    - Estrategias para los planes de acción

6.6.3 Proceso de Entrenamiento

Como resultado del proceso de análisis de riesgos se identifican una serie de fallas en: la infraestructura tecnológica, los procesos de negocio y el recurso humano.

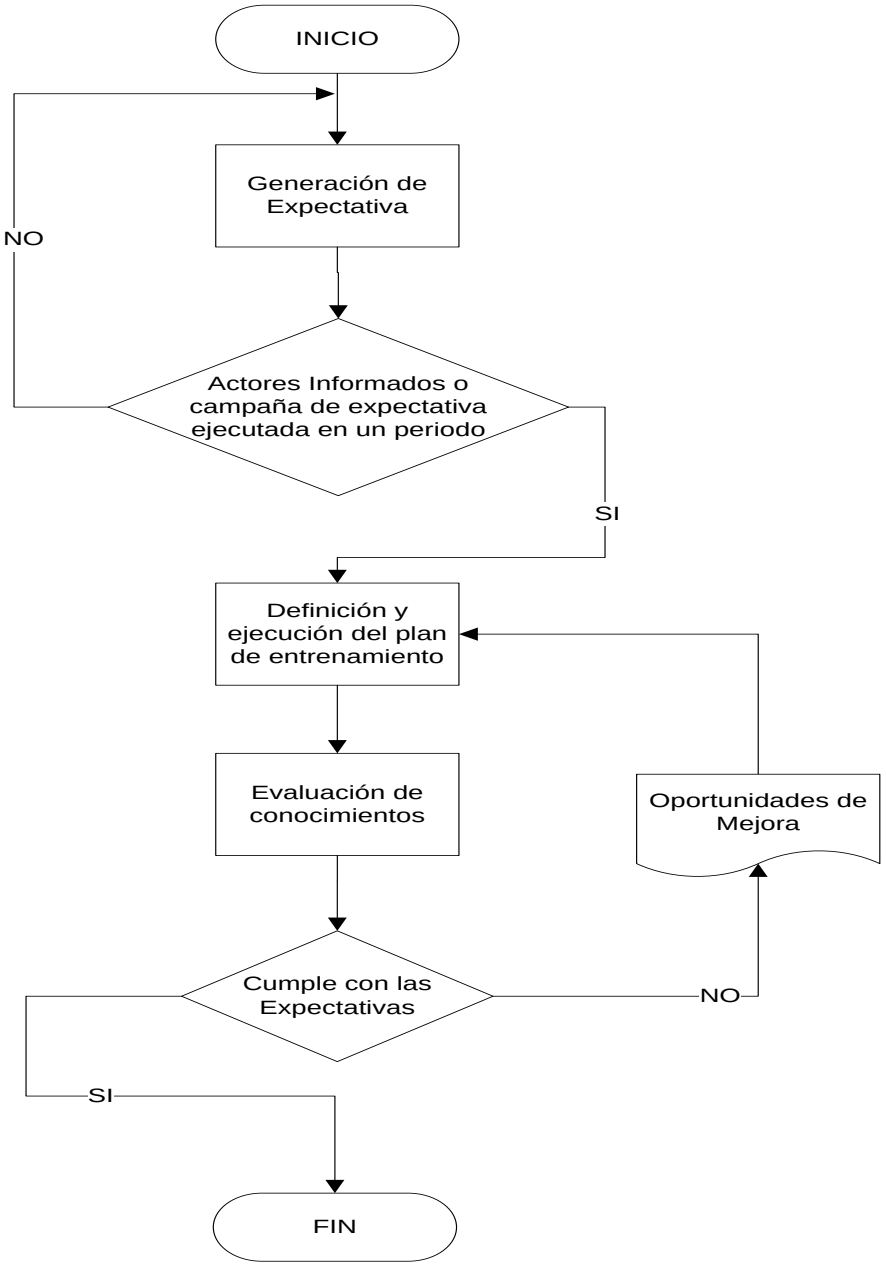
En el recurso humano se encuentran los actores del negocio: usuarios, alta gerencia, clientes, proveedores, entre otros, a quienes se hace necesario formar en pro de generar una cultura de SI, de tal manera que se cambien las estructuras mentales respecto a lo que se debe y no se debe hacer dentro y fuera del sistema de información del negocio.

Se debe tener en cuenta que al interior de las organizaciones existe rotación de personal: ingreso de empleados, cambios de roles, cambios en las funciones, retiro de empleados, entre otros. Los cambios en el personal requieren que el proceso de entrenamiento sea continuo logrando de esta manera mantener actualizado el personal en los conocimientos de cada uno de los actores de la ASI.

6.6.3.1 Diagrama de Flujo para el Entrenamiento

La Figura 13 muestra el proceso para llevar a cabo el Entrenamiento, que permitirá vislumbrar el nivel del compromiso e interiorización adquirido por los actores del negocio en el tema de seguridad de la información, como orientación en el desarrollo de sus funciones.

Figura 13 Diagrama de Flujo para el Entrenamiento



6.6.3.2 Desarrollo del procedimiento de entrenamiento

- Generación de expectativa: consiste en generar inquietud por medio de la publicidad, la cual cree entre los actores del negocio una actitud expectante, dicha publicidad se realiza mediante envío de correos utilizando la plataforma interna, mensajes en la página web principal, afiches o semejantes sobre las distintas carteleras, entrega de plegables o volantes en la entrada de empresa. Esta actividad se debe realizar hasta que la campaña que le llegue a todos los actores del negocio, o por un periodo determinado el cual deberá ser definido por la organización teniendo en cuenta su tamaño, su actividad económica, su distribución geográfica, entre otros factores.

- Definición y ejecución del plan de entrenamiento: es el proceso de incorporación de los conceptos de SI en el negocio, pero antes de ello se deberá realizar un diagnóstico que permita determinar el conocimiento respecto a SI con el que cuenta los empleados.

  - Diseñar un instrumento (encuestas) que permita evaluar el nivel de conocimiento que tienen los actores del negocio en SI y de su arquitectura. Debido a la diversidad de roles de los actores del negocio se hace necesario definir diferentes tipos de encuestas.

    El tamaño de la muestra para la aplicación del instrumento, estadísticamente se realiza mediante muestreo aleatorio simple de la población por área de la empresa. El siguiente es un ejemplo para el cálculo del tamaño de la muestra; dado que no se tiene provisto el dato de la cantidad de personas se asume el valor de p=0,5 con un nivel de confianza del 95% y un error máximo admitido de 0.1; el tamaño de la muestra es:

$$n = \frac{Z_{\infty}^2 * p * q}{d^2}$$

    Donde:

    Z_{∞}^2= 1,962 (ya que la seguridad es del 95%)
    p = proporción esperada (en este caso 5% = 0,05)
    q = 1 – p (en este caso 1 – 0,05 = 0,95)
    d = precisión (en este caso deseamos un 1%)

    Despejando:

    $n = (1.96^2 * 0.5 * 0.5) / 0.1^2 = 96$
    n= 96 personas a encuestar

Hay que tener en cuenta que si se quiere un número pequeño de la muestra el porcentaje del error asumido debe ser mayor, además que a mayor nivel de confianza, mayor es el número de la muestra.

- En el Anexo I se podrá encontrar algunos ejemplos de preguntas que puede tener en cuenta para la elaboración de la encuesta.

- Antes que el instrumento sea aplicado, se recomienda realizar una prueba piloto, para ello seleccione un número pequeño de actores del negocio por rol, los cuales serán encargados de evaluar y generar recomendaciones referentes al instrumento; para ello, estas personas deberán responder la encuesta, con el fin de identificar oportunidades de mejora en cuanto la claridad en la formulación de preguntas y respuestas, además del hecho de incluir nuevas preguntas y redefinir el número de preguntas. Para realizar dicha actividad de forma organizada se recomienda que los encuestados diligencien el formato disponible en el Anexo I.3.

- Mejorar el instrumento realizando las correcciones con base en las recomendaciones de los participantes de la prueba piloto.

- Una vez se realicen los cambios sugeridos por los participantes de la prueba piloto, se procede a aplicar la encuesta teniendo en cuenta los datos de población y muestra identificados previamente.

- Aplicada la encuesta se consolidaran los datos obtenidos y se realizará el análisis estadístico de los resultados arrojados por el instrumento, de esta manera se podrán identificar elementos claves para la definición del plan de entrenamiento adecuado a las necesidades del negocio.

- Para la elaboración del plan de entrenamiento es importante que la organización tenga en cuenta el desarrollo de campañas que centren la atención de los usuarios como:

  - Elaboración de salva pantallas con mensajes y elementos que generen recordación en los usuarios. Elaboración de cartillas de capacitación.
  - Desarrollo de charlas informativas.
  - Impresión de afiches informativos que generen recordación.
  - Emplear herramientas dinámicas como flash para la elaboración de manuales de seguridad de la información.
  - Ayudas disponibles en páginas web de uso libre como por ejemplo en www.inteco.es en la cual existen video tutoriales sobre SI.

- Diseñado el plan de entrenamiento, este debe ser revisado por el equipo de trabajo conformado por la Alta Gerencia y el Arquitecto de Seguridad, este último requiere el aval y apoyo de la Alta Gerencia en la gestión de los recursos para la ejecución del mismo.

- Si la Alta Gerencia derivado de su revisión decide hacer algún tipo de consideración o cambio deberá diligenciar el formato disponible en el Anexo I.4.

- El plan de entrenamiento estará listo para su ejecución si la Alta Gerencia, luego de su revisión, decide no hacer consideraciones o cambios. Durante la ejecución del plan de entrenamiento se deberán realizar evaluaciones del nivel de pertinencia de las herramientas empleadas para el entrenamiento de los actores del negocio, en pro de garantizar la eficiencia de las mismas.

- Cronograma de trabajo o de ejecución del plan de entrenamiento: se deben definir fechas o periodos para llevar a cabo la ejecución del plan de entrenamiento y el responsable de su implementación.

  - Para la definición del cronograma se pueden utilizar herramientas especializadas como Microsoft Project (ver formato del Anexo I.5):

- El cronograma de trabajo es sometido a verificación y aprobación por parte de la Alta Gerencia.

  - Si hay consideraciones o cambios al cronograma de trabajo se realimenta, corrigiendo los periodos u horarios.
  - Aplicados los cambios, se somete nuevamente a revisión por parte de los interesados (Alta Gerencia y Arquitecto de Seguridad).
  - De pasar la revisión sin nuevas consideraciones, termina el proceso y se continúa con la ejecución del cronograma de trabajo.

- Ejecución de las actividades del aprendizaje: es la ejecución del cronograma de actividades, esto es, de las acciones pertinentes en la formación y concienciación de los actores del negocio Se debe tener en cuenta el tipo de aprendizaje a utilizar, especialmente diferenciando si son profesionales de TI o usuarios finales (secretarías, directivos, clientes, proveedores, administrativos, entre otros).

  - Si el aprendizaje es para el usuario final, el proceso de aprendizaje se ceñirá a las reuniones o charlas, envío de correos, pruebas escritas, ventanas pedagógicas, videos, circulares, entre otras actividades, métodos o herramientas apropiadas para este tipo de actores del negocio.

- Si el aprendizaje es para los profesionales de TI, se debe pensar en brindar algún tipo de formación académica, que pueden ser: diplomados, especializaciones, cursos de certificación (*CISSP*, *Ethical Hacking*, entre otros), que permitan adquirir las competencias técnicas y operativas necesarias para materializar las expectativas de las directivas en la implementación de los controles preventivos, detectivos y correctivos que resultaron del análisis de riesgos, así como el aseguramiento de los servicios y sistemas de información del negocio.

- Evaluación de conocimientos: es necesario verificar si las actividades desarrolladas para sensibilizar y concienciar a los actores del negocio desde la ejecución del proceso de aprendizaje han cumplido con su objetivo. La evaluación se puede desarrollar mediante:

  - Visitas para identificar si se está cumpliendo con las recomendaciones impartidas a través del entrenamiento.

  - Una evaluación de conocimiento general de la ASI.

  - Diseñar un cuestionario donde se evidencien situaciones que atentan contra la seguridad de la información a fin de establecer el accionar de los interesados.

- ¿El entrenamiento cumplió con el objetivo?: si la respuesta es no, se deben listar o enunciar las oportunidades de mejora al respecto y por medio de las actividades de actualización del MASI, contribuir a la mejora del diseño del plan de entrenamiento, esto puede tener un registro mediante el diligenciamiento del formato propuesto en el Anexo I.6.

- Si la respuesta es sí se deberán documentar las lecciones aprendidas mediante el diligenciamiento del formato disponible en el Anexo I.4 y se da por finalizada la actividad.

6.6.4 Observación y atención de incidentes

La gestión de incidentes está basada en los lineamientos establecidos por ITIL V3 en su proceso de operación del servicio. En el Anexo J se especifican las actividades consideradas en MASI para la observación y atención de incidentes.

6.6.4.1 Diagrama de Flujo para la Observación y Atención de Incidentes

La Figura 14 muestra el proceso definido que se recomienda para llevar a cabo la Observación y Atención de Incidentes, que permitirá identificar la forma como se deben llevar a cabo la solución a eventualidades de la ASI.

Figura 14 Diagrama de Flujo para la Observación y Atención de Incidentes

- Reporte del incidente: esta etapa corresponde a la identificación del incidente o evento por parte de personal vinculado por la organización y su respectiva notificación al punto único de contacto, es decir, a la persona o equipo encargado de solucionar el incidente.

- Clasificación del incidente: en este ítem se evalúa el nivel de riesgo del incidente lo proporciona un punto de partida para establecer la prioridad de atención del mismo.

- Diagnóstico inicial: con base en la información suministrada en el reporte del incidente, se identifica si este puede ser resuelto por el punto único de contacto o si se requiere escalar el mismo.

- Escalamiento: el escalamiento del incidente será desarrollado a quien el punto único de contacto considere apropiado. El Arquitecto de Seguridad deberá apoyar el proceso de investigación y solución del incidente.

- Investigación y diagnóstico: para esto se deberán investigar todas las fuentes con el fin de identificar las causas del incidente y mitigarlas, en caso que se requiera se podrá contactar a un grupo interdisciplinario que apoye la investigación.

- Resolución: consiste en la documentación de la solución al incidente.

- Comunicación: una vez el incidente sea solucionado se debe informar a quien lo reportó que éste ha sido resuelto.

- Cierre: El Arquitecto de SI deberá confirmar oficialmente el cierre del caso luego que se identifique satisfacción por parte de quien reportó el incidente.

6.6.5 Proceso de revisión y evaluación

La revisión y evaluación de ASI permite verificar si ésta contribuye o no a la incorporación de la seguridad en los procesos de negocio. Para ello se toma como insumo los resultados del análisis de riesgos, además de los incidentes reportados. Teniendo en cuenta que la SI es un proceso dinámico, la revisión y evaluación permite identificar factores que puedan ocasionar problemas y por ende realizar las respectivas acciones para su corrección. Dentro de los aspectos a evaluar y revisar se tiene:

- Los elementos de la Arquitectura de Seguridad
- Los actores del negocio
- La infraestructura de TI (revisión y evaluación de tipo técnico)

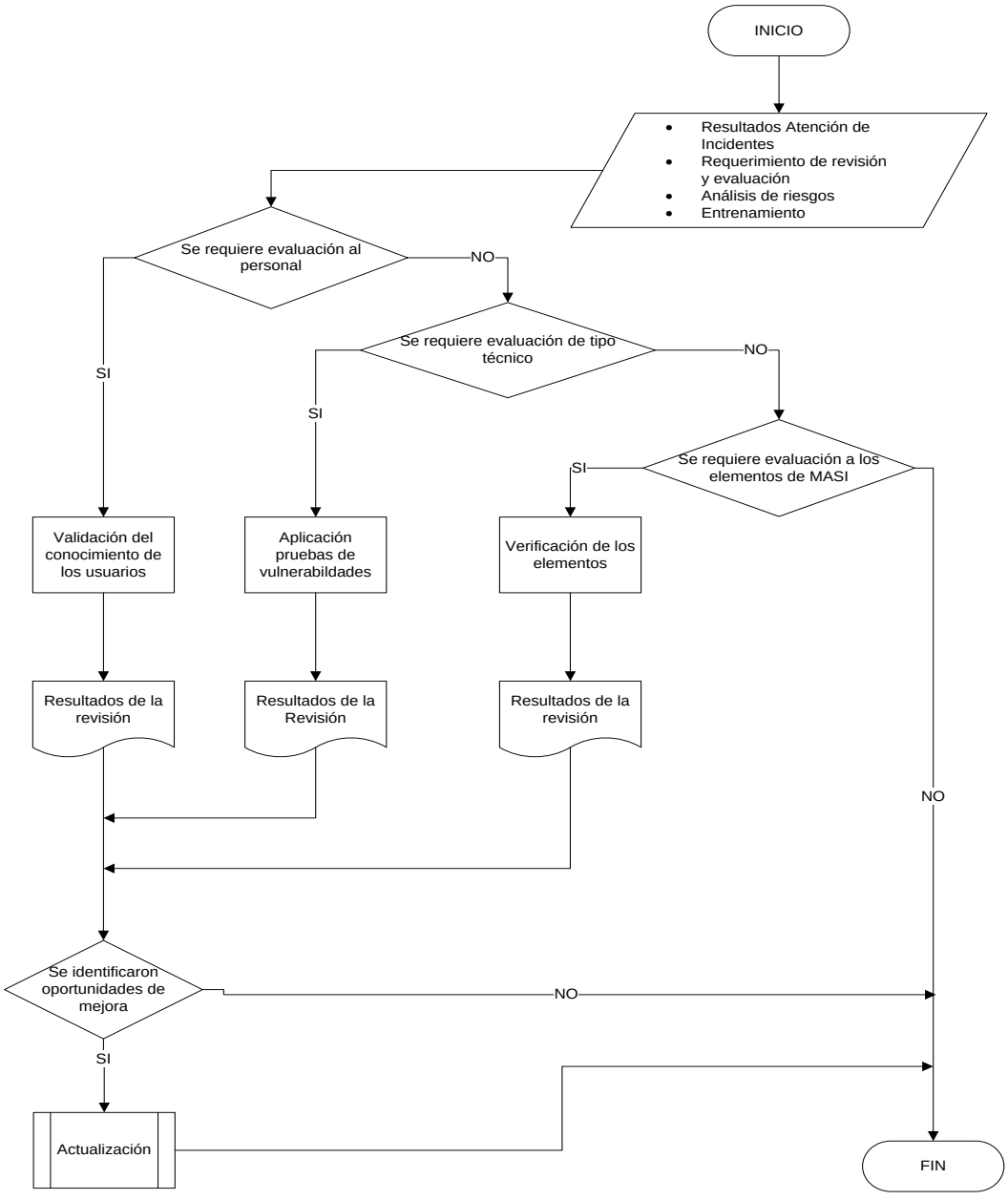
Este proceso apoya la actualización de los elementos de la ASI, el análisis de riesgos y el entrenamiento del personal.

6.6.5.1 Diagrama de Flujo para el elemento Revisión y Evaluación

La Figura 15 muestra el proceso definido que se recomienda para llevar a cabo la Revisión y Evaluación, que permitirá verificar el nivel de eficacia y eficiencia que

ha tenido el proceso de Entrenamiento referente al cumplimiento de los compromisos y buenas prácticas en el desarrollo de sus funciones, de igual manera el cómo se ha actuado frente a la atención de eventualidades y si lo que se hizo por solucionarlas fue óptimo, y por último si lo definido para cada elemento de ASI está o no alineado con las expectativas del negocio.

Figura 15 Diagrama de Flujo para la Revisión y Evaluación de ASI



6.6.5.2 Desarrollo del procedimiento de revisión y evaluación

- ¿La revisión y evaluación es al personal?, si la respuesta es sí se procede a:
    - Validar el conocimiento de los usuarios; para esto se puede emplear una prueba de conocimientos relacionada con los elementos de la arquitectura o realizar visitas que permitan identificar el nivel de cumplimiento de la política, directrices y normas de seguridad.
    - Identificar las oportunidades de mejora las cuales serán evaluadas en el proceso de actualización de ASI.
- ¿La revisión y evaluación es de tipo técnico?, si la respuesta es sí, se someten los controles, activos y las aplicaciones del sistema de información del negocio a pruebas de vulnerabilidades técnicas, con el fin de encontrar vulnerabilidades. Para la aplicación de dicha prueba diligencie el formato del Anexo J.
    - Identificar las oportunidades de mejora las cuales serán evaluadas en el proceso de actualización de ASI.
- ¿La revisión y evaluación es a los elementos de la ASI?, si la respuesta es sí, se deberán evaluar los diferentes elementos de ASI a través de una verificación para identificar el estado del arte de ASI dentro de la organización; para ello se podrá emplear la lista de verificación disponible en la tabla 3.

Tabla 3. Lista de Verificación de los Elementos de la ASI.

Lista de Verificación de los Elementos de la ASI	SI/NO
Negocio	
¿El formato de Levantamiento de Información del Negocio se encuentra actualizado?	
¿Las metas del Negocio se encuentran relacionadas con las metas de la arquitectura?	
Marco normativo de Seguridad	
¿Se han reportado incidentes sobre incumplimientos en el marco normativo?	
A través de las visitas de campo ¿se han identificado eventos que atentan contra la seguridad de la información?	
Gestión de la Arquitectura de Seguridad	
¿Se han realizado las actividades de evaluación de riesgo?	
¿Se cuenta con reportes de Incidentes de Seguridad de la Información?	
Los incidentes de seguridad de la información reportados ¿han sido resueltos?	
¿Los planes de tratamiento para la mitigación de los riesgos han sido eficaces?	

Lista de Verificación de los Elementos de la ASI	SI/NO
¿Se ha disminuido los niveles de riesgo de los activos de información?	
¿Se han realizado mantenimientos a la ASI?	
Acuerdos	
La Alta Gerencia y el Arquitecto de Seguridad ¿efectúan reuniones continuas?	
Infraestructura de Seguridad	
¿Se han identificado intentos de ataques a la plataforma tecnológica?	
¿Se han reportado incidentes relacionados con la no disponibilidad de los servicios de tecnología?	

- Identificar las oportunidades de mejora las cuales serán evaluadas en el procedimiento de actualización de ASI. cosiste

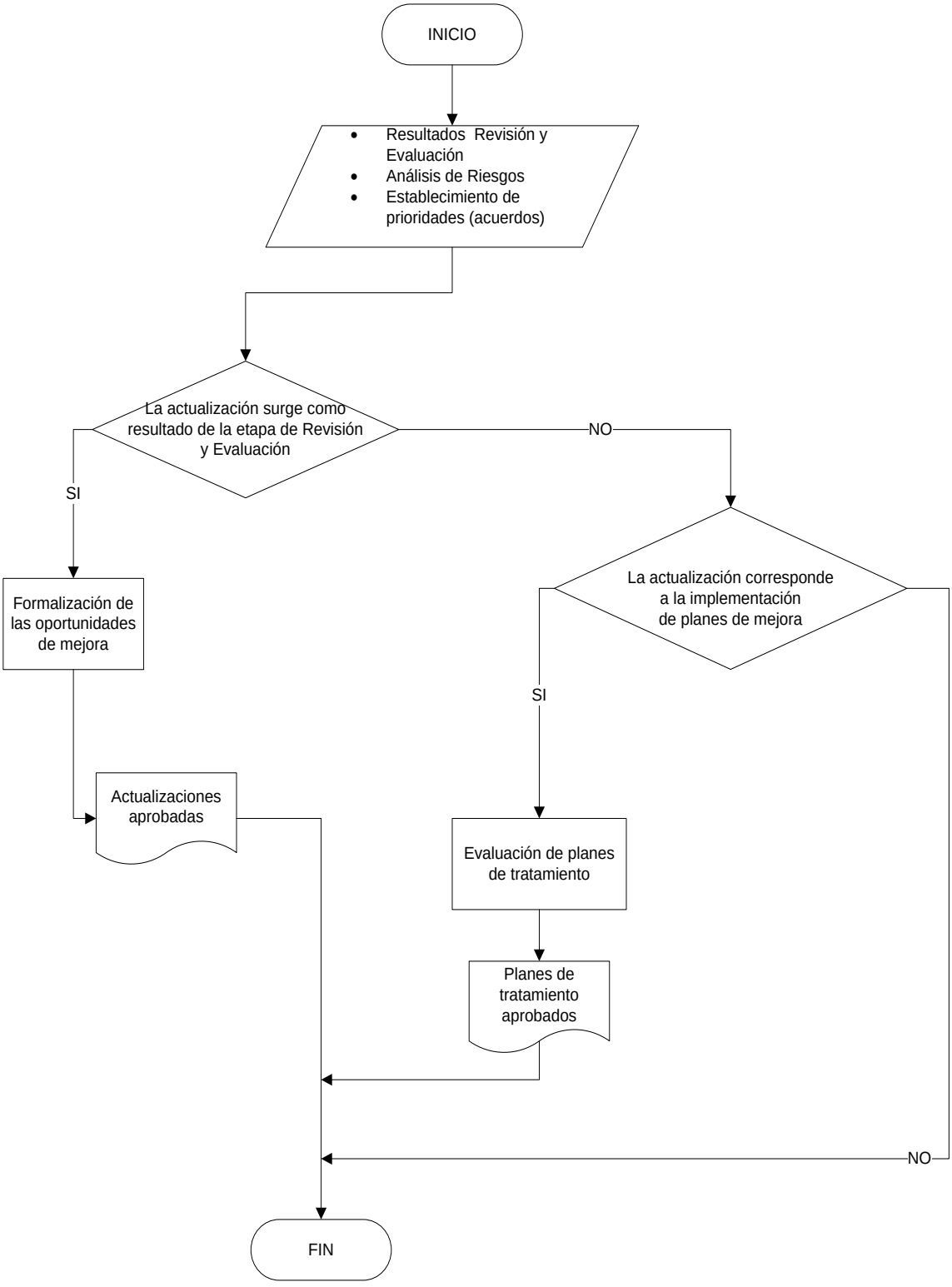
6.6.6 Actualización

Este elemento está enfocado en la estructuración de las actividades que van a permitir formalizar la oportunidades de mejora identificadas en el proceso de evaluación y monitorización y los planes de mejoramiento identificados en el proceso de análisis de riesgos.

6.6.6.1 Diagrama de Flujo para la Actualización

La Figura 16 muestra el proceso para llevar a cabo la Actualización, lo cual que permitirá estudiar y avalar los cambios sobre la ASI.

Figura 16 Diagrama de Flujo para la Actualización



6.6.6.2 Desarrollo del procedimiento de actualización

- Identificación de las oportunidades de mejora: teniendo en cuenta los resultados de la etapa de revisión y evaluación se deberá realizar el registro de las actualizaciones, para ello se puede emplear el formato disponible en el Anexo K, además de los planes de mejora que fueron identificados en el proceso de análisis de riesgo.

- Consideración de la Alta Gerencia: la ejecución del proceso está acompañado por la convocatoria a una reunión por solicitud del Arquitecto de SI, donde se expondrán las consideraciones referentes a las oportunidades de mejora para la ASI y la forma en cómo se llevarían a cabo según el Anexo K.

- Aprobación de actualizaciones: la Alta Gerencia teniendo en cuenta lo expuesto por el Arquitecto de SI, decide si las recomendaciones de oportunidades de mejora expuestas por el Arquitecto son viables de acuerdo a los recursos con los que cuente la organización. dicha aprobación debe registrarse en el formato del Anexo K correspondiente a la actualización aprobada. Para la aprobación de las actualizaciones referentes a la implementación de planes de mejora se debe considerar del elemento acuerdos el proceso de establecimiento de prioridades.

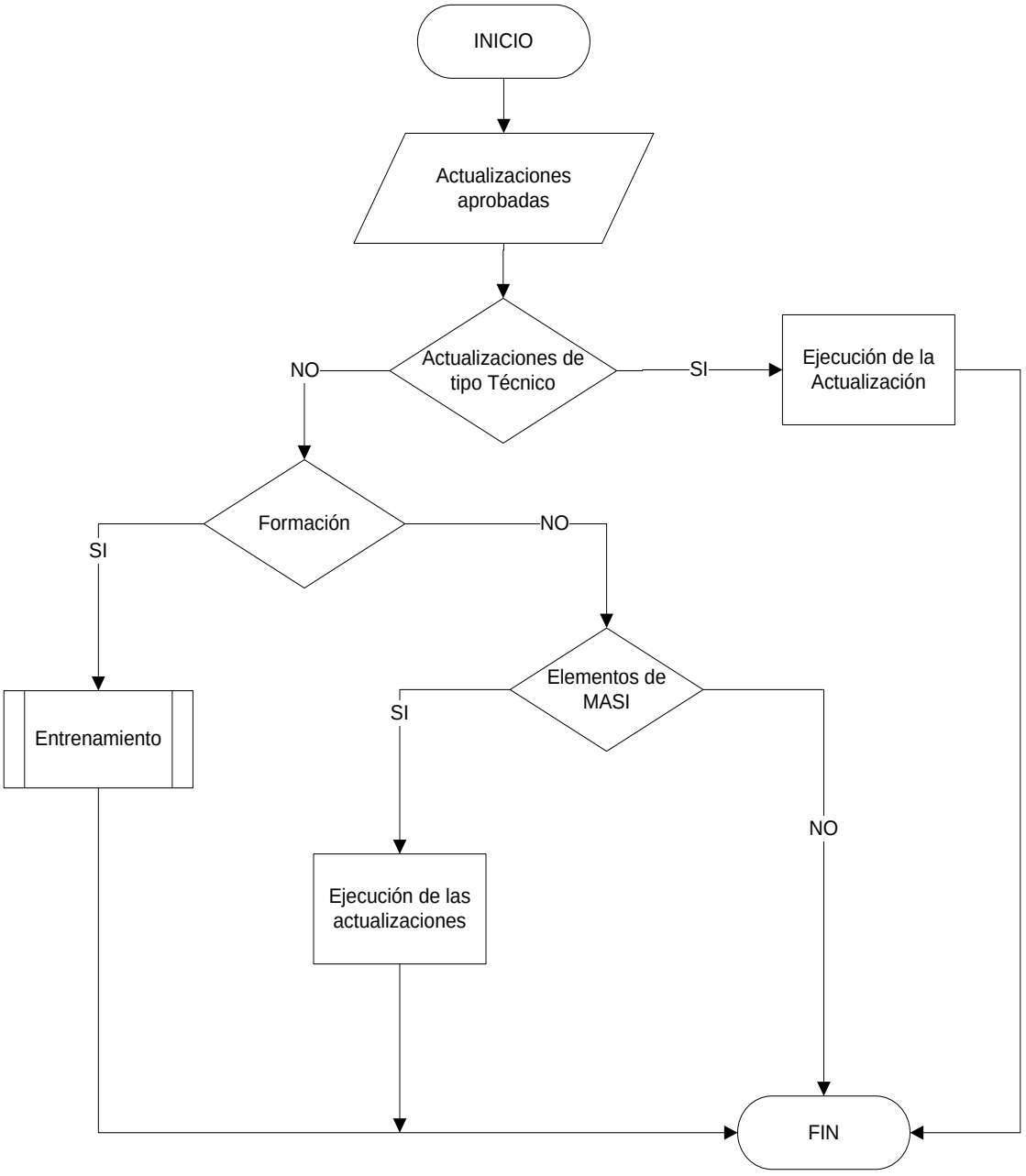
6.6.7 Mantenimiento

Permite la implementación de las actualizaciones aprobadas por la Alta Gerencia y concertadas con el Arquitecto de Seguridad (Ver Anexo L).

6.6.7.1 Diagrama de Flujo del Mantenimiento

La Figura 17 muestra el proceso definido que se recomienda para llevar a cabo el Mantenimiento el cual permitirá la implementación e implantación de las actualizaciones frente a los cambios o redefiniciones de los elementos de la ASI.

Figura 17 Diagrama de Flujo para el Mantenimiento de ASI



6.6.7.2 Desarrollo del procedimiento de mantenimiento

- Identificar el tipo de mantenimiento que será realizado teniendo en cuenta los resultados de la actualización.

- ¿El mantenimiento es de tipo es técnico?, de ser así se debe:

- Someter la solución a un ambiente de pruebas: mínimo de 24 hrs. antes de ser puesto en producción si el mantenimiento es crítico, de no serlo 36 hrs. como mínimo y máximo entre 48 y 76 hrs.
- Delegar en una persona o grupo capacitado y entrenado la implementación de la puesta en producción del mantenimiento; en caso que no se cuente con personal capacitado se podrán definir otras estrategias como son la contratación de de terceros o la capacitación al personal interno para que ejecute la actividad, entre otras.
- Aplicación de la actualización o puesta en producción del mantenimiento.
- Verificación de cualquier tipo de comportamiento anormal del sistema.

- Si la respuesta de la pregunta anterior es no, se pregunta: ¿es a los elementos de ASI?, de responder si, este debe:

  - Realizar la enmienda de los documentos de ASI que lo requieran.
  - Derogar los documentos que fueron modificados.
  - Realizar propaganda dirigida a los actores resaltando los cambios en los elementos de ASI.

- Ahora, como la actualización no es a la infraestructura ni a los elementos de ASI, queda solamente preguntar si es de formación, de ser así se debe:

  - Intensificar el programa de aprendizaje, charlas, instrumentos, folletos, entre otros.
  - Desarrollo de pruebas de concepto mejor enfocadas.
  - Verificación de cualquier tipo de comportamiento anormal del sistema.

6.7 INFRAESTRUCTURA DE SEGURIDAD DE LA INFORMACIÓN

Para el aseguramiento de la plataforma tecnológica se identificaron tres modelos [20]:

- Por oscuridad: modelo que se basa en el desconocimiento o la desinformación, es decir, entre menos divulgación se haga de los servicios, arquitectura de red, entre otros, el nivel de probabilidad de materialización de los riesgos es bajo.

- Del perímetro: modelo en el cual se fortalecen los puntos de conexión y acceso desde internet hacia la red privada por medio básicamente de: *firewall*, *proxy*, *IDS*, *IPS*, entre otros.

- En profundidad: modelo que no solo tiene en cuenta los puntos de acceso y conexión, ya que si se logra vulnerar un firewall, un proxy o cualquier otro elemento de protección, el atacante estaría dentro de la red privada. La

defensa en profundidad establece una serie de anillos, capas o niveles de seguridad con diferentes medidas de protección, de tal manera que al vulnerarse un primer anillo, el atacante se encuentre con un nivel de protección mayor al anterior que fue vulnerado, así el atacante antes de llegar a los datos tendrá que pasar una a una las diferentes contramedidas de seguridad establecidas en cada uno de los anillos. Este modelo conlleva a que la probabilidad de que el atacante logre su objetivo disminuya y la probabilidad de ser detectado aumente, gracias a los mecanismos de monitorización y gestión empleados por el administrador.

La definición del elemento de Infraestructura de Seguridad de la Información del MASI se realizará con base en el concepto de "*Defensa en Profundidad*", debido a que se considera uno de los más completos y adecuados para MASI.

Referente al diseño de infraestructuras de seguridad de red basada en el concepto de Defensa en Profundidad, se tuvieron en cuenta dos modelos:

- Modelo de Defensa en Profundidad de Microsoft [21]

  Este es un modelo conformado por siete capas, de las cuales la capa de políticas, procedimientos y concienciación y la capa de seguridad física (Ver Figura 18), tienen incidencia directa sobre las capas restantes: perímetro, red interna, *host*, aplicación y datos. A continuación se realiza una breve descripción de cada una de las capas:

Figura 18 Modelo de Defensa en Profundidad de Microsoft

Fuente: Basado en [21]

- Políticas, procedimientos y concienciación: directrices de seguridad de uso aceptable de los activos de información del negocio para los usuarios y, necesariamente deben contar con el aval de las directivas para lograr su cumplimiento.
- Seguridad Física: si bien existen medidas de protección lógicas, resulta necesario definir otro tipo de controles que complementen las medidas de este tipo adoptadas, de tal manera que permitan vigilar y prevenir el estado físico de los activos, por ello se hace necesario pensar en cámaras de vigilancia, puertas con candados magnéticos, sistemas biométricos, entre otros.
- Perímetro: busca proteger los puntos de acceso y de conexión desde internet hacia la red privada, básicamente mediante *firewalls*, *proxy* o algún otro mecanismo de control de acceso.
- Red Interna: todas aquellas medidas de protección para la red privada dentro de las cuales se encuentran la segmentación de la red, *IPSec*[7] y dispositivos de detección y prevención de intrusos de red.
- *Host*: se entiende por *host* tanto los servidores como los equipos de usuario final, por tanto, los mecanismos de protección para esta capa son específicos para la protección de estos dos elementos dentro de la infraestructura de red. Algunos de estos mecanismos son: administración de actualizaciones, *firewalls* distribuidos, antivirus, auditoria, entre otros.
- Aplicación: en esta capa del modelo se definen las medidas de protección tanto para las aplicaciones configuradas en los servidores (*IIS*[8], SGBD[9], entre otras), así como aquellas aplicaciones típicas del cliente (*Outlook*, *Office*, *Office Comunicator*, entre otras).
- Datos: es la última capa o nivel del modelo dado que su enfoque es la protección de los datos; se deben tener en cuenta entonces elementos que permitan la protección de la confidencialidad (ej: listas de acceso), la integridad (ej: cifrado) y la disponibilidad (ej: copias de seguridad). En esta capa también se habla del *EFS*[10] cuyo enfoque es el cifrado del sistema de archivos como por el *BitLocker*[11].

[7] IPSec: "Es un entorno de estándares abiertos para garantizar comunicaciones privadas y seguras a través de redes *Internet Protocol* (IP), mediante el uso de servicios de seguridad basados en cifrado" Tomado de [25].
[8] IIS: Servicios de información de Internet.
[9] SGBS: Sistema Gestor de Base de Datos.
[10] EFS: Sistema de cifrado de archivos.
[11] *BitLocker*: tecnología de cifrado aplicada a las unidades de Windows en las versiones *Ultimate* y *Enterprise* del Vista y 7.

- Modelo SAFE de CISCO

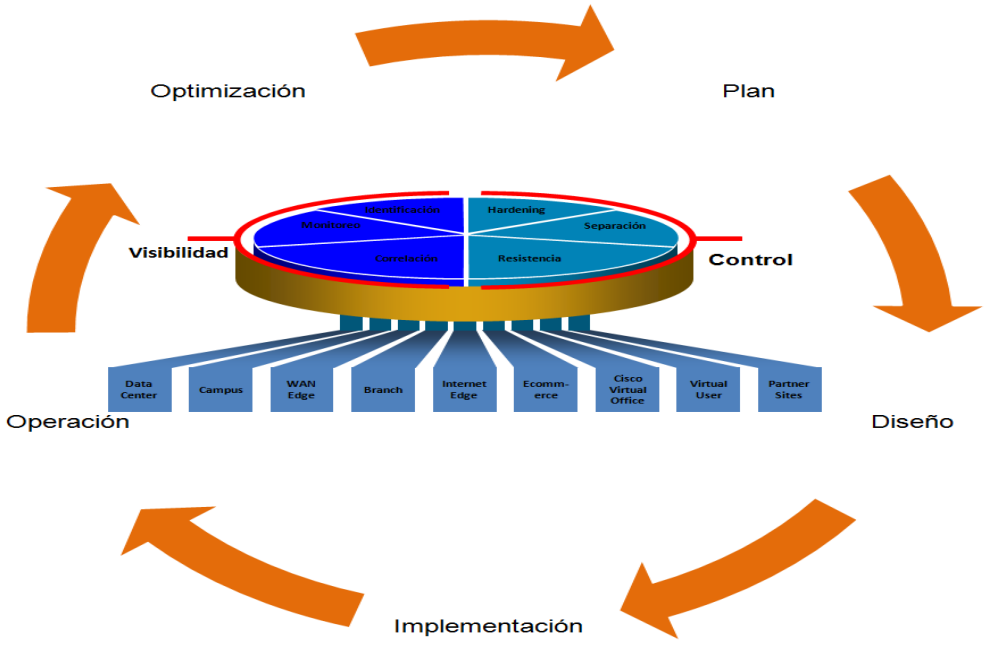
La definición del modelo SAFE como lo muestra la Figura 19 está enmarcada en dos aspectos denominados visibilidad y control, fundamentales para el modelo. A continuación se describen las características de cada aspecto:

- Visibilidad: está enfocada en el conocimiento detallado del estado de cada uno de los elementos que componen la red de comunicaciones, para ello se apoya en tecnologías de identificación, monitorización y correlación de eventos.

- Control: busca aumentar la capacidad de resistencia de la red ante eventos internos o externos mediante procesos de aseguramiento, definición de roles para usuarios, segmentación de la red de comunicaciones y definición de perfiles para los servicios.

El modelo se encuentra inmerso en un ciclo de mejora continua enmarcado en cinco elementos: plan, diseño, implementación, operación y optimización. A su vez, divide la infraestructura de red en módulos funcionales en los cuales interactúan los elementos definidos para garantizar los aspectos de visibilidad y control.

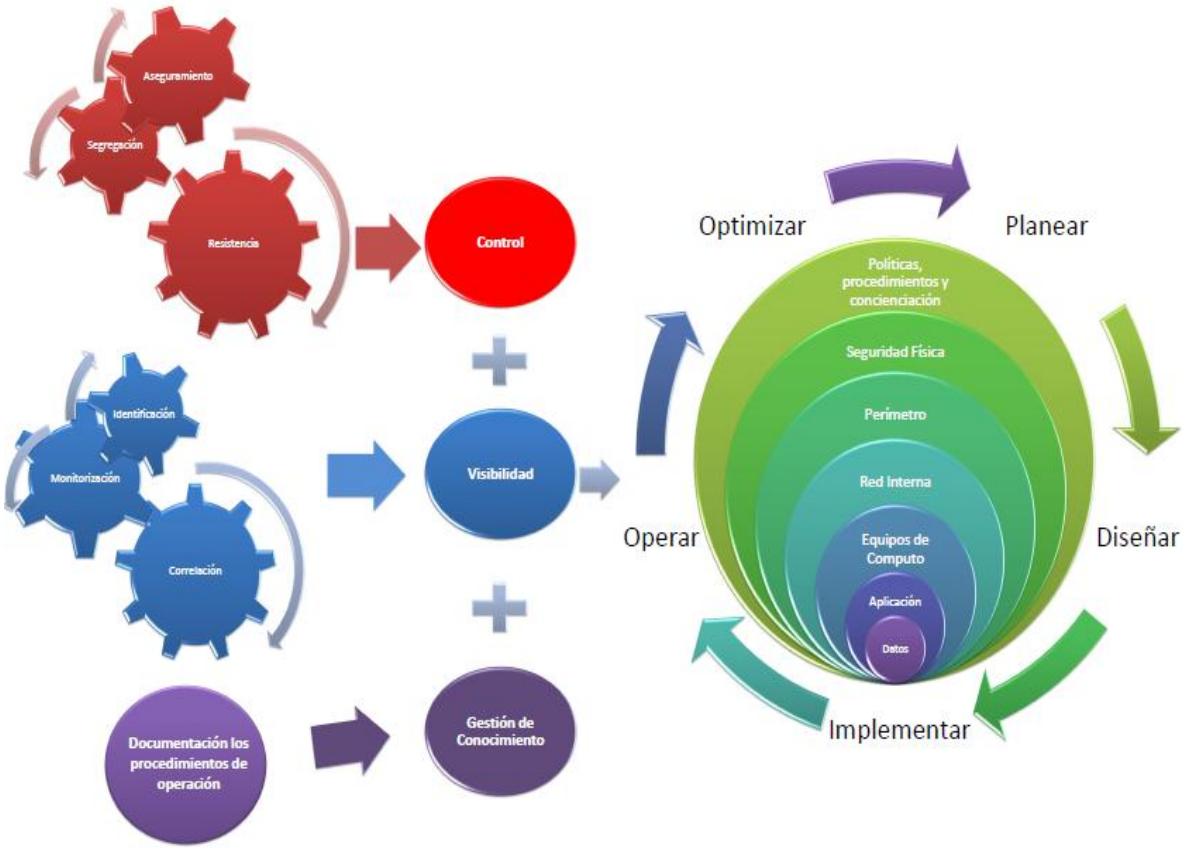
Figura 19 Adaptación del SAFE CISCO.



Fuente: Adaptado de [22]

Teniendo en cuenta los modelos de defensa en profundidad de Microsoft y el SAFE de Cisco, la definición del modelo para la infraestructura del MASI está enmarcado en los elementos del modelo defensa en profundidad de Microsoft debido a que estos elementos poseen características genéricas fácilmente identificables en cualquier negocio; se complementa con los aspectos de visibilidad y control del SAFE Cisco y su ciclo de mejora continua en cada uno de los procesos de visibilidad (identificación, monitoreo y correlación de eventos), y control (*hardening* y políticas, segregación y atención de incidentes); además, como valor agregado se pensó en la necesidad de realizar gestión del conocimiento (documentación), de tal manera que la adaptación de éstos dos modelos para MASI implique realizar los esfuerzos necesarios para salvaguardar el normal funcionamiento de la red privada mediante el aseguramiento de los dispositivos que la conforman (ver Figura 20).

Figura 20 Modelo de Infraestructura MASI



La Tabla 4 referencia, por cada elemento que conforma la propuesta de la Infraestructura de Seguridad para MASI, los dispositivos, herramientas o tecnologías sugeridas que se deben tener en cuenta para la formalización de cada

anillo que conforma el modelo, basado en el modelo de Seguridad en Profundidad de Microsoft.

Tabla 4 Dispositivos de la Infraestructura del MASI

Perímetro	Red Interna	Host	Aplicación	Datos
• Firewalls • Proxy (Reverso y Web) • IDS / IPS • VPN	• Seguridad de la Red • VLANs • NIDS / NIPS • DAC (ACLs) • SSL • SSH • IPSec	• HIDS / HIPS • Actualización SO (parches) • Antivirus • Líneas Base • MAC (permisos)	• Firewall (WAF[12]) • Buenas Prácticas de Programación • RBAC (perfiles)	• Cifrado • Prevención de fugas de Información • EFS • Borrado Seguro
Seguridad Física: CCTV, *Smart Cards*, Biométricos, Controles Ambientales (HVAC[13])				
Políticas, Procedimientos y Concienciación: Marco Normativo, Entrenamiento (Gestión de la Seguridad de la Información)				

- **Gestión del Conocimiento:** para el negocio debe ser transparente que pese a la ausencia de personal (por enfermedad, despido o renuncia) el funcionamiento de la plataforma tecnológica no se afecte, por ello se hace necesario implementar estrategias de documentación de los procedimientos operativos que se efectúan en el manejo y administración de los diferentes dispositivos que la conforman, de tal manera que cualquier miembro del equipo pueda sortear cualquier eventualidad mientras se soluciona el impase.

- **Visibilidad:** Los ítems que conforman este elemento son:

    - Identificación: está enfocado en la definición de los elementos que permiten tener un conocimiento detallado acerca de los elementos que conforman la plataforma tecnológica.
    - Monitorización: permite la identificación e implementación de mecanismos que permitan conocer el estado de cada uno de los componentes de la infraestructura tecnológica.
    - Correlación: contribuye para que la información obtenida mediante la monitorización pueda ser evaluada, de tal forma que sea posible determinar anomalías o intrusiones que pudieran haber afectado diferentes elementos de la plataforma tecnológica. Esto se realiza

[12] WAF: por sus siglas en ingles *Web Application Firewall*, generalmente encaminado a la prevención de ataques tipo *sql injection y Cross-site Scripting* (XSS)

[13] HVAC: pos sus siglas en ingles *Heating, Ventilating and Air Conditioning*, básicamente es un sistema encargado de adaptar las condiciones ambientales de los centros de cómputo.

teniendo en cuenta que la información de los eventos de red se encuentra ubicada en un repositorio central, haciendo posible la identificación de amenazas potenciales que pueden ser mitigadas antes de que impacten el negocio.

- **Control:** Los ítems que conforman este elemento son:

    - Aseguramiento: está enfocado en la definición de las directrices que permitirán desarrollar procedimientos basados en buenas prácticas de configuración encaminados a la mitigación de vulnerabilidades inherentes a los diferentes elementos que conforman la plataforma tecnológica.
    - Segregación: con su implementación se busca la segmentar la red de datos del sistema de información, y la definición de perfiles para los servicios.
    - Resistencia: tiene como fin fortalecer la capacidad de recuperación de los elementos de la infraestructura ante eventos internos o externos.

6.8 ACUERDOS

El elemento de acuerdos tiene como objetivo principal establecer la línea de comunicación ente la Alta Gerencia y el Arquitecto de SI, además establece a la Alta Gerencia como cabeza visible en la formalización de la ASI, logrando de ésta manera que se involucre en el proceso; para ello se recomienda establecer los siguientes aspectos:

- Definición del rol Arquitecto de Seguridad de la Información: se podrá tener en cuenta lo descrito en el capítulo 7, donde básicamente se destaca que es importante el entendimiento que éste debe tener con la Alta Gerencia. Se debe lograr el uso de un lenguaje estratégico que permita el flujo de información transparente entre ambas partes, entendido y transmitido verticalmente de lo táctico a lo operacional en el contexto de negocio, permitiendo cumplir satisfactoriamente con las necesidades del negocio definidas por la Alta Gerencia. Se recomienda que este rol sea revisado al menos una vez al año, con base en los resultados arrojados en la ejecución de cada uno de los elementos del MASI.

- Definición de funciones y responsabilidades: con base en una revisión consensuada entre los dueños de los procesos del negocio, el Arquitecto de SI y la Alta Gerencia, redefinen las funciones de los diferentes cargos existentes en la organización, con el fin de incluir dentro de estas responsabilidades la alineación con el cumplimiento de los requerimientos de seguridad.

- Establecer prioridades: mediante los procesos de análisis de riesgos y revisión y evaluación se identifican dentro del negocio riegos y puntos críticos que van a entorpecer el normal funcionamiento de la ASI, y para evitar que esto suceda es importante que se definan los niveles de inversión en cuanto a las acciones que serán ejecutadas para su tratamiento. Teniendo en cuenta que estas acciones pueden ser priorizadas con base en la matriz de riesgos, dentro de éstas acciones está contemplado el hecho que la organización con pleno conocimiento de lo que esto implica decida asumir el riesgo, es decir, no ejecutar ninguna acción para el tratamiento de los riesgos o puntos críticos identificados, o por el contrario, apoyar completamente la ASI y por ende, el mejoramiento del nivel de seguridad de la organización.

- Materialización del compromiso: tanto la Alta Gerencia como el Arquitecto de SI deben estar comprometidos en la definición de tareas conjuntas para cumplir con los objetivos del negocio y de seguridad, de tal manera que si la Alta Gerencia invierte en los proyectos de seguridad propuestos, estos sean ejecutados teniendo en cuenta que cumplan con las expectativas del negocio, logrando que esto trascienda a cada uno de los actores del negocio.

- Definición el nivel de inversión: la Alta Gerencia debe definir dentro del presupuesto, rubros que apoyen la formalización de los compromisos y de las prioridades expuestas por el Arquitecto de SI, de tal manera que se corrobore el compromiso adquirido en la implantación del MASI.

- Participación del Arquitecto de SI dentro de las actividades definidas en la agenda de trabajo de la Alta Gerencia: para conocer y entender cuáles son las expectativas del negocio y así trazar un plan de trabajo en el marco de la seguridad de la información acorde o alineado con las expectativas del negocio, al Arquitecto de SI se le debe dar la oportunidad de participar activamente de las diferentes reuniones que la Alta Gerencia realice, para que de esta manera pueda interiorizar las necesidades del negocio y llevarlas a la ASI. Por otro lado, esto permite que el Arquitecto de SI pueda realizar una rendición de cuentas alineado su agenda y la de su equipo de trabajo (área de seguridad) con la de Alta Gerencia, con ello mediante un lenguaje estratégico dar a conocer el estado de los proyectos de seguridad y en general del MASI.

7 ARQUITECTO DE SEGURIDAD DE LA INFORMACIÓN

Hoy por hoy el contexto en el cual se desarrolla el negocio se encuentra sumido en un incesante cambio de las teorías y modelos de administración. Esto ha conllevado a que los profesionales tengan que adaptar sus estructuras mentales, su formación y sus habilidades a cargos enmarcados en un contexto cambiante cada vez más exigente y competido.

La Seguridad de la Información no es ajena a las nuevas exigencias del contexto de los negocios, realmente es todo lo contrario. Debido a la tendencia del negocio en incorporar tecnologías para la transmisión, almacenamiento y procesamiento de la información; se hizo necesario repensar el valor de la información para el negocio a tal punto que ésta no es considerada como un activo avalorado, sino como un activo con valor para el negocio el cual es necesario asegurar. Para ello se exigen competencias en cuanto a: formación, habilidades y conocimientos.

En una primera revisión, esta necesidad parecía estar resuelta con el concepto de un profesional CIO (Chief Information Officer) cuyo trabajo está enmarcado en diseñar e implementar iniciativas de TI, mediante una visión y liderazgo proactivas que conlleven a que la idea de negocio se mantenga competitiva en el mercado. El CIO logra materializar esto mediante [3]:

- La alineación la política de TI con las estrategias de TI y las estrategias del negocio.
- La planeación tecnológica de los procesos de negocio, incluido la definición del responsable y los colaboradores.
- La alineación de las aplicaciones (nuevas y existentes) con las iniciativas del negocio.
- Las decisiones de inversión y operación en cuanto el diseño e implantación de la infraestructura de TI.
- La decisión frente a la tercerización en la prestación de servicios de TI.
- El establecimiento de relaciones estratégicas de TI para el negocio entre proveedores y consultores.
- La transferencia de tecnología para clientes y proveedores con el fin de aumentar la rentabilidad y los ingresos.

- El establecimiento de mecanismos de seguridad en los dispositivos de la infraestructura de TI, con el fin de reducir el riesgo en un nivel manejable y aceptable.
- La capacitación a los usuarios de TI asegurando el uso productivo de los sistemas de información nuevos y existentes.

En conclusión el trabajo del CIO es completo y estratégico, más aún teniendo en cuenta que éste es miembro de Junta Directiva de la organización. La revisión efectuada referente al rol del CIO permite concluir que éste solamente enmarca su trabajo a nivel de TI, pese a tener un valor agregado al alinear TI con las estrategias del negocio, pero esto dentro del esquema general del MASI no es suficiente, debido a que el CIO podría estar descuidando puntos claves dentro de la ASI.

Para que MASI tenga un norte es necesario pensar en una persona con el nivel de conocimiento adecuado, es decir, que su formación, conocimiento y habilidades complementen las del CIO a través de lo que se denomina **ARQUITECTO DE SEGURIDAD DE LA INFORMACIÓN**, el cual al ser un concepto relativamente nuevo no hay una directriz clara que lo defina.

MASI define al Arquitecto de SI como aquella persona con competencia a nivel de: definición de normativas, conocimiento en estrategias de negocio, tecnologías de la información y gestión de seguridad (ver Figura 21). A continuación se detallan las funciones, formación y roles por cada una de las competencias.

Figura 21 Competencias del Arquitecto de Seguridad de la Información.

Tabla 5 Formación, Funciones y Roles del Arquitecto de SI para la competencia de Estrategias del Negocio

Tabla 6 Formación, Funciones y Roles del Arquitecto de SI para la competencia de Normativa Corporativa

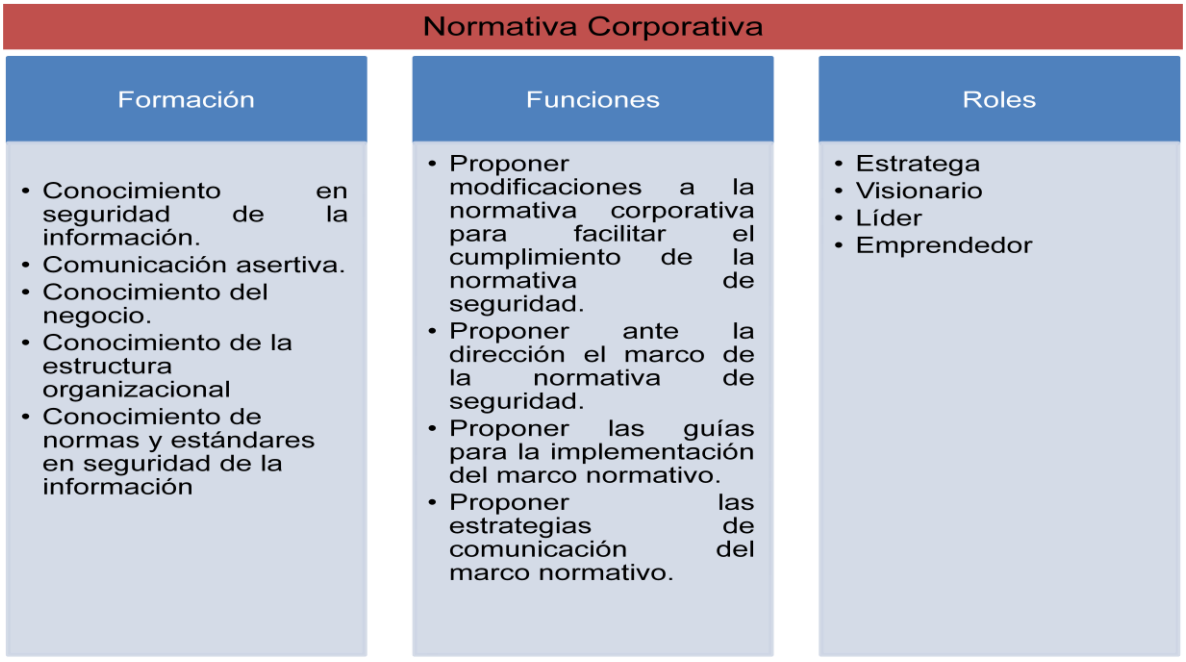


Tabla 7 Formación, Funciones y Roles del Arquitecto de SI para la competencia de Tecnologías de Información

Tecnologías de la Información		
Formación	**Funciones**	**Roles**
• Conocimientos en plataformas tecnológicas. • Conocimientos en nuevas tecnologías de la información. • Conocimientos en seguridad de la información. • Conocimiento en seguridad informática.	• Proponer soluciones de tecnología que agilicen los procesos de negocio de la compañía. • Incorporar procedimientos de seguridad en la implantación y mantenimiento de la plataforma tecnológica. • Proponer soluciones basadas en el conocimiento del negocio. • Promover los procesos de gestión documental.	• Estratega • Visionario • Líder • Emprendedor • Investigador

Tabla 8 Formación, Funciones y Roles del Arquitecto para la competencia Gestión de la ASI

Gestión de ASI		
Formación	**Funciones**	**Roles**
• Conocimiento en metodologías de mejora continua. • Conocimiento en gestión de riesgos. • Conocimientos en gestión de incidentes. • Conocimiento en procesos de entrenamiento. • Conocimiento en gestión de vulnerabilidades.	• Proponer el procedimiento para la gestión de riesgos. • Proponer el procedimiento para la gestión de incidentes. • Proponer las actividades a desarrollar para los planes de entrenamiento en seguridad de la información. • Propender por la actualización y mantenimiento de los elementos de ASI. • Definir las actividades a realizar para la ejecución de pruebas de vulnerabilidades. • Implementar y operar la Arquitectura de Seguridad de la Información.	• Organizado • Metódico • Estratega • Visionario • Líder • Emprendedor

CONCLUSIONES

- La Arquitectura de Seguridad de la Información es un esquema administrativo interdisciplinario, por tal razón debe estar en constante realimentación, ello le permitirá evolucionar de la mano del crecimiento del negocio y su entorno; con ello se garantiza que la Arquitectura de Seguridad de la Información cumpla y está alineada con las necesidades del negocio.

- La gestión del modelo de arquitectura de seguridad de la información permite el mejoramiento continuo de los diferentes elementos que lo componen, por tanto es indispensable que las actividades definidas en el mismo se ejecuten de manera organizada.

- MASI permite establecer el canal de comunicación necesario para alinear la agenda interna de la Alta Gerencia con la del Arquitecto de SI, con el ánimo de atender las necesidades e invertir en los asuntos concernientes a la Seguridad de la Información.

- El marco normativo establece la política y las directrices de seguridad de la información las cuales reflejan las expectativas (pretensiones, alcance) de la Alta Gerencia, por ello deben estar redactadas en términos generales de forma que sean entendibles por todos los actores del negocio.

- Las normas definen el comportamiento de estricto cumplimiento por parte de los actores del negocio (usuarios, proveedores, clientes, entre otros) y los procedimientos reflejan el cómo, es decir, las acciones para cumplir con las normas y deben ser aprobadas por la Alta Gerencia, además de establecer que su cumplimiento esté inmerso en la normativa organizacional.

- El conocimiento del negocio en el cual se implementará MASI es uno de los requisitos fundamentales que deberá cumplir el Arquitecto de SI y su equipo de trabajo, debido a que de ello depende que las decisiones tomadas estén alineadas con la estrategia del negocio.

- La asignación de funciones y roles al Arquitecto de SI de la información es de vital importancia, debido a que esto afianza la responsabilidad y encamina los esfuerzos para la implementación del MASI.

- El rol del Arquitecto de Seguridad de la Información pese a no tener un consenso que permita dar una definición, si es un cargo complejo y exigente, por tal razón las competencias deben estar sólidamente fundamentadas en la preparación y la experiencia del aspirante.

RECOMENDACIONES

- Desarrollar un plan de trabajo mancomunado entre las Directivas y el Arquitecto de Seguridad de la Información, que permita la inclusión y priorización de los temas concernientes a la Seguridad de la Información, y con ello materializar el compromiso y los niveles de inversión que está dispuesta a asumir la Alta Gerencia con respecto a la Seguridad de la Información y el funcionamiento del MASI.

- Definir planes de capacitación anuales a todos los involucrados en la operación de la Arquitectura de Seguridad de la Información, de tal manera que se refuercen las competencias y se propenda por el mejoramiento continuo de la misma.

- Definir reuniones de seguimiento en intervalos planificados para la realimentación de la Arquitectura de Seguridad de la Información, de tal manera que se pueda revisar que lo definido ha sido o no acertado para el mejoramiento continuo tanto del negocio como de la Arquitectura de Seguridad de la Información.

- El desarrollo y mejoramiento del negocio y su contexto suscita la necesidad de repensar la Arquitectura de Seguridad de la Información, de tal manera que esta se adapte a los nuevos requerimientos; por ello se recomienda a la Alta Gerencia tener presente en sus reuniones al Arquitecto de Seguridad de la Información, con el fin de que éste pueda asesorar a la Alta Gerencia en la inclusión de la seguridad de la información en cada uno de los proyectos que se encuentren analizando para el continuo desarrollo y mejoramiento de la idea de negocio.

- Incentivar en todos los actores (usuarios, proveedores, clientes, entre otros,) el cumplimiento de la normativa, así como la colaboración para lograr un ambiente adecuado para el funcionamiento de la arquitectura de seguridad de la información y los procesos de la misma.

- Tener en cuenta que el negocio debe contar con modelos de seguridad que apoyen su competitividad, MASI es uno de ellos ya que permite administrar (diseñar, planear, dirigir y controlar) los procesos estratégicos, tácticos y operacionales del negocio, de frente a la consolidación y permanencia de éste en el contexto de la competitividad de los mercados.

- Definir la metodología para la medición de la eficacia y la validación del MASI dentro de las organizaciones.

- Desarrollo de una aplicación que permita la sistematización de los registros referentes a los formatos definidos para la formalización de los procesos inherentes a los elementos que conforman MASI.

REFERENCIAS

[1] CANO, Jeimy. Arquitecturas de Seguridad Informática: *Entre la administración y el gobierno de la Seguridad de la Información*. En: SEMINARIO DE ACTUALIZACIÓN EN SEGURIDAD INFORMÁTICA. (2008: Bucaramanga). Documento Modulo I Seminario de Actualización en Seguridad Informática. Bucaramanga: Facultad de Ingeniería Informática, 2008, p 28.

[2]INSTITUTO COLOMBIANO DE NORMAS TECNICAS Y CERTIFICACION. NTC-ISO/IEC 27002. Bogotá. ICONTEC, 2007.

[3]KILLMEYER, Jan. Information Security Architecture: An Integrated Approach to Security in the Organization. 2ª edición. Estados Unidos: Auerbach, 2006. 393p

[4] IYER, Bala. GOTTLIEB, Richard. The Four-Domain Architecture: An approach to support enterprise architecture design. *Julio 21 de 2004.*Disponible en Web: http://www.research.ibm.com/journal/sj/433/iyer.html

[5] INTERNATIONAL PROFESSIONAL ASSOCIATION THAT DEALS WITH IT GOVERNANCE. COBIT 4.1. Estados Unidos. ISACA, 2007.

[6] INSTITUTO COLOMBIANO DE NORMAS TECNICAS Y CERTIFICACION. NTC-ISO/IEC 27001. Bogotá. ICONTEC, 2006.

[7] SysAdmin Audit, Networking and Security Institute. Information Systems Security Architecture: A Novel Approach to Layered Protection. Estados Unidos. SANS, 2004.

[8] PARADA, Diego. CALVO, July. Diseño de la arquitectura de seguridad de la red de la Universidad Pontificia Bolivariana. Bucaramanga, 2008, 219p. Proyecto de grado (Ingeniería en Informática). Universidad Pontificia Bolivariana. Facultad de Ingeniería Informática.

[9] DE, Zuani. ELIO, Rafael. Introducción a la administración de organizaciones. 1ª edición. Argentina: Valletta, 2005. 498p.

[10] “Definición del plan de desarrollo”, Enero de 2010. Disponible: http://definicion.de/plan-de-desarrollo/.

[11] MICROSOFT. Academia Latinoamericana de Seguridad Modulo 3. MICROSOFT, Estados Unidos. 2006.

[12] FIRMA-E. Guía para la elaboración del marco normativo de un sistema de gestión de la seguridad de la información (SGSI). España. FIRMA-E, 2007.
[13] MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS. Experiencias en el cumplimiento de la DA 669/04. Argentina. Ministerio de Justicia y Derechos Humanos.

[14] ROBBINS, Stephen. COULTER, Mary. Administración. 8ª edición. Madrid: Prentice Hall, 2006, 640p

[15] HOFFMAN, Douglas. BATESON, John. Fundamentos de marketing de servicios: conceptos, estrategias y casos. 2ª edición. Mexico: Thomson, 2003, 569p.

[16]VAN DEN BERGHE, Édgar. Gestión y gerencia empresariales aplicadas al siglo XXI. 1ª edición. Bogotá: ECOE, 2005, 247p.

[17] "Aspectos Éticos de Seguridad de la Información, notas de clase para Especialización en Seguridad Informática, Facultad de Ingeniería Informática, Universidad Pontificia bolivariana Seccional Bucaramanga, Julio de 2009

[18] CANO, Jeimy. Computación forense: descubriendo los rastros informáticos. 10ª edición. México: Alfaomega, 2009, 329p.

[19] "Definición de Metodología", Enero de 2010. Disponible: http://definicion.de/metodologia/.

[20] Almanza, Andrés. Seguridad en Redes y Sistemas Operativos. Universidad Pontificia Bolivariana, Colombia. 2009.

[21] Mora, Cristian. "Implementación de Sistemas de Información Seguros" [San Pedro Sula, Honduras]: Julio de 2005. Disponible en Web: www.iimv.org/actividades2/05Tecnolog/Microsoft.ppt.

[22] Cisco. Cisco SAFE Solution Overview. Cisco, Estados Unidos. 2009.

[23] HELLRIEGEL, Don. JACKSON, Susan. SLOCUM, Jhon. Administración un Enfoque Basado en Competencias. 10ª edición. México: Thomson, 2005. 519p.

[24] SARUBBI, Juan Pablo. Técnicas de Defensa: Mecanismos Comunes Bajo Variantes del Sistema Operativo UNIX. Buenos Aires, 2008, 06p. Proyecto de grado (Licenciatura en Sistemas de Información). Universidad de Luján. Facultad de Licenciaturas.

[25] “IPSec (Internet Protocol Security)”, Junio de 2010. Disponible: IPSec (Internet Protocol Security).

ANEXOS

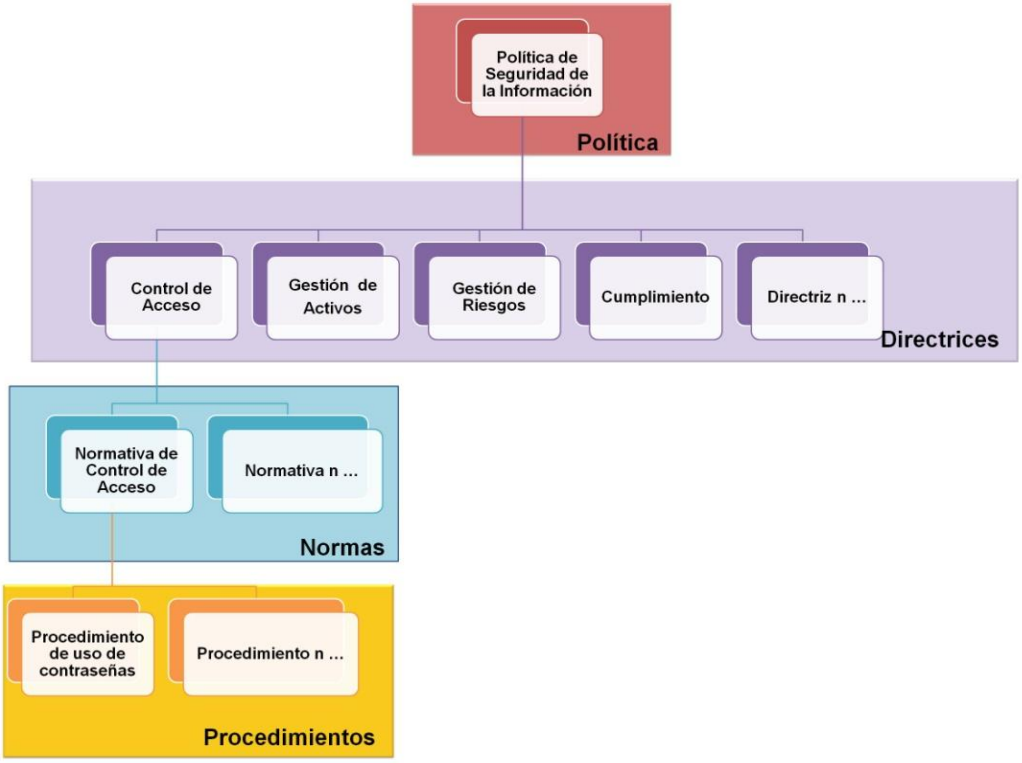
ANEXO A. FORMATO DE LEVANTAMIENTO DE INFORMACIÓN DE NEGOCIO

LevantamientodeInformaciónde Negocio.x

ANEXO B. CONSIDERACIONES MARCO NORMATIVO DE SEGURIDAD DE LA INFORMACIÓN

Lo descrito a continuación corresponde a la formalización de lo contemplado en el elemento marco normativo de MASI, el cual hace referencia a la creación de la política de seguridad de la información y los documentos que apoyen su cumplimiento.

Figura 22. Despliegue de la Política de Seguridad de la Información.



En los Anexos B.1.1 y B.2 se realiza el despliegue de la directriz referente al control de acceso, la normativa relacionada con la gestión de contraseñas y los procedimientos asociados al cumplimiento de esta normativa. Se debe tener en cuenta que esta información corresponde a una guía que puede ser empleada por las organizaciones, lo que significa que éstas deberán verificar la pertinencia de lo definido de acuerdo a sus requerimientos.

B.1. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La política de seguridad de la información nace de la preocupación de la Alta Gerencia por la protección de sus activos de información con base en el análisis

de sus estrategias del negocio, por tal razón la Alta Gerencia ha estudiado y avalado la implementación y aplicación del documento de "Política de Seguridad de la información". Es así como la política de seguridad de la Información busca establecer los lineamientos que enmarcaran el accionar de los usuarios en cuanto a la protección de la disponibilidad, integridad, y confidencialidad de los activos de información, bajo el marco referencial de la ISO 27002:2005, mediante la generación de estructuras mentales y culturales en torno a la Seguridad de la Información que conciencien a los usuarios de la necesidad de contar con mecanismos de protección, teniendo en cuenta buenas prácticas.

Por tanto, la política, sus directrices, normas, procedimientos y demás elementos normativos establecen lineamientos de obligatorio cumplimiento por empleados, contratistas y cualquier otro ente que establezca alguna relación con el negocio. Es responsabilidad de estos reportar los incidentes que atenten contra la seguridad de los activos de información.

El cumplimiento de las políticas no excluye el cumplimiento de las leyes que rigen en el país, la Alta Gerencia establecerá un plan de acción para la sensibilización de la política de tal manera que se facilite el entendimiento y aplicación por parte de los actores del negocio; para los cargos que requieran capacitación específica en materia de seguridad de la información, la Alta Gerencia avalará y dispondrá de los recursos necesarios para que los colaboradores inicien un proceso de formación.

El incumplimiento de la Política de SI es motivo de investigación disciplinaria por parte de los entes de control interno del negocio, serán ellos los responsables de investigar y dictaminar la sanción la cual deberá ser presentada a la Alta Gerencia. En caso que el involucrado sea un colaborador de control interno, la Alta Gerencia será la encargada de definir un equipo competente para la realización de la investigación. En caso que el incidente conlleve a un delito tipificado por la ley, el equipo de control interno informará a la Alta Gerencia quien deberá informar a las autoridades competentes para garantizar el debido proceso.

B.1.1. Directriz de Control de Acceso

La organización deberá proveer los recursos para la definición e implementación de mecanismos de seguridad para controlar el acceso a la información del negocio, independientemente de su ubicación y medio de almacenamiento. Los usuarios tienen la responsabilidad de seguir las normas y procedimientos definidos para el cumplimiento de la política.

B.2. NORMAS DE CONTROL DE ACCESO

A continuación se describen las normas de seguridad para el establecimiento de los controles de acceso, cada norma tiene asociado uno o más procedimientos los cuales detallan las actividades a desarrollar para el cumplimiento de la misma.

- **Norma 1**
  - **Descripción**
    - El área de seguridad de la información y el área de gestión de servicios de la información deberán definir los procedimientos, lineamientos de seguridad y buenas prácticas para mitigar los riesgos relacionados con los accesos no autorizados a los sistemas de información.
  - **Procedimientos asociados.**
    - Procedimiento de gestión de contraseñas para usuarios
- **Norma 2**
  - **Descripción**
    - Los usuarios autorizados son responsables de la correcta administración de sus permisos de acceso y de la aplicación de las normas y procedimientos definidos para tal fin.
- **Norma 3**
  - **Descripción**
    - La organización deberá proveer los recursos para que los procesos de tecnología y seguridad de la información definan e implementen los mecanismos de seguridad para controlar el acceso a los servicios de red.

- **Norma 4**
  - **Descripción**
    - La organización deberá proveer los recursos para que los procesos de tecnología y seguridad de la información definan e implementen los mecanismos de seguridad para controlar el acceso al sistema operativo.
  - **Procedimientos asociados**
    - Procedimiento de Uso de contraseñas
- **Norma 5**
  - **Descripción**
    - La organización deberá proveer los recursos para que los procesos de tecnología y seguridad de la información definan e implementen los mecanismos de seguridad para controlar el acceso a la información contenida en las aplicaciones y dentro de ellas.
- **Norma 6**
  - **Descripción**
    - La organización deberá proveer los recursos para que los procesos de tecnología y seguridad de la información definan e implementen los mecanismos de seguridad para controlar el acceso a la información cuando se empleen los servicios de computación móvil y trabajo remoto.

B.3. PROCEDIMIENTO DE USO DE CONTRASEÑAS

B.3.1. DECLARACIÓN DE CONFIDENCIALIDAD DE CONTRASEÑAS

Una vez se han asignado los permisos a los usuarios en los servicios de red, éste deberá firmar una nota de compromiso en el cual se establece que el usuario deberá mantener la confidencialidad de sus contraseñas, este requisito es indispensable a fin de evitar los accesos no autorizados a los sistemas de información.

A continuación de muestra la nota de compromiso respecto la declaración de confidencialidad de contraseñas.

Premisa: Se debe tener en cuenta que en aquellas organizaciones que no se cuente con mecanismo automáticos para determinar la fortaleza de las contraseñas, dentro de la declaración de confidencialidad se deberá considerar como responsabilidad del usuario la definición de contraseñas fuertes.

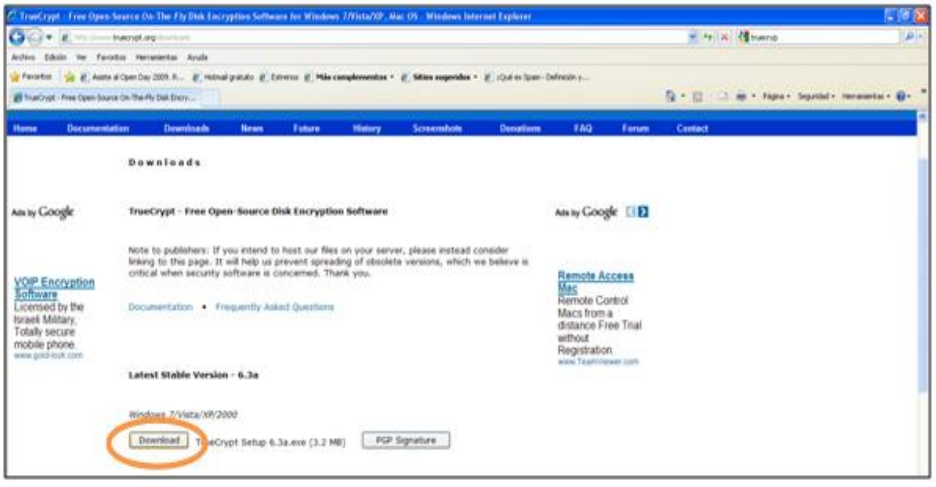
Yo _____ identificado con número de cédula _____ de _____, vinculado con la organización en el área de _____ me comprometo a mantener en secreto las contraseñas que me han asignado para el acceso a los diferentes sistemas de información y servicios de red.

_____
Firma
CC.

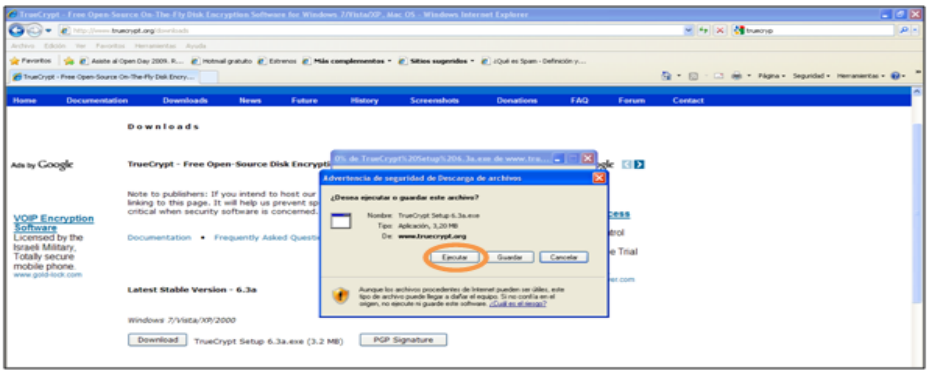
B.3.2. ALMACENAMIENTO DE CONTRASEÑAS[14]

En caso que se requiera almacenar un archivo con contraseñas en su equipo de cómputo se recomienda emplear un software que permita el cifrado de archivos en el disco duro, a continuación se presenta la explicación de cómo realizar este proceso con el software denominado *TrueCrypt*. Se seleccionó esta herramienta debido a que es de uso libre.

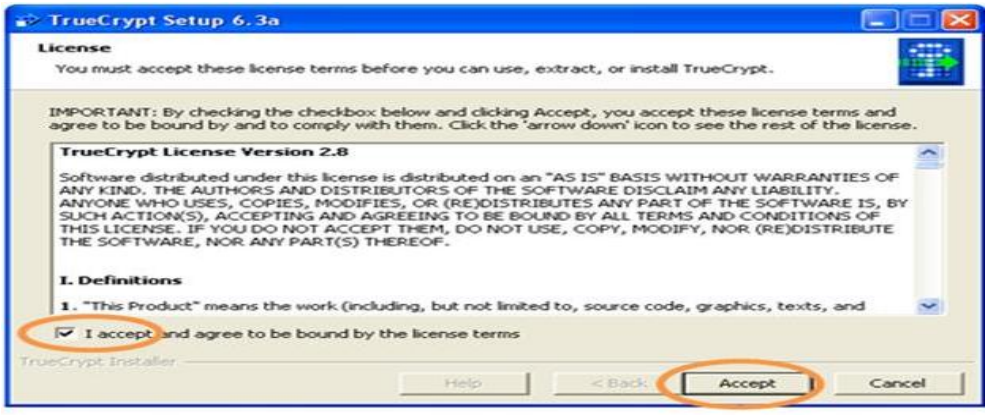
- Descargar el software T*rueCrypt* disponible en el enlace: http://www.truecrypt.org/downloads. Este software es empleado para crear unidades cifradas en el disco duro.



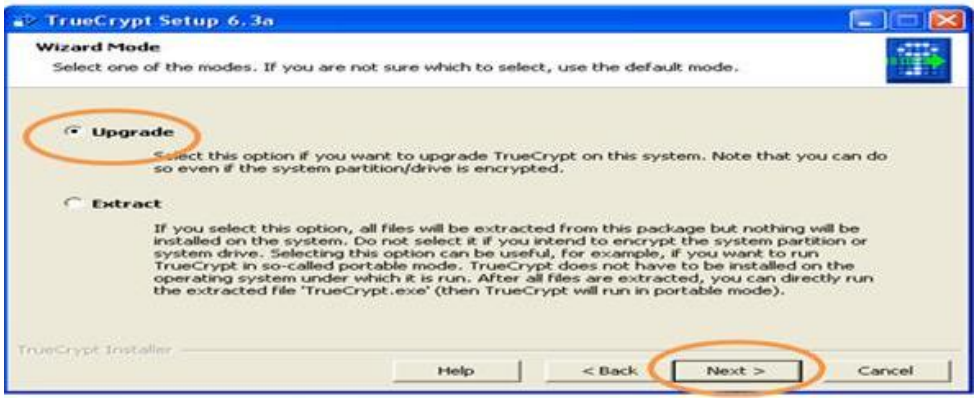
[14] Este procedimiento debe ser empleado solo cuando se considere absolutamente necesario



- Instalar el Software
- **Aceptar los términos de referencia**

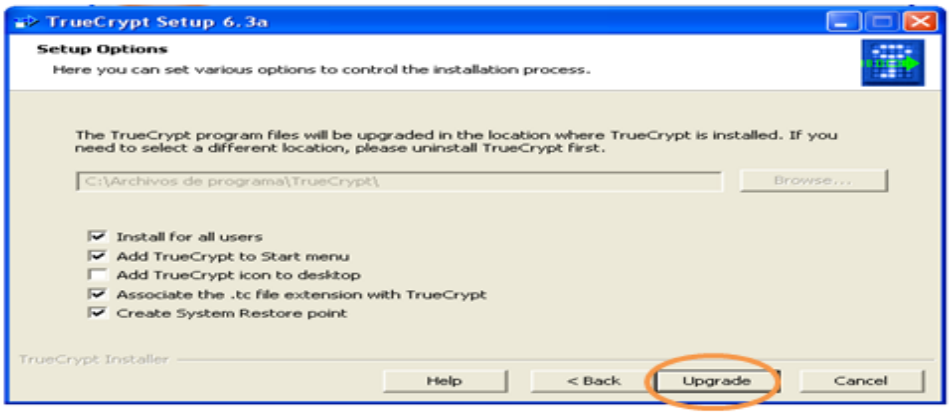


- **Selección del modo**
  - Se recomienda dejar las opciones por omisión del software.

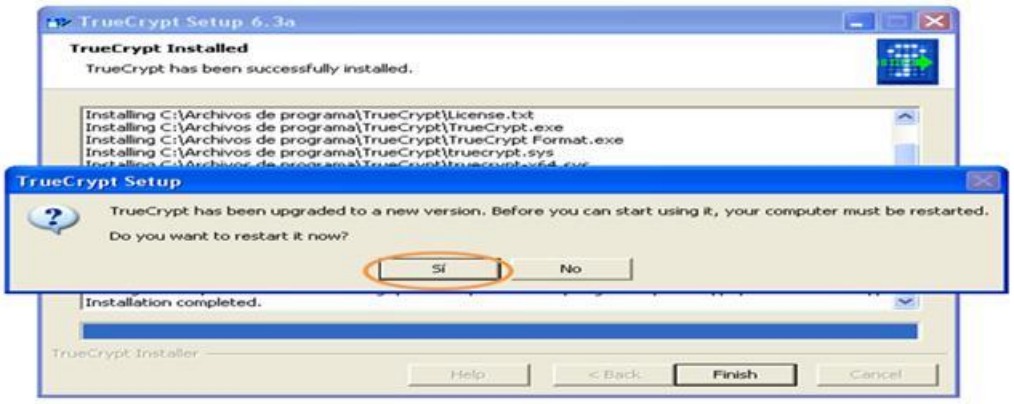


- **Opciones de administración**

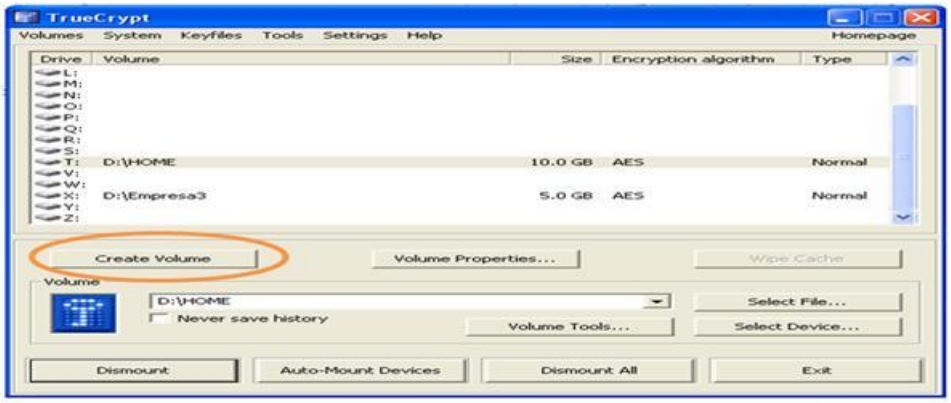
Se recomienda dejar las opciones por omisión del software.

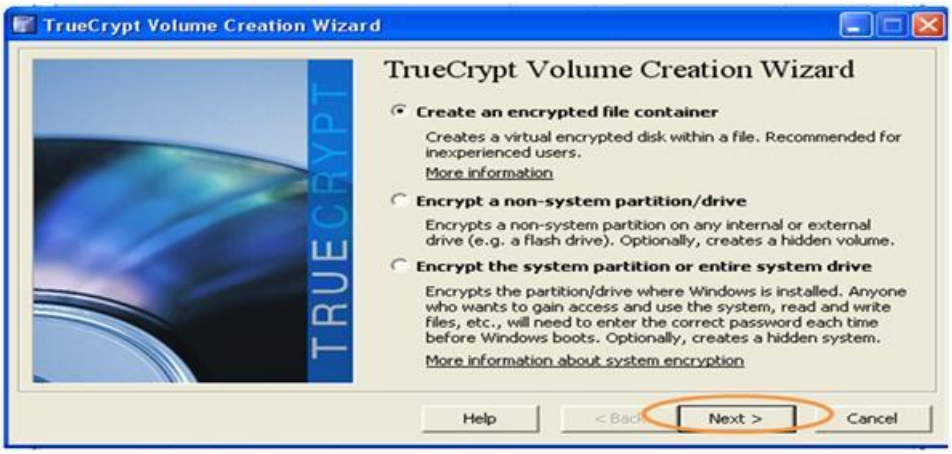


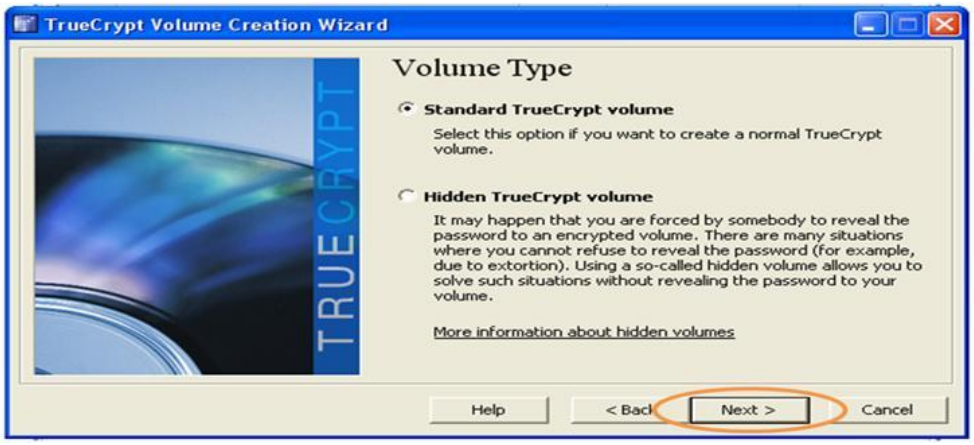
- **Instalación finalizada**



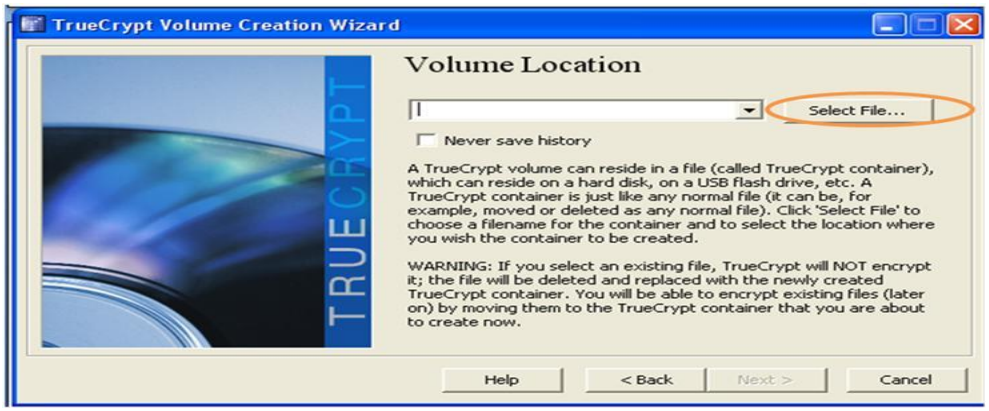
- **Creación de la unidad cifrada**



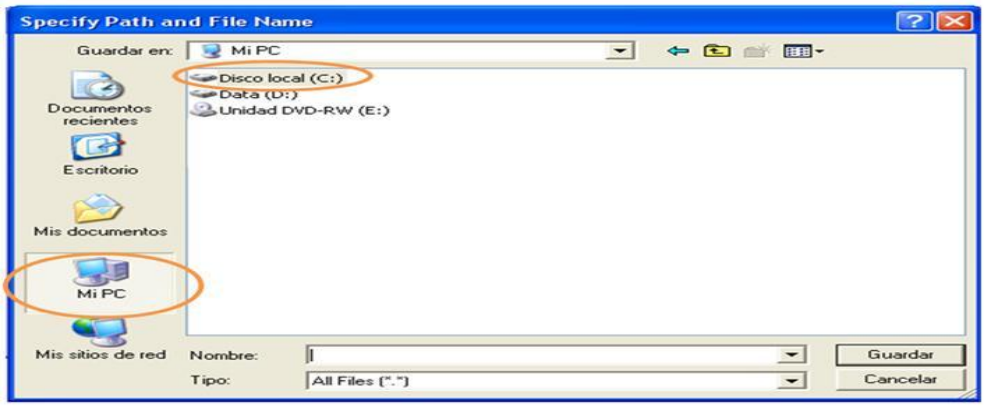




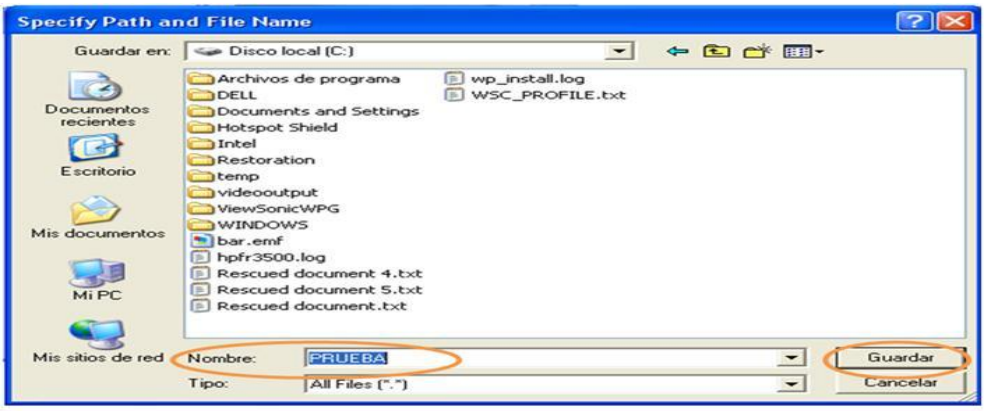
- **Selección de la ubicación de la unidad cifrada**



Seleccionar Mi PC y seleccionar la partición del disco en el cual se quiere almacenar la unidad cifrada.



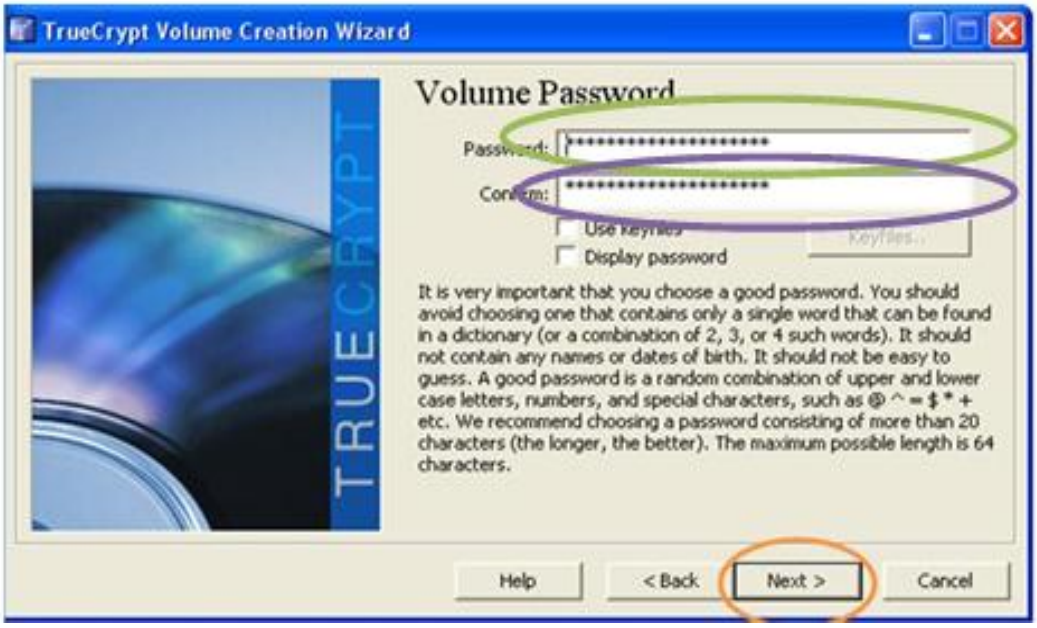
Escribir el nombre con el cual se quiere almacenar la unidad cifrada



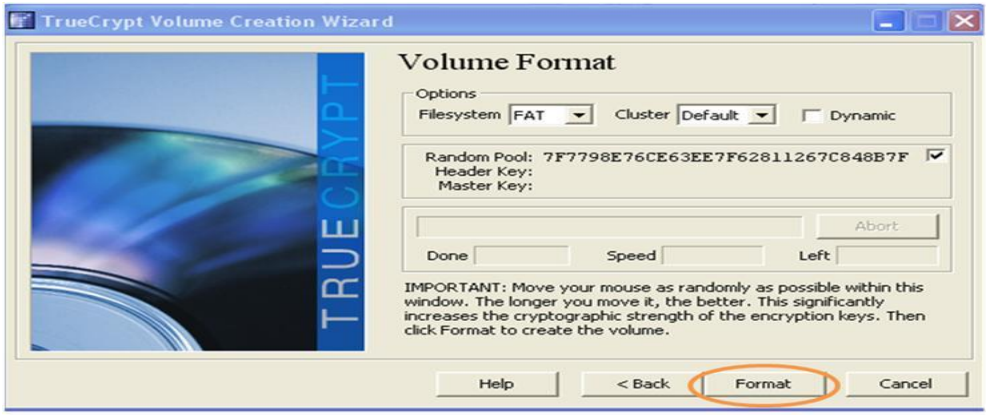
Seleccionar el tipo de algoritmo de cifrado, para ello se puede dejar la configuración por omisión de la herramienta.

Seleccionar el tamaño de la unidad cifrada. En el espacio demarcado con el círculo verde se digita el tamaño que se crea conveniente en éste. Como se requiere exclusivamente para almacenar un archivo de contraseñas, se reserva un espacio pequeño.

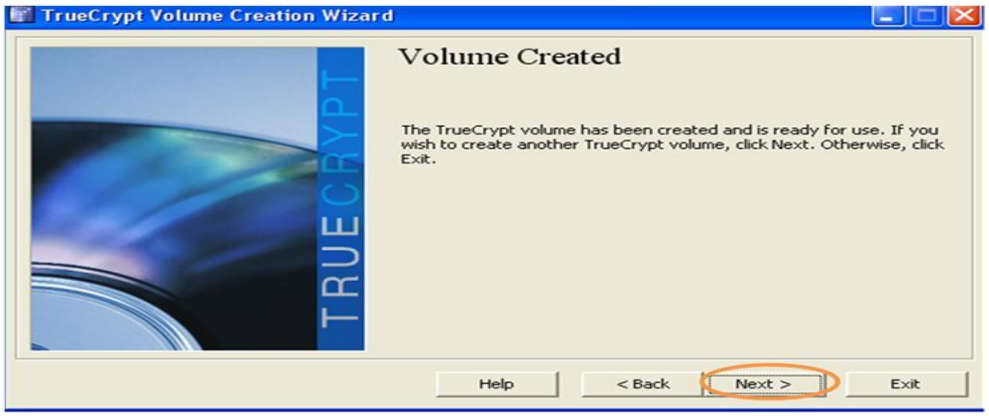
En el espacio demarcado con el círculo verde digitar la contraseña, se debe tener en cuenta que el olvido de esta contraseña trae consigo la pérdida de la disponibilidad de la información almacenada en la unidad, debido a que no existe en la herramienta procedimiento de recuperación de contraseña.
En el espacio demarcado con el círculo morado se escribe nuevamente la contraseña:

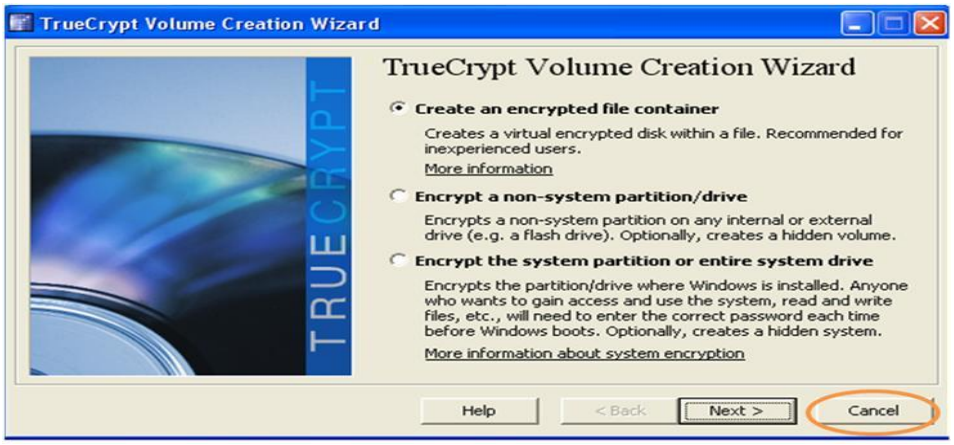


- **Formato de la unidad cifrada**

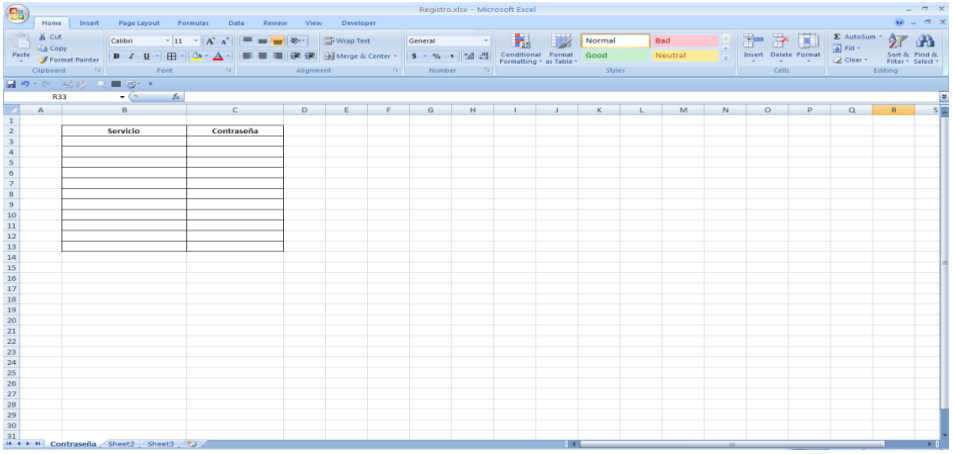


- **Unidad creada exitosamente**

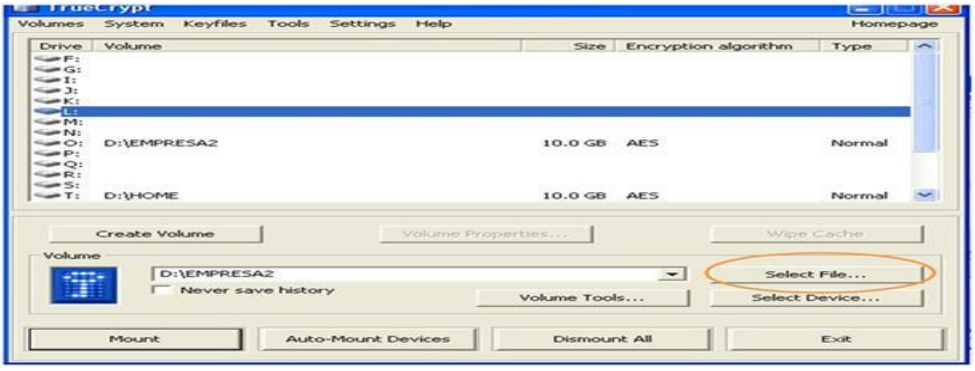




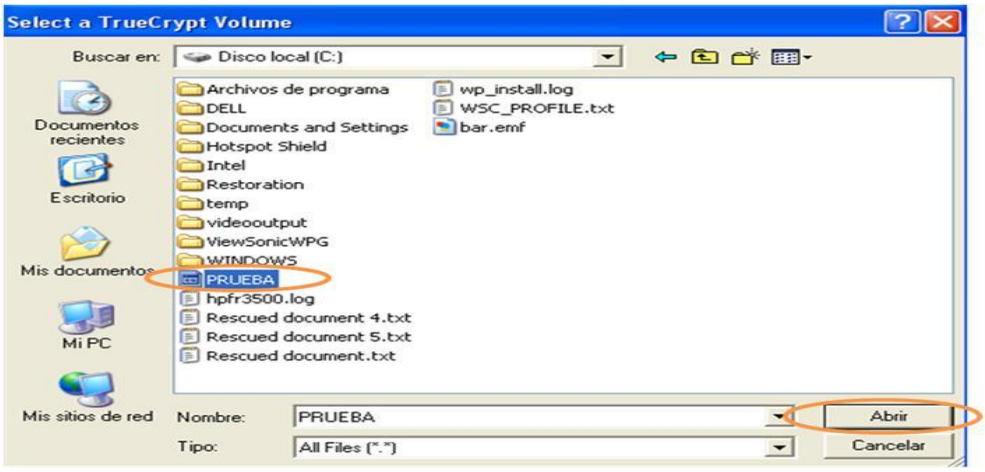
Crear un archivo preferiblemente en Excel el cual puede ser empleado para detallar el nombre del servicio y la contraseña asociado al mismo.



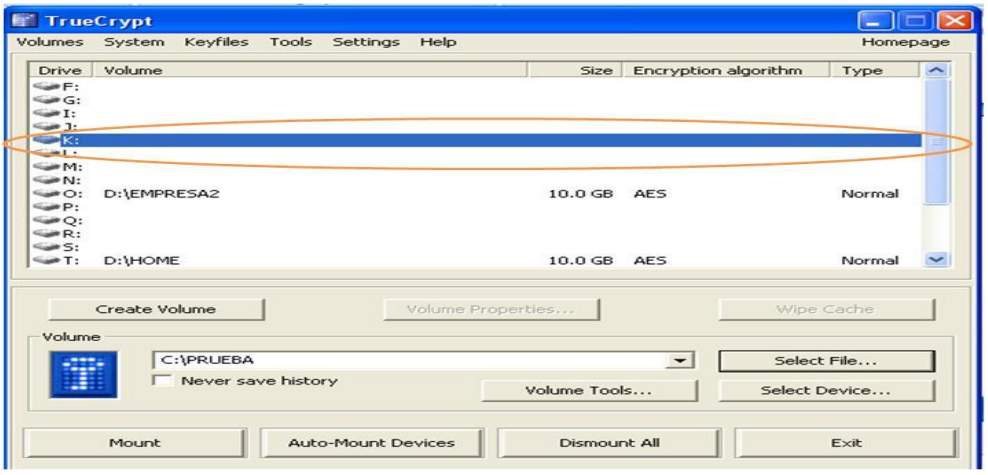
- **Montar la unidad cifrada en la cual se almacenará el archivo con contraseñas**



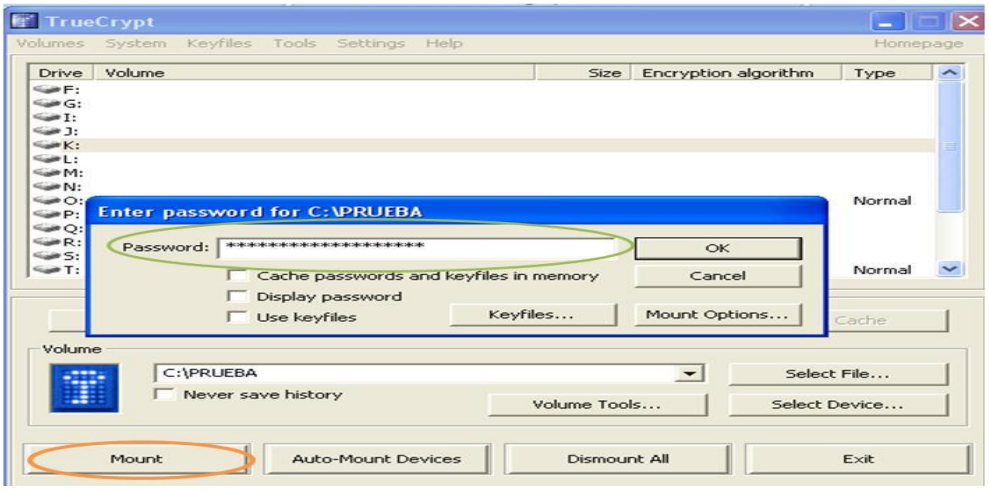
Buscar la unidad que se creó con anterioridad en la partición C:/ del disco.

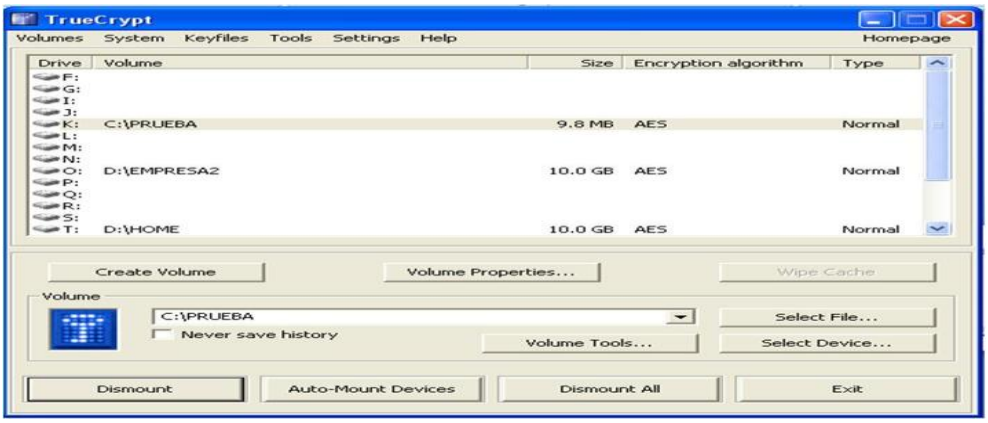


Seleccionar el nombre de unidad que se le quiere dar a la partición cifrada.

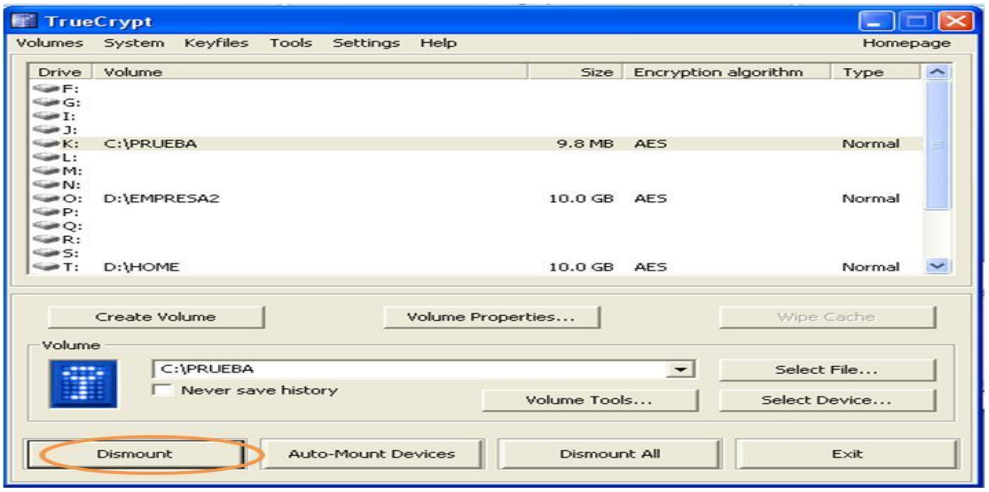


Una vez se ha seleccionado el nombre de la unidad se selecciona la opción *Mount* resaltada por el círculo naranja, luego de ello, se habilita una ventana en la cual se debe digitar la contraseña en el espacio demarcado por el círculo de color verde.

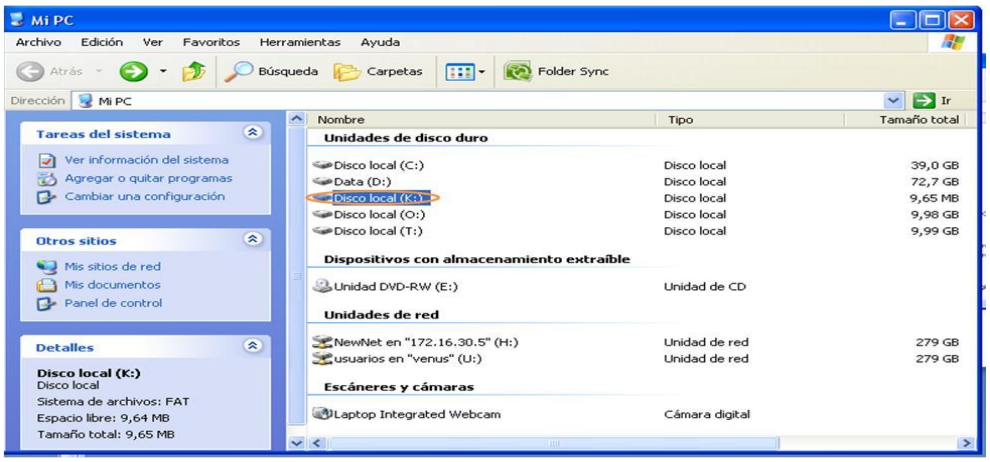


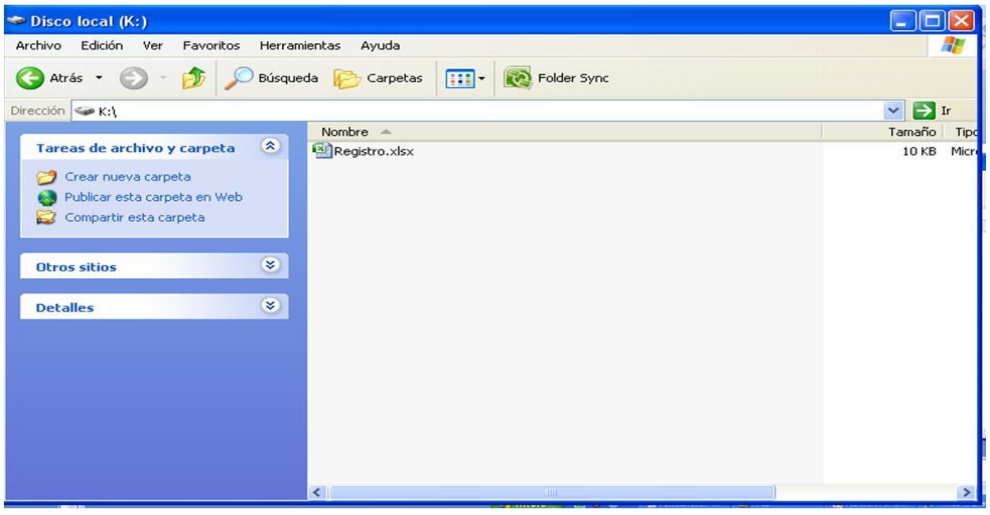


Para desmontar la unidad cifrada, se debe seleccionar la opción que está demarcada por el círculo naranja *Dismount*.



- **Ubicación de la unidad**





B.3.3. USO DE CONTRASEÑAS

Las contraseñas son de uso personal e intransferible, para ello los usuarios deben abstenerse de darlas a conocer a terceros, de mantenerlas escritas o almacenadas en lugares que sean de fácil acceso a intrusos. Las contraseñas deben cumplir las siguientes características:

- Se recomienda que la longitud de la clave debe ser mayor a ocho (8) caracteres.

- Evitar utilizar secuencias de letras o números que se encuentren seguidos en el teclado del computador como “qwertyui”, secuencias comunes como “abcdef” o el mismo carácter repetido varias veces como “aaaaaaaa”, “11111111”.

- Evitar que las contraseñas contengan: nombres comunes, datos personales, fechas de acontecimientos personales o palabras que se encuentren en diccionarios de cualquier idioma, por ejemplo: “elefante”, “sombrilla”, “password”, “alejandra”, “03031975”.

- Se recomienda que éstas sean modificadas en un término máximo de 90 días.

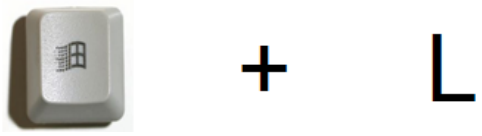
- Se recomienda alternar mayúsculas y minúsculas, usar signos alfanuméricos por ejemplo:

    - M1ca$aL1nda (es una forma de escribir “Mi casa linda”)
      mGjFaL10am (son las iníciales de la frase “me gusta jugar futbol a las 10 am”).

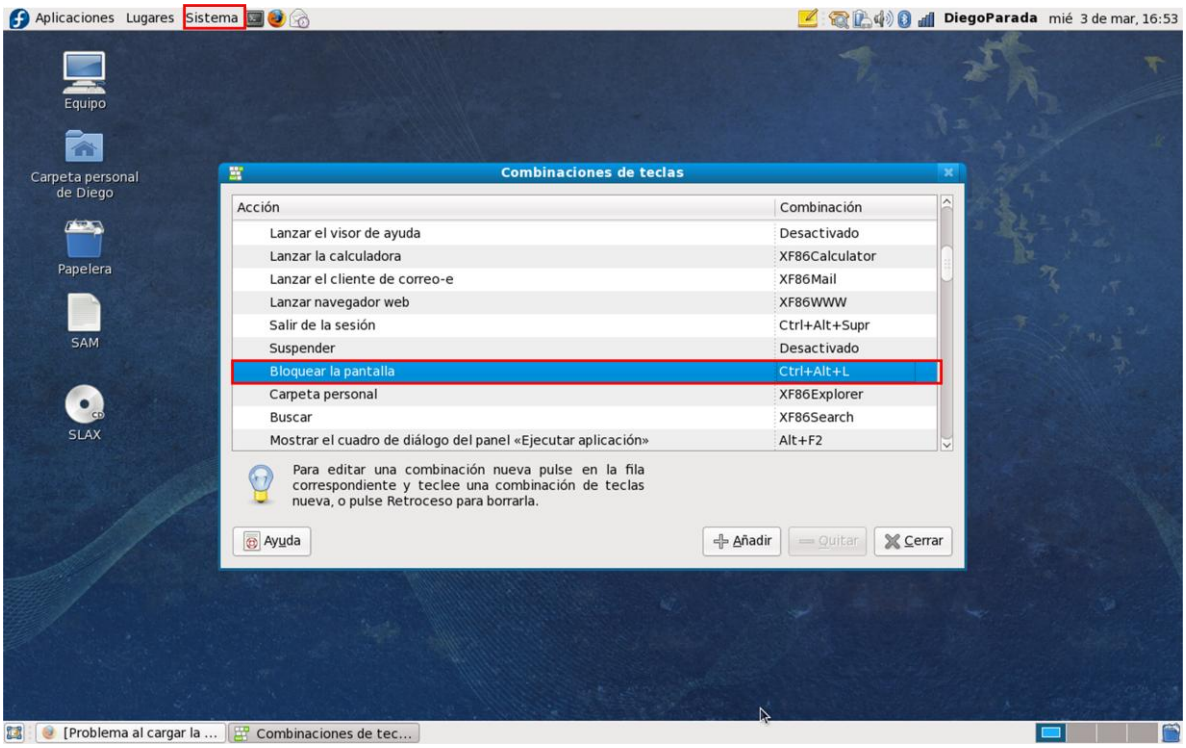
B.3.4. EQUIPO DE USUARIO DESATENDIDO

Los usuarios deben evitar dejar el computador sin bloquear si se van ausentar de su puesto de trabajo.

- Para bloquear la sesión en sistemas operativos Windows emplear la combinación de teclas mostrada a continuación:



- En sistemas operativos Linux, a diferencia de Windows, el bloqueo de sesión no es una opción predeterminada del Sistema Operativo, por ende hay que configurarla manualmente. En la barra de opciones se selecciona *Sistema* (recuadro rojo de la figura) y esto despliega un menú donde se localiza la opción *Combinación de Teclas*, como lo muestra la figura.



Para el ejemplo, la combinación de teclas configurada es:

B.3.5. ESCRITORIO DESPEJADO Y PANTALLA DESPEJADA

Se debe evitar colocar en lugares visibles la información que sea importante para el negocio ya que facilita al personal no autorizado tener acceso a la misma. Esta información deberá ser almacenada en un inmueble (archivador, caja fuerte, entre otros), que permita guardarla con las especificaciones de seguridad pertinentes al tipo de información.

ANEXO C. FORMATO DE INVENTARIO DE ACTIVOS

Activos.xlsx

ANEXO D. GENERALIDADES PARA DILIGENCIAMIENTO DEL FORMATO DE INVENTARIO DE ACTIVOS

- Diligenciar los campos de información general los cuales están compuestos por:

  - Nombre del proceso
  - Nombre de las personas que componen el equipo de trabajo
  - Nombre del líder del equipo de trabajo

    - Esta información permitirá conocer quiénes fueron los encargados de proporcionar la información para el diligenciamiento del formato de inventario de activos además del proceso en el cual fueron identificados.

- Tipo de activo: corresponde a una característica que permite determinar si este corresponde a:

  - Información: activos que corresponden a la memoria documental de las organizaciones (contratos, acuerdos, información general), procedimientos de operación (procedimientos de funcionamiento de servicios, aplicaciones, de recuperación), información de auditoría (registros de auditoría, información de investigaciones), planes de continuidad, entre otros [2].
  - Activos de software: herramientas de software empleadas por los colaboradores de organización para el cumplimiento de sus funciones dentro de las cuales se encuentran: Los desarrollos propios del negocio, las de tipo comercial, entre otras [2].
  - Activos físicos: todos los equipos de hardware, como por ejemplo: computadores, servidores, equipos de comunicaciones, medios removibles, plantas eléctricas, UPS, entre otros [2].
  - Servicios: servicios de tecnología, servicios públicos, aire acondicionado, calefacción, entre otros [2].
  - Personas: identificar los colaboradores de los procesos teniendo en cuenta sus calificaciones, habilidades y experiencia [2].
  - Intangibles: Activos como la reputación e imagen de la organización [2].

- Descripción: en este campo se digita la información referente al activo, la información que se considere pertinente o importante.

- Formato: identificar el formato (.doc, .xls, .dot, entre otros) del activo en caso que aplique.

- Ubicación: corresponde al lugar en el cual se encuentra almacenado el activo.

- Propietario: corresponde a la persona, área o proceso dueño del activo de información, es quien puede asignar permisos de acceso, niveles de acceso, y quien dispone la medidas de protección para el activo.

- Custodio: algunos activos en determinado momento pueden estar a cargo de personas, áreas o procesos diferentes a su propietario, por tal razón, es importante identificar cuáles activos de información están a cargo de alguien diferente a su propietario, debido a que este debe cumplir con las disposiciones de seguridad establecidas por su propietario.

- Importancia de las propiedades

  - Confidencialidad:

    - Confidencial: activo al cual solo tienen al acceso ciertas personas dentro de la organización. Los accesos son autorizados por el propietario de la información.
    - Uso de un Proceso: activo al cual tienen acceso todos los empleados de un proceso.
    - Uso Organizacional: activo al cual tiene acceso toda la organización.
    - Público: Activo al cual tienen acceso personas dentro y fuera de la organización.

  - Integridad:

    - Requerida: activo de información que por su importancia requiere un nivel de integridad alto (estados financieros, servicio web, entre otros).
    - No Requerida: activo de información cuyo nivel de integridad no es tan importante para el negocio (copias de documentos, entre otros).

  - Disponibilidad:

    - Alta: activo de información que el negocio requiere se encuentre disponible todo el tiempo disponible, de no ser así la organización podría ver afectada su operación.
    - Media: activo de información que de no estar disponible podría afectar la operación de uno o más procesos.
    - Baja: activo de información que de no estar disponible el impacto para la organización es mínimo.

- Importancia del Activo: corresponde al nivel de importancia del activo teniendo en cuenta el nivel de confidencialidad, integridad y disponibilidad de los mismos; para mayor información consultar en Anexo C en la pestaña Valor del Activo.
- Etiqueta del Activo: corresponde a la etiqueta que deberá ser dispuesta en los activos la cual permite determinar las medidas de protección del activo teniendo en cuenta su nivel de confidencialidad, integridad y disponibilidad.

Una vez se tenga el inventario de activos de información, es necesario analizar la información obtenida en las entrevistas y generar un documento donde se definan las medidas de protección de los activos teniendo en cuenta los niveles de clasificación en cuanto a las características evaluadas (confidencialidad, integridad y disponibilidad).

ANEXO E. CATÁLOGO DE AMENAZAS

Catálogo de Amenazas
Replicación de Malware
Fugas de Información
Alteración de la Información
Destrucción de la Información
Divulgación de la información
Vulnerabilidad de software (Servicios y Aplicaciones)
Software desactualizado (Servicios y Aplicaciones)
Acceso no Autorizado
Intercepción de Tráfico e Información
Ataques de denegación de servicio
Daño en discos de almacenamiento
Errores en la monitorización
Errores de configuración (Administradores)
Daño físico de dispositivos
Renuncia del Personal
Caída de los canales de comunicación
Ingeniería social
Ataques de monitorización (sniffing)
Abuso de privilegios de usuario
Robo de información
Indisponibilidad de personal

ANEXO F. CATÁLOGO DE VULNERABILIDADES

Catálogo de Vulnerabilidades
Falta de capacitación del personal
Falta de revocación de derechos de accesos
Deficiencias en la monitorización del cumplimiento de procedimientos
Deficiencias en la monitorización de equipos activos de red
Falta de mantenimientos
Inconformidad de los colaboradores
Falta de previsión de necesitadas tecnológicas
Almacenamiento inadecuado de los activos
Control inadecuado de cambios
Inadecuada gestión de usuarios
Inexistencia o inadecuada gestión de desarrollo de software
Inexistencia o inadecuada gestión de vulnerabilidades
Falta de protección contra virus o códigos maliciosos
Inexistencia de procedimientos para el uso del software o herramientas de cifrado
Inexistencia o falta de gestión de red
Inexistencia o falta de normas de gestión de copias de seguridad
Falta de procedimientos o instructivos para el tratamiento de la información
Inadecuada protección de medios removibles
Falta de sensibilización de Seguridad de la Información

ANEXO G. TABLA VALORES DE PROBABILIDAD E IMPACTO

G.1. TABLA DE VALORES DE PROBABILIDAD

Los valores de la probabilidad definidos en la siguiente tabla podrán ser modificados por cada organización. Para el caso del MASI estos son los sugeridos:

Probabilidad		Valor
Muy Alto	Evento que ocurre más de trece veces en el año.	20
Alto	Evento que ocurre de cinco a doce veces en el año.	15
Medio	Evento que ocurre de dos a cuatro veces en el año.	10
Bajo	Evento que nunca ocurre u ocurre una vez en el año.	5

G.2. TABLA DE VALORES DE IMPACTO

Los valores de la impacto definidos en la siguiente tabla podrán ser modificados por cada organización. Para el caso del MASI estos son los sugeridos:

Impacto		Valor
Catastrófico	Consecuencias de la materialización del riesgo que pueden afectar la operación del negocio por largo tiempo.	20
Mayor	Consecuencias de la materialización del riesgo que pueden afectar la operación de más de un proceso de negocio.	15
Medio	Consecuencias de la materialización del riesgo que pueden afectar la operación de un proceso de negocio.	10
Bajo	Consecuencias de la materialización del riesgo que pueden afectar la operación de una persona o área del negocio.	5

G.3. MATRIZ DE VALORACIÓN DE RIESGO

Riesgos.xlsx

ANEXO H. INSTRUCTIVO DILIGENCIAMIENTO DE LA MATRIZ DE RIESGO

H.1 Valoración del Riesgo Intrínseco

- Identificador del riesgo: número consecutivo que identifica el riesgo

- Activo: esta información debe ser consultada en el inventario de activos de información.

- Descripción: esta información debe ser consultada en el inventario de activos de información.

- Amenaza: dependerán del activo de información que se esté analizando. Esta información es proporcionada en conjunto entre el propietario y el custodio del activo de información. Para identificarlas se recomienda tener en cuenta el catálogo de amenazas definido (Anexo E).

- Vulnerabilidad: dependerán del activo de información que se esté analizando. Esta información es proporcionada en conjunto entre el propietario y el custodio del activo de información. Para identificarlas se recomienda tener en cuenta el catálogo de amenazas definido (Anexo F).

- Probabilidad: la probabilidad debe ser establecida para cada par amenaza vs. vulnerabilidad, este valor dependerá de la posibilidad de que la amenaza se aproveche de la vulnerabilidad y se materialice el riesgo. Para establecer este valor se debe tener en cuenta la escala de probabilidad definida en el Anexo G.1.

- Impacto: el impacto debe ser establecido para cada par amenaza vs. vulnerabilidad, este valor dependerá de las consecuencias de materialización de un riesgo. Para establecer este valor se debe tener en cuenta la escala de impacto definida en el Anexo G.2.

- Criticidad: la criticidad del riesgo está dada por la relación entre el impacto y la probabilidad que materialización del riesgo. Para ello se debe emplear la matriz de riesgos, teniendo en cuenta los niveles de riesgo que son: Extremo, Tolerable y Aceptable.

H.2 Valoración del riesgo residual

- Selección de controles: para la selección de controles se debe tener en cuenta el par amenaza vs. vulnerabilidad y el activo de información que se está analizando.

- Probabilidad: teniendo en cuenta los controles identificados establecer el nuevo nivel de probabilidad.

- Impacto: teniendo en cuenta los controles identificados establecer el nuevo nivel de impacto.

- Opciones de tratamiento: las opciones de tratamiento son:

    - Evitar el riesgo: esta opción es la menos aconsejable debido a que se basa en la eliminación de la fuente de riesgo, lo que en la mayoría de los casos es imposible, debido a que para lograrlo se tendría que no emplear el activo que lo genera.

    - Reducir el riesgo: consiste en la definición e implementación de planes de tratamiento para la mitigación del riesgo.

    - Transferir el riesgo: esto consiste en la compra de pólizas, o el establecimiento de contratos con terceros para el manejo de las actividades que generen del riesgo de tal forma que el tercero será el encargado de gestionarlo.

    - Asumir el riesgo: no tomar ninguna acción frente al riesgo, es decir que se asumen las consecuencias de su materialización.

- Identificador del plan: seleccionar los planes de tratamiento enfocados en la mitigación del riesgo y asociarlos al riesgo

- Planes de tratamiento de riesgos: los planes de tratamiento se definen teniendo en cuenta los riesgos que se encuentran en los niveles no aceptables (extremo y tolerable) y que cuya opción de tratamiento sea reducir el riesgo. para ello se debe diligenciar el formato establecido en el formato de riesgos.

    - Identificador del plan: Número consecutivo que identifica el plan de tratamiento.
    - Identificador del riesgo: Identificador del riesgo que está siendo mitigado por el plan.
    - Nombre del plan: nombre que permite identificar el plan de tratamiento.
    - Descripción del plan: en este campo se describen las características del plan y los objetivos del mismo.

- Justificación del plan: Se describen las razones por las cuales es necesaria la implementación del plan.

- Etapas del plan: nombre de un conjunto de actividades que van a permitir la ejecución del plan.

- Actividades de cada etapa: actividades definidas para la ejecución de una etapa.

- Responsable de la ejecución de la actividad: persona, área, proceso u otro que está encargado de la ejecución de una actividad.

- Responsable del plan: persona, área, proceso u otro encargado de la coordinación y ejecución del todo el plan.

ANEXO I. ENTRENAMIENTO

I.1. ENCUESTA CONOCIMIENTOS GENERALES

1. De los servicios/aplicativos que presta la organización, ¿cuáles conoce?[15]

   a. Correo ☐
   b. Aplicación 1 ☐
   c. Aplicación 2 ☐
   e. Intranet ☐
   g. Otros ☐

   ¿Cuáles?:_____

2. De los servicios/aplicativos mencionados anteriormente, ¿cuáles usa regularmente?

   a. Correo ☐
   b. Aplicación 1 ☐
   c. Aplicación 2 ☐
   e. Intranet ☐
   f. Otros ☐

   ¿Cuáles?:_____

3. Para acceder a cada uno de estos servicios/aplicativos usted debe ingresar un usuario y una contraseña por servicio/aplicativo. Especifique la forma como usted ingresa a cada uno de ellos.

   a. Un usuario y una contraseña igual para todos los servicios
   b. Con usuarios y contraseñas diferentes para cada servicio
   c. Un usuario para todos los servicios pero con contraseña diferente
   d. Con usuario diferente pero igual contraseña para todos los Servicios
   e. Otro
      ¿Cuál?:_____

4. ¿De cuántos caracteres alfanuméricos (letras, caracteres especiales y números) está compuesta su contraseña?

   a. Los mínimos requeridos por el sistema o servicios ☐

[15] Esta información deberá ser modificada dependiendo de los servicios o aplicaciones con cuente en la organización.

b. Un carácter más de los mínimos
d. Dos caracteres más de los mínimos
e. Otro
¿Cuántos? _____

5. Tiene su contraseña escrita en:

a. Agenda
b. Pos-it
c. Ninguno
e. Otro

¿Cuál?:_____

6. ¿Ha permitido que otra persona ingrese con su Usuario?

SI NO

Si su respuesta a la pregunta anterior fue "AFIRMATIVA" diríjase a la pregunta 7 de lo contrario continúe con la pregunta 8.

7. ¿Quién?:
_____

8. ¿Su contraseña de acceso a los sistemas de información o servicios es conocida por personas diferentes a usted?

SI NO

Si su respuesta a la pregunta anterior fue "AFIRMATIVA" diríjase a la pregunta 9, de lo contrario continúe con la pregunta 10.

9. ¿Quién?:
_____

10. ¿A quién llama cuando tiene alguno de los siguientes problemas: fallas en el sistema operativo, acceso a nuevos servicios, contraseñas, virus, o cualquier otra aplicación?

a. Área de tecnología
b. Compañero de Trabajo
c. Jefe Inmediato
d. Otro

¿Cuál?:_____

11. ¿Está su equipo de trabajo protegido por algún tipo de autentificación?

a. Contraseña BIOS (cargue de la máquina) ☐
b. Contraseña de sesión del Sistema Operativo ☐
c. Otras ☐

¿Cuáles?:_____

12. Cuando se levanta de su sitio de trabajo porque necesita ausentarse, usted:

a. Cierra sesión ☐
b. Activa el Protector de Pantalla ☐
c. Suspende el PC ☐
d. Apaga el PC ☐
f. Otra ☐

¿Cuál?:_____

13. ¿Almacena información en las carpetas compartidas que son de uso público en la organización?

SI NO

Si su respuesta a la pregunta anterior fue "AFIRMATIVA" diríjase a la pregunta 14, de lo contrario continúe con la pregunta 15.

14. ¿Qué tipo de información almacena en las carpetas compartidas de uso público?

a. Información personal (Fotos, Videos) ☐
b. Trabajos ☐
c. Otra ☐
¿Cuál?: _____

15. ¿En su sitio de trabajo (oficina) se dispone de un lugar seguro donde se guarden los documentos impresos?

SI NO

16. ¿Usted deja algunos documentos sobre el escritorio?

SI NO

Si su respuesta a la pregunta anterior fue "AFIRMATIVA" diríjase a la pregunta 17, de lo contrario continúe con la pregunta 18.

17. ¿Qué tipo de documentos son dejados sobre el escritorio?

a. Documentos informativos de su dependencia
b. Documentos que contienen información de empleados de la empresa
c. Documentos personales
d. Otro

Cuál: _____

18. ¿Utiliza como papel reciclaje documentos que hayan sido impresos con información personal, informes, proyectos, entre otros?

SI NO

Si su respuesta a la pregunta anterior fue "AFIRMATIVA" diríjase a la pregunta 19, de lo contrario continúe con la pregunta 20.

19. ¿Se realiza una inspección de los documentos que van hacer utilizados como papel reciclaje?

SI NO

20. ¿Comparte archivos o carpetas en su computador para que sean vistos por otros usuarios de la red?

SI NO

Si su respuesta a la pregunta anterior fue "AFIRMATIVA" diríjase a la pregunta 21, de lo contrario continúe con la pregunta 22.

21. ¿Qué tipo de información comparte por la red?

a. Información personal (fotos, videos, datos de contacto) ☐
b. Documentos informativos de la dependencia ☐
c. Documentos informativos de la organización ☐

d. Información personal de los miembros de la organización ☐
e. Otra ☐

¿Cuál?: _____

22. ¿Utiliza su computador personal (portátil) en la organización?

SI NO

.

23. En su computador personal almacena información:

a Relativa a sus funciones en la organización ☐
b Personal ☐
c Personal y de la organización ☐
d Otra ☐

¿Cuál?:_____

I.2. ENTREVISTA ÁREA DE TECNOLOGÍA DE INFORMACIÓN

1. ¿La red de datos, cuenta con alguna de las siguientes Tecnologías de la Información?

		SI	NO
a.	Equipos de cómputo:		
	Escritorio		
	Portátiles		
	Servidores		
b.	Intranet		
c.	Red Local		
d.	Inalámbrica		
e.	Extranet		

Si su respuesta a la pregunta anterior en el numeral "b" fue "AFIRMATIVA" diríjase a la pregunta 2, de lo contrario continúe con la pregunta 4.

2. ¿Cuáles son los servicios que presta la Intranet?

		NO	SI
a.	Correo		
b.	Web		
c.	FTP		
d.	DNS		
e	Otro		

¿Cuáles?: _____

Si su respuesta a la pregunta anterior en el numeral "b" fue "AFIRMATIVA" diríjase a la pregunta 3, de lo contrario continúe con la pregunta 4.

3. ¿Cuáles servicios Web son prestados a través de:

   a. ¿Intranet?:

   b. ¿Extranet?:

   c. ¿Internet?:

4. ¿Qué tecnología es utilizada para interconectar las diferentes sedes de la organización?

		NO	SI
a.	VPN		
b.	WAN		

5. ¿Qué tipo de conexión es utilizada en la WAN?

		SI	NO
a.	Canales Dedicados		
b.	Conmutación de Paquetes		
c.	Conmutación de Circuitos		

Especifique el protocolo con el cual funciona la conexión: _____

6. ¿En la red de datos de la organización, se utiliza alguno de los siguientes servicios de seguridad?

		SI	NO
a.	Antivirus		
b.	Detección de Intrusos		
	IPS		
	IDS		
c.	Aseguramiento de Servidores		
d.	Mecanismos de autentificación		
	Firmas digitales		
	Password y *Login*		
	SSL		
	PKI		
e.	Cifrado		

7. ¿Con qué periodicidad se realizan actualizaciones y parches de los servicios de la Red?

Periodicidad / Servicio	Inmediata	Periódica	Ocasional	No
Antivirus				
IPS				
IDS				
SO Servidores				
SO Clientes				
Password Servidores				
Password Dispositivos de Red				

Nota:
Definición de la periodicidad de las actualizaciones: Inmediata (se realizan cuando el proveedor la tiene disponible), Periódica (se realizan cada determinado tiempo), Ocasional (se realizan de vez en cuando), No (no se realizan porque no existe la cultura)

8. ¿Se realizan copias de seguridad (*Backups*) de la información institucional?

SI NO

Si su respuesta a la pregunta anterior fue " AFIRMATIVA " diríjase a la pregunta 9, de lo contrario continúe con la pregunta 12.

9. ¿Cuál es el método empleado para la realización de copias de seguridad (*Backups)*?

_____

10. ¿Con qué periodicidad se realizan las copias de seguridad?

a. Diariamente ☐
b. Semanalmente ☐
c. Mensualmente ☐
d. Ocasionalmente ☐
e. Nunca ☐

11. ¿Dónde se almacenan las copias de seguridad?

a. Al interior de la organización ☐
b. Al exterior de la organización ☐
c. Otro

¿Cuál?:_____

12. ¿Existe la administración de registros de eventos?

SI NO

Si su respuesta a la pregunta anterior fue "AFIRMATIVA" diríjase a la pregunta 13, de lo contrario continúe con la pregunta 17.

13. La administración de los registros de eventos se hace a nivel de:

a. Servidores ☐
b. Dispositivos de interconectividad ☐
c. Aplicaciones ☐
d. Servicios críticos ☐

14. ¿Con qué periodicidad son revisados los registros de eventos?

		SI	NO
a.	Diariamente	☐	☐
b.	Semanalmente	☐	☐
c.	Mensualmente	☐	☐
d.	Ocasionalmente	☐	☐
e.	Nunca	☐	☐

15. ¿Qué tratamiento reciben los registros de eventos una vez revisados?

a. Almacenados ☐
b. Borrados ☐
c. Otra ☐

¿Cuál?:_____

Si su respuesta a la pregunta anterior fue “a. Almacenados” diríjase a la pregunta 16, de lo contrario continúe con la pregunta 17.

16. ¿De qué forma son almacenados?

    _____
    _____

17. ¿Cómo se tiene configurado el tiempo en cada uno de los servidores del sistema de información del negocio?

    a. Por medio de NTP ☐
    b. Se configura en cada servidor ☐
    c. Otro ☐

    ¿Cuál?:_____

18. ¿Se protege el acceso físico al (los) centro(s) de comunicación(es) donde se encuentran los servidores y los dispositivos de comunicaciones?

    SI NO

19. ¿Se cuenta con monitorización de la red de comunicaciones?

    SI NO

Si su respuesta a la pregunta anterior fue "AFIRMATIVA" diríjase a la pregunta 20, de lo contrario continúe con la pregunta 22.

20. ¿Cómo se realiza la monitorización?

    a. SNMP ☐
    b. Otro ☐

    ¿Cuál?:_____

21. ¿Con qué periodicidad se hace esta monitorización?

		SI	NO
a.	Diariamente		
b.	Semanalmente		
c.	Mensualmente		
d.	Ocasionalmente		

22. ¿Se cuenta con algún plan de recuperación de desastres (DRP)?

SI NO

Si su respuesta a la pregunta anterior fue "AFIRMATIVA" diríjase a la pregunta 23, de lo contrario continúe con la pregunta 24.

23. Este plan de recuperación de desastres:

		SI	NO
a.	Ha sido probado		
b.	No ha sido probado		

24. ¿Se ha presentado algún tipo de ataque informático?

SI NO

Si su respuesta a la pregunta anterior fue "AFIRMATIVA" diríjase a la pregunta 25, de lo contrario continúe con la pregunta 28.

25. ¿Qué acciones fueron realizadas?

Durante el incidente: _____
_____

Después del incidente: _____
_____

26. ¿Cuál fue el ataque que se presentó?

_____
_____
_____

27. ¿En qué nivel afectó el funcionamiento de los Sistemas de Información de la organización?

a	Bajo	
b	Medio	
c	Alto	
d	Otro	

¿Cuál?:_____

28. ¿Se cuenta con documentación referente al diseño de la infraestructura de la red de datos?

SI NO

Si su respuesta a la pregunta anterior fue "NEGATIVA" diríjase a la pregunta 29, de lo contrario continúe con la pregunta 30.

29. ¿Por qué?

_____
_____
_____

30. ¿La documentación del diseño de la infraestructura de red de datos se encuentra actualizada a la fecha?

SI NO

31. ¿Cuál es la importancia que tiene la Seguridad de la información en el área de tecnología?

a.	Muy importante	
b.	Importante	
c.	Poco Importante	
d.	Sin Importancia	

32. ¿Se cuenta con personal calificado para el desarrollo de la seguridad informática en la organización?

SI NO

Si su respuesta a la pregunta anterior fue "AFIRMATIVA" diríjase a la pregunta 33 de lo contrario continúe con la pregunta 34.

33. ¿Cuál es el nivel educativo de esta personal?

_____
_____

34. Cuándo los llama una empresa proveedora de servicios para realizar un soporte técnico ustedes:

a. Contestan todas las preguntas que les son hechas ☐
b. Regresan la llamada para verificar que si se trata de un soporte técnico ☐
c. Otra ☐

¿Cuál?: _____

I.3 FORMATO DE EVALUACIÓN DE LA ENCUESTA

Preguntas de la Encuesta		
Pregunta	**Observación**	**Recomendación**
Formato Empleado para la Entrevista		
Preguntas Sugeridas		

I.4 FORMATO DE IDENTIFICACIÓN DE OPORTUNIDADES DE MEJORA PLAN DE ENTRENAMIENTO

Plan de Entrenamiento		
Programa	**Observación**	**Recomendación**
Formato Empleado en las Actividades del Programa		
Consideración o Cambio		

I.5 CRONOGRAMA DE ACTIVIDADES DEL PLAN DE ENTRENAMIENTO

Actividad	Responsable	Mes																				Horario
		Semana 1					Semana 2					Semana 3					Semana 4					
		1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	

I.6 LECCIONES APRENDIDAS Y OPORTUNIDADES DE MEJORA

Evaluación del Proceso de Aprendizaje		
Programa	**Observación**	**Recomendación**
Observaciones Generales		

ANEXO J . REVISIÓN Y EVALUACIÓN

J.1. ANÁLISIS DE VULNERABILIDADES TÉCNICAS

Pruebas de Análisis de Vulnerabilidades Técnicas	
Fecha:	
Titulo de la Prueba	
El nombre que identifica la prueba a realizarse.	
Objetivo de la Prueba	
Qué se persigue con la realización de la prueba.	
Descripción de la Prueba	
En qué consiste la prueba, es decir que herramientas y metodología se seguirá para conseguir el objetivo.	
Forma de Ejecución	
Los pasos necesarios y el orden como se llevará a cabo la prueba, además el encargado de dicha prueba.	
Resultados esperados	
Sabiendo cómo funcionan las herramientas y lo que se quiere lograr con su uso, plasmar las expectativas que se tienen al aplicar la prueba.	
Desarrollo del Informe	
Esta dado por un anexo el cual muestra los resultados que arroja la prueba, en especial si cumple o no con el objetivo y con los resultados esperados.	

J.2. REVISIÓN Y EVALUACIÓN DEL ENTRENAMIENTO (PRUEBAS DE CONCEPTO)

Ficha Técnica de la Prueba de Concepto	
Fecha:	**Hora:**
Titulo del Simulacro	
El nombre que identifica la prueba a realizarse.	
Objetivo del Simulacro	
Qué se persigue con la realización del simulacro.	
Descripción de la Prueba	
En qué consiste la prueba, es decir qué aspectos se evaluaran y qué metodología se seguirá para conseguir el objetivo.	
Forma de Ejecución	
Los pasos necesarios y en orden como se llevará a cabo la prueba, además el encargado de dicha prueba.	
Resultados esperados	
El encargado de llevar a cabo el simulacro, describe las expectativas que se tienen con su desarrollo.	
Desarrollo del Informe	
Está dado por un anexo el cual muestra los resultados que arroja el simulacro, en especial si se cumplieron con los objetivos y con los resultados esperados.	

J.3. OBSERVACIÓN Y ATENCIÓN DE INCIDENTES

J.3.1. Instructivo para la gestión de incidentes

La gestión de incidentes está basada en los lineamientos establecidos por ITIL V3 en su proceso de operación del servicio, ITIL divide la gestión de incidentes en las siguientes etapas:

- Identificación

Los incidentes podrán ser reportados por cualquier empleado de la organización, para ello se recomienda que la empresa cuente con una herramienta de reporte de incidentes que pueda ser usada por los diferentes empleados. El uso de esta herramienta deberá ser promovido a través de las campañas de entrenamiento de la arquitectura de seguridad de la información.

Además de lo anterior, se recomienda que se cuente con un punto único de contacto para que los usuarios que tengan problemas en el reporte de incidentes a través de la herramienta lo puedan realizar telefónicamente.

Reporte de Incidentes	
Fecha	**Hora**
El día, el mes y año en el que se presenta el incidente.	Hora, minutos y segundos en el que ocurre el incidente.
Incidente	
El nombre que identifica el incidente.	
Activos Afectados	
Mencionar según la clasificación de activos del Análisis de Riesgos, los activos que se vieron comprometidos en el incidente.	
Descripción del incidente	
Explicación detallada del incidente.	
Información adicional del incidente	
• Lugar donde se identificó el incidente: • Persona que identificó el incidente: • Jefe inmediato de quien reporta el incidente: • Área a la cual pertenece: • Datos de contacto:	

- Riesgo

El equipo del punto de contacto deberá analizar el riesgo del incidente de seguridad para ello podrán contar con el apoyo del Arquitecto de Seguridad de la Información. Para el análisis del incidente se podrá emplear la siguiente tabla de valoración:

Impacto		**MATRIZ DE RIESGO – INCIDENTES**		
Alto	15			
Mayor	10			
Bajo	5			
Urgencia		5	10	15
		Baja	Media	Alta

- Clasificación del incidente

Teniendo en cuenta la valoración de riesgo del incidente se podrá identificar la clasificación del mismo.

Riesgo	**Descripción**
Critico	El incidente puede causar un impacto alto para la operación del negocio. Requiere de atención inmediata.

Riesgo	Descripción
Importante	El incidente se cataloga como urgente, pero su impacto no es significativo, por tal razón, su atención puede estar sujeta a la solución de los casos en nivel crítico
Bajo	Los casos en este nivel pueden ser desarrollados luego de la atención de casos con niveles de riesgo crítico. Sin dejar de lado que tienen que ser resueltos debido a que puede tener consecuencias con el tiempo.

- Diagnóstico Inicial

Teniendo en cuenta la información suministrada por quien reporta el incidente, realizar una valoración inicial del mismo; en algunos casos se requerirá visitar el área donde ocurrió el incidente y realizar preguntas a quien identificó y reportó el incidente. En caso que con la información existente no se pueda dar solución al incidente, éste deberá ser escalado a quien considere apropiado por la persona que se encuentra analizando el incidente.

- Escalamiento

El Arquitecto de SI deberá contactar a quien fue escalado el incidente para apoyar el trabajo que será realizado.

- Investigación y diagnóstico

Se deben investigar todas las fuentes posibles de información para encontrar la causa del incidente. En caso que se requiera se debe contactar a un grupo interdisciplinario que apoye la solución del incidente, para esto se puede utilizar el apoyo de personal externo a la organización para que la investigación se desarrolle en el menor tiempo posible y así evitar un mayor impacto al negocio.

- Resolución

Una vez se ha encontrado la solución y las causas que ocasionaron el incidente se proceden a realizar la respectiva documentación del caso.

Reporte de Resolución de Incidentes	
Fecha	**Hora**
El día, el mes y año en el que se presenta el incidente.	Hora, minutos y segundos en el que ocurre el incidente.
Incidente	
El nombre que identifica el incidente.	
Activos Afectados	
Mencionar según la clasificación de activos del Análisis de Riesgos, los activos que se vieron comprometidos en el incidente.	
Descripción del incidente	
Explicación detallada del incidente.	
Información adicional del incidente	
• Lugar donde se identificó el incidente: • Persona que identificó el incidente: • Jefe inmediato de quien reporta el incidente: • Área a la cual pertenece: • Datos de contacto:	
Descripción detallada de incidente	
Se deberá realizar una descripción detallada del incidente con base en la información de quien lo reportó y en la información empleada para su solución.	
Equipo de atención al incidente	
Si fue necesario convocar al equipo de atención a incidentes se deberá describir quiénes conformaron el grupo de atención.	
Descripción de la solución	
Descripción detallada de la solución del incidente, en caso que se requiera esto podrá estar acompañada por manuales o instructivos.	
Descripción de la causas	
Descripción detallada de las causas que provocaron el incidente.	
Lecciones aprendidas	
Descripción de las lecciones aprendidas durante la atención del incidente.	

- Comunicación

Informar a quien notificó el incidente que éste fue solucionado.

- Cierre

El Arquitecto de Seguridad de la Información deberá confirmar oficialmente el cierre del caso luego que se identifique la satisfacción de quien reportó el incidente.

ANEXO K. ACTUALIZACIÓN

Actualización
Tipo de Actualización

Arquitectura de Seguridad	
Negocio	
Marco Normativo	
Política de Seguridad	
Directrices	
Normas	
Procedimientos	
Normativa Corporativa	
Gestión de Seguridad	
Análisis de Riesgos	
Observación y Atención de Incidentes	
Revisión y Evaluación	
Entrenamiento	
Actualización	
Mantenimiento	
Acuerdos	
Infraestructura de Seguridad	
Gestión del Conocimiento	
Directrices, Nomas, Procedimientos y Concienciación	
Seguridad Física	
Perímetro	
Red Interna	
Host	
Aplicación	
Datos	
Visibilidad	
Control	

Se debe marcar con una X el elemento de la Arquitectura de Seguridad o el proceso de la Gestión de la Seguridad que se quiere actualizar.

Fecha
El día, el mes y año en el que se presenta la actualización.
Objetivo de la Actualización

Mencionar el porqué, el cómo y el para qué se debe realizar dicha actualización.

Sustentación

Fundamentar el objetivo por el cual es necesario realizar dicha actualización y el riesgo en el que se incurre al no hacerlo.

Firma y Nombre del Arquitecto de Seguridad de la Información

_____
Nombre.
Cargo.

La persona que diligencia este formato solicitando la actualización debe firmar con nombre y cargo.

Aprobación de la Solicitud

SI	NO

Se debe marcar con una X

Tratamiento de lo Asumido

Acciones que se ejecutarán en los casos en los que no se desarrollen las actualizaciones.

Firma y Nombre de quien Aprueba

_____
Nombre
Cargo

La persona que realizó y evaluó la solicitud de la actualización debe firmar con nombre, y cargo.

ANEXO L. MANTENIMIENTO

Mantenimiento

Nivel del Mantenimiento

Arquitectura de Seguridad	
Negocio	
Marco Normativo	
Política de Seguridad	
Directrices	
Normas	
Procedimientos	
Normativa Corporativa	
Gestión de Seguridad	
Análisis de Riesgos	
Observación y Atención de Incidentes	
Revisión y Evaluación	
Entrenamiento	
Actualización	
Mantenimiento	
Acuerdos	
Infraestructura de Seguridad	
Gestión del Conocimiento	
Directrices, Normas, Procedimientos y Concienciación	
Seguridad Física	
Perímetro	
Red Interna	
Host	
Aplicación	
Datos	
Visibilidad	
Control	

Se debe marcar con una X el elemento de la Arquitectura de Seguridad o el proceso de la Gestión de la Seguridad al que se realizará el mantenimiento.

Fecha

El día, el mes y año en que inicia el proceso de mantenimiento.

Encargado

Director	
Arquitecto de Seguridad de la Información	
Oficial de Seguridad Informática	
Departamento de TI	
Terceros	

Se debe marcar con una X estipulando quién realiza la evaluación del proceso de implementación del mantenimiento.

Objetivo del mantenimiento

Mencionar el por qué, el cómo y el para qué se debe realizar dicho mantenimiento.

Sustentación

Fundamentar si se cumplió el objetivo que se perseguía con la implementación de dicho mantenimiento, de no ser así explicar las causas por las que la actualización no cumplió con el objetivo trazado.

Firma y Nombre del Encargado

_____

Nombre
Cargo
Persona que dirigió el desarrollo del mantenimiento.

Revisado

SI	NO

Se debe marcar con una X el hecho de estar de satisfecho o insatisfecho con el mantenimiento.

Firma y Nombre del encargado de la aprobación

_____

Nombre
Cargo
Persona que realizó y evaluó la solicitud de mantenimiento.