PLANIFICACIÓN ESTRATÉGICA Y PLAN DE SEGURIDAD INFORMÁTICA DE FABRIL FAME S.A.

José Luis Rojas, Juan José Vela, Mario Ron, Víctor Páliz
Departamento de Ciencias de la Computación, Escuela Politécnica del Ejército, Sangolquí, Ecuador.
zeluiz_01@hotmail.com
juanjo_vela2@hotmail.com
mbron@espe.edu.ec
victor.paliz@agrocalidad.gob.ec

RESUMEN:

El presente proyecto tiene como principal objetivo aplicar la metodología PETI para desarrollar el Plan Estratégico Informático y la metodología Magerit, junto con la norma ISO 27002 para el desarrollo del Plan de Seguridad Informática del Departamento de Sistemas de la empresa FAME S.A.

El Plan Estratégico Informático tiene como objetivo proveer un marco para administrar y proyectar los cambios internos y externos que ocupan un lugar en el entorno. Considera un dominio de aplicación dinámico, que integra las visiones estratégicas de negocio/organizacional, con la visión estratégica de Tecnología de Información en una percepción única final.

Por otro lado en el Plan de Seguridad Informático, se realiza un análisis de riesgos que implica la evaluación del impacto que una violación de la seguridad tiene en FAME; señala los riesgos existentes, identificando las amenazas que acechan al sistema de información, y determina la vulnerabilidad de los sistemas ante dichas amenazas. Los resultados del análisis de riesgos obtenidos han permitido recomendar las medidas apropiadas que deberían adoptarse para conocer, prevenir, impedir, reducir o controlar los riesgos identificados y así reducir al mínimo su potencialidad o sus posibles perjuicios.

ABSTRACT: This project's main goal is to apply the PETI methodology for developing the Strategic Plan and the MAGERIT methodology and The ISO/IEC 27002 for developing the Security Plan of the FAME`s IT Department.

The IT's Strategic Plan aims to provide a framework for managing and projecting internal and external changes that have a place in the environment. Consider a dynamic application domain, which integrates the strategic visions of business / organizational with the strategic vision of Information Technology in a unique insight.

By other way the IT´s Security Plan performs a risk analysis that involves the impact evaluation of a security violation has in FAME; points out the risks, identifying threats to the information system, and determines the vulnerability of the system having such threats. The risk analysis results obtained have allowed recommending appropriate measures to be taken to know, prevent, reduce or take control of the identified risks and minimize their potential or possible damage.

1. INTRODUCCIÓN

El reto de las organizaciones siempre ha radicado en la creación de una ventaja competitiva, lo que involucra el establecimiento de excelencia en precio, producto, servicio o realización. En términos tecnológicos, la creación de una ventaja competitiva se concentra en la búsqueda e identificación de nuevos sistemas de TI, que generen una diferencia con respecto a otros competidores, mejorando la participación en el mercado y aumentando las ganancias. Muchas empresas han crecido y se han consolidado rápidamente en el mercado, porque supieron aprovechar el potencial de la información y la TI con respecto a sus competidores. Otras, por el contrario, han perdido terreno, debido a que sus competidores establecieron una ventaja tecnológica.

Tradicionalmente se considera que el análisis de riesgos es fundamental para la gestión de la seguridad de los sistemas de información. Mediante su aplicación, se obtiene información acerca de los activos, la valoración del impacto que para la organización puede suponer la pérdida de los mismos y la identificación de las amenazas a las que están expuestos. Por tanto, el análisis constituye el núcleo central de toda actuación organizada y sistemática en materia de seguridad para mejorar la gestión global del riesgo. Es lógico que así sea, ya que los resultados obtenidos acaban influyendo en la estrategia de la organización (por ejemplo mediante cambios en la política de seguridad) y en la realización de mejoras concretas, sobre todo a través de la implantación de salvaguardas.

2. METODOLOGÍA

2.1 Metodología PETI

La metodología PETI (Planeación Estratégica de Tecnología de Información) es ampliamente reconocida como una herramienta para ordenar los esfuerzos de incorporación de TI.

Establece las políticas requeridas para controlar la adquisición, el uso y la administración de los recursos de TI. Integra la perspectiva de negocios/organizacional con el enfoque de TI (ver figura 1), estableciendo un desarrollo informático que responde a las necesidades de la organización y contribuye al éxito de la empresa. Su desarrollo está relacionado con la creación de un plan de transformación, que va del estado actual en que se encuentra la organización, a su estado final esperado de automatización, esto, en concordancia con la estrategia de negocios y con el propósito de crear una ventaja competitiva.

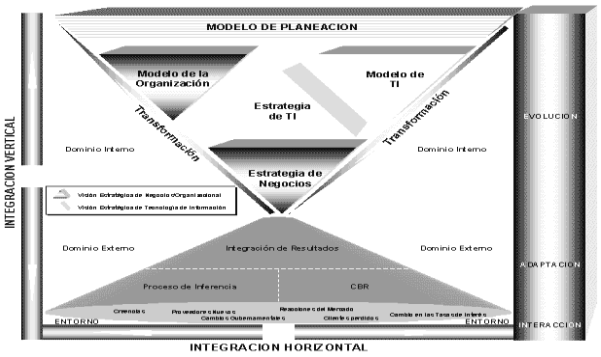

Figura 1. Modelo PETI

En este modelo, el mundo real está compuesto por entidades relacionadas unas con otras, que, bajo la generación de eventos, cambian el comportamiento del entorno. La concepción del modelo está basada en tres conceptos fundamentales (ver figura 2): interacción, adaptación y evolución.

El concepto de interacción es propuesto para incorporar o rechazar hechos relacionados con las condiciones del entorno. En nuestro modelo, el mundo real es un sistema de interacciones entre entidades (empresas, proveedores, consumidores, gobierno, organismos, etc.). Las entidades toman posiciones estratégicas particulares, jugando papeles diferentes. Las interacciones son establecidas por la interrelación entre los roles que cada entidad tiene en el dominio de aplicación. El comportamiento del entorno es inducido por la interacción entre entidades.

La ocurrencia de un incidente (creencias, reacciones del mercado u otros), que cambia las condiciones del entorno, es llamado evento. Cada entidad tiene la opción de considerar el suceso de un evento, e incorporar o rechazar hechos relacionados con los cambios en las condiciones del entorno. La aceptación o el rechazo depende de los intereses de cada entidad. Ejemplos de condiciones que pueden ser aceptadas o rechazadas, son: cambios en los planes económicos, creencias políticas, tendencias tecnológicas nuevas y crecimiento en las tasas de interés, entre otras.

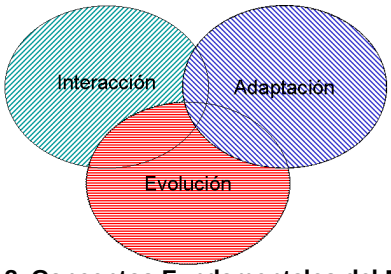

Figura 2. Conceptos Fundamentales del Modelo

Cabe notar que el concepto de interacción ha sido ampliamente reconocido en la literatura. Las ideas de Bertrand establecen que una organización es un sistema social de interacciones entre entidades, restringido por normas y expectativas compartidas.

El concepto de adaptación es introducido para incorporar estrategias de negocio. Dos métodos diferentes son propuestos para llevar a cabo esta tarea. Por un lado, se utiliza un método de inferencia, que toma como materia prima los hechos relacionados con las condiciones del entorno y genera estrategias de negocio nuevas. Por otro lado, el modelo utiliza una base de casos anteriores, que permite la incorporación de estrategias de negocio ya probadas en condiciones similares del entorno, por la misma entidad o por otras. Cada caso es soportado por un conjunto de antecedentes acerca de las condiciones del entorno. La recuperación de casos se lleva a cabo estableciendo una asociación directa, entre la base de hechos de condiciones del entorno y los antecedentes en la base de antecedentes de casos anteriores.

- La estrategia de negocios es el medio por el cual una empresa determina su curso de acción futuro.
- La estrategia de TI es un conjunto de lineamientos estratégicos, establecidos para relacionar el desarrollo del modelo de TI con la dirección estratégica del negocio y el comportamiento de la organización.
- El modelo de la organización está relacionado con un mecanismo capaz de diseñar a detalle el comportamiento y estructura de la organización. [3]
- El modelo de TI se concentra en la construcción de la arquitectura y estructura de TI, que establece un marco para la especificación de las aplicaciones y la integración de la información.
- El modelo de planeación está relacionado con la creación de un plan; las prioridades para desarrollar dicho plan; un análisis costo/beneficio, y un estudio de administración del riesgo.

El proceso de transformación se identifica con una pirámide inversa (ver figura 3), en la que las estrategias de negocio representan los "axiomas" del arquetipo de la organización. Estos axiomas son principios fundamentales considerados como verdaderos, en virtud de que son congruentes con la realidad del entorno. En todo caso, la PETI trata de estar en contacto con el mundo que la rodea, para dar a su construcción la mayor coherencia lógica posible (en contraste con la definición de los axiomas matemáticos, que tratan de alejarse de la realidad). Nótese que la estrategia de negocios impacta directamente en la generación o selección de un plan. Por esta razón la estrategia de negocios puede ser vista como una condición especial sobre el proceso de PETI.

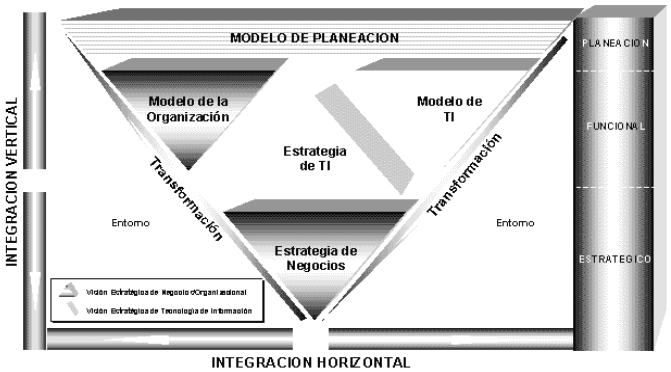

Figura 3. Evolución de las Estrategias de Negocio

Las proposiciones de la organización (estrategia de TI, modelo de la organización, modelo de TI y modelo de planeación) se deducen a partir de los axiomas, mediante un método lógico de inferencia. Por consiguiente, toda proposición es correcta o verdadera si se puede deducir a partir de los axiomas.

Esta definición concuerda con el hecho de que la eficiencia de una empresa y el uso efectivo de la TI, depende de la correspondencia que existe con las estrategias de negocios. Si las estrategias de negocios fuesen incompatibles con su estructura física y sus capacidades de TI, el funcionamiento de sus áreas funcionales sería deficiente.

Determinar que una proposición organizacional es verdadera, se reduce a entender si los axiomas que la sustentan son congruentes con la realidad. En nuestro entorno, la certeza de las proposiciones se apoya en definiciones evolutivas. Los axiomas organizacionales no son absolutos, sino que evolucionan con los cambios internos y externos del entorno.

La interdependencia entre los componentes del modelo se establece a través de una integración vertical y horizontal, creada por una referencia cruzada bidireccional. Esta condición da como resultado un proceso de planeación dinámico, en el que cada componente está en concordancia con todos los demás, y evoluciona con los cambios del entorno. El orden de aplicación natural de la pirámide es "Abajo/Arriba"-"Izquierda/Derecha" y está dividido en tres niveles: estratégico, funcional y planeación.

2.2 Metodología MAGERIT

Magerit es una metodología que se esfuerza por enfatizarse en dividir los activos de la organización en variados grupos, para identificar más riesgos y poder tomar contramedidas para evitar así cualquier inconveniente.
La razón de ser de MAGERIT está directamente relacionada con la generalización del uso de las tecnologías de la información, que supone unos beneficios evidentes para los ciudadanos; pero también da lugar a ciertos riesgos que deben minimizarse con medidas de seguridad que generen confianza.

En el periodo transcurrido desde la publicación de la primera versión de Magerit (1997) hasta la fecha, el análisis de riesgos se ha venido consolidando como paso necesario para la gestión de la seguridad.

La Evaluación del riesgo es fundamental para llevar cabo planes de seguridad y de contingencia dentro de la organización, para poder gestionarlos y hacerse riguroso frente a posibles ataques a los datos y la información tanto de la organización, como de los servicios que presta.

Objetivos de Mágerit:

1. Concienciar a los responsables de los sistemas de información de la existencia de riesgos y de la necesidad de atajarlos a tiempo.
2. Ofrecer un método sistemático para analizar tales riesgos.
3. Ayudar a descubrir y planificar las medidas oportunas para mantener los riesgos bajo control.

4. Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

3. DISEÑO E IMPLEMENTACIÓN

3.1 Implementación Metodología PETI

Todo el proceso comienza con un análisis de la situación actual en la fase I, que produce el modelo funcional imperante en la empresa. En este paso se evalúa de manera general el entendimiento de la estrategia de negocios, la eficiencia de los procesos operativos y la aceptación de TI en la organización.

La fase II, relacionada con la creación de un modelo de la organización, inicia con un análisis del entorno y el establecimiento de la estrategia de negocios. Continúa con el diseño en detalle de los modelos operativos, que van a producir en parte los requerimientos de TI necesarios para mejorar la eficiencia y la productividad de la empresa. Posteriormente, se construye la estructura de la organización, que especifica puestos, perfiles, habilidades, etc., necesarios para administrar la empresa. La fase termina con la construcción de una arquitectura de información, que identifica las necesidades globales de información de la empresa. El modelo es descrito con la utilización de términos y conceptos de negocio/organización, independientemente del soporte computacional.

La fase III trata del desarrollo de un modelo de TI. En su primer módulo, tiene como objetivo la transformación de las estrategias de negocios en una estrategia de TI. Sigue con la construcción de la arquitectura de sistemas, que establece un marco para la especificación de las aplicaciones y la integración de la información. Luego se definen los elementos clave y las características esenciales de la arquitectura tecnológica (Hardware y comunicaciones), que establece la plataforma en la que los sistemas van a funcionar. Continúa con el diseño en detalle de los modelos operativos de TI, que describen el funcionamiento del área informática. Finaliza con la definición sobre la estructura de la organización de TI, necesaria para administrar los requerimientos informáticos.

Finalmente, la fase IV se concentra en la elaboración de un modelo de planeación. Primero se establecen las prioridades para la implantación de la TI y los procesos operativos. Luego se define un plan de implantación, que determina el orden de desarrollo de los proyectos de negocios/organización y de TI. Continúa con un estudio de la recuperación de la inversión, a través de un análisis costo/beneficio. Todo el proceso finaliza con un estudio de administración del riesgo, que se encarga de reconocer la existencia de amenazas que puedan poner en peligro el éxito del PETI.

3.2 Análisis de Riesgos mediante el empleo de Metodología Mágerit y Pilar

La aproximación metódica es la única posible, si se pretende que el análisis sirva de soporte a la inevitable toma de decisiones. Como se ha indicado con anterioridad, en el caso de FAME se optó por aplicar la metodología Mágerit para se realización. Las fases seguidas fueron:

1. Recopilación de información.
2. Identificación de los activos relevantes.
3. Valoración de los activos.
4. Determinación de las amenazas potenciales sobre cada activo.
5. Identificación del grado de vulnerabilidad de cada activo a las amenazas que le afectan.
6. Estimación del impacto sobre el activo de la materialización de la amenaza.
7. Medida del riesgo, analizando el impacto ponderado por la frecuencia de ocurrencia de la amenaza.

Puesto que el empleo de Mágerit es complejo y prácticamente imposible de realizar a mano cuando el número de activos es relativamente grande, se justifica la necesidad de disponer de una ayuda en forma de herramienta de soporte.

Además, el inevitable mantenimiento futuro, necesario para la propia organización y para una hipotética certificación, con cambios en el inventario de activos y en la naturaleza de los mismos, impone la adopción de una herramienta que automatice la generación de sucesivas versiones.

La herramienta elegida ha sido Pilar, que ofrece un amplio conjunto de utilidades para la realización de un análisis cualitativo. Gracias a Pilar ha sido relativamente sencillo sistematizar el proceso laborioso de carga de datos y calcular con posterioridad los impactos y los riesgos. Los resultados obtenidos por la propia herramienta aportan una versión simplificada de la complejidad del problema, mediante la que es posible comprender mejor el mismo y adoptar conclusiones razonadas.

Como punto de partida para la realización del análisis, se efectuaron entrevistas con diversos responsables de la organización, generando a continuación un acta que se remitió a cada uno de los entrevistados para que tuvieran oportunidad de corregir posibles errores de interpretación o matizar las cuestiones que consideraran adecuadas.

A continuación, los activos definidos se agruparon en cinco capas diferentes en función de su naturaleza. Para su valoración se tuvo en cuenta la importancia dada por los entrevistados a los servicios en disponibilidad, integridad y autenticidad de los usuarios del servicio y de quien accede a los datos.

En base a los datos obtenidos y al análisis de la organización, se realizó una asociación de dependencias para los diferentes activos en el árbol creado. A continuación, asignando un rango de valoración de 0 a 10 para cada dimensión y activo, y considerando las relaciones de dependencia definidas con anterioridad, se construyó el Modelo de Valor.

Tomando como referencia el conjunto de amenazas previstas para cada activo por la herramienta Pilar y considerando la opinión y experiencia de los usuarios, fue posible determinar la frecuencia de materialización de una amenaza (modelada con una tasa anual de ocurrencia) y la medida de la degradación de cada activo. La información se organizó en el Mapa de Riesgos.

Para valorar el impacto de la materialización de una amenaza sobre cada activo, se ha tenido en cuenta:

1. Impacto acumulado: El valor acumulado de cada activo (su propio valor más el de todos los otros activos que dependen de él) y las amenazas a que está expuesto.
2. Impacto repercutido: Se calcula teniendo en cuenta el valor del propio activo y los impactos que resultan sobre los activos de los que depende.

Por último, se realizó una valoración individual del riesgo a que está expuesto el conjunto de activos estudiado. El riesgo acumulado se estimó en función del valor de cada activo y sus dependencias, teniendo en cuenta que el impacto sobre un activo produce daños directos sobre ese activo e indirectos sobre los que dependen de él. El riesgo repercutido se calculó teniendo en cuenta sólo el valor de cada activo, sin considerar las dependencias.

En resumen, el empleo de la metodología Mágerit y la herramienta Pilar en el trabajo realizado ha permitido:

- Mejorar el conocimiento sobre el estado de seguridad de los sistemas de información y las medidas de seguridad asociadas a ellos.
- Sistematizar el estudio, de forma que no haya elementos que permanezcan al margen del análisis, asignando a cada uno la importancia relativa que le corresponde.
- Incorporar mecanismos de seguridad en los propios sistemas de información.

Una vez obtenido el análisis de riesgos, pues se procede con la elaboración del Plan de Seguridad Informática, basado en la norma ISO 27002 siguiendo todos y cada de sus dominios (ver Figura 4), objetivos de control y controles, relacionándolos con los resultados obtenidos del mencionado AR y estableciendo salvaguardas.

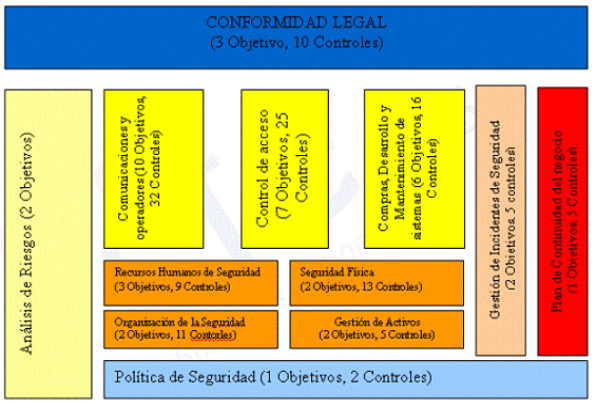

Figura 4. Dominios de la ISO/IEC 27002

El éxito del proyecto se pone de manifiesto en la adopción de numerosas salvaguardas mediante decisiones adoptadas a nivel directivo, que han contribuido a disminuir el nivel de riesgo a que estaba sometida inicialmente la organización.

4. RESULTADOS

Los resultados obtenidos fueron analizados en conjunto con el personal de la organización que participó en el proyecto. Las estrategias de tecnología y las recomendaciones planteadas en cuanto a seguridad de la información, fueron evaluadas y aprobadas.

Para asegurar que todo lo expuesto en el proyecto sea tomado en cuenta y pueda ser implementado a corto, mediano o largo plazo será necesario que el personal tome conciencia, reconozca sus falencias y apoyen un cambio en la cultura organizacional.

5. TRABAJOS RELACIONADOS

Existen algunos trabajos relacionados que se han encontrado durante la investigación, en esta sección se han incluido los más relevantes:

Análisis de Riesgos en la Agencia Estatal de Meteorología mediante el empleo de Magerit y PILAR, por Julio González Breña. En este trabajo se realiza el análisis de riesgos y gestión de salvaguardas de la Agencia Estatal de Meteorología de España.

Planeamiento Estratégico de Tecnología de Información de la Escuela Superior Privada de Tecnología SENATI, por Najarro Bellido. En este trabajo se realiza el plan estratégico informático aplicando todos los módulos y fases de la metodología PETI.

6. CONCLUSIONES Y TRABAJO FUTURO

En esta investigación se ha podido evidenciar que la metodología utilizada para el desarrollo ha permitido establecer un plan estratégico y de seguridad informática confiable, estructurados y tomando en cuenta los aspectos más importantes de la empresa. La información obtenida mediante las metodologías aplicadas han permitido entender el giro de negocio de FAME S.A., y se ha logrado establecer lineamientos que permitan apalancar dicha estrategia mediante el uso y protección de las Tecnologías de Información.

Como trabajo futuro se debe ejecutar e implementar los planes desarrollados dentro de la empresa, además de tener un continuo seguimiento, evaluación y adaptación a los cambios que se presenten a futuro dentro de la organización FAME S.A.

REFERENCIAS

[1] Bertrand, A. L. (1972) Social Organization: A General System and Role Theory Perspective. Davis, F.A. (ed.), Philadelphia: P. A.
[2] Aamodt, A., Paza, E. (1994) Case Based Reasoning: Foundational Issues, Methodological Variations, and System approaches. AI Communications, 7(1): 39-59.
[3] Hammer, M. (1990) Reengineering Work: Don´t Automate, Obliterate. Hardvard Business Review, July-August, pp. 104-112.
[4] Javier Areitio, (2007) Seguridad de la Información. Redes, Informática y Sistemas de Información, Idiomas: Español