DISEÑO E IMPLEMENTACIÓN DE UNA POLÍTICA DE SEGURIDAD

NÉSTOR DARÍO DUQUE MÉNDEZ*

PC: Auditoría, seguridad, políticas de seguridad, plan de seguridad.
KW: Audit, security, computer security policies, security plan.

RESUMEN

El término Políticas de Seguridad, en particular las de Informática PSI, se usa de muchas formas y dando connotaciones diferentes, lo cual en ocasiones hace que se pierda, para muchos, su gran importancia en la tarea de la implementación de la seguridad en las empresas. Este artículo presenta una visión integral y compleja de este problema y la forma de enfrentar la ardua tarea de diseñar e implantar las PSI, a las cuales solo se hará referencia como Políticas de Seguridad. Se divide en etapas, iniciando en el proceso de venta de la idea, generando conciencia sobre la importancia de su definición para las organizaciones, continuando con las actividades relacionadas con el conocimiento de los activos y servicios informáticos y los riesgos a que están expuestos, llevando al diseño de las PSI representadas en un documento formal y dando las pautas para su implantación y constante actualización. Para su mayor entendimiento se representa en forma gráfica los elementos a tener en cuenta en cada paso. Podría cambiarse el nombre de este artículo y denominarlo Diseño de Políticas de Seguridad y Plan de Implementación y recogería completamente el objetivo que le ha sido encomendado.

ABSTRACT

The term Security Policies, in individual those of informatics PSI, is used in many forms and gives different connotations, which sometimes causes that, for many, the great importance in the task of the security implementation in companies is lost. This

* Profesor Universidad Nacional de Colombia. Sede Manizales. Departamento de Informática y Computación.

paper presents an integral and complex vision for this problem and the way to confront the arduous task of PSI design and implant. PSI is divided in stages, initiating in the idea marketing process, regarding its definition for the organizations, continuing with the activities related to the knowledge of the assets and T.I. services and the risks to that they are exposed, forwards to the design of the PSI represented in a formal document and set to the standards for its implantation and constant update. For its greater understanding, the elements to consider in each step in graphical form are represented. The name of this article could change and denominate as Security Policies design and implanting plan and would completely reach the objective that has been entrusted him.

Introducción

Rodríguez [ROD95] define la Política de Seguridad como el grupo de reglas y regulaciones que dicta cómo una organización protege, maneja y distribuye información sensible. En la práctica, es usual que la referencia a este término se haga teniendo en mente unas cuantas directrices sobre claves de acceso y respaldo de información. Pero las Políticas de Seguridad se deben enfocar desde una perspectiva de mayor importancia, pues son pieza fundamental en el proyecto de plan de seguridad de una instalación. Como lo plantea Cabrera Martín [CAB00] la forma adecuada para plantear la planificación de la seguridad en una organización debe partir siempre de la definición de una Política de Seguridad que determine el QUÉ se quiere hacer en materia de seguridad en la organización para a partir de ello decidir mediante un adecuado plan de implementación el CÓMO se alcanzarán en la practica los objetivos fijados.

Algunos autores orientados a temas de seguridad informática le han dado gran importancia, tal es el caso de Chris Hare y Karanjit Siyan, quienes en su libro de seguridad en redes han dedicado un capitulo completo a Política de Seguridad, planteando que "definir una Política de Seguridad de red significa elaborar procedimientos y planes que salvaguarden los recursos de la red contra la pérdida y daño" [HAR97]. La RFC 1244, posteriormente actualizada con RFC 2196 aborda en detalle la Política de Seguridad de un sitio. Este último documento, a pesar de referirse a ambientes expuestos a Internet, será importante guía para el desarrollo de este artículo [FAQ97]. Apoyados en la definición de RFC 2196 una Política de Seguridad es un documento formal de reglas para todos los usuarios que tienen acceso a los recursos, tecnologías e información de la organización. No es una descripción técnica

de mecanismos de seguridad, ni una expresión legal que involucre sanciones a conductas de los empleados, es mas bien una descripción de lo que deseamos proteger y el por qué de ello [CAN01].

Para lograr estos objetivos se debe pasar por una serie de pasos que involucran muchos aspectos y personas. Como plantea el trabajo citado de Hare y Siyan, se parte de la visión que se tenga de la seguridad, la que se mueve entre dos posturas o enfoques:

1. Lo que no esté expresamente permitido está prohibido
2. Lo que no esté expresamente prohibido está permitido.

Como una forma de englobar todo lo planteado anteriormente y viendo este asunto desde una óptica integral, como un proceso donde el documento formal es solo un paso y entendiendo la seguridad informática como los procedimientos y mecanismos utilizados para garantizar un razonable grado de protección de los recursos informáticos, se presenta a continuación una propuesta de metodología que facilita esta labor, que como se aprecia no es nada fácil.

Etapas en el diseño e implementación de una política de seguridad

Como se muestra en la figura 1, el diseñar una Política de Seguridad para su posterior implementación no puede ser un acto caprichoso, de momento, de moda; es un proyecto completo que debe ser asumido con la mayor responsabilidad si se quiere lograr el efecto buscado. Cada una de estas etapas cumple papel importante en el exitoso final del proyecto.

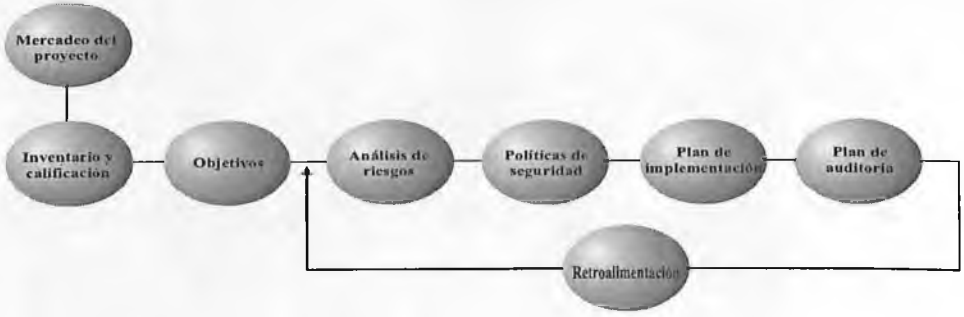

Fig. 1. Etapas en el diseño e implementación de una política de seguridad

Recorriendo cada uno podemos ver que tareas en concreto se deben desarrollar y cual es la razón para su inclusión en la propuesta metodológica planteada.

Mercadeo del Proyecto

Vender un nuevo proyecto nunca es fácil y mas si se trata de asuntos relacionados con la seguridad en sistemas, donde muchos consideran que no tienen riesgos o no son de su interés y piensan que las Políticas de Seguridad basta con copiarlas de otras instalaciones o usar el sentido común para expedir un recetario de normas. Como se aprecia en la figura 2, se pueden usar diferentes estrategias para involucrar a la alta gerencia en el proyecto, sin la participación de la cual jamás se logrará llevarlo al punto que se requiere. Esta etapa enfrenta el poco interés de las altas directivas de la empresa, el desconocimiento de la importancia de la seguridad informática y el exceso de tecnicismo de los expertos en seguridad. Para facilitar el trabajo de concientización es bueno apoyarse en casos de fallos de seguridad ocurridos en negocios similares y los efectos generados; hacer notar la responsabilidad que cabe a las empresas que no han realizado los esfuerzos necesarios para minimizar los riesgos y que debido a ello pueden infringir normas legales o afectar a otros; para finalizar se puede evaluar la razón costo/beneficio de las medidas tendientes a enfrentar con seriedad los aspectos relativos a seguridad y que el no hacerlo podría llevar a graves problemas de imagen y prestigio de la organización.

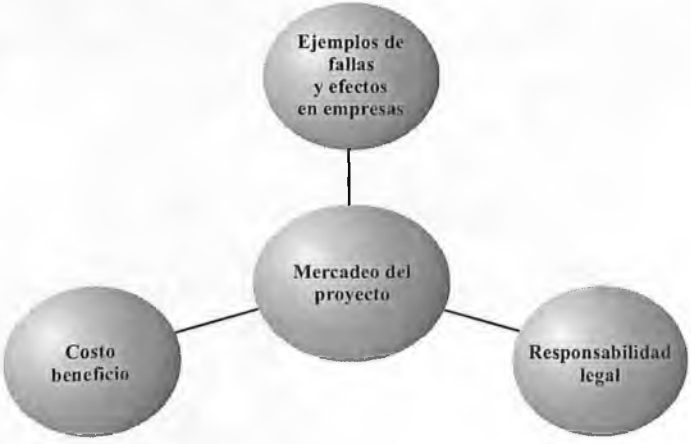

Fig. 2. Etapa de mercadeo del proyecto

Inventario y Calificación

Para saber que hay que proteger es necesario hacer un juicioso inventario de recursos informáticos (hardware, software y liveware), y de los servicios ofrecidos, donde se determine la importancia para la organización y el grado de criticidad de cada uno. En la figura 3 se aprecian estos elementos.

Fig. 3. Etapa de inventario y calificación

Determinar los Objetivos

Están asociados, como se aprecia en la figura 4, a los objetivos de la Seguridad Informática, orientados a proteger la organización contra amenazas que atenten contra:

1. La continuidad de las operaciones.
2. La confidencialidad y privacidad de la información manejada.
3. La confiabilidad y exactitud el sistema
4. La seguridad física.

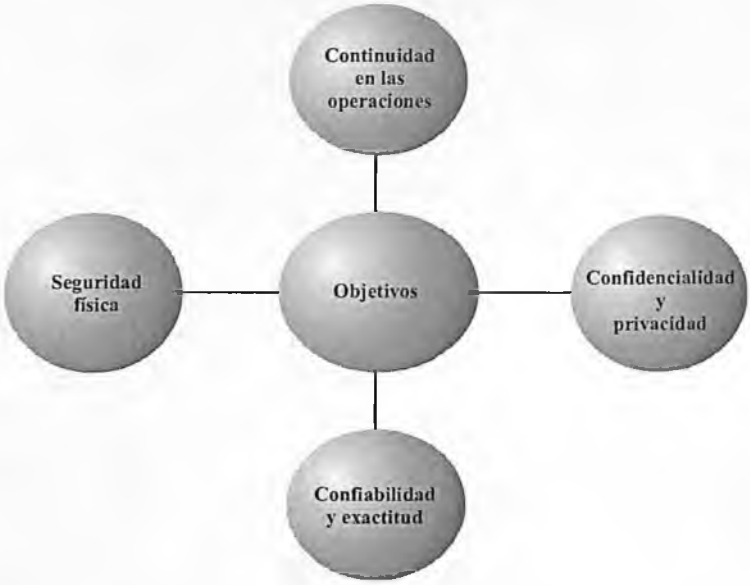

Fig. 4. Objetivos de la seguridad

Muchos son los riesgos a que se ve expuesta una instalación informática que podrían desviarla de las metas trazadas y la Política de Seguridad debe convertirse en la línea base para enfrentar estas situaciones, para lo cual se debe realizar un estudio concienzudo de las amenazas reales o potenciales.

Análisis de Amenazas

En la figura 5 se aprecian algunas de las posibilidades que se tienen de conocer los riesgos que se presentan para los diferentes recursos de la organización.

La metodología de **Análisis de Riesgos,** desagrega la situación de riesgo evaluada en Escenarios de Riesgos [AUD92]. A partir de esto se procede a:

1. Elegir un Escenario de Riesgo E.R.

2. Determinar las Actividades Sujetas a Control (A.S.C.) asociadas al E.R.

3. Elegir una A.S.C.
4. Identificar amenazas relacionadas a la A.S.C. elegida.
5. Tomar una amenaza.
6. Preseleccionar la mezcla de controles para proteger la instalación contra la amenaza elegida
7. Repetir los pasos 3 a 6.
8. Escoger otro E.R. hasta que se hayan agotado y repetir desde paso 2.
9. Seleccionar los controles a recomendar.

Fig. 5. Métodos de análisis de amenazas

Como se aprecia es un método bastante dispendioso, sobre todo cuando las instalaciones son de tamaño considerable.

Los **formatos de calificación** recogen la información de cada recurso, la importancia relativa que tiene, los tipos de usuarios asociados a situaciones indeseables, las posibles amenazas y las medidas a implantar para proteger suficientemente los activos contra esos riesgos.

Como otra forma, pero casi siempre acompañando algunos de los métodos anteriores se recurre a la **opinión de expertos** y a las **vivencias de los usuarios** del sistema, para recolectar información de los probables riesgos y los efectos a que están expuestos los procesos o corrientes de información.

Política de Seguridad Informática

Después de los pasos previos y con los conocimientos ganados se procede a la construcción del documento formal que incluirá los diversos elementos y para lo cual se deben tener en cuenta los aspectos mostrados en la figura 6. Debe entenderse esta etapa como la del diseño de la Política de Seguridad y deben quedar especificados los diferentes componentes que cubrirá y la forma como se aplicará la misma.

La Política de Seguridad tiene dos **propósitos** centrales: Informar a todos los usuarios sobre las obligaciones que deben asumir respecto a la seguridad asociada a los recursos de tecnología de Información T.I y dar las guías para actuar ante posibles amenazas y problemas presentados.

Para que pueda convertirse en esa línea guía, es necesario involucrar a los diferentes sectores en la organización: Alta gerencia, responsables de T.I., los encargados de seguridad, los auditores, gerentes de las dependencias y representantes de los usuarios.

El documento formal debe **definir elementos** asociados la adquisición de hardware, software y contratación de servicios externos teniendo presente los aspectos referentes a seguridad (outsourcing, mantenimiento a hardware y/o software, desarrollo de aplicaciones, administración de proyectos, etc.); las disposiciones sobre privacidad y control de acceso incluidas las políticas de autenticación; las responsabilidades asociadas a las métodos de actuación y el manejo de incidentes. Un aspecto importante es la declaración de disponibilidad, entendida como el compromiso que hace el área de sistemas informáticos sobre el mínimo nivel la prestación de servicios en términos de tiempo y cobertura que se garantizará [FAQ97].

Un reto importante es lograr todo lo anterior emitiendo un documento sencillo y claro, apoyado por la alta dirección, que permita la normal actuación, haciendo de las políticas procedimientos inmersos en los tareas cotidianas, enfocados a los problemas relevantes, fácil de ajustar a los cambios permanentes, que garanticen su cumplimiento apoyándose en herramientas de seguridad antes que orientado a castigar a los

infractores, lo cual no se descarta. Pero hay que resaltar algunas características que hacen de ella una **buena Política de Seguridad:** La constante actualización y el hacerla pública y respaldada por los usuarios en la vida practica.

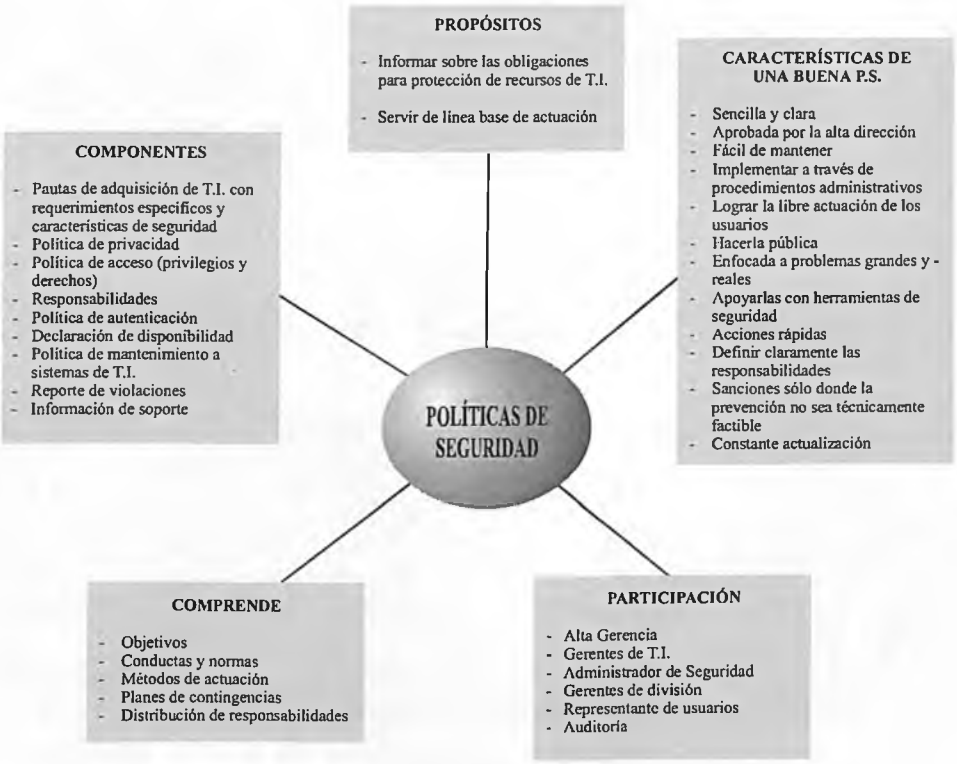

Fig. 6. Elementos asociados a las políticas de seguridad

Plan de Implementación

Terminado el diseño, se procede a la fase de construcción. La figura 7 muestra a grandes rasgos las tareas que se deben realizar.

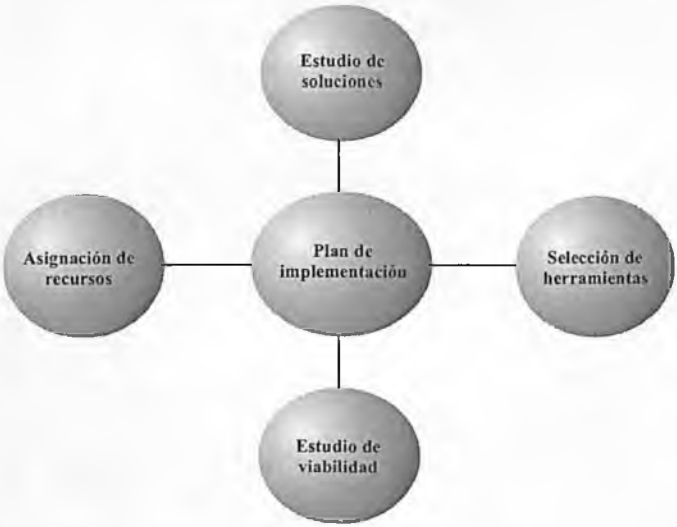

Fig. 7. Plan de implementación

Plan de Auditoría

En un medio cambiante y en especial en las nuevas tecnologías informáticas y de comunicación, no ha pasado mucho tiempo sin que las condiciones varíen, esto puede llevar a nuevos riesgos y debe actuarse proactivamente para lograr los sistemas autocontrolados que tanto se pregonan. La labor de auditoría entendida como la evaluación y análisis de esa realidad, en forma critica, objetiva e independiente, con el objeto de evaluar el grado de protección que presenta una instalación ante las amenazas a que está expuesta; es parte importante del diseño e implantación de Políticas de Seguridad. No basta con diseñar buenas políticas es necesario llevarlas a la práctica en forma correcta y garantizar que se adecuan a nuevas condiciones.

Retroalimentación

La implementación de Políticas de Seguridad, genera diferentes situaciones en los negocios lo que obliga al mantenimiento constante. Los cambios deben iniciarse con un nuevo análisis de riesgos en el sistema de información o detectados en la labor de auditoria.

Conclusiones

La Política de Seguridad es una herramienta de gran valor para enfrentar el Plan de Seguridad de una instalación y debe entenderse como un proceso integral que parte de la situación real y se construye teniendo en cuenta los recursos y riesgos a que esta expuesta la organización, convirtiéndola en una línea guía de operación y actuación para proteger los activos y garantizar la continuidad y calidad de los servicios ofrecidos. Pensar en que es suficiente con emitir un documento formal y general, sin consultar la realidad de la empresa en particular y sin lograr vincular a los diferentes sectores involucrados conducirá a resultados estériles. Igual situación si luego de implementada no se está revisando y actualizando permanentemente para ajustarla a los nuevos riesgos.

BIBLIOGRAFÍA

[ROD95] RODRÍGUEZ, LUIS ÁNGEL. Seguridad de la Información en Sistemas de Computo. Ventura Ediciones, México, 1995.

[CAB00] CABRERA MARTÍN, ÁLVARO. Políticas de Seguridad. Boletín del Criptonomicón #71.Madrid, 2000.

[HAR97] HARE, CHRIS. SIYAN, KARANJIT. Firewall y la Seguridad en Internet. Segunda edición. Prentice Hall. México. 1997.

[FAQ97] FAQS ORGANIZATION. RFC2196 - Site Security Handbook. Septiembre 1997. http://www.faqs.org/rfcs/index.html.

[CAN01] CANO, JEIMY J. Pautas y Recomendaciones para Elaborar Políticas de Seguridad Informática (PSI). Bogotá. 2001.

[AUD92] AUDISIS LTDA. Seminario Auditoría de Sistemas. Bogotá. 1996.