Conclusiones

Conclusiones

La implementación de políticas de seguridad informática en una organización es una solución integral que no sólo busca proteger, preservar, administrar de una manera eficiente todo tipo de recursos con los que cuenta una organización, sino que también busca dar solución, prevenir, evitar, controlar y minimizar los daños de incidentes que afectan a la organización, por esto, preparar y capacitar al personal en temas asociados a la seguridad informática y cómo hacer frente a incidentes que se llegarán a presentar con el fin de responder de una manera adecuada es una de las principales metas de esta estrategia.

Contrariamente a lo que podría pensarse como un obstáculo para la realización de las diversas actividades por el hecho de ser necesario seguir y respetar lineamientos, recomendaciones, reglas, normas o protocolos, que pudieran entorpecer los procesos, actividades y trabajo que se realiza es una idea errónea por el hecho de que previamente a la implementación de las políticas se realiza un análisis o estudio ya que esta estrategia tiene como uno de sus principios no interferir o interferir lo menos posible en los procesos y actividades que se realizan en la organización.

Por otra parte es necesario capacitar al personal para que éste pueda tomar un papel activo dentro de la organización de manera que aplique este conocimiento en las diversas actividades que realiza dentro y fuera de la organización con el propósito de proteger de una forma adecuada la información que se le confía, así como la propia.

Contar con una buena implementación de políticas de seguridad informática debe ser un punto clave en toda organización, de lo contrario se habrá caído nuevamente en un error que puede perjudicar y causar pérdidas graves que pudieran haberse prevenido, sin embargo, es necesario destacar que para que dicha implementación sea efectiva debe tener el apoyo y participación de todas las áreas, departamentos o ramas que integran la organización.

Las políticas de seguridad informática son la base para todo programa de seguridad por lo que es necesario contar con una documentación adecuada la cual debe contener un programa de difusión, monitoreo, revisión y actualización como parte de un ciclo para el mantenimiento de esta estrategia, esto es, que exista un ciclo de mejora continua ya que en la medida en que cada una de las fases de mantenimiento y desarrollo de las políticas de seguridad informática sean desarrolladas se tendrá un mejor resultado. (Figura C.1).

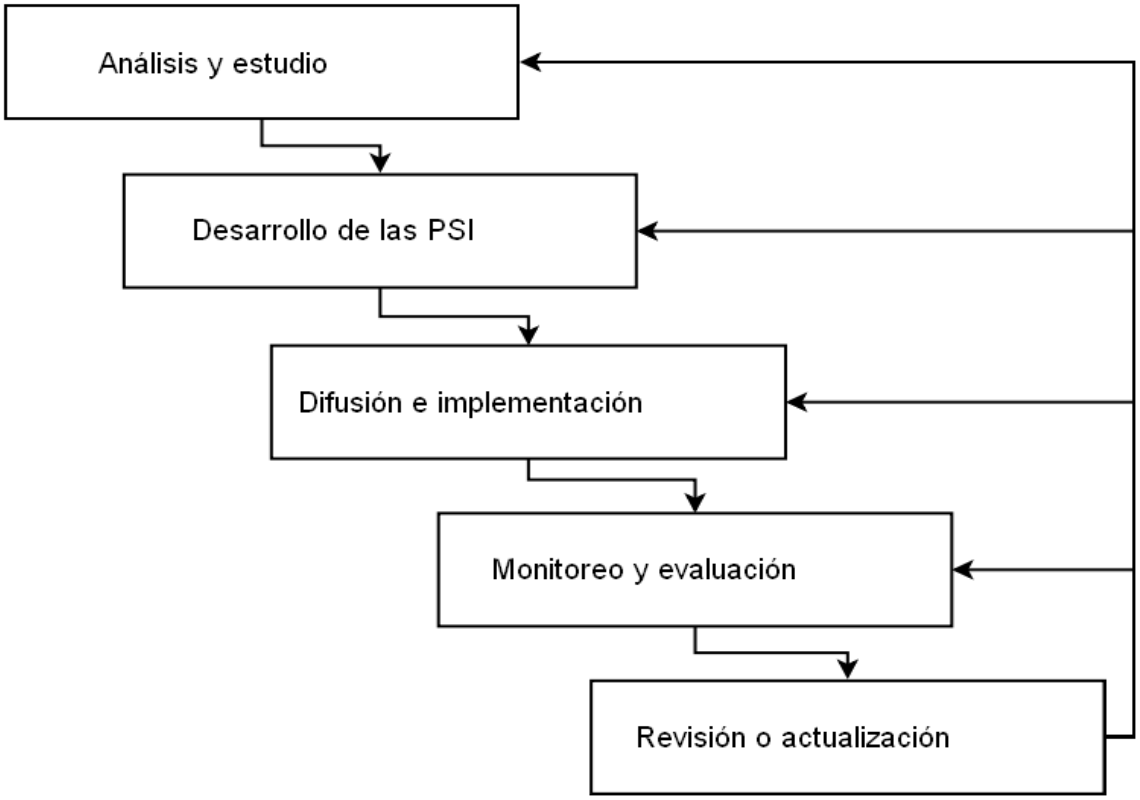

Figura C.1 Ciclo de mantenimiento y desarrollo de las Políticas de Seguridad Informática (PSI).

La investigación realizada fue aplicada para el caso particular de la Facultad de Ingeniería (FI), es decir, se realizó una revisión y actualización de las políticas de seguridad en cómputo, la cual consistió en la aplicación de lineamientos y recomendaciones para el desarrollo de políticas con el fin de que el documento que se tiene sea más completo, actualizado y claro, esto aunado a una propuesta de difusión que consiste en la creación de una página web que está diseñada con la finalidad de que el usuario pueda consultar las políticas de seguridad de una manera más sencilla y rápida.

Con la idea de tener una mejor difusión de esta información, este documento contiene también diferentes recomendaciones para ayudar a la propagación y divulgación del conocimiento sobre el área de la seguridad informática en la comunidad que conforma la Facultad de Ingeniería (FI).

Además de la realización de esta propuesta, la investigación presenta una serie de recomendaciones y lineamientos que pueden ser apoyo para el desarrollo y revisión de políticas o

reglamentos complementarios por parte de las diferentes áreas, departamentos o divisiones que la conforman.

Se proponen también diversas estrategias para la realización de revisiones y actualizaciones posteriores a las Políticas de Seguridad en Cómputo de la Facultad de Ingeniería (PSC-FI), con el objetivo de que los responsables de la seguridad informática o en cómputo implementen una metodología de mejora continua de manera que los procesos en la implementación, así como los diferentes servicios y actividades que se realizan en la organización para el mantenimiento de un nivel adecuado de seguridad informática mejoren y puedan incorporar cambios de manera más dinámica y en menor tiempo.