Difusión de las políticas de seguridad informática de la Facultad de Ingeniería

6. Difusión de las políticas de seguridad informática de la Facultad de Ingeniería

La difusión de las PSI es parte indispensable dentro de cualquier programa de seguridad informática que se quiera implementar por el hecho de requerir que todos y cada uno de los que conforman la organización formen parte de este esfuerzo conjunto para la generación de un buen nivel de seguridad, el cual trae consigo ventajas para el mejor aprovechamiento de los recursos informáticos de la misma forma al evitar diversos tipos de incidentes.

Se podría pensar que difundir las políticas de seguridad a todo el personal es el equivalente a entregar información que cualquiera pudiera usar para la realización de un ataque, sin embargo, esto no es así.

Para aclarar esta idea se puede decir que publicar las políticas de seguridad es como colocar un cartel para que todos los habitantes de un edificio estén enterados de la importancia de seguir reglas como son: que al salir deben cerrar con llave y que en el caso de que alguno de ellos perdiera dicha llave debe avisar de inmediato al responsable de la puerta.

Esta información contrariamente a lo que se piensa no proporciona algún dato que pueda ser utilizado por algún atacante, sino que por el contrario, le notifica que la puerta está cerrada y que en caso de conseguir o robar alguna llave esto haría que los habitantes informaran de la situación para la realización de acciones preventivas o que corrigieran dicho error.

Al igual que el cartel en el edificio el cual contiene las reglas, explica la importancia de los lineamientos contenidos en él y que puede ser visto por todo el mundo (habitantes, vecinos, invitados y extraños), las políticas de seguridad establecen lo que se debe o necesita y el porqué, pero no establecen él cómo[20].

Al no establecer él cómo, qué herramientas, dispositivos, y en qué forma se realizó la implementación dificulta la tarea de un atacante al desconocer los tipos de tecnologías, marcas, dispositivos, y herramientas que fueron utilizadas para la implementación de las políticas, esto aunado al conocimiento de la existencia de diversas medidas preventivas y reactivas complica y dificulta más la tarea del atacante, lo que pudiera hacer que éste perdiera su interés por la complejidad, y el costo necesario para la realización de un ataque.

[20] Capítulo 3 en el apartado 3.3 Correcta redacción de las políticas de seguridad.

La etapa de difusión consiste en propagar, divulgar y difundir las PSI, así como sus objetivos, metas y beneficios con el fin de crear conciencia en todo el personal de la organización acerca de lo importante que es que se sigan y se respeten aun cuando el personal no se encuentre dentro de la organización.

Para que se cumpla esta etapa es necesario que se tenga en cuenta que existen usuarios, los cuales no tienen un conocimiento básico o poseen limitaciones con respecto al lenguaje relacionado con los temas de la seguridad informática, por lo cual es necesario el uso de un lenguaje, así como términos adecuados mediante el cual estos usuarios puedan comprender a cabalidad, de manera que se les facilite la curva de aprendizaje.

De esta forma al buscar que dichos usuarios entiendan de una manera general estos temas es un gran avance en la etapa de difusión, no obstante es necesario también el motivar a estos usuarios a querer aprender acerca del tema, a que estén interesados de manera que puedan ser capacitados de una mejor y más rápida forma.

Con el fin de motivar y hacer esto posible es necesario mostrar las ventajas o beneficios que se obtienen al seguir las políticas de seguridad, es decir, se debe mostrar a los usuarios la parte práctica en la cual se muestre la eficacia de esta estrategia que busca el no sólo proteger a la organización, sino que va aun más allá protegiendo los activos personales de cada usuario.

Por lo anterior se puede afirmar que la difusión consiste en divulgar la información y el conocimiento acerca de las políticas de seguridad desde un punto más práctico y amistoso, es decir, que busque acercar estos temas al usuario de una manera amigable con el objetivo de motivar a todo tipo de usuario para que se capacite, respete y promueva el uso de las PSI en todo momento tanto dentro como fuera de la organización.

Sin embargo, en ocasiones esto no se llega a concretar, por diversas razones como son la falta de tiempo, de recursos, la falta de personal, la falta de apoyo por parte de la organización, o por fallas en la estrategia de difusión. Los resultados obtenidos provenientes de fallas en programa de difusión son el ver a las PSI como una pérdida total o parcial de tiempo y de recursos por el hecho de que los usuarios no siguen y respetan las políticas, esto en otras palabras; seguir y respetar procedimientos, lineamientos y normas que el usuario califica como “molestas y poco prácticas”.

La falta de resultados es uno de los principales argumentos que pueden ser usados para desacreditar la efectividad de las políticas de seguridad por el hecho de que la gente piensa que esta estrategia resolverá y hará desaparecer cualquier tipo de problema asociado con la se-

guridad informática, como pasa cuando alguien tiene problemas con los distintos tipos de malware (virus, gusanos principalmente), se piensa que al instalar un antivirus resolverá todos los problemas que tiene el equipo, sin embargo, esto no es así, ya que en caso de que el antivirus no resolviera los problemas, el usuario decide cambiar de antivirus por el hecho de que éste no es efectivo.

En el caso de las PSI, los resultados y la efectividad dependen en gran manera de la participación y capacitación adecuada de todo el personal que conforma la organización ya que en la manera en que cada individuo entienda la importancia de la información que le fue confiada para la realización de su trabajo, así como la propia, estará directamente relacionada con el nivel de seguridad, es decir, entre mejor capacitación y participación del personal haya, el nivel de seguridad será mucho más alto.

Por lo anterior, es necesario que en cualquier organización exista una capacitación adecuada[21] (Tabla 6.1), la cual depende en gran parte de que exista un programa de difusión que tenga el objetivo de acercar al usuario a las PSI.

Tabla 6.1 Casos que se presentan al capacitar al usuario.

Capacitación		
Buena	Mala	Errónea
Bien capacitado tiene una clara idea de lo importante que es la información. Sabe cómo proteger los activos o bienes tanto propios como los que la organización confía en él.	Está expuesto a un posible incidente por no tener una buena capacitación. Propensión a cometer errores que pueden facilitar la pérdida, destrucción, mal uso de la información o el facilitar un incidente.	Actúa con temor ante cualquier tipo de actividad con la idea de que todo el mundo es un posible atacante que busca robar o destruir su información.

[21] Capítulo 3, apartado 3.4 Puntos importantes a considerar en las políticas de seguridad, sobre las ventajas asociadas a un buen documento.

6.1 Propuestas para una mejor difusión

La realización de una propuesta efectiva para la difusión de las PSI que provea al usuario con el conocimiento necesario para entender acerca de estos temas y que pueda hacer frente a incidentes de manera que pueda realizar y aplicar medidas preventivas así como reaccionar ante incidentes que puedan acontecer en el futuro.

Con el objetivo de realizar una propuesta efectiva es necesario la obtención de observaciones, comentarios y la retroalimentación por parte del personal de la organización respecto a los conocimientos sobre estos temas, cuáles son las medidas que ellos realizan al tener algún tipo de incidente, dónde sería un buen lugar para almacenar, consultar y distribuir información relacionada con estos temas, etcétera.

El recopilar información del estado de capacitación, conocimiento y actividades del personal es sumamente importante para la realización de un buen programa de difusión. Es por esto que se buscó la obtención de esta información a través de entrevistas a responsables de la seguridad informática, así como encuestas aplicadas a la población en general de la Facultad de Ingeniería con el fin de realizar una buena propuesta.

Para la realización de esta etapa se recomiendan las siguientes acciones, con base en las observaciones realizadas anteriormente, así como de los resultados obtenidos de la aplicación de la encuesta[22]:

1. Uso de publicidad

El uso de publicidad que contenga información concreta acerca de las PSC de la Facultad de Ingeniería (FI), esta información puede ser una dirección electrónica donde se encuentre una página, esto con el fin de que la información que contenga este cartel sólo sea para informar al usuario acerca del lugar donde se puede encontrar dicha información, sin embargo, es necesario que el cartel contenga información acerca del tema que indique lo que encontrará y para qué es, así como alguna ilustración acorde con el tema que pueda dar una idea y atrape la atención del usuario.

[22] Pueden consultarse los documentos en los apéndices 1, 3 y 2 respectivamente.

Un ejemplo de este tipo de carteles o publicidad se muestra a continuación, en la cual se hace mención de una serie de fallas que pueden evitarse. (Figura 6.1).

Figura 6.1 Publicidad para difusión de las PSC-FI

Este tipo de errores que los usuarios cometen y los problemas más comunes con los que los usuarios tienen que batallar son una fuente de ideas que se pueden utilizar para ayudar a la difusión y atrapar la atención de los usuarios con el fin de que visiten y conozcan el sitio donde puedan consultar las políticas.

Este tipo de publicidad debe ser puesta en lugares donde exista una gran afluencia de usuarios, es decir, en lugares donde exista un tránsito abundante o en lugares establecidos para la difusión de otro tipo de publicidad donde normalmente los usuarios acudan en busca de información de algún otro tipo.

Con este objetivo la encuesta[23] aplicada a alumnos de la Facultad de Ingeniería (FI), reveló que uno de los lugares donde los alumnos se enteran de información concerniente a diversas actividades además de ser uno de los lugares más frecuentado por los alumnos es la biblioteca, por lo que éste sería un buen lugar para colocar publicidad. De la misma forma se puede realizar algún tipo de publicidad en la página principal de la Facultad donde se

[23] Apéndice 2, Encuesta aplicada a alumnos de la FI, UNAM.

busque y el visitante pueda consultar dicha información en una página especializada acerca del tema.

Algunos otros lugares en donde la comunidad de la Facultada de Ingeniería (FI) busca o se entera de diversos avisos son la entrada principal del Edificio Principal, los lugares que se tienen para colocar publicidad (pizarrones), la entrada de los laboratorios, pasillos y en los salones.

2. Platicas, campañas, conferencias y seminarios

El dar pláticas introductorias a los profesores y académicos de toda la Facultad de ingeniería (FI), es una de las maneras en las que se puede propagar y capacitar a una buena parte del personal ya que a través de ésta todo el conocimiento llega a los alumnos. Los procedimientos, las acciones y las medidas que los académicos tomen y comenten al momento de trabajar con los alumnos ayudarán a los alumnos y demás personal que labora con los académicos a entender y a consultar las Políticas de Seguridad en cómputo de la Facultad de Ingeniería (PSC-FI).

Estas pláticas pueden ser también impartidas a los alumnos y personal administrativo a lo largo de campañas cada semestre, las cuales abarquen los temas relacionados con las PSI así como temas asociados a la Seguridad Informática, éstos deben ser abordados de manera práctica, es decir, deben ser enfocados a usuarios con un conocimiento muy básico o casi nulo que ayude a comprender acerca de ellos, en otras palabras facilitar el aprendizaje de cierto conocimiento básico con el fin de acercar más a los usuarios a las políticas y a la seguridad informática y que éstos no tomen a las PSC-FI como un documento más.

A lo largo de esta campaña debe fomentarse el uso y consulta de las PSC-FI, además es necesaria la realización de mesas redondas, seminarios o talleres en los cuales los usuarios puedan participar más activamente para comentar sus dudas e inquietudes acerca del tema, las cuales deben ser esclarecidas y contestadas.

Los talleres y seminarios pueden ser organizados por las diferentes divisiones a lo largo del semestre en coordinación con expertos del tema con el fin de que se puedan realizar diferentes actividades como capacitación de personal, desarrollo de políticas, difusión de las mismas, aclaración de dudas, revisión de políticas internas o reglamentos, entre otras.

3. Sitio WEB

Como parte de este trabajo se diseñó y construyó un sitio web, el cual tiene como meta ser una herramienta para la difusión de las PSC-FI, con este propósito se ideó que el diseño de dicho sitio esté enfocado a la simplicidad, buscando que auxilie al usuario en la búsqueda, capacitación y enseñanza de información de manera que no sea ajena o tediosa para los usuarios sino que sea una herramienta práctica que promueva el uso y consulta de los documentos (PSC-FI) para la prevención, solución, corrección, e implementación de medidas que ayuden a establecer un nivel apropiado de seguridad informática.

Para la etapa de diseño de la página se siguió la normatividad web[24], la cual regula la información contenida en las páginas, el uso de logotipos, las imágenes, así como el establecimiento de lineamientos y recomendaciones para el diseño de las mismas. Tomando en cuenta lo anterior y que el sitio que se estaba diseñando contendría información que el usuario debe ver de una manera respetuosa y a la vez ligada con la formalidad de la organización, se optó por el uso de los colores rojo y blanco, por el hecho de ser éstos colores asociados con la Facultad de Ingeniería además de estar presentes en la página principal.

El diseño que se eligió para el sitio fue escogido con base en que lo principal de éste es la información contenida, por lo que se decidió que el contenido debía estar a la izquierda, de manera que el usuario enfocará su atención en esa parte. Se decidió colocar un menú principal en la parte superior que no cambiara para facilitar la navegación dentro del sitio y un menú auxiliar, el cual se encuentra en la parte derecha conteniendo vínculos (links) que tuvieran información asociada con el contenido de la página.

A continuación se muestra un esbozo de la estructura definida anteriormente, (Figura 6.2).

[24] http://www.ingenieria.unam.mx/cacfi/documentos/normativiadweb.pdf, 2010

<table>
<tr><td>Logo FI</td><td>Título de la página</td><td>Logo UNAM</td></tr>
<tr><td colspan="3">Menú principal</td></tr>
<tr><td colspan="2">Contenido</td><td>Menú de navegación</td></tr>
<tr><td colspan="3">Pie de página</td></tr>
</table>

Figura 6.2 Diseño de la página web

Estructura general y organización del sitio.

El menú principal está estructurado para poder ir a las 4 páginas principales, las cuales están auxiliadas por el menú de navegación que puede o no cambiar dependiendo del contenido del sitio con la finalidad de proporcionar rapidez al momento de buscar información.

A continuación se presenta una breve descripción de las 4 páginas principales y sus contenidos.

1. **Inicio**

Es la página inicial en la cual se tiene la bienvenida al sitio, un resumen sobre lo que éste contiene y un mapa general, por último tiene un apartado sobre los requerimientos del sitio.

2. **PSC-FI**

Dentro de esta página se encuentra un breve resumen acerca de las PSC-FI, su filosofía, y su objetivo general, también contiene un mapa que ayuda al usuario a navegar por este documento. Cada una de las partes en las que fue estructurado este documento cuenta con una breve descripción con el fin de agilizar la búsqueda de información por parte del usuario, es decir, se facilita la consulta de información.

Se decidió que las PSC-FI fueran estructuradas en 4 partes las cuales son:

a. Generalidades

Contiene documentos que tratan acerca de las políticas como la filosofía a seguir, el organismo responsable del documento, los servicios de seguridad que se buscan con la implementación de las políticas.

b. Políticas

A lo largo de esta parte se tratan las políticas a implementar dentro de la FI, además de las sanciones aplicables para cada caso.

c. Buenas prácticas

Esta parte tiene las recomendaciones para el uso e implementación de algunas de las tecnologías, surge como apoyo para las políticas.

d. Códigos de ética

Los códigos de ética son lineamientos que deben seguir el personal y la comunidad en general de la FI, estos códigos contemplan la actitud y la normatividad a seguir por toda la comunidad en todo momento.

e. Gestión de contraseñas

Con el objetivo de una mejor organización se buscó que hubiera un apartado el cual pudiera ser de ayuda para la gestión de las contraseñas ya que es uno de los recursos más utilizados de acceso y autenticación.

f. Glosario

Es un compendio de definiciones con el fin de esclarecer algunos términos utilizados.

3. **FAQ**

En esta parte se tienen las Frequently Asked Questions (FAQ), lo que en español se puede traducir como preguntas frecuentes, las cuales buscan dar respuesta a las dudas que le puedan surgir al usuario al navegar o ingresar a la página.

4. **Descargas**

La página contiene documentos y archivos como las PSC-FI, una guía para el desarrollo de PSI, un formato para reportar incidentes de seguridad, entre otros.

Herramientas y tecnologías utilizadas para la construcción del sitio.

Para la realización del sitio se tomaron en cuenta diversas consideraciones como el uso de las tonalidades en los colores, un ejemplo de esto es que el fondo, el cual no es completamente blanco ya que un fondo blanco contrasta mucho y puede ser molesto. En cuanto a las tonalidades de los colores utilizados están asociados con la seriedad y sobriedad por el hecho de que el sitio contendrá información que el usuario no debe tomar a la ligera, de manera que esto debe verse reflejado a lo largo de todo el sitio.

En la construcción de este sitio se decidió el uso de Cascading Style Sheets (CSS) u hojas de estilo CSS con la idea de dar estructura al documento, ya que este tipo de código es compatible con todos los navegadores, además de ser un recurso muy socorrido por los programadores de páginas HTML o páginas WEB.

La programación de la hoja de estilo fue de manera externa, es decir, el archivo CSS está referido a cada una de las páginas HTML, con lo que se obtuvo una ventaja al reducir el código, otra ventaja es que al tener un solo archivo CSS se puede cambiar una gran variante en las características del sitio con sólo modificar ese archivo.

Por las ventajas y características que proporciona el uso de las hojas de estilo se decidió su uso, la cual fue programada en bloc de notas o editor de archivo de texto plano.

Las páginas fueron desarrolladas en editores de texto plano, al igual que se realizó con las hojas de estilo CSS, en este caso son archivos HTML y la aplicación (verificador de contraseñas), fue realizado en Macromedia Flash esto con el objetivo de que fuera más agradable para el usuario, además de ser uno de los programas más utilizados en los sitios WEB.

Un punto importante al respecto del uso de esta herramienta para la realización del verificador de contraseñas fue el que Macromedia Flash ofrece software gratuito a los usuarios para la ejecución este tipo de aplicaciones en los diversos navegadores. Esta aplicación tiene el objetivo de ser una herramienta para la ayuda del usuario en el tema de gestión de contraseñas por lo que dentro del sitio se ofrece al usuario el poder descargar un archivo ejecutable para su uso personal.

Por otra parte los archivos a descargar fueron exportados a archivos PDF, ya que el software para leer este tipo de archivos también es gratuito y muy usado para la lectura y consulta en la publicación de artículos, libros electrónicos, reportes, lecturas diversas, etcétera.

Se buscó también que el sitio tuviera un motor de búsqueda interno, es decir, que fuera independiente, además de ser gratuito, por lo que se decidió el uso de PHP para la implementación de búsquedas de información dentro de las páginas del sitio.

Estas tecnologías y herramientas fueron usadas por no presentar costo alguno para los usuarios ni para la organización, además de que son compatibles con los distintos navegadores en sus versiones más recientes, algunos de los navegadores más populares son: Internet Explorer de Microsoft, Mozilla Firefox por Mozilla Corporation, Crome de Google, Safari de Mac OS X y Opera de Opera Software.

Para que esto fuera posible el código utilizado en el sitio es compatible con estos exploradores en sus versiones más recientes, sin embargo, es recomendable el uso de Mozilla Firefox para la navegación en este sitio, no obstante, cabe aclarar que el sitio es totalmente compatible con el uso de Internet Explorer como explorador, el cual es aun el navegador de internet más utilizado.

Es importante mencionar que para la correcta ejecución del sitio se recomienda que se autorice el uso de los scripts y se instalen algunas aplicaciones como son el Adobe Flash Player (para la correcta ejecución del verificador de contraseñas) y el Adobe Acrobat Reader (para la lectura de algunos documentos). Este tipo de requerimientos ya están contemplados dentro del sitio por lo que el usuario pude consultar y recibir ayuda para la descarga de estas aplicaciones.

Con respecto a la organización y estructuración del contenido de las políticas se procedió a reunir y reorganizar o reestructurar la información acerca de las políticas de seguridad a manera de crear el sitio con el objetivo de que la navegación a través de éste sea lo más funcional, es decir, que el usuario pueda navegar por el sitio y encontrar la información de

la forma más directa y rápida. En la siguiente figura se muestra una vista previa de una de las páginas (Figura 6.3).

Figura 6.3 Vista previa de la página

6.2 Actualización periódica de las políticas de seguridad informática de la Facultad de Ingeniería

En la realización de una actualización de las PSI de la FI, (PSC-FI) es necesario definir una estrategia para la actualización que establecer un tiempo de revisión por el hecho de buscar más la efectividad y funcionalidad que el cumplimiento de una planificación, por lo cual es necesario aclarar que una actualización es parte de un programa de mantenimiento de políticas el cual consta de varias etapas que se han descrito a lo largo de este trabajo.

Las etapas del mantenimiento y desarrollo de políticas de seguridad son:

1. Análisis y estudio
2. Desarrollo de las PSI
3. Difusión e implementación
4. Monitoreo y evaluación
5. Revisión y actualización

Este ciclo es necesario para la mejora continua de las PSI, y es indispensable que aun cuando se crea que es una etapa de ellas se considere como un todo y se lleve a cabo de manera eficiente, práctica, y detallada ya que dependiendo de la calidad con la que se lleve a cabo será directamente relacionada con los resultados que se obtendrán, es por esto que cada una de estas etapas no deben verse como elementos o parte sino como parte de un todo ya que en la medida en que cada una de estas etapas sea realizada, estará directamente asociada con los resultados.

A continuación se hace un breve resumen de este ciclo.

La primera etapa es el análisis y estudio de la organización en la cual se busca el saber qué se quiere proteger y de qué o quién se quiere proteger, ya terminada esta etapa se continúa con el desarrollo de políticas en la cual con la información recopilada se procede a la realización de normas, reglamentos, lineamientos, buenas prácticas, etcétera.

Terminadas estas dos etapas se procede a difundir las políticas creadas para que los usuarios y los administradores procedan a implementar dichas políticas dentro de sus centros de trabajo y laboratorios. Una vez implementadas las políticas viene la etapa de monitoreo y evaluación, en esta etapa las políticas implementadas son evaluadas por los usuarios, es decir, si son apropiadas, si causan conflicto en los procesos o actividades que desempeñan los usuarios, si requieren algún tipo de cambio o las políticas no funcionan y deben ser modificadas.

En esta etapa se realizan reportes que son enviados a los encargados de la seguridad y expertos que evalúan el desempeño de las políticas para rediseñar, modificar o realizar cambios que serán presentados ante un comité el cual estudiará dichos reportes para revisión o actualización de las PSI.

En la última etapa se tienen las observaciones, reportes y las evaluaciones que serán tomadas en cuenta por un comité que realizará la revisión, de manera que pueda corregir, cambiar o desarrollar nuevas políticas.

Es importante el mencionar que el comité encargado de la revisión y actualización evaluará toda la información obtenida y determinará a cuál de las cinco etapas debe recurrir de manera que se solucione y corrija el problema, es decir, desde esta última etapa se puede ir a cualquiera de las anteriores para continuar el ciclo de manera normal, pasando por las etapas faltantes esto con la meta de mejorar, cambiar o corregir las PSI.

Para ilustrar el ciclo del que se está hablando supóngase que al terminar se encuentra en la última etapa (Revisión o actualización) y la evaluación determinó que existió una falla en la difusión e implantación por lo que para eso es necesario volver a dicha etapa para la realización de acciones correctivas, por lo que después de realizar dichas acciones se procedería a la etapa de Monitoreo y evaluación (que es la etapa siguiente), una vez concluida ésta, se pasaría a la última etapa evaluando la nueva información recopilada proveniente de las acciones previamente tomadas pudiendo así nuevamente saltar a alguna de las etapas anteriores. En la Figura 6.4 se presenta un esquema de este ciclo.

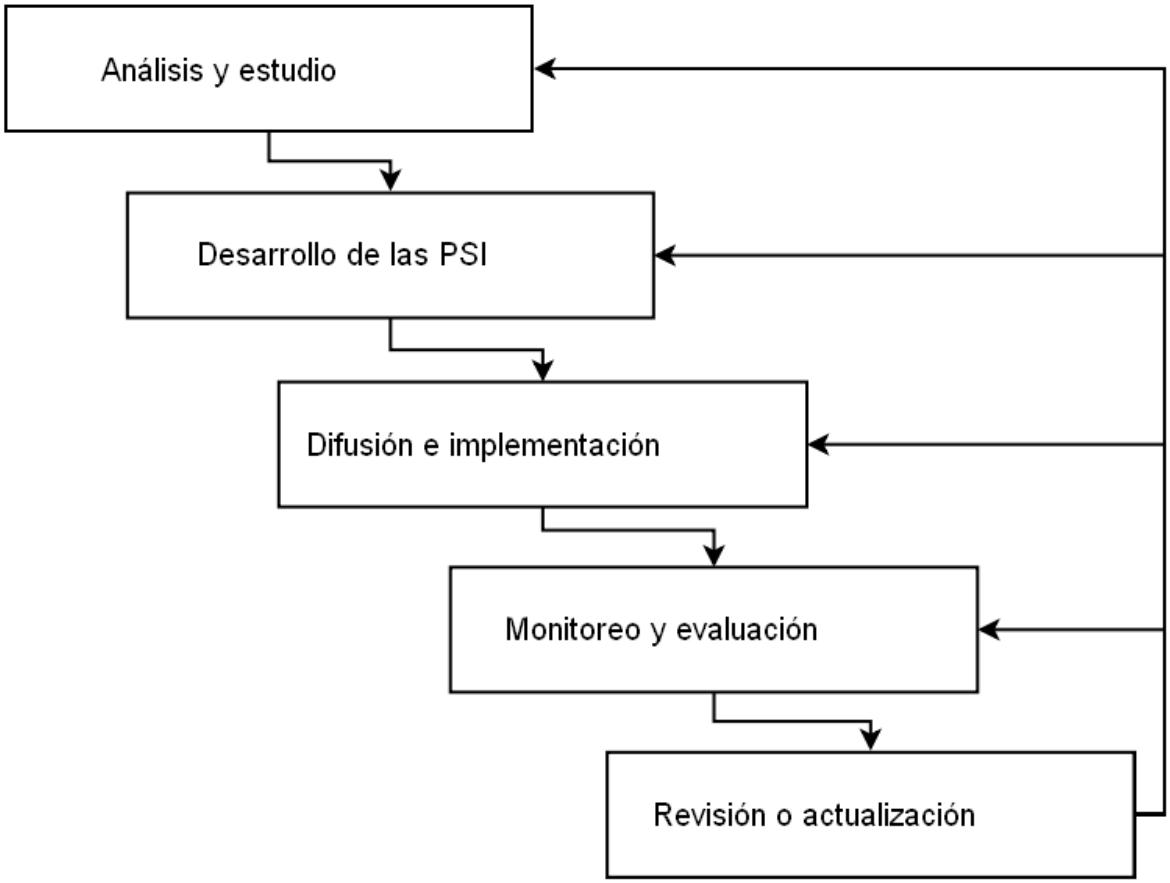

Figura 6.4 Ciclo de mantenimiento y desarrollo de las PSI

Un aspecto importante que se debe establecer para que este ciclo de mejora funcione, es la estrategia que se seguirá para la realización de la actualización o revisión de las PSI ya que dependiendo de la estrategia que fije la organización será cómo y qué tan rápido se dará este ciclo.

En el caso de la realización de una actualización periódica de las PSC-FI, se propone una estrategia mixta la cual constaría el uso de los 3 tipos de estrategias[25], las cuales se resumen a continuación.

[25] Capítulo 5. Revisión de las políticas de seguridad informática de la FI.

1. Revisiones planificadas o periódicas las cuales son propuestas por el personal del CACFI cada cierto tiempo.

2. Revisiones o actualizaciones dinámicas promovidas por usuarios, administradores o personal mediante reportes evaluados por el DSC-FI y presentados al CACFI en caso de ser requerido un cambio o corrección.

3. Revisiones emergentes, las cuales pueden ocurrir en caso de un incidente muy grave que ponga en riesgo a la organización y que requiera de la respuesta inmediata.

Utilizar una estrategia mixta permite que la Facultad de Ingeniería (FI), pueda realizar cambios, correcciones y mejoras a los documentos (PSC-FI) de manera más flexible, lo que beneficiaría enormemente por el hecho de contar con un programa de mejoramiento continuo de las PSI, permitiendo así que las políticas avancen junto con el desarrollo tecnológico.

Si esta estrategia fuese aprobada se tendría la necesidad de capacitar a los administradores principalmente para poder implementarla con el fin de que ellos colaboraran con esta estrategia, la cual depende en gran medida de las observaciones, reportes y comentarios generados por la implementación y difusión de las PSC-FI.

La actualización y revisión de las políticas debe ser un esfuerzo conjunto y coordinado con un fin común, el cual consiste en monitorear, evaluar, proponer, capacitar al personal y dar seguimiento a este trabajo con el fin de mejorar continuamente el nivel de seguridad en la organización, el cual resultará en la reducción de todo tipo de incidentes dentro de las instalaciones, de la misma forma se busca que al capacitar adecuadamente a los usuarios acerca de las PSI, los incidentes en los equipos asociados (equipos de alumnos, académicos y demás personal), también disminuyan.

Si los usuarios siguen y respetan las PSI tanto dentro de la Facultad de Ingeniería (FI) como fuera de ella protegerán de una mejor y más eficiente forma los activos de los usuarios así como los recursos informáticos entre los cuales se encuentran todo tipo de cuentas como son, las bancarias, de correo electrónico, para acceso a servidores, así como las cuentas usadas para la compra y venta de artículos por internet entre otras.

Con el fin de tener las PSC-FI con una mayor disponibilidad, un sitio WEB presenta ventajas cono son el ahorro en la impresión del documento, la disponibilidad en cuanto a horario

y descarga, facilitando así la consulta; la cual puede hacerse desde cualquier equipo conectado a internet.

Otra de las ventajas es la facilidad de cambios y actualización de la información, la cual puede ser modificada de manera repetitiva e ilimitada, además de tener un gran potencial para la difusión, la cual lo hace uno de los mejores medios para que los usuarios puedan acceder y consultar la información contenida en el sitio.

El acceso y la disponibilidad de la información hace que un sitio WEB sea una buena estrategia para la difusión de las políticas de seguridad, por lo anterior se propone el dar mantenimiento constante a la página que contendrá las PSC-FI con el fin de darle continuidad al trabajo que se realiza sobre las PSI en la Facultad de Ingeniería (FI).