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

5. Revisión de las políticas de seguridad informática de la Facultad de Ingeniería

La revisión de las políticas de seguridad es una de las etapas necesarias una vez que las políticas ya están funcionando dentro de una organización, no obstante el tiempo que transcurre desde que éstas ya están implementadas dentro de la organización hasta su primera revisión es variable, ya que no existe un tiempo determinado.

Este periodo de tiempo no está estipulado, sin embargo, el ingeniero y analista de sistemas de seguridad informática Scott Barman opina que la revisión de las políticas de seguridad debe estar dentro de un lapso de entre 6 meses y un año, por el hecho de ser tiempo suficiente para encontrar patrones que requieren algún tipo de ajuste.

El periodo de revisión de las políticas debe ser establecido por el comité de seguridad de manera empírica, dependiendo de diversos factores que afectan a la organización entre los que se encuentran la experiencia del personal de seguridad, las necesidades de seguridad que se tengan, cambios en la organización, el alza en número de incidentes, entre otros.

De esta forma las organizaciones (universidades en Australia y en Estados Unidos), teniendo en mente el hecho de darle seguimiento de manera continua y de manera permanente han ideado una metodología o estrategia mediante la cual se pretende el mejorar las PSI, involucrando a todos los usuarios de manera que ellos junto con responsables, administradores y personal de seguridad informática realicen modificaciones de una manera más dinámica.

Para que esta metodología funcione, todos los usuarios deben haber sido capacitados previamente en las PSI, una vez capacitados todos los usuarios pueden participar en la propuesta de modificaciones, ajustes o cambios para la mejora de las PSI. Las propuestas y observaciones deben pasar primeramente por un primer filtro, el cual consiste en la revisión de dicha propuesta por parte del administrador o responsable donde surgió la propuesta.

Una vez que el personal responsable y administradores acuerdan que la propuesta es viable y que ésta es en beneficio para la organización, acuerdan entregar el trabajo al personal de seguridad que revisa, evalúa, analiza y estudia las observaciones para elaborar una propuesta la cual será presentada al comité de seguridad para su aprobación. (Figura 5.1)

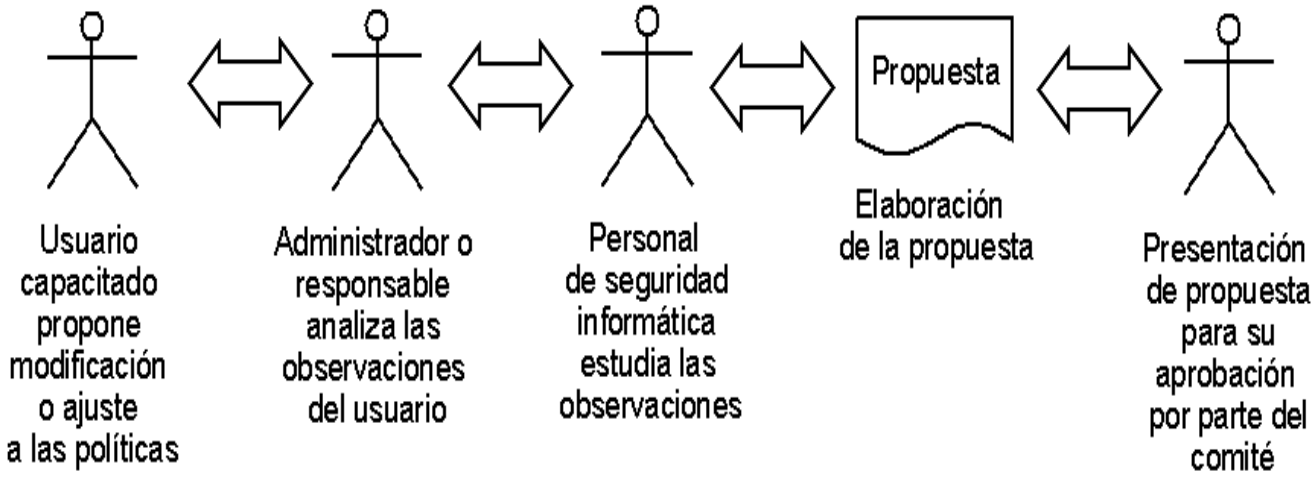

Figura 5.1 Metodología dinámica para la modificación y actualización de políticas.

Esta estrategia está encaminada a la realización de modificaciones pequeñas que consiste en hacer correcciones, pequeñas actualizaciones y ajustes mínimos con el fin de mejorar el documento, hacer que éste sea más claro, incluir algún detalle o algún dato, también puede consistir en actualizaciones respecto a términos relacionados con el tema, etcétera.

La realización de políticas emergentes y cambios es una posibilidad en esta estrategia al encontrarse alguna vulnerabilidad no contemplada con anterioridad que al ser analizada y estudiada por el personal de seguridad fuera de un alto riesgo para la organización.

Es necesario dejar claro que las observaciones o propuestas en ocasiones son hechas principalmente por administradores o personal responsable de implementar las PSI ya que dicho personal es el que tendrá que lidiar y estar más en contacto con los protocolos, recomendaciones, normas, políticas, problemas e inconvenientes que las PSI pudieran causar pues en ocasiones las políticas pueden hacer que las actividades resulten más complicadas por lo que puede ser caso de modificación con el fin de agilizar, facilitar o simplificar dicho proceso.

La segunda estrategia utilizada para la actualización y revisión de las políticas es aquella que es planificada e incluye o requiere que un grupo de trabajo revise, estudie y analice la situación actual de la organización con la finalidad de realizar una propuesta o generar un reporte con ideas, observaciones, políticas, normas o recomendaciones que serán analizadas con el fin de aprobarlas posteriormente por el comité.

Para esta estrategia se busca encontrar posibles problemas o situaciones que se estén presentado en la organización que en un futuro pudieran ser causa de un incidente grave que por medio de su inclusión en las PSI pudiera evitarse, es decir, previene posibles incidentes que pudieran haber quedado fuera en el desarrollo o revisión anterior.

El uso de estas dos estrategias en conjunto o la combinación de ellas para la actualización y revisión de las PSI es una manera efectiva de mantener este documento vigente ya que con una se requiere un trabajo continuo que ofrece como resultado un documento de mejor calidad y que en caso de encontrar algún posible problema, ofrece la posibilidad de corregir dicho error, con la otra se tiene un plan programado que se va trabajando con tiempo y que puede alimentarse con observaciones, notas, información, reportes obtenidos de la primera estrategia.

Existe por último otra estrategia para la revisión de las PSI que se presenta cuando una organización sufre cambios significativos internos o externos, cuando es afectada por agentes o situaciones externas que la obligan a reaccionar o por incidentes graves que afecten sus actividades.

Este tipo de agentes que se llegan a presentar en ocasiones pueden desencadenar una nueva política o una revisión de manera emergente que tiene como objetivo amortiguar los efectos para que la organización pueda seguir adelante. Algunas de éstas pueden ser provocadas por diversas causas, entre las cuales están las siguientes.

- Cambios externos en la organización.
- Cambios en la política de gobierno o legislación.
- Cambios internos dentro de la organización.
- Incidentes recurrentes o graves que afecten a la organización.

Una verificación emergente no busca revisar todas las PSI, sólo reaccionar ante éstas y poder realizar los cambios necesarios para disminuir el impacto del fenómeno o variante que pone en peligro afecta a la organización. Como consecuencia de la presencia de cambio que afecta considerablemente a la organización, suele resultar en la implementación del plan de contingencias durante un tiempo, sin embargo, la revisión de emergencia busca crear o generar una nueva política o serie de ellas que ayuden a la organización a reaccionar

ante dicha situación de tal manera que ésta vuelva a la normalidad y que los cambios sufridos afecten mínimamente las actividades.

A continuación se presenta una tabla que contiene algunas de las ideas más representativas de las tres estrategias para la revisión actualización y modificación de las PSI. (Tabla 5.1)

Tabla 5.1 Estrategias para la revisión, modificación y actualización de las políticas de seguridad

Tipo de estrategia	**Ventajas**	**Desventajas**
Dinámica	Participación de todos los usuarios Modificaciones emergentes Corrección de errores	Modificaciones no muy grandes Mas trabajo para administradores
Planificada	Revisión completa de las PSI Estudio, análisis y respuesta a problemáticas que afectan la organización.	Carga más fuerte de trabajo Errores u omisiones serán corregidos hasta la próxima revisión.
Emergente	Modificación para hacer frente a la emergencia y así afrontar la situación	Modificaciones o creación de nuevas políticas sólo destinadas a amortiguar los efectos provocados por un suceso inesperado

La etapa que comprende la revisión de las políticas es un proceso permanente, en otras palabras, tiene que ser un trabajo constante que no tiene fin y que debe realizarse dentro de la organización, con esto no se puede asegurar que no existirán fallas o que no se presentarán incidentes de ningún tipo.

"Even the best policy writers will omit something because it is impossible to predict everything that could happen."[13]

Esta frase en inglés puede explicarse en español en el siguiente párrafo:

Aun contando con el mejor personal y expertos en la rama de las PSI, se cometerán errores y omitirán puntos, ya que es imposible poder predecir lo que podría llegar a pasar. Siempre existirán fallas en el documento que tendrán que ser depuradas, ajustadas, cambiadas o desarrolladas.

Por lo anterior, la revisión de las PSI es un trabajo continuo y vital para el mantenimiento de un buen nivel de seguridad dentro de cualquier organización, el cual traerá consigo muchas ventajas ya antes mencionadas en este trabajo.

El no realizar la revisión, la actualización o la falta de mantenimiento hace que los usuarios menosprecien y no tomen de manera seria las PSI, esto provocará que con el paso del tiempo los usuarios ignoren este documento hasta que se presente algún incidente grave con repercusiones para la organización.

Esta situación genera pérdidas para la organización, ya que el trabajo y los recursos invertidos para la capacitación del personal se pierden al no contar con una programa de seguridad que carece de una metodología que realice una actualización o una revisión de las PSI, actividad que es igual de importante que los trabajos de capacitación, vigilancia, monitoreo e implementación.

La seguridad informática es trabajo de toda la organización, esto es, debe ser un trabajo continuo que incluye a todos los usuarios (administradores, directivos, personal técnico, operativo, mantenimiento, etcétera), debe ser un proceso proactivo, permanente, constante, que siempre tenga por objetivo estar preparado en caso de cualquier incidente y no un proceso reactivo que sólo actúe o dé respuesta cuando un incidente se presente.

[13]Scott Barman, Writing information security policies, New riders, pag. 170.

5.1 Por qué es importante una revisión de las políticas de seguridad informática de la Facultad de Ingeniería

Realizar una revisión de las PSI o PSC de la FI es de gran utilidad ya que el documento actualizado beneficiará a la organización de diversas maneras, algunas de ellas se mencionan y explican a continuación:

a) Gestión y aprovechamiento de los recursos

Tener conocimiento del porqué de las medidas que se implementan y para qué se colocan dentro de una organización facilita el proceso de planificación, diseño, organización y control de actividades con el fin de aprovechar de una mejor manera los recursos informáticos, humanos, y demás activos.

b) Mayor difusión

Contar con la capacidad de proporcionar información a todo tipo de usuarios con el fin de que se capaciten, conozcan y sepan de las políticas, recomendaciones, buenas prácticas, de las nuevas tecnologías, de la importancia de su información personal y de la cual son responsables, tendrá efectos positivos para la organización.

c) Capacitación de los usuarios

Usuarios bien capacitados son capaces de mejorar los procesos, cuidar de una mejor forma los equipos y la información que se les confía tanto para la organización como para la propia, de manera que las pérdidas, malos manejos, errores, e incidentes de todo tipo disminuyan.

d) Compra o adquisición de equipo

Las PSI contienen recomendaciones que al momento de adquirir un equipo se deben tener en cuenta con el fin de cumplir ciertos requerimientos, por esto, la compra de equipo debe ser evaluada no sólo en el costo económico sino también en qué tan bueno y efectivo será para el trabajo en el que se utilizará.

e) Minimización de posibles incidentes

El que se contengan nuevas políticas, recomendaciones, buenas prácticas y artículos que ayuden a los usuarios en general a saber lo importante que es el tener conocimiento acerca de la seguridad informática, es decir, una capacitación adecuada con la cual al paso del tiempo se cree una conciencia que minimizará los incidentes.

La capacitación de usuarios en general es de gran importancia ya que incidentes y problemas pueden ser evitados y corregidos mediante una capacitación adecuada. Este tipo de beneficios obtenidos por la difusión y capacitación de los usuarios es importante; un ejemplo de esto es una unidad de médicos cuyas actividades requieren el uso de equipos personales de cómputo.

Con cierta frecuencia se presentan problemas con sus equipos a causa del malware, el cual se propaga al usar memorias USB (USB flash drive), para copiar y transferir archivos de un equipo a otro. Este malware es difícil de erradicar, hace las computadoras más lentas y en algunas ocasiones se presenta la pérdida o eliminación de archivos de las mismas, por esto, es conveniente que uno de los médicos que realiza actividades sea capacitado acerca de los diferentes tipos de malware, el cómo se propaga este tipo en específico, como evitarlo, las repercusiones y consecuencias así como las medidas puede tomar en caso de que algún equipo esté infectado.

Como resultado de la capacitación es posible notar cómo disminuyen los incidentes y las fallas en los equipos, es posible que él prestara ayuda a los colegas que acudieran a él en caso de contaminarse con algún tipo de malware.[14]

De la misma forma, capacitar a los usuarios acerca de la seguridad informática y la importancia que tiene es de gran ayuda para tener la capacidad de prevenir y reaccionar ante incidentes que por mínimos que éstos sean pueden afectar de manera grave las actividades.

La actualización de las PSC de la FI es de gran importancia ya que se busca que los usuarios en general creen una conciencia sobre estos temas, lo cual ayudará a prevenir accidentes y capacitará a éstos para reaccionar de manera adecuada ante los posibles incidentes que se llegaran a presentar. Es importante añadir que los usuarios en general seguirán procedimientos establecidos por expertos en la rama de la seguridad informática, que en caso de

[14] Ver apéndice 6, carta expedida por el médico capacitado.

que estos procedimientos llegaran a fallar, podrán ayudar o auxiliar para resolver dicho problema.

Las PSC de la FI vigentes, datan del año 2003, por lo que no han sido revisadas y actualizadas por cerca de seis años, lo que es una vulnerabilidad y está totalmente en contra de todo lo planteado anteriormente.

La falta de actualización de las políticas en un principio puede causar cierto sentimiento de inseguridad en los usuarios por la falta de actualización en el documento, no obstante, con el paso del tiempo puede llegar a no ocurrir ningún tipo de incidente en el mejor de los casos, lo que provocará confusión y menosprecio por las políticas. Sin embargo, en el momento que se presente un incidente, el usuario recurrirá a ellas para responder al mismo, lo que se hubiera podido evitar al tener una conciencia de la importancia de las PSI.

Al no contar con un programa que contemple la revisión de las PSI es posible que éstas se consideren o se hagan obsoletas, poco fiables e inservibles en algunos casos al momento de implementar algún programa de seguridad, al configurar un servidor, mecanismo de seguridad o herramienta para el monitoreo de una red.

Esta falta de lineamientos para la implementación o configuración de cualquier equipo, software, cuentas, etcétera, hace que el personal pueda configurar de manera incorrecta estas aplicaciones, dejando así a la organización expuesta a cualquier tipo de incidente de seguridad que pudiera darse por un error humano o de manera intencional.

Un ejemplo de esto sería dejar la cuenta de administrador de un servidor de manera abierta o incluso que todos los administradores o personal pudieran acceder a dicha cuenta, lo que ocasionaría la pérdida de información en todas sus formas como son la edición o corrupción de archivos, borrado, copia de archivos personales, acceso a información personal, infección por malware, entre muchos más. Esto podría causar un incidente grave en caso de contener información importante para una organización como un banco.

En el caso concreto de la FI, la falta de normatividad en cuanto a las redes inalámbricas ha creado que dichas redes crezcan de manera descontrolada y que los equipos no estén protegidos ni configurados de manera adecuada. Esto puede provocar que usuarios no autorizados usen estas redes para otros propósitos totalmente ajenos a los que se buscan.

La actualización de las PSC de la FI es una necesidad para el buen funcionamiento, ya que por medio de éstas, el departamento de cómputo de seguridad (DSC), implementa medidas necesarias para la protección de los equipos que funcionan dentro de la facultad así como la

información que contienen éstos y algunos servicios que se prestan para la atención a los alumnos, académicos y directivos.

El buen funcionamiento y aprovechamiento de los recursos que tiene la FI dependen de la aplicación de las PSI que buscan que los recursos estén disponibles para su uso por parte de todos los que integran la facultad.

En ocasiones ignorar o no seguir los lineamientos que se estipulan en las políticas respecto al uso apropiado de los recursos, puede crear problemas dentro de la facultad, un ejemplo de esto es el conectar programas P2P, así como las violaciones a los derechos de autor que son actos que perjudican a la facultad al tener que desviar recursos para solucionar este tipo de incidentes, o al consumir gran parte del ancho de banda en dicha conexión lo cual puede inhabilitar o crear problemas en la red.

Muchos de los incidentes que se presentan podrían ser evitados si los usuarios tuvieran noción o idea de qué tanto pueden perjudicar sus acciones a la FI. Las PSI buscan crear esta conciencia en el usuario con el fin de protegerlo por ser parte de este organismo, esto significa que el usuario forma parte de esta organización aun cuando no se encuentre dentro de sus instalaciones o aun cuando navega por internet sigue siendo parte y representante de la facultad.

Por esto, es que el usuario debe concientizarse de que todo el tiempo, dentro y fuera de las instalaciones, en su proceder y actuar, forma parte de la FI. No obstante esto es en lo último que piensa el usuario (personal que labora o desempeña alguna actividad dentro de la FI, alumno, académico, directivo, personal de mantenimiento, etcétera), cuando realiza alguna acción contenida o no dentro de las PSI.

Este documento que no sólo comprende a personas que laboran con equipos de cómputo y que erróneamente se piensa que está orientado a una parte de la FI, sino que contrariamente a este pensamiento, las PSI están dirigidas a todo aquel que realiza alguna actividad dentro la facultad y que busca proteger todo tipo de bienes (incluyendo la información de todo tipo, recursos, prestigio y nombre, entre otros).

Las PSI deben ser un documento que esté en un ciclo de mejora continua y que sea una guía para los usuarios que busque enseñar y mostrar cuán importante es su información y los recursos que la FI pone a su cuidado. Estos lineamientos y recomendaciones deben poder ayudar a la disminución de todo tipo de incidentes haciendo que éstos sean evitados en lo posible.

Con la revisión de este documento de manera continua se busca mejorar la seguridad dentro del campus y que los recursos, actividades y demás bienes sean protegidos de manera adecuada para garantizar la continuidad del trabajo que se está realizando.

5.2 Actualización de las políticas de seguridad informática de la FI

La revisión de las PSC es necesaria para la actualización de este documento ya que actualmente existe una falta de normatividad que podría dar lugar a posibles incidentes, por esto es necesario realizar la actualización del documento que incluya los cambios necesarios para evitar así esos posibles percances que afecten a la FI.

Las fallas o errores en la redacción dentro de las PSC pueden crear vacíos o faltas de normatividad que ocasionan actividades que pueden afectar o causar algún tipo de problemática que afecte a la FI, por esto es necesario realizar los cambios indispensables a este documento para que sea lo más claro posible y no cause ningún tipo de confusión.

Desde que se tiene este documento se han realizado trabajos que no están contemplados en el mismo como la formación del Departamento de Seguridad en Cómputo (DSC), dedicado a la seguridad informática cuya función es el asesorar y brindar seguridad a las redes de cómputo de la FI.

No obstante, es necesario agregar que los asignados para hacer respetar las PSI dentro de la FI son los responsables de cada área y que la función del DSC es la de vigilar, monitorear, notificar y auxiliar a las diferentes áreas, divisiones y departamentos, ya que al ser una organización tan grande y que al prestar diferentes servicios dentro de ella, se estructuró por divisiones, las cuales están a su vez organizadas en sub-organizaciones más pequeñas (áreas, departamentos y laboratorios). Por este motivo, el encargado de hacer respetar las PSC es el responsable de cada área, departamento o laboratorio.[15]

El DSC es el encargado de vigilar y monitorear el tráfico de las redes de la FI, él está preparado para dar seguimiento y responder en caso de presentarse un incidente de seguridad no grave, para el cual se procede a notificar al jefe de área, quien, dependiendo de los procedimientos, dará respuesta al incidente, contando de antemano con el DSC que puede proporcionar asistencia en caso de ser requerida. Si se presenta un incidente de alto impacto o

[15] La transcripción de las entrevistas realizadas a los ingenieros encargados pueden consultarse en el apéndice 1.

grave éste se transfiere como un caso especial que deberá atenderse por el Comité de Seguridad de la FI (CACFI).[16]

Por otra parte, es importante añadir que dentro de los servicios que presta a la FI el DSC es el de realizar revisiones, auditorías y análisis forenses en caso de ser solicitados éstos por parte de los responsables del área, departamentos, y administradores de laboratorios, ya que cuenta con el personal calificado para la realización de estas actividades.

Otro punto que se debe incluir en las PSI es la realización de una política sobre las redes inalámbricas que han proliferado en la FI de manera no controlada. La falta de gestión de estas redes es tratada en otro trabajo de tesis[17] que hace mención y un análisis de esta problemática. De este trabajo se desprenden algunas recomendaciones las cuales serán utilizadas para el desarrollo de políticas para las redes inalámbricas (WIFI).

Es necesario también actualizar las políticas con base en los cambios que han surgido dentro de la dependencia, tal es el caso del manejo de los términos empleados que han variado con los cambios internos en la estructura de la misma facultad. Además de esto, para la revisión se aplicarán las recomendaciones para la redacción de las PSI vistas en el capítulo 3.

De la misma forma se crearon algunas políticas y buenas prácticas referentes a las áreas de colaboración conjunta, tecnologías emergentes, actualización de políticas y gestiones de contraseña entre otros.

5.3 Propuesta para la modificación de las políticas de seguridad informática de la Facultad de Ingeniería

La elaboración de esta propuesta, la cual es una revisión de las políticas que actualmente están vigentes, consiste en una actualización de términos basados en los cambios existentes dentro de la organización, además de la aplicación de las diferentes recomendaciones sobre la correcta redacción de las PSI vistas en el capítulo 3.

[16] http://www.ingenieria.unam.mx/cacfi/paginas/presentacion.html

[17] Guerrero Martínez Edson Armando, Gestión de redes inalámbricas en la Facultad de Ingeniería.

La propuesta aquí presentada fue elaborada con base en diversas recomendaciones que deben estar en todas las PSI, como son los controles contenidos en las normas ISO 27001 y la ISM[3] en la parte referente a políticas. También se revisó el trabajo previo por parte del ingeniero Edson Armando Guerrero Martínez cuyo trabajo de tesis es acerca de la gestión y la problemática de las redes inalámbricas en la FI.

En su trabajo de tesis, el ingeniero Edson Guerrero, realizó un análisis sobre la problemática de la proliferación de las redes inalámbricas en la FI y cómo es que éstas pueden llegar a causar algún tipo de incidente, así como los riesgos que conlleva la falta de una gestión adecuada de estas redes. Además realizó una serie de recomendaciones y redactó un compendio de buenas prácticas, las cuales contribuyeron con la redacción de las políticas sobre las redes inalámbricas.

De igual forma se realizaron entrevistas a los ingenieros Rafael Sandoval Vázquez que es jefe del departamento de seguridad en cómputo y a Noé Cruz Marín, jefe del departamento de redes y operación de servidores, los cuales realizaron observaciones y recomendaciones que fueron tomadas en cuenta para la edición, modificación y actualización de este documento.

Se obtuvo también información sobre los usuarios de la FI para complementar la elaboración de esta propuesta mediante la realización de una encuesta cuyo objetivo es la obtención de datos acerca de qué tanto conocimiento sobre el tema tienen los usuarios, qué capacitación tienen, la preparación en temas de seguridad informática, si tienen noción de la existencia de las PSC de la FI, entre otras.

La encuesta fue aplicada a poco más de 200 alumnos pertenecientes a todas y a diferentes semestres de las carreras que se imparten en la Facultad de Ingeniería durante el semestre 2010-1, presentándose a continuación algunos de los resultados.[18]

a) Seguridad Informática

Poco más del 60% de los encuestado definen o entienden por seguridad informática el uso o implementación de mecanismos para la seguridad, confidencialidad y protección de información, datos y equipos, es decir, las respuestas de los encuestados están asociadas a la implementación de mecanismos de protección para las diversas tecnologías de la información (TI), las redes, los sistemas de cómputo y sistemas informáticos, así como para la pro-

[18] La encuesta que se aplicó, así como los resultados de ésta pueden verse en los apéndices 2 y 3 respectivamente.

tección de toda la información almacenada, transmitida y accedida por medios digitales. A continuación se presentan algunas de las respuestas de los entrevistados a la pregunta ¿Qué es la seguridad informática?

- Son sistemas informáticos que impiden conocer datos los cuales no comparto
- Es proteger la información personal contra virus y/o programas que deterioran o borren ésta
- Tener antivirus en mi computadora así como vigilancia en la red y uso de antispyware
- Seguridad en las computadoras contra hackers y otros

Acerca de los objetivos y la importancia de la seguridad informática, las diversas respuestas son en su mayoría asociadas a la protección de la información digital contenida en dispositivos electrónicos y sistemas de cómputo con el 60%, a éste le sigue conservar la integridad de la información digital la cual abarca cuentas de bancos, registros escolares, información personal. Figuran también los ataques por virus, gusanos, troyanos, y toda clase de malware, así como intrusiones por parte de expertos en la materia de informática (hackers).

b) Políticas de seguridades informáticas y buenas prácticas

Los datos obtenidos acerca del conocimiento de esta área muestran que cerca de un 54% de los encuestados considera que la FI tiene un buen nivel de seguridad, sin embargo, cuando fueron cuestionados acerca de si tenían conocimiento sobre qué eran las buenas prácticas, el 64.5% contestó que no sabía lo que eran, de la misma forma los encuestados indicaron con un 60.5% no saber o no tener conocimiento sobre qué son las PSI.

Con esto en mente los usuarios fueron interrogados con respecto a su conocimiento de reglamentos internos en laboratorios, centros de cómputo, a lo cual sólo un 41% de ellos contestó tener noción o conocimiento acerca de éstos.

Cabe señalar que en cuanto a la existencia de las PSC de la FI, el 87.5% de ellos respondieron no conocer nada al respecto, dato que es muy interesante ya que muestra que la difusión y capacitación con respeto al tema es mínima.

Estos resultados muestran la falta de capacitación de la comunidad de la FI, no obstante, es necesario mencionar que conforme los encuestados son de semestres más avanzados su conocimiento respecto al tema mejora notablemente, principalmente los relacionados con las carreras de computación, eléctrica electrónica, y telecomunicaciones, ya que estas carreras son las que están más en contacto con las tecnologías de la información (TI).

Con la información obtenida de encuestas y entrevistas, observaciones, recomendaciones, los cambios y modificaciones serán tomados en cuenta para la elaboración de la propuesta de modificación a las PSC de la FI, la cual tendrá que ser analizada y modificada en caso de ser necesario para su aprobación por el Consejo Académico en Cómputo de la Facultad de Ingeniería (CACFI), que es el órgano encargado de realizar las revisiones y actualizaciones a este documento tan importante.

5.4 Reestructuración y redacción de las políticas de seguridad informática

La reestructuración de las políticas es importante, pues con una mejor estructura se busca que la información pueda ser encontrada de manera más fácil y rápida por todo tipo de usuarios que la requieran para la realización de sus actividades.

De esta forma la reestructuración busca hacer más eficientes los procesos no sólo de búsqueda y consulta sino también de actualización y modificación del documento al llevar un orden en cuanto a los tiempos, al proceso de autorización por parte de los responsables, al evitar confusiones con términos de manera que éstos sean claros, determinar las responsabilidades que tiene cada parte, entre otras.

Esto aunado a una buena redacción que esté dirigida a la comunidad de tal manera que tenga un nivel adecuado en cuanto al uso del lenguaje, sin entrar en tecnicismos que hagan que el documento sea tedioso y difícil de entender para un usuario que no posea conocimientos avanzados en el área, buscando siempre que la lectura de éste no represente un problema o que el lector tenga que pasar mucho tiempo para poder entenderlo.

Al considerar a los usuarios (toda la comunidad de la FI) a los que va dirigido y qué tan importantes son para la organización, el que se entienda que la seguridad informática empieza y es posible gracias al esfuerzo de todos y que los lineamientos, recomendaciones, normas, reglamentos, políticas y buenas prácticas son necesarios para que todas las activi-

dades, trabajos, investigaciones, etcétera, deben seguirse todo el tiempo y no sólo cuando esté presente el administrador, responsable o encargado, ya que al hacer excepciones es cuando se puede presentar algún incidente.

Este tipo de incidentes que parecen inocentes y que hacen que los usuarios vean a las PSI como normas absurdas pasan todo el tiempo, un ejemplo de esto es cuando la secretaria del jefe sabe su clave para entrar a la computadora o para acceder a ciertos recursos, lo cual se podría justificar ya que en caso de que el jefe no esté, la secretaria puede realizar ciertas actividades, sin embargo, el que ella tenga la clave es una violación clara de las PSI, ya que podría encontrar información a la que no debe acceder, autorizar movimientos, o bien puede causar algún incidente al no tener la capacitación adecuada.

Una solución para esta situación sería la creación de una política que autorizara a la secretaria para la realización de ciertas actividades, las cuales serían supervisadas por el jefe y no proveer la clave de acceso o contraseña, ya que el uso de éstas es personal.
El uso de contraseñas puede ser comparado con el uso del cepillo de dientes, en otras palabras, una persona no le prestaría su cepillo de dientes a otra, aun cuando ésta no tuviera, o incluso cuando la otra requiera usarlo, la persona en cuestión tendría que conseguir uno nuevo. Es lo mismo y funciona de igual forma con las contraseñas.

Esta reestructuración busca también crear y hacer hincapié en que los lectores entiendan la importancia de las políticas, buenas prácticas, los protocolos para el manejo, uso de todas las tecnologías y cómo es que éstas benefician, ayudan y aplican a todos los recursos que la FI les proporciona.

Finalmente para la revisión de las PSC de la Facultad de Ingeniería se tomaron en cuenta los puntos, recomendaciones, y lineamientos mencionados a lo largo de este capítulo con el fin de realizar una propuesta, la cual se anexa en este trabajo con el título "Propuesta de Revisión, Actualización y Difusión de Las Políticas de Seguridad en Cómputo para la Facultad de Ingeniería" [19]

[19] Propuesta de Revisión, Actualización y Difusión de Las Políticas de Seguridad en Cómputo para la Facultad de Ingeniería puede consultarse en el apéndice 4.