Estándares a considerar para la redacción de las políticas de seguridad

4. Estándares a considerar para la redacción de las políticas de seguridad

A través del tiempo las organizaciones han desarrollado metodologías y estrategias para trabajar así como desarrollar diversas actividades de manera más organizada y más eficiente; esto aunado a la necesidad de un trabajo de manera colaborativa con otras áreas, departamentos, grupos de trabajo e incluso con otras organizaciones, al tener que compartir, intercambiar, usar, y complementar tareas crea la necesidad de tener criterios, lineamientos y especificaciones para que exista la interoperabilidad.

La existencia de un orden o una estructura facilita que diversos y diferentes grupos puedan realizar trabajo de manera conjunta, esto se debe a que se busca que los grupos de trabajo sean multidisciplinarios.

Es por esto que existe la necesidad de la estandarización de procedimientos, criterios, términos, lineamientos y normas en el desarrollo de productos, actividades y en la forma de trabajo conjunto, es decir, el definir una serie de normas y especificaciones permite que diversos grupos de trabajo puedan trabajar de manera más productiva y organizada. A este tipo de estrategia cuyo objetivo es la interoperabilidad entre diversos grupos de trabajo u organizaciones es denominada estándar.

En el área de seguridad informática existen estándares los cuales son un compendio de recomendaciones que se deben tomar en cuenta al momento de implementar algún tipo de seguridad, sin embargo, aún no existe algún estándar para la redacción de las políticas de seguridad informática, que como se ha tratado en los capítulos anteriores, es sumamente importante para cualquier organización.

La redacción de las políticas de seguridad puede parecer poco importante, sin embargo, el seguir ciertos principios es en realidad una ventaja para una organización, por el hecho de tener la información de manera más organizada y estructurada, facilita su manejo, esto aunado a una estandarización de términos, evita problemas y confusiones, además mejora y agiliza la búsqueda de información así como su consulta y edición.

Tener o llevar un orden (estandarización) en la redacción de las políticas de seguridad es importante ya que el hacerlo asegura que el trabajo y esfuerzo conjunto de las diferentes áreas o departamentos conformados por administradores, personal de seguridad, administrativos y otros expertos en la rama sea más efectivo, y claro para los usuarios que en ocasiones carecen o desconocen de conocimientos relacionados con la seguridad informática.

Un documento claro y que posea una estructura bien definida, de manera que el personal de una organización pueda realizar búsquedas en el documento, consultar dicha información de manera confiable, es una de las metas de las políticas de seguridad, de esta manera facilita el que usuarios, administradores, jefes, directivos, y demás personal que labora en la organización confíen, estén conscientes de la importancia de este documento y conozcan la estructura del documento con el fin de facilitar la revisión, su modificación y la actualización de las políticas.

El que una organización tenga este tipo de documento, es una tarea difícil que por lo general se deja al final por ser una parte tediosa, sin embargo, el contar con documentos bien estructurados es una ventaja clara cuando se requiere realizar alguna actividad, implementación, capacitación, y si se presenta un incidente de seguridad el cual requiere una respuesta rápida por parte del personal así como para la integración de personal a algún proyecto, área o departamento.

4.1 Definición de estándar

Una documentación sólida donde estén contenidos los diferentes criterios, normas y lineamientos mediante las cuales se regulen los procedimientos y actividades dentro de una organización es indispensable para que se pueda tener una mejor gestión, colaboración, búsqueda, coordinación entre otras muchas más actividades.

Los documentos donde se describen y detallan los procedimientos, actividades, la organización y la operación de una organización con el objetivo de coordinar diversas áreas o departamentos para la realización de ciertas actividades se llaman normatividad o estandarización de procedimientos. Este tipo de documentos parece ser una parte muy formal y tediosa, sin embargo, es sumamente necesaria y útil cuando una organización se expande, crece, tiene algún problema, incidente, cuando existe la necesidad de trabajar de manera conjunta o colaborativa con otra, la adquisición de equipo, contratar o capacitar nuevo personal que se integra, etcétera.

Contar con estándares que ayuden a la integración y la interoperabilidad de departamentos o áreas de una organización, así como a la toma de decisiones y la respuesta a incidentes, es parte de las ventajas de esta metodología. Tener estándares permite dar continuidad, seguimiento, mejora, mantenimiento, actualización, simplificación e interoperabilidad de las diversas actividades, trabajos y productos.

Al trabajar con este tipo de metodologías es enriquecedor para el personal por el hecho de aprender y adquirir conocimientos, es decir, una base de conocimientos básicos que todos comparten, un mismo vocabulario (en ocasiones algunos conceptos pueden manejarse de manera distinta, lo que puede llegar a causar confusión), es decir, una unificación en conceptos, metodologías, procedimientos, de manera que se facilite y agilice el trabajo.

La existencia de un estándar ayuda a que el personal que ingresa a una organización se incorpore, que ayude al crecimiento y al alcance de los objetivos de la organización de una manera más dinámica, de la misma forma el que exista la continuidad de un trabajo o la necesidad de suplir ciertas necesidades existentes así como la no dependencia de un grupo o persona para la realización de cierto trabajo, que nadie más sabe cómo hacerlo.

Es pertinente el aclarar que un estándar es un sinónimo de la palabra norma, es decir, estándar es una palabra proveniente del idioma inglés que con el paso del tiempo se ha incorporado al castellano. No obstante que dichas palabras significan lo mismo, la palabra estándar es utilizada cuando se requiere formalidad, esto es, el uso que tiene de manera internacional, es decir, la palabra estándar es usada para denotar más importancia, una formalidad más rigurosa pese a que las dos significan exactamente lo mismo.

A continuación se define este concepto de manera formal.

- Estándar

Es una estructura bien definida de criterios, especificaciones y lineamientos en la que se describen procedimientos, características, metodologías, referencias, y definiciones para establecer una uniformidad en el desarrollo de actividades y trabajo de manera conjunta.

Basarse en un estándar en ocasiones puede crear descontento por el hecho de requerir formalismo para diversas actividades, sin embargo, esto no es del todo correcto, pues existen ventajas como se mencionan a continuación: la existencia de estándares implica el desarrollo de actividades de manera más ordenada, se busca que todo el personal que labore en la organización pueda dar un seguimiento al trabajo previo, es decir, que no requiera la inversión de mucho tiempo para encontrar la información necesaria al desarrollar algún trabajo o actividad necesaria, con esto se busca que la curva de aprendizaje se disminuya de manera considerable.

4.2 Estándares que existen respecto a las políticas de seguridad

Los estándares existentes a nivel internacional que hacen referencia de manera directa a las políticas de seguridad informática, es decir, que tratan o abordan estos temas son las normas ISO 27001 e ISM[3] (Information Security Management Maturity Model, lo que se puede traducir como Gestión de Modelos de Madurez de la Seguridad de la Información), también conocida como ISM3 que es la abreviación y mezcla de sus siglas en inglés por contener al último de esta tres palabras que inician con la letra M.

a) ISO/IEC 27001[8]

La norma ISO/IEC 27001 que es una colaboración entre la Organización Internacional de Estándares y de la Comisión Internacional de Electrotécnica publicada en el 2005, es un esfuerzo conjunto dirigido a la estandarización de los controles requeridos para el establecimiento y mantenimiento, así como para la mejora en los Sistemas de Gestión de la Seguridad Informática (SGSI), que es el término central manejado por esta norma cuya finalidad es el gestionar, administrar o encargarse de la seguridad informática mediante un proceso sistemático y documentado para llevar un orden

Esta norma busca que una organización tenga un nivel adecuado de seguridad en el cual se conozcan los riesgos a los que la organización está expuesta, se asuman, gestionen, y se minimicen en lo posible de manera estructurada, ordenada, documentada y eficiente.

Para clarificar más la idea de los SGSI en el contexto de la norma ISO 27001, se puede definir de la siguiente manera:

- Es el conjunto de políticas relacionadas con el manejo, administración, dirección, y gestión de la seguridad informática.

Metodología para la mejora continua

En este tipo de metodología busca la efectividad y eficiencia del proceso de gestión de la seguridad informática dentro de la organización, también busca la adaptación a los cambios que surjan en la organización de manera interna y externa con el paso del tiempo, expresa-

[8] http://www.iso27001security.com/, 2009

do de otra manera, el enfoque de esta metodología es la mejora continua de los procesos y de su administración.

Para la obtención de esta mejora continua esta metodología establece las siguientes fases.

1. Planear
2. Hacer
3. Verificar
4. Actuar

1. Planear (Establecimiento del SGSI)

Establecer objetivos, procesos y procedimientos que requieren políticas de manera que el riesgo sea reducido y pueda ser manejable, con esto se busca que las políticas diseñadas sean acorde con los objetivos propuestos.

2. Hacer (Implementación del SGSI)

Se busca el implementar y operar la política a través de los procesos, controles y procedimientos necesarios.

3. Verificar (Verificación del SGSI)

Evaluar, comprobar, medir y verificar el desempeño de la implementación realizada en comparación con la política realizando un reporte para su documentación y revisión por parte de la gerencia de la organización.

4. Actuar (Mantenimiento del SGSI)

Consiste en la corrección y prevención de las acciones basadas en los resultados de la auditoría realizada en conjunto con toda la información relevante al tema como pueden ser reportes, observaciones, notas o propuestas.

En el caso de la planeación, ésta consiste en el diseño de políticas necesarias basadas en el análisis previo y en una evaluación de la problemática en cuestión. Seguido de esta fase se tiene la implementación que consiste en la ejecución de los diversos controles ya diseñados, a continuación se comprueba y revisa que la solución al problema sea efectiva a través de una comparación entre los resultados obtenidos y los resultados esperados.

Una vez realizada esta evaluación se procede a la última fase, la cual consiste en el análisis de los datos obtenidos para la realización de los cambios en caso de ser necesarios, en caso contrario se procede a depurar y filtrar aún más los resultados para con esto poder encontrar alguna parte que se pueda mejorar. (Ver figura 4.1)

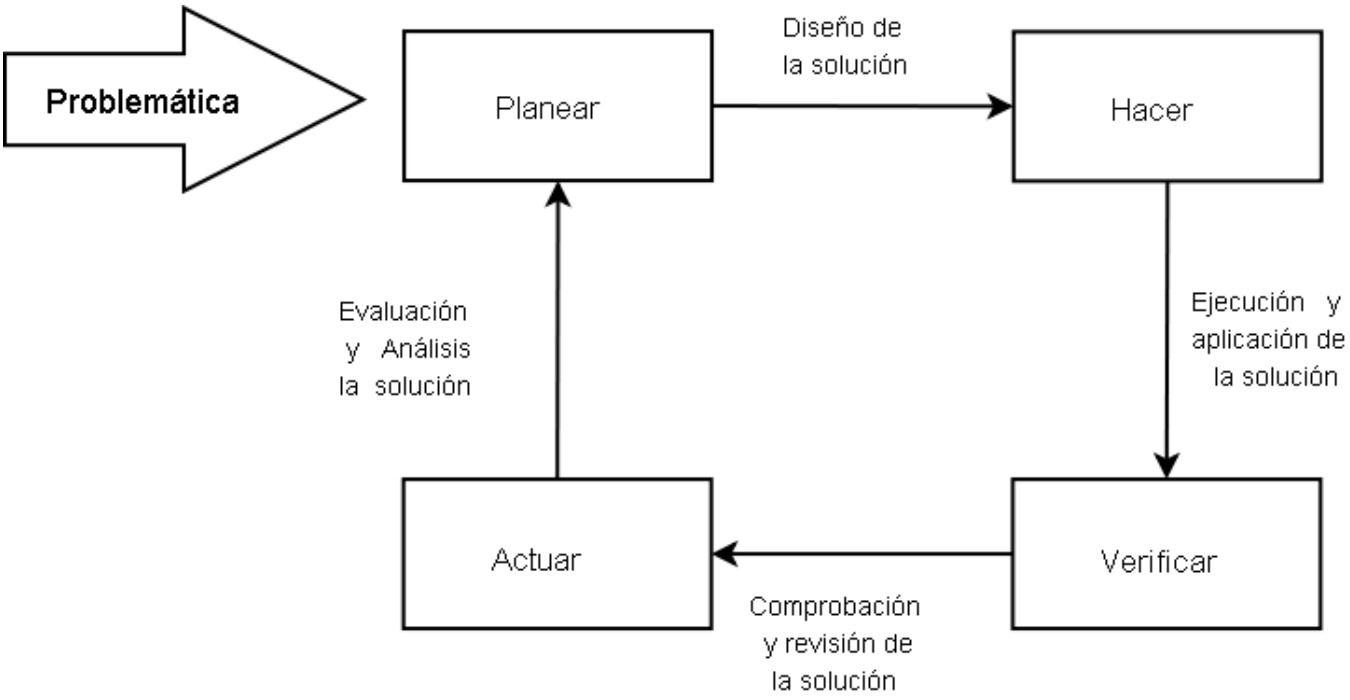

Figura 4.1 Fases de la metodología para la mejora continua.

La norma ISO 27001 es una norma auditable que busca la seguridad de la información y no sólo de los sistemas informáticos, esta norma maneja que la protección de la información no sólo se limita a los archivos digitales, sino a todo tipo de información (Capítulo 1.1

Conceptos básico de la seguridad informática). La norma define este concepto de la siguiente manera:

"Se entiende por información a todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración."[9]

Crear una conciencia de la importancia de la seguridad, crear documentación adecuada conforme se avanza en la implementación y mejoramiento de la seguridad, así como tener los controles que se requieren para tener un nivel apropiado de seguridad son algunas metas y objetivos de esta norma.

b) ISM^3 [10]

En el caso de ISM^3 o ISM3, es un estándar que busca la creación de sistemas de gestión de seguridad basados en procesos, es decir, busca detectar procesos o actividades dentro de la organización que afecten la productividad, la calidad, la eficiencia o causen algún efecto negativo dentro de ésta. Esta metodología se basa en niveles de madurez (cinco niveles), que son la inversión y alcance de un nivel aceptable de seguridad con la función de cubrir las diversas necesidades de seguridad, invirtiendo en ésta de manera rentable, por lo que es una metodología bastante flexible.

ISM^3 es compatible con diversos estándares a nivel internacional como son ISO 27001 y la serie ISO 9000 sobre la calidad del servicio, además este estándar busca aprovechar documentos, políticas y trabajos previos para la mejora de la seguridad y la eficiencia en los procesos.

Algunas de las ventajas que ofrece es que trabaja basado en procesos que buscan ser medibles para así poder cuantificar la eficacia de éstos, es decir, busca la creación de normas, indicadores o políticas medibles para ayudar a la organización, otra ventaja es que no se requiere una gran inversión, por lo que puede ser una opción para todo tipo de organizaciones que ya tienen un trabajo previo con respecto a la seguridad y que quieren mejorarla.

[9] http://www.iso27000.es/doc_sgsi_all.htm

[10] http://www.ism3.com/

Las recomendaciones de este estándar son de gran ayuda para el desarrollo y para la mejora en el desempeño de la seguridad dentro una organización, sin embargo se debe ya tener un trabajo previo a esto. Esta metodología no requiere un análisis de riesgos, lo que agiliza y baja los costos de la seguridad, no obstante es importante tomar en cuenta que al no realizar un análisis a profundidad deja muchas vulnerabilidades sin descubrir, lo que puede causar un incidente grave.

El uso conjunto de estas dos estrategias para la implementación y desarrollo de seguridad en la organización en conjunto es posible, ya que ISM^3 es compatible con la norma ISO 27001, es decir, los controles de esta norma buscan el desarrollo paulatino de las medidas contenidas en la ISO 27001.

c) Estándares y recomendaciones respecto a la redacción de las Políticas de seguridad informática (PSI)

Estas estrategias se encargan de nombrar y describir objetivos y metas, tipos de controles que son necesarios, puntos a contener dentro de las políticas, entre otros. No obstante, no existe un estándar en cuanto a la redacción que éstas deben seguir, como existe en otras áreas, tal es el caso del tipo de controles que se debe tener implementados dentro de una organización, es decir, se conoce lo que se quiere hacer y a dónde se quiere llegar pero no se sabe el cómo.

Es por esto que expertos en la rama de la seguridad informática, especializados en la parte de consultoría sobre políticas de seguridad, han publicado documentos para la revisión, redacción y desarrollo de las mismas, esto aunado a los estándares internacionales relacionados a las políticas, ya mencionados, son de gran ayuda para alcanzar este objetivo.

Los estándares internacionales como la norma ISO 27001 y la ISM^3 hacen mención de los controles de seguridad, políticas, terminología, recomendaciones y definiciones que deben estar contenidos en la documentación para un sistema de gestión de seguridad o SGSI. En el caso de la norma ISO 27001, se trata el tema de políticas de seguridad informática y en el cual se describen de manera general los objetivos y los controles que deben tener, pero no menciona el cómo redactar dicho documento.

En esta parte entrarían las recomendaciones de expertos en el tema de la seguridad, que han desarrollado diversas estrategias, recomendaciones, metodologías para la redacción de las políticas, así como para su revisión y mejoramiento, de estos artículos, escritos y publica-

ciones es de donde se puede echar mano para el establecimiento de un estándar interno o marco de trabajo para la organización.

Algunos de los documento revisados en este trabajo son publicaciones de diversas organizaciones como el SANS, el CERT, Universidades y Gobiernos de España, Francia, Inglaterra y del continente Americano, Microsoft, Symantec, entre otros, así como publicaciones y artículos de consultores expertos en esta rama entre los que están, Scott Barman, Gordon "Fyodor" Lyon, Dancho Danchev, David J. lineman, Simson Garfinkel, Gene Spafford, Alan Shwartz, por mencionar algunos de ellos.

Sin embargo, hay una clara necesidad de estandarizar o de crear un documento que de manera formal pueda contener las recomendaciones más importantes basadas en estas publicaciones desarrolladas por los expertos, de manera que puedan ser utilizados para el mejoramiento y desarrollo de políticas de una manera más estructurada, sencilla, rápida y de manera eficiente que satisfaga las necesidades de seguridad de la organización.

El desarrollo de políticas de seguridad como estándares para la redacción de las políticas de seguridad de una organización varía dependiendo del autor, sin embargo, el objetivo de este documento es el hacer un compendio de las principales y más efectivas estrategias para el desarrollo de un estándar respecto a la redacción de las políticas de seguridad.

Con base en esto se realizó la revisión de diversas publicaciones las cuales resultaron en una serie de recomendaciones vistas en el capítulo anterior. (Figura 4.2)

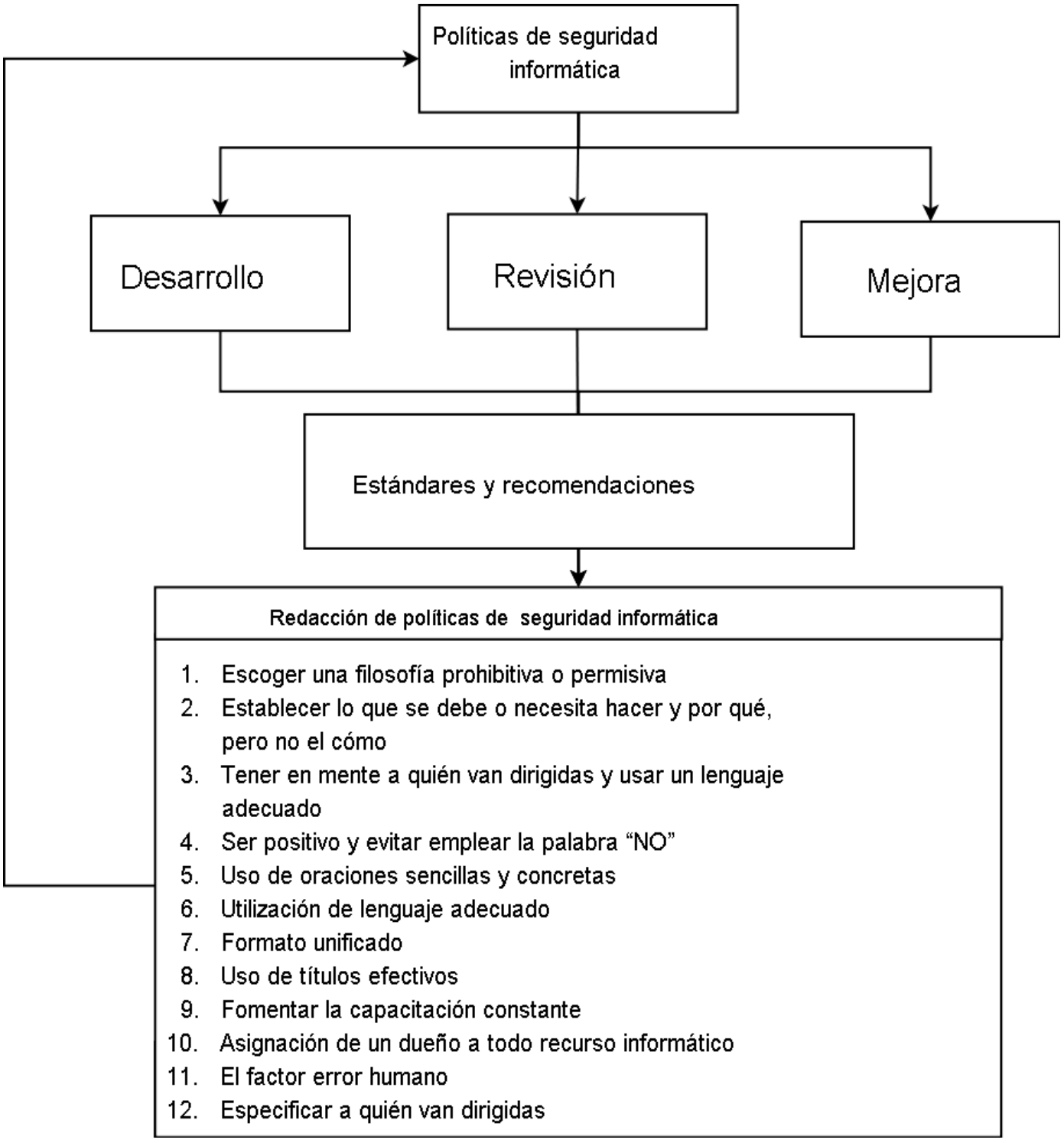

Figura 4.2 Proceso mediante el cual se busca el desarrollo, revisión y mejora de las PSI.

4.3 Estándares a considerar en las políticas de la Facultad de Ingeniería

En la actualidad la existencia de un estándar o recomendaciones con respecto al desarrollo y mantenimiento de políticas para la Facultad de Ingeniería (FI), es inexistente por el momento. Para el tiempo (marzo 2003), en el que las políticas que se tienen vigentes actualmente se desarrollaron fueron un gran avance y un gran aporte de los administradores, responsables, directivos y demás personal que se vio envuelto en el proceso para su desarrollo.

Hoy la actualización es necesaria ya que con el paso del tiempo han surgido y se han comercializado (popularizado), diferentes tecnologías que en las políticas actuales no se contemplan, el crecimiento de las redes, la diversidad y especialización de los departamentos, la existencia de nuevos laboratorios y centros de cómputo, la demanda de servicios informáticos.

Las necesidades creadas por la disminución de la productividad, la contaminación de las redes por diferentes tipos de malware, incidentes de seguridad, la generación del tráfico excesivo creado por programas de "peer-to-peer" (P2P), hacía que redes completas colapsaran y que por lo consiguiente tuvieran que ser sacadas fuera de la red, esto aunado a las violaciones que se daban a la propiedad intelectual, acoso, violencia, amenazas, y difamación de manera electrónica, requerían una respuesta inmediata. Por este motivo se decidió el realizar un documento el cual norme y dé respuesta a este tipo de problemas que se venía agravando con el paso del tiempo.

Con el fin de apoyar a la creación de este tipo de documentos surgió un trabajo de tesis titulado:

"Estrategias, procedimientos y políticas para implementar la seguridad informática en organizaciones con sistemas Linux red hat caso: unidad de servicios de cómputo académico de la Facultad de Ingeniería"[11]

En este documento también se anexaron otros como el código de ética informática, el código deontológico en la informática y el código de ética universitario con el fin de que tanto el personal como el usuario final siguiera estos códigos en caso de haber algún punto no considerado dentro de las políticas y que todo el personal por ser parte de la FI tenga en

[11] Roberto Carlos Zúñiga Ramírez y Yesenia Carrera Fournier, Estrategias, procedimientos y políticas para implementar la seguridad informática en organizaciones con sistemas Linux red hat caso : unidad de servicios de computo académico de la Facultad de Ingeniería, Tesis UNAM 2003

mente un comportamiento ético y correcto al desarrollar cualquier actividad dentro y fuera de ella, ya que es un representante de la misma.

Este trabajo cuyo resultado fueron las políticas vigentes en cómputo para la FI, tiene como objetivo principal buscar que el usuario haga buen uso de los equipos y recursos computacionales que se le confían, no obstante, el término de seguridad en cómputo hace referencia a una parte de la seguridad informática, la cual sólo busca proteger todo tipo de equipos relacionados con el cómputo.

La seguridad informática difiere de la seguridad en cómputo, ya que ésta última tiene un campo de acción menor, así como objetivos y metas más concretas, es necesario dejar claro que la seguridad en cómputo es una rama de la seguridad informática por lo que comparte las mismas definiciones y bases.

Sin embargo, el hecho de limitar las políticas a un campo menor es una medida establecida con el fin de que las sub-organizaciones que conforman la FI (divisiones, departamentos, y áreas) puedan tener mayor flexibilidad en su trabajo, es decir, que cada una de ellas pueda ser independiente una de la otra, por esto cada una de estas sub-organizaciones cuenta con su propio personal para satisfacer sus necesidades en cuanto al cómputo, por esto, años más tarde se decidió la creación de un organismo independiente que fuera el encargado de la vigilancia de su cumplimiento, el cual busca apoyar, ayudar y coordinar los trabajos en el área de la seguridad.

Este organismo cuyo objetivo es el de ayudar a coordinar, vigilar, asesorar y responder a los incidentes es el Departamento de Seguridad en Cómputo de la FI (DSCFI), el cual capacita y presta servicios para el buen funcionamiento de los equipos y recursos computacionales.

De esta misma forma se creó el Comité Asesor de Cómputo (CACFI) que es el órgano conformado por representantes de todas las áreas que conforman la Facultad de Ingeniería cuyo objetivo es el de promover y asesorar el óptimo desarrollo informático, es decir, busca conjuntar los esfuerzos de las diferentes áreas que conforman la Facultad para lograr un desarrollo integral en temas de computación, procurar la normatividad, la estandarización y en general, buscar mecanismos de racionalización y optimización en materia de cómputo.[12]

[12] http://www.ingenieria.unam.mx/cacfi/documentos/art_comite.pdf, 2009

Consideraciones para la creación de políticas de seguridad en la Facultad de Ingeniería

La seguridad informática y la seguridad en cómputo son dos términos que con frecuencia son confundidos por los usuarios, sin embargo, son sinónimos. La seguridad en cómputo es una parte de la seguridad informática, es decir, la seguridad en cómputo forma parte de la seguridad informática, sin embargo, ésta se enfoca principalmente en informar, asesorar, desarrollar políticas y procedimientos así como prestar diferentes servicios de seguridad con la finalidad de reducir los incidentes y problemas de seguridad en equipos de cómputo o asociados a ellos.

Esta rama de la seguridad informática está más enfocada a la seguridad de los equipos de cómputo y recursos informáticos por ser éstos las herramientas más utilizadas para el procesamiento, almacenamiento y transmisión de la información, sin embargo, aun cuando la seguridad en cómputo abarca muchas o la mayor parte de todas las áreas de la seguridad informática, ésta tiene un campo más limitado.

Por lo anterior, definiciones como el de información limitan su campo de acción por lo que la información no asociada o no necesaria para el buen funcionamiento de los recursos informáticos o equipos de cómputo no tiene mucho peso.

Con el fin de ejemplificar esta discrepancia, la información que el usuario tiene sobre datos referentes a la organización como son: horarios de entrada y salida, el lugar donde se guardan llaves, horarios, entradas a las instalaciones, números e información personal sobre los empleados que laboran y datos asociados a ellos, procedimientos no documentados necesarios para el buen funcionamiento de la organización, entre otros, es información que cada sub-organización maneja de manera interna, lo cual es parte de la independencia de la que se hablaba.

Este tipo de consideraciones fueron analizadas al momento de la realización de las políticas de seguridad que se encuentran vigentes, ya que al diseñar y desarrollar este tipo de documentos se deben analizar factores con el fin de que las actividades, trabajos y tareas que se desarrollan en la organización sean afectadas de manera mínima o nula.

Algunas otras consideraciones que se tomaron en cuenta al desarrollar las políticas de seguridad fueron la relación de los sindicatos presentes en la FI, el costo económico y los cambios internos en caso de la creación de un organismo que estuviera a cargo de la seguridad de manera centralizada, la diversidad de actividades que se desarrollan dentro de la organi-

zación, la discrepancia en ideas sobre la seguridad, la falta de recursos y la necesidad de éstos para dedicarlos a la seguridad, la desidia y la falta de interés en temas de seguridad informática. Por lo anterior, se creó y desarrolló el modelo que se tiene actualmente, el cual busca la mejora continua de la seguridad dentro de la FI.

Para la revisión de las políticas fue necesario conocer y recopilar información sobre el origen, las consideraciones hechas por parte del equipo que las elaboró, las limitaciones existentes, las necesidades actuales, el trabajo, actividades y funcionamiento del Departamento de Seguridad en Cómputo (DSCFI), así como el del Comité Asesor de Cómputo (CACFI), de la misma forma las observaciones de administradores que laboran en distintos laboratorios. Esto con el fin de conocer el entorno y las variables asociadas a las políticas vigentes de manera que el trabajo tenga una continuidad.

Se tomaron en cuenta las recomendaciones y observaciones de estándares como ISM3 el cual maneja que el nivel más bajo para una organización como la FI, debe ser el nivel 2 (por el tamaño, la necesidad de seguridad y el rubro de la organización, éste debe ser el nivel mínimo para una organización de este tipo).

Las estrategias, metodologías, trabajos y actividades que se mencionan en este estándar son desarrolladas por el DSCFI y el CACFI que trabajan de manera conjunta con las demás divisiones con el fin de mantener un nivel apropiado de seguridad, sin embargo, es necesario el hecho de que exista más difusión en temas de seguridad dentro de la FI, así como una mejor comunicación con los administradores y encargados de laboratorios pues algunos desconocen la existencia o en caso de conocerla, ignoran el contenido del documento.

Algunas de las acciones necesarias que maneja el ISM3 son el monitoreo, el cual en las PSC de la FI fue uno de los puntos que se actualizó con el fin de clarificar su importancia y su propósito, esto es, el análisis del tráfico en las redes así como su monitoreo con el fin de detectar amenazas, corregir y prevenir problemas de diferentes índoles en la red de la FI.

De la misma forma ISM3 define, maneja y clasifica términos como son:

a) Objetivos de la seguridad→ Continuidad, Prevención de pérdidas en activos, Rentabilidad, Mantenimiento del renombre de la organización, Protección del derecho de autor, Protección de la privacidad.

b) Tipos de Amenazas → Error Humano, Incompetencia, Fraude, Corrupción,

c) Metas de la seguridad → En este caso se manejan estadísticas como por ejemplo el alcanzar tazas de robos y pérdidas económicas del 1% anuales.

Con la finalidad de actualizar las políticas se revisó el estándar ISO 27001 e ISM3 en sus partes concernientes a políticas de seguridad y se tomaron en cuenta las observaciones, publicaciones y artículos de expertos y personal que labora en la FI (DSCFI, administradores y responsables de distintos laboratorios), con la finalidad de realizar una propuesta de actualización, la cual sea analizada por el CACFI para su modificación en caso de ser necesaria y posteriormente aprobada.

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

La revisión de las PSC que se presenta en este trabajo tiene como finalidad la realización de una propuesta de actualización que busca ser de ayuda a los administradores, responsables y encargados. La base y justificación de los cambios realizados para la actualización de las políticas de seguridad son con base en la investigación realizada ya previamente presentada.

Por otra parte también se pretende el sentar una base y manual para futuras revisiones y actualizaciones para dicha políticas, las cuales tendrán que ir cambiando y mejorando paulatinamente con el paso del tiempo. Es importante aclarar que siempre existirán fallas y vacíos por llenar, sin embargo, el objetivo de este documento es minimizar esas fallas al proponer una metodología para mejorar y crear conciencia de la importancia que éstas tienen para la organización.

Este documento busca ofrecer una ayuda clara para las distintas áreas, departamentos, laboratorios y divisiones para el desarrollo, mantenimiento y mejoramiento de reglamentos internos, políticas, o normatividades.
Algunos de los puntos más importantes para esta revisión de las PSI de la FI son los siguientes:

- ✓ **Redacción de las políticas con base en las recomendaciones ya mencionadas.**

La revisión de las políticas usando recomendaciones tiene como finalidad hacer que la lectura de éstas sea más fácil de entender, además de evitar interpretaciones personales haciendo que el documento sea lo más claro posible.

- ✓ **Incluir en las PSI un apartado sobre la gestión de contraseñas.**

El incluir un apartado sobre la gestión de contraseñas que describe las estrategias para la protección de éstas que son mecanismos para el acceso a recursos de todo tipo como son el correo electrónico, cuentas bancarias, cuentas en equipos de cómputo, información personal entre otras. Conocer las técnicas, recomendaciones y estrategias para la protección de contraseñas evita y minimiza el que puedan ser utilizadas para cometer ilícitos o utilizarlas de manera indebida para ocasionar distintos tipos de pérdidas.

- ✓ **Incluir políticas para las redes inalámbricas.**

La falta de políticas que contengan recomendaciones y regulen el uso, administración y crecimiento de las redes inalámbricas son necesarias por el hecho de ser un punto desde el cual se pudiera presentar algún incidente de seguridad. Por otro lado, tener políticas que gestionen de manera apropiada estas redes permite tener un mejor aprovechamiento de las mismas.

- ✓ **Esclarecer las funciones que tiene el departamento de seguridad en cómputo como organismo independiente existente en la Facultad de Ingeniería.**

La función del departamento de seguridad en cómputo como un organismo independiente de cualquier área, que cuenta con personal capacitado, dar apoyo, respuesta y seguimiento ante un incidente de seguridad, así como asesoría y apoyo técnico cuando sea requerido.

- ✓ **Realizar un documento más claro y accesible para usuarios con un menor conocimiento de la seguridad informática.**

El que usuarios ajenos al área de la informática y el cómputo sean capaces de entender la importancia de toda la seguridad de la información, con el fin de que hagan buen uso y protejan de manera adecuada todos los bienes que les son confiado o asignados así como los propios, es un principio básico que es necesario en estos tiempos en que la tecnología se vuelve más popular para la realización de cualquier trámite, pago, consulta, etcétera.

- ✓ **Crear una conciencia en todos los usuarios acerca de la seguridad informática.**

Hacer que los usuarios sepan qué tan importante es su información (número de cuenta, cuentas de correo electrónico, RFC, fecha de nacimiento, dirección, datos de sus familiares, números telefónicos, horarios, cuentas bancarias y bienes en general), cómo protegerla, su uso correcto, cómo reaccionar en caso de algún incidente de seguridad, son consecuencias de la creación de una conciencia acerca de la seguridad informática.

- ✓ **Incluir a las nuevas tecnologías.**

El que nuevas tecnologías estén contempladas y tengan un procedimiento para que puedan ser implementadas es necesario para minimizar y prevenir algún mal uso, interferencia con otras tecnologías, o el que su utilización pueda causar algún tipo de problemas.

- ✓ **Incluir políticas para entidades externas.**

Las medidas en caso de presentarse la necesidad de trabajar de manera colaborativa o de requerir la contratación de personal externo para realizar algún tipo de actividad, es un evento que se presenta con más frecuencia. Esto implica compartir recursos informáticos e información con personas externas, por lo que es necesaria la existencia de normas que regulen estos eventos.

- ✓ **Incluir apartados sobre las buenas prácticas**

El incluir buenas prácticas dentro de este documento busca que responsables y demás personal tengan en cuenta dichas recomendaciones con el fin de mejorar la seguridad y el aprovechamiento de los recursos dentro de sus actividades.

4.5 Estandarización de las políticas de seguridad informática de la de la Facultad de Ingeniería

La estandarización de las PSI busca que exista la interoperabilidad y el trabajo colaborativo dentro de la organización, es decir, que haya una mejor comunicación entre las distintas áreas, divisiones, dependencias, departamentos y laboratorios que conforman la FI.

Uno de los objetivos de este trabajo es realizar una propuesta para tener un estándar para la redacción de las PSI, esta recopilación busca facilitar, unificar, simplificar la redacción de las políticas con el fin de mejorar su contenido y hacer que éste sea más sencillo para usuarios con poco conocimiento en el área de cómputo, busca también crear conciencia de la importancia de la información y la manera correcta para su utilización.

El concepto de estandarización dentro de este contexto se puede definir de la siguiente manera:

- Estandarización

Es la creación, elaboración, redacción, o esclarecimiento de normas y procedimientos dentro de una organización cuyo objetivo es el de simplificar, unificar y especificar con el fin de garantizar el acoplamiento de los distintos organismos que lo conforman.

Las políticas de seguridad en cómputo (PSC) de la FI, aun cuando no están actualizadas comprenden muchos puntos y controles mencionados en la norma ISO 27001 que actualmente está vigente, la cual fue publicada en el 2005, es decir, la estructura y las políticas contenidas son acorde y siguen las indicaciones actuales de la norma ISO 27001, por mencionar algunas de ellas están las siguientes:

- La gestión de Activos → Inventarios, uso apropiado, propiedad de los activos.
- Seguridad de los recursos humanos → Roles y responsabilidad, selección y términos, condiciones de empleo.

- Seguridad física y ambiental → Perímetro de seguridad física, seguridad de oficinas, habitaciones y medios, protección contra amenazas externas y ambientales.

- Seguridad del equipo → Ubicación y protección del equipo, servicios públicos, mantenimiento de equipo.

- Entrega de servicio → Monitoreo y revisión de los servicios de terceros

- Protección contra software malicioso y código móvil → Controles contra software malicioso

- Respaldo → Respaldo de la información

- Gestión de seguridad en redes → Controles de red, seguridad de los servicios de red.

- Monitoreo → Registro de auditoría, registro de fallas.

- Control de Acceso → Política de control de acceso, gestión de privilegios, gestión de la clave de usuario.

Los controles mencionados contenidos en la norma ISO 27001 no son los únicos que están considerados dentro de las PSI de la FI, por lo que el documento que se tiene vigente desde el 2003 es un buen documento ya que contempla muchos de los controles y políticas que se mencionan en una norma posterior (ISO 27001 publicada en el 2005).

Es importante que los administradores y usuarios en general lean todo este documento y no solo el apartado de políticas ya que muchos de los controles que se manejan en el estándar ISO 27001 están incluidos en los postulados y en los códigos de ética. En esta parte del documento se hace referencia a la calidad del trabajo, las responsabilidades sobre el desarrollo de software, el trato hacia los usuarios, la capacitación del personal, la actitud de servicio y los valores deseables en el personal que labora.

Las PSC que se encuentran vigentes están íntimamente relacionadas con las PSI y aun cuando tienen un campo de acción más limitado, estas hacen mención y buscan el poder abarcar otras áreas y campos mediante los códigos, postulados, y principios contenidos los cuales amplían su campo de acción buscando el proteger de una mejor manera los recursos y la información de manera más integral.

4.6 Redacción de las políticas de seguridad informática de la Facultad de Ingeniería

La redacción de las PSC de la FI consistirá en la revisión de las políticas que actualmente se tienen siguiendo las recomendaciones para la correcta redacción de las PSI, las recomendaciones hechas por el jefe del departamento de seguridad en cómputo Ing. Rafael Sandoval Vázquez, y el jefe del departamento de redes y operación de servidores el Ing. Noé Cruz Marín, así como otros interesados en el tema.

Con esto se busca la existencia de un documento actualizado, incluyendo las nuevas tecnologías que se han estado implementando dentro de la FI, se busca también que los usuarios en general tengan un documento que puedan consultar de manera más clara y de manera más rápida.

Por otra parte se desea tener una mejor estructura que ayude a la búsqueda más eficiente y efectiva de temas de interés, de tal manera que el usuario pueda ir directamente al apartado de su interés y que el contenido quede lo más claro posible sin lugar a interpretaciones personales o dudas de ningún tipo.

El que esta información que sólo se busca cuando se presenta un incidente o algún problema sea una lectura más fácil de realizar para un usuario ajeno a la rama de la seguridad informática y que con la lectura obtenga así un conocimiento básico para proteger los bienes a su custodia de una mejor forma así como los propios.

Por otro lado con esto se busca incluir a las PSC de la FI un anexo donde se especifiquen las recomendaciones para la redacción y desarrollo de las PSI las cuales son importantes para la continuidad del trabajo que se viene realizando. Con esto se busca que el usuario este más involucrado en los temas de seguridad que a futuro serán una herramienta muy útil para su vida y desarrollo profesional.