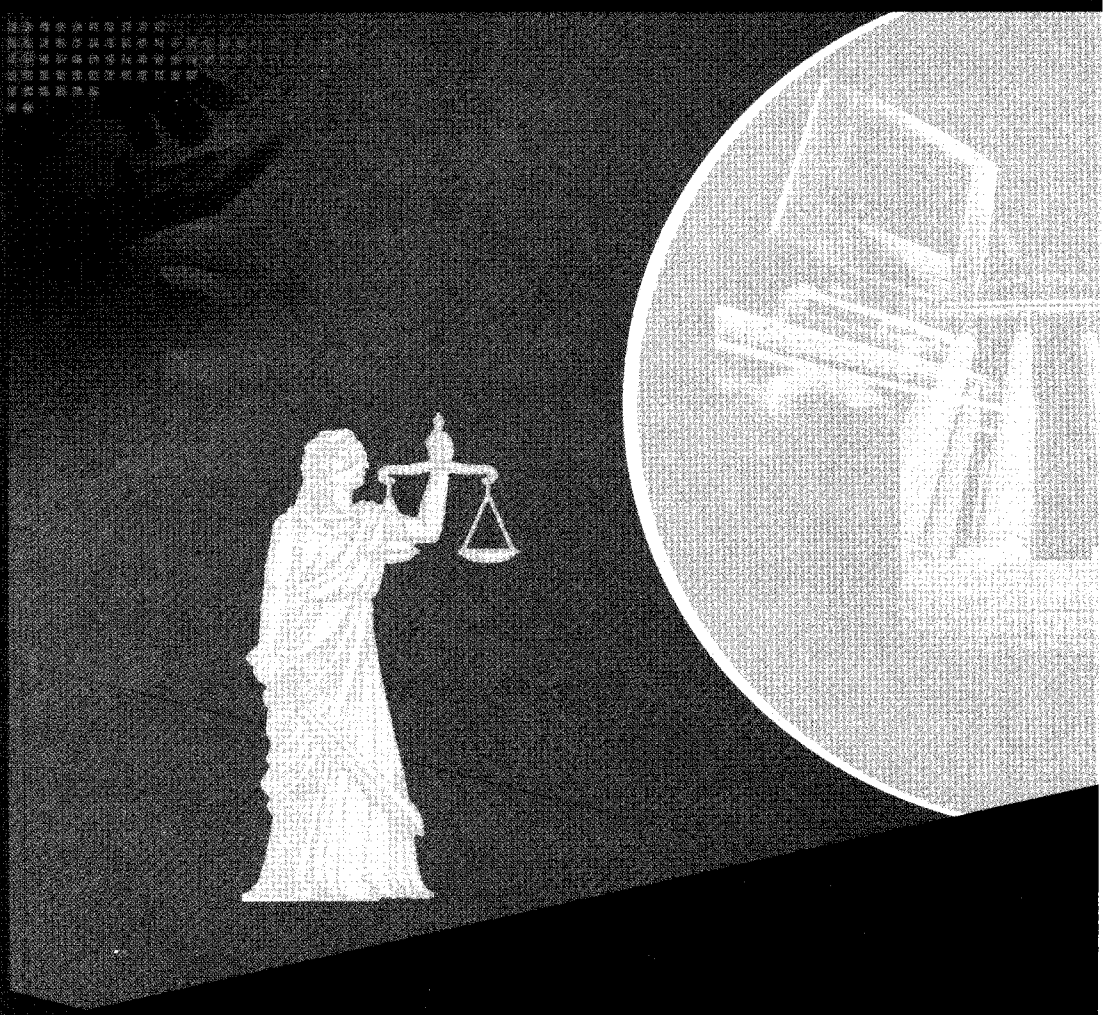
Techno-Legal Aspects of Information Society and New Economy an Overview



Edited by
A. Mendez-Vilas
J.A. Mesa Gonzalez
F. Zapico Alonso
V. Guerrero Bote
J. Mesa González

INFORMATION SOCIETY SERIES
Nº 1

TECHNO-LEGAL ASPECTS OF INFORMATION SOCIETY AND NEW ECONOMY: AN OVERVIEW

Series "Information Society", N°1

Edited by

A.Mendez-Vilas (*Formatex)*
J.A. Mesa Gonzalez (*Formatex)*
J. Mesa González (Innovatex)
V.Guerrero Bote (*University of Extremadura)*
F.Zapico Alonso (*University of Extremadura)*

C / Encarnacion, 3 1°E (Semillero de Empresas)
06001 Badajoz, Spain
D.L. Vol. I: BA-341-03
ISBN: 84-607-8104-6
Printed in Spain
Impreso por Indugrafic, S.L. (Badajoz)

Las Políticas de Seguridad como Apoyo a la Falta de Legislación Informática

M. Farias-Elinos[1,3] , Ma. C. Mendoza-Diaz [2,3] ,L. Gómez-Velazco[2,3]

[1]Lab. de Investigación y Desarrollo de Tecnología Avanzada (LIDETEA), Coord. Gral. de Investigación, Dir. de Posgrado e Investigación, Universidad La Salle
Benjamín Franklin 47, Col. Hipódromo Condesa, México, DF, 06140
Tel: +52-55-5278-9530 x 2390, Fax: +52-55-5515-7631
e-mail: elinos@ci.ulsa.mx
[2]Dirección de Telemática, Centro de Investigación Científica y de Educación Superior de Ensenada (CICESE).
Km. 107 Carretera Tijuana-Ensenada, Ensenada, B.C. México. 22800
Tel: +52-64-6174-5050 x 23108, Fax +52-64-6175-0537
e-mail: mmendoza@ptd.net, lgomez@cicese.mx
[3]Grupo de Seguridad de Internet-2 México, http://seguridad.internet2.ulsa.mx/

Palabras clave: Políticas de seguridad, legislación, seguridad.

Resumen. En la actualidad uno de los problemas que se enfrentan con el uso de las tecnologías de información es la falta de una legislación informática que esté al día, siendo los países en desarrollo los mas atrasados en este aspecto. Esto conlleva a un problema que enfrentan todas las organizaciones, que es el cómo poder protegerse contra el mal uso de los sistemas de cómputo y de los enlaces de telecomunicaciones, o contra la intrusión de algún cracker. Esto nos lleva a tener que definir una serie de reglas que nos permitan eliminar en lo posible el uso inadecuado de los recursos que pueda ocasionar algún daño a la organización. Estas reglas se conocen como "políticas de seguridad", y en su construcción surgen una serie de preguntas como: ¿Quiénes son los que deben de desarrollar las políticas?, ¿Quiénes deben de darle la importancia requerida?, ¿Cómo pueden éstas ayudar a la falta de legislación?, ¿qué deben de abarcar?, ¿Cómo hacerlas cumplir?. Aspectos importantes que deben contemplarse al momento de realizar las políticas de seguridad, son conocer qué está legislado y conocer también si existen estándares internacionales para utilizarlos de referencia y apoyo en las políticas de seguridad desarrolladas.

Otro factor también importante de las políticas, es que son un documento que se debe ser actualizando constantemente, ya que la tecnología no es estática, ni la legislación, y sobre todo, el comportamiento de los usuarios.

Introducción

El uso de las tecnologías de información en el mundo es cada vez más evidente, entre sus características se destaca su comportamiento cambiante y revolucionario. Para la mayoría de las organizaciones estar conectadas a Internet no es un lujo sino más bien una necesidad de atravesar fronteras tanto en el ámbito económico como en el social y cultural.

Por ello, puede decirse que estar al día en el uso de las tecnologías de información tiene un elevado costo. Por un lado, la necesidad de poder protegerse contra el mal uso (interno y/o externo) de los sistemas de cómputo y de los enlaces de telecomunicaciones, o contra la intrusión de algún cracker a su sistema de red. Por otro lado, enfrentarse a la falta de cultura informática y por consecuencia a la falta de seguridad en cómputo en las organizaciones y a la presencia casi nula de una legislación informática, principalmente en los países en desarrollo.

En cuanto a legislación informática ha sido poco y aislado el trabajo que se ha realizado, por lo que campos como la protección jurídica de la información personal, la protección jurídica del software, los delitos informáticos, entre otros de igual importancia, estan aún lejos de ser legislados en su totalidad.

Este trabajo propone la definición de "políticas de seguridad" como una forma de eliminar en lo posible el uso inadecuado de los recursos de cómputo y telecomunicaciones en una organización, así como, una forma

de "aliviar" la falta de legislación informática que regule en este ámbito el comportamiento de los individuos (usuarios) y de la sociedad en general.

Podemos entender como políticas de seguridad, el conjunto de reglas y principios que gobiernan una entidad u organismo, donde cada regla define una acción, mecanismo y/o procedimiento. Entre las características más relevantes a considerar durante su definición son: enfoque a la problemática particular de cada organización; contar con una estructura bien definida; vigencia y flexibilidad para su actualización; que establezca obligaciones y derechos; que sean aprobadas y difundidas por los directivos, administradores y usuarios de la organización[1]. De tal forma, que las organizaciones puedan contar con un documento de políticas de seguridad en cómputo que las guien en su actuación en casos de violación de la seguridad y que sirvan de apoyo para ir a la par de la tecnología cubriendo la falta de legislación.

En el documento el lector también encontrará una exposición de dos casos de estudio que reflejan la problemántica anteriomente plasmada.

Legislación mexicana

Se define como derecho informático "el conjunto de leyes, normas y principios aplicables a los hechos y actos derivados de la informática"[2]. Lo cual es muy diferente a la "Jurídica informática" la cual de define como "el conjunto de estudios e instrumentos derivados de la aplicación de la Informática al derecho, es decir, a los procesos de creación, aplicación y conocimiento del derecho"[3]

Para muchas naciones, actualmente la función de seguridad de tecnologías de la información es sustantiva, incluyendo la protección de la soberanía, ya que los efectos de riesgos manifestados pueden traducirse en lamentables pérdidas humanas y/o económicas cuantiosas. Es por ello que se destinan presupuestos elevados para la implantación de mecanismos de protección de infraestructura tecnológica y sobre todo a la información, considerados como activos de las organizaciones.

Uno de los factores en contra que se tienen actualmente es la aceleración que presentan los avances tecnológicos, sobre todo en países en desarrollo donde existe un retrazo, o hasta una falta de legislación informática. En el caso de México, la existencia de una legislación informática es nula, sin embargo lo que se ha realizado, son adaptaciones de algunas leyes hacia el ámbito tecnológico, como sería la Ley federal de derechos de autor.

En México, algunos aspectos reconocidos por las leyes mexicanas en cuanto a materia de informática son[4]:

Ley federal de derechos de autor
Ley de la propiedad industrial
Ley federal de telecomunicaciones
Código penal federal
Código civil federal

Así mismo existe una serie de propuestas enfocadas a cuestiones informáticas como la Ley federal de protección a la protección de datos personales[4], así como una norma oficial mexicana (NOM-151-SCFI-2001)

A nivel internacional, un país con avances y aportaciones notables a la unificación de criterios jurídicos en la Unión Europea es España. Entre la legislación informática que ha desarrollado, destaca el proyecto de ley sobre firma electrónica que ha sido aprobada por la Unión Europea; para lo cual, se creará un medio de identidad para navegar con altos niveles de seguridad por Internet, y que surtirá la misma eficacia jurídica que una firma manuscrita sobre papel y será admisible como prueba para efectos procesales, a través de cualesquiera de los medios admitidos en Derecho.

En el caso de América, Estados Unidos es sin duda el país con importantes aportaciones en la consolidación de un marco jurídico informático, aunque cabe señalar que en América Latina ya se tienen avances, sin embargo se puede tener como notable el caso Argentino, país que cuenta con infraestructuras

educativas específicas para el derecho informático. Es importante continuar con actividades de intercambio y cooperación entre países con avances considerables en esta materia[4]

Definición de Políticas de Seguridad

Cuando en una organización surge la iniciativa de generar sus propias políticas de seguridad, puede enfrentarse a un gran número de interrogantes, como, ¿Quiénes son los responsables de desarrollar las políticas?, ¿Quiénes deben de darle la importancia requerida?, ¿Qué deben de abarcar?, ¿Qué características deben tener?, ¿Cómo hacerlas cumplir?. Por ello, el proceso de definición de políticas que aqui se presenta abarca las siguientes etapas: *planeación y preparación, desarrollo (redacción y edición), aprobación, difusión y aplicación, revisión y actualización.*

Desde la *etapa de planeación* de las políticas, es necesario contar con el apoyo del cuerpo directivo de la organización en cuanto a la definición de las mismas. Y conocer la postura institucional en cuanto a la política de seguridad informática general que deberá seguirse durante el desarrollo de las políticas de seguridad particulares. Además es importante, detectar la problemática de la organización a través de un análisis de riesgos, definir qué se debe proteger y contra qué, así como, informarse acerca de los aspectos informáticos legislados en el país o entidad donde se vayan a aplicar.

Para iniciar su *desarrollo*, es importante contar con una persona que sea responsable de dar seguimiento al proceso de definición de las políticas y de "desatorar" el proceso cuando sea necesario, normalmente se le nombra "coordinador".

En la redacción de las políticas, es necesaria la participación de los *administradores de sistemas* de cómputo; una *persona que represente la postura del cuerpo directivo*, encargado de guiar el desarrollo de las mismas de acuerdo a la política institucional en cuanto a la seguridad de sus activos; un *asesor jurídico*, que vigile que en la redacción de las políticas no se violen las garantias individuales de los usuarios y que esten de acuerdo con la actual legislación en el área de aplicación; y algun(os) *usuario(s) de la red*, que aporten información sobre los usos de la tecnología en sus actividades, de tal forma que servicios criticos para la actividad de la organización no se vean afectados sino protegidos.

Entre las principales características a considerar para el documento de políticas durante su desarrollo, se encuentran:

- Enfocar la política hacia la problemática particular de la organización.
- Contar con un documento con una estructura bien definida.
- Definición clara y precisa de los enunciados.
- Que exponga de manera explícita el ámbito de aplicación.
- Que se establezcan obligaciones y derechos tanto para los administradores como para los usuarios;
- Que defina claramente las sansiones a las que estará sujeto quien no se apegue a las políticas de seguridad institucionales.
- Que el documento cuente con vigencia y flexibilidad para su actualización.

Una vez concluída la redacción de las políticas, se procede con su *aprobación*. Esta etapa consiste normalmente de una revisión final exhaustiva por parte del cuerpo directivo/colegiado de la organización, hasta su aprobación. En algunos casos el tiempo de duración del documento en esta etapa es largo (meses), ya que dependerá en cierta forma de la disposición, prioridad del documento ante los directivos. De allí que es indispensable vender la idea desde su planeación.

La *difusión y aplicación* de políticas es el siguiente paso, es de vital importancia difundir el documento a través de diversos medios como, página principal de la organización, correo electrónico, trípticos, en la apertura de cuentas a nuevos usuarios, publicación en revistas internas electrónicas y tradicionales, etc. de tal forma que sea conocido por todos los usuarios de la organización, y que sea transparente su aplicación y seguimiento. Las políticas deben ser aplicadas tanto por los directivos como por los administradores y los usuarios, ya que la seguridad no depende de una sola persona sino de cada uno de los individuos que forman una organización.

El proceso de definición de politicas de seguridad es contínuo aún después de ser aprobadas, difundidas y aplicadas, ya que su siguiente etapa es la de *revisión y actualización* de acuerdo a la naturaleza cambiante de las tecnologías de información.

Fortalezas

La Política de Seguridad como se ha definido antes, es creada de forma explícita para un sistema según sean sus características como misión, recursos, tipo de red y de usuarios, etc. De tal forma que, la Institución puede crear un mecanismo de control al crear la Política de Seguridad apropiada a sus necesidades, a voluntad y apegada a sus reglamentos administrativos y técnicos (en caso de existir) para definir el buen uso de sus recursos y como apoyo a posteriores procedimientos legales en dado caso.

Una fortaleza es un elemento que favorece de forma sustantiva el desempeño en este caso de un sistema de sómputo y comunicaciones de una institución. Al invertir en una Política de Seguridad se obtienen fortalezas como las siguientes:

a) **Uso definido de los recursos**, es común entre las organizaciones adquirir recursos e iniciar su funcionamiento sin una definición escrita y sin divulgación entre sus usuarios sobre el tipo de servicio que brindará y sus restricciones (si existen).

b) **Derechos y obligaciones definidas para cada tipo de usuario**, es importante definir y difundir esta información entre todos los usuarios del sistema, de tal forma que cada usuario conozca sus alcances y limitaciones sobre los recursos.

c) **Guías técnicas para la protección de recursos**, información de gran utilidad para los usuarios, la seguridad es una responsabilidad compartida entre todos los usuarios de un sistema, son tan importantes las técnicas locales (la clave robusta de un usuario) como las técnicas aplicadas a niveles globales (firewalls). La institución elige las herramientas más apropiadas para sus recursos y disemina el conocimiento para su aplicación por todos.

d) **Análisis de riesgos sobre inventarios de recursos,** es también común la falta de estudios de este tipo, siendo de gran relevancia para el desarrollo mismo de las políticas y el conocimiento de las debilidades del sistema. Esta información define la diversidad de riesgos y propone la prioridad y nivel de protección de los recursos; elementos que son necesarios para la generación de planes de contingencia

e) **Sanciones definidas dentro del marco ejecutivo de la institución**, en caso de mal uso de los recursos, la institución tendrá una herramienta para aplicar las sanciones apropiadas sobre un marco de reglas locales y conocidas por todos. Es importante mencionar que las sanciones definidas en una Política de Seguridad no pueden estar en contra de las leyes estatales y/o federales, las políticas son un apoyo a la falta de legislación, de ninguna manera pueden contradecirla.

f) **Planes de contingencia,** dentro del documento de las politicas se encuentran enunciados todos los planes de contingencia generados para el sistema.

g) **Pueden modificarse cuando sea necesario,** las políticas deben crecer con la institución, ajustarse tanto a los cambios internos como a los cambios en la ley gubernamental. Los cambios los propone un comité o grupo de seguridad en respuesta a elementos nuevos o cambios importantes (técnicos y/o administrativos) y éste decide cuándo y cómo cambiarlas para mantener su actualidad.

h) **Un documento firmado por los directivos y que es *la ley* dentro de la institución,** las políticas pueden ser el marco de referencia de todos en un sistema, para practicar buenos hábitos, contribuir al desarrollo óptimo de la institución, aportar para fortalecer la cultura informática en la institución. Un documento que apoye a la institución dentro de su dominio a falta de legislación informática en el marco jurídico.

Casos de estudio

Caso CICESE.

El Centro de Investigación Científica y de Educación Superior de Ensenada (CICESE) es una institución dedicada a realizar investigación básica y aplicada [5]. Red-CICESE es el nombre oficial de un conjunto de facilidades y recursos informáticos, así como la infraestructura de telecomunicaciones y servicios asociados tanto local como remotos, provistos por la Dirección de Telemática [6] del CICESE como apoyo para el desarrollo de las actividades sustantivas del Centro.

El uso de los recursos informáticos era definido solo por el reglamento de cómputo en sus inicios y se transformó después como el reglamento de la Red-CICESE [7], sin embargo, ante el constante crecimiento de usuarios (internos y externos) y recursos, al crecimiento exponencial de Internet y su diversidad, las necesidades institucionales cambiaron. Surgió la necesidad de contar con una infraestructura de red protegida, con servicios de cómputo seguros, al mismo tiempo que se provee a los usuarios con los recursos informáticos en la cantidad y calidad que ellos demandan. De esta manera, las políticas de seguridad informática del CICESE emergen como el instrumento para concientizar a sus miembros acerca de la importancia y sensibilidad de la información y servicios críticos, de la superación de fallas y de las debilidades, de tal forma que permiten al Centro cumplir con su misión

Para iniciar el desarrollo del documento de políticas se creo un grupo de trabajo responsable de la elaboración de la política de seguridad informática para la institución. Durante su generación el reto principal fue convencer a algunos directivos y usuarios potenciales acerca de la necesidad de crearlas, ya que debido al constante crecimiento de las redes a nivel mundial, al incremento de accesos (usuarios con conexión) a Internet y al cambiante mundo de las telecomunicaciones, se requería contemplar una política "restringida" que permitiera garantizar la protección de la información y la disponiblidad de los recursos para los usuarios en tiempo y calidad. Otro aspecto delicado de decisión al que se enfrentó el grupo de seguridad fue en llegar a un acuerdo sobre cómo enfocar la política de acuerdo a la problemática particular de la institución en ese momento, es decir, en alcanzar un equilibrio entre libertad y restricción en el uso de los recursos sin que se vieran afectadas las actividades de investigación y administrativas del CICESE.

Como debe ser el caso en muchas instituciones, la firma de un documento oficial puede tomar bastante tiempo. En este caso, hubo un lapso de poco más de un año entre la creación de la primer versión, las revisiones por el Comité de Informática y su firma por el Director General. El apoyo de los directivos en todo momento fue positivo, sin embargo, se requirió que sucediera un incidente que afectara la imagen externa del Centro para captar la inmediata atención de las autoridades, la revisión final y su firma.

Dentro de los puntos destacados de una política son las estrategias de difusión y modificaciones. En este caso la primer difusión a nivel institucional provino de Dirección General en forma escrita, el documento se encuentra en línea en formato pdf, y puede accederse a través del sitio oficial del Centro en la sección de Estatutos, Reglamentos y Políticas[8] y en el sitio oficial de. la Dirección de Telemática. Adicionalmente se informa su existencia a cada nuevo usuario en el correo electrónico de bienvenida, y es referido en cada sospecha de incidente de seguridad.

El documento está bastante completo en cuanto a los derechos y obligaciones de usuarios, y a la definición del uso de los recursos en la Red-CICESE, sin embargo, adolesce de guías técnicas de protección de hardware y software, así como recomendaciones de seguridad para los usuarios. Estas secciones se encuentran en desarrollo y serán agregadas en un futuro próximo.

La Red-CICESE por su índole académica y por la estructura de usuarios, donde cada estudiante (quienes suelen ser los más inquietos) está asociado a un docente académico responsable, simplifica la tarea del Oficial de seguridad, ya que cualquier sospecha es reportada al académico o en todo caso a los coordinadores de posgrado, quienes de forma inmediata y con la autoridad requerida atienden el incidente y son solucionados fácilmente. Las políticas se han aplicado en varias ocasiones, casi en su totalidad por incidentes relacionados con inquietudes sobre programas, contenido pornográfico y/o uso de las cuentas de correo electrónico para fines no relacionados con el quehacer del Centro.

Caso CUDI.

Con el desarrollo de la siguiente generación de la Internet-2 a nivel mundial, México se une a este esfuerzo en Abril de 1999[8] creando la Corporación Universitaria para el Desarrollo de Internet (CUDI)[10], se define como RedCUDI a la infraestructura de telecomunicaciones y recursos informáticos

que conforman la red nacional de alta capacidad, así como todos aquellos recursos que estén disponibles por parte de las instituciones de educación superior y centros de investigación que coadyuven a la realización de las actividades académicas y de investigación.

Desde el inicio de la red se crearon diversos grupos de trabajo[11], entre ellos el grupo de seguridad[12] conformado por lo menos, de un miembro de la mayoría de las instituciones académicas que están dentro de RedCUDI, entre los objetivos de este grupo está la generación de las políticas de seguridad (las cuales se encuentran en este momento en revisión por el Comité de Desarrollo de la Red (CDR) así como las recomendaciones de seguridad para la parte telecomunicaciones y de aplicaciones que pasarían por la Internet2 de México.

En este caso, por ser una red que apenas está en desarrollo, permite poder definir las políticas de seguridad, reglamentaciones, especificaciones sin tantos problemas burocráticos, además de enfocarse a los recursos que están en el *backbone* y lo que transita por éste; dejando a cada institución con una autonomía en su red interna, pero respetando los lineamientos que se establezcan en RedCUDI. Para ello se creo una serie de documentos denominados *solicitud de comentarios para México* (RFCMX)[13] como un repositorio donde se publicarán todos los lineamientos, especificaciones y recomendaciones que se generen por los diversos grupos de trabajo de CUDI que deberán ser respetados e implementados por cada institución que se conecte a RedCUDI. Esto permite el definir estándares de facto muy parecidos a los RFC[14] que se generan en la Internet comercial, pero con la diferencia de que los documentos generados se realizan en consenso en los grupos, y posteriormente en los comités respectivos. Aprovechando esto, se han definido las políticas generales de seguridad de RedCUDI, las cuales han sido desarrolladas por el grupo de seguridad, y actualmente se encuentran en la etapa de aprobación por parte del CDR.

Dentro de los puntos que se destacan en las políticas estan: a) la figura del oficial de seguridad que debe tener cada miembro de CUDI, b) cada miembro de CUDI debe tener sus propias políticas de seguridad que no deben de contradecir las de RedCUDI, c) la forma en que un afiliado con problemas deberá pedir ayuda al asociado con el cual está conectado, d) y lo más importante, si existe un problema de seguridad se realizará una desconexión inmediata de la red miembro en cuestión hacia la RedCUDI y no podrá ser reactivada su conexión hasta no tener el visto bueno del grupo de seguridad, esto con el fin de garantizar la seguridad de RedCUDI.

Conclusiones

Las políticas de seguridad, así como las leyes que se generan, por si mismas no resuelven los problemas, a menos que realmente se apliquen, y se realice una vigilancia sobre su aplicación. Por otro lado, la seguridad no es un problema donde sólo una persona intervenga, sino es algo donde cada individuo que pertenece a una organización debe de participar y hacer conciencia de los efectos en caso de cumplir las políticas establecidas.

Las políticas no es un documento restrictivo, sino un forma de obtener un buen funcionamiento de la tecnología informática, así como garantizar la privacidad, disponibilidad y la veracidad de la información. Adicionalmente es una forma de reducir el mal uso que se le puede dar a las tecnologías existentes.

Algo importante, es que las políticas deben ser un documento en constante actualización, sobre todo si consideramos que la tecnología cambia a un ritmo muy acelerado.

Este documento propone las políticas de seguridad como un recurso para enfrentar la falta de legislación, pero de ninguna manera sustituirla. Es inminente la necesidad de reacción por parte de los grupos legislativos, para brindar medios legales a los ciudadanos de una nación, para defender los derechos a privacidad, confidencialidad e integridad de sus bienes informáticos.

Referencias

[1] M. Farias-Elinos, "La Importancia de la seguridad informatica: las politicas y la legislacion", 1ra. Semana de seguridad informatica, ESIME-Culhuaca, IPN, Mexico, del 26 al 30 de agosto del 2002.

[2] Téllez Valdés Julio; "derecho informático"; McGraw-Hill; Mexico 1996.

[3] Rodríguez,Hernández Victor; " La informática jurídica y su papel en el Derecho Mexicano"; electronical magazine of Computer right; http://www.vlex.com

[4] L. Arroyo, M. Farias-Elinos; "Importancia del marco jurídico en la función de auditoría informática", 1er. Congreso Iberoamericano de Seguridad Informática, Morelia, Mexico, February, 2002

[5] Centro de Investigación Científica y de Educación de Ensenada; http://www.cicese.mx; 2002

[6] Dirección de Telemática, CICESE; http://telematica.cicese.mx, 2002

[7] Reglamento para el uso de Red-CICESE; http://www.cicese.mx/cicese/normas/regla_27sep_2001.htm, Septiembre, 2000.

[8] Estatutos, Reglamentos y Políticas, http://www.cicese.mx/cicese/normas/, 2002

[9] Acta de la Asamblea Constitutiva de Corporación Universitaria para el Desarrollo de Internet, Asociación Civil. http://www.cudi.edu.mx/members/acta_final.pdf

[10] Corporación Universitaria para el Desarrollo de Internet, http://www.cudi.edu.mx, 2000

[11] Grupos de trabajo de RedCUDI, http://www.cudi.edu.mx/, 2001

[12] Grupo de Seruridad de CUDI, http://seguridad.internet2.ulsa.mx, 2001

[13] Solicitud de Comentarios para México (RFCMX) http://rfc.cudi.edu.mx, 2002

[14] Request for Comments (RFC), http://www.rfc-editor.org, 2002