Technical Profiles for Mexican Internet User to Improve Informatics Security

F. D. Felipe *IPN México,* F. Ch. Noya, *IPN México,* and I.S. Martínez *IPN México*

***Abstract*—In this work we present technical profiles for computer and Internet user. These profiles are made taking in account academic formation from high school to undergraduate studies in Mexico. We have analyzed high school schedules from the most important Mexican Universities. We made a similar task with undergraduate studies considering engineering, social and humanistic careers and also medical and health studies. We consider to do this work technical training, international standards about Informatics Security, Data Centers installation and operation standards. We propose four profiles including knowledge, competence for computer and Internet users to improve the Informatics Security and to prevent risks about cybercrime.**

***Index Terms*— Informatics Security, Technical Profiles, Internet, Cybercrime, Prevention.**

I. Introduction

LOS riesgos de a los que se enfrentan los usuarios de computadoras, conectadas o no a Internet han crecido de forma acelerada en los últimos diez años y se prevé que lo sigan haciendo en un futuro inmediato. Delitos como robo de identidad, fraudes financieros o bien ataques al equipo de cómputo del dueño o usuario de una computadora por medio de virus, caballos de Troya, malwares entre otros o bien que la computadora sea utilizada por personas anónimas para delinquir, sin que el propietario del equipo se entere son sólo algunos ejemplos de esos riesgos [5]. El crecimiento de tales delitos en el mundo ha sido tal que la Organización de las Naciones Unidas, en su conferencia mundial para prevenir el crimen, lo ha situado en el primer lugar de importancia, tanto por el gran número de delitos de este tipo que ocurren como por el gran impacto económico que tiene en la sociedad. Si bien hasta el momento gran parte de las personas en el mundo ignora al riesgo que está expuesto al utilizar una computadora, todavía menos conoce cuáles son los riesgos indirectos a los que se ve sometido de forma indirecta. Una situación más es el uso de equipos de cómputo de terceros para realizar crímenes informáticos, esto es la computadora de algún usuario común es utilizada, sin que esta persona esté enterada, para cometer afectaciones o delitos en un tercer equipo. Lo anterior se hace instalando un programa zombie o robot para que ejecute tareas de forma oculta o anónima para realizar esas tareas delictivas [2][3] [4].

Lo anterior obliga a cualquier usuario a tomar medidas de seguridad informática para protegerse, hasta cierto grado de tales riesgos. Hoy en día todas las computadoras deben utilizar al menos un antivirus, aunado a una herramienta para protección de ataques a través de Internet. Sin embargo no es suficiente comprar e instalar herramientas de protección, si el usuario no tiene un accionar seguro en su computadora y no detecta riesgos al trabajar con Internet. Se ha comprobado que buena parte de los incidentes de seguridad informática son propiciados o facilitados por los usuarios de Internet. Por ejemplo entrar a descargar música pirata pone en riesgo la computadora donde se trabaja y se hace vulnerable a la red de computadoras que brinda el servicio de Internet. Esto también se debe a la falta de comunicación entre los equipos de Seguridad Informática de una organización y los empleados que son usuarios de la red. Esto se repite incluso para personal técnico en sistemas computacionales como los desarrolladores de sistemas que se sienten limitados por las reglas de Seguridad que debieran de seguirse cotidianamente en la organización.

La situación antes descrita tiene su origen en varias causas que a continuación se describen brevemente. El primer aspecto es la formación académica que se recibe en México al respecto de la Seguridad Informática, en el nivel medio superior o bachillerato no existe ninguna materia que toque este tema o brinde práctica al respecto. Algo similar sucede en el nivel licenciatura, existen cursos de programación, de desarrollo de sistemas, manejo de Internet y otros, pero sólo en algunas materias se toca de manera tangencial el tema. Por otra parte las organizaciones no tienen considerado en sus perfiles laborales esta formación y pocas veces brindan entrenamiento o información al respecto. Aunado a esto, apenas se empieza a implementar la reglamentación y normatividad de manejo seguro de información. La situación fuera de México no es muy diferente, se han hecho estudios en varias partes del mundo, pero por ejemplo en Sudáfrica se han enfocado en usuarios de Café Internet [1]. En otra investigación, hecha en Inglaterra se enfocó en encontrar las causas o temas que provocan la fuga de información personal y si bien se obtienen resultados semejantes a esta propuesta no se contempla el tema educativo [13]. Por último un estudio en Ghana se enfoca a las prácticas de seguridad y no sobre la formación que debieran tener los usuarios a priori antes de iniciar sus actividades en Internet [14].

F. Felipe, F. Noya e I. Martínez son profesores de tiempo completo en el Instituto Politécnico Nacional de México en la Escuela Superior de Ingeniería Mecánica y Eléctrica Unidad Zacatenco, sus respectivos correos son ffelipe@ipn.mx, fnoya@ipn y ignacioms21@hotmail.con

978-1-5090-2435-3/16/$31.00 ©2016 IEEE

II. Análisis

A. Formación Académica La formación académica que se recibe en México compone la primer parte de este análisis. Una revisión de los programas de estudio del bachillerato en México, de las principales instituciones académicas, Instituto Politécnico Nacional (IPN), Universidad Nacional Autónoma de México (UNAM), el Colegio de Bachilleres (CdB) e Instituciones Privadas muestra que la Seguridad Informática no se toca directamente en sus planes de estudio. Por ejemplo la UNAM imparte tres materias, en ese nivel educativo que se enfocan en el manejo de un Sistema Operativo, manejo de procesadores de texto, elaboración de presentaciones y manejo de hojas electrónicas. Esas materias son comunes a todos sus estudiantes. Para los alumnos que deciden estudiar ciencias exactas toman tres materias del área computacional adicionales que se enfocan a Programación, Aplicaciones Industriales de la Informática, pero ninguna enfocada a la Seguridad Informática [12]. En el IPN sucede algo similar y se imparten las materias ya mencionadas al uso de la computadora para el manejo de información, además el IPN imparte materias más especializadas, debido a que busca que sus jóvenes egresados del bachillerato tengan una formación laboral. Las materias como Diseño Asistido por Computadora, Programación de Máquinas Herramientas de Control Numérico o Programación Avanzada, sin embargo tampoco tocan el tema de la Seguridad Informática [9].

La otra gran institución en México, por el número de estudiantes en sus aulas es el Colegio de Bachilleres, tiene materias de Manejo de Bases de Datos y otra dedicada al manejo de Internet, también tiene las materias enfocadas a Procesadores de Texto, Hojas electrónica y Sistema Operativo y se repite la situación de no abordar la Seguridad Informática. SI bien lo anterior puede parecer una omisión muy grande, se sabe por comentarios que si se hacen comentarios e incluso se dedican clases a abordar el tema en casi cualquier escuela, pero no está contemplado en los planes de estudio y tampoco está ordenado el conocimiento que se imparte por lo que quedan grandes huecos al respecto [11].

Para la educación superior o de pregrado el análisis se ha organizado en cuatro grandes áreas de conocimiento a saber: Humanísticas y de Ciencias Sociales, Investigación e Ingenierías, Económico Administrativas y por último las ciencias de la salud. En el primer grupo se consideraron licenciaturas en Derecho, Literatura y Letras, Filosofía, Pedagogía e Historia. Existen carreras muy similares con otros nombres, pero las anteriores son las más significativas. En general no se encuentran materias enfocadas a herramientas computacionales y mucho menos algo relacionado con la Seguridad Informática. Sólo se encontró como materia optativa de Computación, pero que puede acreditarse con cursos fuera de las aulas o si se cursó en el bachillerato.

Para el segundo grupo, Económico Administrativas, se consideraron licenciaturas como Contaduría, Administración, Economía, Relaciones Internacionales, todas ellas tienen materias computacionales que son muy útiles para su desempeño profesional. En el caso de la carrera de Administración de la UNAM tiene una materia llamada Tecnologías de la Información que toca temáticas como administración de proyectos, presentaciones por computadora, pero en ningún caso se tiene un tema de Seguridad Informática. Otra carrera del área es Mercadotecnia que se imparte en la Universidad del Valle de México que tiene una materia similar, Herramientas Computacionales que tiene la misma carencia.

El área de Ciencias de Salud no se cuenta con materias de Computación con una notable excepción: La carrera de Médico de la UNAM tiene una materia que tiene materias de tema computacional enfocadas a la Inteligencia Artificial, Diagnóstico Médico Computarizado y Búsqueda de Información y se repite la situación con la inexistencia sobre Seguridad Informática. Algunas de las carreras de esta área son Medicina, Odontología, Nutrición, Optometría y Psicología [9] [12].

Las carreras de Ciencias e Ingeniería, por su naturaleza, incluyen bastantes materias en las que se incluyen herramientas computacionales, algunas son: Redes de Computadoras, Bases de Datos, Inteligencia Artificial y varias enfocadas a los Lenguajes de Programación. Estas materias son muy específicas para expertos del área computacional y es muy sorprendente que sólo exista una materia enfocada a ese tema entre especialistas y sólo de una carrera. Algunas de las licenciaturas de este grupo son: Ingeniero en Computación, Licenciados en Ciencias Sistemas Computacionales, Licenciados en Informática y varias muy parecidas. En otro grupo caen Ingenieros como los Industriales, Civiles, Mecatrónicos, Mecánicos, Arquitectos, también se incluyen carrera como la de Físico y Matemáticas. En este último grupo se repite la situación de manejar varias herramientas computacionales, pero enfocadas al Diseño Asistido por Computadora, Simulación de Sistemas, Análisis Numérico y algunas muy similares, pero con las mismas carencias expuestas para todas las carreras en México [9] [12]

B. Certificaciones, Estándares, Normas y Leyes sobre redes/Seguridad.

Las carreras de Los profesionales dedicados a las tecnologías de Información en México trabajan en varias áreas o especialidades, algunas de ellas son: Redes de Datos, Telefonía, Aplicaciones para Dispositivos Móviles, Desarrollo de Sistemas de Información, Sistemas embebidos y algunas áreas más. Todos deben aprender diversas metodologías de trabajo, conocer y apegarse a estándares industriales y en varios casos respetar normas obligatorias en su trabajo cotidiano, en varias de ellas se tienen contempladas, en mayor o menor grado, temáticas relacionadas con la Seguridad Informática, de alguna manera informal tienen que seguir reglas sobre Seguridad Informática, es una necesidad indispensable para ellos, sin embargo el nivel de manejo y conocimiento es muy dispar y en ocasiones muy superficial, a continuación se describen algunas normas, estándares o certificaciones comunes en el medio de las TI´s.

La certificación CISCO en Redes de Computadoras es la más común en el mundo occidental, se divide en la actualidad en cinco niveles o capas, que van desde un nivel básico hasta el último nivel de especialización, estos niveles son *Entry*, *Associate*, *Professional*, *Expert* y *Architec* , los ingenieros que desean certificarse y obtienen certificaciones en diversas área o especializaciones. En total se tienen veintisiete certificaciones y de ellas tres se enfocan directamente en Seguridad. Es importante remarcar que los ingenieros que no se certifican en Seguridad no conocen todos los parámetros y detalles para implantarla a grados de alto rendimiento en sus organizaciones [18].

La Certificación ITIL (Information Technology Infraestructure Library) nació por la necesidad de estandarizar procesos y administrar servicios relacionados con las tecnologías de la información. Aunque se considera que el gobierno británico promovió fuertemente la adopción de esos estándares también es cierto que muchas empresas como IBM ya había propugnado para llegar a esa estandarización. ITIL está pensada como una guía que debe ajustarse y aplicarse de acuerdo a las necesidades de la organización que está usando la guía. La versión 3 de ITIL consta de cinco libros enfocados en: La estrategia del Servicio; Diseño del Servicio, Transición del Servicio, Operación del Servicio y Mejora Continua del Servicio. A su vez el libro del diseño del servicio considera en su apartado siete la Gestión de la Seguridad de la Información. Si bien puede considerarse que no se le da la importancia debida no debe olvidarse que ITIL está encaminado a un diseño global de la organización y ningún punto es más importante o valioso que otro, quienes pueden darle un lugar preponderante o dejarlo en un segundo término son los diseñadores de los servicios de TI. La situación que ocurre en México es que sólo las grandes organizaciones siguen las recomendaciones ITIL o las áreas de gobierno muy grandes, el común de las organizaciones no las sigue y por tanto no hay una visión global de la Seguridad Informática en la organización[19].

La Organización Internacional para la Estandarización (ISO por sus siglas en inglés) tiene dedicada toda una serie de estándares para la administración de servicios de tecnologías de la información, en especial la serie 27000 está dedicada a la administración de la Seguridad de la Información en las organizaciones, existen otros estándares en esta serie y pudiera parecer que la Seguridad está relegada o minimizada, sin embargo al consultar el estándar se entiende fácilmente que abarca todos los aspectos necesarios para implementar la Seguridad Informática en una Organización y también debe adaptarse más que adoptarse porque el estándar toca puntos que muchas organizaciones no realizan, por ejemplo existe un apartado para revisar y especificar el software desarrollado para vender por la organización, pero no todas se dedican a esa actividad por lo que no deben tocar ese punto durante la implantación del estándar. Aquí se tiene la misma situación que con la ITIL, en México sólo grandes organizaciones se enfocan a manejar este estándar [16].

Por último en esta sección se mencionaran las leyes vigentes en México. En el año del 2012 entró en vigencia la Ley Federal de protección de datos personales en Posesión de particulares. La ley señala, entre otras disposiciones, las obligaciones que tienen entidades gubernamentales y entidades privadas cuando guardan los datos personales y privados del público que trata con ellos. En uno de sus artículos, el sesenta Factores para determinar las medidas de Seguridad, señala en el apartado III que el responsable de resguardar la información debe considerar “El desarrollo tecnológico”. Sin embargo en ningún lugar se señalan cual es el Desarrollo Tecnológico o cuáles son esas normas de tipo técnico que debieran seguirse. Esta ley es la única que hacer referencia a las obligaciones, con respecto a las Seguridad de los datos y que de manera indirecta toca la Seguridad Informática [20]. Por otra parte existen en todo el mundo leyes que previenen los delitos informáticos y por tanto obligan a entidades a implementar medidas para garantizar la Seguridad Informática. Por ejemplo en los Estados Unidos de América se publicó en 1986 la Act Computer Abuse, en esa acta se tipifican diversos delitos que tienen que ver con el acceso no autorizado a computadoras y los medios de comunicación que utilizan y sobre todo utilizar información de la gente para obtener beneficios indebidos[7]. La Unión Europea, por su parte ha trabajado desde hace años y en octubre del año 2001 se estableció un Convenio sobre la Ciberdelincuencia [21]. En América Latina también se han implantado leyes similares, como en Colombia que en enero del año 2009 se modificó el Código Penal para contemplar estos delitos [8].

C. Entrenamiento y capacitaciónt

El último tema de este análisis es que sucede en México con la capacitación y el entrenamiento del personal en las organizaciones en México. En entrevistas realizadas a responsables de redes de computadoras, de Seguridad Informática incluso de desarrollo de sistemas. se encontraron entre otras cosas que el factor humano es el principal factor que afecta los sistemas de seguridad, dos que el entrenamiento que reciben los empleados es casi nula, por razones de espacio no se reproducen las dos tipos de entrevistas que se hicieron y la primera fue abierta. Los responsables de la Seguridad consideran a los elementos de la organización como actores que sólo deben ceñirse a las reglas que se les imponen sin que ellos participen proactivamente en el diseño de las políticas y medidas de Seguridad, lo anterior genera una desconexión entre el personal de la empresa y estos equipos de Seguridad. En México el entrenamiento y la capacitación, en cualquier tema laboral, son poco implantados por la mayoría de las empresas, generalmente los grandes consorcios si acostumbran realizar estas actividades, pero aun ellos dedican pocos esfuerzos en este sentido.

III. DEFINICIÓN DE PERFILES

Clasificación de perfiles. El análisis de la sección anterior muestra que la formación en Seguridad Informática que pueden obtener las personas por medios formales es muy pobre. En el ámbito laboral la situación se repite. Para

facilitar y orientar a las personas o sus empleadores se propone la siguiente clasificación de usuarios que permitirá detallar posteriormente los perfiles técnicos y laborales que ellos requieren para incrementar los niveles de Seguridad Informática en el entorno que se desenvuelven al usar computadoras conectadas a Internet. La tabla No 1 muestra esa clasificación:

TABLA I
Clasificación de Usuarios

Tipo de Usuario	Formación mínima	Observaciones
Usuario General	Bachillerato	Trabajo en Hogar, Escuelas
Empleado de Organización	Bachillerato o Educación Superior	Trabajo no especializado, atención al público
Desarrolladores	Ingeniería Informática Sistemas Computacionales	Labores Técnicas
Personal de TI´s y Seguridad Informática	Ingeniería Informática Sistemas Computacionales	Prevención de Problemas

Los usuarios generales no tienen una responsabilidad especial en alguna organización, el uso que hacen de computadoras es para acceder a Internet, principalmente por diversión o por necesidades de tipo académico. La formación académica que tienen es por lo general del bachillerato, al menos en México, por obvias razones el entrenamiento o capacitación que reciben es nula.

Un empleado de una organización ya tiene, por lo general, una formación académica mínima de bachillerato, muchos profesionistas caen en este rubro, por ejemplo, contadores, administradores, abogados o médicos entre otros. En muchos casos también entran ingenieros, pero que no realizan actividades de Tecnologías de la Información.

Los dos últimos casos son diferentes, prácticamente todos, tienen una formación académica relacionada con las TI´s, en México las principales carreras de este tipo son Ingenieros en Computación, Licenciados en Informática, Ingenieros en Sistemas Computacionales y otras más con planes de estudio construidos alrededor de las TI´s. En cambio cada caso o grupo de usuario se va especializando debido a su desempeño profesional cotidiano, el segundo grupo, el encargado de la Seguridad Informática y del manejo de las Tecnologías de Información se mezclan en su trabajo diario y en México se da el caso que el área de TI´s se encarga de la Seguridad o bien es un departamento especial que con el tiempo, por su tamaño termina separándose en funciones.

Perfiles Técnico laborales. Las habilidades y conocimientos que debieran tener los usuarios de computadoras e Internet, para incrementar la seguridad están descritos en la tabla No. Dos:

TABLA II
Perfiles Técnicos y Laborales

Tipo de Usuario	Formación mínima
Usuario General	Terminología elemental de Seguridad Informática Identificación de Sitios Peligrosos Identificación de Actividades Riesgosas Aspectos y riesgos legales del uso de computadoras e Internet.
Empleado de Organización	Identificación de Sitios y direcciones institucionales. Conocimiento y Aplicación de Políticas y Reglas de Seguridad de la Organización. Diagnóstico básico de fallas del equipo y de ataques y Problemas de Seguridad
Desarrolladores	Conocimiento y aplicación de normas y estándares de Seguridad. Conocimiento de Tecnologías de Implementación de Sistemas de Seguridad.
Personal de TI´s y Seguridad Informática	Implantación de Sistemas de Seguridad Identificación de Situaciones de Riesgos y e Ataques Informáticos. Identificación de debilidades en Aplicaciones adquiridas o desarrolladas por la organización Implantación de Sistemas de Prevención de Desastres Informáticos. Implantación y Seguimiento de Planes de Continuidad del Negocio.

Cada perfil debiera conocer y manejar adecuadamente los del nivel anterior, pero por simplicidad se detallan las de cada nivel en cada fila de la tabla.

En entrevistas con responsables de Seguridad Informática de grandes organizaciones recomiendan que sus expertos se especialicen a su vez en otras áreas como éstas:

- **Seguridad Perimetral:** Firewall, IDS/IPS, WAN, DMZ, Análisis de vulnerabilidades de Sitios WEB Internos, propios Hosteados, Externos contratados.
- **Plataforma de Sistema Operativo:** Windows y Unix, Seguridad en directorio activo, Antivirus, toda la suite, Análisis de vulnerabilidades internas, Aplicación de Parches, distribución masiva de software, inventario técnico detallado de Hardware, inventario de software, monitoreo, reconocimiento y manejo de alertas y respaldo de información.
- **Plataforma de Bases de Datos**. Seguridad en todas las bases de datos, integridad y confiabilidad de los datos y monitoreo de las mismas.
- **Plataforma apps**. Encargarse de la seguridad de todas las aplicaciones, por ejemplo ERP del análisis de vulnerabilidades y técnicas de monitoreo de las mismas.
- **Prevención y recuperación de Desastres Informáticos.** Análisis de Riesgos, Planes de Prevención, Sistemas de respaldos, Sistemas alternativos de operación, Planes de Recuperación de Desastres.

Puede preverse que cada organización difiere en estructuras, necesidades y riesgos y que las medidas de entrenamiento y capacitación que adopté deben de acomodar lo mejor posible

para ellas, los planes de Prevención y recuperación de Desastres son un tema que no debe dejarse de lado por ningún motivo.

IV. Conclusiones

Se ha hecho una propuesta descriptiva de los perfiles técnicos y laborales para que usuarios de computadoras e Internet en México tengan el conocimiento. La habilidad técnica y el comportamiento para incrementar la Seguridad Informática en su entorno. Esta descripción también puede servir de modelo para que organizaciones gubernamentales, empresas de todo tamaño y organizaciones sociales lo hagan con el factor humano que trabaja o colabora cotidianamente con ellos.

Se infiere del análisis de Planes y Programas de Estudio a nivel bachillerato y Superior, esto es licenciaturas, que se tiene una deficiencia en este aspecto en el Sistema Educativo Nacional de México y en un futuro inmediato debiera haber una discusión al respecto sin olvidar los aspectos legales y tecnológicos. Con respecto a los empleadores convendría ampliar los perfiles conforme a la norma ISO-31000 [19] o bien prácticas similares de prevención y administración de riesgos., sin embargo el cumplimiento de esta norma es muy pobre en México.

V. Agradecimientos

Los autores agradecen el apoyo recibido por los Sistemas de Becas por Exclusividad de la COFAA (SIBE) y del Programa de Estímulos al Desempeño Docente del IPN (EDD). Este trabajo es derivado del Proyecto de Investigación **“Seguridad Informática, clave 20150536”** de la Secretaría de Investigación y Postgrado del Instituto Politécnico Nacional de México.

VI. Referencias

Periodicas:

[1] Thaga A., 2013. “Information Security Issues Facing Internet Café Users”. International Journal of Computer Science and Electronics Engineering Volume 1 Issue 5.

Libros:

[2] Gercke, M., 2012 “Understanding cybercrime: Phenomena, challenges and legal response”. Unión Internacional de Telecomunicaciones.

[3] Gercke, M., 2009 “El Ciberdelito Guía para los países en desarrollo”, Unión Internacional de Telecomunicaciones.

[4] Piña, L. 2012 “Los Delitos Informáticos previstos y sancionados en el Ordenamiento Jurídico Mexicano”, UAEM.

[5] Salomon, D. 2010, “Elements of Computer Security” Springer England

Reportes Técnicos:

[6] Internet Engineering Task Force, 2014. http://www.ietf.org/about/mission.html.

[7] Cornell University, 2008 https://www.law.cornell.edu/uscode/pdf/uscode18/lii_usc_TI_18_PA_I_CH_47_SE_1030.pdf USA.

[8] Alcaldia de Bogota 2010. www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492. Colombia.

[9] IPN 2015 www.ipn.mx/alumnos/

[10] Internet Engineering Task Force, 2014. http://www.ietf.org/about/mission.html.

[11] Colegio de Bachuilleres 2015. Planes de Estudio. http://www.cbachilleres.edu.mx/cbportal/index.php/component/content/article/178

[12] UNAM, Planes y Programas de Estudio. www.unam.mx

Papers en Memorias de Conferencias (Publicadas):

[13] Blythe J., Coventry L., Little Linda 2015 “Unpacking security policy compliance: The motivators and barriers of employees’ security behaviors” Symposium on Usable Privacy and Security, Cánada.

[14] Chen J., Paik M., McCabe K., 2014 “Exploring Internet Security perceptions and practices in Urban Ghana”. Symposium on Usable Privacy and Security, USA.

[15] ONU 2012 *Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal*, Brasil.

Estándares y Leyes:

[16] ISO 2015.” Information Security management system implementation guidance”. http://www.iso27001security.com/html/27003.html

[17] ISO 2015. “Risk Management”. http://www.iso.org/iso/home/standards/iso31000.htm.

[18] CISCO, 2015, Track de Certificaciones. 2015. http://www.cisco.com/c/en/us/training-events/training-certifications/certifications.html#~Cert.

[19] ISO 2015 “Guidance on the application of service management systems” http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=51987.

[20] Cámara de Diputados 2012. http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf México

[21] Unión Europea “Convenio sobre Ciberdelincuencia. 2001. http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/Documents/Convention%20and%20protocol/ETS_185_spanish.PDF

VII. Biografias

Federico Felipe Durán. Es profesor de la Academia de Computación de la carrera de Ingeniería en Comunicaciones y Electrónica de la Escuela Superior de Ingeniería Mecánica y Eléctrica del Instituto Politécnico Nacional de México. Sus áreas de interés incluyen Seguridad Informática y la Ingeniería de Sistemas. Federico Felipe es Ingeniero en Comunicaciones y Electrónica por el IPN (1984) y realizó estudios de Postgrado en Ingeniería Eléctrica en el Centro de Investigación y Estudios Avanzados (1987).

Fernando Noya Chávez. Es profesor de tiempo completo de la Academia de Computación de la carrera de Ingeniería en Comunicaciones y Electrónica de la Escuela Superior de Ingeniería Mecánica y Eléctrica del Instituto Politécnico Nacional de México. Ha laborado en la iniciativa privada y en el sector público en áreas de redes de computadoras y de seguridad informática, Es Ingeniero en Comunicaciones y Electrónica (1992) por el IPN y por la misma institución Maestro en Ciencias en Ingeniería de Telecomunicaciones (2004).

Ignacio Martínez Sánchez. Obtuvo el título de ingeniero Mecánico en la Escuela Superior de Ingeniería Mecánica y Eléctrica. Obtiene el grado de Maestro en Ciencias en Ingeniería de Sistemas en la misma Escuela. Actualmente es profesor investigador en la carrera de Ingeniería en Control y Automatización de la ESIME Zacatenco. Sus áreas de interés son la educación en la ingeniería, Ingeniería de Sistemas y los sistemas de Calidad.