Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2008 Proceedings

Americas Conference on Information Systems (AMCIS)

2008

Social Cognitive Theory: Information Security Awareness and Practice

Santos M. Galvez
TUI University, sgalvez@tuiu.edu

Indira R. Guzman
TUI University, iguzman@tuiu.edu

Teoria Social Cognitiva: Concientización y Prácticas de la Seguridad de la Información

Social Cognitive Theory: Information Security Awareness and Practice

Santos M. Galvez
TUI University
sgalvez@tuiu.edu

Indira R. Guzman
TUI University
iguzman@tuiu.edu

ABSTRACT

In this paper, the authors discuss employees' beliefs about their abilities to competently use computer information security tools in the determination of effective information security practices within organizations. In the first section the authors present a background about information security practices at work. Then, the authors present a research approach based on social cognitive theory applied in the information security context within organizations to address the individual and environmental factors that explain information security behavior of end users. The objective of the literature review is to describe the definition and operationalization of constructs such as *information security awareness* and *information security practice* as the mediating and dependent variables, and the independent variables of support within the organization, encouragement by others, others' use as environmental factors in the information security context; and finally, self-efficacy and outcome expectations as the individual factors. A research model with a set of propositions is presented to improve the understanding of the personal and environmental factors that influence the effective security practices of organizational employees.

RESUMEN

En este trabajo, los autores discuten las creencias de los empleados acerca de su capacidad de utilizar en forma competente el uso computacional de herramientas de seguridad de la informacion en la determinación efectiva de prácticas de seguridad de la información dentro de las organizaciones. En la primera sección los autores presentan los antecedentes acerca de las prácticas de seguridad más comunes dentro de organizaciones. A continuación, los autores presentan un enfoque de investigación basado en la teoría social cognitiva (TSC) aplicada en el contexto de seguridad de la información dentro de las organizaciones para analizar los factores individuales y ambientales que explican el comportamiento relacionado a seguridad de la información (SI) de los usuarios finales. El objetivo de la revisión de la literatura es describir la definición y operacionalizacion de las variables, como la concientizacion de seguridad de la información y la practica de la seguridad de la información como variables mediadoras y dependientes, y las variables independientes de apoyo dentro de la organización, la exhortación de los demás, otros factores ambientales el contexto de seguridad de la información; Y, por último, autoeficacia y expectativas de resultados como los factores individuales. Se presenta un modelo de investigación con un conjunto de proposiciones para mejorar el entendimiento de los factores personales y ambientales que influyen en el desempeño eficaz de las prácticas de seguridad de la información por los empleados de una empresa.

Keywords

Socio Cognitive Theory; Information Security; Information Security Behavior

Palabras clave:

Teoría social cognitiva, la seguridad de la información; comportamiento de la seguridad de la información

INTRODUCCIÓN

Con la aparición en todo el mundo del protocolo TCP/IP para Internet en 1973, el mundo se "abrio" al mundo de Internet. Los individuos, las organizaciones y la sociedad en su conjunto comenzó a explorar la riqueza y todas las potencialidades que el nuevo servicio ofrece y lo han utilizado en todo tipo de actividades. La apertura al mundo a Internet ha sido una gran oportunidad para la gente y las empresas, pero también es una oportunidad para que la gente que tiene otro tipo de intenciones como los hackers quienes buscan acceder a la información de las organizaciones sin la autorizacion debida.

Según DarkReading.com (2006) los costos de los delitos informaticos son considerables. Por ejemplo, cuando las identificaciones y contraseñas son robadas y usadas para delitos informaticos, la pérdida promedio por incidente fue de $ 1,5 millones. Por otro lado, según un estudio reciente realizado por el Yankee Group se indica que más de la mitad de las empresas aseguran que la interrupcion del Intenet cuesta más de 1000 dólares por hora; por último, en un estudio publicado en 2004, el Aberdeen Group encontró que el costo de las interrupciones en negocios basado en Internet es de aproximadamente 2 millones de dólares por incidente. Estas cifras son sólo la punta del iceberg en la representación de los costos asociados con la destrucción intencional de las actividades relacionadas con el ordenador.

Existe una amplia variedad de riesgos de seguridad de la informacion como virus, gusanos, los ataques para la negación de servicios, spoofing, el robo de contraseñas, la ingeniería social, la explotación del software, troyanos, y la violacion de autoridad y autorización que puede tener un efecto muy negativo en las operaciones de una organización (Chen, Shaw, Yang, 2006). Respecto al dualismo de la seguridad (Cano, 2004), el aspecto “subjetivo” de SI requiere tener un entendimiento de las técnicas de seguridad informática para reducir los riesgos e implementar controles. El aspecto “objetivo” de la inseguridad informatica se refiere al conocimiento de las vulnerabilidades en SI para tomar medidas correctivas. En ambos casos, el compartamiento de los usuarios es determinante en el proceso de prevencion de ataques informaticos. Como las amenazas de seguridad han aumentado, la necesidad de proteger los datos empresariales se ha convertido en una necesidad imperiosa. Aunque algunos de estos ataques pueden ser originados externamente, la mayoría de ellos están directamente o indirectamente originados por empleados que trabajan dentro de la empresa. Por ejemplo, el más peligroso y quizá el método más fácil, para adquirir información es mediante la ingeniería social. Arief y Besnard (2005) se refieren a ésta como "la debilidad del wetware" donde "el objetivo es engañar a la gente para que revele contraseñas u otra información que comprometa los sistemas de seguridad del sistema escogido" (p. 5). La Ingeniería social de este tipo se aprovecha del impulso basico humano de ayudar a otras personas, lo que los psicólogos y los sociólogos llaman la conducta prosocial (Stanton y Stam, 2006). Muchas veces, el problema no es la tecnología, pero el compromiso debido a la tecnología por parte del usuario. Es importante, por tanto, comprender los factores que influyen en el comportamiento humano de la seguridad de la información.

De acuerdo con Chen, Shaw, Yang (2006), la falta de seguridad, el conocimiento y la conciencia por parte de los usuarios de los sistemas de información es un gran problema de seguridad dentro de las organizaciones. Las amenazas de la seguridad de la información, podrían minimizarse si los usuarios internos de los sistemas de información de una organización realizan prácticas de manera efectiva (Ryan, 2006). Basándose en la Teoría Social Cognitiva (Bandura, 1977), el presente trabajo, propone un modelo de investigación para comprender los factores personales y ambientales que influyen en el desempeño eficaz de las prácticas de seguridad de la información por los usuarios de los sistemas de información dentro de las organizaciones.

En las siguientes secciones de este documento, en primer lugar, hablamos de la teoría social cognitiva (TSC). TSC sirve de base para comprender: la situación del medio ambiente o características, por ejemplo, las presiones sociales tales como el exhortacion de los demás, la utilización por otros, y el apoyo a utilizar las herramientas de seguridad de la información, factores cognitivos personales incluyendo auto-eficacia, expectativas de resultados, así como las características demográficas, y el comportamiento de la seguridad de la información, que está compuesto de la concientizacion de seguridad de la información (CSI) y la practica de la seguridad de la información (PSI) tal como lo define y operacionaliza Ryan (2006).

Un conjunto de propuestas son ofrecidas en este documento las cuales estan basadas en el modelo TSC. Por último, se abordan las consecuencias de la aplicación de este modelo, y las fortalezas y limitaciones de este enfoque.

BASE TEÓRICA - LA TEORÍA SOCIAL COGNITIVA

La teoría social cognitiva define la conducta humana como un triádico donde existe una relacion dinámica y recíproca entre el medio ambiente, los factores personales, y el comportamiento humano (Bandura, 1977, 1997). Las personas eligen el

entorno en que existen y se ven influidas por el entorno. El comportamiento se ve afectado por el ambiente, que a su vez se ve afectado por el comportamiento humano. Por último, el comportamiento está influenciado por factores personales del individuo quien a su vez, afectan el comportamiento de los otros factores (Compeau y Higgins, 1995). Según esta teoría, el comportamiento de una persona es única y mutuamente determinado por cada uno de estos tres factores: a) las influencias ambientales como son la presión social o las características únicas situacionales (de tipo cognitivo); b) los factores personales, entre ellos la personalidad y las características demográficas y, por último c) el comportamiento (Compeau y Higgins, 1995, p.190).

Según Bandura (2002) la teoría social cognitiva adopta una perspectiva agencial. Existen tres modos de agencia muy bien distinguidos por esta teoría. Uno de ellos es agencia personal que se implementa en forma individual; Agencia Proxy es cuando la gente influye en los demás para actuar en su nombre con la finalidad de garantizar los resultados deseados. El tercero se refiere al comportamiento real de los individuos influenciados y las influencias de otros agentes. Agencia Colectiva es cuando la gente actúa con el proposito de forjar su futuro. Se ejerce a través del grupo de acción. Sin embargo, en este estudio, nos enfocamos en la agencia personal o el individualismo en el contexto de seguridad de la información. De hecho, la TSC tiene muchas dimensiones, pero en esta investigación tratamos el rol de los factores cognitivos en el comportamiento individual, de manera similar a Campeau y Higgins (1995), pero aplicada a la seguridad de la información. Empezamos definiendo comportamiento de seguridad de la información, los factores personales y, por último, los factores ambientales.

COMPORTAMIENTO DE SEGURIDAD DE LA INFORMACIÓN

Comportamiento de Seguridad de la Información se compone de concientizacion de seguridad de la información, la práctica de seguridad de la información.

CSI – Concientizacion de seguridad de la información

Debido a la creciente amenaza contra la seguridad de los diferentes sistemas de información en las organizaciones, no es suficiente confiar en las tecnologías de seguridad, como los sistemas de deteccion interna y antivirus tanto como hardware y software. Según Goodhue y Straub (1991); Straub y Welke (1998); Dhillon y Backhouse, (2001); Hu et al. (2006), la seguridad de la información es un problema socio-tecnológico que requiere una comprensión completa del eslabón más débil de la defensa contra las amenazas a la seguridad: El comportamiento humano y las actitudes sobre el uso de estas tecnologías de seguridad. Según una encuesta sobre infracciones del Departamento de Comercio e Industria de Seguridad de la Información en el 2004 se informo que el ser humano es el eslabón más débil en la cadena de control de seguridad (Chen et al., 2006). Por lo tanto, una de las medidas preventivas sugeridas por Timms, Potter, y Beard (2004) fue el de crear una cultura consciente de la seguridad que tendria la misión de educar al personal acerca de los diferentes riesgos de seguridad y sus responsabilidades.

Dentro de la literatura, el concepto de concientizacion se ha definido por ejemplo como "Concientizacion tecnologíca" por Deniv y Hu (2007), como "la conciencia del usuario planteada y el interés en conocer acerca de los temas tecnológicos y estrategias para tratar con ellos" (p.391). Dinev y Hu (2007), definen la concientizacion de la innovación como "la medida en que la población objetivo es consciente de una innovación y se formula una percepción general de lo que implica". Existen también algunas definiciones de la "concientizacion de seguridad" en la literatura con diferentes niveles de implicación en rendimiento. Por ejemplo, en un documento del Instituto Nacional de Estándares y Tecnología, Lisa Lindholm define la concientizacion de seguridad como "una responsabilidad y la comprensión individual suficientes para cumplir con las políticas". También indica que la concientizacion de seguridad es el mejor retorno de la inversión para los programas de seguridad de la información. Según Siponen (2000), CSI se utiliza para referirse a un estado donde las personas de una organización son conscientes de su misión de seguridad, así como idealmente dedicados a la misma. En seguridad de la información, la sensibilización es muy importante, asi como lo es la seguridad a nivel técnico y los procedimientos, pues los procesos pueden ser mal utilizados, mal interpretados o no utilizados por las personas perdiendo de esa manera su eficacia real (1989 1989 1996 ; Straub, 1990; Straub y Welke, 1998). Por último, sobre la base de una revisión de la literatura, Chen et al. (2006) define CSI como la atención a la seguridad en el que se reconocen las preocupaciones de seguridad de la informacion y la necesidad de responder apropiadamente (Chen et al. 2006). Estas definiciones no implican sólo estar informado sobre los problemas de seguridad, pero en realidad que se responda y reaccione ante estos problems, por lo tanto, esta actitud puede ser considerada como un factor de *comportamiento*. Es importante mencionar que esta definición implica también un comportamiento cognitivo.

El aumento de la concientización sobre la seguridad debe minimizar las fallas relacionadas a amenazas a la seguridad y aumentar la eficacia de las técnicas y los procedimientos en contra de las amenzas de seguridad en una organización. Para este estudio, por lo tanto, definimos como CSI como la conciencia del usuario y el interés en conocer sobre los problemas de seguridad y las estrategias para hacerles frente. CSI es uno de los comportamientos de seguridad de la información.

Con el fin de operacionalizar esta variable, encontramos tres modos de medición de la concientizacion en la literatura de Sistemas de Informacion: Uno de Disiv y Hu (2007), otro de Chen et al. (2006) y, por último, uno de Ryan (2006). Utilizamos el enfoque de Ryan (2006), ya que este está más explícitamente dirigido a la seguridad de la información. Ryan (2006) analizó inicialmente una serie de 12 atributos de las variables CSI agrupadas por temas demográficos, la tecnología, la política y la amenaza de contexto. Él terminó con 9 puntos de vista CSI: tecnología, la amenaza de contexto, la autenticación de los usuarios, la política formal, física, control de acceso, la política de información, la encriptacion, y de gestión de la seguridad. La puesta en marcha de esta variable CSI tal como se presenta en el trabajo de Ryan está incluido en el Apéndice A.

PSI – Practicas de seguridad de la información

Según Berghel (2007) en la seguridad de la información de negocios, hay una serie de diferentes modelos de seguridad propuestas por los profesionales y las organizaciones. Estos modelos de seguridad estan basados en los principios de privilegio, de defensa en profundidad, la base de referencia de seguridad, el endurecimiento de perímetro, detección de intrusos, prevención de intrusiones que están tratando de minimizar las vulnerabilidades y amenazas reales o potenciales. La diferencia entre estos modelos es la estrategia contra las vulnerabilidades y amenazas. Por ejemplo, basados en el tiempo de seguridad (TBS) se utiliza el tiempo como principal medida de riesgo. El margen de seguridad aumenta con la advertencia previa, de modo que, siempre y cuando la antelada notificación es superior a la suma de la detección y los tiempos de respuesta en que la información está protegida. Por otra parte, el principio de mínimo privilegio (PMP) se basa en los controles. Esta estrategia varía inversamente con el grado de control otorgado a la aplicacion o el usuario.

En la actualidad, existen diferentes organizaciones bien conocidas que promueven las normas específicas de seguridad, como el COBIT (Control Objectives for Information and related Technology) Objetivos de Control para la Información y Tecnología relacionada, el Sistema de Información Federal de Control Manual de Auditoría (FISCAM), el Certificado de Auditores de Sistemas de Información (CISA), el BSI 7799/ISO 17799/ISO 27001 normas de las mejores prácticas. Estas normas coinciden con las normas de la legislación o de los mandatos del gobierno, como el Acta de Portabilidad y Responsabilidad del Seguro de Salud (HIPAA = Health Insurance Portability and Accountability Act) (Berghel, 2007). La Organización de Seguridad de la Información (ISO) estandart adopta la forma de directrices y recomendaciones destinadas a servir como un punto de referencia único para la identificación de la gama de controles necesarios para la mayoría de las situaciones en que se utilizan los sistemas de información (Veiga y Eloff, 2007). La ISO / IEC 27000 es una serie estándar de la seguridad de la información publicada por la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC) como ISO / IEC 17799:2005 y luego pasa a ser el ISO / IEC 27002:2005. Como declaró Eloff Veiga (2007), ISO 17799 se ha ido ganado el reconocimiento como una norma esencial para la seguridad de la información, donde ISO27001 (2005) se considera como parte de la norma ISO / IEC 17799 y se propone como una estrategia de mejora continua a través de un proceso de establecimiento, implementación, funcionamiento, supervisión, revisión, mantenimiento y mejora de la organización de la información de gestión de la seguridad (ISO, 2005; IEC, 2005).

Dado que estas políticas de seguridad deben aplicarse dentro de las organizaciones, los empleados que las siguen son en realidad los que realizan prácticas de seguridad de manera efectiva. Ma y Pearson (2005) empíricamente validaron siete de las diez variables de las directrices y las prácticas más aceptados por profesionales de la tecnología de la información: ISO / IEC 17799: 2005 y BS 7799. Sobre la base del análisis de estas variables, Ryan (2006) creo una escala cuestionario que incluye preguntas para evaluar PSI de los usuarios tomando en cuenta los mismos nueve puntos de vista que han sido utilizados en el cuestionario de CSI. La puesta en marcha de la operacionalizacion de esta variable como fue hecha for Ryan está incluida en el Apéndice B. Estas dos variables representan el comportamiento de la seguridad de la información, CSI es la base para PSI. Por lo tanto, en este documento se propone:

> Proposición 1. Cuanto mayor sea la concientizacion de la seguridad de la información, mayor es la practica de seguridad de la información .

FACTORES PERSONALES DE SEGURIDAD DE LA INFORMACIÓN

Bandura, afirma que hay dos series de expectativas como las principales fuerzas de guiar el comportamiento cognitivo: una relativa a los resultados y otra a la auto-eficacia (creencias acerca de la capacidad de realizar una determinada conducta). Auto-eficacia influye en decisiones acerca de los comportamientos a los que se comprometen.

Auto-Eficacia de Seguridad de la Información (InfoSec)

Según Bandura (1977), auto-eficacia es la percepción individual o creencias de que uno tiene la capacidad de realizar un determinado comportamiento y las suficientes habilidades para realizar tareas, en las que el individuo también tiende a hacer las tareas con éxito (Compeau y Higgins, 1995; Ryan, 2006). Compeau y Higgins (1995) elaboraron y validaron por primera

vez, una variable para entender el impacto de la auto-eficacia en reacciones individuales hacia la tecnología informática denominada "autoeficacia computacional" (AEC=Computer Self efficacy). Los autores inicialmente desarrollaron un modelo teórico basado en la teoría social cognitiva (Bandura, 1986) que incluye la nueva medida del AEC. Luego se puso a prueba su modelo en una muestra de 1020 trabajadores del conocimiento en Canadá, se llego a la conclusión de que la auto-eficacia desempeña un papel importante en la configuración de los sentimientos y comportamientos hacia el uso de la computadora. Las personas con alta autoeficacia usaban más las computadoras, disfrutando más del uso, y experimentaron menos ansiedad (Compeau y Higgins, 1995). Afecto y ansiedad también tuvieron un impacto significativo en el uso de la computadora. Los autores presentan un estudio de seguimiento publicado en 1995. Ponen a prueba un subconjunto del modelo probado en el documento de 1995, pero utilizando los datos longitudinales recogidos de más de 394 usuarios finales con un año de intervalo. Los resultados confirmaron que tanto la auto eficacia y las expectativas de resultados de impacto sobre las expectativas de un individuo impactaban el comportamiento afectivo a las tecnologías de la información. En este estudio se pretende utilizar la misma escala o cuestionario del documento de 1995 contar con la fiabilidad del instrumento. Los autores concluyeron que autoeficacia es un fuerte y significativo predictor de afecto, la ansiedad y el uso un año más tarde. Auto-eficacia regula el funcionamiento humano de forma cognitiva, motivacional y afectivo en los procesos de toma de decisiones (Bandura, 2002).

TSC ha demostrado ser un poderoso mecanismo para explicar y predecir las reacciones humanas que rigen el comportamiento y ha sido ampliamente utilizado por los investigadores. Hayashi, et al. (2004) llevó a cabo un experimento de campo para poner a prueba una propuesta de modelo de integración de investigación. El modelo se basa en el AEC, la Tecnología aceptación modelo, el modelo de expectativa-Confirmación (ECM) y la teoria de computación de usuario final. Se utilizó con la intención de evaluar alumnos que continúaban utilizando el sistema de e-learning (enseñanza en linea) como un vehículo para asimilar las Tecnologias de Informacion. Por otro lado, Havelka (2003) utiliza datos de los estudiantes matriculados en el curso MIS en una gran universidad del Medio Oeste (aproximadamente 15000 estudiantes) para poner a prueba la autoeficacia del software y la ansiedad entre los estudiantes con diferentes predictores demográficos tales como académicos, los años de experiencia en el uso de ordenadores, cantidad de cursos relacionados con el ordenador, etc. El autor concluye que los estudiantes de diferentes areas de estudio tienen diferentes niveles de auto-eficacia, y una relación negativa entre la auoteficacia del Software y la ansiedad computacional. Smith (2005) utiliza datos de los estudiantes en una gran universidad del Medio Oeste (alrededor de 310) para examinar las diferencias raciales y de género en el acceso y la participación en los cursos de tecnología de la información en los niveles secundario y postsecundario de la educación. El investigador encontró que las mujeres tuvieron un menor número de cursos relacionados a tecnología de la información comparado con los datos de hombres. Los no blancos tuvieron un menor número de cursos en la tecnología de la información comparados con la gente blanca en el nivel secundario y postsecundario.

En este estudio, la variable de la AEC está adaptada al contexto de seguridad de la información, como fue hecho por Ryan (2006). AEC se define como la percepción individual o de creencias que uno tiene la capacidad de realizar conductas de seguridad de la información y por tener suficientes habilidades para realizar tareas de seguridad, en que el individuo también tiende a hacer las tareas con éxito. Las tareas de seguridad se refieren específicamente a la capacidad de instalación y puesta en marcha de software de seguridad a nivel de usuario. Si los usuarios finales son capaces de instalar y configurar software de seguridad básicos en sus computadoras, esto influirá en sus prácticas reales de la seguridad de la información. Por lo tanto, en este documento se propone,

> Proposición 2: Cuanta más alta es la autoeficacia computacional en la seguridad de la información, mayor es la concientizacion de seguridad de la información.

La operacionalizacion de la variable PSI tal como se presento en el trabajo de Ryan está incluida en el Apéndice B.

Las expectativas acerca de los resultados en Seguridad de la Información (InfoSec)

Como se dice por Campeau y Higgins (1995), las expectativas acerca de los resultados han sido consideradas por muchos investigadores de Sistemas de Informacion, por ejemplo, Davis (1989), Thompson (1991) y Robey (1979). Basandonse en las expectativas de los resultados, las personas tienen más posibilidades de tomar conductas que creen que se traducirán en resultados importantes en contraste con las otras conductas que no creen terminaran en resultados favorables. En la seguridad de la información, los usuarios no son realmente capaces de ver los resultados de las consecuencias favorables de ser seguro, sino que ellos ven más rápidamente las consecuencias de no ser seguro cuando un ataque es ya ha sido una realidad en la red. Sobre la base de este enfoque, este estudio postula que no habrá una relación positiva entre la autoeficacia y las expectativas de los resultados de la seguridad de la información, como se muestra en el modelo con un signo negativo. Por lo tanto, sugerimos que:

Proposición 3: Cuanta más alta es la autoeficacia computacional en la seguridad de la información, menores son las expectativas en los resultados de seguridad de la información.

CARACTERÍSTICAS AMBIENTALES

Tras el modelo presentado por Campeau y Higgins (1995), nosostros proponemos evaluar los factores ambientales basados en el estimulo por otros, el uso de los demás y el apoyo de la organización para utilizar las herramientas de seguridad de la información.

Estímulo por otros

Según la teoria social cognitiva, el comportamiento en una situación determinada se ve afectada por el medio ambiente o las características situacionales (Campeau y Higgins, 1995). El fomento de otras personas, que forman parte de las referencias del grupo se puede esperar que puede influir en la autoeficacia y las expectativas de resultado. Por lo tanto, los incentivos de uso de herramientas de seguridad de la información, es representado por la persuasión verbal (por ejemplo, capacitacion) por otras personas de las que un individuo espera obtener orientación sobre las expectativas del comportamiento real que finalmente van a influir en CSI y PSI.

Proposición 4a: Cuanto mas alto es el fomento de las prácticas de seguridad de la información (uso) por miembros de la organización, es mas alto la autoeficacia computacional del individuo en la seguridad de la información.

Proposición 4b: Cuanto mayor sea el fomento de las prácticas de seguridad de la información (uso) de los miembros de la organización, son mas altos los resultados de expectativa del individuo en la seguridad de la información.

El uso actual por otros

"El fomento del empleo es una de las fuentes de influencia en la auto-eficacia y expectativas de resultado" (Campeau y Higgins, 1995). El comportamiento real de los demás con respecto a la utilización de herramientas de seguridad de la información, esta relacionado con el uso de la información y la formación de auto-eficacia y expectativas del resultado. A sabiendas de que otras personas ponen en práctica comportamientos de seguridad de la información como el uso de la contraseña, puede influir positivamente en la practica actual del individuo de utilizar una contraseña. Por lo tanto, sugerimos que,

Proposición 5a bis: Cuanto mayor es el uso de herramientas de sistemas de seguridad por los demás dentro de la organización (del grupo de referencia), la AUE del individuo en la uso de seguridad de la información es mas alta.

Proposición 5b: Cuanto mayor es el uso de herramientas de sistemas de seguridad por los demás dentro de la organización (del grupo de referencia), son mas altas las expectativas de los resultados en Seguridad de la Informacion.

Soporte:

"El apoyo de la organización para las herramientas de seguridad de la informacion se puede esperar que influencie en los individuos y su sentido de autoeficacia" (Campeau y Higgins, 1995). La disponibilidad de la asistencia a personas que provean apoyo para utilizar las herramientas de seguridad de la información, deberían aumentar su capacidad y, por tanto, CSI y PSI. Por lo tanto, proponemos:

Proposición 6 a: Cuanto mayor sea el apoyo y soporte al uso de seguridad de la informacion en la organización, mayor es la autoeficacia computacional en la seguridad de la información.

Proposición 6 b: Cuanto mayor sea el apoyo a la seguridad de la informacion en la organización, mayor son las expectativas del resultado del individuo en la seguridad de la información.

Basándose en el examen preliminar de la teoría y de su implicación en el contexto de seguridad de la información, hemos presentado un total de 6 proposiciones representadas en el modelo de investigación gráfica en la figura1.

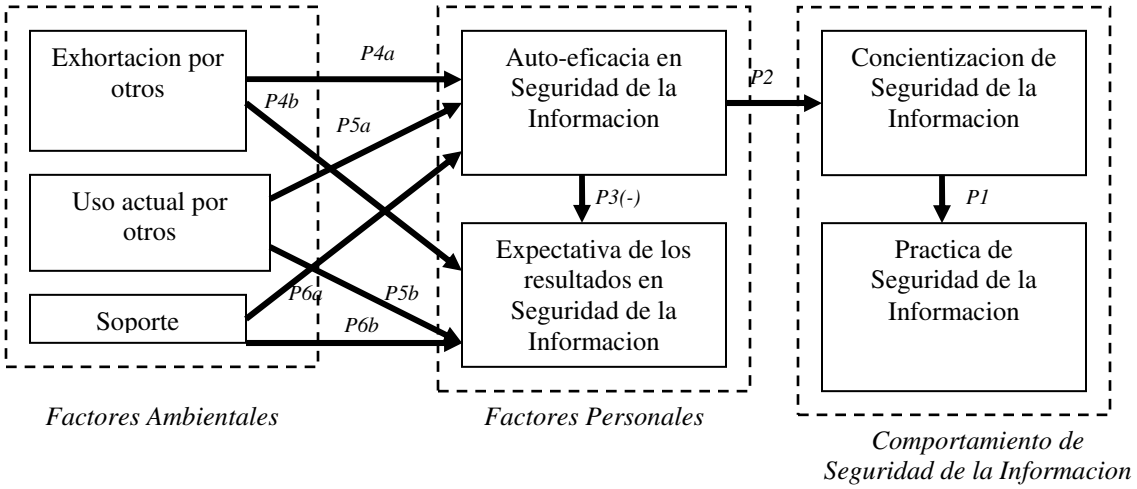

Figura 1. Modelo del Comportamiento de Seguridad de la Información basado en Teoria Social Cognitiva

(Adaptado de Campeau y Higgins, 1995 y Ryan, 2006)

.

CONCLUSIÓN

En este documento se ha hecho una revision de la literatura en el tema de seguridad de la información y la teoría social cognitiva. La principal contribución de este trabajo es la presentación de un modelo que toma la TSC aplicada a la seguridad de la información. En el análisis de la literatura, se provee una definición de CSI y PSI y ademas aquellas variables vinculadas teoreticamente como los factores individuales y ambientales. Ryan (2006) definió las tres variables CSI, PSI y autoeficacia en el contexto de la seguridad de la información, pero no vinculo estas variables utilizando la TSC. Con el modelo propuesto se podria explicar el éxito o fracaso de las prácticas de seguridad impulsadas por las reacciones socio cognitivitas de las personas, los factores ambientales definidos, así como las competencias de cada individuo de mantener, instalar y configurar las herramientas básicas de seguridad en virtud de las políticas de seguridad existentes en una organizacion. Los trabajos de investigacion realizados anteriomente han demostrado que la TSC puede efectivamente predecir el comportamiento de los individuos que podrían ser afectados por los factores ambientales (comportamiento fomentado y soportado por tros) y los factores personales (como autoeficacia computacional). De la misma manera, el modelo propuesto puede generar un mejor entendimiento de estos factores en el ambito de SI que por ultimo, podrían influir en el uso, mayor concientizacion y cumplimiento de las practicas de seguridad de la información dentro de las organizaciones. En este trabajo, el modelo propuesto tiene como objetivo explicar las creencias de los usuarios acerca de su capacidad para utilizar las herramientas computacionales de SI. Este modelo teorico debe ser probado empiricamente tanto en Ingles como en Español.

Agradecimientos

Los autores desean agradecer al Dr. Stephen Fitzgerald su orientación en este proyecto.

REFERENCIAS

Agarwal, R., Sambamurthy, V., & Stair, R. (2000). The Evolving Relationship between General and Specific Computer Self-Efficacy: An Empirical Investigation. Information Systems Research,, 11(4), 418-430.

Arief, B. and D. Besnard (2005). Technical and Human Issues in Computer-Based Systems Security. Centre for Software Reliability, School of Computing Science, University of Newcastle upon Tyne. Retrieved November 28, 2007 from, http://www.dirc.org.uk/publications/techreports/papers/5.pdf

Bandura, A. (1977). Self-efficacy: Toward a unifying theory of behavioral change. Psychological Review, 84, 191-215.

Bandura, A. (1997). Self-efficacy: The exercise of control. New York: W.H. Freeman and Company.

Bandura, A. (2002). Social Cognitive Theory in Cultural Context. Applied Psychology: An International Review, 51(2), 269-290.

Berghel, H. (2007). Better-Than-Nothing Security Practices. Communications of the ACM, 50(8), 15-18.

Cano, J. J. (2004). Inseguridad Informática: Un Concepto Dual En Seguridad Informática. Retrieved from the World Wide Web on 04/25/08 from **http://www.virusprot.com/Art47.html**

Chen, C.C., R S Shaw, and S.C. Yang. (2006). Mitigating Information Security Risks By Increasing User Security Awareness: A Case Study Of An Information Security Awareness System. Information Technology, Learning, and Performance Journal, 24(1), 1-14.

Compeau, D. R. and C. A. Higgins (1995). "Application of social cognitive theory to training for computer skills." Information Systems Research 6(2): 118.

Compeau, D. R. and C. A. Higgins (1995). "Computer self-efficacy: Development of a measure and initial test." MIS Quarterly 19(2): 189.

DarkReading.com (2006). How Much Does a Hack Cost? Retrieved December 1, 2007 from, http://www.darkreading.com/document.asp?doc_id=101631

Dhillon, G. and Backhouse, J. (2001) "Current Direction in IS Security Research: Towards Socio-Organizational Perspectives," Information Systems Journal, 11, 127-153.

Dinev, T., & Hu, Q. (2007). The Centrality of Awareness in the Formation of User Behavioral Intention toward Protective Information Technologies *. Journal of the Association for Information Systems, 8(7), 386.

Goodhue, D.L. and Straub, D.W. 1991. Security concerns of system users: A study of perceptions of the adequacy of security, Information & Management 20, 13-27.

Havelka, D. (2003). "Predicting software self efficacy among business students: A preliminary assessment." Journal of Information Systems Education 14(2): 145.

Hayashi, A., C. Chen, et al. (2004). "The Role of Social Presence and Moderating Role of Computer Self Efficacy in Predicting the Continuance Usage of E-Learning Systems." Journal of Information Systems Education 15(2): 139.

Hu, Q., Hart, P., and Cooke, D. (2006) "The Role of External Influences on Organizational Information Security Practices: An Institutional Perspective," Proceedings of the 39th Hawaii International Conference on Systems Science (HICSS 39), January 4-7, Hawaii, USA. CD-ROM, IEEE Computer Society.

Lee, C.-C., H. K. Cheng, et al. (2007). "An empirical study of mobile commerce in insurance industry: Task-technology fit and individual differences." Decision Support Systems 43(1): 95.

Lindholm, l. (2006). Security Awareness. Retrieved, 2008, from the World Wide Web: http://csrc.nist.gov/organizations/fissea/2006-conference/Lindholm-FISSEA2006.pdf

Marakas, G. M., M. Y. Yi, et al. (1998). "The multilevel and multifaceted character of computer self-efficacy: Toward clarification of the construct and an integrative framework for research." Information Systems Research 9(2): 126.

Marakas, G. M., R. D. Johnson, et al. (2007). "The Evolving Nature of the Computer Self-Efficacy Construct: An Empirical Investigation of Measurement Construction, Validity, Reliability and Stability Over Time." Journal of the Association for Information Systems 8(1): 15.

Reed, K., D. H. Doty, et al. (2005). "The Impact of Aging on Self-efficacy and Computer Skill Acquisition." Journal of Managerial Issues 17(2): 212.

Ryan, James Emory (2006) A comparison of information security trends between formal and informal environments. Ph.D. dissertation, Auburn University, United States -- Alabama. Retrieved October 22, 2007, from ProQuest Digital Dissertations database. (Publication No. AAT 3225287).

Sheng, Y. P., J. M. Pearson, et al. (2003). "Organizational culture and employees' computer self-efficacy: An emperical study." Information Resources Management Journal 16(3): 42.

Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. Information Management & Computer Security, 8(1), 31.

Smith, S. M. (2005). "The Digital Divide: Gender and Racial Differences In Information Technology Education." Information Technology, Learning, and Performance Journal 23(1): 13.

Stanton, J. M., & Stam, K. R. (2006). The Visible Employee: Using Workplace Monitoring and Surveillance to Protect Information Assets - Without Compromising Employee Privacy or Trust. Medford, NJ: Information Today, Inc.

Straub, D. W. and Welke, R. J. 1998. Coping with Systems Risk: Security Planning Models for Management Decision Making. MIS Quarterly, 22, 4, 441-469.

Thatcher, J. B. and P. L. Perrewe (2002). "An empirical examination of individual traits as antecendents to computer anxiety and computer self-efficacy." MIS Quarterly 26(4): 381.

Torkzadeh, G., J. C.-J. Chang, et al. (2006). "A contingency model of computer and Internet self-efficacy." Information & Management 43(4): 541.

Vara, V. (2007). Ten Things Your IT Department Won't Tell You. Wall Street Journal, pp. R1.

Apéndice A: Escala propuesta para la medicion de CSI (Concientizacion de Seguridad de la Información)

(Escala traducida de Ryan, 2006).

Con respecto a la tecnología de la información y su seguridad, soy consciente…

Item de respuesta variable (que se espera relación de sentido)

T, TA A01 Software Antivirus para detectar y eliminar virus conocidos (+)

T, TS A02 Software antivirus requiere actualizaciones frecuentes (+)

T,TA A03 Software Firewall puede bloquear los ataques de red (+)

T, TA A04 Personal Software Firewall puede bloquear puertos lógicos para acceder a / desde un ordenador (+)

FP, TU A05 Políticas de uso aceptable sugieren mantener las contrasenas fuertemente protegidos (+)

FP, TS A06 Política de Protección de virus requiere el uso de software y las actualizaciones disponibles (+)

FP, TE A07 OIT ofrece red privada virtual (VPN) de software para uso fuera de la intranet (+)

FP, TS A08 Politica de Protección de virus requiere la restricción del acceso a los ordenadores con virus (+)

FP, TU A09 Política de Uso Aceptable dicta que redes de acceso con cable e inalámbricas requieren (+)

Un usuario-ID y contraseña

IP, TA A10 otros usuarios indican que los virus informáticos pueden infectar a los mensajes de correo electrónico o archivos adjuntos (+)

C A11 como usuario, mi conocimiento de las amenazas al ordenador desempeña un papel significativo (+)

C, TP A12 actual, recuperacion de datos de back-up es necesario (+)

C, TU A13 contraseña secreta es fundamental (+)

C, TA A14 de la repercusión que puede tener un virus en un sistema informático (+)

C, TA A15 del impacto que el spyware o adware puede tener en un sistema informático (+)

C, TA A16 del impacto de los ataques de redes que pueden tener en un sistema informático (+)

C, TA A17 de la vulnerabilidad compartida con dispositivos como archivos, discos, impresoras o (+)

C, TE A18 encriptacion puede impedir el acceso no autorizado a información sensible (+)

(Es decir, números de tarjetas de crédito, números de seguro social, mensajes de correo electrónico confidenciales

o documentos)

C, TS A19 Software requiere decisiones y actualizaciones periódicas (+)

CSI Ver clave:

Tecnología (T) de amenazas de contexto (C) C: autenticación de usuario (TU)

Política formal (FP) C: Física (TP) C: Control de Acceso (TA)

Política informal (IP) C: Encriptacion (TE) C: Administración de la Seguridad (TS)

Apéndice B: Escala propuesta para la variable PSI (Practicas de seguridad de la información)

(Escala traducida de Ryan, 2006).

El negocio de sistemas informáticos…

Tema de respuesta variable (elemento de disuasión y / o preventivas) (relación de espera)

FP, TU W01 cierro la sesión cuando me salgo del sistema informático (p) (+)

FP, TA W02 apago el ordenador cuando salgo de un sistema informático (p) (+)

FP, TU W03 todas las sesiones electronicas requieren de un unico usuario-ID y contraseña (p) (+)

IP, TP W04 yo hago copia de seguridad de mis datos en dispositivos confiables (discos, CDRW, etc) (p) (+)

IP, TP W05 yo testeo la restauración de mi copia de seguridad que he creado (p) (+)

FP, TS W06 yo compruebo que el software de protección contra virus está activado y actualizado (p) (+)

FP, TA W07 yo siempre dependo del software de la universidad para software de protección de virus y sus actualizaciones (p) (+)

TS, T W08 yo chequeo las nuevas versiones de software de protección de virus (p) (+)

TS, T W09 yo examino el log del software de protección virus por actualizaciones y scaneo de dispositivos (p) (+)

TA, T W10 software personal de firewall supervisa el tráfico en / de mi computadora (s) (p) (+)

TA, IP W11 como navego por la Web, yo permito a los navegadores aceptar cookies de los diferentes sitios Web (p) (-)

TA, T W12 como navego por la Web, yo permito a los navegadores la descarga de software que sea necesario (p) (-)

TU, T W13 yo permito al software que guarde las identificaciones de usuario y contraseñas para que el retorno de las visitas sea mas rapido(p) (-)

TA, T W14 yo me conecto remotamente a los ordenadores y discos compartidos, impresoras, archivos (p) (-)

T, TA W15 yo utilizo software de transferencia de archivos para mover de una manera segura archivos entre computadoras (p) (+)

T, TA W16 yo almaceno el correo electrónico en mi ordenador y no el servidor de correo electronico (p) (-)

IP, TA W17 yo abro mensajes de correo electrónico, independientemente de conocer la identidad del autor (d) (-)

TE, T W18 yo encripto archivos confidenciales con contraseñas (p) (+)

TE, T W19 yo busco por "https: / /" antes de efectuar las transacciones financieras en Internet (p) (+)

TA, chimenea W20 Otras personas comparten la computadora (s) que habitualmente utilizan para el acceso a Internet (d) (-)

TA, T W21 virus afectan el rendimiento de mi equipo (p) (+)

T, TA W22 software de protección de virus identifica y límita el impacto de virus en mi ordenador (p) (+)

TU, FP I W23 yo en forma rutinaria eligo cambiar mi contraseña (s) (d) (+)

TP, FP I W24 yo utilizo una secuencia de caracteres como Ij4Gf4Se% f # como la contraseña de mi computadora (d) (+)

Tecnología (T) de amenazas de contexto (C) C: autenticación de usuario (TU)

Política formal (FP) C: Física (TP) C: Control de Acceso (TA)

Política informal (IP) C: Encriptacion (TE) C: Administración de la Seguridad (TS)

Apendice C: Escala propuesta para la variable AEC (Autoeficacia computacional)

(Adaptada y traducida de Compeau y Higgins, 1995)

En su opinión, usted puede instalar y configurar software de seguridad…

AEC01 … Si no hubiera nadie al lado suyo para indicarle?

AEC02 … Si nunca ha utilizado una aplicacion similar a esta?

AEC03 … Si tuviera sólo los manuales de referencias?

AEC04 … Si hubiera visto a otra persona utilizarlo antes de intentar yo mismo?

AEC05 … Si pudiera llamar a alguien para que me ayude en caso que tenga problemas?

AEC06 … Si alguien me hubiera ayudado a empezar?

AEC07 … Si yo tuviera un montón de tiempo para la realización de las tareas?

AEC08 … Si tuviera la infraestructura que facilite la asistencia?

AEC09 … Si alguien me mostrara la manera de hacer primero?

AEC10 … Si yo hubiera utilizado antes de aplicaciones similares para obtener el mismo objetivo?