RISI 9(1), 09 - 22 (2012)
REVISTA DE INVESTIGACIÓN DE SISTEMAS E INFORMÁTICA
FACULTAD DE INGENIERÍA DE SISTEMAS E INFORMÁTICA
UNIVERRSIDAD NACIONAL MAYOR DE SAN MARCOS
ISSN 1815-0268 (versión impresa)
ISSN 1816-3823 (versión electrónica)

Un modelo de evaluación de factores críticos de éxito en la implementación de la seguridad en sistemas de información respecto a la intención del usuario

A model of assessment of critical success factors in the implementation of safety systems of information concerning the intention of the user

Henry I. Condori A.

Universidad Nacional de Altiplano Puno

E-mail: hcondori@unap.pe

David Mauricio S.

Universidad Nacional Mayor de San Marcos
Facultad de Ingeniería de Sistemas e Informática – FISI

dms_research@yahoo.com

RESUMEN

La seguridad de información normalmente ha sido considerada como un problema tecnológico y a su vez una solución tecnológica, dejando de lado la percepción del usuario, quien es el actor principal en el éxito de las políticas de seguridad [28]. En el caso del Perú, la implementación de normas de seguridad alcanza el 54% del sector público. En este sentido existen varios esfuerzos para determinar los factores de éxito en la implementación de la Seguridad de Sistemas de Información, pero su enfoque no ha estado dirigido desde la perspectiva del usuario. En el presente trabajo se plantea un modelo de evaluación basado en seis factores fuertemente aceptados: compromiso de la gerencia, cultura organizacional, misión de la organización, recursos y presupuesto, formación y capacitación, conciencia de la necesidad de seguridad por el personal; que además incorpora dos factores adicionales: soporte hacia el usuario y experiencia del usuario, y considera la teoría del comportamiento planificado (TPB). El modelo propuesto permite determinar y evaluar los factores críticos de éxito para implementar seguridad de información desde la perspectiva del usuario, con la finalidad de garantizar una implementación exitosa de la seguridad de sistemas de información o efectuar los ajustes necesarios para su éxito, además, para facilitar su implementación, se acompaña una guía metodológica que se ha aplicado en la Universidad Nacional del Altiplano.

Palabras clave: Seguridad de Información, Factores Críticos de éxito, Intención del Usuario, Sistemas de Información.

ABSTRACT

Information security usually has been considered as a technological problem and at the same time a technological solution, aside from the perception of the user, who is the main actor in the success of [33] security policies. In Peru, the implementation of safety standards reached 54% of the public sector. In this sense there are several efforts to determine success factors in the implementation of the security of information systems, but its approach has not been addressed from the perspective of the user. In this study an evaluation model based on six factors strongly accepted arises: commitment of management, organizational culture, Mission of the Organization, resources and budget, training and training, awareness of the need for security personnel; that also includes two additional factors: support towards the user and the user experience, and considers the theory of planned behavior (TPB). The proposed model allows to determine and evaluate the critical success factors for implementing information security from the perspective of the user, in order to ensure a successful implementation of the security of information systems or make necessary adjustments to its success, in addition, to facilitate its implementation, accompanied by a methodological guide that has been applied in the National University of the Altiplano.

Keywords: Information security, critical factors of success, user intent, information systems.

1. INTRODUCCION

EN la actualidad, la información es el bien de mayor valor para las empresas [2].

El progreso de la informática y de las redes de comunicación no sólo ha sido un beneficio para las mismas, debido a que tienen mayores niveles de sistematización, sino que generan un mayor nivel de prevención y responsabilidad frente a las amenazas sobre dicha información. Además, surge la necesidad de evaluar la Seguridad de información para determinar su efectividad y los factores críticos de impacto individual y organizacional que los afectan.

La seguridad de información se ha vuelto crucial en las organizaciones, en tal sentido surge la necesidad de su evaluación para determinar sus beneficios y los factores de más impacto. Como referencia se tiene el reporte de Ponemon Institute [21], sobre costos de las brechas de seguridad en USA, el mismo que indica que la fuga de datos en las empresas sigue siendo uno de

los eventos más costosos para las organizaciones, toda vez que el costo promedio para resolver este tipo de brechas creció de $6.65 millones de dólares a más de $6.75 millones de dólares para 2009", además, durante 2009, por cada archivo perdido o robado, las compañías deben pagar un promedio de $214 dólares, contra los $202 dólares que tenían que desembolsar en 2008.

La seguridad de información, normalmente, ha sido tratada como un problema tecnológico y, a su vez, con una solución tecnológica. Lo cual es inadecuado debido a que la seguridad de información tiene que ver con la gestión del riesgo [28], y la gestión del riesgo se refiere a descubrir y medir las amenazas; para con los objetivos de la información en la organización y tomar acciones contra tales amenazas; gran parte deestas amenazas parten de la conducta del usuario, convirtiéndose en crucial. Al respecto, Tipton & Krause [26] señalan que la Seguridad está basada enlas personas, además manifiestan: "Si se piensa quela tecnología puede resolver los problemas deseguridad, entonces no se entiende los problemas o la tecnología".

Para reducir los riesgos y asegurar protección de la información, las organizaciones a menudo confían en soluciones basadas en tecnología [10]. Aunque estos tipos de soluciones ayudan a mejorar la protección de la información, la confianza exclusiva en dichos medios rara vez es suficiente como para eliminar el riesgo[8] [23]; pues sin el compromiso de los usuarios del sistema cualquier medida de seguridad a implementarse será nula o poco efectiva.

En tal sentido, surge la necesidad de determinar cuáles son los factores que condicionan la intención de usuario para implementar seguridad de información en un contexto organizacional. En el presente trabajo se propone un modelo de evaluación de los factores críticos de éxito para implementar seguridad de información desde la perspectiva del usuario, con la finalidad de garantizar una implementación exitosa o efectuar los ajustes necesarios para su éxito. El modelo propuesto considera seis factores fuertemente aceptados: compromiso de la gerencia, cultura organizacional, misión de la organización, recursos y presupuesto, formación y capacitación, conciencia de la necesidad de seguridad por el perso-

nal; además incorpora dos factores: soporte hacia el usuario y experiencia del usuario, y considera la teoría del comportamiento planificado (TPB).

El artículo se organiza en 5 secciones. En la sección 2 hacemos una revisión del estado del arte sobre los factores críticos de éxito en seguridad de la información. En la sección3, se presenta el modelo propuesto, que considera: factores, dimensiones, la intensión para implementar seguridad en el sistema de información, la construcción del modelo, y la implementación del mismo. Un caso de estudio desarrollado es presentado en la sección 4. Finalmente las conclusiones son presentadas en la sección 5.

2. ESTADO DEL ARTE

De acuerdo a la revisión del estado del arte en cuanto a los factores críticos de éxito, cada autor considera un conjunto de factores dependiendo de las características propias del estudio que ha llevado a cabo, por lo que en primera instancia se realizó la selección de factores tomando en cuenta aquellos que se han referenciado con mayor frecuencia y su similitud en comparativa de los estudios previos referenciados, que consecuentemente se constituyen en los más aceptados en el ámbito científico de la Seguridad en Sistemas de Información. La tabla 1, presenta los factores críticos de éxitos para la implementación de seguridad de sistemas de información.

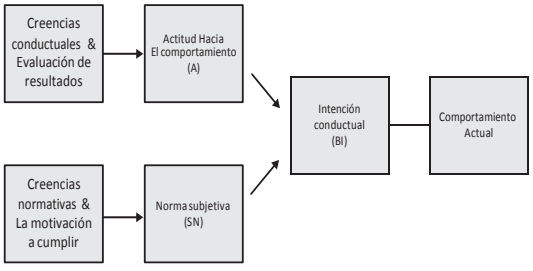
TABLA 1
Factores Críticos de Éxito para la Implementación de Seguridad de Sistemas de Información

Factores	Autores
Compromiso de la gerencia	Abu-Zineh[1], ISO/IEC 27002[15], ISO/IEC 17799[14], INDECOPI[13], Al-Awadi & Renaud[5], Bjorck[6], Partida & Ezingeard Henley[20], Kankanhalli, Hock-hai, Bernard, & Kwok-kee[16].
Cultura organizacional	Nosworthy[18], ISO/IEC 27002[15], ISO/IEC 17799[14], INDECOPI[13], Partida & Ezingeard Henley[20].
Misión de la organización	Al-Awadi & Renaud[5], Abu-Zineh[1], ISO/IEC 27002[15], ISO/IEC 17799[14], INDECOPI[13], Partida & Ezingeard Henley[20], Siponen[22].
Recursos y presupuesto	ISO/IEC 27002[15], ISO/IEC 17799[14], INDECOPI[13], Al-Awadi & Renaud[5], Bjorck[6].
Formación y capacitación	Abu-Zineh[1], ISO/IEC 27002[15], ISO/IEC 17799[14], INDECOPI[13], Nosworthy[18], Al-Awadi & Renaud[5], Bjorck[6].
Conciencia de la necesidad de seguridad por el personal	Abu-Zineh[1], ISO/IEC 27002[15], ISO/IEC 17799[14], INDECOPI[13], Nosworthy[18], Al-Awadi & Renaud[5], Bjorck[6], Partida & Ezingeard Henley[20].

2.1 Teoría de la Acción Razonada (TRA)

La Teoría de la Acción Razonada (Theory of Reasoned Action) es un modelo de la Psicología Social desarrollado por Martin Fishbein y Icek Ajzen [4], para la predicción y comprensión de la conducta humana. A diferencia de otras teorías, no se centra en los valores y la personalidad, sino que propone que la conducta de una persona está condicionada por su intención de llevarla a cabo (si desea o no hacerlo). Esta intención es función de dos factores: su actitud (de naturaleza personal) y sus normas subjetivas (de naturaleza social). La actitud está determinada por sus creencias sobre las consecuencias de esta conducta, mediatizadas por su evaluación de dichas consecuencias. Las creencias se definen por la probabilidad subjetiva de que la realización de una conducta particular producirá resultados concretos.

Fig. 1. Modelo de la Teoría de la Acción Razonada basado en Fishbein & Ajzen [11].



2.3 Teoría del Comportamiento Planificado (TPB)

La Teoría del Comportamiento Planificado (Theory of Planned Behavior) es una extensión de la Teoría de la Acción Razonada propuesta por Icek Ajzen [3]. Considera los mismos factores que la Teoría de la Acción Razonada, pero añadiendo la variable denominada control conductual percibido, que representa la percepción de la facilidad o dificultad de realizar una conducta específica (si va a ser capaz o no, si será fácil o difícil) y que recoge tanto la experiencia como la previsión de dificultades. Por lo tanto, la Teoría del Comportamiento Planificado considera la intención en función de tres factores: las creencias sobre las consecuencias probables de la conducta (actitud), las creencias sobre las expectativas normativas de otros (normas subjetivas) y las creencias sobre la presencia de factores que pueden facilitar u obstaculizar el comportamiento. Ajzen introduce el grado con que un individuo cree controlar su vida y cuán previsibles son los acontecimientos que influyen en ella.

3. PROPUESTA DEL MODELO

3.1 Factores

Como parte del proceso de definición de factores, se ha tomado la referencia a los estudios expuestos en la Tabla 1, para ser adaptados al presente modelo:

a. Compromiso de la Gerencia. Villegas señala que se han realizado muchos estudios, siendo el apoyo de los directivos uno de los factores más importantes en el éxito de los SI, debido a su gran poder de tomar decisiones, pudiéndose resumir las razones de mayor importancia de los directivos en que proporcionan los recursos humanos y materiales al desarrollo de SI; son promotores del cambio con la implantación de un sistema y proporcionan el tiempo necesario al personal involucrado [27].

Uno de los puntos más importantes, para todas las partes interesadas en una protección de la información, es obtener suficiente soporte de la alta gerencia. Si la alta gerencia de las organizaciones entiende la importancia de proteger los activos de información, entonces apoyarán los planes de seguridad con recursos financieros y técnicos; las organizaciones con menos soporte de alta dirección son propensas a invertir menos en Seguridad de Información. Esto conduciría a las organizaciones hacia problemas serios de protección de la información, siendo necesario incrementar el interés en la Seguridad [16].

b. Cultura Organizacional. La cultura organizacional es un área estudiada por diversos investigadores y se encuentra vinculada con la interacción de valores, actitudes y conductas compartidas por todos los miembros de una empresa u organización [27].

El enfoque de seguridad a implementar debe ser consistente con la cultura organizacional [18][15][14][13][20]. En este punto es necesario resaltar el elemento político, pues a nivel estatal gran parte de las decisiones son apoyadas o desvirtuadas en función a la politización en relación a determinado proyecto.

c. Misión de la Organización. Los objetivos y metas claras de la organización son esenciales para implementar políticas de protección de la información, y que teniendo una cultura de información segura en la organización incidirá en su éxito [5]. Si la misión de la organización no está direccionada, la organización continuará luchando para asegurar su información y los empleados no se responsabilizarán seriamente y no seguirán ni respetarán las líneas directivas en la política de protección de la información.

Sin tener los objetivos y metas claras, antes de implementar seguridad será difícil cumplir con una política de seguridad, objetivos y actividades que reflejen los objetivos del negocio de la organización [5][22].

d. Recursos y presupuesto. Sin un presupuesto apropiado, las organizaciones no estarán dotadas con suficientes recursos para garantizar la adecuada protección de la información.

Bjorck indica que el presupuesto, como la facilidad financiera, en primer lugar, racionalmente estima los costos y, en segundo lugar, evalúa el acceso requerido a los recursos para lograr la implementación exitosa de protección de la información[6]. Las organizaciones requieren el financiamiento adecuado para lograr protección de la información de forma efectiva.

La falta de presupuesto asignado a la seguridad de información da paso a la inversión insuficiente en controles apropiados.

Para el modelo propuesto, se define este constructor como los recursos percibidos, es decir, el grado en el cual un individuo cree tener lo necesario, esto en función a proyectos anteriores (no necesariamente de seguridad, pero sí en el ámbito de sistemas de información). Los que pueden ser habilidades, hardware, software, dinero, documentación, datos, materiales, tiempo y asistencia de personal de sistemas.

e. Formación y Capacitación. Las organizaciones deben tener una constante de educación y programas de entrenamiento para lograr el resultado requerido de la implementación de una política de protección de la información.

El sentido común indica que hay una necesidad para poner esfuerzo en entrenar y educar a los empleados, porque son quienes van a necesitar acceder a los sistemas de información empleando mecanismos de protección de la información y normas [5].

Los empleados que son deficientemente entrenados en términos de la seguridad o con escaso conocimiento de operación de equipos de cómputo y sistemas de información permitirán vulnerabilidades, por consiguiente, los errores de esos usuarios surgirán sin que ellos se percaten.

f. Conciencia de la Necesidad de Seguridad por el personal. McKay, referenciando en el informe de índice de conciencia en seguridad a nivel mundial, concluyó que las organizaciones alrededor del mundo no pueden concientizar a sus empleados en los asuntos de seguridad y las consecuencias. Sin embargo, no hay prueba en la literatura que los programas de conciencia juegan un papel decisivo en disminuir conductas inseguras; o que haga una diferencia en asegurar la protección de la información y de esta forma fomentar el cumplimiento creciente de las políticas de protección de la información [17].

Las fallas del personal pueden debilitar aun las medidas más fuertes de seguridad. Por ejemplo, las prácticas comunes de dejar encendida la computadora en los recesos, apuntar contraseñas en notas adhesivas en el monitor de la computadora, o revelar información confidencial a personas desautorizadas.

Como la persona es una amenaza continua y una perturbación para mantener un ambiente seguro de información, pues la tecnología es una herramienta de que puede ser usada apropiadamente o indebidamente[5], se requieren programas de concientización y entrenamiento para que la implementación de seguridad de información sea exitosa.

Más allá de los indicadores ampliamente aceptados, y considerando los vacíos en cuanto a brindar una mayor importancia a la percepción del usuario, se plantean dos nuevos factores:

g. Soporte hacia el usuario. Se conceptualiza como el grupo específico que está disponible para la asistencia hacia el usuario que tiene dificultades en la interacción con el sistema de información, tanto en hardware, software y redes [12]. Es necesario tener presente que, si el usuario ha percibido un mal servicio de soporte, esto afectará su futura intención de que la Seguridad de los Sistemas de Información sea implementada.

h. Experiencia del usuario. Taylor & Todd encontraron las diferencias significativas en la intención para usar tecnología entre usuarios experimentados e inexpertos [24]. Thompson, Higgins & Howell se encontraron con que la experiencia tuvo una influencia positiva significativa en el uso [25]. Es necesario aclarar que el factor experiencia no ha sido empleado para estudios específicos en la implementación de seguridad de información.

3.2 Dimensiones

Se ha considerado las dimensiones de la teoría del comportamiento planificado: actitud, norma subjetiva, y control conductual percibido. Y que ha continuación adaptamos para la implementación de la seguridad en sistemas de información.

a. Actitud para Implementar Seguridad en Sistemas de Información. Se considera así al discernimiento personal que diferencia el comportamiento bueno o malo y está en función de creencias[4]. Para el presente estudio, se traduce en la actitud que muestra el usuario en cuanto a la futura implementación de Seguridad en Sistemas de Información, pues ciertamente, por más políticas, hardware, software de seguridad que se implemente, si no existe la actitud positiva y proactiva del usuario, poco será el impacto del plan de seguridad implementado, o bien sus medidas serán poco efectivas en el tiempo, pues no serán sostenibles.

b. Norma Subjetiva. En el modelo TBP, es considerado como un determinado comportamiento que se define como la valoración particular de cada usuario realiza, en función a las personas que cree que son importantes para él, pues influyen en su percepción[4]; por lo que dicha percepción está condicionada a su comportamiento.

Para el presente estudio, se trata de evaluar que tan determinante es la motivación y creencias normativas para que exista la intención de Implementar Seguridad en Sistemas de Información. Por ejemplo, si para determinado usuario, el compañero de trabajo, a quien el primero considera como el más experto, y éste último está convencido de la necesidad de implementar seguridad en los sistemas de información, el primero acoge el criterio del segundo, manifestando intención favorable y positiva respecto a implementar seguridad, pues subjetivamente el segundo ha sido un referente para el primero.

c. Control conductual percibido. El Control conductual percibido es un postulado para tener una relación positiva entre la intención y el comportamiento real. Según Ajzen, tiene relación para qué tan fácil o difícil debería llevar un cierto comportamiento, pues denota un grado subjetivo de control sobre el desempeño de un comportamiento en vez de la probabilidad percibida en la que un comportamiento repercutirá en un determinado resultado. Para el presente caso se traduce en la creencia de control que tiene el usuario en cuanto a

su autodesempeño con la implementación del plan de seguridad, el soporte que puede recibir y los recursos que dispone. Por ejemplo, si con base a las experiencias anteriores con sistemas de información ha recibido un soporte deficiente o los sistemas no cubren sus expectativas, y por lo tanto cree que su adaptación será difícil, concluirá que volverá a ser así, por lo que será reticente a la implementación un plan de seguridad en los sistemas de información con que interactúa.

3.3 La Intención para Implementar Seguridad en S.I.

La intención conductista es un antecedente para el comportamiento real [3]. Indica el propósito de hacer algo y se considera un buen pronosticador del comportamiento real. Lo cual podría ser afectado por actitudes, la norma subjetiva y el control conductual percibido.

En el presente estudio se trata de evaluar justamente qué factores condicionan la intencionalidad y consecuentemente el futuro comportamiento real para que la implementación de Seguridad en Sistemas de Información sea exitosa desde la perspectiva del usuario.

3.4 Construcción del Modelo

Considerando:

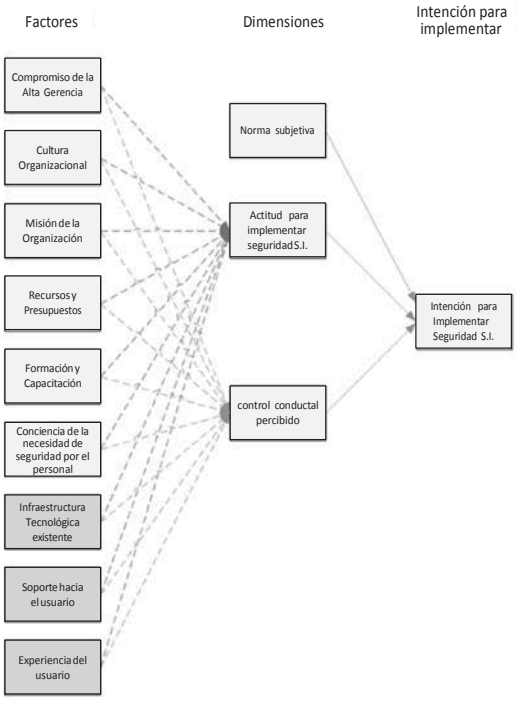
- La Teoría de la Acción Razonada y la Teoría de Comportamiento Planificado proveen la base para un análisis de la relación entre la actitud, intención y comportamiento. Ambas teorías han sido usadas ampliamente en la literatura de TI, incluyendo en el contexto de cumplimiento de políticas de seguridad [19].
- Del estudio de TAM y TAM2, se determina que la intención de uso es el factor determinante para la implementación de una nueva tecnología, y que a su vez dicho modelo está basado en La Teoría de la Acción Razonada, que es un modelo de la Psicología Social desarrollado por Martin Fishbein y Icek Ajzen [4]; y que a su vez se orientan a evaluar el éxito de la seguridad de información una vez implementado y no antes de su implementación, como ocurre con el modelo propuesto.
- Ajzen[3] critica su modelo original de la Teoría de la Acción Razonada (1980), indicando que carece de una dimensión, agregando el control conductual percibido en su nueva propuesta Teoría del Comportamiento Planificado (1991), y que viene siendo empleada ampliamente en investigaciones en cuanto a seguridad de información [19][8][7].

Se propone un modelo que considera 8 factores debidamente sustentados en la literatura (ver sección 3.1), el uso de la Teoría del Comportamiento Planificado de Ajzen que se compone de tres dimensiones: actitud, norma subjetiva y control conductual percibido (ver sección 3.2) y finalmente su relación con la intención conductual para implementar seguridad de sistemas de información.

El modelo propuesto (ver Figura 3) trata de una evaluación previa a la implementación, que se sustenta en que los estudios de intencionalidad conductual que conducen a determinado comportamiento actual o futuro[3] se puede observar desde dos perspectivas temporales: pre-implementación y post-implementación [9].

Las flechas señalan relaciones fuertemente aceptadas [3] y las flechas entre líneas señalan son las relaciones propuestas.

Fig. 3. Modelo propuesto de Evaluación de los Factores Críticos para la Implementación de Seguridad en Sistemas de Información en la intención del Usuario.



Considerando la justificación de cada constructor en el modelo, se incorporan las hipótesis que se resumen en la Tabla 2, en conformidad con el mapa del modelo de evaluación propuesto en la Figura 3.

TABLA 2
Hipótesis del Modelo de Evaluación de los Factores Críticos para la Implementación de Seguridad en Sistemas de Información en la intención del Usuario.

Código	Descripción
H1	El compromiso de la alta gerencia influye en la Actitud para implementar Seguridad en Sistemas de Información.
H2	El compromiso de la alta gerencia influye en el control conductual percibido.
H3	La Cultura Organizacional influye en la Actitud para implementar Seguridad en Sistemas de Información.
H4	La Cultura Organizacional influye en el control conductual percibido.
H5	La Misión de la Organización influye en la Actitud para implementar Seguridad en Sistemas de Información.
H6	La Misión de la Organización influye en el control conductual percibido.
H7	Los Recursos y Presupuesto están relacionados con la Actitud para implementar Seguridad en Sistemas de Información.
H8	Los Recursos y Presupuesto están relacionados con el control conductual percibido.
H9	La Formación y Capacitación influye en la Actitud para implementar Seguridad en Sistemas de Información.
H10	La Formación y Capacitación influye en el control conductual percibido.
H11	La Conciencia de la necesidad de seguridad por el personal influye en la Actitud para implementar Seguridad en Sistemas de Información.
H12	La Conciencia de la necesidad de seguridad por el personal influye en el control conductual percibido.
H13	El Soporte hacia el usuario influye en la Actitud para implementar Seguridad en Sistemas de Información.
H14	El Soporte hacia el usuario influye en el control conductual percibido.
H15	La Experiencia del usuario influye en la Actitud para implementar Seguridad en Sistemas de Información.
H16	La Experiencia del usuario influye en el control conductual percibido.
H17	La Actitud para implementar Seguridad en Sistemas de Información influye en la Intención para Implementar Seguridad en Sistemas de Información.
H18	El control conductual percibido influye en la Intención para Implementar Seguridad en Sistemas de Información.
H19	La Norma subjetiva influye en la Intención para Implementar Seguridad en Sistemas de Información.

3.4 Implementación del Modelo Propuesto

Para la adecuada implementación del modelo se ha acogido y adaptado la guía metodológica propuesta por Villegas [27].

La Guía Metodológica (Figura 4) inicia con la selección del proceso de negocio y el Sistema de Información donde se desea evaluar y su descripción, así como la conformación de un equipo de trabajo multidisciplinario (pasos 4 al 8). Luego, se debe seleccionar las preguntas pertinentes para cada variable y ajustarlas de acuerdo al contexto organizacional, entendiendo la realidad propia de cada entidad (pasos 9 y 10).

Los pasos 12 al 15 especifican la forma de establecer el diseño, la validación evaluación y consistencia de los instrumentos en relación a las variables y sus relación y el modelo en forma global.

El paso 15 resume el proceso de validar las relaciones de los factores, las dimensiones y la intención, traducida en hipótesis probadas estadísticamente.

Finalmente, se plasma las conclusiones de los resultados del estudio, aspecto que servirá de base para controlar los factores de influencia.

4 CASO DE ESTUDIO: UNA-PUNO

4.1 Selección del Sistema

Se planteó el desarrollo del caso Universidad Nacional del Altiplano (UNA-Puno), institución pública de carácter estatal, ubicada en el departamento de Puno, provincia de Puno, distrito de Puno. En cuanto a la población académica y administrativa, se conforma de 15,344 estudiantes, 1,009 docentes y 681 administrativos, al finalizar el año 2010.

Por lo que, para el desarrollo más eficiente de las funciones de gestión administrativa, se ha desarrollado un sistema de información integral que involucra las funciones administrativas de gestión por medio del cual interactúan las diversas dependencias de la UNA-Puno, desde los procesos de planeación y presupuesto hasta la ejecución, así como el control respectivo; con el fin de soportar las actividades académicas.

4.2 Descripción del Sistema

El sistema Integral Administrativo de la UNA-Puno considera los siguientes procesos críticos de apoyo

implementados y que son utilizados por las diversas dependencias:

- Planificación y control presupuestal.
- Control Presupuestal.
- Adquisición de Bienes y servicios (Abastecimientos, Almacenes).
- Gestión de Tesorería y Caja.
- Gestión de Contaduría.
- Gestión de Recursos Humanos.
- Gestión de servicios.
- Gestión y monitoreo de obras y proyectos.
- Gestión de matrículas y pagos.
- Gestión de trámites académicos.
- Control de bienes patrimoniales.

En tal sentido, dicho sistema de Información integral se constituye en una herramienta estratégica para el logro de objetivos instituciones, y así garantizar el funcionamiento de los procesos críticos.

4.3 Conformación del Equipo de Trabajo

El equipo estaba conformado por:

- Un investigador principal.
- Un personal de apoyo para el procesamiento estadístico.

4.4 Selección de Factores Críticos de Éxito, Dimensiones y la Intención para Implementar Seguridad en S.I.

Se seleccionó los siguientes factores críticos de éxito:

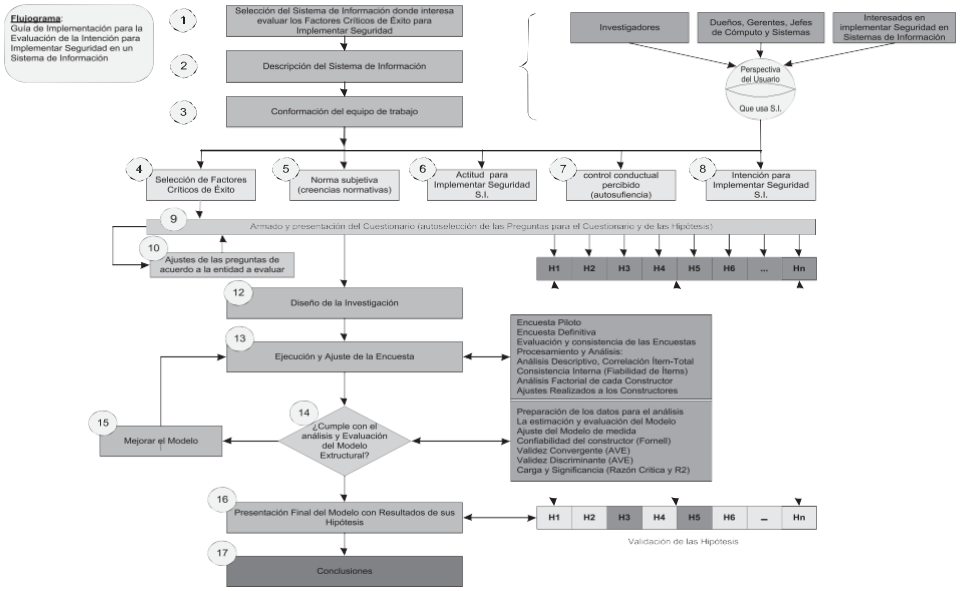
a) Compromiso de la Gerencia (CG).
b) Cultura Organizacional (CO).
c) Misión de la Organización (MO).
d) Recursos y Presupuesto (RP).
e) Formación y Capacitación (FC).
f) Conciencia de la Necesidad de Seguridad por el personal (CNS).
g) Infraestructura Tecnológica (IT).
h) Soporte hacia el usuario (SHU).
i) Experiencia del usuario (EU).

En conformidad con la Guía Metodológica, se seleccionó las tres dimensiones de éxito propuestos:

j) Actitud para Implementar Seguridad en Sistemas de Información (AIS).
k) Norma Subjetiva (NS).
l) Control conductual percibido (CCP)
m) Intención para implementar seguridad en los sistemas de información (ISS).

Además de considerar el constructo principal del modelo: la Intención para Implementar Seguridad en los Sistemas de Información.

Fig. 4. Flujo grama para la implementación de la Guía Metodológica del Modelo



4.5 Armado y presentación final del cuestionario y Ajuste de las Preguntas

Conforme a la propuesta del modelo, se plantea la totalidad de las 19 hipótesis, conforme a la Figura 3 y la Tabla 2.En cuanto al ajuste de las preguntas, el detalle del cuestionario propuesto se encuentra en el diseño de la investigación.

4.6 Diseño de la Investigación

La presente investigación es cuantitativa; en vista que se usa la recolección de datos para probar hipótesis con base en la medición numérica y el análisis estadístico que permita establecer patrones de comportamiento en el presente caso de estudio.

El caso estudio es una investigación con un diseño no experimental de tipo transversal; pues se trata de un estudio donde el objetivo es conocer la percepción de los usuarios de los sistemas en Universidad Nacional del Altiplano, sin realizar algún tipo de manipulación intencional, sino conocer su comportamiento y percepción de forma natural, sin involucrar ningún efecto exterior; así mismo, es transversal, porque la recolección de los datos se ha desarrollado en un periodo determinado que corresponde a noviembre del 2011.

Se optó por la selección de una muestra probabilística para el caso estudio, ya que se contaba con una población total objetivo de 143 usuarios en las diferentes dependencias de la UNA-Puno que usan el sistema.En vista que se conoce la población, con un nivel de confianza del 95%, una variabilidad positiva de 0,05 y un porcentaje de error del 5%, se determina 84 usuarios, como la cantidad mínima representativa.

4.7 Ejecución y ajuste de la encuesta

4.7.1 Encuesta Piloto

Dado el modelo propuesto, se ha desarrollado una encuesta piloto para determinar algunos indicadores estadísticos, así como observar la aplicación de la encuesta en el trabajo de campo y poder incorporar algunos ajustes para la encuesta final. Se obtuvo en total 31 encuestas como tamaño de la encuesta piloto.

Un problema resaltante ha sido en preguntas como:

"¿Existen factores políticos internos que afectan a usted como usuario y al desarrollo de un proyecto de Sistemas?".

Que han generado una respuesta incoherente o dejada en blanco, en vista que buscaba mediante un criterio mandatorio la calificación del usuario, y éste sentía comprometer su afirmación con posibles repercusiones futuras, a pesar que la encuesta era anónima, como tal, entendiendo que en el caso de instituciones públicas existe un alto grado politización, algunas preguntas podrían afectar dichos "supuestos intereses", por lo tanto, se hace necesario evaluarlos y adecuarlos a cada contexto. En el presente caso, se reformuló la pregunta de la siguiente manera:

"¿Considera que Existen factores políticos internos que afectan a usted en su trabajo y a la implementación de proyectos de Sistemas?"

De las 70 preguntas planteadas, se ha obtenido 66 preguntas fiables (Alfa de Cronbach superior a 0.7).

4.7.2 Encuesta Definitiva

El cuestionario final está integrado por siete (07) preguntas de control, así como 66 preguntas que han sido divididos en 13 factores. Se realizaron 139 encuestas, rechazaron para el estudio a 11, quedando como encuestas válidas a 128 (tamaño que garantiza un nivel de confianza del 95%, dado que es superior a la muestra mínima requerida).

4.7.3 Análisis descriptivo

A partir de las tabulaciones de las preguntas de control, se efectuó el análisis descriptivo de las 7 variables de control incluidas en el estudio, obteniéndose los siguientes resultados:

- El 48.4% fueron de sexo masculino y 51,6% de sexo femenino. Siendo la proporción de personal de sexo masculino con femenino proporcional.
- Rango de edad: la edad del personal de fluctúa entre los 40 a 49 años, con 45,3%, seguido de las de 50 a 59 años de edad con 42,2%, de 20 a 29 años con 9.4%, y por último, personas entre 30 a 39 años con 3,1%. Por lo tanto el perfil que se presenta se inclina más al personal adulto en la operación de los sistemas de información.
- Nivel máximo de estudios: 54,7% cuenta con un nivel de estudios superior con universitaria completa, 28.1% con estudios de postgrado, 9.4% superior incompleta y 7.8% superior no universitaria completa. Observándose una mayor cantidad de personal profesional que opera los sistemas de información.

- Tiempos de trabajar en la institución: 71.9% de los encuestados indicó trabajar 11 a más años, 10.9% de 6 a 10 años, 9.4% menor a un año, 4.7% de 1 a 2 años y, finalmente, 3.1% de 3 a 5 años. Se observa una mayor cantidad de personal estable, por el tiempo que labora en la institución, siendo la rotación baja.
- Conocimiento de Informática y computación: el 43.8% indica conocimientos regulares, 28.1% conocimiento avanzado, 23.4% conocimiento básico, 3.1% conocimiento muy básico y, finalmente, 1.6% conocimiento experto. Lo que muestra que existe una mayor cantidad de personal que tiene conocimientos regulares a avanzados.
- Años que se utiliza sistemas de información administrativa: un 40.6% manifiesta que 11 a más años, 23.4% de 3 a 5 años, 20.3% de 6 a 10 años, 10.9% de 1 a 2 años y, finalmente, 4.7% menor a un año. Lo que muestra buen tiempo de experiencia del personal trabajando con sistemas de información.
- Horas aproximadas a la semana que usa el sistema: 29.7% usa el Sistema de Información de 0 a 10 horas, 26.6% de 46 horas a más, 20.3% de 31 a 40 horas, 14.1% de 11 a 20 horas y, finalmente, 9.4% de 21 a 30 horas.

4.7.4 nsistencia Interna

Se ha desarrollado a través de la correlación ítem-total y el Alfa de Crombach, resultando 64 preguntas (ítems) aceptables de las 66 (Tabla 3).

TABLA 3
Estadísticos de fiabilidad por factor para el caso estudio UNA-Puno

FACTORES	Abrev.	Casos			Estadísticos de fiabilidad	
		Válidos	Excluidos(as)	Total	N de ítems	Alfa de Cronbach
FACTOR 1	CAG	128	0	128	5	0.874
FACTOR 2	CO	128	0	128	7	0.770
FACTOR 3	MO	128	0	128	6	0.778
FACTOR 4	RP	128	0	128	7	0.828
FACTOR 5	FC	128	0	128	5	0.874
FACTOR 6	CNS	128	0	128	7	0.874
FACTOR 7	IT	128	0	128	3	0.786
FACTOR 8	SHU	128	0	128	4	0.864
FACTOR 9	EU	128	0	128	5	0.742
FACTOR 10	AIS	128	0	128	4	0.904
FACTOR 11	CCP	128	0	128	3	0.931
FACTOR 12	NS	128	0	128	4	0.805
FACTOR 13	ISS	128	0	128	4	0.959
TOTAL		128	0	128	64	

4.7.5 Análisis factorial de cada constructor

A partir de los resultados iníciales, se ha reajustado los factores o constructores de acuerdo al número de ítems o preguntas que se integren más a cada uno de ellos, y que permita una mejor evaluación para el desarrollo del análisis estructural. Del proceso realizado se ha obtenido finalmente 57 ítems (preguntas), que han sido ajustadas a cada constructor.

Así mismo, el análisis factorial a esta nueva formación de constructores nos ha demostrado que su formación con dichos ítems ha mejorado, ya que todos forman un solo grupo con una representación de la varianza mayor a 50%.

Pero es necesario mencionar que el factor 12 presenta un KMO cercano al mínimo de 0,7, por lo que es considerado, no pudiendo mejorar más (Tabla 4).

TABLA 4
Constructores ajustados por cada factor para el caso estudio UNA-Puno

FACTORES	Abrev.	ítems	Alfa de Cronbach	Indicadores de Aplicación		Resultados	
				determ.	KMO>0,7	Fact.	Varianza Explicada %
FACTOR 1	CAG	5	0.874	0.074	0.816	1	66.668
FACTOR 2	CO	5	0.745	0.310	0.749	1	50.156
FACTOR 3	MO	5	0.779	0.165	0.704	1	54.536
FACTOR 4	RP	5	0.842	0.176	0.736	1	68.195
FACTOR 5	FC	5	0.874	0.074	0.846	1	67.078
FACTOR 6	CNS	6	0.875	0.032	0.828	1	62.404
FACTOR 7	IT	3	0.786	0.410	0.692	1	70.239
FACTOR 8	SHU	4	0.864	0.105	0.730	1	71.223
FACTOR 9	EU	4	0.789	0.262	0.717	1	61.653
FACTOR 10	AIS	4	0.904	0.057	0.817	1	78.023
FACTOR 11	CCP	3	0.931	0.085	0.761	1	87.863
FACTOR 12	NS	4	0.805	0.183	0.697	1	63.727
FACTOR 13	ISS	4	0.959	0.009	0.871	1	89.062
	TOTAL	57					

4.7.6 Análisis y evaluación del modelo estructural

El tamaño de muestra se encuentra dentro de lo permitido (128), así mismo, se ha utilizado el método del bootstrap, generándose 500 muestras representativas; además, se ha utilizado los programas SPSS y AMOS versión 19.0.

La Tabla 5 muestra que la confiabilidad interna de los constructores está dada en un rango (desde 0,828 al 0,970), superando los requerimientos mínimos de

0,707. Para los indicadores reflectivos, AVE, todos cumplen con valores superiores a 0.5; sólo el factor 2 no cumple con un valor de AVE de 0,50 (es el valor 0,493 del factor cultura organizacional), que se encuentra bastante cercano al mínimo.

TABLA 5
Confiabilidad y validez convergente de los coeficientes Caso UNA-Puno

FACTORES	Abrev.	ítems	Confiabilidad Interna >0.707	Alfa de Cronbach	AVE >0.5	R2
FACTOR 1	CAG	5	0.874	0.874	0.586	no aplica
FACTOR 2	CO	5	0.828	0.746	0.493	no aplica
FACTOR 3	MO	5	0.852	0.783	0.542	no aplica
FACTOR 4	RP	5	0.883	0.836	0.604	no aplica
FACTOR 5	FC	5	0.908	0.876	0.666	no aplica
FACTOR 6	CNS	6	0.907	0.877	0.622	no aplica
FACTOR 7	IT	3	0.864	0.788	0.681	no aplica
FACTOR 8	SHU	4	0.902	0.865	0.699	no aplica
FACTOR 9	EU	4	0.863	0.789	0.613	no aplica
FACTOR 10	AIS	4	0.934	0.905	0.780	0.779
FACTOR 11	CCP	3	0.956	0.931	0.879	0.481
FACTOR 12	NS	4	0.873	0.804	0.636	no aplica
FACTOR 13	ISS	4	0.970	0.959	0.891	0.608
	TOTAL	54				

4.8 Análisis de los Resultados

4.8.1 Análisis de los Factores Críticos de Éxito con las dimensiones

La Cultura Organizacional (0.439), los Recursos y Presupuesto (-0.558) y la Conciencia de la necesidad de seguridad por el personal (0.431) contribuyen a la dimensión de Actitud para Implementar Seguridad en Sistemas de Información. Estos factores tienen coeficientes path significativos de 0.439, -0.558, 0.431, respectivamente, que en conjunto explican el 77.9% de la varianza de este factor. El atributo con mayor importancia, por su path y nivel de significancia, es Recursos y Presupuesto.

El compromiso de la alta gerencia (-0.212), la Misión de la Organización (0.268), la Formación y Capacitación (0.357), la Conciencia de la necesidad de seguridad por el personal (0.325) y la Experiencia del usuario (0.304) contribuyen a la dimensión del control conductual percibido. Estos factores tienen coeficientes path significativos de -0.212, 0.268, 0.357, 0.325, 0.304, respectivamente, que en conjunto explican el 48.1% de la varianza de este factor. El factor con mayor importancia, por su path y nivel de significancia, es la Formación y Capacitación.

TABLA 6
Resumen de los parámetros estimados y su razón crítica Caso UNA-Puno

Pesos de la regresion	Estimación del coeficiente PATH no estandarizado	Errores tipicos (S.E.)	Razón crítica (C.R.) +/- 1,96	Estimación del coeficiente PATH estandarizado R2 > 0,2	Clasificación
AIS <— CAG	-0.081	0.074	-1.083	-0.063	No aceptada
CCP <— CAG	-0.230	0.085	-2.726	-0.212	Aceptada
AIS <— SHU	0.160	0.056	2.852	0.166	No aceptada
CCP <— SHU	-0.040	0.061	-0.648	-0.048	No aceptada
AIS <— CO	0.837	0.199	4.200	0.439	Aceptada
CCP <— CO	0.220	0.135	1.635	0.135	No aceptada
AIS <— MO	-0.095	0.067	-1.426	-0.081	No aceptada
CCP <— MO	0.270	0.077	3.511	0.268	Aceptada
AIS <— RP	-0.744	0.101	-7.340	-0.558	Aceptada
CCP <— RP	-0.126	0.087	-1.458	-0.111	No aceptada
AIS <— FC	0.175	0.078	2.239	0.131	No aceptada
CCP <— FC	0.405	0.091	4.432	0.357	Aceptada
AIS <— CNS	0.672	0.119	5.666	0.431	Aceptada
CCP <— CNS	0.432	0.111	3.899	0.325	Aceptada
CCP <— EU	0.405	0.113	3.583	0.304	Aceptada
AIS <— EU	0.201	0.096	2.095	0.129	No aceptada
▮S <— AIS	0.379	0.058	6.545	0.463	Aceptada
▮S <— CCP	0.444	0.069	6.397	0.463	Aceptada
▮S <— NS	0.284	0.109	2.595	0.181	No aceptada

4.8.2 Análisis de las dimensiones relacionado con la intención de implementar seguridad por parte del usuario

La Actitud para implementar Seguridad en Sistemas de Información (0.463) y el control conductual percibido (0.463) tienen un impacto significante, por sus coeficientes path 0.463, 0.463, en la Intención para Implementar Seguridad en Sistemas de Información y explican el 60.8% de la varianza del factor principal.

La dimensión Norma subjetiva no tiene significancia en el presente caso, pues tanto el R2 y su coeficiente path son bajos, a pesar de ser un elemento ampliamente probado de la teoría del comportamiento planificado propuesto por Ajzen.

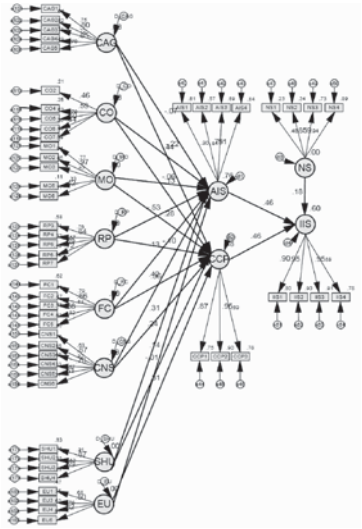


Fig. 5. Modelo evaluado: caso de estudio UNA-Puno

4.8.3 Análisis Global

El modelo de investigación propuesto se ha evaluado con base a la estadística multivariante; para medir la confiabilidad de cada ítem, la validez de los constructores, confiabilidad compuesta, la validez discriminante y demostrar si la intención para implementar seguridad de información está influenciada en el nivel macro por factores específicos.

Dentro de todo el modelo, los factores más importantes o que influyen a la Actitud para implementar Seguridad en Sistemas de Información son:

- En un primer lugar los Recursos y Presupuesto, donde su valor path es -0.558, que afecta negativamente; ello en razón a que como ocurre en la mayoría de instituciones públicas, como en el caso de UNA-Puno, la falta de presupuesto es un factor determinante para implementar un plan de seguridad de información.
- La Cultura Organizacional con un path de 0.439, que revela la existencia de normas y valores que influyen positivamente en la situación estudiada.
- La Conciencia de la necesidad de seguridad por el personal con un path de 0.431, que revela el grado de conciencia que tiene del personal de la UNA-Puno respecto a la necesidad de implementar seguridad en los sistemas de información.

En cuanto al control conductual percibido, también llamado autosuficiencia, se ve influenciada por:

- En primer lugar la Formación y Capacitación con un path de 0.357, que muestra que la capacitación es muy importante para garantizar la implementación del plan de seguridad.
- La Conciencia de la necesidad de seguridad por el personal con un path de 0.325, mostrando que la conciencia acerca de la seguridad determina la autosuficiencia en el personal, por lo que el trabajo en programas de concientización es importante.
- La Experiencia del usuario con un path de 0.304, influye en la autosuficiencia, lo que es lógico que un usuario más experimentado pueda adaptarse mejor a la implementación de un plan de seguridad.
- La Misión de la Organización con un path de 0.268, influye en la autosuficiencia, ciertamente si la organización traduce la misión y visión a los empleados y que a su vez los S.I. contribuyen a ésta, esto permite una implementación exitosa.
- El compromiso de la alta gerencia con un path de -0.212, influye en forma inversa en el control conductual percibido, debiéndose al poco involucramiento de los jefes y directivos en los proyectos de seguridad.

En cuanto a la Intención para implementar Seguridad en los Sistemas de Información, son significativos la Actitud para implementar Seguridad en Sistemas de Información con path de 0.463 y el control conductual percibido con path de 0.463, que explican el 60.8% de la varianza del factor principal. No es significativa la dimensión Norma subjetiva, según el caso de estudio.

De los resultados obtenidos, es posible determinar que los factores que son necesarios controlar, en primer lugar están referidos a los recursos y presupuesto, influenciando negativamente, por lo que una asignación presupuestal adecuada para el plan de seguridad y su correspondiente implementación es imprescindible, pues para el usuario sin ello el plan no tendrá el éxito esperado. Por otro lado, la cultura organizacional así como la conciencia de la necesidad de seguridad, influyen positivamente en la actitud del usuario, pues muestra que es importante en su trabajo con sistemas de información.

En cuanto a la autosuficiencia que es percibida por el usuario, son importantes en forma positiva la formación y capacitación, pues el usuario siente que con una adecuada capacitación logrará adaptarse al plan de seguridad a implementarse; lo que se encuentra asociado a su experiencia con proyectos tecnológicos previamente desarrollados, pues mientras mayor sea su experiencia su intención será mejor. La conciencia sobre la seguridad también influye fuertemente, por un lado, los empleados poco conscientes tendrán poca intención hacia la implementación de un plan de seguridad, por otro, la misión clara de la organización influye en su intencionalidad. Pero el compromiso de la alta gerencia influye negativamente, principalmente reflejado el hecho por el cual la carga del proceso de implementación de cualquier solución tecnológica es encomendada al área de T.I. con escaza participación de los demás directivos, aspecto que influye en la percepción del usuario.

Todos los factores mencionados deben controlarse adecuadamente para garantizar el éxito en la implementación del plan e seguridad en S.I. para la UNA-Puno.

5 CONCLUSIONES

Se ha propuesto un modelo de evaluación de factores críticos de éxito en la implementación de la seguridad en sistemas de información respecto a la intención del usuario. El modelo propuesto contempla ocho factores: compromiso de la gerencia, cultura organizacional, misión de la organización, recursos y presupuestos, formación y capacitación, conciencia de la necesidad de seguridad, soporte hacia el usuario, experiencia del usuario; tres dimensiones: norma subjetiva, actitud para implementar seguridad de la información, y control conductual percibido; y la intención para implementar seguridad de sistemas de información.

El modelo propuesto es de gran relevancia para las instituciones que desean tener éxito en implementar un plan de seguridad en sistemas de información, pues el modelo propuesto permite identificar las barreras que impiden implementar un plan de seguridad, lo que permite con antelación tomar medidas correctivas para mitigar dichas barreras. Además permite identificar los factores que influyen positivamente en la intención del usuario, que son indispensables a considerar para tener éxito en la implementación de un plan de seguridad.

Se realizó un caso de estudio en la Universidad Nacional del Altiplano Puno, en donde se aplicó el modelo propuesto, y se encontró que los factores que influyen en la actitud para implementar seguridad en sistemas de información son: los recursos y presupuesto, que influye negativamente, pues para el usuario sin ello el plan no tendrá el éxito esperado; la cultura organizacional y la conciencia de la necesidad de seguridad son factores que influyen positivamente en la actitud del usuario, pues muestra que es importante en su trabajo con sistemas de información. Respecto a los otros factores estás deben acogerse como parte del proyecto de implementación en dicha entidad.

REFERENCIAS

[1] Abu-Zineh, S. (2006). Success Factors of Information Security Management: A Comparative Analysis between Jordanian and Finnish Companies. M.Sc. Thesis: HANKEN The Swedish School of Economics and Business Administration.

[2] Academia Lationoamericana de la Seguridad Informática. (2011, 01 14). Unidad 1: Introducción a la Seguridad de Información. (MIcrosoft Technet) Retrieved from http://www.mslatam.com/latam/technet/cso/Html-ES/home.asp

[3] Ajzen, I. (1991). The theory of planned behavior. Organizational behavior and human decision processes(50), 179 -211.

[4] Ajzen, I., & Fishbein, M. (1980). Understanding attitudes and predicting social behavior. Englewood Cliffs. N.J., Inc. U.S.A: Prentice Hall.

[5] Al-Awadi, M., & Renaud, K. (2008). Success Factors in Information Security Implementation in Organizations. University of Glasgow.

[6] Bjorck, F. (2002). Implementing Information Security Management Systems – An Empirical Study of Critical Success Factors.

[7] Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS Quarterly, Vol. 34 (No. 3), pp. 523-548.

[8] Cavusoglu, H., & Etal. (2010). Information Security Control Resources in Organizations: A Multidimensional View and Their Key Drivers. Sauder School of Business, University of British Columbia.

[9] Chuttur, M. (2009). Overview of the Technology Acceptance Model: Origins,Developments and Future Directions. Sprouts: Working Papers , 9 (37), 1-20.

[10] Ernst & Young. (2008). Moving Beyond Compliance: Ernst & Young's 2008 Global Information Security Survey. Retrieved from http://www.ey.com/Publication/vwLUAssets/2008_Global_Information_Security_Survey_english/$FILE/2008_GISS_ingles.pdf

[11] Fishbein, M., & Ajzen, I. (1975). Belief, attitude, intention and behavior: an introduction to theory and research. Reading, MA: Addison-Wesley.

[12] Huang, E., & Hao Chuang, M. (2007). Extending the theory of planned behaviour as a model to explain post-merger employee behaviour of IS use. Computers in Human Behavior, 240–257.

[13] INDECOPI. (2007). Norma Técnica Peruana "NTP-ISO/ IEC 17799:2007 EDI. Tecnología de la Información segunda versión. Lima.

[14] ISO/IEC. (2005). ISO/IEC 17799:2000 Information technology – Code of practice for information secu-

rity 2d Ed. Switzerland: International Organization for Standardization. Retrieved 03 03, 2011, from http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=33441&IC

[15] ISO/IEC. (2007). ISO/IEC 27002 Code of practice for information security management. USA.

[16] Kankanhalli, A., Hock-hai, T., Bernard, C., & Kwok-kee, W. (2003). An integrative study of information systems security effectiveness. international Journal of information management, 139154.

[17] McKay, J. (2003). Pitching the Policy: implementing IT Security Policy through Awareness. USA: SANS Institute.

[18] Nosworthy, J. D. (2000). Implementing information security in the 21st century – Do You Have the Balancing Factors? computer& security(19), 337-347.

[19] Pahnila, S., Siponen, M., & Mahmood, A. (2007). Employees behavior towards IS security policy compliance. In 40th Hawaii International Conference on System Sciences (HICSS 07)

[20] Partida, A., & Ezingeard Henley, J.-N. (2007). Critical Success Factors and Requirements for Achieving Business Benefits from Information Security. Proceedings of European and Mediterranean Conference on Information Systems 2007 (EMCIS2007), 66-76.

[21] Ponemon Institute. (2010). 2009 Annual Study: Global Cost of Data Breach, Understanding Financial Impact, Customer Turnover and Preventive Solutions. USA: Ponemon Institute PGP.

[22] Siponen, M. T. (2000). A Conceptual Foundation for Organizational Information Security Awareness. Information Management & Computer Security, Vol. 8(No. 1), pp. 31-41.

[23] Siponen, M. T. (2005). An Analysis of the Traditional IS Security Approaches: Implications for Research and Practice. European Journal of Information Systems, 14(3), pp. 303-315.

[24] Taylor, S., & Todd, P. (1995). Assessing IT usage: The role of prior experience. MIS Quarterly, 19 (4), 561-570.

[25] Thompson, R., Higgins, C., & Howell, J. M. (1994). Influence of experience on personal computer utilization: Testing a conceptual model. Journal of Management Information Systems, 11 (1), 167-188.

[26] Tipton, H. F., & Krause, M. (2006). Information Security Management Handbook. USA: CRC Press.

[27] Villegas Ortega, J. H. (2009). Un modelo de evaluación de los atributos críticos de éxito de los sistemas de información en el desempeño individual, cooperativo y organizacional. Magister Thesis Ingeniería de Sistemas: Universidad Nacional Mayor de San Marcos.

[28] Whitman, M. E., Caylor, J., Fendler, P., & Baker, D. (2005). Rebuilding the Human Firewall. Information Security Curriculum Development Conference, Kennesaw, GA, USA. ACM, 104-106.

Condori Alejo, Henry I. Docente Asociado del Departamento de Ingeniería de Sistemas de la Universidad Nacional del Altiplano, Magister en Ciencias en Ingeniería de Sistemas y Computación, con mención en Gestión de Tecnologías de información.

Mauricio Sanchez, David S. Docente Principal de la Facultad de Ingeniería de Sistemas de la Universidad Nacional Mayor de San Marcos, Doctor en Ciencias en Ingeniería de Sistemas y Computación por la Universidad Federal de Río de Janeiro de Brasil.