Universidad Inca Garcilaso de la Vega

Escuela de Post-Grado

Maestría en Ingeniería de Sistemas y Computación

TESIS

Un Modelo de Evaluación de Factores Críticos de Éxito en la Implementación de la Seguridad en Sistemas de Información para determinar su influencia en la intención del usuario.

Presentada por:

HENRY IVÁN CONDORI ALEJO

Para optar el grado Académico de Maestro en Ciencias en Ingeniería de Sistemas y Computación con mención en Gestión de Tecnologías de la Información

LIMA - PERÚ
2012

Índice

Índice de Figuras

Índice de Tablas

Resumen

La seguridad de información normalmente ha sido considerada como un problema tecnológico y a su vez una solución tecnológica. Lo que es totalmente falso, pues la Seguridad está basada en las personas; sin la participación del usuario no es posible reducir los riesgos y asegurar la protección de la información; las organizaciones a menudo confían en soluciones basadas en tecnologías dejando de lado la percepción del usuario, quien es el actor principal.

En tal sentido, el Modelo de Evaluación de Factores Críticos de Éxito para la Implementación de Seguridad en Sistemas de Información en la intención del usuario, plantea un conjunto de constructores claves como son: 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, Infraestructura Tecnológica, Soporte hacia el usuario, Experiencia del usuario; combinados con la teoría del comportamiento planificado (TPB), que permite determinar y evaluar los factores críticos de éxito para implementar seguridad desde la perspectiva del usuario, con la finalidad de garantizar una implementación exitosa de la Seguridad de SI o efectuar los ajustes necesarios para su éxito. El modelo se apoya en una guía metodológica, que permite su aplicación a escenarios reales. Mediante la aplicación de la Guía propuesta se ha evaluado la Universidad Nacional del Altiplano, encontrando que los factores determinantes son: los recursos y presupuesto, la cultura organizacional, la conciencia de la necesidad de seguridad información y la formación y capacitación; se obtuvo una varianza del factor principal de 60.8%, en base a 128 observaciones válidas correspondientes a los usuarios del Sistemas Integral Administrativo de la UNA-Puno.

Palabras clave: Seguridad de Información, Factores Críticos de éxito, intención del usuario, sistemas de información.

Abstract

Information security has generally been regarded as a technological problem and also a technological solution. What is totally false, because the security is based on the people, without their participation is not possible to reduce risks and ensure the information security, organizations often rely on technology-based solutions apart from the user's perception who is the lead actor, but little has been done to determine the factors that influence their intention to Implement Security in Information Systems.

In this regard, the Model to Evaluate Critical Success Factors for Implementation of Security in Information Systems in the user's intent sets a number of key factors such as: management commitment, organizational culture, organizational mission, Resources and budget, education and training, awareness of the need for security personnel, technology infrastructure, user's support, user's experience combined with the theory of planned behavior (TPB), so determine and assess the critical factors success in implementing security from the perspective of the user in various scenarios where required to implement security in IS, in order to ensure successful implementation of IS Security or make the necessary adjustments to their success. The model supports a methodological guide, which allows its application to real scenarios. By applying the proposed Guide has assessed the Universidad Nacional del Altiplano, finding that the determining factors are: the resources and budget, organizational culture, awareness of the need for security and training information and training, it obtained a variance main factor of 60.8%, based on 128 valid observations for UNA-Puno Information Systems users.

Key words: Information Security, Critical Success Factors, user's intent, Information systems.

Introducción

Considerando que la adopción de Sistemas de Información es masiva en el contexto empresarial, surge la necesidad de proteger la información que forma parte de dichos sistemas, pues dicha información se torna crítica e invaluable, pues concentra el día a día de la organización.

En tal sentido se realiza un esfuerzo considerable para garantizar la seguridad de la información, que principalmente se enfoca en medios tecnológicos como cortafuegos, software de seguridad, licencias, bloqueo de puertos, etc. Pero de acuerdo a estudios realizados, se ha podido determinar que el principal elemento en la implementación de la seguridad es el usuario, esto quiere decir, por más buena que sea determinada política, tecnología aplicada, si no existe la intención positiva del usuario para que el plan de seguridad de determinada empresa funcione, simplemente no tendrá los efectos deseados.

Al respecto (Tipton & Krause, 2006) señalan que la Seguridad está basada en las personas, además manifiestan -“Si se piensa que la tecnología puede resolver los problemas de seguridad, entonces no se entiende los problemas o la tecnología”.

Es más, para reducir los riesgos y asegurar protección de la información, las organizaciones a menudo confían en soluciones basadas en tecnologías (Ernst & Young, 2008), dejando de lado la percepción del usuario, quien es el actor principal.

En tal sentido, surge la necesidad de determinar cuáles son los factores que condicionan la intención de usuario para implementar la seguridad de información en un contexto organizacional.

El presente estudio en particular, plantea como respuesta, el desarrollo de un modelo para determinar los factores críticos, que ha sido aplicado a la Universidad Nacional de Altiplano, mostrando así los factores que influyen en dicho caso particular. Lo que no significa que el modelo sea aplicable a dicho

caso, sino que permite ser aplicado a cualquier organización, donde se requiera determinar los factores que influencian la intención del usuario.

Es importante conocer dichos factores antes de la implementación de la Seguridad en Sistemas de Información, pues, permitirá controlarlos y lograr como consecuencia una implementación exitosa.

La presente Tesis ha sido organizada en 7 capítulos. En el Capítulo 1, se presenta los fundamentos teóricos donde se describen los antecedentes, los principales conceptos asociados con el modelo propuesto, los cuales son abordados a lo largo de la presente investigación. Son parte de este capítulo: Las definiciones de seguridad, los estándares de seguridad, los factores críticos de éxito, los sistemas de información. Así como el estado del arte, detallando los diferentes estudios acerca de los factores críticos de éxito para implementar seguridad, así como los modelos de evaluación, los cuales van apareciendo cronológicamente, para finalmente, terminar con la descripción de la Teoría del Comportamiento Planificado (TPB) propuesta por Ajzen; se brinda de este modo, el marco sobre el cual se formula la presente investigación.

En el Capítulo 2, se describe el problema de investigación, partiendo de la realidad problemática, estableciendo el problema de investigación, los correspondientes objetivos y las hipótesis; así como la importancia del estudio.

En el Capítulo 3, se describe la metodología que se ha empleado, que principalmente se basa en un estudio explicativo, trasversal y de diseño factorial.

En el Capítulo 4, se presentan los resultados alcanzados en aplicación del modelo propuesto con la correspondiente contrastación y discusión. En primer lugar, se describe el aporte teórico, donde se presenta el modelo de evaluación propuesto; se expone los principales factores críticos de éxito, las influencias, sus características y su interrelación con los factores a tener en cuenta en la implementación de Seguridad en los Sistemas de Información. En segundo lugar, se presenta la Guía Metodológica de implementación del modelo

propuesto en el Capítulo precedente, que se sintetiza en 17 pasos para el proceso de evaluación aplicando el modelo propuesto. En tercer lugar se presentan los resultados de la aplicación del modelo en la Universidad Nacional del Altiplano.

Finalmente, en el Capítulo 5, se detallan las conclusiones referidas a la aplicación del modelo propuesto, la guía metodológica, el cuestionario y el caso de estudio; luego, se presentan las recomendaciones.

CAPÍTULO I

FUNDAMENTOS TEÓRICOS

1.1 Antecedentes de la Investigación

(Anderson J. P., 1980), como pionero en la seguridad de información describe la importancia del comportamiento enfocado hacia la seguridad, donde da por primera vez una definición de los principales agentes de las amenazas informáticas.

Con el transcurso de los años y el empleo de las computadoras para automatizar los procesos de información, la preocupación por la seguridad de información se ha incrementado, tal es así que según el CERT de la Universidad de Carnage Mellon de Estados Unidos (Community Emergency Response Team) (CERT, 2008), dedicado a la evaluación de incidentes de seguridad, los casos de vulnerabilidades de seguridad de información desde su registro inicial el 1995, fueron 171 casos, al año 2007 registró 7236 casos, lo que claramente muestra el incremento de la inseguridad de información.

Por otro lado, la investigación de (Córdova Rodriguez, 2003), realiza un diagnóstico de la situación actual en cuanto a su estructura interna y a la seguridad de la información de una entidad financiera y diseña un Plan de Seguridad de la Información que permita desarrollar operaciones seguras basadas en políticas y estándares claros y conocidos por todo el personal de la entidad. Este trabajo describe en detalle cómo diseñar el plan de seguridad de la información para lo cual se realiza una evaluación de riesgos y vulnerabilidades a los que está expuesta la entidad, luego se desarrollaron políticas y estándares de seguridad de la información con el fin de contar con una guía para la protección de la información. Finalmente el plan de implementación propuesto, describe las actividades que se deben realizar, las etapas incluidas en su desarrollo y el tiempo estimado en su ejecución.

En el año 2004, (INDECOPI, 2004), publica la primera versión de la Norma Técnica Peruana “NTP-ISO/ IEC 17799:2004 EDI. Tecnología de la

Información. Código de buenas prácticas para la gestión de la seguridad de la información, basado en el estándar internacional ISO 17799. Seguidamente la Presidencia de Consejo de Ministros, mediante Resolución Ministerial Nº 224-2004-PCM en fecha 23 de julio de 2004, aprobó el uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 17799:2004 EDI. Tecnología de la Información para las entidades del sector público.

(Villena Aguilar, 2006), realizó una investigación de las normas y estándares que van difundiéndose con mayor énfasis en el mercado peruano, en especial en el sector financiero a partir de los cuales se planteó un esquema de gestión de seguridad de información que puede ser empleado por una institución financiera en el Perú, con el objetivo de cumplir con las normas de regulación vigentes en lo relacionado a la Seguridad de Información que son exigidas para este tipo de instituciones del sector financiero.

Como parte de la preocupación en seguridad, (Sanchez Acevedo & Segura Castañeda, 2006), plantean una guia metodológica para obtener el Retorno de Inversión en Seguridad de Información.

Es necesario resaltar el estudio de (Rayme Serrano, 2007), realizado en tres Universidades de Lima Metropolitana: la Universidad Nacional Mayor de San Marcos (UNMSM), la Universidad Nacional Federico Villarreal (UNFV) y la Universidad Privada San Juan Bautista (UPSJB), teniendo como objetivo proponer estrategias de Gestión de Seguridad de la Información y sus implicancias en la calidad y eficacia en los servicios críticos de las universidades. El estudio reveló que las estrategias que se deben utilizar en la gestión de seguridad de la información son: primero, la importancia de desarrollar políticas de seguridad: UNMSM 37 %, UNFV 19% y UPSJB 24%; segundo, los programas de capacitación al personal, donde los expertos consultados informaron el interés por asistir: UNMSM 60%, UNFV 70% y UPSJB 70% y tercero, la protección a los recursos de información.

Se da un nuevo paso en la adopción de normas técnicas internacionales al publicarse la segunda versión de la Norma Técnica Peruana "NTP-ISO/ IEC 17799:2007 EDI Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información (INDECOPI, 2007), que

actualiza la anterior versión del a NTP publicada en el año 2004, concordante con la actualización del estándar internacional ISO 17799. Del mismo modo, la Presidencia de Consejo de Ministros, mediante Resolución Ministerial Nº 246-2007-PCM, del 22 de agosto de 2007, aprobó el uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 17799:2007 EDI. Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información. 2a. Edición" en todas las entidades integrantes del Sistema Nacional de Informática.

La propuesta de (Sánchez, Villafranca, Fernández-Medina, & Piatini, 2007), da a conocer, una nueva metodología para la gestión de la seguridad y su madurez en las PYMES. Esta metodología permite a las PYMES desarrollar y mantener un SGSI con un coste en recursos aceptable para este tipo de empresas; definiendo cómo se debe utilizar esta metodología y las mejoras que ofrece con respecto a otras metodologías que afrontan el problema de forma parcial, o de manera bastante costosa para las PYMES. Las características ofrecidas por la nueva metodología y su orientación a las PYMES fue muy bien recibida, y su aplicación a resultado muy positiva ya que permitió acceder a este tipo de empresas al uso de sistemas de gestión de seguridad de la información, siendo sus principales características los resultados a corto plazo y la reducción de los costos que supone el uso de otras metodologías.

A su vez, (Cabrera García, García Castro, & Salinas Romero, 2009), plantean que las organizaciones que contratan el servicio de Outsourcing (tercerización) no tienen bien establecidos sus lineamientos y políticas ante la adquisición de este servicio; de igual forma las organizaciones que prestan el servicio no poseen lineamientos que certifiquen que el servicio que brindan es 100% ético y seguro, por lo cual proponen un modelo de seguridad en las aplicaciones Web desarrolladas por un tercero, que proporciona un respaldo hacia las empresas que contratan el Outsourcing con el fin de proteger la información que se encuentra en juego durante el desarrollo de la aplicación. El modelo se concentra en una serie de lineamientos y políticas basados en las leyes mexicanas como la Ley Federal de Derechos de Autor, la Ley Federal del Trabajo y la Constitución Política de los Estados Unidos Mexicanos; incluyendo también las mejores prácticas como ITIL y COBIT.

Kimberley y Gurvirender plantean el desarrollo de un modelo de Éxito de la Seguridad de Sistemas de Información en el contexto del Gobierno, donde se indica que, la seguridad de información y en especial la seguridad de sistemas de información ha cobrado vital importancia, a pesar de ello, poco se ha hecho para entender sus dimensiones en el contexto organizacional del éxito de la seguridad de información, de forma tal que proponen un modelo con seis dimensiones de seguridad (Dunkerley & Tejay, 2009)

Al igual que otros países, en referencia a la constante preocupación respecto a seguridad de información, el Perú, a través de la PCM (Presidencia de Consejo de Ministros, 2009), el 22 de agosto del 2009, crea el Grupo de trabajo denominado Coordinadora a Respuestas de Emergencias en Redes Teleinformáticas de la Administración Pública de Perú (PeCERT), formado como parte de la ONGEI y que como objetivo principal tiene: registrar, coordinar, asesorar en cuanto a incidentes y mejoramiento de la seguridad de información.

1.2 Marco Teórico

1.2.1 Seguridad de Información

1.2.1.1 Información

La información es el recurso clave para quien trabaja con el conocimiento en general, y especialmente para el ejecutivo. Así Druker, manifiesta que, “- Cada vez más, la información crea el eslabón con sus colegas y con su organización y con su red”. En otras palabras, la información es el elemento que permite que aquéllos que trabajan con el conocimiento lleven a cabo su labor. Por otra parte, solamente los que trabajan con el conocimiento y especialmente los ejecutivos, pueden decidir cómo organizar su información para convertirla en un recurso clave para una acción eficaz, pues mientras no está organizada la información sigue siendo datos (Druker, 1999).

Según Idalberto Chiavenato, información "es un conjunto de datos con un significado, o sea, que reduce la incertidumbre o que aumenta el conocimiento de algo. En verdad, la información es un mensaje con significado en un determinado contexto, disponible para uso inmediato y que proporciona orientación a las acciones por el hecho de reducir el margen de incertidumbre con respecto a nuestras decisiones" (Chiavenato, 2006).

Para Ferrell y Hirt, la información "comprende los datos y conocimientos que se usan en la toma de decisiones" (Ferrell & Geoffrey, 2004).

Según Czinkota y Kotabe, la información "consiste en datos seleccionados y ordenados con un propósito específico" (Czinkota & Masaaki, 2001).

1.2.1.2 Concepto Seguridad

(Peso Navarro, 2004), indica que, la Seguridad viene a ser la protección de los activos frente a acciones o situaciones no deseadas, mediante la implantación

de los controles, lo que suele suponer una inversión y un esfuerzo. Y todo ello en las entidades para proteger los intereses de los accionistas, de los empleados, de los clientes, de los proveedores y de los ciudadanos afectados según el sector.

1.2.1.3 Concepto Seguridad de Información

La información es un activo que, como otros activos importantes del negocio, tiene valor para la organización y requiere en consecuencia una protección adecuada (INDECOPI, 2007); además indicando que se encuentra sometida a diversas amenazas.

La seguridad de la información protege a la información, propiamente dicha, de un amplio rango de amenazas para asegurar la continuidad del negocio, minimizar los daños a la organización y maximizar el retorno de las inversiones y las oportunidades de negocios.(INDECOPI, 2004).

Se entiende por seguridad de la información a todas aquellas medidas preventivas y reactivas del hombre, de las organizaciones y de los sistemas tecnológicos que permitan resguardar y proteger la información buscando mantener la confidencialidad, la autenticidad y Integridad de la misma. Diferenciando el concepto de seguridad de la información con el de seguridad informática, en que este último sólo se encarga de la seguridad en el medio informático.(Fitzgerald, 2007).

1.2.1.4 Principios

Al ser la protección de los activos, uno de los objetivos principales de la seguridad de información, esto significa mantenerlos seguros frente a las diversas amenazas a las que se enfrentan y que pueden afectar su funcionalidad de diferentes maneras: corrupción, acceso indebido e incluso hurto y eliminación.

(Academia Lationoamericana de la Seguridad Informática, 2011), la Seguridad Informática se basa en la preservación de unos principios básicos, los cuales son enumerados y definidos por diferentes autores, con algunas variantes. Cada uno de dichos principios tiene un propósito específico dentro del marco del objetivo de la seguridad informática (Harris, 2004). Los cuales son:

a) Confidencialidad

Este principio tiene como propósito asegurar que sólo la persona o personas autorizadas tengan acceso a cierta información. La información, dentro y fuera de una organización, no siempre puede ser conocida por cualquier individuo, si no por el contrario, está destinada para cierto grupo de personas, y en muchas ocasiones, a una sola persona. Esto significa que se debe asegurar que las personas no autorizadas, no tengan acceso a la información restringida para ellos. La confidencialidad de la información debe prevalecer y permanecer, por espacios de tiempo determinados, tanto en su lugar de almacenamiento, es decir en los sistemas y dispositivos en los que reside dentro la red, como durante su procesamiento y tránsito, hasta llegar a su destino final (Stoneburner, 2001).

b) Integridad

La integridad tiene como propósito principal, garantizar que la información no sea modificada o alterada en su contenido por sujetos no autorizados o de forma indebida. Asimismo, la integridad se aplica a los sistemas, teniendo como propósito garantizar la exactitud y confiabilidad de los mismos. Debido a esto, la integridad como principio de la Seguridad Informática, se ha definido en dos partes: integridad de los datos e integridad de los sistemas.

La integridad de los datos, se refiere a que la información y los programas solo deben ser modificados de manera autorizada por las personas indicadas para ello. Estas alteraciones pueden darse por inserciones, sustituciones o eliminaciones de contenido de la información. Por su parte, la integridad de los sistemas, hace referencia a que todo sistema debe poder cumplir su función a

cabalidad, sin ninguna violación o modificación del mismo, en su estructura física y/o lógica, sin perder necesariamente su disponibilidad (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, 1995).

c) Disponibilidad

Este principio tiene como propósito, asegurar que la información y los sistemas que la soportan, estén disponibles en el momento en que se necesiten, para los usuarios autorizados a utilizarlos. Al referirse a los sistemas que soportan la información, se trata de toda la estructura física y tecnológica que permite el acceso, tránsito y almacenamiento de la información (Academia Lationoamericana de la Seguridad Informática, 2011).
Adicionalmente, la disponibilidad hace referencia a la capacidad que deben tener los sistemas de recuperarse ante interrupciones del servicio, de una manera segura que garantice el continuo desarrollo de la productividad de la organización sin mayores inconvenientes (Harris, 2004).

Se han presentado varias interpretaciones y discusiones alrededor de los principios de integridad y confidencialidad; dichas discusiones radican en la pertinencia de dichos principios a los sistemas que soportan la información. Algunos autores argumentan que la confidencialidad y la integridad conciernen únicamente a la información, mientras que la disponibilidad atañe a la información y a los sistemas que la soportan (Brinkley & SChell, 1995).
Mientras que otros, plantean la integridad y la disponibilidad como principios relativos a dichos sistemas que soportan la información (Harris, 2004).

Figura 1 Principios de la Seguridad de Información

1.2.1.5 Necesidad de la seguridad de la información

En la actualidad, la información y consecuentemente los procesos que se encuentran vinculados a ésta, amplían su relevancia, pues son necesarios en conjunto como un sistema para el logro de objetivos estratégicos y competitividad de la organización, basado en la confidencialidad, integridad y disponibilidad.

Las organizaciones y sus sistemas de información se enfrentan, cada vez más, con riesgos e inseguridades procedentes de una amplia variedad de fuentes, incluyendo fraudes basados en informáticas, espionaje, sabotaje, vandalismo, incendios o inundaciones. Ciertas fuentes de daños como virus informáticos y ataques de intrusión o de negación de servicios se están volviendo cada vez más comunes, ambiciosos y sofisticados(Rayme Serrano, 2007).

(Aceituno, 2004) es muy preciso al señalar que: "- El único sistema verdaderamente seguro es aquel que se encuentra apagado, encerrado en una caja fuerte de titanio, enterrado en un bloque de hormigón, rodeado de gas nervioso y vigilado por guardias armados y muy bien pagados. Incluso entonces yo no apostaría mi vida por ello."

(Peso Navarro, 2004), menciona que en un principio, la información estaba recluida en unas salas, verdaderos templos dentro de las empresas y de las Administraciones Públicas, su protección era relativamente fácil, prácticamente consistía en defender físicamente el recinto del Centro de Proceso de Datos y eran pocos los miembros en acceder a esos datos informatizados. En una segunda fase, la información empezó a salir y a circular por toda la empresa a través de las redes de comunicación. Asimismo, el número de personas que podía acceder a los datos informatizados aumentó considerablemente; aunque con ciertas restricciones. El tercer salto ocurrió con la aparición de los ordenadores personales y la utilización generalizada de las redes públicas o el Internet. La aparición y utilización masiva de Internet ha hecho que el tema de la seguridad en la sociedad de la información sea prioritario a la hora de buscar soluciones.

Los autores (Laudon & Laudon, 2004), sostienen que antes de la automatización con computadoras, los datos acerca de individuos y organizaciones se mantenían y protegían en forma de expedientes en papel

dispersos en distintas unidades de negocios o de organización. Los sistemas de información concentran los datos en archivos de computadoras a los que podrían tener fácil acceso un gran número de personas y grupos externos de la organización.

La seguridad que se puede lograr por medios técnicos se encuentra limitada, por lo que, el aspecto técnico debe apoyarse en la gestión y procedimientos adecuados, que deben estar basados en un estándar y metodología propia de la seguridad de información.

Un fallo de seguridad, es cualquier incidente que la compromete, es decir, que pone en peligro cualquiera de los parámetros con los que se valora la seguridad: la confidencialidad, la disponibilidad o la integridad de la información. Con la actual complejidad de los sistemas de información, con una economía y un comercio que se basan en intercambios y comunicaciones a lo largo y ancho del mundo, con un número creciente de usuarios que no sólo se conectan desde dentro sino también desde fuera de la organización, es fácil hacerse una idea del reto que presenta evitar que sucedan cosas como (Instituto Nacional de Tecnologías de la comunicación (INTECO), 2010):

- Fallos en las comunicaciones.
- Fallos en el suministro eléctrico.
- Fallos humanos de usuarios internos, usuarios externos, administradores, programadores, etc.
- Fallos en los sistemas de información: redes, aplicaciones, equipos, etc.
- Virus informáticos, gusanos, troyanos, etc. que inundan la red.
- Accesos no autorizados a los sistemas o la información.
- Incumplimiento de una ley o un reglamento.

1.2.1.6 Historia y Evolución

Los problemas de seguridad surgen mucho antes de la interconexión de computadoras en los años 70’s y 80’s; estos se remontan a los inicios del desarrollo de las máquinas de tiempo compartido, donde se presentaban riesgos de acceso no autorizado y modificación de información. Previo a estos desarrollos, se hablaba de seguridad desde los inicios de la Segunda Guerra Mundial, donde surgieron los problemas de comunicación segura entre las

diferentes tropas en misión; para solucionar estos problemas se empezó a hablar del cifrado de mensajes (Rayme Serrano, 2007)

Por lo que, el proceso de evolución de la seguridad hasta llegar a la seguridad de información, entendiendo que dicho proceso no solo involucra los elementos técnicos de protección sino la gestión y políticas en el ámbito de las tecnologías de información, tiene un largo camino en poco tiempo.

A continuación se describen algunos de los hechos históricos que han marcado los inicios y evolución de la seguridad informática (Macmillan, 2002):

- A finales de los años 50 los computadores trabajaban con registros especiales para definir particiones en memoria para el uso de programas separados y asegurar que un programa en ejecución no pueda acceder a particiones de otro programa. La memoria virtual ofrece mecanismos que permiten proteger la información como si estuviese es su propia partición de memoria; las particiones y el concepto de memoria virtual proveen una de las primeras medidas de protección de seguridad en ambientes multiusuarios.
- A principios de los años 60, los sistemas de tiempo compartido proveían almacenamiento de información a usuarios individuales. Este sistema fue seguro usando control de acceso, que permitía al dueño de la información, especificar y autorizar accesos a otros diferentes usuarios. La primera característica de la seguridad fue la protección de contraseñas de usuarios, donde los sistemas de autenticación codificaban la imagen de éstas.
- En 1968 el sistema Multics del MIT, presentó algunas características de seguridad y privacidad, donde se prestó mucha atención a identificar un pequeño kernel en el sistema operativo, que garantizara que todas las políticas de seguridad del sistema fueran permitidas.
- En 1969, vino la aparición de ARPANET (Advanced Research Project Agency Network) comenzando con cuatro nodos, hasta convertirse en lo que es hoy en día Internet. Este continuo aumento de interconexiones, incrementó el riesgo de acceso a usuarios externos no autorizados y asimismo, el conocimiento sobre temas de seguridad a los administradores y propietarios de las redes.

- El Unix-Unix System Mail (UUCP) en 1975 permitía a usuarios Unix ejecutar comandos en un sistema Unix secundario. Este permitía que correos electrónicos y archivos fuesen transferidos automáticamente entre sistemas, lo que también permitía a los atacantes borrar o sobre escribir los archivos de configuración. Como no había una administración central del UUCP en la red, el ARPANET hizo un acercamiento al control de los problemas de seguridad que no se aplicaban. En los siguientes años se empezó a hablar sobre criptografía con llave pública y firmas digitales, debido a la necesidad de permitir comunicación confidencial entre dos usuarios. Esto ha generado que la criptografía sea un tema importante en el desarrollo de la seguridad informática.
- En 1978 (Morris y Thompson) realizaron un estudio que demostraba que adivinar contraseñas a partir de datos personales de los usuarios, como son el nombre, teléfono, fecha de nacimiento, era más eficiente que decodificar las imágenes de dichas contraseñas. Estos fueron los primeros pasos de la ingeniería social, dentro del área de seguridad informática, y donde evolucionan así mismo, los principios de la misma, y en específico, la confidencialidad.
- En el mismo año nace una nueva preocupación de la seguridad informática, que consiste en la protección de los pagos electrónicos a través de la red que comenzaron a hacerse disponibles a los clientes. Este tipo de transacciones se tradujo en la necesidad de un alto nivel de seguridad, evolucionando así los conceptos de confidencialidad e integridad.
- El crecimiento exponencial de la red, comenzó a requerir un DNS (Directory Name Server) dinámico, que actualizara la base de datos de asociación de nombres y direcciones. Estos nuevos servidores se convierten en otro blanco para los atacantes y suplantadores. Los virus informáticos tienen un crecimiento notable y se convierten en una seria amenaza para los administradores de seguridad informática y para los usuarios.

- En 1988, se destaca el primer ataque a gran escala, a través de gusanos cibernéticos, que podrían llegar a infectar en horas un porcentaje significativo de la red. Este hecho permite reconocer las vulnerabilidades que se tienen en la red.
- La seguridad, encuentra otro interés profundo en los años previos a 1993, donde los atacantes utilizan métodos de sniffing (rastreo) para detectar contraseñas, y spoofing (suplantación) o usan los mismos computadores con identificadores falsos para transmitir sus propios paquetes al ganar accesos al sistema.

A raíz de dicho crecimiento de las redes, se comenzaron a presentar abusos computacionales causados por los mismos usuarios. Estos abusos se pueden clasificar en (Bailey, 1995): robo de recursos computacionales, interrupción de servicio, divulgación no autorizada de información y modificación no autorizada de información. A partir de estos abusos, y a partir de la evolución de los principios de la seguridad informática a través del tiempo, hoy en día se tiene un modelo actual basado en dichos principios de confidencialidad, integridad y disponibilidad, que buscan proteger la información, recursos y personas que hacen uso de ésta, tratando así de evitar el continuo crecimiento a dichos abusos. Dichos principios han ido evolucionando a través del tiempo, lo que no significa que hayan surgido solo hasta esta época.

Se pueden definir además seis clases de abusos técnicos por los que debe preocuparse la seguridad informática (Bailey, 1995): Errores humanos, abuso de usuarios autorizados, exploración directa, exploración con software especializado, penetración directa, mecanismos de subversión de seguridad.

1.2.1.7 Gobierno de la Seguridad de información

Aunque no hay ninguna definición universalmente aceptada para el gobierno de seguridad de información, el propósito de tal gobierno es asegurar que las actividades de seguridad de información apropiadas se llevan a cabo con el propósito que los riesgos se minimicen apropiadamente, las inversiones de seguridad de información estén apropiadamente dirigidas, el programa de seguridad tenga visibilidad para la dirección, así como éste plantee las

preguntas apropiadas que determinen la eficacia del programa de seguridad de información (Fitzgerald, 2007).

El IT Governance Institute (ITGI) define el gobierno de TI como "Una estructura de relaciones y procesos para dirigir y controlar la empresa para conseguir los objetivos de la empresa añadiendo el valor mientras se balancean el riesgo versus el retorno de inversión sobre TI y sus procesos." El ITGI propone que el gobierno de seguridad de información deba ser considerado parte del gobierno de TI, y que los directivos estén informados sobre la seguridad de información.

1.2.1.8 Beneficios de la Seguridad de Información

Existen numerosas e importantes razones para afrontar el desarrollo y la implantación de un Sistema de Gestión de la Seguridad (Instituto Nacional de Tecnologías de la comunicación (INTECO), 2010):

- Reducción de costes. Esta debería ser una de las principales motivaciones para llevar a cabo la implantación de un SGSI, ya que incide directamente sobre la rentabilidad económica de una organización. No suele serlo porque lo que se ve en un principio es el coste del mismo, sin embargo, en un breve plazo, se puede observar como el SGSI evita varias situaciones que suponen un coste, a veces importante. Al detectar los principales focos de fallos y errores, y eliminarlos o reducirlos hasta donde es posible, se evitan costosos incidentes de seguridad, que hasta entonces se asumían como cosas que pasan. A veces se evitan incidentes que hubieran ocurrido de no haber tomado las medidas a tiempo, y eso es difícil de cuantificar, pero no por ello es menos real. A veces los beneficios surgen de manera imprevista, como la reducción de primas de seguros en algunas pólizas debido a la justificación de la protección de los activos asegurados.

- Optimizar los recursos y las inversiones en tecnología. Con un SGSI las decisiones se tomarán en base a información fiable sobre el estado de los sistemas de información y a los objetivos de la organización. Habrá

una motivación de negocio detrás de estas decisiones, por lo que la dirección podrá comprenderlas y apoyarlas de manera más consciente. La organización dejará de depender exclusivamente de la experiencia o pericia del responsable de informática, o más peligroso aún, del proveedor habitual de informática, a la hora de valorar las distintas opciones de compra.

- Protección del negocio. Con un SGSI en marcha se evitan interrupciones en el flujo de ingresos, ya que se está asegurando de una manera eficaz la disponibilidad de los activos de información y, por lo tanto, de los servicios que la organización ofrece. Esto en cuanto a la actividad cotidiana, pero también se está preparado para recuperarse ante incidentes más o menos graves e incluso garantizar la continuidad del negocio, afrontando un desastre sin que peligre el negocio a largo plazo.

- Mejora de la competitividad. Cualquier mejora en la gestión de la organización redunda en beneficio de la eficacia y la eficiencia de la misma, haciéndola más competitiva. Además hay que considerar el impacto que suponen el aumento de la confianza de los clientes en el negocio, la diferenciación frente a los competidores y una mejor preparación para asumir retos tecnológicos.

- Cumplimiento legal y reglamentario. Cada vez son más numerosas las leyes, reglamentos y normativas que tienen implicaciones en la seguridad de la información. Gestionando de manera coordinada la seguridad permite un marco donde incorporar los nuevos requisitos y poder demostrar ante los organismos correspondientes el cumplimiento de los mismos.

- Mantener y mejorar la imagen corporativa. Los clientes percibirán la organización como una empresa responsable, comprometida con la mejora de sus procesos, productos y servicios. Debido a la exposición de cualquier organización a un fallo de seguridad que pueda acabar en la prensa, este punto puede ser un catalizador de esfuerzos, ya que

nadie quiere que su marca quede asociada a un problema de seguridad o una multa por incumplimiento, por las repercusiones que acarrea.

1.2.2 Estándares de Seguridad de Información

Una variedad de estándares y buenas prácticas han sido creados para respaldar la auditoría de controles de seguridad implementados. Estos recursos son valiosos para ayudar con el diseño de un programa de seguridad, cuando definen los controles necesarios para proveer sistemas de información seguros. Muchos de éstos han ganado un grado de la aprobación dentro de la comunidad de seguridad de información y cada uno añade valor a la inversión de seguridad de información. Aunque es necesario aclarar que varios de éstos no fueron diseñados respaldar la seguridad de información específicamente, muchos de los procesos dentro de estas prácticas respaldan los aspectos diferentes de la confidencialidad, la integridad, y la disponibilidad (Fitzgerald, 2007).

Por lo tanto, a toda organización que haga uso de las tecnologías de información, se recomienda implementar buenas prácticas de seguridad, pues en muchas ocasiones, no seguir un proceso de implementación adecuado puede generar vacíos por la misma complejidad de las organizaciones, en ese sentido, aumenta la posibilidad de riesgos en la información.

El origen del primer estándar en seguridad de la información fue desarrollado en los años 1990, en Inglaterra, como respuesta a las necesidades de la industria, el gobierno y las empresas para fomentar un entendimiento común sobre el tema y establecer lineamientos generales. En 1995, el estándar BS 7799 es oficialmente presentado. En 1998 se establecen las características de un Sistema de Gestión de la Seguridad de la Información (SGSI) que permita un proceso de certificación, conocida como BS 7799 parte 2.

En diciembre del 2000 la Organización de Estándares Internacionales (ISO) incorpora la primera parte de la norma BS 7799, rebautizada como ISO 17799,

la cual se presenta bajo la forma de guías de orientación y recomendaciones en el área de Seguridad de la información (Rayme Serrano, 2007).

La Seguridad de la Información tiene asignada la serie 27000 dentro de los estándares ISO/IEC, siendo un conjunto de estándares desarrollados por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission) que proporcionan un marco de gestión de la seguridad de la información, que puede ser empleado por cualquier tipo de organización, grande o pequeña, pública o privada (ISO/IEC, 2005).

- ISO/IEC 27000: Contiene términos y definiciones empleados en toda la serie 27000.
- ISO/IEC 27001: Sistemas de Gestión de la Seguridad de la Información (SGSI). Es la norma que especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información. Es certificable.
- ISO/IEC 27002: (antes ISO17799). Guía de mejores prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información con 11 dominios, 39 objetivos de control y 133 controles. Proporciona recomendaciones de las mejores prácticas en la prevención de la confidencialidad, integridad y disponibilidad. Para ello, la norma se estructura en dominios que cubren la gestión de la seguridad de la información.
- ISO/IEC 27003: Guía de implementación de SGSI e información acerca del uso del modelo PDCA y de los requisitos de sus diferentes fases.
- ISO/IEC 27004: Especifica las métricas y las técnicas de medida aplicables para determinar la eficiencia y eficacia de la implantación de un SGSI y de los controles relacionados.
- ISO 27005: Es una guía de mejores prácticas para la gestión del riesgo de la seguridad de la información y servirá, por tanto, de apoyo a la ISO 27001 y a la implantación de un SGSI. Incluye partes de la ISO 13335.

- ISO 27006: Especifica los requisitos para acreditación de entidades de auditoría y certificación de sistemas de gestión de seguridad de la información (SGSI).

1.2.3 Factores Críticos de Éxito

1.2.3.1 Definición

(Rockart, 1982), define a los factores críticos de éxito como: “las áreas clave en las que son absolutamente necesarios los resultados favorables para que un gerente alcance sus metas”. Otro concepto es aportado por (Grant, 1996), que define a los factores críticos de éxito como: “los elementos que hacen que una empresa sea exitosa”.

Por otro lado (Eberhagen & Naseroladl, 1992), definen a los factores críticos de éxito como: “aquellas pocas variables que afectan a un administrador, para alcanzar sus metas en su actual o futuras áreas de actividad”.

El uso del concepto de los Factores de Éxito como una metodología de sistemas de información, fue introducido por John Rockart, como un mecanismo para que los ejecutivos pudieran definir sus necesidades de información. Rockart, hizo un bosquejo de lo que podría resultar de una entrevista entre un analista y un CEO.

El primer resultado es un conjunto de factores críticos de éxito para el ejecutivo. Como segundo resultado, las medidas en términos de desempeño para los factores críticos de éxito encontrados.

Rockart especificó que el método se podría utilizar para identificar áreas críticas de interés y para proveer descripciones iniciales de medidas para la información que reflejen estas áreas críticas (Carballo, 1990).

De acuerdo a (Fragoza Ureta, 1994), el método de los factores críticos de éxito básicamente permite la creación de un proyecto fuera de la definición del

problema. Esto se realiza mediante la descomposición de una meta claramente definida en una lista de sub-objetivos llamados factores. La función de los factores críticos de éxito es guiar y enfocar a los directivos hacia las actividades primordiales de su negocio y a pensar en sus necesidades de información más críticas, para el aprovechamiento de los recursos valiosos de una organización, como lo son los financieros, materiales, humanos y de tiempo.

1.2.4 Sistemas de Información

1.2.4.1 Definición

El estudio de los sistemas de información es un campo multidisciplinario, por lo tanto no existe alguna perspectiva o teoría que por sí sola predomine, por consiguiente distintos autores dan a conocer distintas definiciones.

Según (Senn, 1992), es un conjunto de componentes que interaccionan entre sí para lograr un objetivo común.

Para (Whitten, 2003), es una disposición de componentes integrados entre sí cuyo objetivo es satisfacer las necesidades de información de una organización. Es una disposición de personas, actividades, datos, redes y tecnología integrados entre sí con el propósito de apoyar, mejorar las operaciones cotidianas de una empresa, así como satisfacer las necesidades de información las necesidades de información para la resolución de problemas y la toma de decisiones por parte de los directivos de la empresa.

(Laudon & Laudon, 1996), define un sistema de información, como un conjunto de componentes interrelacionados que permiten capturar, procesar, almacenar y distribuir la información para apoyar la toma de decisiones y el control en una institución. Los sistemas de información pueden contener datos acerca de personas, lugares y cosas importantes dentro de la institución y el entorno que la rodea.

1.2.4.2 Tipos de Sistemas de Información

Según (Laudon & Laudon, 1996), los sistemas de información se dividen en:

- Sistemas de Nivel Operativo: Sistemas de información que hacen el seguimiento de las actividades y las transacciones elementales de la organización. (Laudon, 1996, p.15).
- Sistemas de Nivel de Conocimientos: Sistemas de información en los que se apoyan los trabajadores del conocimiento y de la información en una institución. (Laudon, 1996, p.15).
- Sistemas de Nivel Gerencial: Son sistemas de información en los que se apoya el seguimiento, control y toma de decisiones y las actividades administrativas de los administradores de nivel medio. (Laudon, 1996, p.15).
- Sistema de Nivel Estratégico: Sistemas de información que apoyan a las actividades de planeación a largo plazo de los niveles de dirección de la institución. (Laudon, 1996, p.15).

Otra clasificación es propuesta por (Kendall & Kendall, 1997):

- Sistemas de procesamiento de transacciones (TPS): Son sistemas de información computarizados desarrollados para procesar gran cantidad de datos para transacciones rutinarias de los negocios, tales como nomina e inventario. Los TPS eliminan el tedio de las transacciones operacionales necesarias y reducen el tiempo que alguna vez se requirió para ejecutarlas manualmente, aunque las personas deben alimentar datos a los sistemas computarizados.
- Sistemas de automatización de oficina y sistemas de manejo de conocimiento: Al nivel de conocimiento de la organización hay dos clases de sistemas. Los sistemas automatizados de oficina (OAS) que dan soporte a los trabajadores de datos, usan la información para analizarla y transformar datos. Los aspectos familiares incluyen procesamiento de palabras, hojas de cálculo, editor de publicaciones, comunicación mediante correo de voz, correo electrónico y videoconferencias. Los sistemas de manejo de conocimiento (KWS) dan soporte a los trabajadores profesionales, tales como científicos,

ingenieros y doctores, ayudan a crear un nuevo conocimiento que contribuya a la organización o a toda la sociedad.

- Sistemas de información gerencial (MIS): Estos sistemas no reemplazan a los sistemas de procesamiento de transacciones. Los MIS son sistemas de información computarizada que trabajan debido a la interacción resuelta entre personas y computadoras. Requieren que las personas, el software y el hardware trabajen al unísono. Los sistemas de información gerencial producen información que es usada en la toma de decisiones.
- Sistemas de apoyo a decisiones (DSS): Una clase de más alto nivel en los sistemas de información computarizada son los sistemas de apoyo a decisiones (DSS). Es similar al sistema de información gerencial tradicional en que ambos dependen de una base de datos como fuente. Un sistema de apoyo a decisiones se aparta del sistema de información gerencial tradicional, en que enfatiza el apoyo a la toma de decisiones en todas sus fases, estos sistemas están hechos a la medida de la persona o grupo que los usa.
- Sistemas expertos e inteligencia artificial (IA): Los sistemas expertos usan los enfoques del razonamiento de la IA para resolver los problemas que les plantean los usuarios de negocios. Los sistemas expertos son un caso muy especial de un sistema de información, cuyo uso ha sido factible para los negocios a partir de la reciente y amplia disponibilidad de hardware y software tal como las microcomputadoras y sistemas expertos. Un sistema experto, también llamado sistema basado en conocimiento captura en forma afectiva y usa el conocimiento de un experto para resolver un problema particular experimentado en una organización.

1.2.5 Normas Técnicas Peruanas en Seguridad de Información.

1.2.5.1 Norma Técnica Peruana NTP-ISO/ IEC 17799:2004 EDI. Tecnología de la Información[1].

La norma NTP-ISO/IEC 17799, fue una adaptación de la ISO 17799 (actualmente la ISO 27002). La Presidencia del Consejo de Ministros a través de la Oficina Nacional de Gobierno Electrónico, dispone el uso obligatorio Norma Técnica Peruana "NTP – ISO/IEC 17799:2007 EDI, Tecnología de la Información.

Actualmente se encuentra vigente la Norma Técnica Peruana "NTP – ISO/IEC 17799:2007 EDI, Tecnología de la Información: Código de Buenas Prácticas para la Gestión de la Seguridad de la Información" 2ª Edición".

Tabla 1 Evolución de la NTP ISO 17799

Fecha	NTP-ISO/IEC	Resolución Ministerial	Plazo establecido	Observación
23-JUL-2004	17799:2004	224-2004-PCM	18 meses	Cumplir ENE-2006
08-NOV-2005	17799:2004	395-2005-PCM	30-JUN-2006	5 meses más
25-AGO-2007	17799:2007	246-2007-PCM		Sin efecto :2004

La norma NTP-ISO/IEC 17799 tiene 11 dominios que son los siguientes:

- Política de seguridad: Se necesita una política que refleje las expectativas de la organización en materia de seguridad, a fin de suministrar administración con dirección y soporte.
- Aspectos organizativos para la seguridad: Sugiere diseñar una estructura de administración dentro la organización, que establezca la responsabilidad de los grupos en ciertas áreas de la seguridad de la información y un proceso para el manejo de respuesta a incidentes.
- Clasificación y control de activos: Necesita un inventario de los recursos de información de la organización y con base en este

[1] Cambio de dominación de la ISO/IEC 17799:2005 por ISO 27002:2005, Realizado el 01 julio del 2007

conocimiento, debe asegurar que se brinde un nivel adecuado de protección.

- Seguridad de los Recursos Humanos: Establece la necesidad de educar e informar a los empleados actuales y potenciales sobre lo que se espera de ellos en materia de seguridad y asuntos de confidencialidad. También determina cómo incide el papel que desempeñan los empleados en materia de seguridad en el funcionamiento general de la compañía. Se debe implementar un plan para reportar los incidentes.
- Seguridad física y del entorno: Responde a la necesidad de proteger las áreas, el equipo y los controles generales.
- Gestión de comunicaciones y operaciones: Asegurar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información.
- Minimizar el riesgo de falla de los sistemas.
- Proteger la integridad del software y la información.
- Garantizar la protección de la información en las redes y de la infraestructura de soporte.
- Evitar daños a los recursos de información e interrupciones en las actividades de la compañía.
- Control de accesos: Establece la importancia de monitorear y controlar el acceso a la red y los recursos de aplicación como protección contra los abusos internos e intrusos externos.
- Desarrollo y mantenimiento de sistemas: Recuerda que en toda labor de la tecnología de la información, se debe implementar y mantener la seguridad de la información mediante el uso de controles de seguridad de la información en todas las etapas del proceso.
- Gestión de Incidencias: controles para gestionar las incidencias que afectan a la seguridad de Información.
- Gestión de continuidad del negocio: Aconseja estar preparado para contrarrestar las interrupciones en las actividades de la empresa y para proteger los procesos importantes de la empresa en caso de una falla grave o desastre.

- Cumplimiento: Imparte instrucciones a las organizaciones para que verifiquen si el cumplimiento con la norma técnica ISO 17799 concuerda con otros requisitos jurídicos, Requiriéndose una revisión a las políticas de seguridad, al cumplimiento y consideraciones técnicas que se deben hacer en relación con el proceso de auditoría del sistema a fin de garantizar que las empresas obtengan el máximo beneficio.

1.3 Estado del Arte

1.3.1 Factores Críticos de Éxito en Seguridad de Información

1.3.1.1 Estudios Teóricos de los Factores Críticos de Éxito en Seguridad de Información

De acuerdo a (Abu-Zineh, 2006), al citar a (Solms, 1998), señala algunos factores presentados que son a menudo críticos en la implementación de seguridad de Información:

- Los objetivos de seguridad y las actividades deben ser dirigidos sobre la base de los objetivos de la empresa y los requisitos, y llevados por la dirección de la empresa.
- Debe haber un soporte visible y el compromiso de la alta dirección.
- Debe haber un buen entendimiento del riesgo para la seguridad (las amenazas y las vulnerabilidades) en los activos de la compañía, y del nivel de seguridad dentro de la organización.
- La seguridad debe ser difundida eficazmente a todos los directores y empleados
- La orientación exhaustiva sobre la política de seguridad y estándares también debe ser distribuido a todos empleados y contratistas.
- Clasificación de activos y su control.
- Seguridad personal.
- Seguridad física y ambiental.
- Gestión de la red y computadoras.
- Control de acceso a los sistemas.

(Nosworthy, 2000), en su estudio planteó una pregunta "-¿Si no sabemos qué hacer, entonces cómo podemos hacerlo?", trató de encontrar una respuesta convincente para esta pregunta, presentando la política de seguridad de información y algunos factores que tienen un papel importante para el éxito de la Seguridad de Información. Indicando que, estos factores debían ser considerados durante la puesta en práctica en el proceso de aseguramiento de Información (Tabla 2).

Tabla 2 Los factores que deben ser considerados durante la implementación de la Seguridad de Información (Nosworthy, 2000)

FACTOR	PERSPECTIVA DEL AUTOR
Personas	Las personas hacen que las cosas ocurran. Un Sistema de seguridad es inútil sin las personas.
Cultura	La cultura organizativa tiene un papel muy importante en el Sistema de Seguridad. El plan de Seguridad usado para una compañía de fabricación no debe ser el mismo para una compañía de servicios.
Actitud de las personas	Las actitudes de las personas dependen de la manera en que las personas ven la seguridad de información y lo que significa para la organización.
Educación y entrenamiento en seguridad	Los empleados no pueden hacer viable un plan de seguridad de Información sin la educación y entrenamiento suficiente.
Propietario de la información	La propiedad ilustra que la persona que posee la información, tiene la responsabilidad de implementar la seguridad de información.
Descripción del trabajo	La descripción de trabajo debe decir las responsabilidades hacia la seguridad de información, las guías de entrenamiento y los requisitos educativos para el puesto.

Según (INDECOPI, 2007), en referencia al ISO 17799 indica que la experiencia muestra que los siguientes factores suelen ser críticos para el éxito de la implantación de la seguridad de la información en una organización:

a) Una política, objetivos y actividades que reflejen los objetivos del negocio de la organización.
b) Un enfoque para implantar, mantener, monitorear e improvisar la seguridad que sea consistente con la cultura de la organización.
c) El apoyo visible y el compromiso de la alta gerencia.
d) Una buena comprensión de los requisitos de la seguridad, de la evaluación del riesgo y de la gestión del riesgo.
e) La convicción eficaz de la necesidad de la seguridad a todos los directivos y empleados.
f) La distribución de guías sobre la política de seguridad de la información de la organización y de normas a todos los empleados y contratistas.

g) Aprovisionamiento para financiar actividades de gestión de seguridad de la información.
h) La formación y capacitación adecuadas.
i) Establecer un efectivo proceso de gestión de incidentes de la seguridad de información.
j) Un sistema integrado y equilibrado de medida que permita evaluar el rendimiento de la gestión de la seguridad de la información y sugerir mejoras.

1.3.1.2 Estudios Empíricos de los Factores Críticos de Éxito en Seguridad de Información

(Bjorck, 2002), plantea uno de los primeros estudios que presenta hallazgos empíricos sobre los factores críticos de éxito para implementar seguridad de información, el estudio se realizó con consultores de seguridad y auditores, determinando dos frameworks para seguridad:

a) El primero, desde la perspectiva de los auditores, que identifican seis factores críticos de éxito: compromiso de la gerencia, valoración de la necesidad de seguridad de información, enfoque holístico, personal motivado, acceso a competencias externas, proyecto bien estructurado, que se resumen en la figura 2.

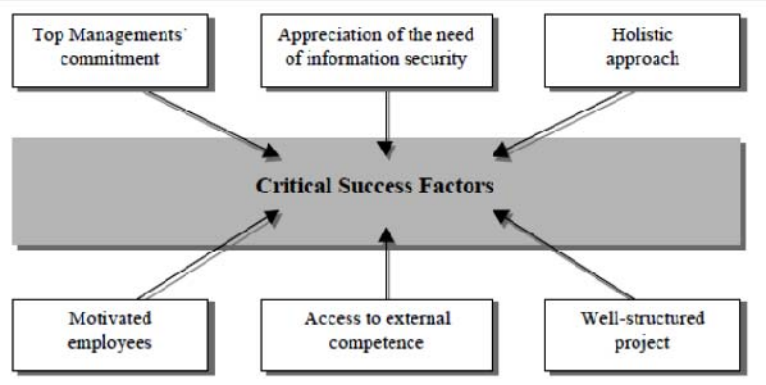

Figura 2 Factores Críticos para la Implementación y Certificación de SGSI desde la perspectiva de los auditores (Bjorck, 2002)

b) Desde la perspectiva de los consultores, el estudio establece un conjunto de seis factores críticos de éxito como son: la capacidad de

gestión del proyecto, capacidad de mando, capacidad financiera, capacidad analítica, capacidad comunicativa, capacidad gerencial, que se resumen en la figura 3.

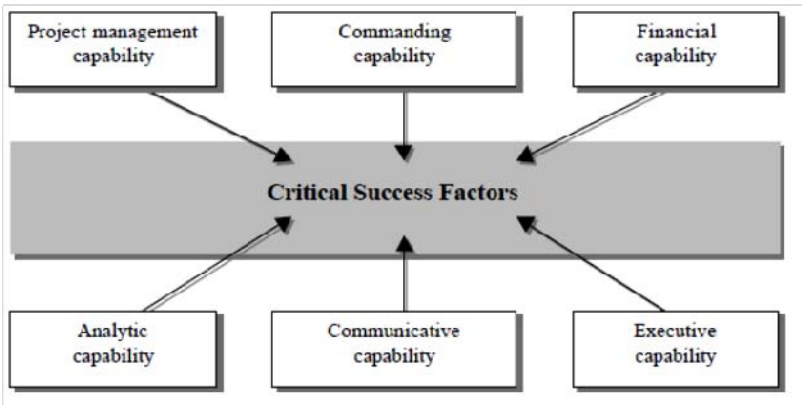

Figura 3 Factores Críticos para la Implementación y Certificación de SGSI desde la perspectiva de los consultores en seguridad (Bjorck, 2002)

Dichos resultados están principalmente enfocados a la aplicación del estándar BS 7799, que es el origen del ISO 17799 (Bjorck, 2002).

(Partida & Ezingeard Henley, 2007), en el estudio acerca de Factores Críticos de Éxito y Requerimientos para lograr beneficios en el negocio a partir de la Seguridad de Información. Indican que, la seguridad de información, al considerarse un factor estratégico de toda organización, y que éste éxito depende del entendimiento claro de la gestión del procesos, así como un alineamiento entre los objetivos del negocio y las políticas de seguridad de información. Como tal, los autores, plantean un conjunto de factores críticos que se resumen en la Tabla 3.

Tabla 3 Factores Críticos de Éxito (Partida & Ezingeard Henley, 2007)

Factores Críticos de Éxito	**Referencia**
Tema 1: Proceso de Gestión y valor	
Obtener el compromiso de dirección	ISO (2004 and 2005); COSO (2004); Appel (2005) y Ezingeard et al., (2004)
Establecer un programa de mejorar la administración de seguridad en la empresa y hacer que se cumpla.	Straub (1998), ISF (2005a).
Seguir un estándar.	May (2002), Von Solms (2005a).
Comunicar el valor de la seguridad de información en la empresa usando un	Scholtz (2004b and 2004c), Coles y Moulton (2003).

lenguaje de riesgos común.	
Determinar la propiedad de riesgo indudablemente.	Coles y Moulton (2003).
Tema 2: Alineamiento	
Reflejar los objetivos de la empresa en elementos de seguridad de información.	Birchall et al. (2004), Scholtz (2004a), ISO (2005).
Conectar la seguridad de información con los sistemas de información y la estrategia en conjunto.	Booker (2006), Leskela et al. (2005), Birchall et al. (2003).
Ser consecuente dentro de la cultura organizativa.	Birchall et al. (2004), Scholtz (2004a), ISO (2005).

En el año 2008, (Al-Awadi & Renaud, 2008), realizan una investigación sobre Factores Críticos para la Implementación de Seguridad en Organizaciones. El estudio identifica los factores críticos de éxito relacionados a la implementación de seguridad en sistemas de información como parte de las organizaciones. Se muestra dichos factores desde la perspectiva de los expertos, además de un análisis cualitativo y cuantitativo de los empleados en cuanto a sus experiencias, con la particularidad que el estudio se realizó para entidades gubernamentales.

Los FCE encontrados son:

a) Conciencia y entrenamiento: Al respecto, (Dhillon, Managing and Controlling Computer Misuse, 1999), indican que las organizaciones deben contar con programas de educación y entrenamiento para garantizar el éxito esperado de la implementación de políticas de seguridad de información. Que es confirmado por (Katz, 2005), al indicar que, el mayor desafío en cuanto a seguridad de información son los empleados.
b) Soporte de la Gerencia: (Fung & Jordan, 2002), indican que en muchos casos la gerencia no se interesa por la medición y calidad de seguridad de información en la organización debido a que piensa que es una labor del departamento de T.I. que debe seleccionar el hardware y software necesario y así mantener a la organización segura. Descuidando así el enfoque estratégico de la seguridad.

c) Presupuesto: El estudio también muestra la vital importancia del presupuesto, pues para lograr una adecuada seguridad de información se requieren los fondos adecuados.
d) Fortalecimiento y adaptación de las Políticas de Seguridad de Información: Las políticas de seguridad de información son la clave para una buena gestión de seguridad de información, más aun como parte de un plan de identificación y aceptación. Por lo tanto, son el primer paso para medir y mitigar las amenazas.
e) La misión de la organización: Bajo el presente estudio algunos expertos manifestaron que, las organizaciones con metas y objetivos claros son esenciales para implementación de políticas de seguridad, y además que cuenten con una cultura de seguridad de información en la organización incidirá en su éxito.

1.3.2 Modelos de Éxito relacionados con la Seguridad en Sistemas de Información

1.3.2.1 Modelo de Delone y McLean (Delone & Mclean, Information systems success: The quest for the dependent variable, 1992)

(Delone & Mclean, Information systems success: The quest for the dependent variable, 1992), realizaron una revisión de cerca de 180 investigaciones publicadas durante el periodo de 1981-1992, que se basan en el trabajo de los tres niveles de comunicación de (Shannon & Weaver, 1949) para crear un modelo de éxito de Sistemas de Información (Mason, 1978).

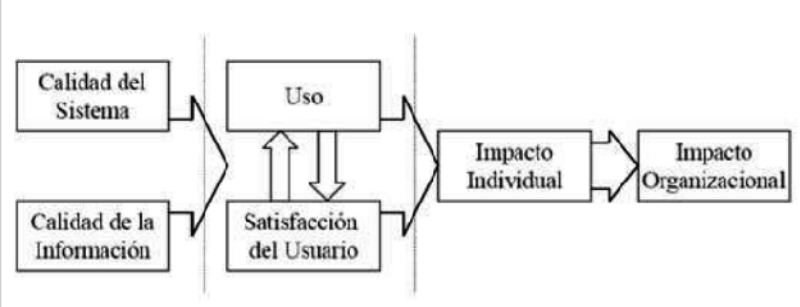

Figura 4: Modelo de éxito de los SI; DeLone y McLean, 1992

Según (Ballantine & etal, 1996), (Seddon & Kiew, 1996), (McGill, Hobbs, & Klobas, 2003), dicho modelo genera dos contribuciones al entendimiento del éxito de los Sistemas de Información (SI):

- Provee un esquema para clasificar la multiplicidad de medidas de éxito de los SI usados en la literatura en tan sólo seis dimensiones;
- El modelo sugiere interdependencias "temporales y causales" entre las categorías.

1.3.2.2 Modelo de DeLone y McLean (Delone & Mclean, The DeLone and McLean model of information systems success: A Ten-Year update, 2003)

Los autores originales, al realizar una revisión de las referencias hechas a su publicación original, encontraron 285 citas en artículos de revistas y congresos del modelo D&M durante el período de 1993 hasta mediados de 2002 (Delone & Mclean, The DeLone and McLean model of information systems success: A Ten-Year update, 2003); para la actualización del año 2003, verificaron y analizaron más de 100 artículos en las revistas de investigación más importantes a fin de informar de la revisión de la medición de éxito de los SI, y basados en las consideraciones de procesos y causales, las seis dimensiones de éxito propuestas están más interrelacionadas que independientes.

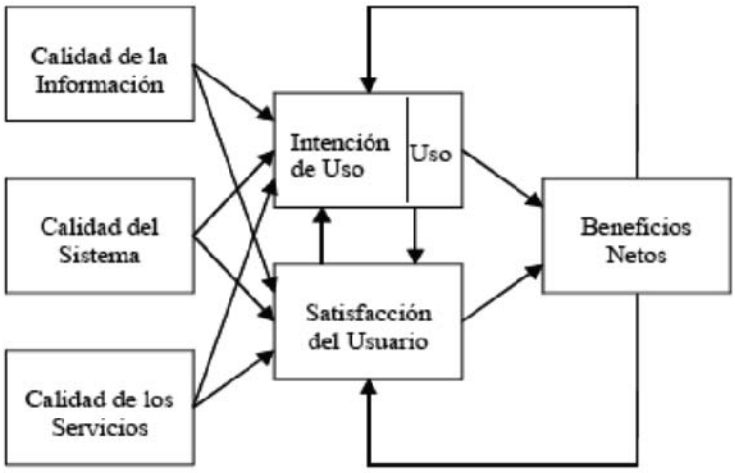

Figura 5: Modelo de éxito de los SI de D&M; Delone y McLean (2003)

El modelo del 2003 contiene seis dimensiones, éstas están interrelacionadas, resultando en un modelo de éxito que indica que la causalidad fluye en la misma dirección como el proceso de información: "calidad de la información", "calidad del sistema", "calidad de los servicios", "intención de uso/uso", "satisfacción del usuario" y "beneficios netos"; y porque las investigaciones han encontrado soporte en las relaciones del modelo (Rai, Lang, & Welker, 2002). Esta actualización del modelo incluye flechas (ligas) para demostrar las asociaciones propuestas entre las dimensiones de éxito en un sentido de proceso, pero no muestra el signo positivo o negativo para aquellas asociaciones en un sentido causal; para la actualización los autores anotan:

- Las tres principales dimensiones: "calidad de la información", "calidad del sistema" y "calidad del servicio", deben medirse o controlarse por separado, porque en forma unida, afectan subsecuentemente el uso y la satisfacción del usuario.
- La "intención de uso" puede ser una medida alternativa en algunos contextos. Esta dimensión es una actitud, aplicada normalmente en el ámbito social-psicológico (Ajzen & Fishbein, 1980), mientras que el "uso" es una conducta. El "uso" y la satisfacción del usuario están firmemente relacionados, en esta relación el "uso" debe preceder la "satisfacción del usuario" en un sentido de proceso. En la experiencia positiva con el "uso", este conducirá hacia una gran "satisfacción del usuario" en un

sentido causal. Similarmente, la “satisfacción del usuario” dirige hacia el incremento de la “intención de uso” así como el “uso”, y como resultado del “uso” y la “satisfacción del usuario”, los beneficios netos suelen llegar.

Para no complicar tanto el modelo, agruparon todas las medidas de “impacto” en la variable “beneficios netos”. (Delone & Mclean, Information systems success, 2002), usan el término “beneficios netos” (unión de impacto individual y organizacional) porque el término original de “impacto” puede ser positivo o negativo, que puede conducir a una confusión. De esta manera, los “beneficios netos” son probablemente, la descripción exacta de la variable final de éxito.

Es necesario aclarar que los “beneficios netos” pueden ser apreciados de diferente forma por los investigadores y estudiosos, así como los factores de éxito, por ello, los autores dejan “libre” la interpretación y uso de este aspecto, a su nuevo modelo (Delone & Mclean, The DeLone and McLean model of information systems success: A Ten-Year update, 2003) añaden la dimensión de “calidad del servicio” tomando como base las investigaciones revisadas.

1.3.2.3 Modelo de la eficacia de Seguridad en Sistemas de Información (Kankanhalli, Hock-hai, Bernard, & Kwok-kee, 2003)

(Kankanhalli, Hock-hai, Bernard, & Kwok-kee, 2003), desarrollaron un modelo de integración de la eficacia de seguridad de información. Empresas singapurenses pequeñas y medianas fueron encuestadas para revisar la habilidad de las medidas proteger contra el mal uso no autorizado o deliberado de posesiones de información por empleados. Factores organizativos como el tamaño organizativo el soporte de dirección superior, y el tipo de la industria influyeron en las medidas de seguridad de información fuertemente. El tamaño organizativo tiene el papel crítico para adoptar el sistema de seguridad de información, las organizaciones más pequeñas padecen de falta de recursos humanos, apoyo financiero y destrezas técnicas. Por lo tanto, las organizaciones más pequeñas cosechan pocos beneficios a diferencia de las organizaciones de mayor tamaño al implementar seguridad de información.

El soporte de la dirección superior era también el factor crítico en la puesta en práctica exitosa del Sistema de Seguridad. El soporte de la dirección representaba la orientación durante la planificación, la participación durante el despliegue. Además, la alta dirección tiene el papel principal en la actitud del usuario hacia el uso de políticas de seguridad. Las organizaciones en industrias diferentes son diferentes en relación con sus requisitos, usos y papel de la seguridad de información.

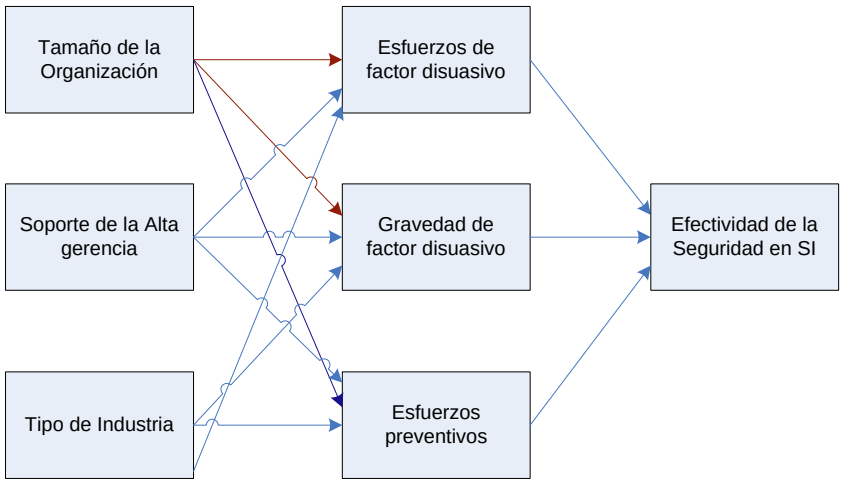

Figura 6 Modelo de la eficacia de seguridad de información (Kankanhalli, Hock-hai, Bernard, & Kwok-kee, 2003)

Este modelo integra tres factores organizativos (el tamaño de la organización, el soporte gerencial y el tipo de industria u organización). Este modelo demuestra cómo trabajan en conjunto para tener eficacia seguridad de sistema de información basada en los esfuerzos de los factores disuasivo y de prevención (Abu-Zineh, 2006).

1.3.2.3 Un Framework para Evaluar la Seguridad en Sistemas de Información (Chaulaa, Yngströmb, & Kowalskic, 2005)

La evaluación de la seguridad en sistemas de información, es un proceso que involucra identificar, reuniendo y analizando la funcionalidad asegurando determinado nivel de criterio, lo que significa medir el cumplimiento de objetivos particulares, para tal efecto se propone un marco de referencia que parte de un sistema no confiable y propone un sistema confiable.

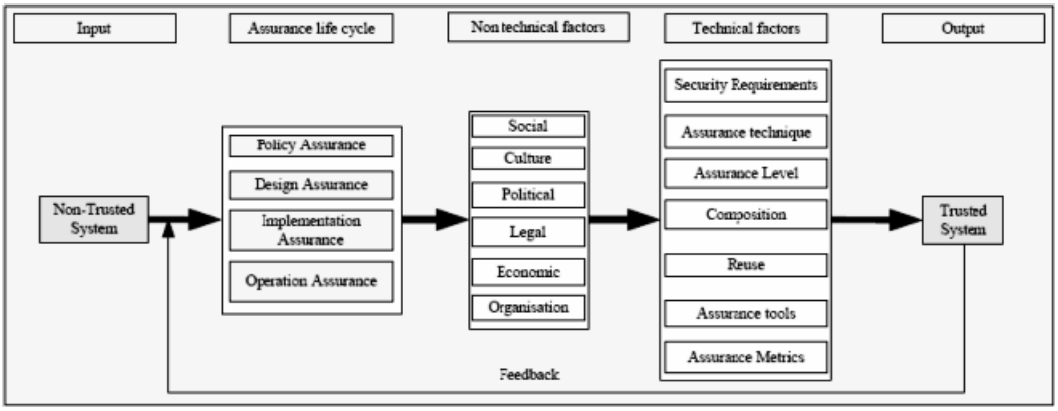

Figura 7: Componentes Clave del Framework de aseguramiento de la seguridad de información.

1.3.2.4 Factores Críticos de Éxito e Indicadores para medir la efectividad de la Gestión de Seguridad de Sistemas de Información (Torres, Sarriegi, Santos, & Serrano, 2006)

El estudio sostiene que existe un débil soporte a los factores críticos de éxito universalmente aceptados, lo que constituye un desafío. La administración de seguridad de información eficaz requiere un enfoque especial sobre identificar los factores de críticos éxito (FCEs) cuando se implementa y asegura un sistema de seguridad de información, para lo cual se muestra un conjunto de 12 FCE identificados, así como 76 indicadores que proveen información valuable para medir el nivel de seguridad, a partir del modelo 3D de "queso suizo" de (Reason, 1997), donde se define tres dimensiones básicas:

a) Controles técnicos: Herramientas de hardware y software que restringen el acceso para edificios, habitaciones, sistemas de computadora y programas para evitar accesos no autorizados o usos incorrectos (antivirus, cortafuegos, documentos de identidad, copias de seguridad, etcétera).
b) Controles formales: Conjunto de políticas y procedimientos para establecer y asegurar el uso eficaz de controles técnicos. Por ejemplo, identificar los roles, las responsabilidades, poner en funcionamiento indicadores y entrenamiento de empleados.
c) Controles informales: Las intervenciones que se relacionan con el despliegue de la seguridad de información digital a través del personal aumentando la fuerza de voluntad de los usuarios.

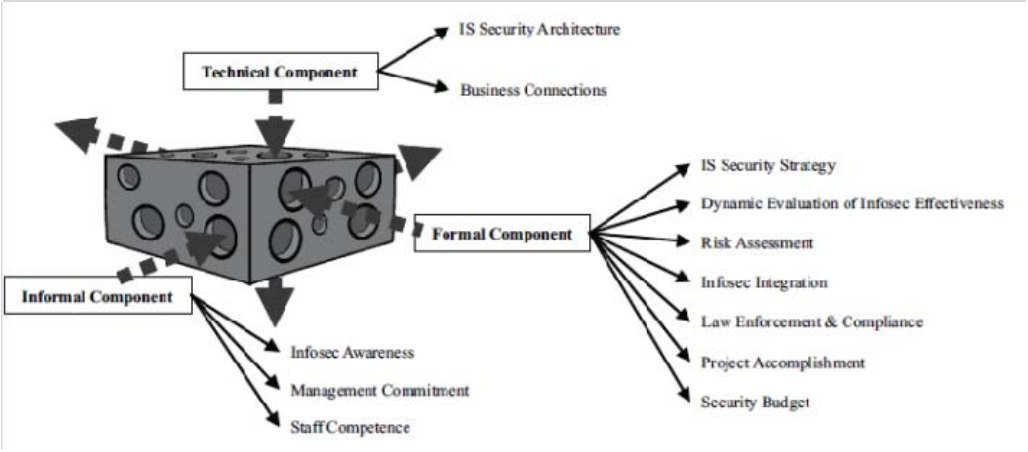

Figura 8 Factores críticos de éxito bajo el modelo 3D de Reason.

Los autores (Torres & Sarriegui, 2003), manifiestan que después de examinar algunas definiciones, la seguridad de información consiste en tres componentes fundamentales: la tecnología, los procesos y las personas, proponiendo una definición "La seguridad de información es un Sentido bien informado de la seguridad de que los riesgos de información y los controles técnicos y formales e informales están en balance dinámico" (Dhillon, Managing and Controlling Computer Misuse, 1999) (Dhillon, Violating of Safeguards by Trusted Personal and Understanding Related Information Security Concerns., 2001) (Dhillon & Moores, Computer crimes: Theorizing About the Enemy Within, 2001).

1.3.2.5 Modelo de Éxito de Seguridad de Sistemas de Información, para el contexto de Gobierno Electrónico (Dunkerley & Tejay, 2009).

El estudio se construyó tomando como base el trabajo de (Shannon & Weaver, 1949), (Mason, 1978) y (Delone & Mclean, The DeLone and McLean model of information systems success: A Ten-Year update, 2003) para desarrollar un modelo que pueda predecir el éxito con la seguridad en una organización. (Delone & Mclean, Information systems success: The quest for the dependent variable, 1992), extendieron los estudios de (Shannon & Weaver, 1949) y (Mason, 1978), para desarrollar un modelo que predice el éxito de los Sistemas de Información, (Shannon & Weaver, 1949) identificaron tres constructores involucrados en la efectividad de las comunicaciones. El primero el nivel técnico, de las comunicaciones que involucra la precisión y eficiencia del

sistema de comunicación que produce información. El segundo, el nivel semántico relacionado al éxito de la información en transmitir la intención del significado que es enviado por el transmisor al receptor. Finalmente el nivel de efectividad es el resultado de la información actual que se tiene en el comportamiento del usuario. (Mason, 1978), adaptó el trabajo (Shannon & Weaver, 1949) para enfocarlo a los sistemas de información. A partir de ello, considerando una revisión de varios autores se plantea la Tabla 4, que muestra las dimensiones de seguridad para los Sistemas de Información según (Dunkerley & Tejay, 2009).

Tabla 4: Dimensiones de la Seguridad de Información para los diferentes niveles de comunicación

Niveles de Comunicación	Dimensiones de Seguridad en SI	Referencias
Técnico	Integridad de la Información Aseguramiento de los Sistemas de Información Continuidad del negocio	Anderson (1972), Denning (1987), Sandhu et al. (1996), Daniels & Spafford (1999).
Semántico	Intención del usuario Experiencia del Usuario	Dhillon (2001), Siponen (2001), Trompeters & Eloff (2001), Schultz (2002), Vroom & von Solms (2004), Stanton et al. (2005), Dinev et al. (2008).
Efectividad	Beneficios de la Seguridad en S.I.	Anderson (2001), Gordon and Loeb (2002), Campbell et al. (2003), Hovav and D'Arcy (2003), Tanaka et al. (2005), Arora et al. (2006).

Tomando como base tales dimensiones, los autores proponen el modelo de Éxito de la seguridad de información, que principalmente está basado en el modelo original de (Delone & Mclean, Information systems success: The quest for the dependent variable, 1992).

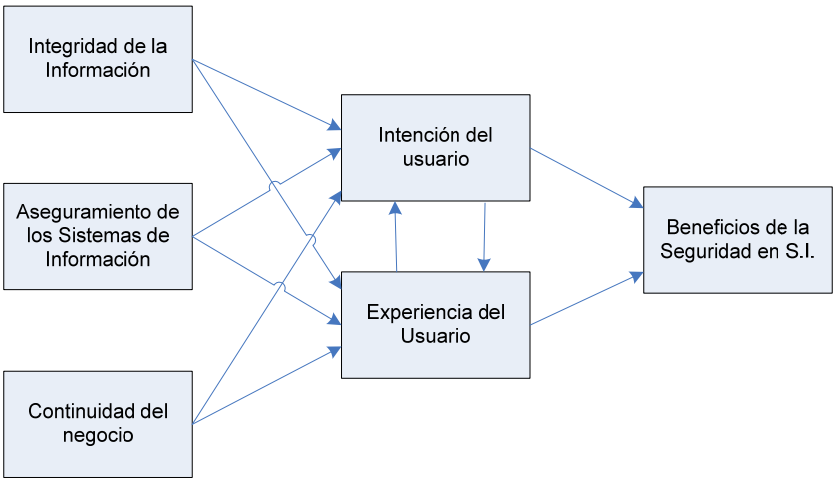

Figura 9: modelo de Éxito de la seguridad de información

1.3.3 Modelos de Intención y Aceptación del Usuario de Tecnología

1.3.3.1 Modelo de Aceptación de la Tecnología original (TAM)(Davis F. D., 1986)

El modelo TAM fue desarrollado por (Davis F. D., 1986). Según (Morlán Santa Catalina, 2010), el Modelo de Aceptación Tecnológica está basado en la Teoría de la Acción Razonada[2] (Fishbein & Ajzen, 1975) (Ajzen & Fishbein, 1980). En consonancia con esta teoría, el Modelo de Aceptación Tecnológica, postula que el uso de una tecnología, o de una innovación informática, está determinado por la intención de uso de dicha tecnología.

Las relaciones del Modelo de Aceptación Tecnológica original (TAM, Technology Acceptance Model) se muestran en la Figura 10. El modelo conocido como TAM explica la aceptación individual de una tecnología informática sobre la base de cuatro variables: la Utilidad percibida, la Facilidad de uso percibida, la Actitud hacia el uso de la tecnología y la Intención de uso.

[2] La Teoría de la Acción Razonada (Theory of Reasoned Action), es un modelo de la Psicología Social desarrollado por Martin Fishbein y Icek Ajzen para la predicción y comprensión de la conducta humana. A diferencia de otros 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) (Morlán Santa Catalina, 2010).

La Utilidad percibida se define como el grado en que una persona piensa que su rendimiento mejorará con el uso de un sistema determinado; y la Facilidad de uso percibida es el grado en que un individuo cree que el uso de la tecnología está libre de esfuerzo. El modelo establece que ambas variables determinan directamente la adopción. Este modelo sugiere también, que la Facilidad de uso percibida influye a su vez en la Utilidad percibida, debido a que las tecnologías que son fáciles de usar pueden ser más útiles. De hecho, el esfuerzo que se ahorra debido al fácil uso de los sistemas se puede redirigir a realizar otro trabajo con el mismo esfuerzo total. Igualmente, cuanto más sencillo es interactuar con un sistema, mayor será el sentido de eficacia, es decir aumentará la auto eficacia (Bandura, 1982).

A su vez, la Actitud hacia el uso de la tecnología es la reacción emocional (gusta o no) ante el uso de un sistema específico. Esta actitud se ve condicionada tanto por la Utilidad percibida como por la Facilidad de uso percibida. Y como se indica, tanto la Utilidad percibida como la Actitud hacia el uso de la tecnología influyen positivamente en la Intención de uso, que a su vez, predice el Uso de la tecnología. La Facilidad de uso percibida tiene un efecto indirecto sobre la Intención de uso de un individuo a través de la Utilidad percibida y de la Actitud hacia el uso de la tecnología (Morlán Santa Catalina, 2010).

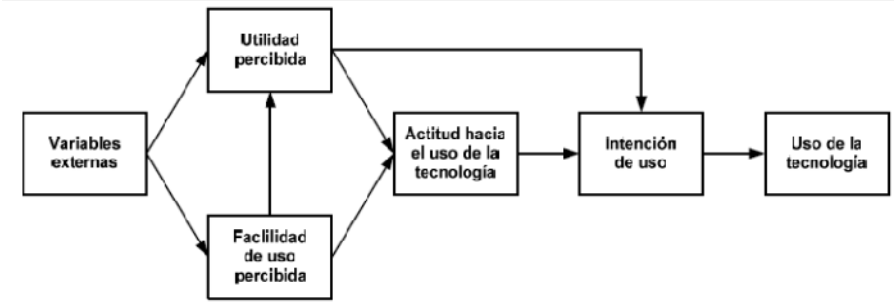

Figura 10 Modelo de Aceptación Tecnológica original (Davis F. , 1989)

El Modelo de Aceptación Tecnológica, considera que se producen influencias de Variables externas sobre la adopción, como la documentación o el asesoramiento al usuario, y que estas operan a través de la Utilidad percibida y la Facilidad de uso percibida. Por lo tanto, se supone que las creencias de los

individuos, al menos en parte, filtran los efectos de las variables organizacionales, sociales e individuales (Figura 10).

Además, la Utilidad percibida y la Facilidad de uso percibida son particularmente importantes para explicar el comportamiento de la Intención de uso de los sistemas de información (Amoako-Gyampah & Salam, 2004); y la comprensión de estas dos variables permite el diseño de intervenciones efectivas para aumentar el uso de nuevos sistemas informáticos (Venkatesh & Davis, A theoretical extension of the technology acceptance model: four longitudinal field studies, 2000).

1.3.3.2 Primera Ampliación del Modelo de Aceptación Tecnológica (TAM2) (Venkatesh & Davis, A theoretical extension of the technology acceptance model: four longitudinal field studies, 2000)

(Venkatesh & Davis, A theoretical extension of the technology acceptance model: four longitudinal field studies, 2000), ampliaron el Modelo de Aceptación de Tecnología original para explicar la Utilidad percibida y la Intención de uso en términos de influencia social y procesos cognitivos. Lo primero que destaca de esta nueva versión, conocida como TAM2, es la eliminación de la variable Actitud hacia el uso de la tecnología estableciéndose la Utilidad percibida y la Facilidad de uso percibida como antecedentes directos de la Intención de uso constituyendo lo que actualmente se conoce como núcleo del Modelo de Aceptación Tecnológica (Figura 11). Tras una serie de investigaciones (Venkatesh & Davis, A theoretical extension of the technology acceptance model: four longitudinal field studies, 2000) concluyeron que las medidas de ajuste de la variable Actitud hacia el uso de la tecnología, no podían ser consideradas como suficientes para mantener ese concepto dentro del modelo. Además argumentan que la relación directa entre la Utilidad percibida y la Intención de uso está basada en reglas de decisión cognitivas para mejorar el rendimiento laboral, por lo que decidieron prescindir del componente emocional representado por la variable Actitud hacia el uso de la tecnología.(Morlán Santa Catalina, 2010).

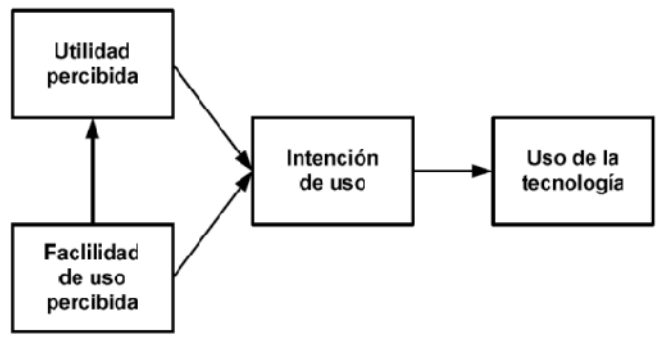

Figura 11 Núcleo del Modelo de Aceptación Tecnológica (Venkatesh & Davis, A theoretical extension of the technology acceptance model: four longitudinal field studies, 2000) adaptado (Morlán Santa Catalina, 2010)

Entre las variables incluidas en TAM2 destaca la Norma subjetiva como condicionante de la Intención de uso en el caso de escenarios obligatorios. La Norma subjetiva, es la medida en que un individuo considera importante que otros piensen que dicho individuo debe utilizar la tecnología en cuestión. Está adaptada a partir de dos teorías, de la Teoría de la Acción Razonada y de la Teoría del Comportamiento Planificado[3](Ajzen I. , 1991). Davis ya había criticado su propio modelo señalando la omisión de dicha variable de la Psicología Social, subrayando la dificultad para distinguir si el comportamiento de uso, está causado por la influencia de los grupos de referencia o por las actitudes, e indicando que necesitaba mayor investigación.

Sin embargo, y curiosamente, a pesar de la importancia de la influencia social como un indicador de la intención y del comportamiento en determinadas situaciones, se ha demostrado que su importancia está condicionada por la Experiencia en el uso tecnología; es decir, las opiniones de los demás tienen peso en las decisiones del uso de la tecnología si antes se ha adquirido la experiencia suficiente como para sentirse seguro de cara a tomar una decisión

[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 es 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 (Morlán Santa Catalina, 2010).

independiente(Venkatesh, Morris, Davis, & Davis, 2003) (Morlán Santa Catalina, 2010) .

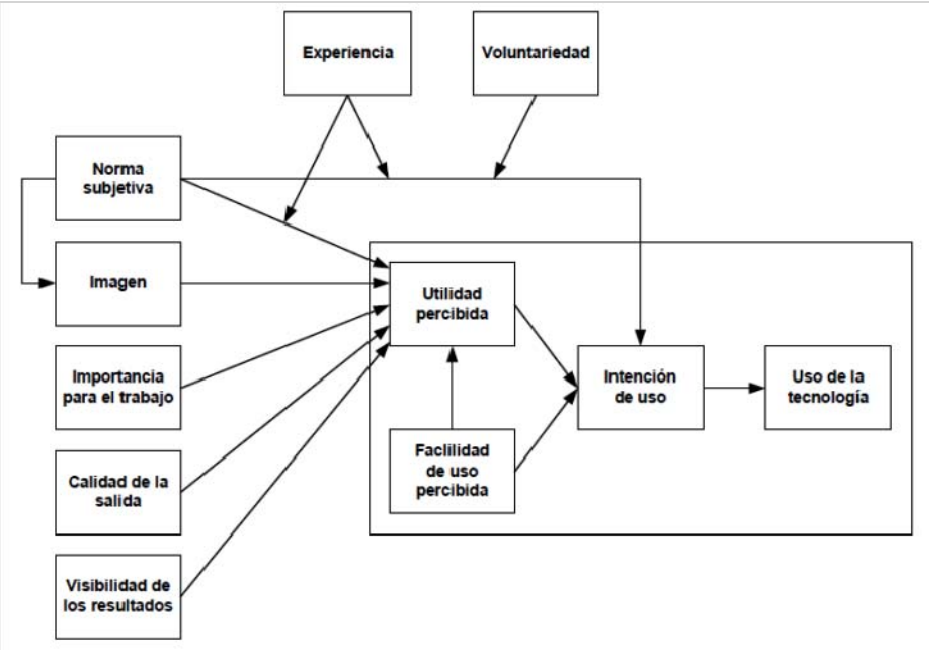

Figura 12 Ampliación del Modelo de Aceptación Tecnológica, TAM2. (Venkatesh & Davis, A theoretical extension of the technology acceptance model: four longitudinal field studies, 2000) adaptado (Morlán Santa Catalina, 2010)

(Venkatesh & Davis, A theoretical extension of the technology acceptance model: four longitudinal field studies, 2000), concluyen que los enfoques de introducción de nuevos sistemas basados en su uso obligatorio, parecen ser menos eficaces a lo largo del tiempo que la utilización de la influencia social para orientar los cambios positivos en la utilidad percibida y sugieren que se deben desarrollar prácticas alternativas sobre la base de la interacción social, como el aumento de la credibilidad de la fuente de información o el diseño de campañas de comunicación para elevar el prestigio asociado al uso del sistema. Y que desde un punto de vista más instrumental, además de diseñar sistemas para adaptar mejor las necesidades de relevancia para el trabajo, mejorar la calidad de la salida, o hacer más fácil su uso, sugieren que las intervenciones prácticas para aumentar la visibilidad de los resultados, como demostraciones prácticas a los usuarios de la efectividad de un nuevo sistema, pueden proporcionar un impulso importante para una aceptación cada vez mayor.

1.3.3.3 Teoría de la Acción Razonada (TRA) (Ajzen & Fishbein, 1980)

La Teoría de la Acción Razonada (Theory of Reasoned Action), es un modelo de la Psicología Social desarrollado por Martin Fishbein y Icek Ajzen (Ajzen & Fishbein, 1980) para la predicción y comprensión de la conducta humana. A diferencia de otros 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. Por norma subjetiva se entiende como la percepción que un individuo tiene de que los demás consideran que debe realizar o no la conducta en cuestión (la presión del grupo). La Teoría de la Acción Razonada considera que el mejor indicador del comportamiento es la intención porque muestra el esfuerzo que los individuos están dispuestos a invertir con el fin de desarrollar una acción. En definitiva, esta teoría se basa en la suposición de que los seres humanos son normalmente racionales y hacen un uso sistemático de la información de que disponen; y que la intención se sitúa en el equilibrio entre lo que se piensa que se debe hacer y lo que se percibe que los otros piensan que se debe hacer. (Morlán Santa Catalina, 2010).

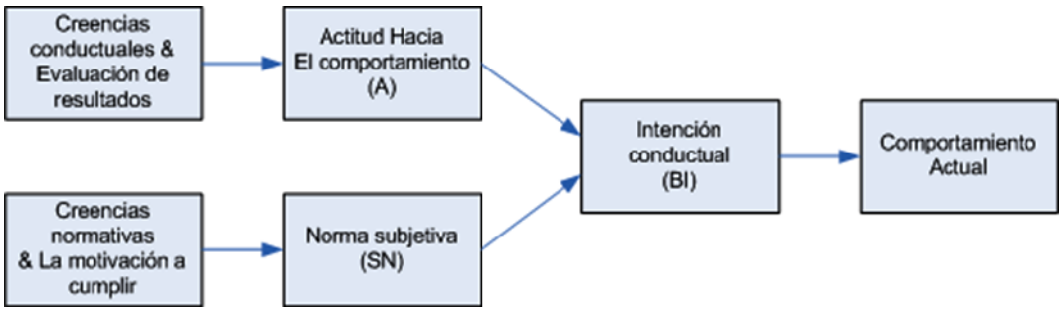

Figura 13 Modelo de la Teoría de la Acción Razonada basado en (Fishbein & Ajzen, 1975)

1.3.3.4 Teoría del Comportamiento Planificado (TPB) (Ajzen I. , 1991)

La Teoría del Comportamiento Planificado (Theory of Planned Behavior), es una extensión de la Teoría de la Acción Razonada propuesta por Icek Ajzen (Ajzen I. , 1991). 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 es 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.

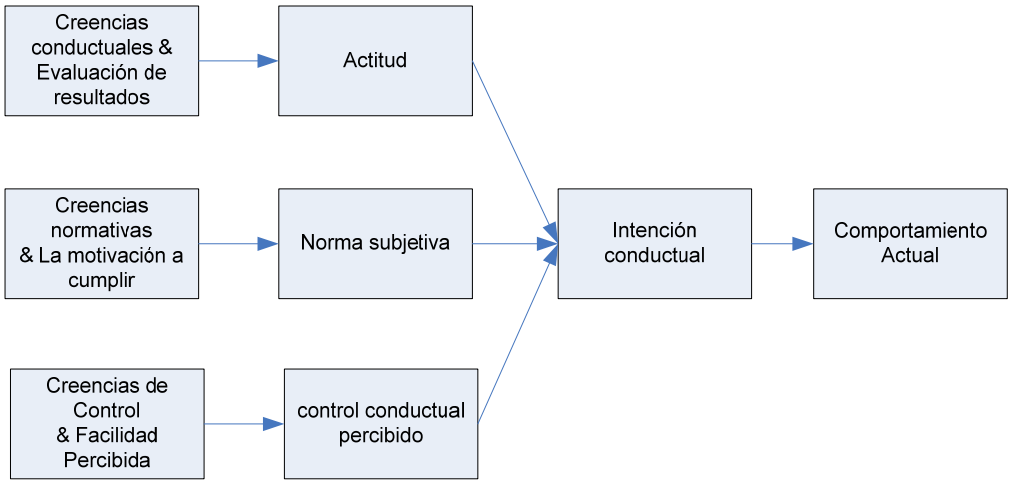

Figura 14 Teoría del Comportamiento Planificado (Ajzen I. , 1991)

1.4 Marco Conceptual

a. Amenazas

El acceso de forma indebida a los datos o información sensible por usuarios no autorizados dentro de una organización también se puede dar por medios ambientales (ISO, 2004).

b. Confidencialidad

Acceso a la información por parte únicamente de quienes estén autorizados.

Se entiende por confidencialidad el servicio de seguridad, o condición, que asegura que la información no pueda estar disponible o ser descubierta poro para personas, entidades o procesos no autorizados. La confidencialidad, a veces denominada secreto o privacidad, se refiere ala capacidad del sistema para evitar que personas no autorizadas puedan acceder a la información almacenada en él. La confidencialidad asegura la protección en base a disposiciones legales o criterios estratégicos de información privada, tal como datos de las nóminas de los empleados, documentos internos sobre estrategias, nuevos productos o campañas, etc. Este aspecto de la seguridad es particularmente importante cuando hablamos de organismos públicos, y más concretamente aquellos relacionados con la defensa (INDECOPI, 2007).

c. Clasificación

Técnica que se utiliza para la identificación, agrupación y distribución sistemática de documentos o cosas semejantes, con características comunes o sistema determinado y que pueden ser con posterioridad diferenciadas según su tipología fundamental. Dicho proceso se aplica de acuerdo a un esquema lógico predeterminado para señalar su ubicación. Cuando se trata de libros o documentos se llama clasificación bibliográfica o documental (Villena Aguilar, 2006).

d. Disponibilidad

Acceso a la información y los sistemas de tratamiento de la misma por parte de los usuarios autorizados cuando lo requieran.

Se entiende por disponibilidad, el grado en que un dato está en el lugar, momento y forma en que es requerido por el usuario autorizado. La situación que se produce cuando se puede acceder a un Sistema de Información en un periodo de tiempo considerado aceptable. Un sistema seguro debe mantener la información disponible para los usuarios. Disponibilidad significa que el sistema, tanto hardware como software, se mantienen funcionando eficientemente y que es capaz de recuperarse rápidamente en caso de fallo (Harris, 2004).

e. Factores Críticos de Éxito (FCE)

Las áreas clave en las que son absolutamente necesarios los resultados favorables para que un gerente en particular alcance sus metas (Rockart, 1982).

Los elementos que hacen que una empresa sea exitosa (Grant, 1996).

Los FCE son variables que se deben tomar en cuenta antes y durante la realización de un proyecto, ya que aportan información valiosa para alcanzar las metas y objetivos de la empresa. Sin embargo, la determinación de que es o que no es un FCE se basa en lo general de un juicio subjetivo, ya que no existe una fórmula para determinar los FCE con claridad. Según (King & Burgess, 2005)

f. Integridad

El concepto de integridad significa que el sistema no debe modificar o corromper la información que almacene, o permitir que alguien no autorizado lo haga. Esta propiedad permite asegurar que no se ha falseado la información. Por ejemplo, que los datos recibidos o recuperados son exactamente los que fueron enviados o almacenados, sin que se haya producido ninguna modificación, adición o borrado. De hecho el problema de la integridad no sólo se refiere a modificaciones intencionadas, sino también a cambios accidentales o no intencionados.

En el ámbito de las redes y las comunicaciones, un aspecto o variante de la integridad es la autenticidad (Harris, 2004).

Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso. La información sólo pueden ser creados y modificados por los usuarios autorizados. Se trata de proporcionar los medios para verificar que el origen de los datos es el correcto, quién los envió y cuándo fueron enviados y recibidos.

g. IEC

Comité Electrotécnico Internacional (International Electrotechnical Committee), organismo internacional que se ocupa de normalizaciones y seguridad Informática.

h. Implementación

Una implementación o implantación es la realización de una aplicación, o la ejecución de un plan, idea, modelo científico, diseño, especificación, estándar, algoritmo o política.

En ciencias de la computación, una implementación es la realización de una especificación técnica o algoritmos como un programa, componente software, u otro sistema de cómputo. (Definiciones, 2010)

i. Intención de la Persona

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) (Ajzen & Fishbein, 1980).

j. ISO

Es el organismo encargado de promover el desarrollo de normas internacionales de fabricación, comercio y comunicación para todas las

ramas industriales a excepción de la eléctrica y la electrónica. Su función principal es la de buscar la estandarización de normas de productos y seguridad para las empresas u organizaciones a nivel internacional. Como por ejemplo el estándar ISO 17799 para la seguridad de información (ISO, 2010).

k. Modelo

Se define como el arquetipo o punto de referencia para imitarlo o reproducirlo (Real Academia Española, 2011). Esquema teórico de un sistema o de una realidad compleja.

l. Modelo Matemático

Un modelo matemático es un tipo de modelo científico, que utiliza algún tipo de formulismo matemático para expresar relaciones, proposiciones sustantivas de hechos, variables, parámetros, entidades y relaciones entre variables y/o entidades u operaciones (Definiciones, 2010).

m. NTP

Norma Técnica Peruana

n. Norma

Documento publicado con la designación de norma o especificación y otros documentos afines que se refieren a los diferentes aspectos de la normalización (INDECOPI, 2004).

o. Política de seguridad

Una política de seguridad es un conjunto de directrices, normas, procedimientos e instrucciones que guía las actuaciones de trabajo y define los criterios de seguridad para que sean adoptados a nivel local o institucional, con el objetivo de establecer, estandarizar y normalizar la seguridad tanto en el ámbito humano como en el tecnológico. A partir de

sus principios, es posible hacer de la seguridad de la información un esfuerzo común, en tanto que todos puedan contar con un arsenal informativo documentado y normalizado, dedicado a la estandarización del método de operación de cada uno de los individuos involucrados en la gestión de la seguridad de la información (Harris, 2004).

p. Recursos de información

Conjunto de elementos físicos y no físicos destinados al uso y manejo de la información para resolver una necesidad o llevar a un buen termino el negocio de una empresa (ISO, 2004).

q. Riesgo

Contingencia o proximidad de un daño. Posibilidad de que se produzca un impacto determinado en un activo, en un dominio o en toda la Organización (Anderson, 1980).

r. Seguridad de Información

Se entiende por seguridad de la información a todas aquellas medidas preventivas y reactivas del hombre, de las organizaciones y de los sistemas tecnológicos que permitan resguardar y proteger la información buscando mantener la confidencialidad, la autenticidad y Integridad de la misma. Diferenciando el concepto de seguridad de la información con el de seguridad informática, en que este último sólo se encarga de la seguridad en el medio informático. (Fitzgerald, 2007).

s. Usuario

En informática, el término usuario designa a la persona o personas que van a manipular de manera directa un producto de software.

Usuario final no es necesariamente sinónimo de cliente o comprador. Una compañía puede ser un importante comprador de software, pero el usuario final puede ser solamente un empleado o grupo de empleados dentro de la compañía, como una secretaria o un digitador. El concepto clave es la interacción directa con el programa, no la propiedad.

Persona que utiliza un dispositivo o un ordenador y realiza múltiples operaciones con distintos propósitos. (Definiciones, 2010).

En el caso del software de gran distribución, el cliente o comprador es por lo general el mismo que el usuario final.

t. Vulnerabilidad

Posibilidad de ocurrencia de la materialización de una amenaza sobre un Activo (ISO, 2004).

CAPÍTULO II

EL PROBLEMA DE INVESTIGACIÓN

2.1 Descripción de la Realidad Problemática

En la actualidad, la información es el bien de mayor valor para las empresas (Academia Lationoamericana de la Seguridad Informática, 2011). 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, el reporte (Ponemon Institute, 2010) sobre costos de las brechas de seguridad, 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 que 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 tratado como un problema tecnológico y a su vez con una solución tecnológica. Lo que es totalmente falso debido a que la seguridad de información tiene que ver con la gestión del riesgo (Whitman, Caylor, Fendler, & Baker, 2005) 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 de estas amenazas parten de la conducta del usuario. Si las

organizaciones fallan en gestionar la seguridad de la información, la integridad se ve comprometida y puede ocurrir pérdidas económicas.

Este punto respecto a la importancia del usuario se convierte en crucial, al respecto (Tipton & Krause, 2006) señalan que la Seguridad está basada en las personas, además manifiestan "-Si se piensa que la tecnología puede resolver los problemas de seguridad, entonces no se entiende los problemas o la tecnología".

Es más, para reducir los riesgos y asegurar protección de la información, las organizaciones a menudo confían en soluciones basadas en tecnología (Ernst & Young, 2008). Aunque estos tipos de soluciones ayudan a mejorar la protección de la información (Straub & Nance, 1990), la confianza exclusiva en dichos medios rara vez es suficiente como para eliminar el riesgo (Cavusoglu & Etal, 2010) (Siponen, 2005). Pues sin el compromiso de los usuarios del sistema cualquier medida de seguridad a implementarse será nula o poco efectiva.

En el contexto nacional, el tema crucial es que, verificando la adopción de prácticas de seguridad basadas en el ISO 17799, del año 2010, según encuesta Nacional de ONGEI, de un total de 271 entidades estatales encuestadas a nivel nacional solo 152 indica que cuenta o está iniciando a implementar un plan de seguridad de información, apreciando un 46% que no tiene plan de seguridad, que en su mayoría corresponde a las provincias. A pesar de contar con un desarrollo en el uso de TI, claramente se muestra el poco éxito en la implementación de Seguridad de Información basado en Norma Técnica Peruana NTP-ISO/ IEC 17799:2007.

Por lo tanto, entendiendo que la implementación de la Seguridad en Sistemas de Información es un aspecto de relevancia estratégica para una organización, no existe modelo que pueda evaluar los factores críticos que condicionan la implementación exitosa de Seguridad de información para Sistemas de Información desde la perspectiva del usuario y específicamente en su intencionalidad, entiendo que el usuario es el protagonista principal en todo

sistema de información y que sin entender sus percepciones es difícil que un plan de seguridad funcione.

Por lo que, el presente estudio busca determinar los Factores Críticos de Éxito y el grado de influencia que ejercen en la intención del usuario, para la Implementación de Seguridad en Sistemas de Información.

2.2 Delimitación de la Investigación

La presente investigación, diseña una guía de implementación del modelo propuesto con sus factores, manteniendo características generales que le permitan ser adaptable a cualquier organización que requiera evaluar los factores críticos de éxito para implementar seguridad desde la perspectiva del usuario.

La propuesta se verificó en una organización de tipo estatal o gubernamental, que fue una Universidad Pública, que para el presente caso particular fue la Universidad Nacional del Altiplano de Puno (UNA-Puno).

2.3 Planteamiento del Problema

2.3.1 Problema Principal

¿Cuál es el grado de influencia que ejercen los Factores Críticos de Éxito en la intención del usuario para la Implementación de Seguridad de Sistemas de Información en la Universidad Nacional del Altiplano-Puno durante el año 2011?

2.3.2 Problemas Específicos

- ¿Los Factores Críticos de Éxito para Implementación de Seguridad de Sistemas de Información serán factibles de ser representados a través de un modelo estructural para su evaluación?

- ¿A partir del modelo estructural desarrollado será factible desarrollar una guía metodológica para evaluar los Factores Críticos de Éxito que influyen en la intención del usuario para la Implementación de Seguridad de Sistemas de Información?
- ¿Es posible determinar el nivel de confianza del modelo estructural, implementado mediante la guía metodológica, para evaluar los Factores Críticos de Éxito que influyen en la intención del usuario para la Implementación de Seguridad de Sistemas de Información de la Universidad Nacional del Altiplano Puno durante el año 2011?

2.4 Objetivos

2.4.1 Objetivo General

Determinar, mediante un modelo estructural, el grado de influencia que ejercen los Factores Críticos de Éxito en la intención del usuario para la Implementación de Seguridad de Sistemas de Información en la Universidad Nacional del Altiplano Puno durante el año 2011.

2.4.2 Objetivos Específicos

- Diseñar un modelo estructural de evaluación de Factores Críticos de Éxito para Implementación de Seguridad de Sistemas de Información.
- Diseñar una guía metodológica que permita evaluar los Factores Críticos de Éxito que influyen en intención del usuario en la Implementación de Seguridad de Sistemas de Información
- Determinar el grado de confianza del modelo estructural, implementado mediante la guía metodológica, para evaluar los Factores Críticos de Éxito que influyen en la intención del usuario para la Implementación de Seguridad de Sistemas de Información de la Universidad Nacional del Altiplano Puno durante el año 2011.

2.5 Hipótesis

2.5.1 Hipótesis Principal

Los factores: 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, Infraestructura Tecnológica, Soporte hacia el usuario, Experiencia del usuario; influyen significativamente en la intención del usuario para la Implementación de Seguridad de Sistemas de Información en la Universidad Nacional del Altiplano Puno durante el año 2011.

2.5.2 Hipótesis Específicas

- 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 La Infraestructura Tecnológica existente influye en la Actitud para implementar Seguridad en Sistemas de Información
- H14 La Infraestructura Tecnológica existente influye en el control conductual percibido
- H15 El Soporte hacia el usuario influye en la Actitud para implementar Seguridad en Sistemas de Información
- H16 El Soporte hacia el usuario influye en el control conductual percibido
- H17 La Experiencia del usuario influye en la Actitud para implementar Seguridad en Sistemas de Información
- H18 La Experiencia del usuario influye en el control conductual percibido
- H19 La Actitud para implementar Seguridad en Sistemas de Información influye en la Intención para Implementar Seguridad en Sistemas de Información
- H20 El control conductual percibido influye en la Intención para Implementar Seguridad en Sistemas de Información
- H21 La Norma subjetiva influye en la Intención para Implementar Seguridad en Sistemas de Información.

2.6 Variables e Indicadores

2.6.1 Variable Independiente

Factores Críticos de Éxito

2.6.1.1 Indicadores

VARIABLE	DIMENSION	INDICADOR	REFERENCIA
Factores Críticos de Éxito	Compromiso de la Alta Gerencia	Apoyo y compromiso	(Medina Quintero, 2005)
		Resistencia al cambio	(Medina Quintero, 2005)
		motivación	(Villegas Ortega, 2009)
		necesidades del negocio	(Medina Quintero, 2005)
		Administración del Presupuesto	(Medina Quintero, 2005)
	Cultura Organizacional	idioma	(Medina Quintero, 2005)
		conducta y actitud	(Medina Quintero, 2005)
		sistema de valores	(Medina Quintero, 2005)
		perspectivas del cambio social	(Villegas Ortega, 2009)
		motivaciones	(Medina Quintero, 2005) (Villegas Ortega, 2009)
	Misión de la Organización	Claridad	(Siponen M. T., 2001)
		Alineamiento	(Al-Awadi & Renaud, 2008)
		Cumplimiento	(McKay, 2003)
		Seguridad	(Abu-Zineh, 2006) (ISO/IEC, 2005) (Siponen M. T., 2001)
	Recursos y Presupuesto	Aprovechamiento óptimo económico y de materiales	(Villegas Ortega, 2009)
		apoyo óptimo de activos humanos	(Villegas Ortega, 2009) (Medina Quintero, 2005)
		aprovisionamiento según Necesidades	(Villegas Ortega, 2009) (Doherty & Fulford, 2005) (Dinnie, 1999)
	Formación y Capacitación	Continuidad	(Dhillon, Managing and Controlling Computer Misuse, 1999)
		Orientación en seguridad de activos	(Al-Awadi & Renaud, 2008)
		Capacitación y formación en temas de seguridad	(Al-Awadi & Renaud, 2008) (Lau, 1988)
		Importancia	(Dhillon, Managing and Controlling Computer Misuse, 1999)
	Conciencia de la necesidad de seguridad por el personal	Importancia	(Siponen M. T., 2001)
		Incidentes de seguridad	(McKay, 2003) (Al-Awadi & Renaud, 2008)
		seguridad de acceso y respaldo	(Katz, 2005) (Hyeun-Suk, Cheongtag, & Young U., 2009)
	Infraestructura Tecnológica existente	Recursos:informatico, estratégico y transaccional	(Medina Quintero, 2005)
		Flujo oportuno de información y comunicación	(Medina Quintero, 2005)
		Comunicación global	Elaboración propia
	Soporte hacia el usuario	Atención y asistencia	(Huang & Hao Chuang, 2007)
		compromiso	(Villegas Ortega, 2009)
		Calidad de soporte	(Huang & Hao Chuang, 2007)
		Calidad de soporte en seguridad de información	(Huang & Hao Chuang, 2007)
	Experiencia del usuario	Experiencia en sistemas y computadoras	(Huang, Patrick Rau, & Salvendy, 2007) (Novakovic, McGill, & Dixon, 2009)
		Solución de problemas	(Huang, Patrick Rau, & Salvendy, 2007) (Novakovic, McGill, & Dixon, 2009)
		Experiencia con seguridad de información	(Huang, Patrick Rau, & Salvendy, 2007) (Novakovic, McGill, & Dixon, 2009)
		Experiencia con tecnologías web	(Venkatesh, Morris, Davis, & Davis, 2003) (Novakovic, McGill, & Dixon, 2009)
		Experiencia con tecnologías de email	(Venkatesh, Morris, Davis, & Davis, 2003) (Novakovic, McGill, & Dixon, 2009)

2.6.2 Variable Dependiente

La intención del usuario para la Implementación de Seguridad en Sistemas de Información

2.6.2.1 Indicadores

VARIABLE	DIMENSION	INDICADOR	REFERENCIA
intención del usuario para la Implementación de Seguridad en Sistemas de Información	**Norma Subjetiva (creencias normativas)**	creencia a nivel organizacional	Adaptado de (Venkatesh, Morris, Davis, & Davis, 2003)
		creencia a nivel de los compañeros de trabajo	Adaptado de (Huang & Hao Chuang, 2007) (Bulgurcu, Cavusoglu, & Benbasat, 2010)
		creencia a nivel de los jefes inmediatos	Adaptado de (Huang & Hao Chuang, 2007) (Bulgurcu, Cavusoglu, & Benbasat, 2010)
		creencia a nivel de los gerentes o autoridades de alto rango	Adaptado de (Huang & Hao Chuang, 2007) (Bulgurcu, Cavusoglu, & Benbasat, 2010)
	Actitud para implementar Seguridad en SI	utilidad	Adaptado de (Venkatesh, Morris, Davis, & Davis, 2003) (Huang & Hao Chuang, 2007) (Bulgurcu, Cavusoglu, & Benbasat, 2010)
		beneficio	Adaptado de (Venkatesh, Morris, Davis, & Davis, 2003) (Huang & Hao Chuang, 2007) (Bulgurcu, Cavusoglu, & Benbasat, 2010)
		necesidad	Adaptado de (Venkatesh, Morris, Davis, & Davis, 2003) (Huang & Hao Chuang, 2007) (Bulgurcu, Cavusoglu, & Benbasat, 2010)
		importancia	Adaptado de (Venkatesh, Morris, Davis, & Davis, 2003) (Huang & Hao Chuang, 2007) (Bulgurcu, Cavusoglu, & Benbasat, 2010)
	Control Conductual Percibido	Habilidades	Adaptado de (Huang & Hao Chuang, 2007) (Bulgurcu, Cavusoglu, & Benbasat, 2010)
		Conocimiento	Adaptado de (Huang & Hao Chuang, 2007) (Bulgurcu, Cavusoglu, & Benbasat, 2010)
		Competencias	Adaptado de (Huang & Hao Chuang, 2007) (Bulgurcu, Cavusoglu, & Benbasat, 2010)

2.7 Justificación

Desde el punto de vista teórico, se plantea un modelo, que puede servir como referencia para la evaluación de los factores críticos de éxito para garantizar la

implementación de la seguridad de información en las organizaciones, con la particularidad que su enfoque principal es la actitud del usuario.

Tal es así, que para lograr un nivel adecuado de protección de información en las organizaciones, identificar sus principales amenazas es un necesidad urgente (Whitman M. E., Enemy at the Gate: Threats to Information Security, 2003). Más aún, cuando el valor de los sistemas de información y la importancia de la información que se protege sube, también lo hace la importancia de la necesidad de su protección.

Muchas organizaciones han encontrado el valor real de la seguridad efectiva después de sopesar repercusiones negativas debido a su brechas de seguridad (Cavusoglu, Mishra, & Raghunathan, 2004).

La seguridad de información se ha convertido en uno de los aspectos de mayor importancia para cualquier organización. De tal forma que las organizaciones necesitan asegurar sus activos de información para mantener un alto nivel de seguridad (Solms, 1998). Lo que repercute en la eficiencia organizacional.

Desde el punto de vista práctico, se busca la aplicabilidad del modelo de evaluación de Factores Críticos de Éxito a través del desarrollo de una guía de implementación; y su aplicación a la Universidad Nacional del Altiplano, pudiendo ser extensible a otras entidades estatales existentes en nuestro país, más aún considerando que con el incremento del uso de computadores en las instituciones públicas (ONGEI, 2009).

CAPÍTULO III

METODOLOGÍA

3.1 Tipo y Diseño de Investigación

Es una investigación aplicada, pues está orientada a lograr un nuevo conocimiento destinado a procurar soluciones que permitan determinar los factores en la implementación exitosa de Seguridad en Sistemas de Información en instituciones; es explicativo, pues determina las causas a un determinado fenómeno, mediante el análisis de la relación entre dos o más variables, ya sea por relación de causalidad, correlación o asociación, en el presente caso los factores críticos de éxito y su efecto la intención del usuario.

Es de tipo transversal; pues se trata de conocer la percepción del usuario en una sola vez, y se procede a su descripción y análisis; la recolección de los datos se ha desarrollado en un periodo determinado que corresponde a noviembre del 2011.

Se emplea un diseño factorial, pues se trata de un estudio donde el objetivo es conocer el grado de influencia de los factores críticos de éxito en la implementación de la seguridad de información, en conjunto, con respecto a 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.

3.2 Población y Muestra

3.2.1 Población

En primer lugar, se determinó cual es el marco muestral y la unidad de análisis, para luego proceder a delimitar la población que será estudiada y sobre la cual

se pretende generalizar los resultados; para ello, se tomó como referencia (marco muestral) el Cuadro de Asignación de Personal de la UNA-Puno. En base a dicha información se ha determinado:

- Universo: el personal que trabaja con el Sistema Integral Administrativo. Dicho personal labora en las diferentes áreas administrativas de la UNA-Puno en la ciudad de Puno.
- Informante: Los usuarios en las diferentes dependencias de la UNA-Puno que, emplean para su trabajo cotidiano el Sistema Integral Administrativo de acuerdo al CAP 2010, seleccionados del total de 681 administrativos de la UNA-Puno.

UNIVERSIDAD NACIONAL DEL ALTIPLANO PUNO

RESUMEN C.A.P. REORDENADO PERSONAL ADMINISTRATIVO

NIVELES REMUNERATIVOS	PAP 2009	CAP REORDENADO	DIFERENCIA
TOTAL FUNCIONARIOS	129	115	-14
DIRECTOR GENERAL	2	2	0
SF6	1	1	0
SF4	1	1	0
DIRECTORES	38	28	-10
SF4	32	26	-6
SF3	6	2	-4
JEFES DE UNIDAD	23	23	0
SF4	2	1	-1
SF3	5	9	4
SF2	12	10	-2
SF1	4	3	-1
FUNCIONARIOS	66	62	-4
SF3	9	8	-1
SF2	48	47	-1
SF1	9	7	-2
PROFESIONALES	32	86	54
SPA	8	8	0
SPB	10	20	10
SPC	13	49	36
SPE	1	9	8
PROF.Y ASIST.DE SALUD	6	6	0
N1	1	1	0
VII	1	1	0
VIII	2	2	0
STA	2	2	0
TECNICOS	256	316	60
STA	125	163	38
STB	43	30	-13
STC	88	123	35
AUXILIARES	258	158	-100
SAA	84	108	24
SAB	9	2	-7
SAC	165	48	-117
TOTAL GENERAL	681	681	0

Fuente : Informe Final de la Comisión de Reordenamiento del CAP Administrativo.

Figura 15 Resumen del CAP 2010 UNA-Puno

3.2.2 Selección de la muestra

En base al total del personal administrativo en las diferentes dependencias que hacen un total de 681, en primer lugar se seleccionó específicamente las oficinas y unidades que interactúan con el sistema, para lo cual se identifica dichas oficinas y unidades, así como la cantidad de personal que utiliza el sistema (Tabla 5).

Tabla 5 Cuadro de Asignación de Personal por Dependencia que usa el Sistema Integral Administrativo UNA-Puno

DEPENDECIA	personal según CAP
OFICINA GENERAL DE PLANIFICACION Y DESARROLLO	2
OFICINA DE PLANES Y PROYECTOS	6
OFICINA DE PRESUPUESTO	6
OFICINA DE RACIONALIZACION	6
OFICINA DE ESTADISTICA	5
OFICINA DE RECURSOS HUMANOS	2
UNIDAD DE ESCALAFON	7
UNIDAD DE REMUNERACIONES	6
UNIDAD DE PENSIONES Y LIQUIDACIONES	6
UNIDAD DE CONTROL DE ASISTENCIA	8
UNIDAD DE CAPACITACION	5
OFICINA DE CONTADURIA GENERAL	8
OFICINA DE GESTION FINANCIERA	2
TESORERIA	10
ABASTECIMIENTOS Y ALMACENES	12
ALMACENES	12
OFICINA DE ARQUITECTURA Y CONSTRUCCIONES	5
OFICINA DE BIENESTAR UNIVERSITARIO	10
OFICINA UNIVERSITARIA ACADEMICA	25
TOTAL	143

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 (Tabla 5) en las diferentes dependencias de la UNA-Puno que usan el sistema. Aplicando al caso:

$$n = \frac{N * Z_{\alpha}^2 p * q}{d^2 * (N-1) + Z_{\alpha}^2 * p * q}$$

Donde:

- n es el tamaño de la muestra;
- N = Total de la población
- Z_a^2 = 1.962 (seguridad del 95%)
- p = proporción esperada (en este caso 5% = 0.05)
- q = 1 – p (en este caso 1-0.05 = 0.95)
- d = precisión (en este caso deseamos un porcentaje de error 3%).

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 tiene:

$$n = \frac{(143)(1.962^2)(0.05)(0.95)}{(0.03^2)(143-1)+(1.962^2)(0.05)(0.95)} = 84$$

Por lo que, la cantidad mínima representativa para el estudio será 84 usuarios.

3.3 Técnicas e Instrumentos de Recolección de datos

Entre las principales técnicas empleadas en el presente trabajo de investigación, se consideró la encuesta, que permitió recabar la información sobre la percepción en relación a loa factores críticos de éxito por parte de los usuarios del sistema de información de la Universidad Nacional del Altiplano Puno.

Para la presente investigación, se ha empleado el cuestionario, que ha sido desarrollado a partir de las variables e indicadores de acuerdo a la investigación teórica y propuesta del investigador.

3.3.1 Tipo de encuesta

Considerando las características de la encuesta, se ha utilizado la encuesta personal y la encuesta por Internet basado en cuestionarios de preguntas cerradas con escala de intervalo (Kendall & Kendall, 1997), para poder cumplir al menos con el tamaño de muestra recomendado (Figura 16).

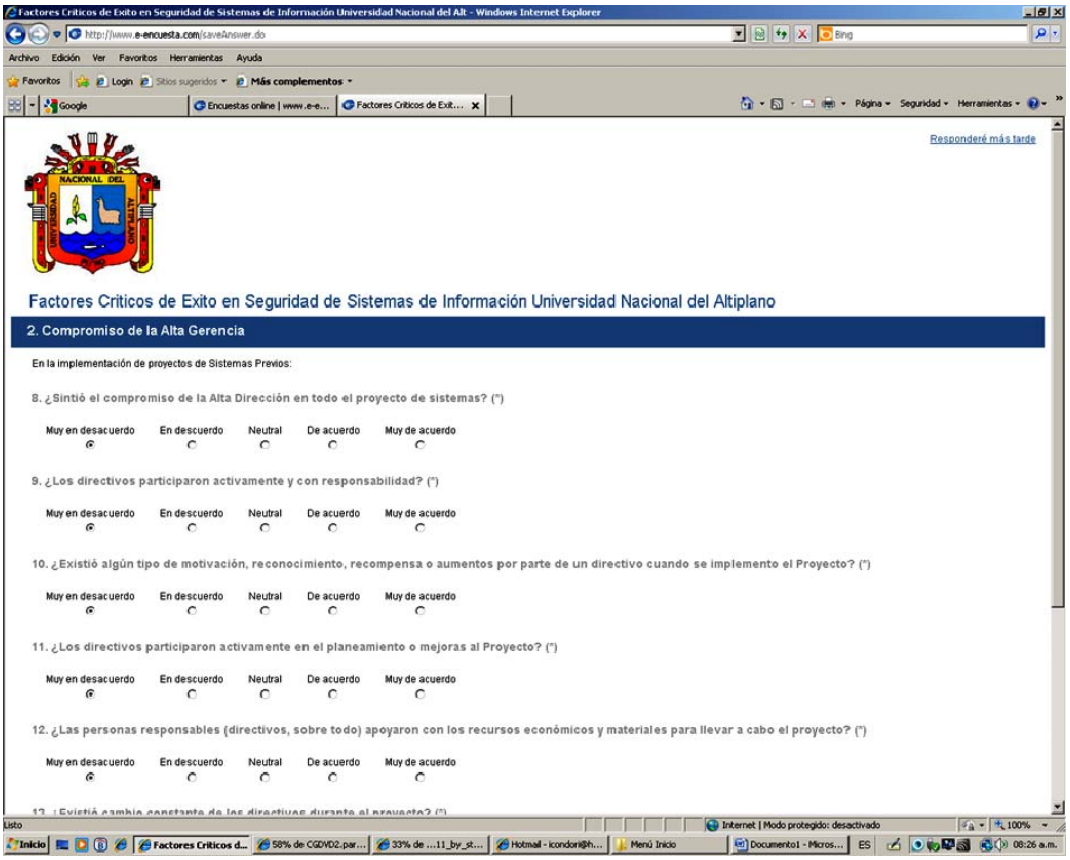

Figura 16 Encuesta Piloto en Web para la UNA-Puno

3.4 Técnicas de Procesamiento y Análisis de Datos

Para el procesamiento, se utilizó el software SPSS v 19, donde se registraron las encuestas aplicadas, bajo un formato predefinido de captura de información en base al cuestionario formulado.

Para el análisis y prueba de hipótesis, se emplea la técnica de análisis multivariante; en particular, el análisis factorial basado en PLS (partial less squares) combinada con el bootstraping con apoyo del software SPSS v 19, AMOS v19 y SmartPLS 2.0.

CAPÍTULO IV

PRESENTACIÓN Y ANÁLISIS DE LOS RESULTADOS

4.1 Presentación de Resultados

4.1.1 Diseño del Modelo Estructural de Evaluación de Factores Críticos de Éxito para la Implementación de Seguridad de Sistemas de Información

El Modelo propuesto se ha desarrollado a partir de un conjunto de factores justificados que se han adaptado para combinarlos con el modelo de la Teoría del Comportamiento Planificado (TPB) de Ajzen que ha servido de base al modelo de aceptación Tecnológica (TAM y TAM2); en vista que, los modelos revisados 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.

En primer lugar se realiza la identificación de Factores Críticos de éxito para Implementar la Seguridad en Sistemas de Información a partir de la revisión del estado del arte.

En segundo lugar, se propone tres factores críticos de éxito en base a los aspectos que se deberían tener en cuenta con relevancia hacia el enfoque conductual del usuario.

En tercer lugar, se propone el modelo, con una descripción detallada de sus componentes, y las hipótesis, en base a la adaptación del modelo TPB, y los factores críticos de éxito propuestos, para evaluar las relaciones de los Factores Críticos de Éxito para la Implementación de Seguridad en Sistemas de Información y la intención del usuario.

4.1.1.1 Identificación de Factores Críticos de éxito para Implementar la Seguridad en Sistemas de Información

4.1.1.1.1 Factores Existentes en la Literatura

De acuerdo a la revisión del estado del arte en cuanto a los factores críticos de éxito (Abu-Zineh, 2006) (ISO/IEC, 2007) (ISO/IEC, 2005) (INDECOPI, 2007) (Nosworthy, 2000) (Al-Awadi & Renaud, 2008) (Bjorck, 2002) (Partida & Ezingeard Henley, 2007) (Kankanhalli, Hock-hai, Bernard, & Kwok-kee, 2003) (Siponen, 2001), es necesario mencionar, que no existe un consenso acerca de cuáles son los factores críticos que posibilitan el éxito en la implementación se seguridad de información; 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.

Por ejemplo, en el estudio de (Abu-Zineh, 2006) se presenta como “compromiso de la alta dirección”, en caso de la norma ISO/IEC 27002 y 17799 “El apoyo visible y el compromiso de la alta gerencia” (ISO/IEC, 2007) (ISO/IEC, 2005) (INDECOPI, 2007), “Soporte de la Gerencia” (Al-Awadi & Renaud, 2008), “compromiso de la gerencia” (Bjorck, 2002), “Obtener el compromiso de dirección” (Partida & Ezingeard Henley, 2007); donde se dan diferentes denominaciones a un mismo factor, que por criterio de similitud equivalen al factor “Compromiso de la Gerencia”.

Tabla 6 Factores Críticos de Éxito para la Implementación de Seguridad de Sistemas de Información

Factores	Autores
compromiso de la gerencia	(Abu-Zineh, 2006) (ISO/IEC, 2007) (ISO/IEC, 2005) (INDECOPI, 2007) (Al-Awadi & Renaud, 2008) (Bjorck, 2002) Auditores (Bjorck, 2002) consultores (Partida & Ezingeard Henley, 2007) (Kankanhalli, Hock-hai, Bernard, & Kwok-kee, 2003)
cultura organizacional	(Nosworthy, 2000) (ISO/IEC, 2007) (ISO/IEC, 2005) (INDECOPI, 2007) (Partida & Ezingeard Henley, 2007)
misión de la organización	(Al-Awadi & Renaud, 2008), Abu-Zineh, 2006) (ISO/IEC, 2007) (ISO/IEC, 2005) (INDECOPI, 2007) (Partida & Ezingeard Henley, 2007) (Siponen, 2001)
Recursos y presupuesto	(ISO/IEC, 2007) (ISO/IEC, 2005) (INDECOPI, 2007) (Al-Awadi & Renaud, 2008) (Bjorck, 2002)
formación y capacitación	(Abu-Zineh, 2006) (ISO/IEC, 2007) (ISO/IEC, 2005) (INDECOPI, 2007) (Nosworthy, 2000) (Al-Awadi & Renaud, 2008) (Bjorck, 2002)
Conciencia de la necesidad de seguridad por el personal	(Abu-Zineh, 2006) (ISO/IEC, 2007) (ISO/IEC, 2005) (INDECOPI, 2007) (Nosworthy, 2000) (Al-Awadi & Renaud, 2008) (Bjorck, 2002) Auditores (Bjorck, 2002) consultores (Partida & Ezingeard Henley, 2007)

Consecuentemente se puede apreciar (Tabla 6), seis factores ampliamente respaldados por la literatura en cuanto a la Implementación de seguridad en Sistemas de Información:

a) Compromiso de la gerencia, factor fundamental cuanto se requiere implementar un proyecto relacionado a los Sistemas de Información, en vista que la toma de decisiones y los aspectos estratégicos organizacionales están a cargo de la "gerencia", sin su apoyo, no es posible el éxito de un proyecto.
b) Cultura Organizacional, que se refiere a Normas y valores existentes en una organización.
c) Misión de la organización, refleja la claridad del rumbo empresarial con objetivos y metas claras.
d) Recursos y Presupuesto, elementos necesarios para la realización del proyecto.
e) Formación y Capacitación, dicho factor es esencial, se resalta la necesidad de posibilitar una mejor preparación del usuario de forma integral.

f) Conciencia de la necesidad de seguridad por el personal, Se entiende como el nivel de convencimiento en la necesidad de seguridad en sistemas de información por parte de los usuarios.

Dichos factores, están enfocados principalmente al aspecto organizacional y la planeación.

Así el aspecto organizacional, se puede definir como la Función de ensamblar y coordinar los recursos humanos, financieros, físicos, de información y otros que sean necesarios para lograr las metas (Bateman & Snell, 2001). En el caso particular de la seguridad de Información son actividades de la organización que se ven involucradas en la implementación de Seguridad en sistemas de información como parte de la necesidad de protección de la información que la organización almacena en los sistemas de información.

En cuanto a la Planeación, se define como la aplicación de conocimiento, habilidades, herramientas y técnicas a las actividades del proyecto a fin de satisfacer las necesidades de los usuarios y de quien así lo requiera (Bennatan, 2000). Por otro lado (Villegas Ortega, 2009) señala que es fundamental para la empresa, ya que la existencia de planes formales garantiza que la organización concentre todos sus recursos y energías en la consecución de sus objetivos, eliminando las ambigüedades sobre las que se espera de cada persona, de cada grupo de trabajo o de cada unidad funcional, requiriéndose para la seguridad de los SI una alineación estrecha con los planes de negocio.

En tal sentido los factores planteados dejan de lado la evaluación del usuario, en cuanto a su conducta como actor social guiado por sus actitudes y percepciones, considerándolo solamente como un elemento o recurso más.

Por otro lado, también se deja de lado evaluar la infraestructura tecnológica existente, pues dicho aspecto condiciona fuertemente la implementación de un plan de seguridad que sea exitoso.

4.1.1.1.2 Factores Propuestos

Como se comento en el punto anterior, más allá de los indicadores ampliamente aceptados, y considerando los vacios en cuanto a brindar una mayor importancia al usuario, así como la percepción de la infraestructura tecnológica actual, se plantean tres nuevos factores.

a. Infraestructura Tecnológica existente

Provee la plataforma (hardware, software, almacenamiento) de informática en la cual las organizaciones pueden construir sus sistemas de información específicos (Laudon & Laudon, 1996). Considerando que la seguridad está estrechamente vinculada a los sistemas de información, es necesaria su evaluación, como parte de la percepción que el usuario tiene de la plataforma existe.

b. Soporte hacia el usuario

Dicho factor, se ha tomado de la propuesta de (Huang & Hao Chuang, 2007) que realiza un estudio de el comportamiento del usuario frente a la fusión de empresas y consecuentemente a la integración de sistemas de información, que en el presente caso, pretende evaluar la percepción que tiene el usuario de la calidad del servicio de soporte tanto en hardware, software y redes; y si influye en la posterior implementación de Seguridad en los Sistemas de Información.

c. Experiencia del usuario

Un factor primordial de influencia es la experiencia, es decir, El conocimiento de los usuarios acerca de las medidas proteccionistas de un sistema de información (Dunkerley K. D., 2011).

El conocimiento del usuario describe la cognición del ambiente organizativo, tanto técnico como no técnico. El conocimiento técnico se aplica a la erudición del usuario respecto a los activos técnicos. Por otra parte, el conocimiento no técnico implica la conciencia de usuario acerca de las normas de actuación sobre seguridad y los controles diversos, protección de activos de información y la misión organizativa (Dunkerley K. D., 2011).

Tal es así que las experiencias pasadas condicionan los comportamientos futuros. La actitud de un usuario inexperto es diferente a un usuario experimentado. Por ejemplo: la aplicación de una política de seguridad por un usuario experimentado será más fácil que un usuario sin experiencia en seguridad.

En tal sentido, la experiencia del usuario es un factor determinante y que debe ser incorporado como parte del modelo, pues dependiendo del conocimiento y habilidades desarrolladas su actitud variará frente a una posible implementación de Seguridad en Sistemas de información. Respaldado con el estudio realizado por (Venkatesh, Morris, Davis, & Davis, 2003).

Tabla 7 Propuesta Integrada de Factores Críticos de Éxito para la Implementación de Seguridad de Sistemas de Información

Factores	**Autores**
Compromiso de la gerencia	(Abu-Zineh, 2006) (ISO/IEC, 2007) (ISO/IEC, 2005) (INDECOPI, 2007) (Al-Awadi & Renaud, 2008) (Bjorck, 2002) Auditores (Bjorck, 2002) consultores (Partida & Ezingeard Henley, 2007) (Kankanhalli, Hock-hai, Bernard, & Kwok-kee, 2003)
Cultura organizacional	(Nosworthy, 2000) (ISO/IEC, 2007) (ISO/IEC, 2005) (INDECOPI, 2007) (Partida & Ezingeard Henley, 2007)
Misión de la organización	(Al-Awadi & Renaud, 2008), Abu-Zineh, 2006) (ISO/IEC, 2007) (ISO/IEC, 2005) (INDECOPI, 2007) (Partida & Ezingeard Henley, 2007) (Siponen, 2001)
Recursos y presupuesto	(ISO/IEC, 2007) (ISO/IEC, 2005) (INDECOPI, 2007) (Al-Awadi & Renaud, 2008) (Bjorck, 2002)
Formación y capacitación	(Abu-Zineh, 2006) (ISO/IEC, 2007) (ISO/IEC, 2005) (INDECOPI, 2007) (Nosworthy, 2000) (Al-Awadi & Renaud, 2008) (Bjorck, 2002)
Conciencia de la necesidad de seguridad por el personal	(Abu-Zineh, 2006) (ISO/IEC, 2007) (ISO/IEC, 2005) (INDECOPI, 2007) (Nosworthy, 2000) (Al-Awadi & Renaud, 2008) (Bjorck, 2002) Auditores (Bjorck, 2002) consultores (Partida & Ezingeard Henley, 2007)
Infraestructura Tecnológica	*Adaptado de los estudios de (Medina Quintero, 2005) (Villegas Ortega, 2009)*
Soporte hacia el usuario	*Adaptado de los estudios de (Huang & Hao Chuang, 2007)*
Experiencia del usuario	*Adaptado de los estudios (Dunkerley K. D., 2011) (Venkatesh, Morris, Davis, & Davis, 2003)*

Es necesario aclarar que, los factores propuestos a partir de la revisión de literatura realizada, no han sido empleados como factores críticos para la implementación de Seguridad en Sistemas de Información en forma explícita, pero si en estudios de sistemas de información; por lo que, se pretende realizar una adaptación como factores para el presente caso.

En cuanto a los factores propuestos, su pertinencia será verificada en la prueba empírica del modelo en la Universidad Nacional del Altiplano.

4.1.1.2 Modelo de Evaluación Propuesto

4.1.1.2.1 Motivación del Modelo

Considerando que, la implementación de la Seguridad en Sistemas de Información es un aspecto de relevancia estratégica para una organización, que consta de muchas perspectivas, y que es importante evaluar los factores críticos que condicionan la implementación exitosa de Seguridad de información para Sistemas de Información desde la perspectiva del usuario en pre-implementación, ha sido necesario realizar una adaptación a partir del modelo TCP propuesto por Ajzen.

En referencia a los estándares de buenas prácticas como el ISO 17799 o el ISO 27002, al ser buenas prácticas genéricas, no evalúan factores que permitan el éxito previo a su implantación; aclarando además, que la realidad de cada organización es diferente una de otra, más aun considerando en el caso peruano la existencia de la NTP 17799 aprobada por (INDECOPI, 2007).

Al respecto (Tipton & Krause, 2006) señalan que la Seguridad está basada en las personas, además manifiestan -“Si se piensa que la tecnología puede resolver los problemas de seguridad, entonces no se entiende los problemas o la tecnología”.

Es más, para reducir los riesgos y asegurar protección de la información, las organizaciones a menudo confían en soluciones basadas en tecnologías (Ernst & Young, 2008). Aunque estos tipos de soluciones ayudan a mejorar la protección de la información (Straub & Nance, 1990), confiando en ellos

exclusivamente (o excesivamente) rara vez es suficiente para eliminar el riesgo (Cavusoglu & Etal, Information Security Control Resources in Organizations: A Multidimensional View and Their Key Drivers, 2010) (Siponen M. T., 2005).

La evidencia empírica y anecdótica señala que el número de incidentes relacionados con la seguridad de la información se incrementa (AIRC, 2008) (Symantec, 2009) del mismo modo que las organizaciones invierten más en soluciones basadas en tecnologías. El éxito en la protección de la información puede ser alcanzado cuando las organizaciones invierten dinero en ambas, tanto soluciones técnicas y socio organizacionales.

Lo que claramente muestra la necesidad de incorporar al usuario como elemento trascendente para lograr implementar la seguridad en Sistemas de Información.

4.1.1.2.2 Descripción General del Modelo

De la revisión de los modelos y sus respectivas variantes para la Seguridad de Sistemas de Información de las propuestas de (Kankanhalli, Hock-hai, Bernard, & Kwok-kee, 2003) (Chaulaa, Yngströmb, & Kowalskic, 2005) (Dunkerley & Tejay, 2009) (Dunkerley K. D., 2011), se determina que, ninguno está orientado a la intención de implementación de Seguridad en Sistemas de Información (ex ante), en vista que plantean su observación una vez realizada la implementación de Seguridad en Sistemas de Información .

En tal sentido, resaltan las adaptaciones hechas al modelo original de Delone, que incluso han llegado a proponer factores para medir el éxito de la seguridad en sistemas de información, teniendo presente que se trata de evaluaciones sobre sistemas de seguridad de información ya implementados y basados en la teoría de tres niveles de Shanon.

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 (Theory of

Reasoned Action TRA), que es un modelo de la Psicología Social desarrollado por Martin Fishbein y Icek Ajzen (Ajzen & Fishbein, 1980).

Resaltando que (Ajzen I. , 1991), 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 (TPB). Que viene siendo empleada ampliamente en la investigación en cuanto a seguridad de información (Pahnila, Siponen, & Mahmood, 2007) (Cavusoglu, Mishra, & Raghunathan, 2004)(Cavusoglu, Cavusoglu, y Raghunathan 2004). (Bulgurcu, Cavusoglu, & Benbasat, 2010).

La Teoría de la Acción Razonada[4] (TRA) (Ajzen & Fishbein, 1980) y la Teoría de Comportamiento Planificado[5] (TPB) (Ajzen I. , 1991), 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 (Pahnila, Siponen, & Mahmood, 2007) (Pahnila et al., 2007).

PBC (Perceived Behavioral Control) también es influenciada por dos creencias: creencia de control y facilidad percibida. Las creencias de control incluyen la disponibilidad de habilidades percibidas, recursos y oportunidades. La facilidad percibida es la valoración personal de la disponibilidad de recursos para el logro de un conjunto de resultados (Chuttur, 2009).

Por lo tanto, el presente modelo propuesto, tiene como base Teoría del Comportamiento Planificado (TPB) (Ajzen I. , 1991) que se compone de tres dimensiones: Actitud, norma subjetiva y control conductual percibido que condicionan la intención conductual.

A partir de los cuales y teniendo como soporte los factores propuestos en la sección anterior, se procedió a construir el modelo. Se debe aclarar que se trata de una evaluación previa a la implementación, que se sustenta en que los

[4] Theory of Reasoned Action (TRA)

[5] Theory of Planned Behavior (TPB)

estudios de intencionalidad conductual que conducen a determinado comportamiento actual o futuro, se puede observar desde dos perspectivas temporales: pre-implementación y post-implementación (Chuttur, 2009).

El presente modelo está orientado a la pre-implementación, es decir antes de implementar la Seguridad en Sistemas de Información, de modo que se pueda evaluar los factores que condicional la Intención para Implementar Seguridad en Sistemas de Información desde la perspectiva del usuario.

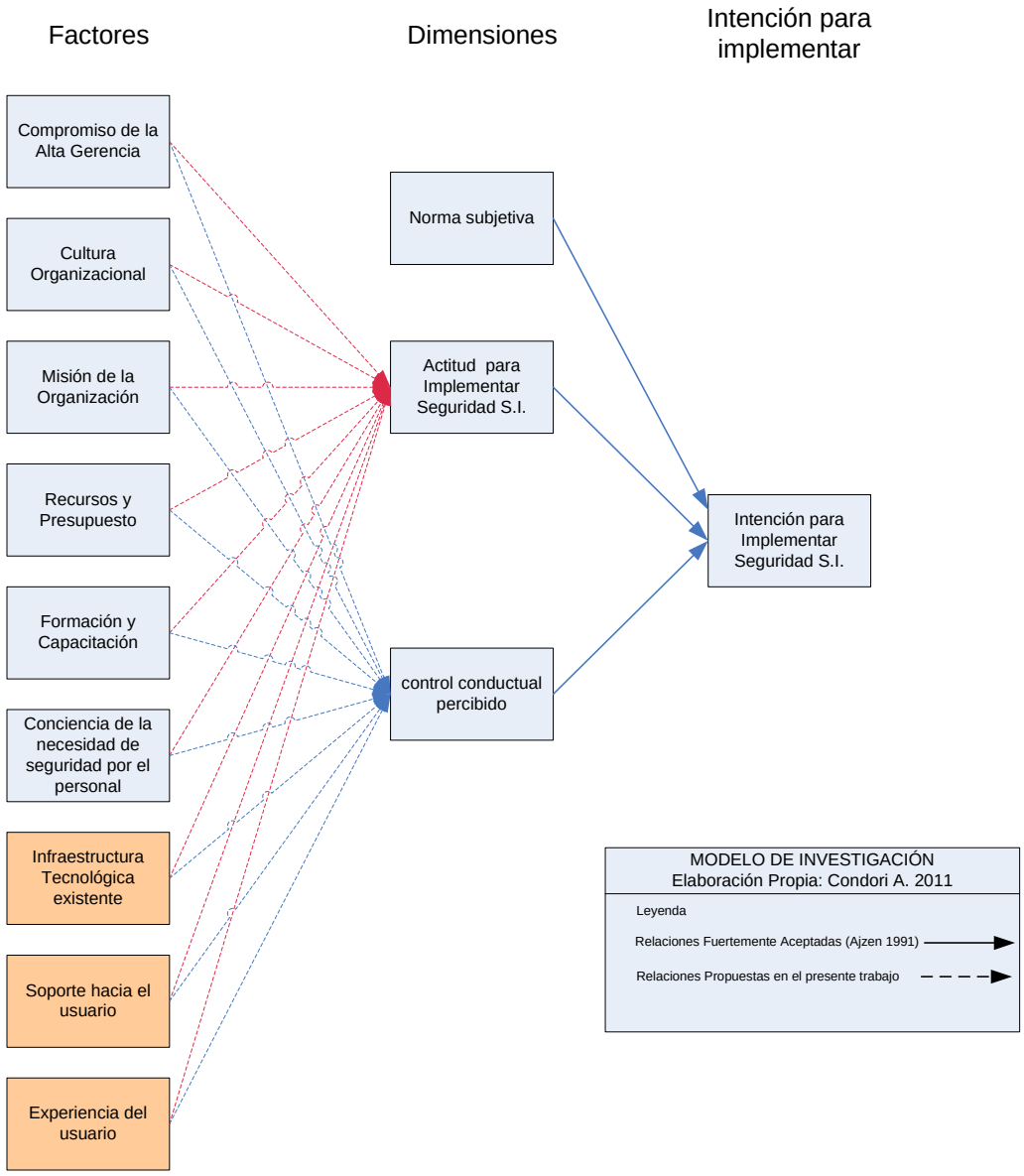

Figura 17 Modelo de investigación propuesto de Evaluación de los Factores Críticos para la Implementación de Seguridad en Sistemas de Información en la intención del Usuario.

4.1.1.2.3 Descripción Específica del modelo

A continuación se detalla de forma específica los componentes del modelo, en particular los Factores críticos de éxito y las dimensiones.

4.1.1.2.3.1 Factores Críticos de éxito

Como parte del proceso de definición de atributos, se ha tomado la referencia a los estudios de (Villegas Ortega, 2009), (Medina Quintero, 2005) a partir de las propuestas de (Abu-Zineh, 2006) (INDECOPI, 2007) (Nosworthy, 2000) (Al-Awadi & Renaud, 2008) (Bjorck, 2002) (Partida & Ezingeard Henley, 2007) para ser adaptados al presente modelo.

a. Compromiso de la Gerencia

(Villegas Ortega, 2009), 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.

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 (Kankanhalli, Hock-hai, Bernard, & Kwok-kee, 2003). Además menciona que, 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.

De acuerdo al estudio de (Al-Awadi & Renaud, 2008), se ha determinado que el entendimiento y necesidades de seguridad se deja en manos de área de TI, que coincide con lo expresado por (Fung & Jordan, 2002), que en muchos casos la gerencia no se interesa por la medición y calidad de seguridad de información en la organización debido a que

piensa que es una labor del departamento de TI, que debe seleccionar el hardware y software necesario y así mantener a la organización segura. Descuidando así el enfoque estratégico de la seguridad de información.
El soporte de la alta dirección es el factor más importante para evitar fracasos de cualquier proyecto.

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 (Villegas Ortega, 2009).
Tal como lo señalan (ISO/IEC, 2007) (ISO/IEC, 2005) (INDECOPI, 2007) (Nosworthy, 2000) (Al-Awadi & Renaud, 2008) (Partida & Ezingeard Henley, 2007), el enfoque de seguridad a implementar debe ser consistente con la cultura organizacional.
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

Siponen, explica en términos de la seguridad, las organizaciones usualmente se cruzan de brazos mientras ninguna cosa sale mal, pero cuando las cosas salen mal, repentinamente ponen atención y grandes esfuerzos se realizan para recobrarse de la situación, pero algunas veces la recuperación completa es imposible. Lo que ciertamente conduce a las organizaciones hacia problemas serios de protección de la información. Es mejor, para tales organizaciones, incrementar el interés por la Seguridad de Información (Siponen, 2001).

Algunos de los expertos afirman que 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 (Al-Awadi & Renaud, 2008).

(McKay, 2003), aclara que si la misión de la organización no está direccionada, la organización continuará luchando para asegurar su información y los empleados no se responsabilizarán seriamente, 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 la seguridad será difícil cumplir con una política de seguridad, objetivos y actividades que reflejen los objetivos del negocio de la organización (Abu-Zineh, 2006) (ISO/IEC, 2007) (ISO/IEC, 2005) (INDECOPI, 2007) (Al-Awadi & Renaud, 2008) (Partida & Ezingeard Henley, 2007) (Siponen, 2001).

d. Recursos y presupuesto

En primer lugar, debemos indicar que sin un presupuesto apropiado, las organizaciones no estarán dotadas con suficientes recursos para garantizar la adecuada protección de la información.
(Bjorck, 2002), 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.
Las organizaciones requieren el financiamiento adecuado (Doherty & Fulford, 2005), para lograr protección de la información efectiva.
La falta de presupuesto asignado a la seguridad de información da paso a la inversión insuficiente en controles apropiados (Dinnie, 1999).

Las organizaciones con falta de software o hardware apropiado, confrontan dificultades en tratar algunas cuestiones de seguridad como los mecanismos de control de acceso, o dar asistencia a los empleados para aplicar buenas prácticas de seguridad, como un cierre de sesión automático o cambios regulares de contraseña.

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

(Dhillon, Managing and Controlling Computer Misuse, 1999), argumenta que, las organizaciones deben tener una constante 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 (Al-Awadi & Renaud, 2008).
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 (Lau, 1988).

f. Conciencia de la Necesidad de Seguridad por el personal

(McKay, 2003), 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.

(Katz, 2005), encuentra que los empleados son la amenaza más grande para la protección de la información.

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 (Al-Awadi & Renaud, 2008). Se requieren programas de concientización y entrenamiento para que la implementación de seguridad de información sea exitosa.

Si los usuarios son inconscientes acerca del riesgo asociado con activos de información, entonces el daño potencial causado por usuarios podría ser imprevisible y los usuarios no serían conscientes de su responsabilidad (Solms y Solms 2004).

g. Infraestructura Tecnológica Existente

La infraestructura tecnológica, es considerada como una herramienta utilizada por los individuos para realizar sus tareas, con el objetivo de emplearla de manera estratégica (herramienta competitiva), informativa (proveer un flujo oportuno de información y comunicación en la organización) o transaccional (apoyo en las operaciones administrativas).

Pues, sin contar con una infraestructura adecuada, la implementación de un plan de seguridad no podrá ser exitosa, como ejemplo: Se tienen servicios de red obsoletos, equipos deteriorados.

h. 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 (Huang & Hao Chuang, 2007). Es necesario tener presente que, si el usuario ha percibido un mal servicio de soporte, afectará su futura intención de que la Seguridad de los Sistemas de Información sea implementada.

i. Experiencia del Usuario

(Taylor & Todd, 1995), encontraron las diferencias significativas en la intención para usar tecnología entre usuarios experimentados e inexpertos. (Thompson, Higgins, & Howell, 1994), se encontraron con que la experiencia tuvo una influencia positiva significativa en el uso. Es necesario aclarar que el factor experiencia no ha sido empleado para estudios específicos en la implementación de seguridad de información.

4.1.1.2.3.2 Dimensiones de la Intención para implementar Seguridad en Sistemas de Información por parte del Usuario.

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 (Ajzen & Fishbein, 1980). 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 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 (Ajzen & Fishbein, 1980); por lo que dicha percepción está condicional en su comportamiento. Esta valoración es dirigida por un número de referentes pertinentes como: amistades, familia y compañeros de trabajo, que influyen en la apreciación del usuario respecto a un hecho particular.

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.

Las creencias normativas se aplican a la valoración de qué tan probable o improbable es el referente de grupos de comportamiento.

La motivación a obedecer se aplica a la valoración personal, de cómo el usuario es motivado a cumplir normas en base a grupos referentes. TPB sugiere una relación positiva entre la norma subjetiva y la intención conductista.

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 (PBC[6]) es un postulado para tener una relación positiva entre la intención y el comportamiento real. Según

[6] Perceived Behavioral Control

(Ajzen I. , 1991), tiene relación para qué tan fácil o difícil debería llevar un cierto comportamiento. PBC 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 auto desempeño con la implementación del plan de seguridad, el soporte que puede recibir y los recursos que dispone.

Por ejemplo: si en 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.

4.1.1.2.3.3 Intención para Implementar Seguridad en Sistemas de Información

La intención conductista es un antecedente para el comportamiento real (Ajzen I. , 1991).

El propósito de hacer o lograr un objetivo. 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 que factores condicional la intencionalidad y consecuentemente el futuro comportamiento real para que la implementación de Seguridad en Sistemas de Información sea exitoso.

4.1.1.2.4 Hipótesis del Modelo Propuesto

Considerando la justificación de cada constructor en el modelo, se incorporan las siguientes hipótesis en conformidad con el mapa del modelo de evaluación propuesto en la Figura 17.

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	La Infraestructura Tecnológica existente influye en la Actitud para implementar Seguridad en Sistemas de Información
H14	La Infraestructura Tecnológica existente influye en el control conductual percibido
H15	El Soporte hacia el usuario influye en la Actitud para implementar Seguridad en Sistemas de Información
H16	El Soporte hacia el usuario influye en el control conductual percibido
H17	La Experiencia del usuario influye en la Actitud para implementar Seguridad en Sistemas de Información
H18	La Experiencia del usuario influye en el control conductual percibido
H19	La Actitud para implementar Seguridad en Sistemas de Información influye en la Intención para Implementar Seguridad en Sistemas de Información
H20	El control conductual percibido influye en la Intención para Implementar Seguridad en Sistemas de Información
H21	La Norma subjetiva influye en la Intención para Implementar Seguridad en Sistemas de Información

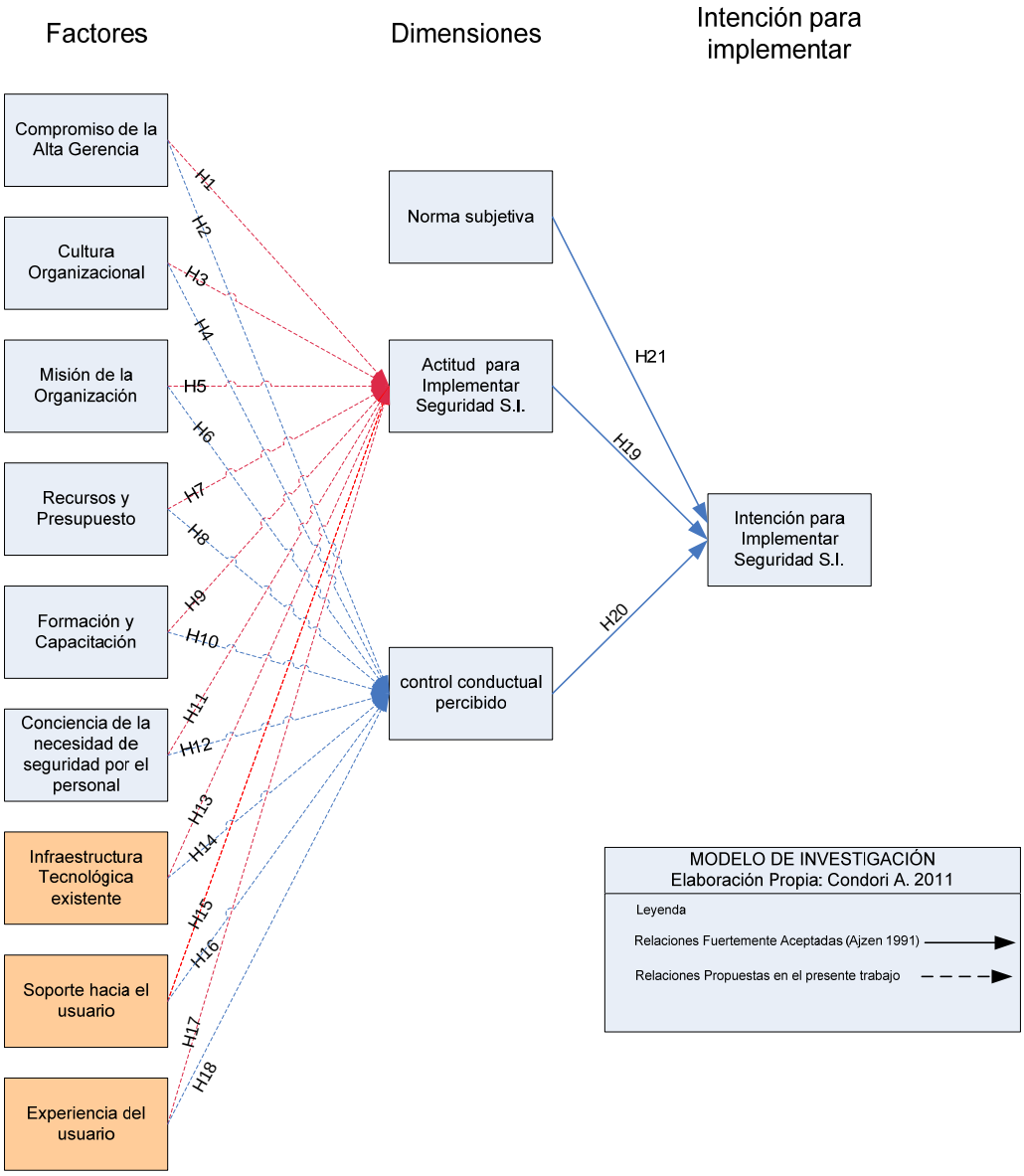

Figura 18 Hipótesis del Modelo de investigación propuesto de Evaluación de los Factores Críticos para la Implementación de Seguridad en Sistemas de Información en la intención del Usuario

4.1.2 Diseño de la Guía Metodológica para Evaluar los Factores Críticos de Éxito que Influyen en la Intención del Usuario en la Implementación de Seguridad en Sistemas de Información

4.1.2.1 Alcance de la Guía Metodológica

La presente Guía Metodológica para evaluar Los Factores Críticos de Éxito para la Implementación de Seguridad en Sistemas de Información, se resume en:

- Puede ser utilizada en cualquier escenario de Sistemas de Información, donde se pretenda Implementar Seguridad de Información, debido a que da la libertad de formular un propio submodelo para evaluar; mas, un mismo modelo aplicado en realidades diferentes producirá resultados divergentes que variarán dependiendo del caso estudiado (Villegas Ortega, 2009).

- Considera, basado en el modelo de TPB (Ajzen I. , 1991) que, la intención esperada para implementar Seguridad en Sistemas de Información requiere: la actitud, la creencia subjetiva, y el control conductual.

- Al igual que el modelo TPB (Ajzen I. , 1991), es preciso aclarar que las interacciones entre los propios factores de implementación y entre las propias dimensiones de éxito, están fuera del alcance de ésta investigación, debido a que se busca la causalidad de ellas.

- Este estudio no considera el síndrome de Bournout, el cual se define como: "Un tipo especial de estrés laboral e institucional generado por aquellas profesiones caracterizadas por una relación constante y directa con otras personas, especialmente en aquellas profesiones que mantienen una relación de ayuda y que supone una relación interpersonal intensa con los beneficiarios del propio trabajo" (Villegas Ortega, 2009).

4.1.2.2 Descripción general de la Guía Metodológica

La presente Guía tiene una implicancia práctica, debido a que sintetiza en sus 17 pasos, la identificación de los factores y dimensiones de mayor incidencia en la intención del usuario, aclarando que ha sido adaptado a partir de la guía propuesta por (Villegas Ortega, 2009) que consta de 18 pasos.

Tal como señala Villegas “El pragmatismo de la Guía puede servir como una herramienta útil a las organizaciones que deseen planear evaluaciones para Implementar Seguridad en sus Sistemas de Información”.

La Guía Metodológica, inicia con la selección del proceso de negocio y el Sistema de Información, donde se desea evaluar los Factores Críticos para la Implementación de Seguridad de Información, así como la conformación de un equipo de trabajo multidisciplinario; seguidamente se sugiere la selección de los factores, las dimensiones, los cuales deben coincidir con la perspectiva de evaluación. La selección de factores permitirá la autoselección de las preguntas de investigación (hipótesis), las preguntas seleccionadas conformarán el cuestionario que finalmente será utilizado para la ejecución de las encuestas piloto o definitiva, una vez efectuadas las encuestas, se procederá a procesar dicha información para finalmente obtener los resultados que permitan validar las hipótesis planteadas (Villegas Ortega, 2009).

4.1.2.3 Descripción específica de la Guía Metodológica

Con la finalidad de describir mejor cada uno de los pasos, la presente Guía Metodológica toma en cuenta el flujo grama presentado en la Figura 19.

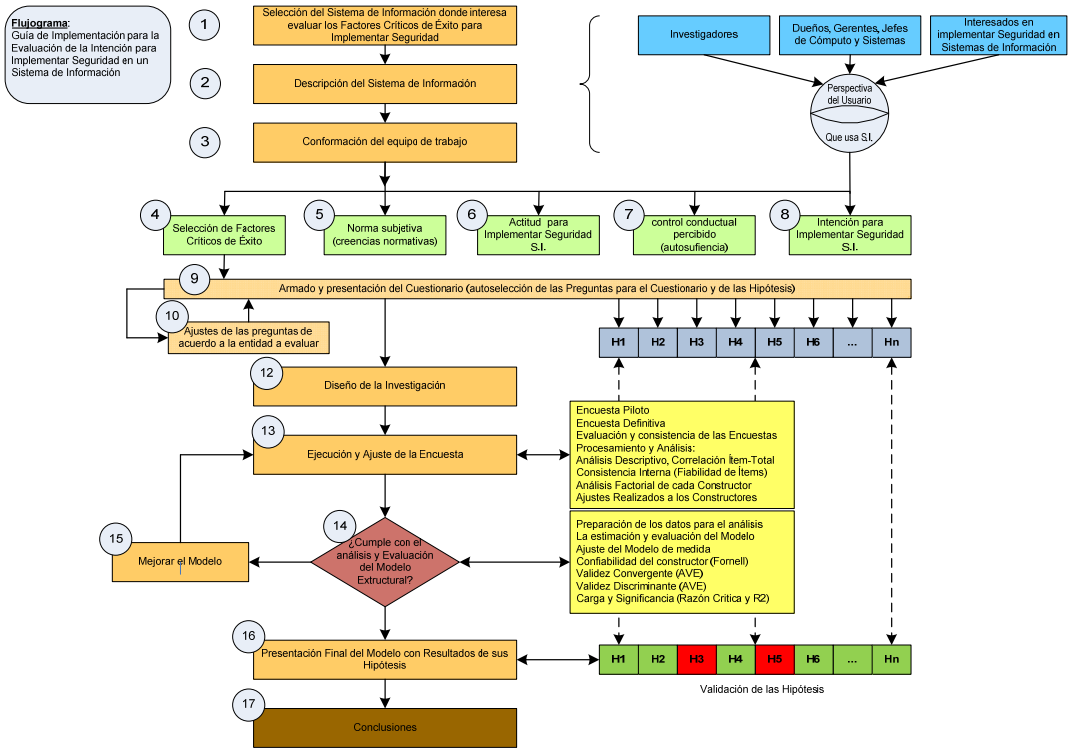

Figura 19 Flujo grama para la implementación de la Guía Metodológica del Modelo

4.1.2.3.1 Selección del Sistema de Información donde interesa evaluar los Factores Críticos de Éxito para Implementar Seguridad.

La selección del Sistema de Información debe cumplir con el requisito fundamental de ser soportado por tecnología computacional, donde se pretenda estudiar los Factores Críticos de Éxito para Implementar Seguridad desde la perspectiva de intención del usuario.

Adicionalmente, se debe tener presente las siguientes recomendaciones adaptadas a partir de (Villegas Ortega, 2009):

- Poder acceder a la empresa o empresas que se desea estudiar;
- Conocer el Sistema de Información o parte del que se desea investigar;
- Identificar la problemática de los posibles factores de quienes se desea evaluar la intencionalidad del usuario;
- Conocer la población aproximada que se desea estudiar, es decir, cuantos usuarios utilizan el sistema de información;
- Tener conocimiento del marco teórico que sustente la investigación, así como el pleno conocimiento del Sistema de Información.

Ejemplo:

> El Sistema de Académico que involucra las matrículas, registro y consulta de notas, sílabos, es crítico para las Entidades Educativas Superiores Públicas por lo que requiere establecer las medidas necesarias de protección que garanticen la Confiabilidad, Integridad, Disponibilidad de la información, pues los incidentes de seguridad en dicho sistema generan impacto severo en la continuidad del negocio. Más aun que, en el caso particular de la Universidad Nacional del Altiplano, cuenta con 15400 estudiantes en pregrado, 789 docentes y 679 empleados administrativos….
>
> …por tanto se selecciona el "SISTEMA ACADEMICO DE LA UNIVERSIDAD NACIONAL DEL ALTIPLANO".

4.1.2.3.2 Descripción del Sistema de Información

En este punto se describe el Sistema de Información y los subsistemas que lo componen que se desea evaluar.

Ejemplo:

> La Universidad Nacional del Altiplano ha implementado un SI denominado: Sistema Académico de gestión de matrículas y notas (SISACAD)…
>
> …Dicho SI, brinda soporte a una de las principales transacciones electrónicas de datos en matrículas, que se interconecta con el sistema bancario bajo el estándar, y que en primer lugar permite…
>
> … Un subsistema de validación de deudas, que verifica…

4.1.2.3.3 Conformación de equipo de trabajo

Tomando como referencia a (Villegas Ortega, 2009), se sugiere la conformación de un equipo de trabajo multidisciplinario, el cual, dado la presente Guía, deberá estar conformado por:

Al menos un investigador principal, el cual puede ser el jefe de sistemas, jefe de proyectos para Implementar Seguridad en Sistemas de Información, consultor en Seguridad o cualquier interesado en evaluar los factores críticos de éxito para implementar seguridad.

Un profesional estadístico para el procesamiento y apoyo en el análisis de la información, de preferencia con especialización en análisis multivariado;

Encuestadores o personal de apoyo para el levantamiento de información.

Ejemplo:

El equipo está conformado por: Ing. Henry Iván Condori Alejo, el cual tendrá la función o rol de investigador principal. Personal de apoyo para el procesamiento de la información. Tres encuestadores presenciales, como personal de apoyo….

4.1.2.3.4 Selección de los Factores críticos de éxito

A continuación se recomienda seleccionar todos los Factores críticos de éxito, los cuales están representados en el modelo, pues el modelo persigue determinar cuáles son los más críticos para implementar Seguridad en contexto organizacional determinado.

Sin embargo es posible la selección parcial de factores, en dicha selección debemos tener presente las siguientes reglas (Villegas Ortega, 2009):

Regla 1. Se debe seleccionar al menos dos factores críticos de éxito, uno debe tener presente que dada la selección de un factor, el modelo sólo medirá los factores seleccionados. La selección debe darse en conformidad con la percepción que su relevancia y pertinencia tengan en el proceso investigado el cual debe estar debidamente justificado:

Ejemplo:

Seleccionaremos los siguientes factores críticos de éxito:

a) Formación y capacitación
b) Conciencia de la necesidad de seguridad por el personal
c) Infraestructura Tecnológica
d) Soporte hacia el usuario
e) Experiencia del usuario

A continuación justificamos cada uno de estos atributos seleccionados:

a) Formación y capacitación, debido que quisiéramos determinar el grado de significancia que este factor tiene en la intención de implementar Seguridad, pues son los usuarios lo que realmente emplean los Sistemas de Información cada día.
b) Conciencia de la necesidad de seguridad por el personal, debido que deseamos medir el facto de conciencia de los usuario frente a los incidentes de seguridad y su relación con la intención de implementar Seguridad. Restando el rol critico del usuario en su actitud para el éxito del plan de seguridad de S.I.

…

Regla 2. Al seleccionar factor, inmediatamente debemos seleccionar todos las dimensiones a los cuales están relacionados, salvo que uno esté interesado en evaluar sólo una dimensión, en dicho caso, se podrá seleccionar dicha dimensión para su evaluación.

Ejemplo:

Del ejemplo anterior, seleccionaremos los siguientes factores críticos de éxito: Formación y capacitación, Conciencia de la necesidad de seguridad por el personal, Infraestructura Tecnológica y Experiencia del usuario, se seleccionarán automáticamente la siguiente dimensión:

- Actitud para Implementar Seguridad S.I.

Regla 3. Al seleccionar un determinado factor, debemos tener presente las características referidas en los factores descritos en 4.2.3, así como la medida asociada para cada pregunta que conforma el atributo. Hay que tener presente que la selección de la cantidad de preguntas (ítems), se sugiere que sean tres (03) como mínimo, según las recomendaciones de muchos autores, aunque lo recomendable es de cinco a siete preguntas para cada factor (constructor). Cabe precisar que nuevas preguntas y factores pueden ser añadidos, los cuales deberán de estar debidamente sustentados (Villegas Ortega, 2009).

Ejemplo:

Selección de la pregunta de investigación asociada al factor: "Formación y Capacitación":			
Factor	**Pregunta de Investigación**	**Fuente**	**Influencia y características Asociadas**
Formación y Capacitación	Su institución lo capacita frecuentemente en temas tecnológicos.	Elaboración propia a partir de (Dhillon, Managing and Controlling Computer Misuse, 1999)	Continuidad formación

A continuación se presenta el listado de preguntas consideradas detalladamente por cada factor crítico de éxito y debidamente justificadas.

Factor: Compromiso de la Alta Gerencia

Se sugiere incorporar las siguientes preguntas al cuestionario:

Tabla 8 Preguntas del Constructor: Compromiso de la Alta Gerencia

Factor	**Pregunta de Investigación En la implementación de proyectos de Sistemas Previos**	**Fuente**	**Influencia y características Asociadas**
Compromiso de la Alta Gerencia	Sintió el compromiso de la Alta Dirección en todo el proyecto de sistemas.	Q16 (Medina Quintero, 2005)	Apoyo y compromiso

	Los directivos participaron activamente y con responsabilidad.	Q17 (Medina Quintero, 2005)	Resistencia al cambio, aceptación del Proyecto.
	Existió algún tipo de motivación, reconocimiento, recompensa o aumentos por parte de un directivo cuando se implemento el Proyecto.	(Villegas Ortega, 2009)	Motiva, financia recursos, incentiva
	Los directivos participaron activamente en el planeamiento o mejoras al Proyecto.	Q18 (Medina Quintero, 2005)	Necesidades del negocio
	Las personas responsables (directivos, sobre todo) apoyaron con los recursos económicos y materiales para llevar a cabo el proyecto.	Q7 (Medina Quintero, 2005)	Administración del presupuesto, financia recursos, incentiva, negocia
	Existió cambio constante de los directivos durante el proyecto.	Elaboración propia	Compromiso
	Los directivos dejan en manos del área de Sistemas los aspectos de seguridad de información.	Elaboración propia	Compromiso

Factor: Cultura Organizacional

Se sugiere incorporar las siguientes preguntas al cuestionario:

Tabla 9 Preguntas del Constructor: Cultura Organizacional

Factor	Pregunta de Investigación	Fuente	Influencia y características Asociadas
Cultura Organizacional	Usted como usuario, tiene los conocimientos necesarios para la operación de una computadora.	Q13 (Medina Quintero, 2005)	Idioma
	Existen relaciones amistosas con el personal de técnico de sistemas.	Q14 (Medina Quintero, 2005)	Conductas, actitudes,
	Existen factores políticos internos que afectan a usted como usuario y al desarrollo de un proyecto de Sistemas.	Q15 (Medina Quintero, 2005)	sistema de valores, pretensiones, motivaciones
	Su entorno laboral es adecuado para el desarrollo de de Seguridad en los Sistemas.	(Villegas Ortega, 2009)	Las perspectivas del cambio social, orientación temporal, idioma
	Considera usted que su ambiente de trabajo favorecería la implementación de Proyecto de Seguridad de Información.	(Villegas Ortega, 2009)	Las perspectivas del cambio social, orientación temporal, idioma
	Una vez iniciado el proyecto de sistemas, usualmente se cancela por factores políticos, económicos u otros intereses.	(Villegas Ortega, 2009)	Las perspectivas del cambio social, externalidades
	Se siente usted muy comprometido con las actividades ligadas a la protección y seguridad de datos de los Sistemas de Información que usa.	Adaptado de(Villegas Ortega, 2009)	sistema de valores, motivaciones

Factor: Misión de la Organización

Se sugiere incorporar las siguientes preguntas al cuestionario:

Tabla 10 Preguntas del Constructor: Misión de la Organización

Factor	Pregunta de Investigación	Fuente	Influencia y características Asociadas
Misión de la Organización	Considera que la misión de la organización es clara.	Elaboración propia a partir de (Siponen M. T., 2001)	Claridad
	En su dependencia se tienen metas y objetivos claros.	Elaboración propia a partir de (Al-Awadi & Renaud, 2008)	Claridad y alineamiento
	Dichas metas y objetivos se cumplen a cabalidad.	Elaboración propia a partir de (McKay, 2003)	cumplimiento
	Los sistemas apoyan al cumplimiento de las metas y objetivos de su dependencia.	Elaboración propia a partir de (Abu-Zineh, 2006) (ISO/IEC, 2005) (Siponen M. T., 2001)	Cumplimiento y alineamiento
	Considera que si existe errores en los sistemas (por virus, fallas, perdida de información, etc.) afectaría el logro de las metas y objetivos de su dependencia.	Elaboración propia a partir de (Abu-Zineh, 2006) (ISO/IEC, 2005) (Siponen M. T., 2001)	Seguridad y cumplimiento
	Considera que la seguridad en los sistemas es importante para el cumplimiento de los planes de su dependencia y su institución.	Elaboración propia a partir de (Abu-Zineh, 2006) (ISO/IEC, 2005) (Siponen M. T., 2001)	Seguridad y cumplimiento

Factor: Recursos y Presupuesto

Se sugiere incorporar las siguientes preguntas al cuestionario:

Tabla 11 Preguntas del Constructor: Recursos y Presupuesto

Factor	Pregunta de Investigación	Fuente	Influencia y características Asociadas
Recursos y Presupuesto	Existe disponibilidad de los recursos materiales (CPU, Muebles, antivirus etc.) que se usa para que los Sistemas funcionen adecuadamente.	Adaptado de (Villegas Ortega, 2009)	Aprovechamiento óptimo de materiales (disponibilidad)

	Siente que hay prioridad en el otorgamiento de los recursos materiales que se usa en su trabajo con los sistemas.	(Villegas Ortega, 2009)	Aprovechamiento óptimo económico y de materiales
	Percibe que se asigna el suficiente personal técnico y de apoyo para el soporte de los sistemas.	Adaptado de Q14 (Medina Quintero, 2005)	Apoyo gerencial , inversión, apoyo óptimo de activos humanos
	Usa todos los materiales que dispone para su trabajo con los Sistemas.	(Villegas Ortega, 2009)	Aprovechamiento óptimo de materiales
	Los recursos que Ud. Solicita para los sistemas son oportunamente atendidos.	Elaboración propia a partir de (Doherty & Fulford, 2005) (Dinnie, 1999)	Necesidades, Aprovechamiento óptimo
	Siente que hay demora en su trabajo por falta de recursos para mejorar los sistemas y que teniendo sistemas más eficientes podría evitar demoras.	Adaptado de (Villegas Ortega, 2009)	Necesidades, Aprovechamiento óptimo
	Cree que son suficientes la cantidad y competencias del personal de sistemas.	Adaptado de (Villegas Ortega, 2009)	Inversión, apoyo óptimo de activos humanos (personal de sistemas competente)
	Si se implementa un proyecto de sistemas, siente que se le asignara los recursos y presupuestos necesarios oportunamente.	Elaboración propia a partir de (Doherty & Fulford, 2005) (Dinnie, 1999)	Necesidades, Aprovechamiento óptimo

Factor: Formación y Capacitación

Se sugiere incorporar las siguientes preguntas al cuestionario:

Tabla 12 Preguntas del Constructor: Formación y Capacitación

Factor	Pregunta de Investigación	Fuente	Influencia y características Asociadas
Formación y Capacitación	Su institución lo capacita frecuentemente en temas de informática y tecnológicos.	Elaboración propia a partir de (Dhillon, Managing and Controlling Computer Misuse, 1999)	Continuidad formación
	Ha recibido capacitación útil por parte del área de sistemas de cómo proteger su información.	Elaboración propia a partir de (Al-Awadi & Renaud, 2008)	Orientación en seguridad de activos
	En su institución los han capacitado o formado en temas de seguridad de información.	Elaboración propia a partir de	Capacitación y formación en temas de

		(Al-Awadi & Renaud, 2008)	seguridad
	En su institución se implementan talleres de formación y entrenamiento en temas de seguridad y protección de información.	Elaboración propia a partir de (Lau, 1988)	Capacitación y formación en temas de seguridad
	Siente que su institución se preocupa por capacitarlo en temas actuales de informática y tecnológicos.	Elaboración propia a partir de (Dhillon, Managing and Controlling Computer Misuse, 1999)	Importancia Capacitación y formación

Factor: Conciencia de la necesidad de seguridad por el personal

Se sugiere incorporar las siguientes preguntas al cuestionario:

Tabla 13 Preguntas del Constructor: Conciencia de la necesidad de seguridad por el personal

Factor	Pregunta de Investigación	Fuente	Influencia y características Asociadas
Conciencia de la necesidad de seguridad por el personal	Considera que la seguridad de la información de su institución es importante y debe tomarse las medidas adecuadas de protección.	Elaboración propia a partir de (Siponen M. T., 2001)	Importancia general
	Siente que necesita seguridad y protección confiable en su computador para evitar pérdida, daños y modificación de la información con que trabaja.	Elaboración propia a partir de (Siponen M. T., 2001)	Importancia particular
	Siente que podría ocurrir que un virus informático ocasione pérdida o deterioro de su información que retrasaría o perjudicaría su trabajo por lo que se debe proteger la información.	Elaboración propia a partir de (McKay, 2003) (Al-Awadi & Renaud, 2008)	Incidentes de seguridad software
	Siente que podría ocurrir que un fallo eléctrico ocasione pérdida o deterioro de su información que retrasaría o perjudicaría su trabajo por lo que se debe proteger la información.	Elaboración propia a partir de (McKay, 2003) (Al-Awadi & Renaud, 2008)	Incidentes de seguridad hardware
	Siente que podría ocurrir que un robo ocasione pérdida o deterioro de su información que retrasaría o perjudicaría su trabajo por lo que se debe proteger la información.	Elaboración propia a partir de (McKay, 2003) (Al-Awadi & Renaud, 2008)	Incidentes de seguridad factores externos
	Es importante cambiar las contraseñas de acceso al sistema frecuentemente.	Elaboración propia a partir de (Katz, 2005)	Conciencia sobre seguridad acceso
	Es importante no compartir su computador, contraseñas del sistema con otras personas.	Elaboración propia a partir de (Katz, 2005)	Conciencia sobre seguridad acceso
	Realiza frecuentemente copias de su información	Elaboración	Conciencia sobre

	(backup).	propia a partir de (Hyeun-Suk, Cheongtag, & Young U., 2009)	el respaldo de seguridad

Factor: Infraestructura Tecnológica existente

Se sugiere incorporar las siguientes preguntas al cuestionario:

Tabla 14 Preguntas del Constructor: Infraestructura Tecnológica existente

Factor	Pregunta de Investigación	Fuente	Influencia y características Asociadas
Infraestructura Tecnológica existente	Cuenta con los recursos informáticos (computadora, impresora) adecuados para realizar su trabajo cotidiano.	Q35 (Medina Quintero, 2005)	Recurso informatico, recurso estratégico recurso transaccional
	Las computadoras trabajan eficientemente y sin fallas.	Q11 (Medina Quintero, 2005)	Recurso informático, recurso estratégico recurso transaccional
	Las computadoras están interconectadas por una red para compartir de información.	Adaptado de Q12 (Medina Quintero, 2005)	Recurso informático, recurso estratégico recurso transaccional
	La información se obtiene a tiempo gracias a la infraestructura existente.	Adaptado de Q26 (Medina Quintero, 2005)	Flujo oportuno de información y comunicación
	Cuenta con el servicio de internet adecuado.	Elaboración propia	Comunicación global

Factor: Soporte hacia el usuario

Se sugiere incorporar las siguientes preguntas al cuestionario:

Tabla 15 Preguntas del Constructor: Soporte hacia el usuario

Factor	Pregunta de Investigación	Fuente	Influencia y características Asociadas
Soporte hacia el usuario	Siente una atención y asistencia técnica eficiente del área de sistemas cuando Ud. Tiene problemas.	Adaptado de (Huang & Hao Chuang, 2007)	Atención y asistencia

	Siente que el área de soporte de sistemas ofrece soluciones en el tiempo adecuado.	Adaptado de (Villegas Ortega, 2009)	compromiso
	Cree que el personal del área de sistemas tiene el suficiente conocimiento y experiencia para ayudarlo cuando tiene problemas con el sistema de información o su computador.	Elaboración propia a partir de (Huang & Hao Chuang, 2007)	Calidad de soporte
	Cree que el personal del área de sistemas tiene el suficiente conocimiento y experiencia para ayudarlo con temas de seguridad de información.	Elaboración propia a partir de (Huang & Hao Chuang, 2007)	Calidad de soporte en seguridad de información

Factor: Experiencia del usuario

Se sugiere incorporar las siguientes preguntas al cuestionario:

Tabla 16 Preguntas del Constructor: Experiencia del usuario

Factor	Pregunta de Investigación	Fuente	Influencia y características Asociadas
Experiencia del usuario	Es un experto en computadoras y sistemas.	Elaboración propia a partir de (Huang, Patrick Rau, & Salvendy, 2007) (Novakovic, McGill, & Dixon, 2009)	Experiencia en sistemas y computadoras
	En cuanto a los problemas que se presentan con el sistema no requiere asistencia técnica.	Elaboración propia a partir de (Huang, Patrick Rau, & Salvendy, 2007) (Novakovic, McGill, & Dixon, 2009)	Solución de problemas
	Conoce y utiliza métodos de seguridad de información para protegerse.	Elaboración propia a partir de (Huang, Patrick Rau, & Salvendy, 2007) (Novakovic, McGill, & Dixon, 2009)	Experiencia con seguridad de información
	Es natural navegar por internet y sabe cómo protegerse de virus y otros ataques.	Elaboración propia a partir de (Venkatesh, Morris, Davis, & Davis, 2003) (Novakovic, McGill, & Dixon, 2009)	Experiencia con tecnologías web
	Es natural utilizar correo electrónico, y sabe cómo protegerse de virus y otros ataques.	Elaboración propia a partir de (Venkatesh, Morris, Davis, &	Experiencia con tecnologías de email

		Davis, 2003) (Novakovic, McGill, & Dixon, 2009)	

4.1.2.5.3.5 Selección de las dimensiones

Se sugiere que de ningún modo se prescinda de las dimensiones, las cuales son fuertemente aceptadas por la mayoría de autores a partir de la TPB de (Ajzen I. , 1991).

Actitud para Implementar Seguridad S.I.

Se sugiere incorporar las siguientes preguntas al cuestionario:

Tabla 17 Preguntas del Constructor: Actitud para Implementar Seguridad S.I.

Factor	Pregunta de Investigación	Fuente	Influencia y características Asociadas
Actitud para Implementar Seguridad S.I.	Implementar seguridad en los Sistemas de Información será útil para mi trabajo.	Adaptado de (Venkatesh, Morris, Davis, & Davis, 2003) (Huang & Hao Chuang, 2007) (Bulgurcu, Cavusoglu, & Benbasat, 2010)	Sentimientos positivos o negativos utilidad
	Las ventajas de utilizar seguridad en los Sistemas de Información sobrepasará sus desventajas.	Adaptado de (Venkatesh, Morris, Davis, & Davis, 2003) (Huang & Hao Chuang, 2007) (Bulgurcu, Cavusoglu, & Benbasat, 2010)	Sentimientos positivos o negativos beneficio
	A futuro creo que será necesario trabajar en un sistema con Seguridad de Información.	Adaptado de (Venkatesh, Morris, Davis, & Davis, 2003) (Huang & Hao Chuang, 2007) (Bulgurcu, Cavusoglu, & Benbasat, 2010)	Sentimientos positivos o negativos necesidad
	Implementar seguridad en los Sistemas de Información es importante.	Adaptado de (Venkatesh, Morris, Davis, & Davis, 2003) (Huang & Hao Chuang, 2007) (Bulgurcu, Cavusoglu, & Benbasat, 2010)	Sentimientos positivos o negativos importancia

Control conductual percibido (autosuficiencia)

Se sugiere incorporar las siguientes preguntas al cuestionario:

Tabla 18 Preguntas del Constructor: Control conductual percibido.

Factor	Pregunta de Investigación	Fuente	Influencia y características Asociadas
Control conductual percibido autosuficiencia	Tengo suficientes habilidades para adaptarme a la Implementación de Seguridad de Información.	Adaptado de (Huang & Hao Chuang, 2007) (Bulgurcu, Cavusoglu, & Benbasat, 2010)	habilidades
	Tengo suficientes conocimientos para adaptarme a la Implementación de Seguridad de Información.	Adaptado de (Huang & Hao Chuang, 2007) (Bulgurcu, Cavusoglu, & Benbasat, 2010)	conocimiento
	Tengo suficientes competencias para adaptarme a la Implementación de Seguridad de Información.	Adaptado de (Huang & Hao Chuang, 2007) (Bulgurcu, Cavusoglu, & Benbasat, 2010)	competencias

Norma subjetiva (creencias normativas)

Se sugiere incorporar las siguientes preguntas al cuestionario:

Tabla 19 Preguntas del Constructor: Norma subjetiva (creencias normativas).

Factor	Pregunta de Investigación	Fuente	Influencia y características Asociadas
Norma subjetiva (creencias normativas)	En general mi institución está preparada para implementar la seguridad en Sistemas de Información.	Adaptado de (Venkatesh, Morris, Davis, & Davis, 2003)	A nivel organizacional
	Mis compañeros de trabajo piensan que se debe implementar la seguridad en Sistemas de Información.	Adaptado de (Huang & Hao Chuang, 2007) (Bulgurcu, Cavusoglu, & Benbasat, 2010)	A nivel de los compañeros de trabajo
	Mi jefe inmediato piensa que se debe implementar la seguridad en Sistemas de Información.	Adaptado de (Huang & Hao Chuang, 2007) (Bulgurcu, Cavusoglu, & Benbasat, 2010)	A nivel de los jefes inmediatos
	Los gerentes/autoridades piensan que se debe implementar la seguridad en Sistemas de Información.	Adaptado de (Huang & Hao Chuang, 2007) (Bulgurcu, Cavusoglu, & Benbasat, 2010)	A nivel de los gerentes o autoridades de alto rango

Intención para Implementar Seguridad en los Sistemas de Información.

Se sugiere incorporar las siguientes preguntas al cuestionario:

Tabla 20 Preguntas del Constructor: Intención para Implementar Seguridad en los Sistemas de Información.

Factor	Pregunta de Investigación	Fuente	Influencia y características Asociadas
Intención para Implementar Seguridad en los Sistemas de Información	Tengo la intención de usar la implementación de la Seguridad en Sistemas de información.	Adaptado de (Venkatesh, Morris, Davis, & Davis, 2003)	Intención de uso
	Tengo la intención de apoyar la implementación de la Seguridad en Sistemas de información.	Adaptado de (Huang & Hao Chuang, 2007) (Bulgurcu, Cavusoglu, & Benbasat, 2010)	Intención de apoyo al proyecto
	Tengo la intención de asumir la responsabilidades de la implementación de la Seguridad en Sistemas de información en <tiempo> meses.	Adaptado de (Huang & Hao Chuang, 2007) (Bulgurcu, Cavusoglu, & Benbasat, 2010)	Intención de asumir responsabilidades
	Tengo la intención de proteger la información y los recursos tecnológicos de acuerdo al Sistema de Seguridad de Información que se implementará.	Adaptado de (Huang & Hao Chuang, 2007) (Bulgurcu, Cavusoglu, & Benbasat, 2010)	Intención de cumplir el plan de seguridad

4.1.2.3.6 Armado y presentación final del cuestionario

Paso seguido, se ensambla el cuestionario con todas las preguntas consideradas en los pasos previos. Hay que tener presente que en la selección de la cantidad de preguntas (ítems), es recomendable, según algunos autores, que sean tres (03) como mínimo, aunque lo ideal es de cinco a siete preguntas para cada factor (constructor) (Villegas Ortega, 2009).

Cabe precisar que nuevas preguntas y factores pueden ser añadidos, los cuales deberán de estar debidamente sustentados (Hair & etal, 1999).

En el Anexo 1 se presenta el cuestionario sugerido al evaluar la Intención para Implementar Seguridad en los Sistemas de Información.

El modelo planteado se fundamenta en la recolección de información mediante cuestionarios, los cuales responden a diferentes constructores, siendo su relación fundamentada por cada una de las 21 hipótesis presentadas en el acápite 4.2.3 y 4.2.4 referidos a los componentes y las hipótesis del modelo propuesto.

En necesario precisar que no es necesaria la selección de todas las hipótesis planteadas en el modelo, sino sólo de las que se desea investigar, pudiendo identificarse nuevas relaciones, las cuales deberán estar debidamente sustentadas en un marco teórico.

Ejemplo:

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 La Actitud para implementar Seguridad en Sistemas de Información influye en Intención para Implementar Seguridad en Sistemas de Información

H14 El control conductual percibido influye en Intención para Implementar Seguridad en Sistemas de Información

4.1.2.3.7 Ajuste de las preguntas en conformidad con el proceso evaluado

Este paso contempla revisar minuciosamente las preguntas que comprenderán el cuestionario, particularizando, si fuera necesario, las preguntas a cada proceso de negocio evaluado (Villegas Ortega, 2009).

Ejemplo:

Se presenta una de las preguntas referidas a la cultura organizacional, particularizada diversos procesos de negocio diferentes: ¿Existió algún tipo de motivación, reconocimiento, recompensa o aumentos por parte de un directivo cuando se implemento el Proyecto de Sistema Académico? ¿Existió algún tipo de motivación, reconocimiento, recompensa o aumentos por parte de un directivo cuando se implemento el Proyecto de Sistema de Adquisiciones? ¿Existió algún tipo de motivación, reconocimiento, recompensa o aumentos por parte de un directivo cuando se implemento el Proyecto de Sistema de Remuneraciones?

4.1.2.3.8 Diseño de la investigación de la Metodología

El término diseño se refiere al plan concebido para obtener la información que se desea (Hernández Sampieri, Fernández Collado, & Baptista Lucio, 2010).

La presente Guía Metodológica emplea un diseño no experimental, es decir, no se varía de forma intencional las variables de interés del estudio, sino que observamos situaciones existentes tal como ocurre en su propia naturaleza, en el presente caso los sistemas de información en la organización.

No se construye ninguna situación, sino que se observan situaciones ya existentes, no provocadas intencionalmente en la investigación. La guía recomienda aplicar la recolección de datos en un sólo momento (Transversal) pudiéndose aplicar en investigaciones posteriores en diferentes momentos,

convirtiéndose en longitudinales, pero aclarando que su principal enfoque es una pre implementación.

De conformidad con la/s perspectiva/s seleccionada/s, se procederá a delimitar la población que va ser estudiada y sobre la cual se pretende generalizar los resultados a partir de la muestra, que debe reflejar de forma representativa a la población (Hernández Sampieri, Fernández Collado, & Baptista Lucio, 2010); se definirá quienes serán las personas que estarán involucradas en el estudio, para lo cual se determinara (Villegas Ortega, 2009):

- La población objetivo; se define el conjunto de personas sobre el cual se realizara el estudio.
- Marco muestral (es la información que ubica y dimensiona al universo);
- El informante;
- Diseño de muestra (Probabilística);
- El tamaño de la muestra;
- El tipo de recolección de datos (encuestas personales, por Internet, correo electrónico, teléfono).

4.1.2.3.9 Ejecución y ajuste de la encuesta

4.1.2.3.9.1 Encuesta piloto

Es conveniente la realización del piloto, de tal forma que permita ajustar los resultados del cuestionario final (encuesta definitiva), de modo que, en base a este estudio preliminar se pueda reestructurar o eliminar algunas preguntas. Es necesario mencionar que la aplicación de una encuesta piloto queda a libertad del investigador, ya que su utilidad se refuerza cuando no se cuenta con estudios preliminares, mas, como se ha sustentado en la selección de las preguntas de cada uno de los constructor, casi todas las preguntas han sido, previamente empleadas por otros investigadores (Villegas Ortega, 2009).

4.1.2.3.9.2 Cuestionario

Tal como lo señala (Villegas Ortega, 2009), se procederá a la aplicación definitiva de la encuesta final a la población objetivo mediante el tipo de encuesta seleccionado. Cabe precisar que de haberse efectuado una encuesta piloto, se deberá considerar los análisis y conclusiones obtenidos en dicho piloto antes de su aplicación,

4.1.2.4.9.3 Evaluación y consistencia de las encuestas

Con los resultados de la encuesta, se procederá a revisar los cuestionarios llenados y evaluar las inconsistencias presentadas en su correcto desarrollo, a continuación puntualizamos algunas pautas de consistencia que podrá usar el investigador:

- Las advertencias, que reflejan una aparente invalidez individual o inconsistencia de relaciones entre variables.
- La cantidad de preguntas respondidas por cada cuestionario, preguntas no contestadas consecutivamente, serán observadas.
- Serán observados los cuestionarios que tengan marcado la misma escala consecutivamente.

4.1.2.3.9.4 Procesamiento y análisis

Con los cuestionarios y efectuada su consistencia, se procede al procesamiento y análisis, empleando las siguientes técnicas (Villegas Ortega, 2009):

4.1.2.3.9.4.1 Estadística Descriptiva

En este análisis se ha incluido: la media, desviación típica, varianza, asimetría y curtosis; de esta forma explora el comportamiento de cada ítem (pregunta) de forma individual y su comportamiento con los demás ítems del factor al que pertenecen. Por lo extenso del presente acápite los resultados pueden presentarse de manera resumida.

4.1.2.3.9.4.2 Análisis de la correlación ítem-total

Está correlación es de gran relevancia porque indica la correlación entre el ítem y el puntaje total, indicando la magnitud y dirección de esta relación. Los ítems

cuyos coeficientes ítem total arrojan valores menores a 0,35 deben ser desechados o reformulados ya que las correlaciones a partir de 0,35 son estadísticamente significativas más allá del nivel del 1% (Cohen & L, 1990). Una baja correlación entre el ítem y el puntaje total puede deberse a una mala redacción del ítem o que este no sirve para medir lo que se desea medir.

4.1.2.3.9.4.3 Consistencia interna (fiabilidad de ítems)

La fiabilidad de un constructor permite comprobar la consistencia interna de todos los indicadores relacionados a este, es decir, se evalúa el grado de rigurosidad en la medición de las variables (Roldán S, Introducción a la técnica partial least squares, 2004). La confiabilidad también denominada “estabilidad de la medición” es evaluada por el alfa de Cronbach, debiendo ser su valor no menor de 0,7. El valor del alfa de Cronbach aumenta cuando las correlaciones entre los ítems y el total son altas, por ello, mejores correlaciones dan mayor fiabilidad al instrumento.

4.1.2.3.9.4.4 Análisis factorial de cada constructor

Se aplica el análisis factorial, el cual se define como una técnica estadística multivariada que se incorpora a la metodología cuantitativa que involucra variables latentes (dependientes o no observables), las cuales no pueden medirse de manera directa, estimándose a través de variables manifiestas (observadas). Para la buena aplicación del análisis factorial, se debe cumplir (Zamora Muñoz, Monroy Cazorla, & Chávez Álvarez, 2009):

- Existencia de correlaciones altas entre los ítems, si en caso se escoja la matriz de correlaciones como análisis.
- índices KMO; prueba que compara la correlación entre dos variables, eliminando el efecto de las variables restantes. Como regla empírica se considera que si KMO<0,5, es inadecuado realizar un análisis factorial a los datos. Otros autores definen que el KMO debe ser mayor a 0,7
- Determinante de la matriz de correlaciones; es una medida global de la correlación entre todas las variables, si este determinante está cercano a cero, será indicativo de que existe una estructura

de correlación importante entre las variables, y el análisis factorial puede ser pertinente.

4.1.2.3.9.4.5 Ajustes realizados a los constructores

Dentro de los resultados obtenidos en el análisis descriptivo, consistencia interna y análisis factorial, se observa y se corrige los patrones respecto a la inadecuada formación de los constructores. Para ello es necesario que se cumpla los parámetros recomendados como los valores de la correlación ítem elemento, Alfa de Cronbach, y análisis factorial, en caso de incumplimiento se deberá ajustar la formación de los constructores para su debida especificación y posterior análisis del modelo estructural.

4.1.2.3.10 Análisis y evaluación del modelo estructural

4.1.2.3.10.1 Preparación de los datos para el análisis

Se procederá a la preparación de los datos para el análisis, incluyendo la presentación de las variables exógenas, endógenas y observadas del modelo.

4.1.2.3.10.2 La estimación del modelo

La estimación puede llevarse a efecto mediante distintos procedimientos que comparten una misma finalidad (Manzano Patiño & Zamora Muñoz, 2009). La guía sugiere utilizar el método de estimación de máxima verosimilitud (ML).

Del mismo modo, la guía permite la aplicación de la técnica de estimación basada en Bootstrapping, el cual permite generar miles de estimaciones del modelo (Hair & etal, 1999).

4.1.2.3.10.3 La evaluación del modelo

Los resultados son examinados buscando estimaciones infractoras, es decir, coeficientes estimados tanto en los modelos de medida como en los estructurales que excedan los límites aceptables (Cea D´Ancona, 2002)

varianzas de error negativas o varianzas de error no significativas para cualquier constructor y los índices de ajuste absoluto, incremental o de parsimonia que sobrepasan los estándares.

Índices de ajuste absoluto, comprueban el ajuste global del modelo de ecuaciones estructurales, incluyendo sus submodelos (estructural y de medición).

Índices de ajuste de parsimonia, relacionan la bondad de ajuste del modelo con el número de coeficientes estimados, el propósito es equilibrar la bondad de ajuste con la "parsimonia" o simplicidad.

Tabla 21 Valores recomendados de los índices de ajuste

Media	Indicador	Macro	Valor
A. Índices de ajuste absoluto	Índice de razón de verosimilitud	Chi 2	Pequeño
	Índice de bondad de ajuste	GFI	>= 0,90
	Raíz cuadrada de la media de res.	RMR	Debe tender a 0
B. Índices de ajuste de parsimonia	Chi 2 normado		1,00 – 3,00
	Criterio de información de Akaike	AIC	Pequeño

4.1.2.3.10.4 Ajuste del modelo de medida

4.1.2.3.10.4.1 Confiabilidad del constructor

La confiabilidad del constructor analiza la consistencia interna de en un bloque de indicadores, se evalúa por medio de la confiabilidad compuesta (composite reliability) que sugiere un 0,707 del estadístico de Fornell (Sánchez-Franco & Roldán, 2005). Así mismo, otros autores indican que un valor de referencia común que indica fiabilidad "aceptable" es 0,70.

4.1.2.3.10.4.2 Validez convergente (varianza extraída media -AVE)

Es la validez convergente de los diferentes ítems destinados a medir un constructor, es decir, si miden realmente lo mismo, entonces el ajuste de dichos ítems será significativo y estarán altamente correlacionados. Esta evaluación se lleva a cabo por medio de la varianza extraída media (AVE,

Average Variance Extracted), que mide el monto de varianza que un constructor captura de sus indicadores, relativa a la varianza contenida en el error de medición y debiera ser más grande que el cuadrado de las correlaciones entre los constructores.

Este estadístico puede ser interpretado como una medida de confiabilidad del constructor y como una medición de la evaluación de la validez discriminante.

Los valores de AVE mayores a 0,50 establece que más de 50% de la varianza del constructor se debe a sus indicadores (Cea D´Ancona, 2002) (Hair & etal, 1999).

4.1.2.3.10.4.3 Validez discriminante (AVE)

Para evaluar la validez discriminante, la raíz cuadrada de AVE debe de ser más grande que la varianza compartida entre el constructor latente y otros latentes en el modelo (Barclay, Higgins, & Thompson, 1995).

4.1.2.3.10.4.4 Carga y significancia

Se indica la fuerza de las relaciones entre las variables dependientes e independientes. Para ello se estima los valores de las razones críticas (C.R.) y los valores de las correlaciones múltiples cuadradas (R2) y cumplir con los valores recomendados:

- Los valores recomendados de las razones criticas (CR), deben superan el valor +/- 1,96 para obtener un nivel de significancia de alfa=0,05. Bajo el cumplimiento de estos valores puede afirmarse que con un mínimo de probabilidad de error en la inferencia, que los coeficientes estimados path son estadísticamente significativos. Es decir las relaciones propuestas entre las variables son ciertas.
- Las correlaciones múltiples cuadradas (R2), indican el poder predictivo del modelo, estas indican la proporción de la varianza de dichas variables observadas, que logra ser explicada por sus predictoras (variables latentes). El valor del R2 debe ser mayor a 0,2 para que un constructor sea considerado aceptable, ya que

representaría el monto de varianza explicada por las variables predictoras.

Los coeficientes path deben ser significantes y directamente consistentes con las expectaciones; juntos, estos dos indicadores (razón crítica y correlaciones múltiples cuadradas), indican qué tan bien el modelo se desempeña, pudiendo aceptar o rechazar las hipótesis planteadas en cada caso de estudio.

4.1.2.3.11 Mejora del modelo

Cuando el modelo analizado no alcanza los niveles adecuados, pueden introducirse algunas modificaciones o correcciones, las cuales generalmente suponen una o varias de las siguientes decisiones:

· Eliminar parámetros no significativos.

· Añadir parámetros que muestren un índice de modificación elevado.

Pero, un mal ajuste del modelo también puede deberse a la omisión no deliberada de alguna variable relevante en la explicación de las relaciones causales que se analizan. Su consideración lleva a un replanteamiento de todo el modelo inicial con la inclusión de nuevas variables y la eliminación de las no significativas (Cea D´Ancona, 2002).

4.1.2.3.12 Presentación final del modelo con resultado de sus hipótesis

En este punto, se presentará el modelo con cada una de sus hipótesis aceptadas y rechazadas:

- análisis de los factores críticos de éxito relacionado con las dimensiones.
- análisis de las dimensiones de éxito relacionados con la intención del usuario para implementar seguridad en sistemas de información.

4.1.3 Evaluación del modelo propuesto en la Universidad Nacional del Altiplano Puno.

Se planteó el desarrollo del caso Universidad Nacional del Altiplano, para lo cual se seguirá con minuciosidad cada uno de los 17 pasos planteados en la Guía Metodológica propuesta. Aclarando que el caso propuesto, está orientado a evaluar cuales son los factores críticos de éxito directamente relacionados con la intención de implementar Seguridad en Sistemas de Información por parte del usuario, en el ámbito de las instituciones públicas y en particular de carácter educativo, para lo cual se inicia con la descripción del contexto general institucional y seguidamente aplicar la guía propuesta, para finalmente mostrar los resultados.

4.1.3.1 Selección del Sistema de Información donde interesa evaluar los Factores Críticos de Éxito para Implementar Seguridad.

La 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.

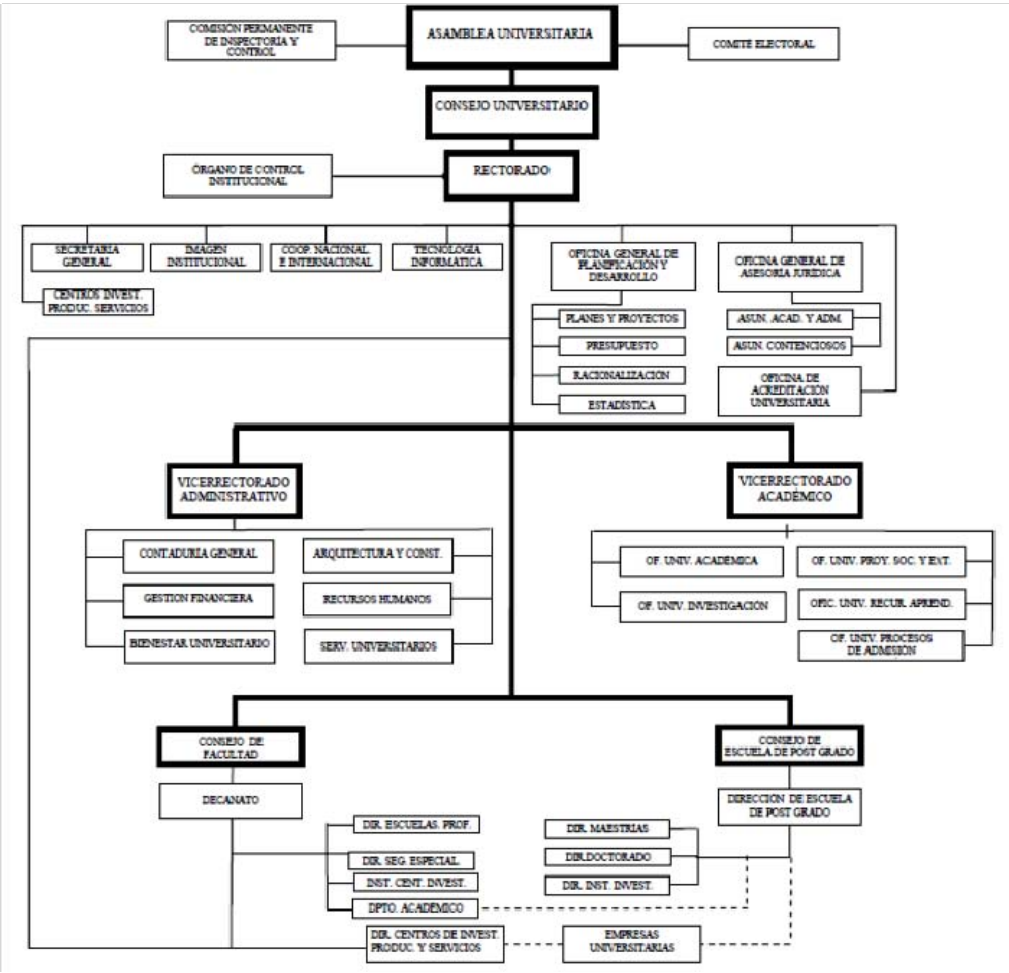

Figura 20 Organigrama Universidad Nacional del Altiplano. Fuente Oficina General de Planificación UNA-Puno

En vista que, dicho sistema involucra los procesos críticos de la UNA-Puno, y que dichos activos de información deben ser adecuadamente resguardados, se selecciona el “SISTEMA INTEGRAL ADMINISTRATIVO DE LA UNIVERSIDAD NACIONAL DEL ALTIPLANO” para el presente estudio.

4.1.3.2 Descripción de Sistema de Información.

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 garantizar el funcionamiento de los procesos críticos.

En cuanto a interconexión, está soportado mediante una plataforma de Red de datos de backbone de 1Gbps y 100mbps en cada terminal, dicho soporte de red interconecta diversos edificios geográficamente distantes en las cuales se tiene las dependencias administrativas en el radio urbano de la ciudad de Puno.

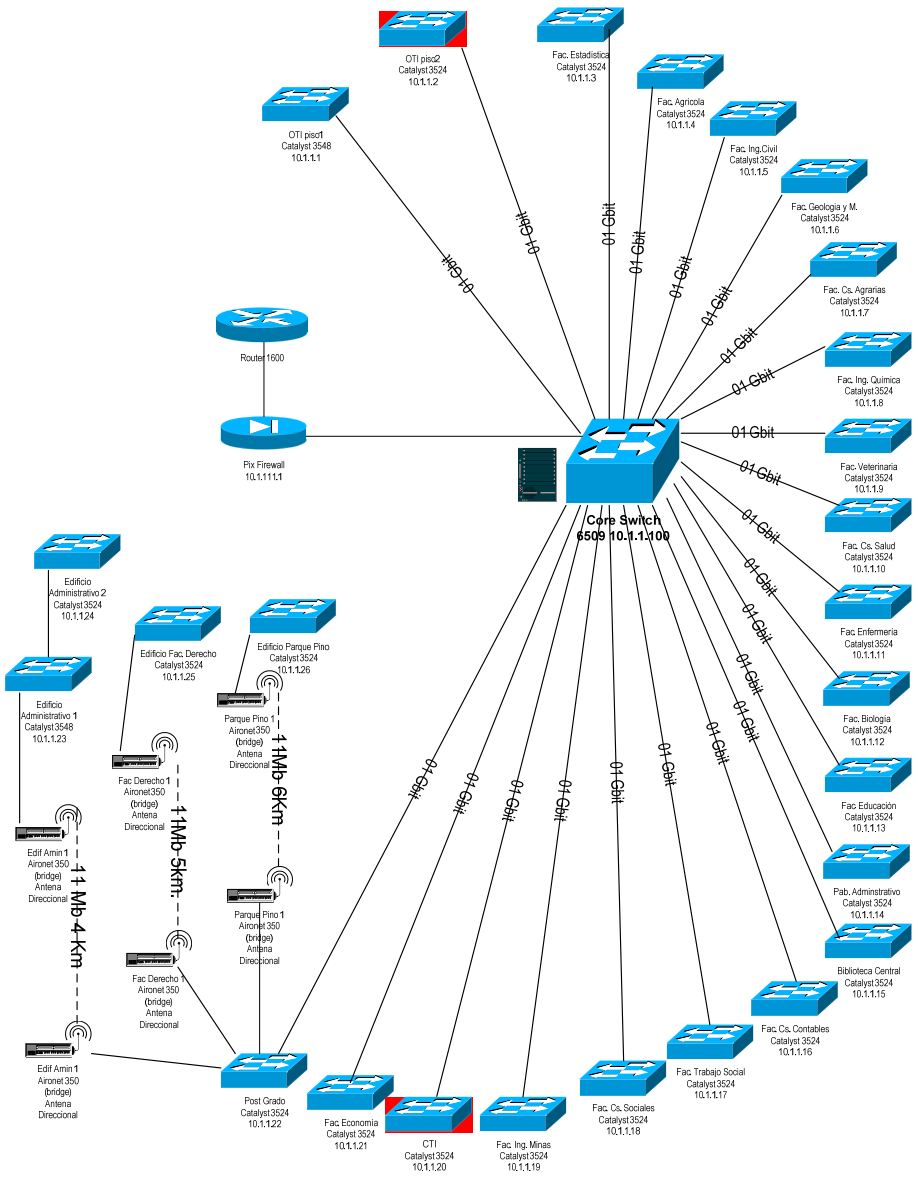

Figura 21 Topología de Red UNA-Puno, como soporte a los sistemas de Información

Es necesario aclarar, que el sistema de información integral, involucra diversas oficinas y dependencias de la UNA-Puno, que emplean en sistema como parte de sus procesos.

El Sistema de Información es una aplicación Cliente/Servidor, trabaja con Base de Datos MySQL bajo Linux.

Figura 22 Pantalla principal del Sistema de Información Integral UNA-Puno.

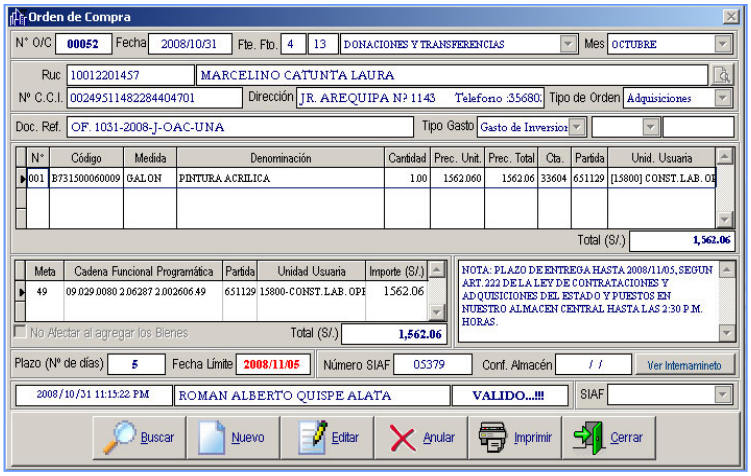

Figura 23 Interface Actual del Sistema de Información Administrativa (UNA-Puno)

Si bien es cierto el Gobierno a través de la PCM hace de uso obligatorio la norma ISO 17799 (INDECOPI, 2007), dicha norma no se ha implementado aun en la UNA-Puno, cumpliendo el requisito inicial del modelo a experimentar que está orientado a determinar que condicionaría una implementación exitosa de Seguridad en los sistemas de información.

Por lo tanto, considerando que el objeto de estudio es evaluar los factores que determinan la intención para implementar seguridad de información en el sistema administrativo de la UNA-Puno, involucra al personal que interactúa con dicho sistema, tomando como referencia el Cuadro de asignación de personal administrativo por cada dependencia.

4.1.3.3 Conformación del equipo de trabajo.

El equipo está conformado por:

- Ing. Henry Iván Condori Alejo, como investigador principal;
- Un personal de apoyo para el procesamiento estadístico;
- Tres encuestadores presenciales, como personal de apoyo.

4.1.3.4 Selección de Factores Críticos de Éxito

Se seleccionó los siguientes factores críticos de éxito:

a. Compromiso de la Gerencia
b. Cultura Organizacional
c. Misión de la Organización
d. Recursos y Presupuesto
e. Formación y Capacitación
f. Conciencia de la Necesidad de Seguridad por el personal
g. Infraestructura Tecnológica
h. Soporte hacia el usuario
i. Experiencia del usuario

A continuación se justifican cada uno de los factores seleccionados:

Compromiso de la Gerencia: Uno de los puntos más importantes, para todas las partes interesadas en la protección de la información, es obtener suficiente soporte de la alta gerencia, en el presente caso se trata de evaluar si el usuario ha sentido el compromiso de la gerencia en la implementación de proyectos previos de Sistemas de Información, lo que ciertamente le genera una expectativa a lo que podría pasar si se implementa la Seguridad de Información como un proyecto futuro. Si anteriormente no hubo compromiso de la gerencia es probable que tampoco lo haya en un nuevo proyecto.

Cultura Organizacional: Se encuentra vinculada con la interacción de valores, actitudes y conductas compartidas por todos los miembros de una empresa u organización (Villegas Ortega, 2009), en el presente caso se trata de evaluar la actual cultura organizacional y en particular el aspecto político, en vista que, en

el caso de instituciones estatales, dicho aspecto es determinante como parte de la cultura organizacional y condiciona la implementación de Seguridad de Información.

Misión de la Organización: Es importante que los usuarios interioricen la misión de la organización y así comprender cuál es el valor de los Sistemas de información, e intrínsecamente de la información para el logro de sus objetivos.

Recursos y Presupuesto: Todo proyecto requiere de recursos y presupuesto adecuados para lograr resultados, en tal sentido se trata de evaluar si el usuario considera que cuenta con los recursos necesarios y si los solicita es atendido en forma oportuna, aspecto que muchas veces resulta crítico por los procedimientos establecidos en el ámbito del sector público.

Formación y Capacitación: El proceso de mejorar las competencias del personal debe ser constante, en el presente caso, se trata de evaluar si el usuario ha recibido y recibe formación y capacitación en temas tecnológicos, en particular orientados a la seguridad de información. Es decir, si el usuario no entiende de Seguridad de información y no está capacitado adecuadamente, tendrá implicancias negativas en la implementación de Seguridad de Información. Por lo que, es necesario recordar que la Seguridad de Información no es solamente la adquisición de hardware y software de protección y respaldo, sino es vital considerar el factor humano.

Conciencia de la Necesidad de Seguridad por el personal: (Katz, 2005) indica que los empleados son la amenaza más grande para la protección de la información, pues debilitan la políticas o medidas de seguridad, y generalmente ocurre por la inconsciencia del usuario, como ejemplo extremo: muchos usuarios prefieren tener accesos a internet ilimitados, sin valorar los riesgos a que exponen la información organizacional. Por lo que, se hace necesario evaluar la conciencia que tiene el usuario.

Infraestructura Tecnológica: Considerado como el conjunto de elementos tecnológicos que da soporte al sistema de información y consecuentemente al usuario en sus tareas diarias, si no existe una adecuada infraestructura

tecnológica, existirá una influencia negativa en la Implementación de Seguridad en el Sistema de Información.

Soporte hacia el usuario: Si bien es cierto que el usuario es quien interactúa con los sistemas día a día, requiere de personal especializado en TI como soporte, se trata de evaluar cual es la expectativa de soporte que tiene el usuario, pues si se implementa Seguridad en el Sistema de Información, se requiere un soporte adecuado para su efectividad, pues caso contrario, para el usuario será una complicación innecesaria más.

Experiencia del usuario: El desempeño de un usuario novato en relación a uno experto, difiere en gran medida, pues es lógico que un usuario con mayor experiencia, pueda responder mejor ante las amenazas de seguridad y la implementación de un plan de seguridad; por lo que, si se quiere implementar Seguridad el Sistema de Información existe la influencia de la experiencia del usuario.

4.1.3.5 Selección de las dimensiones de éxito.

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

a. Actitud para Implementar Seguridad en Sistemas de Información
b. Norma Subjetiva
c. Control conductual percibido

4.1.3.6 Intención para Implementar Seguridad en los Sistemas de Información.

En conformidad con la Guía Metodológica, es necesario considerar el presente constructo, pues es el elemento fundamental del modelo, en vista que se trata de evaluar que factores condicionan la Intención para Implementar Seguridad en los Sistemas de Información desde la perspectiva del usuario.

4.1.3.7 Armado y presentación final del cuestionario.

En la Figura 24 se presenta cada una de las siguientes hipótesis y el modelo propuesto para el presente caso de estudio.

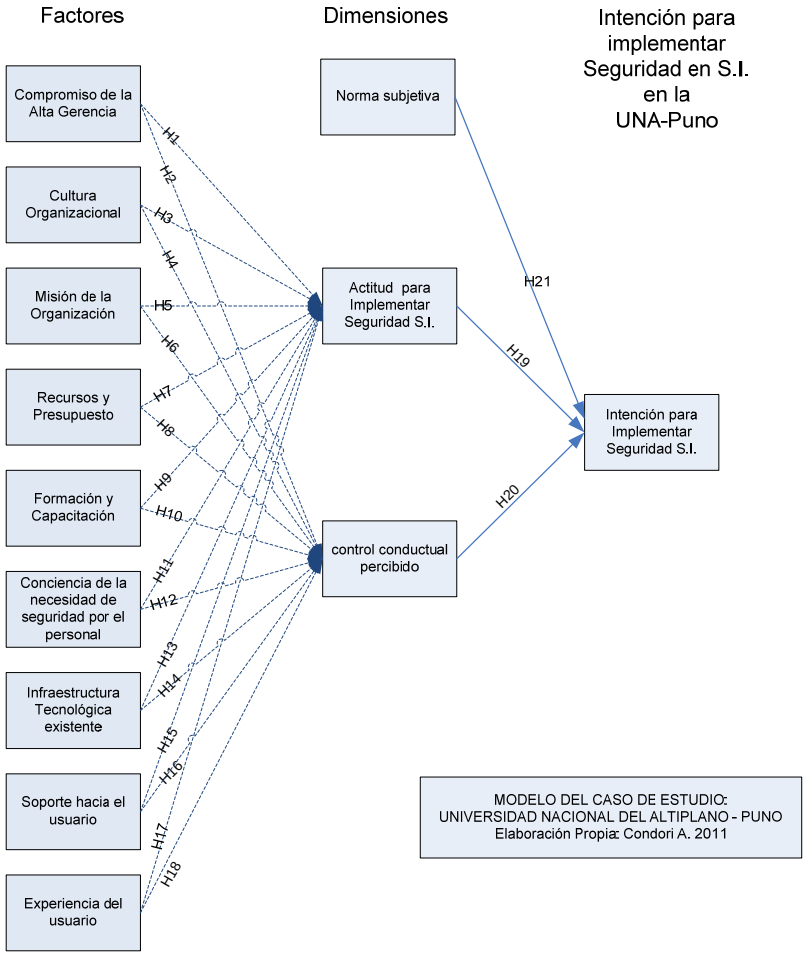

Figura 24 Modelo para el Caso de Estudio: Sistema Integral Administrativo UNA-Puno.

4.1.3.8 Ajuste de las preguntas.

En conformidad con el Sistema evaluado, se han efectuado los ajustes a las preguntas orientadas a la organización en estudio, las cuales se presentan en el Anexo 1.

4.1.3.9 Ejecución y ajuste de la encuesta.

4.1.3.9.1 Encuesta piloto

Dado el modelo propuesto, y el caso de estudio aplicado a la evaluación de los S.I. de Gestión Administrativo en la Universidad Nacional del Altiplano (UNA-Puno) en Puno, 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; así como una alta tasa de rechazo, en promedio del 40%, la encuesta se desarrolló mediante el método muestral sistemático proporcional de forma circular, el tipo de encuesta que se aplicó fue la encuesta personal. Las fechas para realizarlas fueron planteadas inicialmente en la segunda semana del mes de octubre del 2011, pero como en el trabajo de campo no se encontró la receptividad adecuada, es decir, se presentó una alta tasa de rechazo, se extendió el trabajo de campo hasta la segunda semana del mes de noviembre a fin de cumplir con el tamaño mínimo de muestra, para la encuesta piloto.

Tabla 22 Encuestas Piloto Aplicadas

DEPENDENCIA	personal según CAP	Encuestas Piloto
OFICINA GENERAL DE PLANIFICACION Y DESARROLLO	2	0
OFICINA DE PLANES Y PROYECTOS	6	2
OFICINA DE PRESUPUESTO	6	2
OFICINA DE RACIONALIZACION	6	2
OFICINA DE ESTADISTICA	5	1
OFICINA DE RECURSOS HUMANOS	2	0
UNIDAD DE ESCALAFON	7	2
UNIDAD DE REMUNERACIONES	6	1
UNIDAD DE PENSIONES Y LIQUIDACIONES	6	1
UNIDAD DE CONTROL DE ASISTENCIA	8	2
UNIDAD DE CAPACITACION	5	2
OFICINA DE CONTADURIA GENERAL	8	2
OFICINA DE GESTION FINANCIERA	2	0
TESORERIA	10	2
ABASTECIMIENTOS Y ALMACENES	12	3
ALMACENES	12	2
OFICINA DE ARQUITECTURA Y CONSTRUCCIONES	5	1
OFICINA DE BIENESTAR UNIVERSITARIO	10	2
OFICINA UNIVERSITARIA ACADEMICA	25	4
TOTAL	143	31

El cuestionario piloto está integrado por siete (07) preguntas de control, así como setenta (70) preguntas o ítems estructurados de acuerdo con los

objetivos planteados, así mismo, estas 70 preguntas han sido divididas en 13 factores:

1) Compromiso de la Gerencia
2) Cultura Organizacional
3) Misión de la Organización
4) Recursos y Presupuesto
5) Formación y Capacitación
6) Conciencia de la Necesidad de Seguridad por el personal
7) Infraestructura Tecnológica
8) Soporte hacia el usuario
9) Experiencia del usuario
10) Actitud para Implementar Seguridad en Sistemas de Información
11) Norma Subjetiva
12) Control conductual percibido
13) Intención para Implementar Seguridad en los Sistemas de Información

Así mismo, a las personas seleccionadas se les entregó el cuestionario para su llenado respectivo, sin la ayuda previa de un encuestador/entrevistador, a fin de conocer el grado de entendimiento de las preguntas. Estableciendo la premisa: Las personas contestarán todas las preguntas que comprenden, con los valores de las escalas ya establecidas, así también, si en caso no haya comprensión de las preguntas o no se tiene el grado de conocimiento de esta, se dejará sin llenar, para las correcciones correspondientes.

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 imperativo 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?"

Lo que ciertamente baja el tono imperativo de la pregunta.

4.1.3.9.1.1 Análisis Global

El análisis estadístico de los resultados de la aplicación del instrumento final se efectuó mediante el programa SPSS (paquete estadístico para las ciencias sociales, versión 19).

De un total de 31 encuestas, analizando la confiabilidad mediante el indicador de Alfa de Cronbach se ha obtenido los resultados de la tabla 23.

Tabla 23 Estadísticos de fiabilidad, encuesta piloto del caso de estudio UNA-Puno

		Casos			Estadísticos de fiabilidad	
FACTORES	Abrev.	Válidos	Excluidos(as)	Total	N de items	Alfa de Cronbach
FACTOR 1	CAG	31	0	31	7	0.775
FACTOR 2	CO	31	0	31	7	0.791
FACTOR 3	MO	31	0	31	6	0.816
FACTOR 4	RP	31	0	31	8	0.877
FACTOR 5	FC	31	0	31	5	0.894
FACTOR 6	CNS	31	0	31	8	0.884
FACTOR 7	IT	31	0	31	5	0.594
FACTOR 8	SHU	31	0	31	4	0.905
FACTOR 9	EU	31	0	31	5	0.785
FACTOR 10	AIS	31	0	31	4	0.864
FACTOR 11	CCP	31	0	31	3	0.883
FACTOR 12	NS	31	0	31	4	0.853
FACTOR 13	ISS	31	0	31	4	0.937
TOTAL		31	0	31	70	

Se observa que se supera el 0.7 requerido para su validez en los constructores.

Como segunda fase se analiza cada factor en detalle, para ver si se puede mejorar aún más la confiabilidad del cuestionario y de esta manera excluir preguntas y/o factores que no cumplan los límites de confiabilidad.

4.1.3.9.1.2 Análisis por Factores

Compromiso de la Alta Gerencia (CAG)

Analizando la confiabilidad mediante el indicador de Alfa de Cronbach, se ha obtenido:

Estadísticos total-elemento

	Correlación elemento-total corregida	Correlación múltiple al cuadrado	Alfa de Cronbach si se elimina el elemento
CAG1	.548	.463	.736
CAG2	.709	.658	.705
CAG3	.482	.463	.750
CAG4	.671	.702	.711
CAG5	.576	.578	.731
CAG6	.401	.410	.765
CAG7	.201	.330	.816

Realizando el análisis respectivo se encuentra que las preguntas 6 y 7 son bastante bajas en cuanto a confiabilidad; por lo que, se procede a retirarlas, lo que mejora el indicador Alfa de Cronbach de item total a 0.835.

Cultura Organizacional (CO)

Analizando la confiabilidad mediante el indicador de Alfa de Cronbach, se ha obtenido:

Estadísticos total-elemento

	Correlación elemento-total corregida	Correlación múltiple al cuadrado	Alfa de Cronbach si se elimina el elemento
CO1	.366	.214	.790
CO2	.476	.353	.772
CO3	.550	.464	.759
CO4	.389	.359	.786
CO5	.549	.548	.758
CO6	.602	.413	.747
CO7	.712	.598	.728

Realizando el análisis respectivo se encuentra la validez de todas las preguntas, en vista que, todas cumplen la correlación elemento total superior a 0.3, manteniendo el indicador Alfa de Cronbach de item total de 0.791.

Misión de la Organización (MO)

Analizando la confiabilidad mediante el indicador de Alfa de Cronbach, se ha obtenido:

Estadísticos total-elemento

	Correlación elemento-total corregida	Correlación múltiple al cuadrado	Alfa de Cronbach si se elimina el elemento
MO1	.682	.675	.763
MO2	.751	.749	.747
MO3	.580	.475	.788
MO4	.357	.202	.839
MO5	.630	.406	.775
MO6	.521	.300	.799

Realizando el análisis respectivo se encuentra la validez de todas las preguntas, en vista que, todas cumplen la correlación elemento total superior a 0.3, manteniendo el indicador Alfa de Cronbach de item total de 0.816.

Recursos y Presupuesto (RP)

Analizando la confiabilidad mediante el indicador de Alfa de Cronbach, se ha obtenido:

Estadísticos total-elemento

	Correlación elemento-total corregida	Correlación múltiple al cuadrado	Alfa de Cronbach si se elimina el elemento
RP1	.727	.553	.852
RP2	.584	.556	.867
RP3	.707	.651	.855
RP4	.704	.643	.854
RP5	.752	.658	.850
RP6	.480	.442	.879
RP7	.700	.668	.855
RP8	.473	.475	.877

Realizando el análisis respectivo se encuentra la validez de todas las preguntas, en vista que, todas cumplen la correlación elemento total superior a 0.3, manteniendo el indicador Alfa de Cronbach de item total de 0.877.

Formación y Capacitación (FC)

Analizando la confiabilidad mediante el indicador de Alfa de Cronbach, se ha obtenido:

Estadísticos total-elemento

	Correlación elemento-total corregida	Correlación múltiple al cuadrado	Alfa de Cronbach si se elimina el elemento
FC1	.712	.554	.879
FC2	.601	.417	.901
FC3	.779	.659	.862
FC4	.828	.739	.853
FC5	.800	.691	.858

Realizando el análisis respectivo se encuentra la validez de todas las preguntas, en vista que, todas cumplen la correlación elemento total superior a 0.3, manteniendo el indicador Alfa de Cronbach de ítem total de 0.894.

Conciencia de la Necesidad de Seguridad por el Personal (CNS)

Analizando la confiabilidad mediante el indicador de Alfa de Cronbach, se ha obtenido:

Estadísticos total-elemento

	Correlación elemento-total corregida	Correlación múltiple al cuadrado	Alfa de Cronbach si se elimina el elemento
CNS1	.686	.627	.866
CNS2	.772	.810	.857
CNS3	.788	.741	.854
CNS4	.755	.801	.860
CNS5	.608	.558	.873
CNS6	.686	.651	.865
CNS7	.453	.362	.891
CNS8	.525	.349	.882

Realizando el análisis respectivo se encuentra la validez de todas las preguntas, en vista que, todas cumplen la correlación elemento total superior a 0.3, manteniendo el indicador Alfa de Cronbach de ítem total de 0.884.

Infraestructura Tecnológica Existente (IT)

Analizando la confiabilidad mediante el indicador de Alfa de Cronbach, se ha obtenido:

Estadísticos total-elemento

	Correlación elemento-total corregida	Correlación múltiple al cuadrado	Alfa de Cronbach si se elimina el elemento
IT1	.213	.428	.616
IT2	.233	.411	.596
IT3	.415	.359	.506
IT4	.530	.573	.431
IT5	.384	.467	.521

Realizando el análisis respectivo, se encuentra que las preguntas 1 y 2 son bastante bajas en cuanto a confiabilidad; por lo que, se procede a retirarlas, lo que mejora el indicador Alfa de Cronbach de ítem total a 0.789.

Soporte hacia el Usuario (SHU)

Analizando la confiabilidad mediante el indicador de Alfa de Cronbach, se ha obtenido:

Estadísticos total-elemento

	Correlación elemento-total corregida	Correlación múltiple al cuadrado	Alfa de Cronbach si se elimina el elemento
SHU1	.793	.688	.875
SHU2	.898	.812	.835
SHU3	.736	.565	.895
SHU4	.727	.583	.898

Realizando el análisis respectivo se encuentra la validez de todas las preguntas, en vista que, todas cumplen la correlación elemento total superior a 0.3, manteniendo el indicador Alfa de Cronbach de ítem total de 0.905.

Experiencia del Usuario (EU)

Analizando la confiabilidad mediante el indicador de Alfa de Cronbach, se ha obtenido:

Estadísticos total-elemento

	Correlación elemento-total corregida	Correlación múltiple al cuadrado	Alfa de Cronbach si se elimina el elemento
EU1	.683	.580	.702
EU2	.355	.147	.832
EU3	.424	.264	.786
EU4	.751	.653	.694
EU5	.713	.603	.699

Realizando el análisis respectivo se encuentra la validez de todas las preguntas, en vista que, todas cumplen la correlación elemento total superior a 0.3, manteniendo el indicador Alfa de Cronbach de ítem total de 0.785. Existiendo la posibilidad de eliminar la pregunta 2.

Actitud para Implementar Seguridad en el Sistema de Información (AIS)

Analizando la confiabilidad mediante el indicador de Alfa de Cronbach, se ha obtenido:

Estadísticos total-elemento

	Correlación elemento-total corregida	Correlación múltiple al cuadrado	Alfa de Cronbach si se elimina el elemento
AIS1	.722	.595	.825
AIS2	.596	.374	.887
AIS3	.801	.670	.800
AIS4	.787	.646	.793

Realizando el análisis respectivo se encuentra la validez de todas las preguntas, en vista que, todas cumplen la correlación elemento total superior a 0.3, manteniendo el indicador Alfa de Cronbach de ítem total de 0.864.

Control Conductual Percibido - Autosuficiencia (CCP)

Analizando la confiabilidad mediante el indicador de Alfa de Cronbach se ha obtenido:

Estadísticos total-elemento

	Correlación elemento-total corregida	Correlación múltiple al cuadrado	Alfa de Cronbach si se elimina el elemento
CCP1	.701	.594	.895
CCP2	.889	.793	.728
CCP3	.736	.663	.868

Realizando el análisis respectivo se encuentra la validez de todas las preguntas, en vista que, todas cumplen la correlación elemento total superior a 0.3, manteniendo el indicador Alfa de Cronbach de ítem total de 0.883.

Norma Subjetiva – Creencias Normativas (NS)

Analizando la confiabilidad mediante el indicador de Alfa de Cronbach, se ha obtenido:

Estadísticos total-elemento

	Correlación elemento-total corregida	Correlación múltiple al cuadrado	Alfa de Cronbach si se elimina el elemento
NS1	.480	.253	.896
NS2	.709	.521	.816
NS3	.824	.805	.753
NS4	.816	.820	.757

Realizando el análisis respectivo se encuentra la validez de todas las preguntas, en vista que, todas cumplen la correlación elemento total superior a 0.3, manteniendo el indicador Alfa de Cronbach de ítem total de 0.853.

Intención para Implementar Seguridad en los Sistemas de Información (IIS)

Analizando la confiabilidad mediante el indicador de Alfa de Cronbach, se ha obtenido:

Estadísticos total-elemento

	Correlación elemento-total corregida	Correlación múltiple al cuadrado	Alfa de Cronbach si se elimina el elemento
IIS1	.785	.630	.943
IIS2	.869	.758	.913
IIS3	.899	.843	.902
IIS4	.864	.805	.914

Realizando el análisis respectivo se encuentra la validez de todas las preguntas, en vista que, todas cumplen la correlación elemento total superior a 0.3, manteniendo el indicador Alfa de Cronbach de ítem total de 0.937.

4.1.3.9.1.2 Resultados de la Encuesta Piloto

El trabajo de campo realizado, mediante los permisos y visitas personalizadas a cada dependencia de la UNA-Puno, si bien cumple con las características técnicas de un buen trabajo de campo, ha tenido inconvenientes tales como la alta tasa de rechazo (40%) de las dependencias, que en su momento no han colaborado con el estudio, la demora del tiempo de recojo de información a cada uno de lo encuestados, resultando de 30 minutos hasta 60 minutos, ya que realizaban trabajos simultáneos y no tenían el tiempo necesario para hacerlo.

Se recomienda estructurar el mecanismo del recojo de información, y evaluar el mecanismo de acuerdo a la realidad de cada entidad, pues ciertamente de la experiencia, ha sido necesario ser reiterativo en recordarles el llenado de la encuesta.

Para la encuesta final, es necesaria la adecuación del cuestionario, ya que algunas preguntas no se comprenden o existe desconocimiento de las respuestas, por que no son parte de las funciones de los usuarios de los SI evaluados. De las tabulaciones se distingue que las preguntas que tienen al

menos tres personas que no hayan contestado, son las que tienen mayor probabilidad de que no hayan sido entendidas, o en su defecto no son parte de las funciones o del conocimiento de los encuestados. Por lo tanto, se requiere reformular la pregunta a fin de cumplir con los objetivos del estudio o, en el peor de los casos, eliminarla, ya que para los posteriores análisis son necesarias que todas sean contestadas correctamente.

Los resultados de confiabilidad mediante el indicador de Alfa de Cronbach nos permite decir que la consistencia interna del cuestionario es adecuada (instrumento fiable que hace mediciones estables y consistentes, tabla 23). Pero hay que tener cuidado con el factor 7 (infraestructura tecnológica), ya que el valor de Alfa de Cronbach se ha mejorado eliminando preguntas para alcanzar el mínimo.

Efectuado el análisis mediante el Alfa de Cronbach y realizado la validación de preguntas se ha obtenido los factores y las preguntas que cumplen los requisitos para iniciar el estudio definitivo, con un total de 66 preguntas.

Tabla 24 Preguntas consideradas para el caso UNAP-Puno luego del análisis Alfa de Cronbach

		Casos			Estadísticos de fiabilidad	
FACTORES	Abrev.	Válidos	Excluidos(as)	Total	N de items	Alfa de Cronbach
FACTOR 1	CAG	31	0	31	5	0.835
FACTOR 2	CO	31	0	31	7	0.791
FACTOR 3	MO	31	0	31	6	0.816
FACTOR 4	RP	31	0	31	8	0.877
FACTOR 5	FC	31	0	31	5	0.894
FACTOR 6	CNS	31	0	31	8	0.884
FACTOR 7	IT	31	0	31	3	0.789
FACTOR 8	SHU	31	0	31	4	0.905
FACTOR 9	EU	31	0	31	5	0.785
FACTOR 10	AIS	31	0	31	4	0.864
FACTOR 11	CCP	31	0	31	3	0.883
FACTOR 12	NS	31	0	31	4	0.853
FACTOR 13	ISS	31	0	31	4	0.937
TOTAL		31	0	31	66	0.946

4.1.3.9.2 Encuesta Definitiva

El cuestionario final, está integrado por siete (07) preguntas de control, así como 66 preguntas o ítems estructurados de acuerdo con los objetivos planteados, así mismo, estas 66 preguntas han sido divididas en 13 factores (Tabla 25).

Tabla 25 Preguntas consideradas para el caso estudio UNA-Puno

FACTORES	DESCRIPCION DE FACTORES	ÍTEMS O PREGUNTAS
FACTOR 1	Compromiso de la Gerencia	5
FACTOR 2	Cultura Organizacional	7
FACTOR 3	Misión de la Organización	6
FACTOR 4	Recursos y Presupuesto	8
FACTOR 5	Formación y Capacitación	5
FACTOR 6	Conciencia de la Necesidad de Seguridad por el personal	8
FACTOR 7	Infraestructura Tecnológica	3
FACTOR 8	Soporte hacia el usuario	4
FACTOR 9	Experiencia del usuario	5
FACTOR 10	Actitud para Implementar Seguridad en Sistemas de Información	4
FACTOR 11	Control conductual percibido	3
FACTOR 12	Norma Subjetiva	4
FACTOR 13	Intención para Implementar Seguridad en los Sistemas de Información	4

De acuerdo al estudio se ha determinado un tamaño de muestra de 84 casos, lográndose un total de 128 casos válidos; desarrollando una encuesta no probabilística de corte transversal.

4.1.3.9.3 Evaluación y consistencia de los resultados

Una vez obtenido los cuestionarios debidamente llenados, se procedió a su revisión de cada uno de ellos, para poder observar los errores en el llenado, preguntas no contestadas, problemas de consistencia interna.

Del tamaño de total encuestado de 139, se desecharon para el estudio a 11, quedando como encuestas válidas 128, las encuestas desechadas han considerado un patrón de contestación mayor de un ítem en blanco, por cada constructor.

4.1.3.9.4 Procesamiento y análisis

En base a los cuestionarios válidos para el caso estudio UNA-Puno, se ha procedido a su procesamiento, con el programa SPSS versión 19.0, y son:

4.1.3.9.4.1 Análisis descriptivo

Se efectuó el análisis descriptivo de las 7 variables de control incluidas en el estudio, análisis que se presenta en resumen de los resultados de las tabulaciones de las preguntas de control:

- 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 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 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; 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.

4.1.3.9.4.2 Análisis de correlación ítem-total

Los resultados del análisis de correlación, casi todos los ítems (preguntas) han cumplido con el mínimo recomendado. A excepción de: Ítem 26 (RP8), ítem 39 (CNS8).

4.1.3.9.4.3 Consistencia interna (fiabilidad de ítems)

El valor del Alfa de Cronbach (AC) total de los 64 ítems, es igual a 0,947, demostrando tener muy buena consistencia interna en forma conjunta, pero como dentro de los objetivos del estudio está el desarrollar modelos de ecuaciones estructuradas, se hace necesario saber la consistencia interna de cada uno de los factores que complementan el modelo propuesto (Tabla 26).

Tabla 26 Estadísticos de fiabilidad por factor para el caso estudio UNA-Puno

		Casos			Estadísticos de fiabilidad	
FACTORES	Abrev.	Válidos	Excluidos(as)	Total	N de items	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	0.947

De los 13 factores propuestos para el modelo, todos cumplen con los requisitos de consistencia interna con valores Alfa Cronbach muy aceptables.

4.1.3.9.4.4 Análisis factorial de cada constructor

Del cuadro resumen, se observa que el factor 7 tiene un determinante mediana, con una KMO=0.692 cercano al mínimo y con una varianza explicada de 70.239%; el factor 12 presenta un KMO=0.697 cercano al mínimo con una varianza explicada de 63.727%; los factores 2, 3 y 4, según el análisis factorial, se deben separar en dos factores (grupos) que se encuentran mayormente correlacionados (Tabla 27).

Tabla 27 Resultados del análisis factorial para el caso estudio UNA-Puno

				Aplicación		Resultados	
FACTORES	DESCRIPCION DE FACTORES	ÍTEMS	Alfa de Cronbach	determ. (cerca a 0)	KMO>0,7	Fact.	Varianza Explicada %
FACTOR 1	Compromiso de la Gerencia	5	0.874	0.074	0.816	1	66.668
FACTOR 2	Cultura Organizacional	7	0.770	0.154	0.737	2	42.412; 17,296
FACTOR 3	Misión de la Organización	6	0.778	0.131	0.725	2	48.829; 17.398
FACTOR 4	Recursos y Presupuesto	7	0.828	0.036	0.789	2	46.432; 18.210
FACTOR 5	Formación y Capacitación	5	0.874	0.074	0.846	1	67.078
FACTOR 6	Conciencia de la Necesidad de Seguridad por el personal	7	0.874	0.020	0.828	1	58.149
FACTOR 7	Infraestructura Tecnológica	3	0.786	0.410	0.692	1	70.239
FACTOR 8	Soporte hacia el usuario	4	0.864	0.105	0.730	1	71.223
FACTOR 9	Experiencia del usuario	5	0.742	0.229	0.736	1	52.311
FACTOR 10	Actitud para Implementar Seguridad en Sistemas de Información	4	0.904	0.057	0.817	1	78.023
FACTOR 11	Control conductual percibido	3	0.931	0.085	0.761	1	87.863
FACTOR 12	Norma Subjetiva	4	0.805	0.183	0.697	1	63.727
FACTOR 13	Intención para Implementar Seguridad en los Sistemas de Información	4	0.959	0.009	0.871	1	89.062
	TOTAL	64	0.947				

Siendo pertinente realizar un análisis factorial, para los factores 2,3 y 4 que se pueden reducir en “grupos” más homogéneos, y que los ítems de dichos “grupos” presenten mayor correlación, y exista independencia entre dichos grupos.

4.1.3.9.4.5 Ajustes realizados a los constructores

A partir de los resultados iniciales, 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 (tabla 28).

Tabla 28 Constructores ajustados por cada factor para el caso estudio UNA-Puno

				Aplicación		Resultados	
FACTORES	DESCRIPCION DE FACTORES	ÍTEMS	Alfa de Cronbach	determ. (cerca a 0)	KMO>0,7	Fact.	Varianza Explicada %
FACTOR 1	Compromiso de la Gerencia	5	0.874	0.074	0.816	1	66.668
FACTOR 2	Cultura Organizacional	5	0.745	0.310	0.749	1	50.156
FACTOR 3	Misión de la Organización	5	0.779	0.165	0.704	1	54.536
FACTOR 4	Recursos y Presupuesto	5	0.842	0.176	0.736	1	68.195
FACTOR 5	Formación y Capacitación	5	0.874	0.074	0.846	1	67.078
FACTOR 6	Conciencia de la Necesidad de Seguridad por el personal	6	0.875	0.032	0.828	1	62.404
FACTOR 7	Infraestructura Tecnológica	3	0.786	0.410	0.692	1	70.239
FACTOR 8	Soporte hacia el usuario	4	0.864	0.105	0.730	1	71.223
FACTOR 9	Experiencia del usuario	4	0.789	0.262	0.717	1	61.653
FACTOR 10	Actitud para Implementar Seguridad en Sistemas de Información	4	0.904	0.057	0.817	1	78.023
FACTOR 11	Control conductual percibido	3	0.931	0.085	0.761	1	87.863
FACTOR 12	Norma Subjetiva	4	0.805	0.183	0.697	1	63.727
FACTOR 13	Intención para Implementar Seguridad en los Sistemas de Información	4	0.959	0.009	0.871	1	89.062
	TOTAL	57	0.943				

Del análisis realizado, la consideración y exclusión de las preguntas por cada constructor, ha permitido mejorar de forma sustantiva los indicadores estadísticos, así como los resultados descriptivos del estudio; todos los valores de Alfa de Cronbach han sido mayores a 0,70, que es lo mínimo permitido.

Por otro lado no se han realizado ajustes a los constructores que tienen tres o cuatro ítems por cada uno de ellos, en vista qué es lo mínimo permitido para justificar la interpretación de los constructores.

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 sólo grupo con una representación de la varianza mayor a 50%.

Pero es necesario mencionar que el factor 7 y el factor 12, son los presentan un KMO cercano al mínimo de 0,7 por lo que son considerados, no pudiendo optimizarse más.

4.1.3.9.5 Análisis y evaluación del modelo estructural

4.1.3.9.5.1 Preparación de los datos para el análisis

El número de variables total en el modelo final es 57 (Figura 25):

· Latentes endógenas 4 (reflectivos);

· Latentes exógenos 9 (formativos);

· Indicadores o variables observadas 57;

· Términos de error 85;

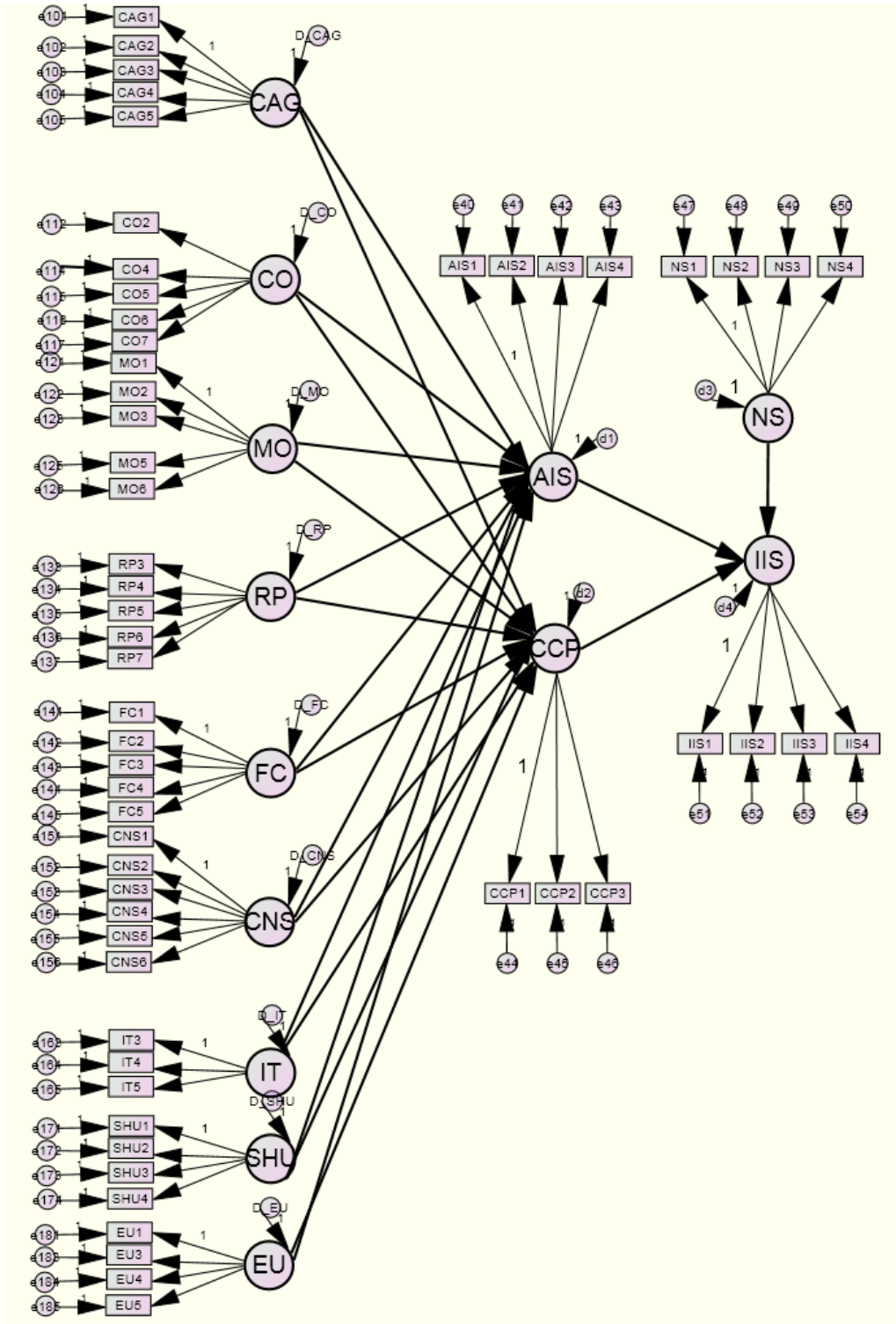

Figura 25 Presentación de la propuesta del modelo inicial, caso de estudio UNA-Puno

El tamaño de muestra se encuentra dentro de lo permitido (128), así mismo, se ha utilizado el método del bootstrap, generándose 500 muestras representativas. Dentro de los estudios de análisis descriptivo no se ha podido observar resultados que mencionen que incumplan de forma asertiva la normalidad por cada variable; las variables observadas y latentes son continuas y se ha considerado encuestas donde todas las preguntas han sido contestadas; así mismo, como se ha utilizado los programas AMOS versión 19.0 y SmartPLS 2.0, se ha empleado las matrices de varianza - covarianza, y también las matrices de correlación, es decir, matrices de varianza – covarianzas estandarizadas.

4.1.3.9.5.2 La estimación del modelo

Se ha utilizado el método de estimación de máxima verosimilitud (ML), porque es, hasta la fecha, el más utilizado para un modelo de ecuación estructural general. Así mismo, el estudio es apropiado para su correcta aplicación ya que su muestra es mayor de 100, que es lo recomendado y que mediante está técnica se adecua a tamaños de muestras relativamente grandes.

Como en el estudio del modelo final se consideró 57 ítems, se ha generado 500 muestras por el método del bootstrap, la cual se encuentra dentro de los recomendados por los investigadores; si bien el estudio cuenta con gran cantidad de variables (ítems) para el estudio, se cumple el objetivo planteado en el caso de estudio

4.1.3.9.5.3 La evaluación del modelo

Inicialmente, para evaluar los resultados se requirió una inspección inicial de las estimaciones infractoras. Una vez que el modelo estuvo establecido como para ofrecer estimaciones aceptables, se evaluó la calidad de ajuste del modelo.

Se examinó los resultados buscando estimaciones infractoras, es decir, coeficientes estimados tanto en los modelos de medida como en los estructurales que excedan los límites aceptables, no se encontró valores que no se ajustaran a lo indicado (Figura 26).

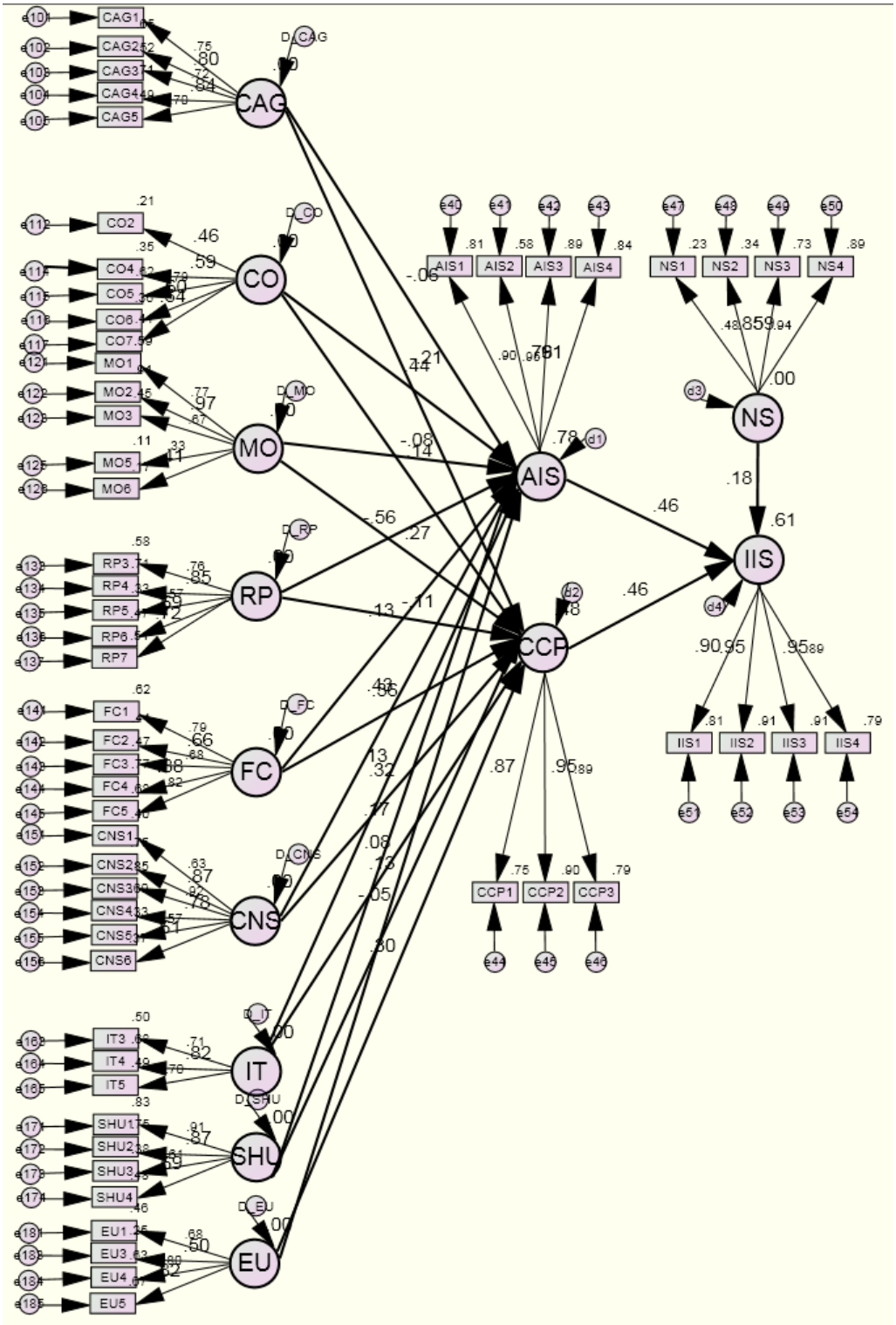

Figura 26 Presentación del modelo evaluado, caso de estudio UNA-Puno

Una vez que se ha establecido que no existen estimaciones infractoras, se procedió a evaluar el ajuste global del modelo con una o más medidas de

calidad de ajuste. Las medidas de calidad de ajuste para el caso estudio se pueden observar en la Tabla 29.

Luego de una revisión de los anteriores tipos de medida de ajuste en conjunto, estos revelan una pauta consistente de evidencia marginal del modelo tal y como se ha propuesto. En conclusión, todas las medidas, en general, indican que el modelo es marginalmente aceptable.

Tabla 29 Índices de ajuste absoluto y de parsimonia, caso estudio UNA-Puno

Media	Indicador	Macro	Valor	Calificación
A. Índices de ajuste absoluto	Índice de razón de verosimilitud	Chi 2		no adecuado
	Índice de bondad de ajuste	GFI	0.524	media
	Raíz cuadrada de la media de res.	RMR	0.215	media alta
B. Índices de ajuste de parsimonia	Chi 2 normado		2.211	adecuado
	Criterio de información de Akaike	AIC	4136.152	media

4.1.3.9.5.4 Ajuste del modelo de medida

4.1.3.9.5.4.1 Confiabilidad del constructor

La Tabla 30, 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.

Tabla 30 Confiabilidad y validez convergente de los coeficientes Caso UNA-Puno

FACTORES	DESCRIPCION DE FACTORES	ÍTEMS	Confiabilidad Interna >0.707	Cronbachs Alpha	AVE >0.5	R2 Cercano a 1
FACTOR 1	Compromiso de la Gerencia	5	0.874	0.874	0.586	no aplica
FACTOR 2	Cultura Organizacional	5	0.828	0.746	0.493	no aplica
FACTOR 3	Misión de la Organización	5	0.852	0.783	0.542	no aplica
FACTOR 4	Recursos y Presupuesto	5	0.883	0.836	0.604	no aplica
FACTOR 5	Formación y Capacitación	5	0.908	0.876	0.666	no aplica
FACTOR 6	Conciencia de la Necesidad de Seguridad por el personal	6	0.907	0.877	0.622	no aplica
FACTOR 7	Infraestructura Tecnológica	3	0.864	0.788	0.681	no aplica
FACTOR 8	Soporte hacia el usuario	4	0.902	0.865	0.699	no aplica
FACTOR 9	Experiencia del usuario	4	0.863	0.789	0.613	no aplica
FACTOR 10	Actitud para Implementar Seguridad en Sistemas de Información	4	0.934	0.905	0.780	0.779
FACTOR 11	Control conductual percibido	3	0.956	0.931	0.879	0.481
FACTOR 12	Norma Subjetiva	4	0.873	0.804	0.636	no aplica
FACTOR 13	Intención para Implementar Seguridad en los Sistemas de Información	4	0.970	0.959	0.891	0.608
	TOTAL	57	0.943			

4.1.3.9.5.4.2 Validez convergente (varianza extraída media -AVE)

Para los indicadores reflectivos (Tabla 30), 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.

4.1.3.9.5.4.3 Validez discriminante

Se examina esta validez, mostrada en la tabla 31 (en diagonal), para las variables reflectivas, indicando que todos los constructores satisfacen esta condición; en otras palabras, por lo que el cuestionario discrimina adecuadamente entre la causa propuesta y el efecto en el constructor. Los datos en diagonal es la raíz cuadrada de la varianza extraída media (AVE) entre el constructo y sus medidas. Para la validez discriminante, estos valores deben de ser mayores a los datos en el mismo renglón y columna (interconstructo).

Tabla 31 Matriz de correlaciones de constructores y valores raíz cuadrada de los AVE Caso UNA-Puno

	AIS	CAG	CCP	CNS	CO	EU	FC	IIS	IT	MO	NS	RP	SHU
AIS	**0.883**												
CAG	0.125	1000											
CCP	0.418	0.201	**0.937**										
CNS	0.535	0.107	0.441	1000									
CO	0.412	0.270	0.396	0.521	1000								
EU	0.261	0.165	0.471	0.283	0.185	1000							
FC	0.049	0.527	0.236	-0.187	0.148	0.206	1000						
IIS	0.626	0.294	0.639	0.482	0.460	0.421	0.226	**0.944**					
IT	0.212	0.180	0.209	0.125	0.348	0.279	0.204	0.221	1000				
MO	0.325	0.341	0.391	0.575	0.557	0.243	0.014	0.433	0.288	1000			
NS	0.280	0.466	0.347	0.326	0.333	0.323	0.287	0.440	0.256	0.387	1000		
RP	0.045	0.294	0.298	0.294	0.690	0.267	0.315	0.268	0.518	0.418	0.206	1000	
SHU	0.244	0.493	0.252	0.272	0.385	0.286	0.243	0.252	0.577	0.277	0.383	0.489	1000

4.1.3.9.5.4.4 Carga y significancia

La Tabla 30, presenta los resultados del R^2, donde el factor 10 y 13 supera a 0,518, lo mínimo permitido, estando el factor 11 cercano al mínimo con 0.481; la Tabla 32 muestra el resultado de cada una de las hipótesis planteadas, para lo cual, en la Figura 26 se detallan en forma gráfica, mostrando el modelo de investigación evaluado empíricamente; indicando, además, que de todo los valores obtenidos (21), diez de ellos se encontraron significativos estadísticamente (con valores CR adecuados). Y once no tienen significancia, aclarando que ciertamente la mayoría de los factores influye en una sola dimensión, los cuales son las relaciones:

- El factor compromiso de la alta gerencia relacionado con la Actitud para implementar Seguridad en Sistemas de Información.
- El Soporte hacia el usuario relacionado con la Actitud para implementar Seguridad en Sistemas de Información.
- El Soporte hacia el usuario relacionado con el control conductual percibido.
- La Cultura Organizacional relacionada con el control conductual percibido.
- La Misión de la Organización relacionado con la Actitud para implementar Seguridad en Sistemas de Información.
- Los Recursos y Presupuesto están relacionados con el control conductual percibido.
- La Formación y Capacitación influye en la Actitud para implementar Seguridad en Sistemas de Información.
- La Infraestructura Tecnológica existente relacionada con la Actitud para implementar Seguridad en Sistemas de Información.
- La Infraestructura Tecnológica existente relacionada con el control conductual percibido.
- La Experiencia del usuario relacionada con la Actitud para implementar Seguridad en Sistemas de Información.

- La Norma subjetiva relacionada con Intención para Implementar Seguridad en Sistemas de Información.

En consecuencia, si estos parámetros “no significativos” se fijan en cero, esto no repercutiría en un ajuste significativamente peor del modelo.

Tabla 32 Resumen de los parámetros estimados y su razón crítica Caso UNA-Puno

Pesos de la regresión			Estimación del coeficiente PATH no estandarizado	Errores típicos (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	<---	IT	0.079	0.083	0.958	0.076	No aceptada
CCP	<---	EU	0.405	0.113	3.583	0.304	Aceptada
AIS	<---	IT	0.157	0.076	2.057	0.129	No aceptada
AIS	<---	EU	0.201	0.096	2.095	0.129	No aceptada
IIS	<---	AIS	0.379	0.058	6.545	0.463	Aceptada
IIS	<---	CCP	0.444	0.069	6.397	0.463	Aceptada
IIS	<---	NS	0.284	0.109	2.595	0.181	No aceptada

4.1.3.9.6 La mejora del modelo

Se procedió con el ajuste indicado de las relaciones que no presentan significancia estadística, esas relaciones son:

- El factor compromiso de la alta gerencia relacionado con la Actitud para implementar Seguridad en Sistemas de Información.

- El Soporte hacia el usuario relacionado con la Actitud para implementar Seguridad en Sistemas de Información.
- El Soporte hacia el usuario relacionado con el control conductual percibido.
- La Cultura Organizacional relacionada con el control conductual percibido.
- La Misión de la Organización relacionado con la Actitud para implementar Seguridad en Sistemas de Información.
- Los Recursos y Presupuesto están relacionados con el control conductual percibido.
- La Formación y Capacitación influye en la Actitud para implementar Seguridad en Sistemas de Información.
- La Infraestructura Tecnológica existente relacionada con la Actitud para implementar Seguridad en Sistemas de Información.
- La Infraestructura Tecnológica existente relacionada con el control conductual percibido.
- La Experiencia del usuario relacionada con la Actitud para implementar Seguridad en Sistemas de Información.
- La Norma subjetiva relacionada con Intención para Implementar Seguridad en Sistemas de Información.

4.1.3.9.7 Presentación final del modelo con resultado de sus hipótesis

En base a los resultados obtenidos y la mejora del modelo, omitiendo las relaciones que no han sido significativas en el análisis, se presenta el modelo final aceptado (Figura 27).

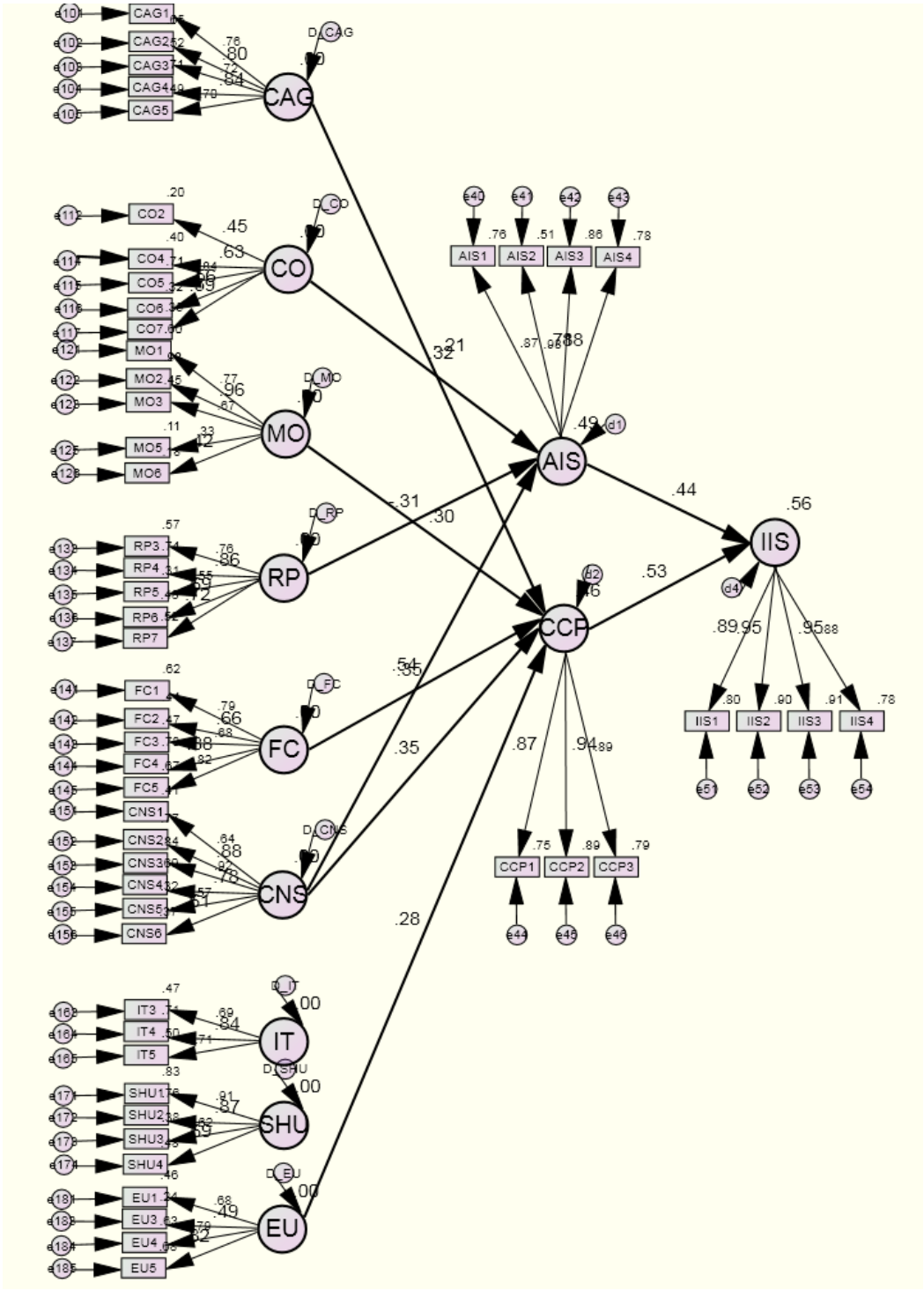

Figura 27 Presentación final con resultado de sus hipótesis, caso de estudio UNA-Puno

4.2 Discusión de Resultados

4.2.1 Análisis de los Factores Críticos de Éxito con las dimensiones

La Cultura Organizacional (0.439), los Recursos y Presupuesto (-0.558), 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), 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.

4.2.2 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 R^2 y su coeficiente path son bajos, a pesar de ser un elemento ampliamente probado de la teoría del comportamiento planificado propuesto por Ajzen.

4.2.3 Análisis Global

El modelo de investigación propuesto se ha evaluado en 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 influenciado en el nivel macro por factores específicos.

Dentro de todo el modelo, que 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 un usuario más experimentado puede 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, 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.

4.3 Contrastación de Hipótesis

Para la prueba de la hipótesis con respecto a los factores propuestos y de acuerdo al tipo de investigación y el diseño seleccionado, se ha utilizado como método de prueba la denominada prueba R^2, proceso que se ha realizado utilizando AMOS 19, considerando que se trabajó aplicando un diseño factorial:

H1: El compromiso de la alta gerencia influye en la Actitud para implementar Seguridad en Sistemas de Información, se rechaza, en vista que su coeficiente path alcanzado es de -0.063, siendo menor a 0.2 con p=0.279, no siendo significativo.

H2 El compromiso de la alta gerencia influye en el control conductual percibido, se acepta, en vista que su coeficiente path alcanzado es de -0.212, siendo superior a 0.2 con p=0.006, siendo significativo.

H3 La Cultura Organizacional influye en la Actitud para implementar Seguridad en Sistemas de Información, se acepta, en vista que su coeficiente

path alcanzado es de 0.439, siendo superior a 0.2 con p<0.001, siendo significativo.

H4 La Cultura Organizacional influye en el control conductual percibido, se rechaza, en vista que su coeficiente path alcanzado es de 0.135, siendo menor a 0.2 con p=0.102, no siendo significativo.

H5 La Misión de la Organización influye en la Actitud para implementar Seguridad en Sistemas de Información, se rechaza, en vista que su coeficiente path alcanzado es de -0.081, siendo menor a 0.2 con p= 0.154, no siendo significativo.

H6 La Misión de la Organización influye en el control conductual percibido, se acepta, en vista que su coeficiente path alcanzado es de 0.268, siendo superior a 0.2 con p<0.001, siendo significativo.

H7 Los Recursos y Presupuesto están relacionados con la Actitud para implementar Seguridad en Sistemas de Información, se acepta, en vista que su coeficiente path alcanzado es de -0.558, siendo superior a 0.2 con p<0.001, siendo significativo.

H8 Los Recursos y Presupuesto están relacionados con el control conductual percibido, se rechaza, en vista que su coeficiente path alcanzado es de -0.111, siendo menor a 0.2 con p= 0.145, no siendo significativo.

H9 La Formación y Capacitación influye en la Actitud para implementar Seguridad en Sistemas de Información, se rechaza, en vista que su coeficiente path alcanzado es de 0.131, siendo menor a 0.2 con p= 0.145, no siendo significativo.

H10 La Formación y Capacitación influye en el control conductual percibido, se acepta, en vista que su coeficiente path alcanzado es de 0.357, siendo superior a 0.2 con p<0.001, siendo significativo.

H11 La Conciencia de la necesidad de seguridad por el personal influye en la Actitud para implementar Seguridad en Sistemas de Información, se acepta, en vista que su coeficiente path alcanzado es de 0.431, siendo superior a 0.2 con p<0.001, siendo significativo.

H12 La Conciencia de la necesidad de seguridad por el personal influye en el control conductual percibido, se acepta, en vista que su coeficiente path alcanzado es de 0.325, siendo superior a 0.2 con p<0.001, siendo significativo.

H13 La Infraestructura Tecnológica existente influye en la Actitud para implementar Seguridad en Sistemas de Información, se rechaza, en vista que su coeficiente path alcanzado es de 0.129, siendo menor a 0.2 con p= 0.04, no siendo significativo.

H14 La Infraestructura Tecnológica existente influye en el control conductual percibido, se rechaza, en vista que su coeficiente path alcanzado es de 0.076, siendo menor a 0.2 con p= 0.338, no siendo significativo.

H15 El Soporte hacia el usuario influye en la Actitud para implementar Seguridad en Sistemas de Información, se rechaza, en vista que su coeficiente path alcanzado es de 0.166, siendo menor a 0.2 con p= 0.004, no siendo significativo.

H16 El Soporte hacia el usuario influye en el control conductual percibido, se rechaza, en vista que su coeficiente path alcanzado es de -0.048, siendo menor a 0.2 con p= 0.517, no siendo significativo.

H17 La Experiencia del usuario influye en la Actitud para implementar Seguridad en Sistemas de Información, se rechaza, en vista que su coeficiente path alcanzado es de 0.129, siendo menor a 0.2 con p= 0.036, no siendo significativo.

H18 La Experiencia del usuario influye en el control conductual percibido, se acepta, en vista que su coeficiente path alcanzado es de 0.304, siendo superior a 0.2 con p<0.001, siendo significativo.

H19 La Actitud para implementar Seguridad en Sistemas de Información influye en Intención para Implementar Seguridad en Sistemas de Información, se acepta, en vista que su coeficiente path alcanzado es de 0.463, siendo superior a 0.2 con p<0.001, siendo significativo.

H20 El control conductual percibido influye en Intención para Implementar Seguridad en Sistemas de Información, se acepta, en vista que su coeficiente

path alcanzado es de 0.463, siendo superior a 0.2 con p<0.001, siendo significativo.

H21 La Norma subjetiva influye en Intención para Implementar Seguridad en Sistemas de Información, se rechaza, en vista que su coeficiente path alcanzado es de 0.181, siendo menor a 0.2 con p= 0.009, no siendo significativo.

Tabla 33 Resultado del Análisis para Contrastación de Hipótesis

Pesos de la regresión			Estimación del coeficiente PATH no estandarizado	Errores típicos (S.E.)	Razón crítica (C.R.) +/- 1,96	Estimación del coeficiente PATH estandarizado R2 > 0,2	p	Clasificación
AIS	<---	CAG	-0.081	0.074	-1.083	-0.063	0.279	No aceptada
CCP	<---	CAG	-0.230	0.085	-2.726	-0.212	0.006	Aceptada
AIS	<---	SHU	0.160	0.056	2.852	0.166	0.004	No aceptada
CCP	<---	SHU	-0.040	0.061	-0.648	-0.048	0.517	No aceptada
AIS	<---	CO	0.837	0.199	4.200	0.439	>0.001	Aceptada
CCP	<---	CO	0.220	0.135	1.635	0.135	0.102	No aceptada
AIS	<---	MO	-0.095	0.067	-1.426	-0.081	0.154	No aceptada
CCP	<---	MO	0.270	0.077	3.511	0.268	>0.001	Aceptada
AIS	<---	RP	-0.744	0.101	-7.340	-0.558	>0.001	Aceptada
CCP	<---	RP	-0.126	0.087	-1.458	-0.111	0.145	No aceptada
AIS	<---	FC	0.175	0.078	2.239	0.131	0.025	No aceptada
CCP	<---	FC	0.405	0.091	4.432	0.357	<0.001	Aceptada
AIS	<---	CNS	0.672	0.119	5.666	0.431	<0.001	Aceptada
CCP	<---	CNS	0.432	0.111	3.899	0.325	<0.001	Aceptada
CCP	<---	IT	0.079	0.083	0.958	0.076	0.338	No aceptada
CCP	<---	EU	0.405	0.113	3.583	0.304	<0.001	Aceptada
AIS	<---	IT	0.157	0.076	2.057	0.129	0.04	No aceptada
AIS	<---	EU	0.201	0.096	2.095	0.129	0.036	No aceptada
IIS	<---	AIS	0.379	0.058	6.545	0.463	<0.001	Aceptada
IIS	<---	CCP	0.444	0.069	6.397	0.463	<0.001	Aceptada
IIS	<---	NS	0.284	0.109	2.595	0.181	0.009	No aceptada

CAPITULO V

Conclusiones y Recomendaciones

5.1 Conclusiones

- Se desarrolló el Modelo de Evaluación de Factores Críticos de Éxito en la Implementación de Seguridad de Sistemas de Información para determinar su influencia en la intención del usuario, con nueve factores y tres dimensiones, adecuadamente sustentadas, tomando como base la teoría del comportamiento planificado (TPB).
- Se diseñó una guía de implementación del modelo propuesto, que considera 17 pasos para una adecuada implementación del modelo, siendo flexible en la selección de factores y soportado con un cuestionario adaptable dependiendo del contexto organizacional que se quiera estudiar.
- Se validó el modelo mediante un caso de estudio que fue la Universidad Nacional del Altiplano Puno, en 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 influenciado en el nivel macro por factores específicos; siguiendo los pasos de la guía de implementación; donde el modelo mostró una varianza explicada en constructor principal de 60.8%, en base a 128 observaciones válidas correspondientes a los usuarios del Sistemas Integral Administrativo de la UNA-Puno y un nivel de confiabilidad del 0.943, respecto a los factores de modelo.
- Dentro de todo el modelo, los factores más importantes por el grado de influencia en la Actitud para implementar Seguridad en Sistemas de Información son:

- En un primer lugar los Recursos y Presupuesto, donde el grado de influencia es -0.558, de acuerdo a su path, 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 donde el grado de influencia es 0.439, de acuerdo a su path, 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 grado de 0.431 path, 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 grado de 0.357 path, 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 grado 0.325 de acuerdo a su path, 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 grado de 0.304 path, influye en la autosuficiencia, lo que es lógico un usuario más experimentado puede adaptarse mejor a la implementación de un plan de seguridad.
  - La Misión de la Organización con un grado de 0.268 path, 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, permite una implementación exitosa.
  - El compromiso de la alta gerencia con un grado de -0.212 en su coeficiente path, 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 un grado de 0.463 en su path y el control conductual percibido con 0.463 path que explican el 60.8% de la varianza del factor principal. No es significativo la dimensión Norma subjetiva, según el caso de estudio.

5.2 Recomendaciones

Las recomendaciones que se proponen se detallan a partir de los objetivos planteados:

Modelo Planteado

En cuanto al modelo planteado podemos sugerir los siguientes:

- Estudiar los constructores más débiles para mejorar el cuestionario.
- Estudiar los factores desde la perspectiva del personal de T.I.

Guía de Implementación

En cuanto a la Guía de Implementación planteada se sugiere los siguientes:

- Implementar más casos de estudios de la Guía de implementación, para su validación.
- Centralizar información estudiada para explotación posterior, principalmente en el sector público.
- Desarrollar un software que permita automatizar la guía de implementación.

Casos de Estudio

En cuanto a los casos de estudio podemos sugerir los siguientes:

- Evaluar otros casos de estudio transversales en otros sectores.
- Efectuar mayores estudios longitudinales en función de los transversales.
- Controlar los factores que se ha detectado para una adecuada implementación de la Seguridad en Sistemas de Información en la Universidad Nacional del Altiplano.

Bibliografía

1. 42010:2007, I. (2007). Systems and Software Engineering – Recommended Practice for Architectural Description of Software-Intensive Systems. USA: ISO.
2. 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.
3. Academia Latinoamericana de la Seguridad Informática. (2011 de 01 de 14). Unidad 1: Introducción a la Seguridad de Información. (MIcrosoft Technet) Obtenido de http://www.mslatam.com/latam/technet/cso/Html-ES/home.asp
4. Academia Latinoamericana de la Seguridad Informática. (14 de 01 de 2011). Unidad 1: Introducción a la Seguridad de Información. (Microsoft Technet) Obtenido de http://www.mslatam.com/latam/technet/cso/Html-ES/home.asp
5. Aceituno, V. (12 de 2004). Definición de seguridad de la información y sus limitaciones. Recuperado el 03 de 03 de 2011, de http://www.fistconference.org/data/presentaciones/queesseguridad.pdf
6. AIRC. (2008). Attack Intelligence Research Center Annual Threat Report: 2008 Overview and 2009 Predictions. Obtenido de http://www.aladdin.com/pdf/airc/AIRC-Annual-Threat-Report2008.pdf
7. Ajzen, I. (1991). The theory of planned behavior. Organizational behavior and human decision processes (50), 179 -211.
8. Ajzen, I., & Fishbein, M. (1980). Understanding attitudes and predicting social behavior. Englewood Cliffs. N.J., Inc. U.S.A: Prentice Hall.
9. Al-Awadi, M., & Renaud, K. (2008). Success Factors in Information Security Implementation in Organizations. University of Glasgow .
10. ALEGSA. (2005). Definición de ataque informático. Recuperado el 05 de 03 de 2011, de http://www.alegsa.com.ar/Dic/ataque%20informatico.php
11. Alfaro, J. (2007). La Arquitectura Empresarial Unificada (AEU) Como Herramienta Estratégica De Modelamiento Organizacional Para La Competitividad Funcional De Las Universidades. Lima: Univ. Federico Villareal.
12. Amoako-Gyampah, K., & Salam, A. (2004). An extension of the technology acceptance model in an ERP implementation environment. Information & Management (41), 731-745.

13. Anderson, J. P. (1980). Computer Security Threat Monitoring and Surveillance. Recuperado el 14 de 02 de 2011, de csrc.nist.gov/publications/history/ande72.pdf
14. Anderson, R. (2001). Why information security is hard – An economic perspective. Proceedings of the 17th Annual Computer Security Applications Conference ACSAC'01. IEEE Computer Society.
15. Andrew, J. (2009). TOGAF™ Version 9 A Pocket Guide. usa: Berkshire: The Open Group.
16. Bailey, D. (1995). Information Security: An Integrated Collection of Essays: Essay 3 A Philosophy of Security Management. California USA: ACSAC.
17. Ballantine, J., & etal. (1996). The Model of information systems success: the search for the dependent variable continues. Information Resources Management Journal , 9 (4), 5-14.
18. Bandura, A. (1982). Self-efficacy mechanism in human agency. The American Psychologist , 37 (2), 122-147.
19. Barbosa Martins, A., & Saibel Santos, C. A. (2005). Uma metodologia para implantação de um sistema de gestão de segurança da informação. Journal of Information Systems and Technology Management , 2 (2), pp 121-136.
20. Barclay, D., Higgins, C., & Thompson, R. (1995). The partial least squares (PLS) approach to causal modeling: personal computer adoption and use as an illustration,Technology Studies. Special Issue on Research Methodology , 2 (2), pp.285-309.
21. Baskerville, R. (1993). Information systems security design methods: Implications for information systems development. ACM Computing Surveys , 25 (4), 375-413.
22. Baskerville, R., & Siponen, S. (2002). An information security meta-policy for emergent organizations. Logistics Information Management , 15 (5/6), 336-346.
23. Bateman, T. S., & Snell, S. A. (2001). Administración. Una ventaja competitiva (4ª edición ed.). México: Mcgraw Hill .
24. Bennatan, E. M. (2000). On time within budget. Software management practices and techniques (Third Edition ed.). U.S.A.: John Wiley and Sons Inc.
25. Bjorck, F. (2002). Implementing Information Security Management Systems – An Empirical Study of Critical Success Factors.
26. Brinkley, D. L., & SChell, R. R. (1995). Information Security: An Integrated Collection of Essays: Essay 1 What is there to worry about? An Introduction to the Computer Security Problem. California USA: ACSAC.
27. 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.
28. Cabrera García, S., García Castro, M. d., & Salinas Romero, J. P. (2009). Modelo de Seguridad en Aplicaciones WEB Desarrolladas por un Tercero. Mexico, Ing Thesis, Instituto Politécnico Nacional.
29. Calder, A., & Watkins, S. (2003). IT Governance: A Manager's Guide to Data Security & BS 7799/ISO 17799. London: Kogan Page Ltd.
30. Cao Avellaneda, J. (2005). Análisis y gestión de riesgos de la seguridad de los sistemas. InforMAS Revista de Ingeniería Informática del CIIRM .
31. Carballo, M. (1990). Estrategias para determinar los factores críticos de éxitos de las empresas y sus efectos en la planeación de sistemas de Información. Tesis. ITESM, Monterrey, N.L.
32. 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 .
33. Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). A Model for Evaluating IT Security Investments. Communications of the ACM , 47 (7), pp. 87-92.
34. Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers. International Journal of Electronic Commerce , 9 (1), 69-104.
35. Cea D´Ancona, Á. (2002). Análisis multivariable teoría y práctica en la investigación social. Síntesis S.A.
36. CERT. (2008). Software Ingenieering Institute. Recuperado el 05 de 02 de 2011, de Carnegie Mellon University: http://www.cert.org/cert/
37. Chaulaa, J. A., Yngströmb, L., & Kowalskic, S. (2005). A Framework for Evaluation of Information Systems Security. Information Security South Africa ISSA 2005 , 62-71.
38. Chiavenato, I. (2006). Introducción a la Teoría General de la Administración. Mexico: McGraw-Hill Interamericana.
39. Chirinos, L. (s.f.). Descentralización: situación y perspectivas. Recuperado el 14 de 02 de 2011, de http://palestra.pucp.edu.pe/?id=228
40. Christopher, A., & Autrey, D. (2003). Managing Information Security Risks The OCTAVE Approach. USA: Addison-Wesley.
41. Chuttur, M. (2009). Overview of the Technology Acceptance Model: Origins,Developments and Future Directions. Sprouts: Working Papers , 9 (37), 1-20.
42. CISCO. (2010). Cisco 3Q10Global Threat Report. Recuperado el 04 de 02 de 2011, de http://www.cisco.com/en/US/prod/collateral/vpndevc/3q10_cisco_threat.pdf

43. Cohen, L., & L, M. (1990). Métodos de investigación educativa. Madrid: La Muralla.
44. Consejo Editorial A.F.A. (2004). Gran Diccionario Jurídico. Lima Perú: Editores Importadores S.A.
45. Contraloría General de la República. (2009). ENCUESTA DE VERIFICACION DE CUMPLIMIENTO DE LA "FORMULACIÓN Y EVALUACIÓN DEL PLAN OPERATIVO INFORMÁTICO DE LAS ENTIDADES DE LA ADMINISTRACIÓN PÚBLICA PARA EL AÑO 2008. Perú.
46. Córdova Rodriguez, N. (2003). Plan de seguridad informática para una entidad financiera. Lima Perú, Ing. Thesis, Universidad Mayor de San Marcos.
47. Cornell University. (2006). Cornel University Dictionary U.S.C § 3542. Recuperado el 04 de 03 de 2011, de http://www.law.cornell.edu/uscode/html/uscode44/usc_sec_44_00003542----000-.html
48. Cressonwood, C. (1999). Policies: The Path to Less Pain & More Gain. Recuperado el 02 de 02 de 2011, de http://www.infosecuritymag.com/articles/1999/augcover.shtml
49. CSI. (2009). 14th Anual CSI Computer Crime and Security Survey. USA: CSI.
50. Cuenca González, Llanos; Ortiz Bas, Ángel; Boza García, Andrés. (2005). Arquitectura de Empresa. Visión General. Gijón: IX Congreso de Ingeniería de Organización.
51. Czinkota, M., & Masaaki, K. (2001). Administración de Mercadotecnia. México: International Thomson Editores.
52. Davis, F. D. (1986). A Technology Acceptance Model for Empirically Testing New End- User Information Systems: Theory and Results,. Cambridge: MIT Sloan School of Management.
53. Davis, F. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. MIS Quarterly (13), 319-340.
54. Definiciones. (2010). Definiciones.de. Recuperado el 2 de 11 de 2011, de http://definicion.de/modelo/
55. Delone, W., & Mclean, E. (1992). Information systems success: The quest for the dependent variable. Information systems research, 3 (1), 60-95.
56. Delone, W., & Mclean, E. R. (2002). Information systems success. Proceedings of the 35th Hawaii international conference on system sciences IEEE .
57. Delone, W., & Mclean, E. (2003). The DeLone and McLean model of information systems success: A Ten-Year update. Journal of Management Information Systems, 19 (4), 9-30.

58. Denning, D. (1987). An intrusion-detection model. IEEE Transactions on Software Engineering, 13 (2), 222–226.
59. Dhillon, G. (1999). Managing and Controlling Computer Misuse. Information Management & Computer Security, 7 (4), 171-175.
60. Dhillon, G. (2001). Violating of Safeguards by Trusted Personal and Understanding Related Information Security Concerns. Computer & Security, 20 (2), 165-172.
61. Dhillon, G., & Backhouse, J. (2001). Current directions in IS security research: Towards socio-organizational perspectives. Information Systems Journal, 11 (2), 127-153.
62. Dhillon, G., & Moores, S. (2001). Computer crimes: Theorizing About the Enemy Within. Computer & Security, 20 (8), 715-723.
63. Dinnie, G. (1999). The Second Annual Global Information Security Survey. Information Management & computer security, Vol. 7 (No. 3), pp. 112-120.
64. Doherty, N. F., & Fulford, H. (2005). Do Information Security Policies Reduce the Incidence of Security Breaches: An Exploratory Analysis Information Resources Management Journal, Vol. 18 (No. 2), pp. 21-39.
65. Druker, P. (1999). Los Desafios de la Gerencia del Siglo XXI. Bogota: Norma.
66. Dunkerley, K. D. (2011). Developing an Information Systems Security Success Model for Organizational Context. Phd. Thesis: Nova Southeastern University.
67. Dunkerley, K., & Tejay, G. (2009). Developing an Information Systems Security Success Model for eGovernment Context. AMCIS 2009 Proceedings, 1-6.
68. Eberhagen, N., & Naseroladl, M. (1992). Critical Success Factor. A survey. University of Váxjó.
69. Erb, M. (s.f.). Gestión de Riesgo en la Seguridad Informática. Recuperado el 03 de 03 de 2011, de http://protejete.wordpress.com/
70. Ernst & Young. (2008). Moving Beyond Compliance: Ernst & Young's 2008 Global Information Security Survey. Obtenido de http://www.ey.com/Publication/vwLUAssets/2008_Global_Information_Security_Survey_english/$FILE/2008_GISS_ingles.pdf
71. Espasa-Calpe. (2005). Diccionario de la lengua española. Recuperado el 02 de 01 de 2011
72. Ferrell, O. C., & Geoffrey, H. (2004). Introducción a los Negocios en un Mundo Cambiante (Cuarta Edición ed.). México: McGraw-Hill Interamericana.
73. Fishbein, M., & Ajzen, I. (1975). Belief, attitude, intention and behavior: an introduction to theory and research. Reading, MA: Addison-Wesley.
74. Fitzgerald, T. (2007). Information Security Governance. En H. Tipton, & M. Krause, Information Security Management Handbook. USA: Auerbach Publications.

75. Fragoza Ureta, J. V. (1994). Definición y Estudio de los factores críticos De éxito para la función de informática. Tesis. ITESM. Monterrey, N.L.
76. Fung, P., & Jordan, E. (2002). Implementation of Information Security: A Knowledge-based Approach.
77. Garbars, K. (2002). Implementing an Effective IT security Program. As part of the information security: SANS Institute.
78. García, A. (2010 de 11 de 12). Arquitectura de Sistemas de Información. Obtenido de http://www.servitel.es/inforsalud97/32/32.htm
79. Gómeza, R., Pérez, D. H., Yezid, D., & Herrerad, A. (2010). Metodología y gobierno de la gestión de riesgos de tecnologías de la información. Revista de ingeniería. Universidad de los Andes (31), 109-118.
80. Grant, R. (1996). Dirección estratégica. Conceptos, técnicas y aplicaciones. Civitas, Madrid.
81. Hair, J. F., & etal. (1999). Análisis multivariante (5ª edición ed.). México: Prentice Hall.
82. Harris, S. (2004). CISSP Certification: All in One Exam Guide. Emerville California USA: Mc Graw Hill.
83. Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, P. (2010). Metodología de la investigación (5ta Edición ed.). México: McGraw-Hill Interamericana.
84. Herrán Escobar, J. G. (2009 de 10 de 2009). Integración entre Arquitectura Empresarial y Gestión de Servicios de TI. Recuperado el 2010 de 12 de 06
85. Holappa, J. M., & Wiander, T. J. (2008). Practical implementation compliant information of an ISO 17799 compliant information security management system using a novel ASD method. Proceedings of the sixth Australasian conference on Information security.
86. Huang, D.-L., Patrick Rau, P.-L., & Salvendy, G. (2007). A Survey of Factors Influencing People's Perception of Information Security. Human-Computer Interaction, Part IV, HCII 2007, LNCS 4553, pp. 906–915.
87. 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.
88. Huerta Barrera, T. R. (1998). Derecho Municipal. México: Porrúa S.A.
89. Hyeun-Suk, R., Cheongtag, K., & Young U., R. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior computers & s e c u r i t y , 1-11.
90. INDECOPI. (2004). Norma Técnica Peruana "NTP-ISO/ IEC 17799:2004 EDI. Tecnología de la Información primera versión. Lima.
91. INDECOPI. (2007). Norma Técnica Peruana "NTP-ISO/ IEC 17799:2007 EDI (ISO 27002:2005). Tecnología de la Información segunda versión. Lima.

92. INDECOPI. (2009). NTP -ISO/IEC 27005,2009 EDI Tecnologías de Información. Técnicas de Seguridad. Gestión de Riesgo en Seguridad de Información. Lima.
93. Instituto Nacional de Tecnologías de la comunicación (INTECO). (2010). Curso de sistema de gestión de la seguridad de la información según la norma UNE-ISO/IEC 27000. España: INTECO.
94. ISO. (2010). International Organization for Standarization. Recuperado el 8 de 8 de 2011, de http://www.iso.org/iso/home.html
95. ISO. (2004). ISO/IEC 13335-1:2004. Recuperado el 03 de 02 de 2011, de www.iso.prg
96. ISO/IEC. (2005). Information technology - Security techniques - Information security management system - Requirements (ISO/IEC27001:2005). USA: ISO/IEC.
97. ISO/IEC. (2005). ISO/IEC 17799:2000 Information technology – Code of practice for information security 2d Ed. Switzerland: International Organization for Standardization.
98. ISO/IEC. (2007). ISO/IEC 27002 Code of practice for information security management. USA.
99. ISO/IEC. (2005). ISO27001 International standard - Information technology - Security techniques - Information security management systems - Requirements. Recuperado el 08 de 02 de 2011, de http://www.iso27000.es/glosario.html
100. IT Governance Institute ITGI. (2007). COBIT 4.1. USA: IT Governance Institute.
101. ITIL. (s.f.). ITIL v3 Official Site. (Office of Govenrment Commerce) Recuperado el 4 de 12 de 2010, de http://www.itil-officialsite.com/
102. 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.
103. Katz, F. H. (2005). The Effect of a University Information Security Survey on Instruction Methods in Information.
104. Kendall, K. E., & Kendall, J. E. (1997). Análisis y Diseño de Sistemas de Información (3ra ed.). Mexico: Prentice Hall Hispanoamerica.
105. King, S. F., & Burgess, T. F. (2005). Beyond critical success factors: a dynamic model of enterprise system innovation. International Journal of Information Management , 26, 59-69.
106. Kotulic, A. G., & Clark, J. G. (2003). Why there aren't more information security research studies. Information & Management , 41 (5), 597-607.
107. Lampson, B. W. (2002). Computer Security in the Real World Principles of Computer Systems. www.research.microsoft.com/lampson.
108. Lau, O. (1988). The Ten Commandments of Security. computer & security (17), 119123.
109. Laudon, K. C., & Laudon, J. P. (1996). Administración de los Sistemas de Información (3ra ed.). México: Prentice Hall.

110. Laudon, K., & Laudon, J. (2004). Sistemas de Información Gerencial. Mexico: Pearson Education.
111. Linares, S., & Paredes, I. (2007). IS2ME (Information Security to the Medium Enterprise) Un Método para Implementar la Seguridad de la Información en las Pequeñas y Medianas Empresas. INSECURE, 13, pp 78-82.
112. Macmillan. (2002). Computer Science Study Guide. USA: Gale Group.
113. Malhotra, Y. (2006). Enterprise Arquitecture: An Overview. Recuperado el 15 de 11 de 2009, de http://www.kmboook.com/enterach.htm
114. Manzano Patiño, A., & Zamora Muñoz, S. (2009). Sistema de ecuaciones estructurales: Una herramienta de investigación. Centro nacional de evaluación para la educación superior A.C. (Ceneval).
115. MAP. (2005). Metodología MAGERIT. Recuperado el 07 de 03 de 2011, de http://www.csi.map.es/csi/pg5m20.htm
116. Martin R., R. E. (2004). Architectural principles for enterprise frameworks www.cs.indiana.edu/pub/techreports/TR594.pdf. Recuperado el 11 de 11 de 2010, de www.cs.indiana.edu/pub/techreports/TR594.pdf
117. Mason, R. (1978). Measuring information output: A communications systems approach. Information & Management, 1 (4), 219-234.
118. McGill, T., Hobbs, V., & Klobas, J. (2003). User-development applications and information systems success: a test of delone & mclean's model. Information resource management journal, 16 (1), 24-45.
119. McKay, J. (2003). Pitching the Policy: implementing IT Security Policy through Awareness. USA: SANS Institute.
120. McSweeney, A. (2009). Enterprise Architecture and TOGAF (The Open Group Architecture Framework). Recuperado el 25 de 11 de 2010, de www.linkedin.com/in/alanmcsweeney
121. Medina Quintero, J. M. (2005). Evaluación del Impacto de los Sistemas de Información en el Desempeño Individual del Usuario. Aplicación en Instituciones Universitarias. PhD Thesis: UNIVERSIDAD POLITÉCNICA DE MADRID.
122. MINISTERIO DE ADMINISTRACIONES PÚBLICAS. (2006). MAGERIT versión 2 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información El Método. Madrid España: MAP.
123. Miroslav, B. (2010). The risk assessment of information system security. Recuperado el 06 de 01 de 2011, de University of Zagreb, Faculty of Organization and Informatics, Varašdin, Croatia: http://www.carnet.hr/CUC/cuc2004/program/radovi/a5_baca/a5_full.pdf.
124. Morlán Santa Catalina, I. (2010). Modelo de Dinámica de Sistemas para la implantación de Tecnologías de la Información en la Gestión Estratégica Universitaria. PhD Thesis: Universidad del País Vasco. España.

125. Myers, B., Kappelman, L. A., & Prybutok, V. R. (1997). A comprehensive model for assessing the quality and productivity of the information systems function: toward a theory for information systems assessment. Information Resources Management Journal, 10.

126. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. (1995). An Introduction to Computer Security: The NIST Handbook. Special Publication 800-12 Washington USA: National Institute of Standards and Technology (NIST).
127. NIST. (2002). Risk Management Guide for Information Technology Systems, NIST Special Publication 800-30. Recuperado el 20 de 01 de 2011, de http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf
128. Nosworthy, J. D. (2000). Implementing information security in the 21st century – Do You Have the Balancing Factors? computer & security (19), 337-347.
129. Novakovic, L., McGill, T., & Dixon, M. (2009). Understanding User Behavior towards Passwords through Acceptance and Use Modelling. International Journal of Information Security and Privacy, 3 (1), 11-29.
130. ONGEI. (2009). Informe de Evaluación del POI Gobierno Central por Sector/Entidad 2009. Lima: ONGEI.
131. ONGEI. (2004). OFICINA NACIONAL DE GOBIERNO ELECTRÓNICO E INFORMÁTICA. Recuperado el 11 de 02 de 2011, de Primera encuesta de Seguridad de la Información en la Administración Pública: http://www.ongei.gob.pe/publicaciones/IEncuestadeSeguridad.pdf
132. ONGEI. (2004). OFICINA NACIONAL DE GOBIERNO ELECTRÓNICO E INFORMÁTICA. Recuperado el 10 de 02 de 2011, de Norma Técnica Peruana: www.ongei.gob.pe/bancos/banco_normas/archivos/P01-PCM-ISO17799-001-V1.pdf
133. Open Group. (2009). TOGAF Version 9 The Open Group Architecture Framework (TOGAF). USA: The Open Group, 2009.
134. Pahnila, S., Siponen, M., & Mahmood, A. (2007). Employees' Behavior towards IS Secur ity Policy Compliance. Proceedings of the 40th Hawaii International Conference on System Sciences.
135. Pahnila, S., Siponen, M., & Mahmood, A. (2007). Employees behavior towards IS security policy compliance. In 40th Hawaii International Conference on System Sciences (HICSS 07).
136. Pallas, G., & Corti, M. E. (2009). Metodología de Implantación de un SGSI en grupos empresariales de relación jerárquica. Uruguay Magister Thesis: Universidad de la República.
137. 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.

138. Peltier, T. R. (2005). Information Security Risk Analysis. USA: CRC Press.
139. Perks, C., & Beveridge, T. (2003). GUIDE TO ENTERPRISE IT ARCHITECTURE. New York USA: Springer Verlag.
140. Peso Navarro, E. (2004). El Documento de Seguridad. España: Dias de Santos.
141. Ponemon Institute. (2010). 2009 Annual Study: Global Cost of Data Breach, Understanding Financial Impact, Customer Turnover and Preventive Solutions. USA: Ponemon Institute PGP.
142. Poyato, C.-C., & Francisco-MORENO, D. (2000). Definición de una política de seguridad. Recuperado el 07 de 03 de 2011, de http://www.rediris.es/cert/doc/docu_rediris/recomendaciones/html/recomendaciones.html
143. Presidencia de Consejo de Ministros. (22 de 08 de 2009). Crean Grupo de Trabajo denominado Coordinadora a Respuestas de Emergencias en Redes Teleinformáticas de la Administración Pública de Perú (PeCERT) . El Peruano, pág. 401351.
144. Rai, A., Lang, S. S., & Welker, R. (2002). Assessing the validity of is success models: test and theoretical analysis. Information Systems Research, 13 (1), 50-69.
145. Rayme Serrano, R. A. (2007). Gestión de seguridad de la información y los servicios críticos de las universidades: un estudio de tres casos en Lima Metropolitana. Lima, Msc. Thesis, Universidad Nacional Mayor de San Marcos.
146. Real Academia Española. (2011). Diccionario de la Real Academia Española (definición de modelo). Recuperado el 11 de 12 de 2011, de http://www.rae.es/rae.html
147. Reason, J. (1997). Managing the Risk of Organizational Accidents. Hants, UK: Ashgate Publishing Ltd.
148. Reynolds, J., & Holbrook, P. (1991). RFC 1244: Site Security Handbook.
149. Rockart, J. F. (1982). The changing role of the information systems executives: A critical success factors perspective. Sloan Managament Review Association.
150. Roldán S, J. L. (2004). Introducción a la técnica partial least squares. España: Departamento de Administración de Empresas y Marketing Universidad de Sevilla.
151. Roldán S, J. L., & Leal, A. (2003). A validation test of an adaptation of the delone and mclean's model in the spanish EIS field, En: J.J. Cano (Ed): Critical Reflections on Information Systems. A systemic approach. Hershey, PA, USA: Idea Group Publishing.
152. Roman Torres, L. Y. (2010). TOGAF & ZACHMAN FRAMEWORK. Recuperado el 2010 de 11 de 11, de

http://auditoriauc20102miju02.wikispaces.com/file/view/Togaf201021700410239.pdf
153. Sanchez Acevedo, N., & Segura Castañeda, J. S. (2006). Una Guía Metodológica para el Cálculo de Retorno de Inversión (ROI), en Seguridad Informática: Un Caso de Estudio. Colombia, Eng Thesis, Pontificia Universidad Javeriana.
154. Sánchez, L. E., Villafranca, D., Fernández-Medina, E., & Piatini, M. (2007). MGSM-PYME: Metodología para la gestión de la seguridad y su madurez en las PYMES. V CONGRESO IBEROAMERICANO DE SEGURIDAD INFORMATICA 2009 CIBSI MONTEVIDEO URUGUAY, pág. 437-450.
155. Sánchez-Franco, M. J., & Roldán, J. L. (2005). Web acceptance and usage model, Comparison between goal-directed and experiential web users. Internet Research, 15 (1), pp. 21-48.
156. Seddon, P., & Kiew, M. (1996). A partial test and development of DeLone and McLean's model of is success. Australian Journal of Information Systems, 4 (1), 90-109.
157. Senn, J. (1992). Análisis y Diseño de Sistemas de Información. México: Mc Graw Hill.
158. Shannon, C., & Weaver, W. (1949). The Mathematical Theory of Communication. Urbana, IL. University of Illinois Press. U.S.A. .
159. SHOPS. (2006). Smart Home Payment Services. Towards the liberalisation of Europe's utilities industry. Espoo vol. 2335: VTT Research Notes.
160. Siponen, M. T. (2001). A Conceptual Foundation for Organizational Information Security Awareness. Information Management & Computer Security, Vol. 8 (No. 1), pp. 31-41.
161. 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.
162. Solms, R. v. (1998). Information Security Management (2): guidelines to the management of information technology security (GMITS). information management & Computer Security , 221223.
163. Stoneburner, G. (2001). NIST Special Publication 800-33: Underlying Technical. Gaithersburg USA: National Institute of Standards and Technology (NIST).
164. Strassmann, P. A. (2009). El arte de presupuestar: como justificar los fondos para Seguridad Informática. Recuperado el 07 de 03 de 2011, de http://www.nextvision.com/
165. Straub, D. W., & Nance, W. D. (1990). Discovering and Disciplining Computer Abuse in Organizations: A Field Study. MIS Quarterly, 22 (4), pp. 441-469.
166. Symantec. (2009). Symantec Internet Security Threat Report: Trends for 2008. Obtenido de

http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_exec_summary_internet_security_threat_report_xiv_04-2009.en-us.pdf
167. Taylor, S., & Todd, P. (1995). Assessing IT usage: The role of prior experience. MIS Quarterly, 19 (4), 561-570.
168. 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.
169. Tipton, H. F., & Krause, M. (2006). Information Security Management Handbook. USA: CRC Press.
170. Torres, J. M., & Sarriegui, J. M. (2003). Dynamics Aspects of Security Management of Information Systems. . Proceedings of Systems Dynamic Society Conference Oxford, UK.
171. Torres, J. M., Sarriegi, J. M., Santos, J., & Serrano, N. (2006). Managing Information Systems Security: Critical Success Factors and Indicators to Measure Effectiveness. Springer-Verlag Berlin Heidelberg ISC 2006 , 530 – 545.
172. Tworek, W., & Chiesa, G. (2004). Lotus Security Handbook. USA: International Business Machines.
173. van Sante, T., & Ermers, J. (2009). TOGAF™ 9 and ITIL® V3 Two Frameworks Whitepaper.
174. Venkatesh, V., & Davis, F. (2000). A theoretical extension of the technology acceptance model: four longitudinal field studies. Management Science, 46 (2), 186-204.
175. Venkatesh, V., Morris, M., Davis, G., & Davis, F. (2003). User acceptance of information technology: Toward a unified view. MIS Quarterly, 27 (3), 425-478.
176. Vernadat, F. (1996). Enterprise Modeling and Integration. Principles and applications. usa: Chapman&Hall.
177. 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.
178. Villena Aguilar, J. A. (2006). Sistema de Gestión De Seguridad De Información Para Una Institución Financiera. Perú, Eng Thesis, Pontificia Universidad Católica del Perú.
179. Weill, P., & Ross, J. (2006). Five Key IT Decisions: Making IT a Strategic Asset. En IT Governance: How Top Performers Manage IT Decision Rights for Superior Results. USA: Harvard Business Press.
180. Whitman, M. E. (2003). Enemy at the Gate: Threats to Information Security. ACM, 46 (8), 91-95.
181. Whitman, M. E., & Mattord, H. J. (2007). Management of Information Security. USA: Course Technology.

182. 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.
183. Whitten, J. (2003). Análisis y Diseño de Sistemas de Información. España: Editorial IRWIN.
184. Wiander, T. J., & Holappa, J. M. (2006). Theoretical framework of ISO 17799 compliant information security management system using novel ASD method. IAEA Technical Meeting on Cyber Security of Nuclear Power Plant Instrumentation, Control and Information Systems, pp 17-20.
185. Wolfang, K. (2009). TOGAF 9 Quick Start Guide for Architects. USA: Wolfnag Keller.
186. Zachman, J. (s.f.). Concepts of the framework for enterprise architecture. Recuperado el 12 de 11 de 2010, de http://members.ozemail.com.au/~visible/papers/zachman3.htm
187. Zamora Muñoz, S., Monroy Cazorla, L., & Chávez Álvarez, C. (2009). Análisis factorial: Una técnica para evaluar la dimensionalidad de las pruebas. Centro Nacional de Evaluación para la Educación Superior A.C. (Ceneval).
188. Zikmund, W. G. (2003). Fundamentos de investigación de mercados. Madrid: Thomson Paraninfo S.A.

ANEXOS

Anexo 1: Cuestionario propuesto para la evaluación de los Factores Críticos de Éxito para la Implementación de Seguridad en Sistemas de Información

UNIVERSIDAD NACIONAL DEL ALTIPLANO – VICE RECTORADO ADMINISTRATIVO

Cuestionario para Usuarios de Sistemas de Información de la Universidad Nacional del Altiplano
Evaluación de Factores Críticos de éxito para Implementar Seguridad en Sistemas de Información

Objetivo. Determinar el impacto de los Factores Críticos de éxito para Implementar Seguridad en Sistemas de Información con la finalidad de evaluar el impacto en la Intención para Implementar Seguridad en los sistemas de información en el proceso Académico y Administrativo, con la finalidad de Implementar Planes Exitosos de Seguridad de Información más adecuados a las necesidades de la organización y los usuarios.
Antes de empezar:

- No escriba su nombre o de la institución en este cuestionario.
- Sus respuestas serán tratadas estadística y confidencialmente en una forma estricta.
- Es importante que *responda a todas las preguntas*.
- *Poner sólo una respuesta*.
- No hay respuestas correctas o capciosas, lo importante es indicar el estado real en su área de trabajo, con respecto a los sistemas de información.
- Su opinión es valiosa. Por favor, durante la encuesta no pregunte las respuestas a sus compañeros/as.

I. En primer lugar, se le pide que conteste las preguntas de índole general:

Datos Generales de Usuario:

Sexo: ☐ Masculino ☐ Femenino

Edad: ☐ De 20 a 29 años ☐ De 30 a 39 años ☐ De 40 a 49 años ☐ De 50 a 59 años ☐ De 60 a más años

Nivel de Estudios:
☐ Superior Incompleta ☐ Superior no Universitaria Completa ☐ Superior Universitaria Completa ☐ Con estudios de Postgrado

Tiempo que trabaja en la Universidad Nacional del Altiplano:
☐ Menor a 1 año ☐ 1 a 2 años ☐ 3 a 5 años ☐ 6 a 10 años ☐ 11 o más años

Conocimientos de Informática y Computación:
☐ Muy Básico ☐ Básico ☐ Regular ☐ Avanzado ☐ Experto

Años usando el/los sistemas de Información Administrativa:
☐ Menor a 1 año ☐ 1 a 2 años ☐ 3 a 5 años ☐ 6 a 10 años ☐ 11 o más años

Horas aproximadas, a la semana, que usa el sistema:
☐ 0 a 10 horas ☐ 11 a 20 horas ☐ 21 a 30 horas ☐ 31 a 40 horas ☐ 41 a más horas

II. Responda los cuestionamientos de acuerdo con su experiencia y percepción, marcando con ✔ o una ✗ o rellenando el recuadro que más se acerque a su respuesta, considerando la escala del 1 al 5.

Ejemplos: 1 2 3 ✔ 5 1 2 3 ✗ 5 1 2 3 ■ 5, donde:

Muy en desacuerdo
1 ---------- 2 ---------- 3 ---------- 4 ---------- 5
Muy inadecuado — Muy de acuerdo — Muy adecuado

Compromiso de la Alta Gerencia

En la implementación de proyectos de Sistemas de Información Previos en su Dependencia:

1. ¿Sintió el compromiso de la Alta Dirección en todo el proyecto de sistemas?	1 2 3 4 5
2. ¿Sintió que los directivos participaron activamente y con responsabilidad?	1 2 3 4 5
3. ¿Existió algún tipo de motivación, reconocimiento, recompensa o aumentos por parte de un directivo cuando se implemento el Proyecto?	1 2 3 4 5
4. ¿Sintió que los directivos participaron activamente en el planeamiento o mejoras al Proyecto?	1 2 3 4 5
5. ¿Sintió que las personas responsables (sobre todo directivos) apoyaron con los recursos económicos y materiales para llevar a cabo el proyecto?	1 2 3 4 5
6. ¿Existió cambio o rotación (cambio constante) de puesto de los directivos durante el proyecto?	1 2 3 4 5
7. ¿Los directivos dejan en manos del área de Sistemas (OTI) los aspectos de seguridad de información?	1 2 3 4 5

Cultura Organizacional

8. ¿Usted como usuario, tiene los conocimientos necesarios para la operación de una computadora?	1 2 3 4 5
9. ¿Siente que Existen relaciones amistosas con el personal técnico de sistemas?	1 2 3 4 5
10. ¿Considera que Existen factores políticos internos que afectan a usted en su trabajo y a la implementación de proyectos de Sistemas?	1 2 3 4 5
11. ¿Considera que su entorno laboral es adecuado para el desarrollo de Seguridad en los Sistemas?	1 2 3 4 5
12. ¿Considera usted que su ambiente de trabajo favorecería la implementación de Seguridad en los Sistemas?	1 2 3 4 5
13. ¿ Considera que Una vez iniciado el Proyecto de Sistemas de información, usualmente no funciona o se cancela por factores políticos, económicos u otros intereses?	1 2 3 4 5
14. ¿Se siente usted muy comprometido con las actividades ligadas a la protección y seguridad de datos de los Sistemas que usa?	1 2 3 4 5

Misión de la Organización

15. ¿Considera que la misión de la Universidad Nacional del Altiplano es clara?	1 2 3 4 5
16. ¿Considera que En su dependencia se tienen metas y objetivos claros?	1 2 3 4 5
17. ¿ Siente que Dichas metas y objetivos se cumplen a cabalidad?	1 2 3 4 5
18. ¿Considera que los sistemas apoyan al cumplimiento de las metas y objetivos de su dependencia?	1 2 3 4 5
19. ¿Considera que si existe errores en los sistemas (por virus, fallas, perdida de información, etc) afectaría el logro de las metas y objetivos de su dependencia?	1 2 3 4 5
20. ¿Considera que la seguridad en los sistemas es importante para el cumplimiento de los planes de su dependencia y de la Universidad?	1 2 3 4 5

Recursos y Presupuesto

21. ¿Considera que Existe disponibilidad de los recursos materiales (CPU, Muebles, antivirus etc.) que se usa para que los Sistemas funcionen adecuadamente?	1 2 3 4 5
22. ¿Siente que hay prioridad en el otorgamiento de los recursos materiales que se usa en su trabajo con los sistemas?	1 2 3 4 5
23. ¿Percibe que se asigna el suficiente personal técnico y de apoyo para el soporte de los sistemas?	1 2 3 4 5
24. ¿Considera que Usa todos los materiales que dispone para su trabajo con los sistemas?	1 2 3 4 5

25. ¿Siente que Los recursos que Ud. Solicita para los sistemas son oportunamente atendidos?	1 2 3 4 5
26. ¿Siente que hay demora en su trabajo por falta de recursos para mejorar los sistemas y que teniendo sistemas más eficientes podría evitar demoras?	1 2 3 4 5
27. ¿Cree que son suficientes el número y competencias del personal de sistemas?	1 2 3 4 5
28. ¿Si se implementa un proyecto de sistemas, siente que se le asignará los recursos y presupuestos necesarios oportunamente?	1 2 3 4 5

Formación y Capacitación

29. ¿Siente que su institución lo capacita frecuentemente en temas de informática y tecnológicos?	1 2 3 4 5
30. ¿Ha recibido capacitación útil por parte del área de sistemas de cómo proteger su información?	1 2 3 4 5
31. ¿En su institución los han capacitado o formado en temas de seguridad de información?	1 2 3 4 5
32. ¿En su institución se implementan talleres de formación y entrenamiento en temas seguridad y protección de información?	1 2 3 4 5
33. ¿Siente que su institución se preocupa por capacitarlo en temas actuales de informática y tecnológicos?	1 2 3 4 5

Conciencia de la necesidad de seguridad por el personal

34. ¿Considera que la seguridad de la información de su institución es importante y debe tomarse las medidas adecuadas de protección?	1 2 3 4 5
35. ¿Siente que necesita seguridad y protección confiable en su computador para evitar pérdida, daños y modificación de la información con que trabaja?	1 2 3 4 5
36. ¿Siente que podría ocurrir que un virus informático ocasione pérdida o deterioro de su información que retrasaría o perjudicaría su trabajo por lo que se debe proteger la información?	1 2 3 4 5
37. ¿Siente que podría ocurrir que un fallo eléctrico ocasione pérdida o deterioro de su información que retrasaría o perjudicaría su trabajo por lo que se debe proteger la información?	1 2 3 4 5
38. ¿Siente que podría ocurrir que un robo ocasione pérdida o deterioro de su información que retrasaría o perjudicaría su trabajo por lo que se debe proteger la información?	1 2 3 4 5
39. ¿Considera que Es importante cambiar las contraseñas de acceso al sistema frecuentemente?	1 2 3 4 5
40. ¿Considera que Es importante NO compartir su computador, contraseñas del sistema con otras personas?	1 2 3 4 5
41. ¿Realiza frecuentemente copias de su información (backup)?	1 2 3 4 5

Infraestructura Tecnológica existente

42. ¿Considera que Cuenta con los recursos informáticos (computadora, impresora) adecuados para realizar su trabajo cotidiano?	1 2 3 4 5
43. ¿Considera que Las computadoras trabajan eficientemente y sin fallas?	1 2 3 4 5
44. ¿Las computadoras están interconectadas por una red para compartir de información?	1 2 3 4 5
45. ¿Siente que La información se obtiene a tiempo gracias a la infraestructura existente?	1 2 3 4 5
46. ¿Siente que Cuenta con el servicio de internet adecuado?	1 2 3 4 5

Soporte hacia el usuario

47. ¿Siente una atención y asistencia técnica eficiente del área de sistemas cuando Ud. Tiene problemas?	1 2 3 4 5
48. ¿Siente que el área de soporte de sistemas ofrece soluciones en el tiempo adecuado?	1 2 3 4 5
49. ¿Cree que el personal del área de sistemas tiene el suficiente conocimiento y experiencia para ayudarlo cuando tiene problemas con el sistema de información o su computador?	1 2 3 4 5
50. ¿Cree que el personal del área de sistemas tiene el suficiente conocimiento y experiencia para ayudarlo con temas de seguridad de información?	1 2 3 4 5

Experiencia del usuario

51. ¿Considera que Es un experto en computadoras y sistemas?	1 2 3 4 5
52. ¿Siente que En cuanto a los problemas que se presentan con el sistema no requiere asistencia técnica?	1 2 3 4 5
53. ¿Considera que Conoce y utiliza métodos de seguridad de información para protegerse?	1 2 3 4 5
54. ¿Siente que Es natural navegar por internet y sabe cómo protegerse de virus y otros ataques?	1 2 3 4 5
55. ¿Siente que Es natural utilizar correo electrónico, y sabe cómo protegerse de virus y otros ataques?	1 2 3 4 5

Actitud para Implementar Seguridad en el Sistema de Información

56. Implementar seguridad en los Sistemas de Información será útil para mi trabajo	1 2 3 4 5
57. Las ventajas de utilizar seguridad en los Sistemas de Información sobrepasará sus desventajas	1 2 3 4 5
58. A futuro creo que será necesario trabajar en un sistema con Seguridad de Información.	1 2 3 4 5
59. Implementar seguridad en los Sistemas de Información es importante.	1 2 3 4 5

Control conductual percibido (autosuficiencia)

60. Tengo suficientes habilidades para adaptarme a la Implementación de Seguridad de Información	1 2 3 4 5
61. Tengo suficientes conocimientos para adaptarme a la Implementación de Seguridad de Información	1 2 3 4 5
62. Tengo suficientes competencias para adaptarme a la Implementación de Seguridad de Información	1 2 3 4 5

Norma subjetiva (creencias normativas)

63. En general mi institución está preparada para implementar la seguridad en Sistemas de Información.	1 2 3 4 5
64. Mis compañeros de trabajo piensan que se debe implementar la seguridad en Sistemas de Información.	1 2 3 4 5
65. Mi jefe inmediato piensa que se debe implementar la seguridad en Sistemas de Información.	1 2 3 4 5
66. Los gerentes/autoridades piensan que se debe implementar la seguridad en Sistemas de Información.	1 2 3 4 5

Intención para Implementar Seguridad en los Sistemas de Información

67. Tengo la intención de usar la implementación de la Seguridad en Sistemas de información	1 2 3 4 5
68. Tengo la intención de apoyar la implementación de la Seguridad en Sistemas de información	1 2 3 4 5
69. Tengo la intención de asumir la responsabilidades de la implementación de la Seguridad en Sistemas de información en tres meses	1 2 3 4 5
70. Tengo la intención de proteger la información y los recursos tecnológicos de acuerdo al Sistema de Seguridad de Información que se implementará	1 2 3 4 5

Anexo 2: Cuestionario definitivo del caso de estudio UNA-Puno

UNIVERSIDAD NACIONAL DEL ALTIPLANO – VICE RECTORADO ADMINISTRATIVO

Cuestionario para Usuarios de Sistemas de Información de la Universidad Nacional del Altiplano
Evaluación de Factores Críticos de éxito para Implementar Seguridad en Sistemas de Información

Objetivo. Determinar el impacto de los Factores Críticos de éxito para Implementar Seguridad en Sistemas de Información con la finalidad de evaluar el impacto en la Intención para Implementar Seguridad en los sistemas de información en el proceso Académico y Administrativo, con la finalidad de Implementar Planes Exitosos de Seguridad de Información más adecuados a las necesidades de la organización y los usuarios.

Antes de empezar:

- No escriba su nombre o de la institución en este cuestionario.
- Sus respuestas serán tratadas estadística y confidencialmente en una forma estricta.
- Es importante que *responda a todas las preguntas*.
- *Poner sólo una respuesta.*
- No hay respuestas correctas o capciosas, lo importante es indicar el estado real en su área de trabajo, con respecto a los sistemas de información.
- Su opinión es valiosa. Por favor, durante la encuesta no pregunte las respuestas a sus compañeros/as.

I. En primer lugar, se le pide que conteste las preguntas de índole general:

Datos Generales de Usuario:

Sexo: ☐ Masculino ☐ Femenino

Edad: ☐ De 20 a 29 años ☐ De 30 a 39 años ☐ De 40 a 49 años ☐ De 50 a 59 años ☐ De 60 a más años

Nivel de Estudios:
☐ Superior Incompleta ☐ Superior no Universitaria Completa ☐ Superior Universitaria Completa ☐ Con estudios de Postgrado

Tiempo que trabaja en la Universidad Nacional del Altiplano:
☐ Menor a 1 año ☐ 1 a 2 años ☐ 3 a 5 años ☐ 6 a 10 años ☐ 11 o más años

Conocimientos de Informática y Computación:
☐ Muy Básico ☐ Básico ☐ Regular ☐ Avanzado ☐ Experto

Años usando el/los sistemas de Información Administrativa:
☐ Menor a 1 año ☐ 1 a 2 años ☐ 3 a 5 años ☐ 6 a 10 años ☐ 11 o más años

Horas aproximadas, a la semana, que usa el sistema:
☐ 0 a 10 horas ☐ 11 a 20 horas ☐ 21 a 30 horas ☐ 31 a 40 horas ☐ 41 a más horas

II. Responda los cuestionamientos de acuerdo con su experiencia y percepción, marcando con ✔ o una ✗ o rellenando el recuadro que más se acerque a su respuesta, considerando la escala del 1 al 5.

Ejemplos: 1 2 3 ✔ 5 1 2 3 ✗ 5 1 2 3 ■ 5, donde:

Muy en desacuerdo — Muy de acuerdo
1 ---------- 2 ---------- 3 ---------- 4 ---------- 5
Muy inadecuado — Muy adecuado

Compromiso de la Alta Gerencia

En la implementación de proyectos de Sistemas de Información Previos en su Dependencia:

1. ¿Sintió el compromiso de la Alta Dirección en todo el proyecto de sistemas?	1 2 3 4 5
2. ¿Sintió que los directivos participaron activamente y con responsabilidad?	1 2 3 4 5

3. ¿Existió algún tipo de motivación, reconocimiento, recompensa o aumentos por parte de un directivo cuando se implemento el Proyecto?	1 2 3 4 5
4. ¿Sintió que los directivos participaron activamente en el planeamiento o mejoras al Proyecto?	1 2 3 4 5
5. ¿Sintió que las personas responsables (sobre todo directivos) apoyaron con los recursos económicos y materiales para llevar a cabo el proyecto?	1 2 3 4 5

Cultura Organizacional

6. ¿Usted como usuario, tiene los conocimientos necesarios para la operación de una computadora?	1 2 3 4 5
7. ¿Siente que Existen relaciones amistosas con el personal técnico de sistemas?	1 2 3 4 5
8. ¿Considera que Existen factores políticos internos que afectan a usted en su trabajo y a la implementación de proyectos de Sistemas?	1 2 3 4 5
9. ¿Considera que su entorno laboral es adecuado para el desarrollo de Seguridad en los Sistemas?	1 2 3 4 5
10. ¿Considera usted que su ambiente de trabajo favorecería la implementación de Seguridad en los Sistemas?	1 2 3 4 5
11. ¿ Considera que Una vez iniciado el Proyecto de Sistemas de información, usualmente no funciona o se cancela por factores políticos, económicos u otros intereses?	1 2 3 4 5
12. ¿Se siente usted muy comprometido con las actividades ligadas a la protección y seguridad de datos de los Sistemas que usa?	1 2 3 4 5

Misión de la Organización

13. ¿Considera que la misión de la Universidad Nacional del Altiplano es clara?	1 2 3 4 5
14. ¿Considera que En su dependencia se tienen metas y objetivos claros?	1 2 3 4 5
15. ¿ Siente que Dichas metas y objetivos se cumplen a cabalidad?	1 2 3 4 5
16. ¿Considera que los sistemas apoyan al cumplimiento de las metas y objetivos de su dependencia?	1 2 3 4 5
17. ¿Considera que si existe errores en los sistemas (por virus, fallas, perdida de información, etc) afectaría el logro de las metas y objetivos de su dependencia?	1 2 3 4 5
18. ¿Considera que la seguridad en los sistemas es importante para el cumplimiento de los planes de su dependencia y de la Universidad?	1 2 3 4 5

Recursos y Presupuesto

19. ¿Considera que Existe disponibilidad de los recursos materiales (CPU, Muebles, antivirus etc.) que se usa para que los Sistemas funcionen adecuadamente?	1 2 3 4 5
20. ¿Siente que hay prioridad en el otorgamiento de los recursos materiales que se usa en su trabajo con los sistemas?	1 2 3 4 5
21. ¿Percibe que se asigna el suficiente personal técnico y de apoyo para el soporte de los sistemas?	1 2 3 4 5
22. ¿Considera que Usa todos los materiales que dispone para su trabajo con los sistemas?	1 2 3 4 5
23. ¿Siente que Los recursos que Ud. Solicita para los sistemas son oportunamente atendidos?	1 2 3 4 5
24. ¿Siente que hay demora en su trabajo por falta de recursos para mejorar los sistemas y que teniendo sistemas más eficientes podría evitar demoras?	1 2 3 4 5
25. ¿Cree que son suficientes el número y competencias del personal de sistemas?	1 2 3 4 5
26. ¿Si se implementa un proyecto de sistemas, siente que se le asignará los recursos y presupuestos necesarios oportunamente?	1 2 3 4 5

Formación y Capacitación

27. ¿Siente que su institución lo capacita frecuentemente en temas de informática y tecnológicos?	1 2 3 4 5
28. ¿Ha recibido capacitación útil por parte del área de sistemas de cómo proteger su información?	1 2 3 4 5
29. ¿En su institución los han capacitado o formado en temas de seguridad de información?	1 2 3 4 5
30. ¿En su institución se implementan talleres de formación y entrenamiento en temas seguridad y protección de información?	1 2 3 4 5
31. ¿Siente que su institución se preocupa por capacitarlo en temas actuales de informática y tecnológicos?	1 2 3 4 5

Conciencia de la necesidad de seguridad por el personal

32. ¿Considera que la seguridad de la información de su institución es importante y debe tomarse las medidas adecuadas de protección?	1 2 3 4 5
33. ¿Siente que necesita seguridad y protección confiable en su computador para evitar pérdida, daños y modificación de la información con que trabaja?	1 2 3 4 5
34. ¿Siente que podría ocurrir que un virus informático ocasione pérdida o deterioro de su información que retrasaría o perjudicaría su trabajo por lo que se debe proteger la información?	1 2 3 4 5
35. ¿Siente que podría ocurrir que un fallo eléctrico ocasione pérdida o deterioro de su información que retrasaría o perjudicaría su trabajo por lo que se debe proteger la información?	1 2 3 4 5
36. ¿Siente que podría ocurrir que un robo ocasione pérdida o deterioro de su información que retrasaría o perjudicaría su trabajo por lo que se debe proteger la información?	1 2 3 4 5
37. ¿Considera que Es importante cambiar las contraseñas de acceso al sistema frecuentemente?	1 2 3 4 5
38. ¿Considera que Es importante NO compartir su computador, contraseñas del sistema con otras personas?	1 2 3 4 5
39. ¿Realiza frecuentemente copias de su información (backup)?	1 2 3 4 5

Infraestructura Tecnológica existente

40. ¿Las computadoras están interconectadas por una red para compartir de información?	1 2 3 4 5
41. ¿Siente que La información se obtiene a tiempo gracias a la infraestructura existente?	1 2 3 4 5
42. ¿Siente que Cuenta con el servicio de internet adecuado?	1 2 3 4 5

Soporte hacia el usuario

43. ¿Siente una atención y asistencia técnica eficiente del área de sistemas cuando Ud. Tiene problemas?	1 2 3 4 5
44. ¿Siente que el área de soporte de sistemas ofrece soluciones en el tiempo adecuado?	1 2 3 4 5
45. ¿Cree que el personal del área de sistemas tiene el suficiente conocimiento y experiencia para ayudarlo cuando tiene problemas con el sistema de información o su computador?	1 2 3 4 5
46. ¿Cree que el personal del área de sistemas tiene el suficiente conocimiento y experiencia para ayudarlo con temas de seguridad de información?	1 2 3 4 5

Experiencia del usuario

47. ¿Considera que Es un experto en computadoras y sistemas?	1 2 3 4 5
48. ¿Siente que En cuanto a los problemas que se presentan con el sistema no requiere asistencia técnica?	1 2 3 4 5
49. ¿Considera que Conoce y utiliza métodos de seguridad de información para protegerse?	1 2 3 4 5
50. ¿Siente que Es natural navegar por internet y sabe cómo protegerse de virus y otros ataques?	1 2 3 4 5
51. ¿Siente que Es natural utilizar correo electrónico, y sabe cómo protegerse de virus y otros ataques?	1 2 3 4 5

Actitud para Implementar Seguridad en el Sistema de Información

52. Implementar seguridad en los Sistemas de Información será útil para mi trabajo	1 2 3 4 5
53. Las ventajas de utilizar seguridad en los Sistemas de Información sobrepasará sus desventajas	1 2 3 4 5
54. A futuro creo que será necesario trabajar en un sistema con Seguridad de Información.	1 2 3 4 5
55. Implementar seguridad en los Sistemas de Información es importante.	1 2 3 4 5

Control conductual percibido (autosuficiencia)

56. Tengo suficientes habilidades para adaptarme a la Implementación de Seguridad de Información	1 2 3 4 5
57. Tengo suficientes conocimientos para adaptarme a la Implementación de Seguridad de Información	1 2 3 4 5
58. Tengo suficientes competencias para adaptarme a la Implementación de Seguridad de Información	1 2 3 4 5

Norma subjetiva (creencias normativas)

59. En general mi institución está preparada para implementar la seguridad en Sistemas de Información.	1 2 3 4 5
60. Mis compañeros de trabajo piensan que se debe implementar la seguridad en Sistemas de Información.	1 2 3 4 5
61. Mi jefe inmediato piensa que se debe implementar la seguridad en Sistemas de Información.	1 2 3 4 5
62. Los gerentes/autoridades piensan que se debe implementar la seguridad en Sistemas de Información.	1 2 3 4 5

Intención para Implementar Seguridad en los Sistemas de Información

63. Tengo la intención de usar la implementación de la Seguridad en Sistemas de información	1 2 3 4 5
64. Tengo la intención de apoyar la implementación de la Seguridad en Sistemas de información	1 2 3 4 5
65. Tengo la intención de asumir la responsabilidades de la implementación de la Seguridad en Sistemas de información en tres meses	1 2 3 4 5
66. Tengo la intención de proteger la información y los recursos tecnológicos de acuerdo al Sistema de Seguridad de Información que se implementará	1 2 3 4 5

Muchas gracias por su cooperación