



ANEXO 1

FORMATO PARA LA PRESENTACIÓN DE PROYECTOS DE INVESTIGACIÓN  
CON EL FINANCIAMIENTO DEL FEDU

1. Título del proyecto

**UN MODELO DE FACTORES QUE INFLUENCIAN LA INTENCIÓN DEL USUARIO PARA LA IMPLEMENTACION DE SEGURIDAD EN SISTEMAS DE INFORMACION**

2. Área de Investigación

Área de investigación	Línea de Investigación	Disciplina OCDE
Ingeniería y Tecnología	Transversal de conocimiento	Industria de la información y Conocimiento

3. Duración del proyecto (meses)

**12**

4. Tipo de proyecto

Individual	<input type="radio"/>
Multidisciplinario	<input checked="" type="radio"/>
Director de tesis pregrado	<input type="radio"/>

4. Datos de los integrantes del proyecto

Apellidos y Nombres	CONDORI ALEJO HENRY IVAN
Escuela Profesional	INGENIERIA DE SISTEMAS
Celular	958315508
Correo Electrónico	<a href="mailto:hcondori@unap.pe">hcondori@unap.pe</a>

Apellidos y Nombres	SOTOMAYOR ALZAMORA GUINA GUADALUPE
Escuela Profesional	INGENIERIA DE SISTEMAS
Celular	953620511
Correo Electrónico	<a href="mailto:guinas@gmail.com">guinas@gmail.com</a>

- I. Título (El proyecto de tesis debe llevar un título que exprese en forma sintética su contenido, haciendo referencia en lo posible, al resultado final que se pretende lograr. Máx. palabras 25)



**UN MODELO DE FACTORES QUE INFLUENCIAN LA INTENCIÓN DEL USUARIO PARA LA IMPLEMENTACION DE SEGURIDAD EN SISTEMAS DE INFORMACION**

- II. Resumen del Proyecto de Tesis (Debe ser suficientemente informativo, presentando -igual que un trabajo científico- una descripción de los principales puntos que se abordarán, objetivos, metodología y resultados que se esperan)**

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.

- III. Palabras claves (Keywords) (Colocadas en orden de importancia. Máx. palabras: cinco)**

Seguridad de Información, implementación de Sistemas de Información, intención del usuario, Teoría del Comportamiento Planificado

- IV. Justificación del proyecto (Describa el problema y su relevancia como objeto de investigación. Es importante una clara definición y delimitación del problema que abordará la investigación, ya que temas cuya definición es difusa o amplísima son difíciles de evaluar y desarrollar)**

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 una 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 sus 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.

- V. Antecedentes del proyecto (Incluya el estado actual del conocimiento en el ámbito nacional e internacional. La revisión bibliográfica debe incluir en lo posible artículos científicos actuales, para evidenciar el conocimiento existente y el aporte de la Tesis propuesta. Esto es importante para el futuro artículo que resultará como producto de este trabajo)

### **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 de la Tecnología está basado en la Teoría de la Acción Razonada<sup>1</sup> (Fishbein & Ajzen, 1975) (Ajzen & Fishbein, 1980). En consonancia con esta teoría, el Modelo de Aceptación de Tecnología 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 de la Tecnología original (TAM, Technology Acceptance Model) se muestran en la Figura 9. 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.

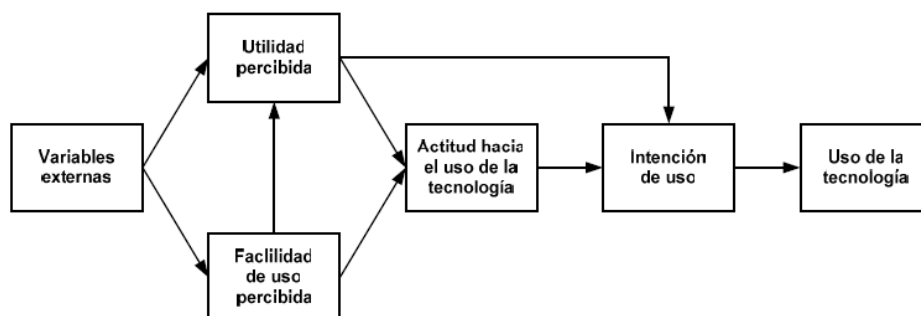
La Utilidad percibida se define como el grado en que una persona piensa que su

---

<sup>1</sup> 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 otras teorías, no se centra en los valores y la personalidad, sino que propone que la conducta de una persona está condicionada por su intención de llevarla a cabo (si desea o no hacerlo). Esta intención es función de dos factores: su actitud (de naturaleza personal) y sus normas subjetivas (de naturaleza social) (Morlán Santa Catalina, 2010).

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 autoeficacia (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 hemos indicado, 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 1 Modelo de Aceptación Tecnológica original (Davis F. , 1989)**

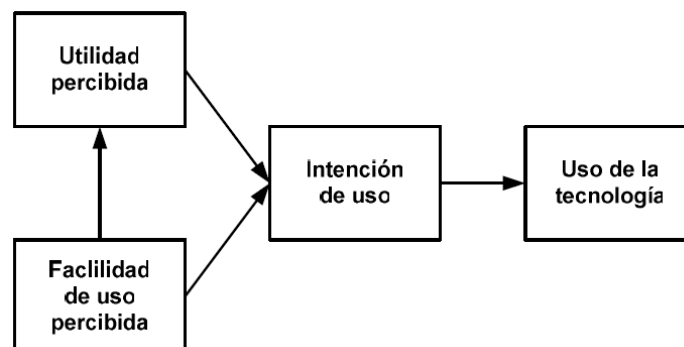
Como se ve en la Figura 9, el Modelo de Aceptación Tecnológica considera que se producen influencias de Variables externas sobre la adopción, como la documentación o el asesoramiento al usuario, y que estas operan a través de la Utilidad percibida y la Facilidad de uso percibida. Por lo tanto, se supone que las creencias de los individuos, al menos en parte, filtran los efectos de las variables organizacionales, sociales e individuales.

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).

### **Primera ampliación del Modelo de Aceptación de la Tecnología (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 (ver Figura 10). 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 2 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

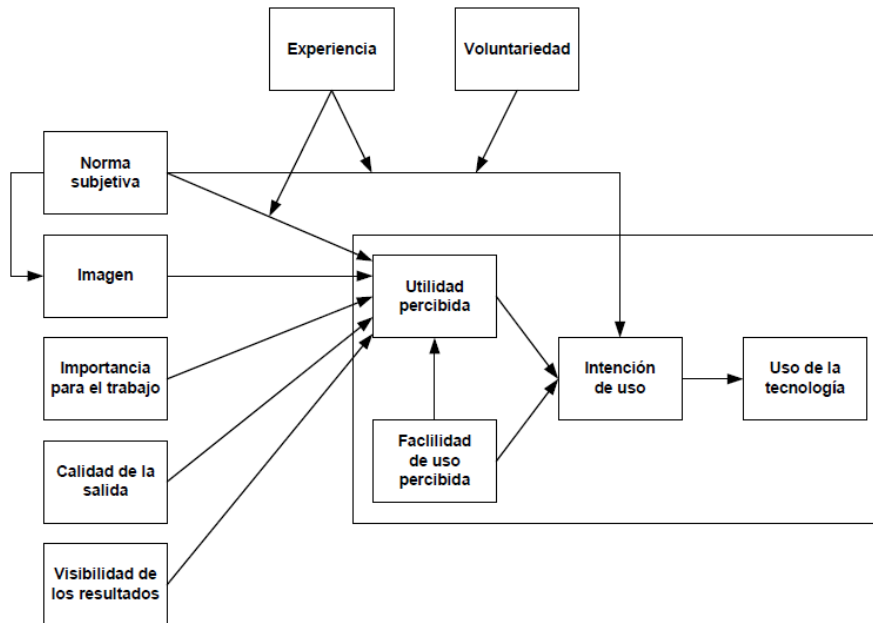


de la Intención de uso en el caso de escenarios obligatorios. La Norma subjetiva, es la medida en que un individuo considera importante que otros piensen que dicho individuo debe utilizar la tecnología en cuestión. Está adaptada a partir de dos teorías, de la Teoría de la Acción Razonada y de la Teoría del Comportamiento Planificado<sup>2</sup> (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 independiente (Venkatesh, Morris, Davis, & Davis, 2003) (Morlán Santa Catalina, 2010).

---

<sup>2</sup> 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).



**Figura 3 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.

**VI. Hipótesis del trabajo (Es el aporte proyectado de la investigación en la solución del problema)**

El modelo determina Los factores críticos que influyen en la intención del usuario para implementar seguridad en sistemas de información

**VII. Objetivo general**

Desarrollar un modelo de Factores críticos que influyen la intención del usuario para la



### VIII. Objetivos específicos

- Revisar los modelos de intención de uso.
- Determinar los factores críticos que influencia en la intencionalidad.
- Establecer el modelo de factores que influyen la intención del usuario para implementar sistemas de seguridad de información.

### IX. Metodología de investigación (Describir el(los) método(s) científico(s) que se empleará(n) para alcanzar los objetivos específicos, en forma coherente a la hipótesis de la investigación. Sustentar, con base bibliográfica, la pertinencia del(los) método(s) en términos de la representatividad de la muestra y de los resultados que se esperan alcanzar. Incluir los análisis estadísticos a utilizar)

Tomando como referencia la situación problemática planteada y la forma como se pretende resolver, el presente proyecto debe ser considerado como un trabajo de "investigación aplicada". Dicha afirmación se sustenta en razón a que, para su desarrollo y contrastación con la realidad, se debe comprobar la validez de la hipótesis de manera experimental para lo cual se empleará todo el cuerpo estructural del método científico. Por otro lado, se hace uso de diversas áreas del conocimiento existentes como los modelos de evaluación de factores, la seguridad en Sistemas de información, estándares de seguridad, modelos de aceptación tecnológica, legislación y gestión gubernamental, en general, todos los tópicos referidos a las tecnologías de la información y gestión de seguridad de información.

Enfoque:

Considerando que el presente estudio hace hincapié en la medición y el análisis de datos con cifras por medio de métodos estadísticos, para medir el efecto del modelo propuesto en el proceso de evaluación, es cuantitativa.

Periodo:

Es longitudinal para el nivel de incertidumbre, en vista que comparará datos obtenidos en dos etapas del proceso de evaluación (pre-test y pos-test).

Alcance:

Los objetivos de del presente estudio es explicativo, dado que están inmersos en la comprobación de hipótesis de relación causal entre variables.

Diseño de Investigación

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.

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 sin realizar algún tipo de manipulación intencional, sino conocer su comportamiento y percepción de forma natural, sin involucrar ningún efecto exterior.

Técnicas de Investigación

Entre las principales técnicas empleadas en el presente trabajo de investigación, se consideró la encuesta.





#### Instrumentos de Recolección de Datos

Para la presente investigación, se ha empleado el cuestionario, que ha sido desarrollado a partir de las variables e indicadores de la operacionalización de variables para el nivel de incertidumbre.

#### 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 least squares) combinada con el bootstrapping con apoyo del software SPSS v 22, AMOS v22.

#### X. Referencias (Listar las citas bibliográficas con el estilo adecuado a su especialidad)

- Ajzen, I. (1991). The theory of planned behavior. *Organizational behavior and human decision processes* (50), 179 -211.
- Ajzen, I., & Fishbein, M. (1980). *Understanding attitudes and predicting social behavior*. Englewood Cliffs. N.J., Inc. U.S.A: Prentice Hall.
- 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.
- 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.
- Bjorck, F. (2002). *Implementing Information Security Management Systems – An Empirical Study of Critical Success Factors*.
- Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). A Model for Evaluating IT Security Investments. *Communications of the ACM* , 47 (7), pp. 87-92.
- 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.
- Delone, W., & Mclean, E. (1992). Information systems success: The quest for the dependent variable. *Information systems research* , 3 (1), 60-95.
- Dunkerley, K. D. (2011). *Developing an Information Systems Security Success Model for Organizational Context*. Phd. Thesis: Nova Southeastern University.
- Dunkerley, K., & Tejay, G. (2009). *Developing an Information Systems Security Success Model for eGovernment Context*. *AMCIS 2009 Proceedings* , 1-6.
- Eberhagen, N., & Naseroladl, M. (1992). *Critical Success Factor. A survey*. University of Vaxjó .
- Erb, M. (s.f.). *Gestión de Riesgo en la Seguridad Informática*. Recuperado el 03 de 03 de 2011, de <http://protejete.wordpress.com/>
- 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](http://www.ey.com/Publication/vwLUAssets/2008_Global_Information_Security_Survey_english/$FILE/2008_GISS_ingles.pdf)



ISO/IEC. (2005). Information technology - Security techniques - Information security management system - Requirements (ISO/IEC27001:2005). USA: ISO/IEC.

ISO/IEC. (2005). ISO/IEC 17799:2000 Information technology - Code of practice for information security 2d Ed. Switzerland: International Organization for Standardization.

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

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>

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.

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.

Siponen, M. T. (2001). A Conceptual Foundation for Organizational Information Security Awareness. Information Management & Computer Security , Vol. 8 (No. 1), pp. 31-41.

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.

Solms, R. v. (1998). Information Security Management (2): guidelines to the management of information technology security (GMITS). information management & Computer Security , 221223.

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 .

Villena Aguilar, J. A. (2006). Sistema de Gestión De Seguridad De Información Para Una Institución Financiera. Perú, Eng Thesis, Pontificia Universidad Católica del Perú.

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.

**XI. Uso de los resultados y contribuciones del proyecto (Señalar el posible uso de los resultados y la contribución de los mismos)**

Permitirá determinar los factores que influyen la intención del usuario en la implementación de seguridad de sistemas de información a través de un modelo multivariado

**XII. Impactos esperados**

**i. Impactos en Ciencia y Tecnología**

Se propone un modelo, que permite determinar los factores de influencia que condicionan la implementación de seguridad en sistemas de información



**ii. Impactos económicos**

El modelo al estimar el nivel de aceptación del usuario, prevee costos innecesarios que podrían incurrirse a raíz de una no adecuada determinación de dichos factores.

**iii. Impactos sociales**

El modelo genera un mejor clima laboral, pues se enfoca en el usuario, pues reduce las brechas de expectativas que se pueda generar.

**iv. Impactos ambientales**

No genera impacto o costo ambiental

**XIII. Recursos necesarios (Infraestructura, equipos y principales tecnologías en uso relacionadas con la temática del proyecto, señale medios y recursos para realizar el proyecto)**

Centro de experimentación, con una entidad que implemente seguridad en sus sistemas de información  
Análisis confirmatorio multivariado.  
Tecnologías de encuestas electrónicas.  
Computadores con capacidad de procesamiento multivariado.

**XIV. Localización del proyecto (indicar donde se llevará a cabo el proyecto)**

Puno

**XV. Cronograma de actividades**

ACTIVIDADES	CALENDARIO 2021											
	1er mes	2do mes	3er mes	4to mes	5to mes	6to mes	7mo mes	8vo mes	9no mes	10mo mes	11vo mes	12vo mes
Selección de antecedentes Documentarios	X	X										
Identificación del Problema y Formulación de los Objetivos			X									
Antecedentes Bibliográficos			X	X	X							
Diseño, Modelo			X	X								
Elaboración de las Técnicas de Recolección de Información			X									
Aplicación y Ejecución				X	X	X	X	X	X	X		
Plan de Análisis e Interpretación de los Datos										X	X	
Desarrollo del Informe											X	X
Presentación												X

**XVI. Presupuesto**

**OBJETIVOS**

ETAPAS DE PROYECTO	DIAS	HORAS	IMPORTE S/
--------------------	------	-------	------------



Análisis Descriptivo	33	100	1000
Diseño	20	160	1200
Implementación	30	300	3000
Pruebas	45	150	900
Verificación	30	150	950
<b>Sub - Total</b>	<b>158</b>	<b>860</b>	<b>7050</b>

**MATERIALES**

DESCRIPCION DE MATEARIALES	Unid	Cantidad	IMPORTE S/
Bibliografía e Información	Unid	2	150
USB	unid	25	17,5
Papel Bond 80 Gr.	millar	10	250
Plumones de Pizarra	unid	5	17,5
Lapiceros	unid	3	4,5
Agenda A4	unid	1	10
Imprevistos	%	10	44,95
<b>Sub - Total</b>			<b>410</b>

**SERVICIOS**

DESCRIPCION DE SERVICIOS	Unid	Cantidad	IMPORTE S/
Internet	horas	480	480
Capacitación	Unid	1	350
Digitación	hojas	500	400
Impresión	hojas	500	600
Empastado y Anillados	Unid	5	300
Imprevistos	%	5	513
<b>Sub - Total</b>			<b>2643</b>

**OTROS**

DESCRIPCION	Unid	Cantidad	IMPORTE S/
Investigación	Unid	1	1300
Viáticos (lugares de investigación)	viajes	2	500
Movilidad (lugares de investigación)	viajes	2	100
Imprevistos	%	5	90
<b>Sub - Total</b>			<b>1990</b>

**RESUMEN**

<b>OBJETIVOS</b>	<b>7050</b>
<b>MATERIALES</b>	<b>410</b>
<b>SERVICIOS</b>	<b>2643</b>
<b>OTROS</b>	<b>1990</b>
<b>TOTAL</b>	<b>12093</b>