UNIVERSIDAD NACIONAL
"PEDRO RUIZ GALLO"
Facultad de Ingeniería Civil, de Sistemas y Arquitectura
Escuela Profesional de Ingeniería de Sistemas

TESIS

LA GESTIÓN DE CONDUCTAS Y COMPORTAMIENTOS EN LOS USUARIOS DE TI Y LA CONCIENTIZACIÓN EN LA SEGURIDAD DE LA INFORMACIÓN EN LA UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO CHICLAYO - LAMBAYEQUE

TESIS

PARA OPTAR POR EL TÍTULO PROFESIONAL DE
INGENIERO DE SISTEMAS

PRESENTADO POR:

ALARCÓN CUBAS, FLOR DE AVELITA

ORJEDA RAMIREZ, JUAN ALBERTO

ASESOR:

M. Sc. Ing. ERNESTO KARLO CELI ARÉVALO

LAMBAYEQUE - PERÚ

2018

UNIVERSIDAD NACIONAL "PEDRO RUIZ GALLO"

Facultad de Ingeniería Civil, de Sistemas Arquitectura

Escuela Profesional de Ingeniería de Sistemas

RESPONSABLES

FLOR DE AVELITA ALARCON CUBAS
RESPONSABLE

JUAN ALBERTO ORJEDA RAMIREZ
RESPONSABLE

HONORABLE JURADO DE SUSTENTACION DE TESIS

Ing. MARÍA DE LOS ANGELES GUZMAN VALLE
PRESIDENTE DE JURADO

Ing. JOSÉ RAMON SANDOVAL JIMENEZ
MIENBRO DE JURADO

Mg.Ing. JESÚS BERNARDO OLAVARRIA PAZ
MIENBRO DE JURADO

Dr.Ing. ERNESTO KARLO CELI AREVALO
PATROCINADOR

ASPECTO INFORMATIVO

1.1. Título del proyecto

La gestión de conductas y comportamientos en los usuarios de TI y la concienciación en la seguridad de la información en la Universidad Nacional Pedro Ruiz Gallo

1.2. Personal investigador

1.2.1. Autores

Flor de Avelita Alarcón Cubas
Bachiller en Ingeniería de Sistemas
Correo: floralarcon@outlook.com

Juan Alberto Orjeda Ramírez
Bachiller en Ingeniería de Sistemas
Correo: jorjeda.ramirez@gmail.com

1.2.2. Asesor

M. Sc. Ing. Ernesto Karlo Celi Arévalo

1.3. Resolución de aprobación

Decreto decanal N° 079-2016 -UNPRG-FICSA

1.4. Escuela Profesional

Ingeniería de Sistemas

1.5. Tipo de investigación

La presente investigación es de tipo relacional.

1.6. Área de investigación

Desarrollo de tecnologías e innovación

1.7. Línea de investigación:

Tecnología de la Información y Comunicación (TIC)

1.8. Localidad e institución donde se realizará el proyecto

Universidad Nacional Pedro Ruiz Gallo Ciudad de Chiclayo – Perú

1.9. Fecha de presentación

Febrero, 2018

DEDICATORIA

La presente investigación está dedicada a Dios, por permitirnos hacer realidad culminar el presente proyecto.

Dedicados a todas las personas que contribuyeron para hacer realidad este sueño.

Dedicado a nuestros padres por todo su apoyo y guía para ser cada día mejores en todos los aspectos de nuestras vidas.

RESUMEN

Actualmente, en el marco de la Seguridad de Información, el factor humano no está tan ampliamente estudiado como otros factores. Por ello la presente investigación se centra en cómo predecir el accionar de los usuarios de TI frente a las Políticas de Seguridad de Información, mediante el estudio de teorías de comportamientos (Teoría del Comportamiento Planificado, Teoría de la Acción Razonada y la Teoría de Disuasión).Del estudio realizado mediante 4 variables integración y compromiso, entrenamiento, Medidas de Disuasión y Motivación, se obtuvo 4 modelos de los cuales se optó por uno de ellos ya que resultado de la prueba de análisis de fiabilidad por Alfa de Cronbach, se obtuvo un 81,4% motivo por el cual afirmamos que el instrumento de recolección es bueno.

ABSTRACT

Currently, in the framework of Information Security, the human factor is not as widely studied as other factors. Therefore, this research focuses on how to predict the actions of IT users against Information Security Policies, through the study of behavioral theories (Theory of Planned Behavior, Theory of Reasoned Action and Theory of Dissuasion) From the study carried out by means of 4 variables, integration and commitment, training, deterrence measures and motivation, 4 models were obtained, of which one of them was chosen as a result of the reliability analysis test by Cronbach's Alpha, a 81.4% reason why we affirm that the collection instrument is good.

INDICE

I. INTRODUCCIÓN

En estos últimos años la información se ha vuelto un activo imprescindible para las empresas lo cual para protegerla se implementan políticas de seguridad de información (PSI).

> Según (Sommestad, Hallberg, Lundholm, & Bengtsson, Las variables que influyen en el cumplimiento de las políticas de seguridad de la Informacion: Una revisión sistemática de los estudios cuantitativos, 2013) el cumplimiento de una adecuada PSI incrementa la seguridad de información de las organizaciones; sin embargo, para el logro de la aplicación de las PSI dentro de una organización, la Alta Dirección necesita orientación de cómo lograr el mejor desempeño del oficial de seguridad y cómo poder desalentar toda acción de mal uso de las políticas de información.

En las organizaciones, los gerentes responsables de la información de seguridad del ordenador establecen políticas de seguridad; sin embargo, si los empleados y los usuarios finales de los sistemas de información organizacionales no entienden la importancia de estas prácticas y no están entusiasmados o dispuestos a seguir las políticas, estos esfuerzos son en vano. Las políticas, especialmente las relacionadas con la seguridad de información, se consideran como meras directrices o instrucciones generales a seguir en lugar de reglas duras y rápidas (Von Solms y Von Solms, 2004).

Las metodologías de gestión de riesgo actuales están básicamente orientadas a evaluar amenazas y encontrar niveles de exposición al riesgo de activos de TI que proceden de infraestructura, computadoras, base de datos; pero aún no se ha dado la importancia debida a quienes generan la mayor cantidad de amenazas, es decir los usuarios de TI.

Las matrices no contemplan los aspectos de evaluación y tratamiento de riesgos relacionados con las fuentes de amenazas de los empleados de manera intencional y no intencional, las cuales se pueden controlar con estrategias y una adecuada gestión de la seguridad de la información.

Existen numerosos estudios en donde se analizan la influencia del componente físico y material sobre el cumplimiento de las PSI; el presente estudio se enfoca

en investigar el componente humano, básicamente el comportamiento y cómo éste afecta al cumplimiento de las políticas de seguridad.

El error humano es un gran factor de riesgo casi incontrolable e impredecible, pero existen teorías que nos ayudan a predecir dicho factor, tales como la Teoría de Disuasión, Teoría del Comportamiento Planificado (TPB) y la Teoría de la Acción Razonada (TRA). Estas teorías están relacionadas con la sociología, antropología, psicología, pero aún no se ha encontrado dichas teorías en el campo de la gestión de las tecnologías de la información, aspecto que motiva la presente investigación.

La TRA Y TPB proporcionan la base y el fundamento para la evaluación de la relación que existe entre la actitud, la intención y el comportamiento del usuario de TI.

El factor humano influye directamente en el cumplimiento de las (PSI) puesto que si un empleado no es consciente de las PSI no podrá aplicarlas y en consecuencia pondría en peligro el legado más valioso de la empresa (información).

Según el estudio realizado por (Herath & Rao, 2009), se demuestra que “La negligencia de los empleados ha llevado a las infracciones que cuesta a las organizaciones millones de dólares en pérdidas’’.

En una línea empírica, D’Arcy y Hovav (2004) siguieron la Teoría de la Disuasión y desarrollaron un modelo teórico que examina el efecto de las contramedidas de seguridad de disuasión sobre la certeza de la percepción y la severidad de las sanciones, que a su vez, conduce a intenciones de mal uso de los SI, mientras que Straub (1990) encuentra que las medidas de disuasión reducen el abuso informático en las organizaciones.

La aplicación de sanciones frente a actos intencionados hace que los usuarios se limiten a realizar infracciones de las políticas de seguridad de la información, no se controlara en su totalidad pero habrá un mayor control de los riesgos a los que se enfrenta la información.

Ahora la pregunta es qué tanto y de qué manera afecta la concienciación de los usuarios al cumplimiento de las políticas de seguridad.

II. PLANTEAMIENTO DEL PROBLEMA

2.1. Descripción del problema

Hoy en día las tecnologías de información dan soporte a los procesos administrativos y académicos de las universidades, sin embargo la incorporación de las TI en las universidades tanto públicas como privadas traen consigo nuevos riesgos, los cuales para que puedan ser gestionados y evaluados requieren de técnicas y metodologías.

La mayoría de las técnicas y metodologías, son enfoques orientados a gestionar y mitigar los riesgos de los activos de TI (servidores, infraestructura de TI, base de datos); sin embargo los escenarios de riesgo ocasionados por las personas/usuarios son amenazas internas que no se pueden gestionar ni mitigar en su totalidad.

Los usuarios representan una gran amenaza en las organizaciones debido a que el daño que pueden ocasionar, por acciones voluntarias o involuntarias, pone en riesgo la seguridad de la información; y al ser provocados por el comportamiento del ser humano son las amenazas que menos se pueden controlar y las que más se dan dentro de una organización.

> Según Russel (2013), existen tres tipos de amenazas internas: usuarios internos malintencionados que roban información o causan daños deliberadamente; usuarios internos que, sin darse cuenta, son explotados por partes externas, y usuarios internos que son descuidados y cometen errores no intencionados.

Según el autor considera que el riesgo más peligroso para una organización son los usuarios con privilegios para acceder a la información, es el caso de un usuario administrador que puede realizar prácticamente cualquier operación en sistemas y también se da el caso en que muchas veces los usuarios suelen tener más derechos de los que necesitan para su función laboral actual.

Por ello, la investigación se basa en la necesidad de implementar técnicas para poder evaluar el comportamiento de los usuarios de TI dentro de la Universidad Nacional Pedro Ruiz Gallo, mediante el estudio de teorías del comportamiento de los miembros (usuarios de TI) que tienen acceso a aplicativos tecnológicos que

contribuyen a una mejor organización y automatización de muchos de los servicios que ofrece la universidad.

2.1.1. Análisis de la percepción de los usuarios de TI en la Universidad Nacional Pedro Ruiz Gallo.

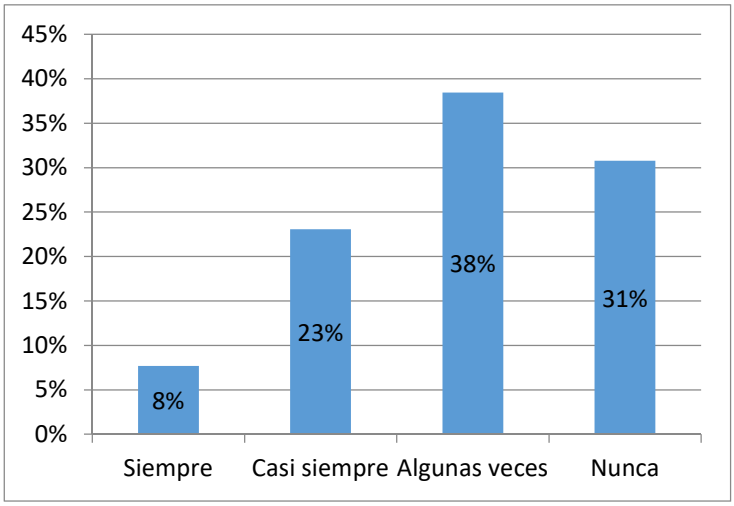
El presente análisis se realizará de la encuesta etnográfica realizada a los usuarios de TI en la Universidad Nacional Pedro Ruiz Gallo.

Descripción de los gráficos asociados a la encuesta etnográfica, la cual se muestra en el anexo N° 1

Pregunta Nº 01

En caso que ocurra alguna incidencia, ¿sabe cómo actuar según las políticas de seguridad de la información de la institución donde labora?

Figura N°1: Gráfica conocimiento de usuario frente a incidencias



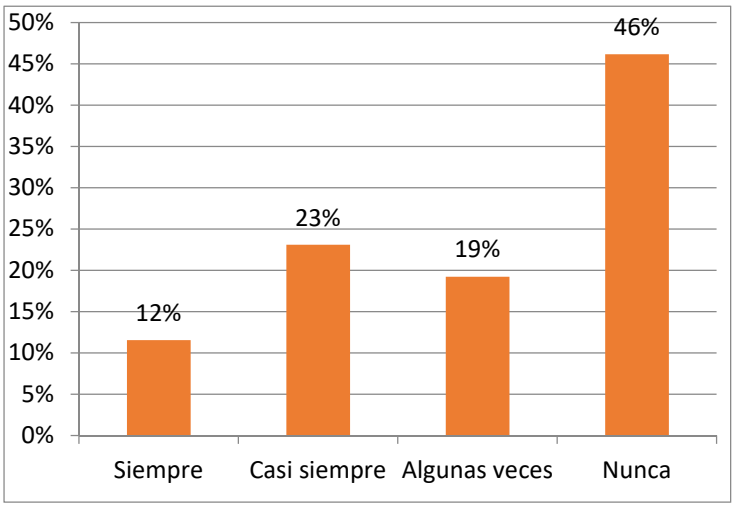
Fuente: Elaboración propia

Interpretación: En la gráfica se observa que el 38% de encuestados indican que “Algunas Veces” saben cómo actuar de acuerdo a las políticas de seguridad de la información de la UNPRG y solo el 8% siempre sabe cómo actuar, lo cual es una cantidad mínima de conocimiento.

Pregunta Nº 02

En el caso de un incidente, ¿usted realiza el registro respectivo?

Figura N°2: Gráfica Registro de incidencia de los usuarios de TI



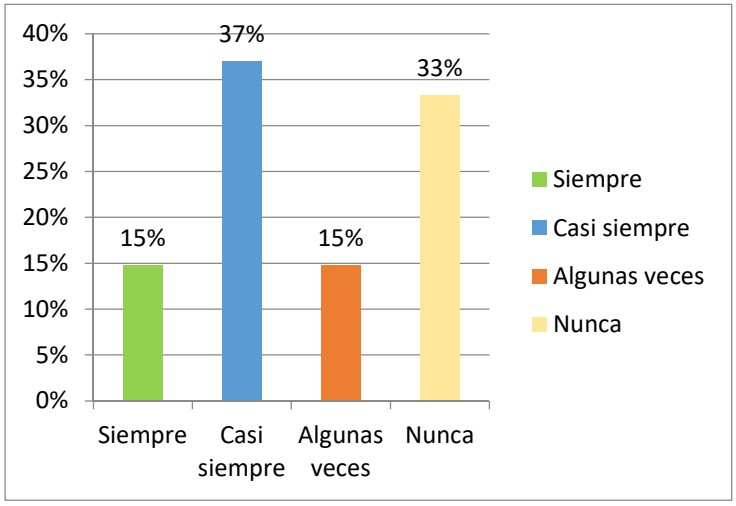
Fuente: Elaboración Propia

Interpretación: En la gráfica se observa que el 46% de encuestados nunca registra los casos que atentan a la seguridad de la información en la UNPRG, lo cual implica que la institución no está preparada para enfrentar futuros riesgos; y solo el 12% siempre realiza el registro respectivo de la incidencias.

Pregunta Nº 03

Si le derivaran la tarea de registrar un incidente, ¿conoce el procedimiento a realizar?

Figura N°3: Gráfica conocimiento de procedimiento del registro de incidencias de los usuarios de TI



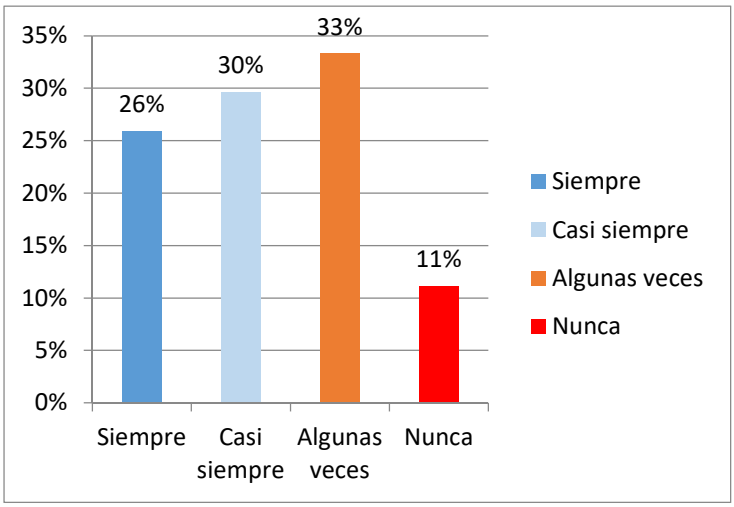
Fuente: Elaboración Propia

Interpretación: Se observa que el más alto porcentaje (37%) casi siempre conoce el procedimiento para realizar el registro de incidencias y un 15% siempre conoce el procedimiento para realizar el registro de las incidencias.

Pregunta Nº 04

Si algún compañero que no pertenece a su área o departamento donde labora usted, le pidiera información, ¿le brindaría dicha información?

Figura N°4: Gráfica para verificar seguridad de la información



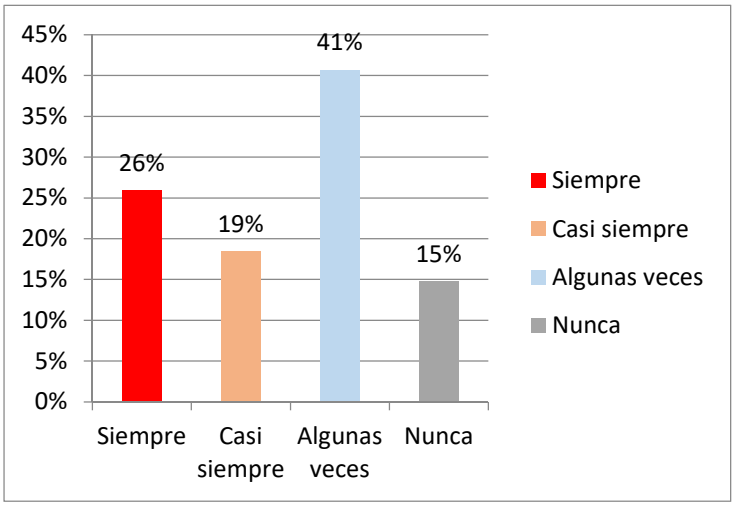
Fuente: Elaboración Propia

Interpretación: Se observa que un 33% de encuestados algunas veces sí brindarían información a compañeros de otras aéreas y únicamente el 11% nunca brinda información, lo cual corrobora falta de compromiso institucional por parte de la persona responsable del área.

Pregunta Nº 05

¿En alguna ocasión ha tenido que brindar información a personas que no pertenece a su área por orden de su jefe?

Figura N°5: Gráfica para verificar seguridad de la información



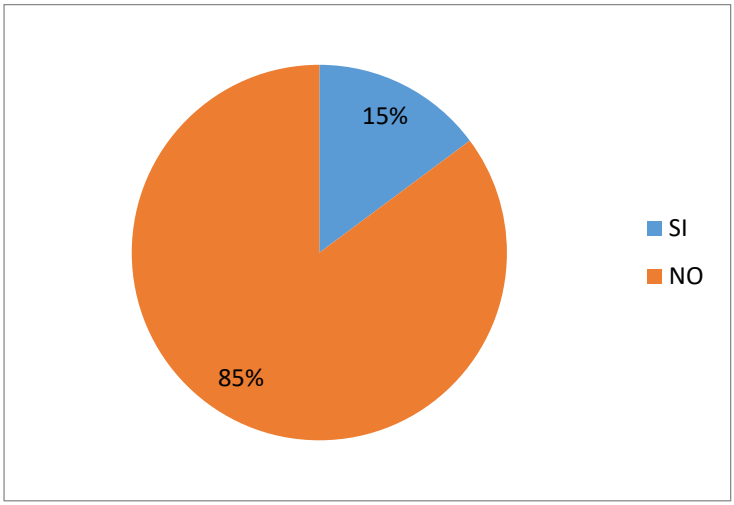
Fuente: Elaboración Propia

Interpretación: En la gráfica se observa que un 41% de encuestados algunas veces han tenido que brindar información a personas de otras áreas por órdenes de su jefe y un 15% nunca brinda dicha información.

Pregunta Nº 06

¿Siente que la capacitación que ha recibido en relación a las políticas de seguridad de la información en los últimos 6 meses le ayuda para resolver cualquier problema o incidente que se presente en su área o departamento?

Figura N°6: Gráfica para medir el grado de aplicación de la capacitación en políticas de seguridad de la información.



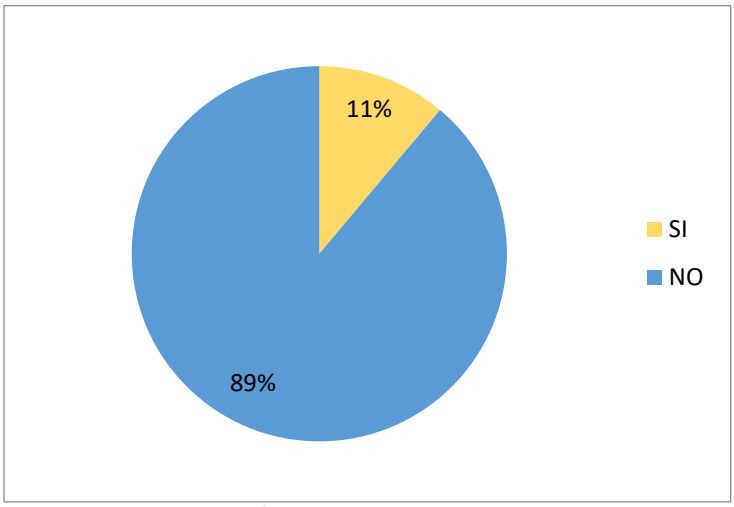
Fuente: Elaboración Propia

Interpretación: La gráfica presenta un alto porcentaje (85%) siente que la capacitación recibida no le ayuda a solucionar los problemas relacionados a la seguridad de la información y solo el 15% considera que la capacitación sí le permite solucionar los problemas.

Pregunta Nº 07

¿En alguna ocasión usted ha recibido algún reconocimiento por haber alertado y registrado algún problema relacionado con las políticas de seguridad de la información?

Figura N°7: Gráfica para medir el grado de reconocimiento por aplicar las políticas de seguridad de la información.



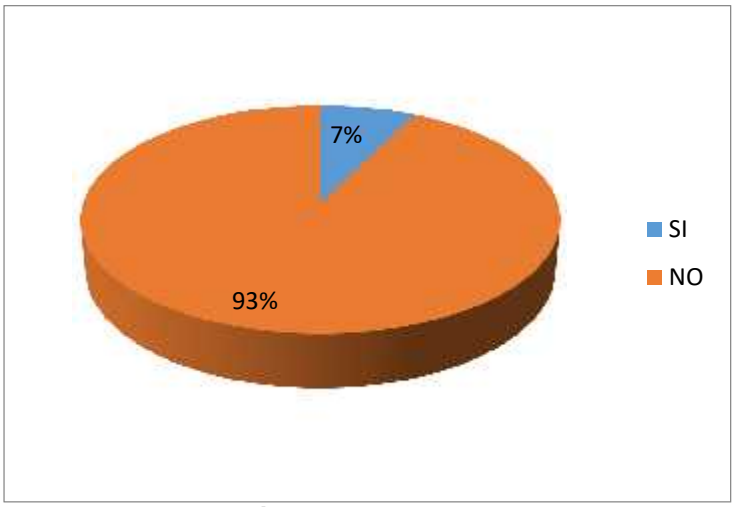
Fuente: Elaboración Propia

Interpretación: La gráfica demuestra que un 89% de los encuestados no ha recibido reconocimiento cuando ha alertado y/o registrado algún problema de seguridad de la información; observándose que solo el 11% sí ha recibido reconocimiento.

Pregunta Nº 08

¿Siente que el compromiso que tiene usted y sus compañeros con el cumplimiento de las políticas de seguridad de la información es reconocido por sus superiores?

Figura N°8: Gráfica para medir el grado de reconocimiento por el compromiso respeto a las políticas de seguridad de la información



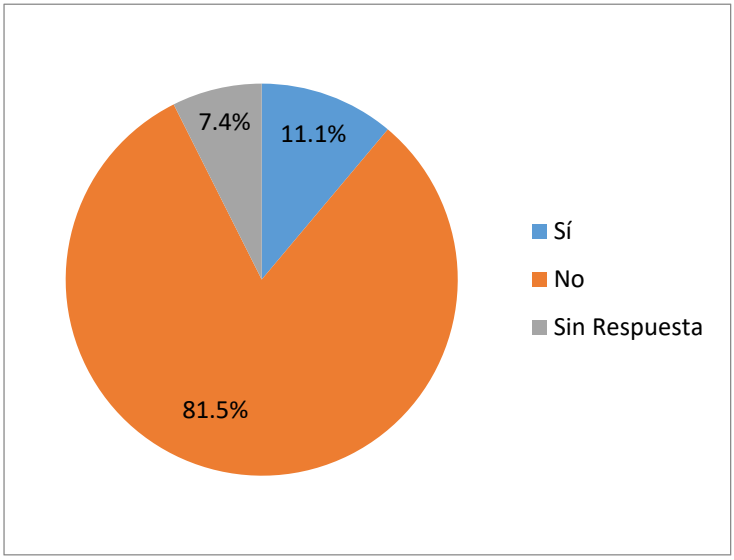
Fuente: Elaboración Propia

Interpretación: El 93% de los encuestados manifiestan que el compromiso que demuestran con la seguridad de la información no es reconocido por sus superiores. El 7% sí considera que su compromiso es reconocido.

Pregunta Nº 09

¿En los últimos 6 meses ha recibido algún reconocimiento por el buen desempeño de sus labores en relación al cumplimiento de las políticas de seguridad? Si es así, ¿qué tan satisfecho está con el reconocimiento?

Figura N°9: Gráfica para medir el grado de reconocimiento por el compromiso respeto a las políticas de seguridad de la información en los últimos 6 meses



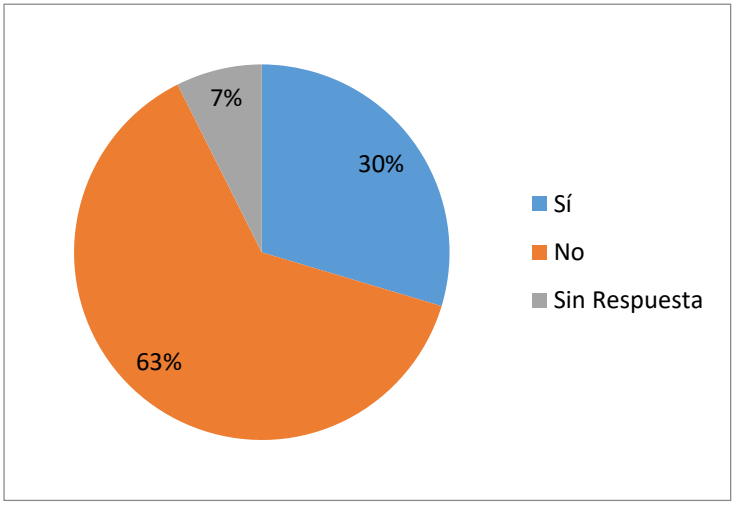
Fuente: Elaboración Propia

Interpretación: En los últimos 6 meses, el 11.1% de los encuestados ha recibido reconocimiento por el buen desempeño de sus labores en relación al cumplimiento de las políticas de seguridad; y el 81.5% no ha recibido reconocimiento.

Pregunta Nº 10

¿Usted está satisfecho con el nivel de preparación y capacitación que le brindan sobre políticas de seguridad de la información en el departamento en el que labora?

Figura Nº 10: Gráfica para medir el grado de satisfacción con el nivel de preparación y capacitación respeto a las políticas de seguridad de la información.



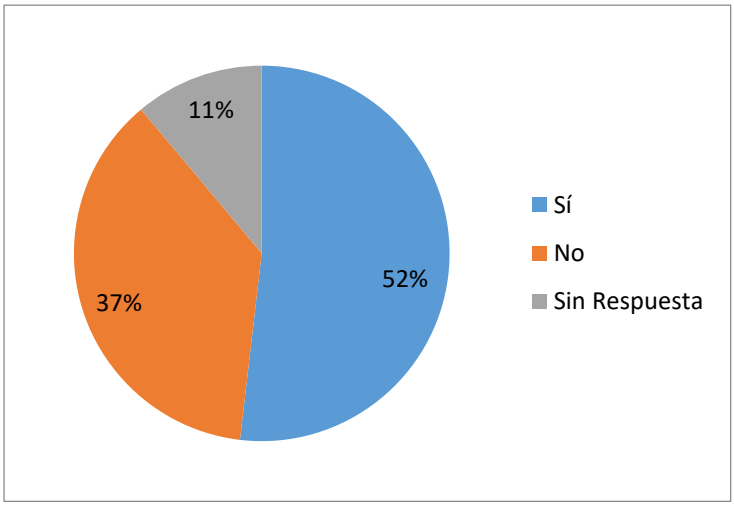
Fuente: Elaboración Propia

Interpretación: El gráfico demuestra un alto porcentaje (63%) de insatisfacción respecto al nivel de preparación y capacitación en políticas de seguridad de la información, en relación al 30% de grado de satisfacción.

Pregunta Nº 11

¿Si usted notará que su compañero está infringiendo las políticas de seguridad de la información, reportaría el suceso a su superior?

Figura Nº 11: Gráfica para medir el grado de identificación institucional



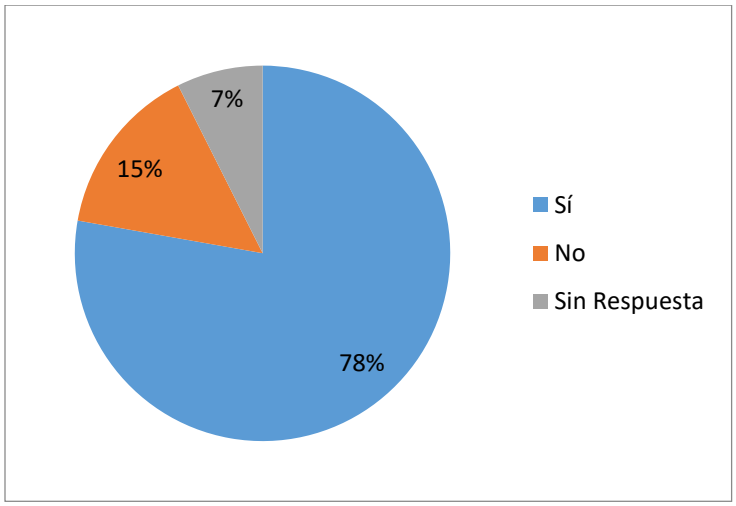
Fuente: Elaboración Propia

Interpretación: El 52% de los encuestados demuestra identificación institucional reportando las infracciones de políticas de seguridad de la información, el 37% denota indiferencia y el 11% no responde.

Pregunta Nº 12

¿Si alguno de sus compañeros le pidiera ayuda para registrar algún incidente usted le brindaría su ayuda?

Figura Nº 12: Gráfica para medir el grado intercambio de conocimiento sobre políticas de seguridad de la información.



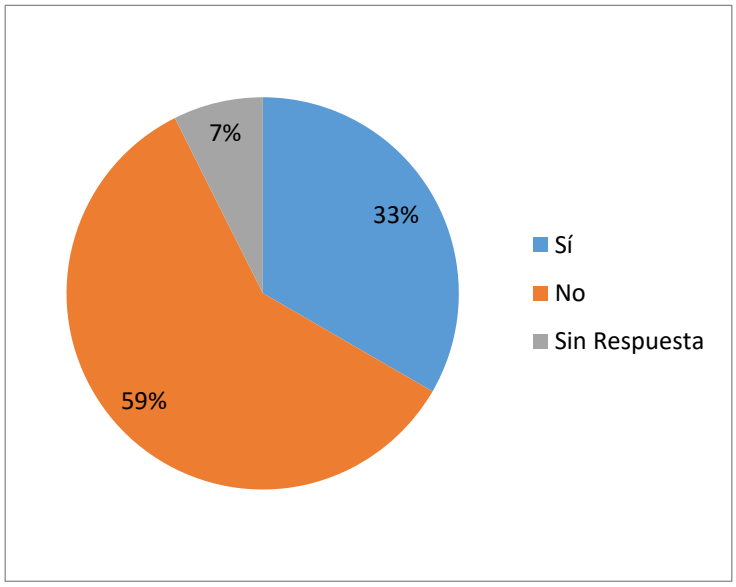
Fuente: Elaboración Propia

Interpretación: El 78% de encuestados comparte conocimientos sobre seguridad de la información con sus compañeros, el 15% no comparte los conocimientos y el 7% no respondió.

Pregunta Nº 13

¿Si se requiere algún tipo de información de la institución, y usted no es la persona encargada de acceder a dicha información le pediría de favor a un compañero de trabajo para que le permita acceder a esos datos?

Figura Nº 13: Gráfica para medir el grado de infracción de las medidas de seguridad de la información.



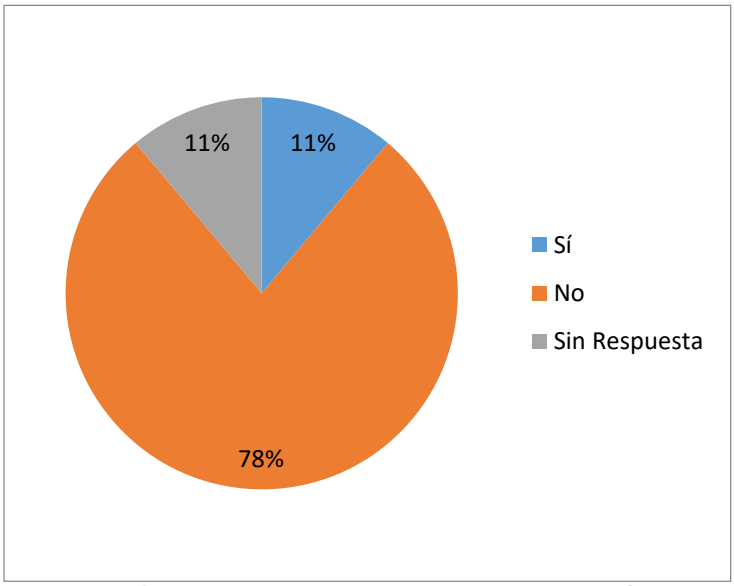
Fuente: Elaboración Propia

Interpretación: El 59% de los encuestados no infringen las medidas de protección de la información, para acceder a información que no le compete, el 33% sí busca acceder a la información no permitida y el 7% no responde.

Pregunta Nº 14

¿Para usted es tedioso que las unidades de seguridad estén capacitando o implementando nuevos controles permanentemente para velar por la seguridad de la información?

Figura Nº 14: Gráfica para medir el grado de aceptación al cambio sobre políticas de seguridad de la información.



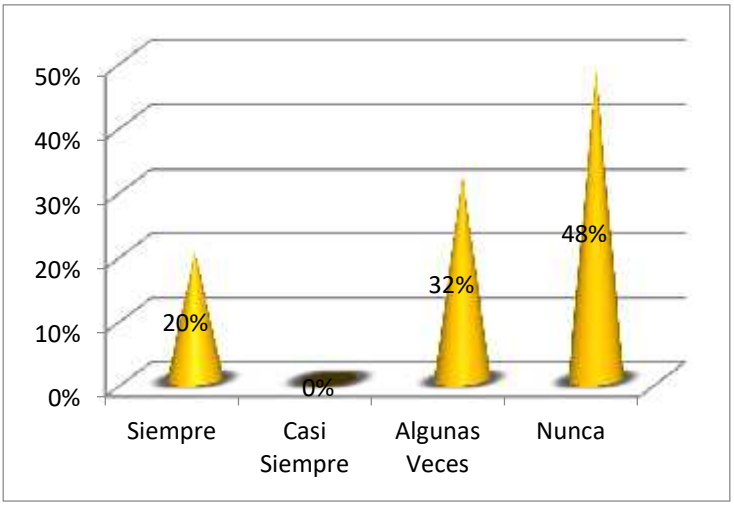
Fuente: Elaboración Propia

Interpretación: El más alto porcentaje (78%) acepta los cambios en la implementación de nuevos controles respecto a las políticas de seguridad de la información, mientras que el 11% se muestra reacio al cambio y otro 11% no respondió.

Pregunta Nº 15

¿Su supervisor o alguien en el trabajo verifican el cumplimiento de los controles de seguridad de la información relacionados a su puesto de trabajo?

Figura Nº 15: Gráfica para medir el grado de verificación del cumplimiento de los controles de seguridad de la información.



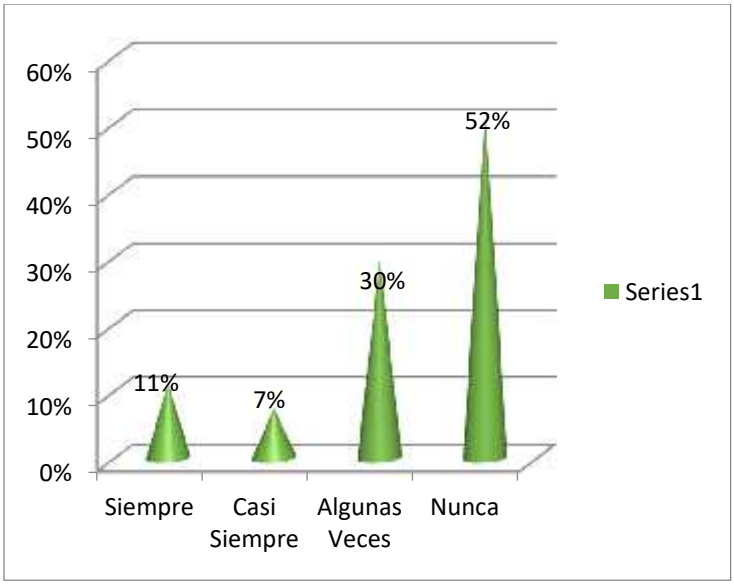
Fuente: Elaboración Propia

Interpretación: Se observa que el más alto porcentaje (48%) manifiesta que nunca se verifica el cumplimiento de los controles de las políticas de seguridad de la información; y el 20% señala que siempre se verifica.

Pregunta Nº 16

¿En la institución donde labora se establecen las medidas necesarias para analizar, evaluar y gestionar el riesgo de que se ocasionen al incumplir las políticas de seguridad en el desarrollo de sus actividades?

Figura Nº 16: Gráfica para medir el grado de uso de medidas necesarias para solucionar problemas de riesgo



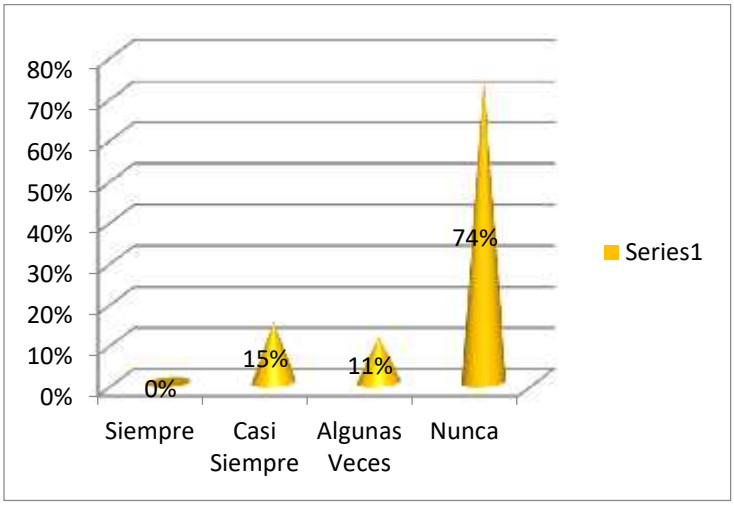
Fuente: Elaboración Propia

Interpretación: El 7% señala que casi siempre se aplica medidas de seguridad, mientras que el más alto porcentaje (52%) manifiesta que nunca se utilizan medias de seguridad para mitigar los riesgos.

Pregunta Nº 17

¿A usted le consideran parte del grupo de personas que evalúan y realizan registro anual de los incidentes que ocurren en el departamento o área en actividades relacionadas con el cumplimiento de las políticas de seguridad de la información?

Figura Nº 17: Gráfica para medir el grado de participación miembro del equipo evaluador de las políticas de seguridad de la información.



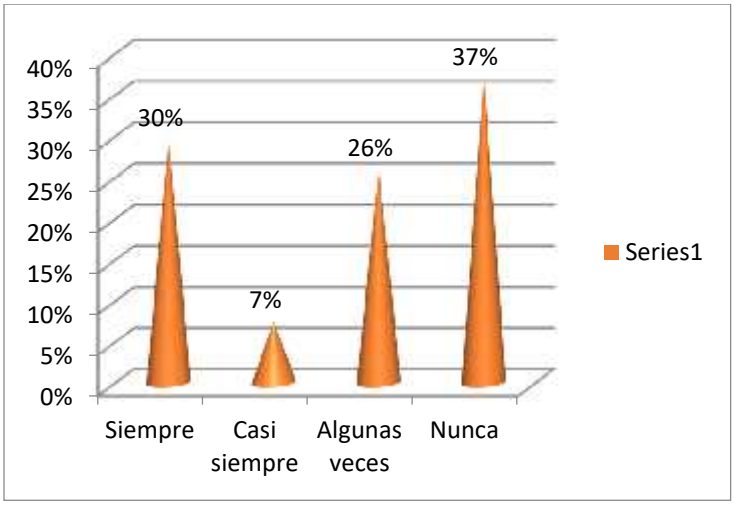
Fuente: Elaboración Propia

Interpretación: El 74% de los encuestados nunca son considerados como integrantes del equipo evaluador, el 15% es convocado casi siempre y el 11% algunas veces.

Pregunta Nº 18

¿Usted tiene la posibilidad de plantear mejoras en relación al cumplimiento de las políticas de seguridad de la información?

Figura Nº 18: Gráfica para medir el grado de posibilidad de plantear mejoras sobre políticas de seguridad de la información.



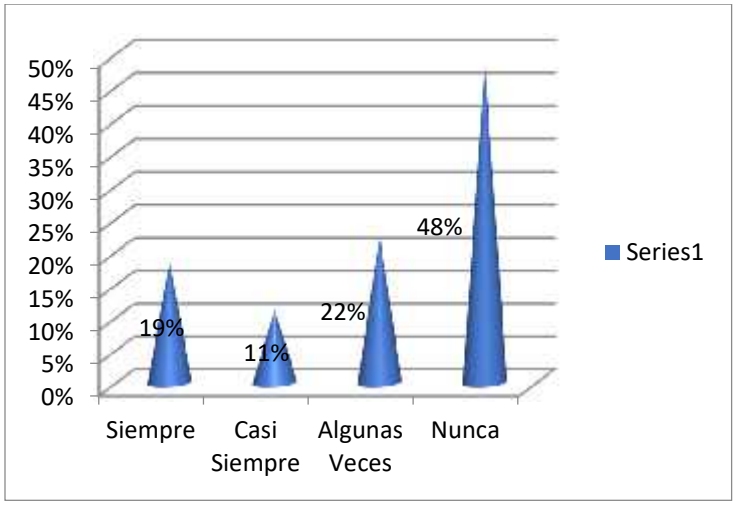
Fuente: Elaboración Propia

Interpretación: El mínimo Porcentaje (7%) casi siempre tiene la posibilidad de plantear mejoras y la mayoría que corresponde al 37%, nunca tienen la posibilidad de plantear mejoras respecto al cumplimiento de las políticas de seguridad.

Pregunta Nº 19

¿En alguna ocasión usted ha hecho uso del registro de incidentes para dar solución a algún problema reiterativo en relación a las políticas de seguridad de la información?

Figura Nº 19: Gráfica para medir el uso de registro de incidentes



Fuente: Elaboración Propia

Interpretación: El 48% de los usuarios nunca ha utilizado el registro de incidentes para solucionar problemas de reincidencia respecto a la seguridad de la información; el 22%, ha utilizado algunas veces; el 19% lo ha hecho siempre; y, el 11% casi siempre utiliza el registro de incidentes.

2.2. Formulación del Problema:

¿Cuál es el impacto que tiene la gestión de los comportamientos de los usuarios de TI en la concientización para el cumplimiento de las políticas de seguridad de la información en la Universidad Nacional Pedro Ruiz Gallo?

2.3. Descripción y delimitación del proyecto

La propuesta planteada en el presente estudio tiene las siguientes características y limitaciones:

A. Nuestra investigación se realizará en la Universidad Nacional Pedro Ruiz Gallo, por tal motivo solo se limitará a aquellas personas que conforman los usuarios de TI que puedan responder a las encuestas planteadas en un inicio para el análisis del problema y finalmente para la demostración de la hipótesis.

B. El presente estudio está basado en teorías como la Teoría del Comportamiento Planificado, la Teoría de Disuasión, la Teoría de la Acción Razonada. Se delimita a hacer un análisis de factores que están directamente relacionados entre el usuario de TI y su entorno Social. Se descarta todo tipo de análisis que tenga relación con la genética, biología.

2.4. Objetivos de la investigación

2.4.1. Objetivo general

Desarrollar un sistema de gestión de los comportamientos de los usuarios de TI que permita mejorar la concientización en el cumplimiento de las políticas de seguridad de la información en la Universidad Nacional Pedro Ruiz Gallo.

2.4.2. Objetivos específicos

- Determinar los factores que están relacionados con la concienciación de los usuarios en relación al cumplimiento de las políticas y controles de seguridad de la información en la Universidad nacional Pedro Ruiz Gallo.

- Desarrollar un modelo conceptual que identifica la relación causal entre los factores que influyen en la concientización para el cumplimiento de las políticas y controles de seguridad de la información en la Universidad Nacional Pedro Ruiz Gallo.

- Diseñar un conjunto de lineamientos para la gestión de conducta y comportamiento de los usuarios de TI en materia de seguridad de la información en la Universidad Nacional Pedro Ruiz Gallo.

- Evaluar el sistema de gestión de conductas y comportamientos de los usuarios como estrategia de mejora de la concienciación en seguridad de la información en la Universidad Nacional Pedro Ruiz Gallo.

2.5. Justificación de la investigación

La presente tesis se justifica:

2.5.1. En lo social

En lo **social** ya que con la investigación permitirá desarrollar un conjunto de controles que ayuden a los responsables de la seguridad de la información en las organizaciones, gestionar y lograr comportamientos de los usuarios de TI como estrategia de mitigación de riesgos.

2.5.2. En lo científico

En lo **científico** el aporte tiene dos perspectivas:

A. Aporte teórico

El **aporte teórico** consiste en el desarrollo de un modelo conceptual que permita explicar los comportamientos de los usuarios de TI en relación al cumplimiento de las PSI. Además que se desarrollará un nuevo fundamento teórico para explicar el funcionamiento de un sistema de gestión de comportamientos de este tipo de usuarios en base a las tres teorías: TRA, TPB y la TD; por lo tanto el resultado es una nueva teoría contextualizada a la realidad de la entidad tomada como estudio.

B. Aporte práctico

El **aporte práctico** de la investigación es un conjunto de lineamientos que lleven a la práctica la ejecución y operatividad del sistema de gestión de comportamientos propuesto, incluyendo: políticas, programas de entrenamiento, controles, etc.

2.5.3. La relevancia social

La **relevancia social** de la investigación estará en dar una visión mejorada de los estándares actuales de seguridad de la información,

estableciendo controles apropiados respecto al factor humano. Y esto a su vez, hará que las políticas de las organizaciones no sólo se enfoque en el aspecto físico sino también en el recurso humano donde se encuentra el mayor riesgo.

2.5.4. En lo económico

En lo **económico** porque los aportes permitirán diseñar y agregar nuevas estrategias y lineamientos, como políticas, programas, procedimientos y controles, que reduzcan las incidencias negativas de seguridad de la información proveniente de errores o acciones intencionales de parte de los usuarios de TI, por lo tanto, permitirá reducir costos relacionados con la prevención y recuperación de los sistemas, debido a las caídas provenientes de este tipo de amenazas.

III. MARCO TEÓRICO Y REVISIÓN LITERARIA

3.1. Antecedente de la investigación

(Herath & Rao, 2009) En su investigación titulada “MOTIVACIÓN PROTECCIÓN Y DISUASIÓN: UN MARCO PARA EL CUMPLIMIENTO DE LA POLÍTICA DE SEGURIDAD EN LAS ORGANIZACIONES” cuyo objetivo fue proponer y evaluar un modelo empírico para entender el efecto de varios factores sobre intenciones de los empleados para cumplir con las políticas de seguridad de la información de una organización. Se realizó una encuesta en la cual se pidió participara varias organizaciones vía internet de los cuales participaron 10 empleados de cada organización, también se estableció contacto con los administradores de690 organizaciones aproximadamente, de las cuales 120 manifestaron su interés en participar. Se obtuvo 312 respuestas, las cuales fueron de los empleados de 78 organizaciones. Los resultados encontrados sugieren que, si los empleados creen que el cumplimiento con las políticas es un obstáculo para su actividad de trabajo del día a día, son menos propensos a tener una opinión favorable hacia la seguridad políticas. Sin embargo, la eficacia percibida de acciones de los empleados se ha encontrado a desempeñar un papel en los comportamientos relacionados con la información de cumplimiento de políticas de seguridad.

(Herath & Rao, 2009) en su investigación titulada “CONCIENCIACIÓN DE LOS USUARIOS EN CONTRAMEDIDAS DE SEGURIDAD Y SU IMPACTO EN EL MAL USO DE LOS SISTEMAS DE INFORMACIÓN: UN ENFOQUE DEDISUASIÓN” cuyo objetivo fue implementar ciertos controles basado en el modelo extendido de la Teoría de Disuasión (TD) que combina el trabajo de la criminología, la psicología social, y la información sistemas. El modelo extendido de la TD se probó por medio de la aplicación de una encuesta a 269 usuarios de computadoras de 8 empresas diferentes. Este modelos disuade a tres prácticas de utilización abusiva: sensibilización de los usuarios de las políticas de seguridad; la educación de seguridad, capacitación y sensibilización programas SETA (Security Education, Training, and Awareness Program); y la supervisión de la computadora,

asimismo sugieren que la percepción de la gravedad de las sanciones, es más eficaz en la reducción de utilización abusiva de las sanciones de la seguridad. Además, hay evidencia de que el impacto de percepción de la sanción varía en función de un nivel de moralidad. Se concluye que se hace un progreso significativo hacia la explicación las relaciones entre las contramedidas de seguridad, sancionar las percepciones, y constituye un uso incorrecto, también se sugiere que la sensibilización de los usuarios de las políticas de seguridad, programas SETA y equipo de monitoreo cada uno tienen algún efecto disuasorio sobre la intención mal uso, y este efecto se logra indirectamente a través de la seguridad percibida y / o severidad de las sanciones. Desde una perspectiva teórica, la investigación presenta una versión extendida de TD y confirma su aplicabilidad a la SI dominio de seguridad.

Teodor Sommestad, JonasHallberg, KristofferLundholm y Johan Bengtsson (2013) en su investigación titulada “LAS VARIABLES QUE INFLUYEN EN EL CUMPLIMIENTO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN: UNA REVISIÓN SISTEMÁTICA DE LOS ESTUDIOS CUANTITATIVOS” cuyo objetivo fue identificar las variables que influyen en el cumplimiento de políticas de seguridad de la información de las organizaciones e identificar la importancia. Se identificaron un total de 60 construcciones psicológicas diferentes de estas variable las cuales están en proceso de revisión, las construcciones provienen de una serie de teorías establecidas como: la Teoría de la Disuasión General (Straub y Welke, 1998), la Teoría de la Protección de la Motivación, la Teoría de la Acción Razonada (Ajzen y Fishbein, 1979), Teoría de la Conducta Planificada (Ajzen, 1991), la Teoría de la Neutralización (Siponen y Vance, 2010), la Teoría de Control Social (Nye, 1958; Wiatrowski, 1981) y (1973) la Teoría de la toma de Decisiones morales de Kohlberg. Se tienen como resultado que en los 29 estudios, más de 60 variables han sido estudiadas en relación con la política de seguridad el cumplimiento y el incumplimiento. Desafortunadamente, no hay ganadores claros se pueden encontrar entre las variables o las teorías que se han extraído de, cada una de las variables sólo explica una pequeña parte de la variación en comportamiento de la

gente y cuando una variable se ha investigado en varios estudios de los resultados a menudo mostrar una variación considerable.

(D'Arcy & Tejaswini, 2011), en su investigación titulada "UNA REVISIÓN Y ANÁLISIS DE LA TEORÍA DE DISUASIÓN EN LA LITERATURA DE SEGURIDAD DE SI: DANDO SENTIDO A RESULTADOS DISPARES" cuyo objetivo fue identificar un conjunto de variables claves de contingencia para la prevención en el contexto de la seguridad de los sistemas de Información. Las variables estuvieron divididas en dos factores: factores individuales y factores contextuales. Se concluye que desde hace muchas décadas atrás se aplica la TD en la seguridad para evaluar la eficacia de las medidas disuasorias para reducir los casos de abuso informático, desde entonces la Teoría de la Disuasión (TD) ha informado un cuerpo considerable de investigación sobre seguridad, sin embargo a pesar de la gran consistencia y comprensión teórica y conocimientos prácticos para el campo de la SI, también ha estado plagada de hallazgos inconsistentes y, a veces contradictorias.

(Quackenbush, 2010) En su investigación titulada "TEORÍA DE LA DISUASIÓN: ¿DÓNDE ESTAMOS?" cuyo objetivo fue evaluar dónde se encuentra hoy en día la TD a través de: una consideración de las distinciones entre diferentes corrientes de la teoría, una discusión de la suposición de la racionalidad en la teoría de la disuasión, un examen de tres distinciones importantes en la disuasión, una evaluación de la difícil tarea de pruebas de la TD, y una descripción general de los desarrollos teóricos recientes. La conclusión principal fue que la TD proporciona una alternativa compatible de manera lógica compatible con la teoría de la disuasión clásica y por lo tanto proporciona la mayor base apropiada para un mayor desarrollo teórico, las pruebas empíricas, y la aplicación de la política.

3.2. Fundamento teórico

En la actualidad muchas investigaciones referentes al estudio de la seguridad de la información relacionados con el comportamiento, actitudes, intenciones y motivación del personal en una organización se han basado en

teorías como: Teoría de la Acción Razonada (TAR), Teoría del Comportamiento Planificado (TPB), Teoría de la Disuasión (TD), para poder predecir la considerable variación que existe de entre el comportamiento real y las intenciones a partir de las actitudes hacia el comportamiento. Estas teorías no sólo son aplicadas en el ámbito social, psicológico, sino que tiene una gran importancia en el al ámbito de la seguridad de la información. Es muy complicado poder predecir el comportamiento del ser humano ya que todos los individuos no reaccionan de la misma es allí donde entran a tallar las teorías dando una mayor precisión, guiando qué factores, variables y marcos metodológicos se pueden seguir. Asimismo podemos rescatar que a veces no solo basta tener una teoría que nos indique cómo disuadir a los actos ilícitos, que castigos recibir los individuos para dejar de cometer dichas acciones sino también verlo desde otra perspectiva que los seres humanos son capaces de aprender y poder cumplir de la manera correcta sus labores, existiendo un gran compromiso no solo del nivel operativo sino también del nivel estratégico de una organización, que ellos promuevan una educación, concientización y motivación en el área que se desempeñe los individuos dentro de una organización mediante la utilización de Programa como: SETA(Security Education, Training, and Awareness). Este utilizan programas de concientización de EducaciónSETAel cual es necesaria para controlar el mal uso de SI (Dhillon 1999, Parker 1998, Whitman 2004). Los Programas SETA pueden tomar muchas formas, y se centran en proporcionar a los usuarios con conocimientos generales de la información de seguridad medio ambiente, junto con las habilidades necesarias para llevar a cabo cualquier requeridos de seguridad procedimientos (Lee y Lee 2002, Whitman2001).

3.2.1. Concienciación de Usuarios

Conciencia de la seguridad de información se puede definir como “la participación pasiva del individuo y el aumento de interés hacia ciertos temas y se considera uno de los componentes clave de concienciación siendo el otro la acción" (Namjoo, 2008). Según el foro de seguridad de la información (2003), la conciencia de seguridad de la información puede ser definida como el grado en que cada miembro del personal entiende la importancia de

la seguridad de la información, los niveles de seguridad de la información adecuada a la organización, sus responsabilidades de seguridad individuales y actos en consecuencia.

La conciencia es un factor que influye de manera considerable en los usuarios de TI, ya que sus actitudes, comportamiento y sobre todo el uso correcto de la información depende de ésta.

3.2.2. Seguridad de la información

Hoy en día los problemas de seguridad se deben principalmente a la insuficiente concienciación sobre la seguridad de los usuarios, que puede ser mitigado sin la necesidad de tecnologías sofisticadas de seguridad.

Según (Chen, Shaw, & Yang, 2006) las amenazas a la seguridad pueden originarse internamente o externamente por agentes humanos o no humanos. Hay amenazas controlables como el hackeo y la mala conducta del empleado pero hay otros fuera del control humano como los desastres naturales. Entre las amenazas internas a la seguridad tenemos errores de seguridad de los usuarios, descuido de seguridad, negligencia de seguridad y ataques a la seguridad. Para proteger la seguridad de la información de los sistemas es necesario “detectar”, “prevenir” y “corregir” las amenazas internas y externas que tratan de explotar alguna vulnerabilidad de los sistemas de información. La falta de conciencia de la seguridad es una de las principales vulnerabilidades para ataques de amenazas internas y externas a la seguridad de información.

(Takemura, 2011) Afirma que “no podemos resolver el problema de la seguridad de la información sólo en función de la tecnología. Incluso si la tecnología es excelente, los seres humanos que usan la tecnología a veces cometen errores porque no son perfectos”. La disminución de este error humano contribuye a la solución de los problemas de seguridad de la información. Por lo tanto, junto con un enfoque de las ciencias naturales, tales como el desarrollo de la tecnología criptográfica, abordaje de las ciencias sociales como la economía, la psicología y la ciencia de la administración han comenzado.

3.2.2.1. Importancia de la implementación de la SGSI

La gestión de seguridad de la información es un proceso sumamente importante dentro de las organizaciones por ello es imprescindible la implementación del SGSI y garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización.

La implementación SGSI permitirá que los riesgos se encuentren de manera documentada, sistematizada, estructurada y repetible, lo cual ayudara a que las decisiones o medidas que se tomen sea de forma eficiente y si fuese necesario adoptar los cambios necesarios que se produzcan para mitigar los riesgos que representen. Si bien es cierto con la implantación del SGSI no se podrá tener un control total de la seguridad de la información en las organizaciones ya que los riesgos a los que se somete no sólo son de origen voluntarios; sino también son involuntarios (provocados accidentalmente como catástrofes naturales o fallas técnicas).

El no implementar un SGSI dentro de una organización es colocar en riesgo el activo más valioso (la información) ya que no existiría medidas ni contingencias para mitigar los posibles sucesos que atenten contra la integridad de la información.

Nuestra investigación está diseñada para implementar las medidas, normas, políticas y procedimiento que la Universidad Nacional Pedro Ruiz Gallo debe implantar para entender, comprender y conocer el comportamiento de los usuarios a través del estudio de teorías como Teoría del Comportamiento Planificado y Teoría de Disuasión con el objetivo salvaguardar el activo más valioso de la organización (información) en todo sus aspectos confidencialidad, integridad y disponibilidad.

3.2.2.2. Estándares para la implementación de los SGSI

El estándar más general y completo para la gestión de la seguridad de la información es la familia ISO 27000, que incluye en sus dominios, entre otros, la gestión de activos, la seguridad asociada al recurso humano, la gestión de comunicaciones y operaciones, el control de acceso y la gestión de la continuidad del negocio, todo enmarcado en un ciclo PHVA (planear-hacer-verificar-actuar; en inglés se denomina *PDCA, plan-do-check-act*) que busca la mejora continua de los procesos, concepto introducido por Walter A. Shewhart y desarrollado por Edwards Deming como parte de la teoría del *Total Quality Management* (TQM). Otros estándares como Magerit, Marion, Mehari y Octave son más específicos, desarrollados para una región particular y para la gestión de riesgos de empresas con diferente naturaleza operativa.

Para la ISO (International Organization for Standardization) un sistema de gestión queda definido por un proceso de 4 etapas, creado por Walter Andrew Shewhart (1891 – 1967) y popularizado por William Edwards Deming (1900 – 1993), Planificar (Plan), Implementar (Do), Medir (Check) y Mejorar (Act).

Planificar: En esta etapa se busca establecer las políticas, objetivos, procesos y procedimientos del SGSI.

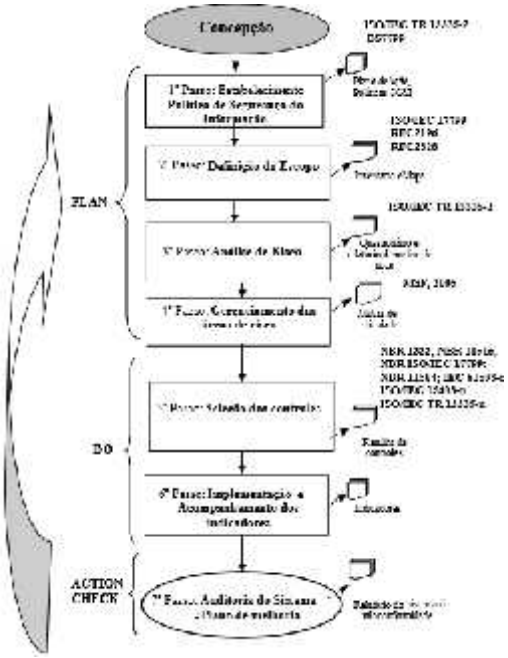
Implementar: En esta etapa se realiza el proceso de implementar y operar las políticas, controles, procesos y procedimientos del SGSI.

Medir: Es la etapa donde se monitorea, evalúa y revisa el SGSI e informar los resultados de gestionar su revisión.

Mejorar: En esta etapa se toma las acciones correctivas y preventivas, basadas en auditorías internas del SGSI y de revisión de gestión u otra información relevante para lograr la mejora continua SGSI.

3.2.2.3. Metodología para la implementación de un sistema de gestión de la seguridad de la información

Figura N°20: gráfica propuesta de la metodología de la seguridad de la información



Fuente: figura propuesta por el artículo la metodología de la seguridad de la información

3.2.3. Norma ISO 27001

Según Gillies, A. (2011), la norma ISO 27001 proporciona un modelo para "establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI)".

3.2.4. Políticas de Seguridad de la Información

Las Políticas de Seguridad contiene directrices detalladas para el uso adecuado e inadecuado de los recursos de la organización considerado por (Whitman, Townsend, & Aalberts, 2001)

Las directrices establecidas para el uso de PSI, pueden ser tomadas por los usuarios de dos maneras, ya sea positiva o negativa conllevando a cometer

acciones intencionadas y no intencionadas que pondría en riesgo la seguridad de la información.

> Desde la perspectiva de la disuasión, las políticas de seguridad se basan en el mismo mecanismo subyacente como las leyes sociales: proporcionar el conocimiento de lo que constituye una conducta inaceptable aumenta la amenaza de castigo por la conducta ilícita (Lee & Lee, 2002)

La gran cantidad de incidentes de mal uso, se han convertido en uno de los casos de gran importancia para entender el comportamiento de los usuarios y reducir este tipo de comportamiento. La teoría general de disuasión sugiere que ciertos controles pueden servir como mecanismos de disuasión mediante el aumento de las amenazas percibidas de castigo por el mal usos de los SI.

> Las estrategias de organización para reducir el riesgo de los sistemas generalmente se dividen en cuatro distintas etapas disuasión, prevención, detección y recuperación (Straub & Welke, 1998) se refieren a estas cuatro etapas colectivamente como el Ciclo de Acción de Seguridad. Sobre la base de este modelo, la gestión de seguridad de SI eficaz debería tratar de maximizar el número de actos abusivos disuadidos y prevenidos y minimizar los que se ha detectado y castigado (Theoharidou, Kokolakis, & Karyda, 2005)

> Existen programas como SETA (Security Education, Training and Awareness) el cual tienen un efecto disuasivo semejante, logrado a través de los esfuerzos de la organización en curso (por ejemplo, reuniones informativas o cursos) que refuerzan pautas de uso aceptables y hacen hincapié en las posibles consecuencias por el mal uso de las políticas de seguridad. Estas actividades de vigilancia se piensan para disuadir de mal uso de SI, aumentando las posibilidades percibidas de detección y castigo por tal comportamiento (Parker 1998, Straub y Nance 1990).

El número de infracciones de seguridad que implican mal uso interno de los recursos es de vital importancia que se dé a conocer y comprender de cómo las organizaciones pueden reducir este comportamiento.

> En una encuesta realizada por el Instituto de Seguridad Informática (Richardson 2007) reportó pérdidas en un promedio de $345,000 entre el 39% de los encuestados capaces de estimar las pérdidas y dispuestos a informar sobre ellos. Curiosamente, la investigación indica que entre el 50% - 75% de seguridad incidentes se originan desde dentro de una organización (Ernst and Young 2003, Information Week 2005), a menudo perpetrados por empleados descontentos (Standage 2002). Por otra parte, las organizaciones a menudo son reacias a revelar dicha información, por temor a la publicidad negativa que podría dañar su imagen y/o precio de las acciones (Hoffer y Straub 1989, Richardson 2007).

La existencia de inseguridad de la información conlleva a que ésta se encuentre vulnerable y pueda ser manipulada de cualquier manera colocando en riesgo y generando pérdidas monetarias a la organización.

3.2.5. Seguridad lógica de los RRHH

La seguridad de los recursos humanos dentro de la organización, debe considerar como recurso humano al personal interno, temporal o partes externas en el aseguramiento de las responsabilidades que son asignadas a cada uno, asociadas con sus respectivos roles, para reducir el riesgo de robo, fraude o uso inadecuado de las instalaciones.

Todo el recurso humano que hace parte de la Organización debe estar consciente de las amenazas y vulnerabilidades relacionadas con la seguridad de la información y sus responsabilidades y deberes en el apoyo que deben brindar a las políticas de seguridad de la información establecidas para la reducción del riesgo de error humano.

3.2.6. Usuarios de TI

Según (Nuñez, 1992), se entiende por usuario a todos los beneficiarios potenciales de un sistema de información que pueden ser individuos, empresas, organismos oficiales y entidades que utilizan o deben utilizar información científica y técnica para la toma de decisiones, concebir nuevos productos, adaptar nuevas estrategias. Los usuarios de la información son parte integrante y final de la cadena de transformación de la información.

Los usuarios sin lugar a duda son quienes ocasionan mayor inseguridad a la información ya que los actos que cometen pueden ser intencionados y no intencionados.

3.2.6.1. Tipos de usuarios

Para García (2004) existe una relación con la unidad de La información, considerando los siguientes tipos de usuarios:

- Usuarios reales: Son personas que siempre concurren a las bibliotecas.
- Usuarios potenciales: Son personas que deberían concurrir a las bibliotecas pero no lo hacen.
- No usuarios: Son aquellas personas que no deberían concurrir a las bibliotecas que no le corresponden.

Según (García, 2004) usuarios se clasifican en función a dos criterios:

- Criterios objetivos: categoría profesional, especialidad, naturaleza de la actividad cual se busca la información, objeto de la relación con los sistemas de información.
- Criterios psicológicos: Actitudes y valores relativos a la información en general y a las relaciones con las unidades de la información en particular.

3.2.7. Conducta

Según José Bleger(1963) etimológicamente la palabra conducta es latina y significa conducida o guiada; es decir, que todas las manifestaciones comprendidas en el término de conducta son acciones conducidas o guiadas por algo que está fuera de las mismas: por la mente.

La conducta se ha convertido en un campo y lenguaje de estudio común para sociólogos, antropólogos y muchos investigadores de distintas disciplinas y escuelas.

3.2.7.1. Tipos de conducta

- Conducta de adaptación: Respuesta encaminada a evitar o reducir la tensión, escapar de ella o afrontar una fuente determinada de tensión.
- Conducta anormal: La conducta se considera anormal cuando se caracteriza por notorias deficiencias de autocontrol, de funcionamiento social o cognoscitivo o por angustia incontrolable.
- Conducta estereotipada: Conducta ocasionada por un conflicto, varía poco, tiene una cualidad ritual y raramente es modificada por sus consecuencias.
- Conducta psicopática (personalidad antisocial): Desorden de la personalidad caracterizada por pautas conductuales que hacen que las personas estén en conflicto con la sociedad. Los psicópatas desdeñan los derechos de otros, se comportan como egoístas, actúan para obtener su propia satisfacción inmediata y parecen olvidarse de las consecuencias de su conducta al control voluntario.

3.2.7.2. Bases psicológicas de la conducta

- Escuelas psicodinámicas:

  En la escuela psicodinámica se enfatiza la importancia de conflictos inconscientes e instintos biológicos en la determinación del comportamiento humano, en la escuela psicodinámica son deterministas por lo que cada acto y sentimiento es el resultado inevitable de fuerzas naturales y acontecimientos previos. Sus máximos representantes son Freud, Jung y Adler.

- Escuelas conductistas:

  Las escuelas conductistas asumen que cada acto es causado por fuerzas naturales se basan en el estudio sistemático de la conducta observable: estímulo-respuesta, su máximo objetivo es descubrir las leyes básicas del aprendizaje. Los representantes de la escuela conductista son Watson, Pavlov (condicionamiento clásico), Skinner (condicionamiento operante).

3.2.8. Comportamiento humano

El comportamiento humano es el conjunto de actos exhibidos por el ser humano y determinados por la cultura, las actitudes, las emociones, los valores de la persona y los valores culturales, la ética, el ejercicio de la autoridad, la relación, la hipnosis, la persuasión, la coerción y/o la genética.

El comportamiento humano no puede confundirse con el comportamiento social que es una acción más desarrollada y que está dirigido a otro sujeto. La aceptación del comportamiento es relativamente evaluada por la norma social y regulada por diferentes medios de control social.

El comportamiento humano es estudiado por las disciplinas académicas de la psicología, la sociología, la economía, la antropología, la criminología y sus diferentes ramas.

Un factor de mucha importancia en el comportamiento humano, social e incluso en la vida diaria es la psicología, que es la ciencia de la vida mental,

tanto de sus fenómenos como de sus condiciones. Fenómenos son lo que llamamos sentimientos, deseos, cogniciones, razonamientos, decisiones y cosas similares; consideradas superficialmente es tal su variedad y complejidad que deja una impresión caótica al observador. Sin una mente saludable y estable no puede haber un comportamiento sano y estable, por tal razón la salud mental influye mucho en el comportamiento humano.

3.2.8.1. Factores del comportamiento humano

Según (Glenn & Malagodi, 1991) los factores del comportamiento humano son:

- ✓ La genética.
- ✓ La actitud: en este grado la persona hace una evaluación favorable o desfavorable del comportamiento.
- ✓ La norma social: ésta es la influencia de la presión social que es percibida por el individuo (creencia normativa) para realizar o no ciertos comportamientos.
- ✓ Control del comportamiento percibido: como las creencias del individuo hacen fácil o difícil la realización del comportamiento.
- ✓ La cultura: influencia entrelazada con la contingencia de diferentes conductas.

3.2.8.1.1. Factores de comportamiento relacionado con la genética

3.2.8.1.1.1. Comportamiento compulsivo y destructivo

Un usuario con dicho comportamiento es impredecible e incluso dañino puesto que no reflexiona de sus actos y su posterior consecuencia, ocasionando daños no intencionados medios y/o graves en la seguridad de información de la organización.

Desde el punto de vista de la seguridad, el hecho de que un usuario tenga el comportamiento compulsivo y destructivo, ya es un riesgo para el

cumplimiento de las políticas de seguridad de la información por el mismo carácter impredecible que se tiene.

El comportamiento compulsivo y destructivo al ser un factor genético, es casi incontrolable; pero factores como el entorno social y familiar en el que se rodean juega un papel muy importante; el hecho de que un usuario asociado a este comportamiento infrinja las PSI, necesariamente no lo hará de manera intencionada.

3.2.8.1.2. Factores del comportamiento relacionados con la actitud

3.2.8.1.2.1. Compromiso

Según el estudio realizado por (Jaik, Tena, & Villanueva, 2010) señala que el compromiso institucional puede ser entendido como un deber moral adquirido hacia una persona o institución, en el cual también hacen mención que los autores Hellriegel, Slocum y Woodman (1999) quienes definen compromiso institucional como “la intensidad de la participación de un empleado y su identificación con la organización, el compromiso organizacional se caracteriza por la creencia y aceptación de las metas y los valores de la organización; disposición a realizar un esfuerzo importante en beneficio de la organización y el deseo de pertenecer a la organización”.

Desde el punto de vista de la seguridad. Un usuario comprometido, se enfocará en alcanzar las metas y objetivos planteados por la institución cumpliendo con las PSI.

Sin embargo es importante saber que el compromiso nace de la libertad y no de la imposición, libertad a formar parte de la organización y sentirse participe de las decisiones. Un usuario no comprometido es vulnerable a cometer actos intencionados y no intencionados que finalmente incumplirán las PSI.

3.2.8.1.2.2. Liderazgo:

Según (Kreitner & Kinicki, 1997), considera el liderazgo como un hecho subjetivo que estructura el poder de un grupo. El liderazgo es también un proceso altamente interactivo y compartido, en el cual los miembros de todos los equipos desarrollan habilidades en un mismo proceso; implica establecer una dirección, visión y estrategias para llegar a una meta, alineando a las personas y al mismo tiempo motivándolas (French & Bell, 1996)

Desde el punto de vista de la seguridad el líder es la persona que fija relaciones y establece una fuerte identificación con sus colaboradores impulsándoles a tener objetivos comunes y una visión compartida por cumplir las PSI; más allá de la obtención de una recompensa.

Si bien es cierto existen colaboradores que no siguen del todo las indicaciones de un líder debido a ciertas actitudes y comportamientos de la personalidad, llevando al colaborador a cometer actos intencionados y no intencionados.

3.2.8.1.3. Factores del comportamiento relacionados con las normas sociales

3.2.8.1.3.1. Moral

El desarrollo moral depende tanto de la estimulación cognoscitiva estructural como de la estimulación social, lo que Kohlberg (1992) denomina toma de rol. La toma de rol implica integrar la actitud de otros, ser consciente de sus pensamientos y sentimientos, ponerse en su lugar.

La moral, emociones y los valores influyen de manera imprescindible en el comportamiento humano.

Desde el punto de vista de la seguridad, la moral es un factor muy importante para el cumplimiento de las PSI; un usuario con valores tiene menos probabilidad de comer actos intencionados a menos que sea influenciado de manera externa y social.

3.2.8.1.4. Factores del comportamiento relacionados con el control del comportamiento percibido

3.2.8.1.4.1. Estrés laboral:

Según Buendía (2002) estrés deriva del griego "stringere" que significa provocar tensión.

Desde el punto de vista de seguridad el estrés es ocasionado por alguna tensión nerviosa excesiva o por el sobre esfuerzo tanto físico como mental; este desequilibrio en el ámbito laboral ocasionaría en los usuarios el incumplimiento total o parcial de las PSI.

El estrés laboral en los usuarios se podría reflejar mediante acciones intencionadas (voluntad propia o por influencia de su entorno social) y no intencionadas (ocasionadas por error) que atenten al cumplimiento de las PSI.

3.2.8.1.4.2. Presión para cumplir metas

Según el estudio realizado por (Rodriguez, 2013) indica que el trabajo bajo presión lleva a relacionar dos eventos de tipo cognitivo, denominados por Richard Lazarus “valoración primaria” y “valoración secundaria”; la primera valoración está referida a la interpretación que hace el sujeto de un evento, que culmina con un juicio del cual se establece que dicho evento es amenazador; la segunda guarda relación con el hecho de que el sujeto advierte que no tiene las habilidades ni los recursos para subsanar el suceso amenazador al que se ve evocado.

Desde el punto de vista de la seguridad; la presión laboral es un factor muy importante para determinar el comportamiento y la capacidad que tendría un usuario al momento de enfrentarse a situaciones en la que se encuentre bajo presión; cumpliendo de la mejor manera las PSI.

El hecho de someter a un usuario a trabajar bajo presión implica que éste pueda realizar actos intencionados y no intencionado.

3.2.8.1.4.3. Tecnologías de control

Según la página (ALEGSA.com.ar), la tecnología (o sistema) de control es cualquier tecnología que permite controlar, generalmente de forma automática (aunque no necesariamente) un ambiente, una máquina. El objetivo de un sistema de control es gobernar la respuesta del sistema controlado sin que deba intervenir directamente un operario sobre los elementos de salida.

Desde el punto de vista de la seguridad, las tecnologías de control se han convertido en un en una herramienta de gran ayuda para los usuarios de TI, para el cumplimiento de las PSI.

Con el uso de tecnologías de control en una institución hace que los errores que se cometa sean menores; sin embargo. No se puede evitar los actos intencionados y no intencionados.

3.2.8.1.5. Factores del comportamiento relacionados con la cultura

3.2.8.1.5.1. Motivación

Según (Maslow, 1954) define la motivación como un conjunto de necesidades jerarquizadas que tiene el individuo, según la importancia que cada persona les concede en función de sus circunstancias.

Desde el punto de vista de la seguridad, la motivación es un factor muy importante para el cumplimiento de las PSI, ya que un usuario motivado es asequible a cumplir las PSI y cualquier otra normativa establecida dentro de la organización; sin embargo existe la posibilidad de que el usuario pueda cometer un acto no intencionado que pueda perjudicar la seguridad de la información.

3.2.8.1.5.2. Entrenamiento

Desde el punto de vista de la seguridad, el entrenamiento es el conjunto de actividades que fortalecen el conocimiento del usuario para que éste pueda cumplir de forma adecuada las PSI.

Es necesario llevar un adecuado entrenamiento pues de lo contrario llevaría al usuario a cometer actos no intencionados por falta de conocimiento.

3.3. Teorías de gestión del comportamiento

3.3.1. Teoría del Comportamiento Planificado (TPB)

El ser humano tiene tendencias psicológicas de reaccionar ante un determinado comportamiento realizando acciones que puede ser intencionales o no intencionales, estas acciones se ven reflejadas en las actitudes que se presentan para mostrar dicho comportamiento lo cual pueden ser tanto acciones razonadas o planificadas.

Según (Eagly y Chaiken, 1993), la actitud es una tendencia psicológica que se expresan mediante la evaluación de una entidad concreta con cierto grado de favorabilidad o desfavorabilidad.

> El concepto de actitud se refiere a las concepciones fundamentales relativas a la naturaleza del ser humano, implica ciertos componentes morales o humanos y exige un compromiso personal y se define como una tendencia o disposición constante a percibir y reaccionar en un sentido; por ejemplo de tolerancia o de intolerancia, de respeto o de crítica, de confianza o de desconfianza (Martín, 1999).

Éstas son algunas de las muchas definiciones de actitud, las cuales nos muestran claramente la implicancia o tendencia psicológica que sostiene en el comportamiento del ser humano. La Actitud va de la mano con la intención, pero puede variar con el tiempo.

La Teoría de la Acción Razonada (TAR) y la Teoría del Comportamiento Planificado (TCP) la cual es una extensión de la TAR, nos darán una mayor claridad del comportamiento del ser humano.

La TAR plantea que el individuo o usuario por lo general se comportan de una manera sensata bajo un control volitivo en el sentido que las personas puedan decidir realizar una acción determinada, teniendo en cuenta las consecuencias de sus actos.

Sin embargo debemos tener muy en claro que la intención de conducta es una función de dos factores: la propia actitud hacia el comportamiento (A) y Norma Subjetiva (SN).

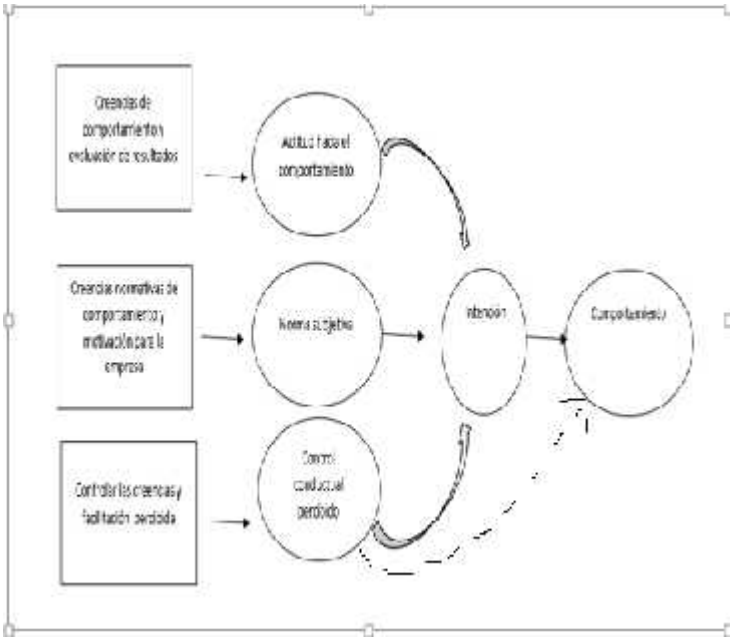
Según (Fishbein & Ajzen, 1975), la TAR está diseñada para predecir comportamientos volitivos de como: ver las noticias en la televisión, votar por el candidato de su preferencia en una elección, comprar pasta de dientes en una farmacia, rezar antes de ir a la cama o donar sangre para la Cruz Roja.

El estar interesados en la comprensión de la conducta humana no sólo basta conocer sus actitudes, sino también debemos de identificar los determinantes de las próximas intenciones en las cuales según la Teoría de la Acción Razonada, la intención de una persona está determinado en dos factores básicos fundamentales uno de naturaleza personal y la otra de influencia social.

El primer factor de naturaleza personal es la evaluación positiva o negativa del individuo de realizar el comportamiento a lo cual se denomina actitud hacia el comportamiento. El segundo factor de la intención es la percepción que tiene la persona de las presiones sociales de su entorno, lo cual ya dependerá de la persona realizar o no realizar dicha conducta, a este factor se denomina norma subjetiva.

En términos generales, podemos darnos cuenta que generalmente las personas tienen la intención de realizar una conducta cuando evalúan de manera positiva y cuando creen que otros personajes importantes de su entorno social piensan que deben llevarla a cabo; es decir de las intenciones a las acciones, es cómo surge la Teoría de la Acción Planificada.

Figura N°21. Gráfica de la Teoría del Comportamiento Planificado



Fuente: Traducido de Ajzen (1991)

La Figura N°21 muestra que la Teoría del Comportamiento Planificado es una extensión de la Teoría de la Acción Razonada.

Ajzen (1985) amplió la Teoría de la Acción Razonada mediante la inclusión de otra construcción, Control Conductual Percibido (PBC, Perceived Behavioral Control), para predecir las intenciones de comportamiento y conducta. El modelo extendido es la Teoría del Comportamiento Planificado.

La diferencia entre estas dos teorías es que la teoría de la conducta planificada ha añadido el control del comportamiento percibido como el determinante de la intención de conducta, así como las creencias de control que afectan el control del comportamiento percibido.

Ambas teorías asumen que los seres humanos son básicamente racionales y hacen uso sistemático de la información disponible para ellos cuando se toman decisiones. La Teoría de la Acción Razonada también asume que el comportamiento objeto de estudio está bajo control volitivo total del ejecutante (Madden, 1992).

Teoría del Comportamiento Planificado se ha aplicado con éxito a diversas situaciones, en la predicción del rendimiento de comportamiento y las intenciones, tales como la predicción de las intenciones de usuario para utilizar un nuevo software (Mathieson, 1991), para llevar a cabo autoexamen de mama (Young, 1991), y evitar la cafeína (Madden, 1992) encontraron que la teoría de la conducta planificada tiene una mejor capacidad de predicción del comportamiento de la teoría de la acción razonada.

Es de vital importancia saber que la que la teoría de la gestión de las conductas no trabaja con la conducta real, sino con la intención de la conducta.

3.3.2. Teoría de Disuasión

Es una de las teorías más usadas en la seguridad de los sistemas de información, en esta teoría entra a tallar la elección racional de la conducta humana, en la cual se puede predecir que una conducta ilícita puedes ser controlada por amenazas de sanciones que sean cierta severas y rápidas. Se ha utilizado la Teoría de la Disuasión (TD) para predecir el comportamiento de los usuarios ya sea de apoyo o perjudicial en la seguridad de la información (SI).

La TD es una perspectiva teórica enraizada en la criminología clásica (Beccaria, 1963), la teoría asume que las personas toman decisiones razonadas hacia perpetrar o abstenerse de la delincuencia basada en la maximización de sus beneficios y la minimización de costos. La teoría clásica de la prevención se centra en las sanciones formales (legales) y postula que cuanto mayor es la certeza percibida, severidad y celeridad (rapidez) de sanciones por un acto ilícito, los individuos están más disuadido de ese acto (Gibbs, 1975). Las ampliaciones del modelo clásico de disuasión incluyen sanciones informales como la desaprobación social, auto-desaprobación (por ejemplo, la vergüenza), y la inhibición moral (Piquero y Tibbetts, 1996).Teoría Contemporánea de la disuasión postula que los individuos incluyen los riesgos y costos de ambas sanciones formales e informales que se perciben en decidir si debe o no participar en una actividad ilícita (Pratt, 2006).

Se debe resaltar que la teoría de la disuasión tiene una gran participación e implicancia en el ámbito de la a seguridad de la información en las organizaciones. Las organizaciones se han enfrentado a muchas amenazas a la seguridad a través de la combinación de una serie de controles ya sea físicos, técnicos y administrativos. Encuestas de la industria indican que la garantía de seguridad de la información es una prioridad alta dirección en muchas organizaciones (Ernst y Young, 2009; PwC / OSC / CIO, 2010).

Por ejemplo, la norma ISO / IEC 27002, uno de los estándares más ampliamente adoptado para la gestión de seguridad de la información, se basa fuertemente en la teoría de la disuasión en la recomendación de políticas, directrices y programas de sensibilización que definen claramente las consecuencias y sanciones para los empleados que los recursos de la empresa mal uso (Theoharidou, 2005).

Es imprescindible destacar que el individuo tiene muchas perspectivas, pero cada una de ellas está sujeta en hacer un determinado acto para obtener un determinado beneficio. El ser humano es consciente delas consecuencias y riesgos que puede ocasionar un acto, la cual puede convertirse en un acto ilícito o de apoyo. El hecho de ser consciente es capaz de reconocer que su acto merece una sanción que puede ser una sanción formal o una sanción informal. El que exista una sanción no quiere decir que todos los individuos se amedrentan ante ello siempre habrá alguno que buscara sus beneficios sin importar las consecuencias.

La TD ofrece dos enfoques dominantes para modelar los efectos teóricos de las amenazas de sanción percibidas: **aditivo y multiplicativo** (Cochran, 2008).Los modelos de aproximación aditivo perciben certeza y severidad de las sanciones por separado. Los modelos multiplicativos enfoque sanciones como el producto de su seguridad percibida y la gravedad.

3.4. Teoría de la Acción Razonada (TAR)

La Teoría de la Acción Razonada (TRA, Theory of Reasoned Action) aparece durante la primera mitad del siglo pasado en la academia estadounidense como una crítica al modelo de la economía que se intentaba construir en Europa por académicos de orientación socialdemócrata y socialista. La TAR además de destruir los supuestos fundamentales de esta teoría, introdujo una revolución teórica y metodológica para las ciencias sociales.

La TRA es una perspectiva teórica general de las ciencias del comportamiento humano, y su ámbito es el de la interacción humana, es decir, se refiere a toda clase de situaciones sociales. La TRA representa una innovación teórica y metodológica revolucionaria y ambiciosa del último medio siglo, ha pasado de ser una ciencia estrictamente axiomática a ser una ciencia híbrida entre la formalización matemática, la modelación experimental y comparativa (es decir, sensible al contexto y a la historia).

Cabe mencionar una diferencia entre la proposición de la teoría evolutiva de la elección racional y la racionalidad acotada que propuso el politólogo Herbert Simón (1985), Premio Nobel de Economía en 1978, quien sugirió que la mayoría de los motivos o presencias que se observaban en la acción racional son exógenos, es decir, provienen del entorno social y acotan la exigencia puramente egoísta. Gintis y sus colegas aceptan esta situación, pero retoman la ortodoxia e insisten en que la "cultura" no debe tratarse como variable exógena, lo cual significa sacrificar la variedad por la *justeza*. La "en dogeneidad" es la carta original de la teoría tal como la presentó Kenneth Arrow, y la continuó una larga serie de eminencias científicas.

El asunto que más altera a los sociólogos es la insistencia irrenunciable al reduccionismo en las explicaciones de la conducta social establecida por la teoría de la elección racional. Existen muchos motivos y el estudio del pasado y del presente nos convence de ello cada día. La cuestión es si esos motivos

aparentemente no guiados por el interés propio pueden explicarse también por éste. La respuesta de la TRA es afirmativa. Es decir, confirma que sí es posible una explicación reduccionista. No obstante, como el filósofo Daniel Dennett (1999, pág. 123) y Elster (2007, pág. 257) nos recuerda, existen al menos dos formas de reduccionismo: el mezquino o duro, que casi siempre termina como un reductio ad absurdum, y el bueno o heurístico. Este último es un ingrediente indispensable en el desarrollo de la ciencia, sea física, biológica o social. La TRA recurre al reduccionismo, y ése es su punto a la vez fuerte y débil. El principio de racionalidad de la acción es necesario, más no suficiente. No es posible prescindir de él, pero con frecuencia su uso es una descripción de conductas maximizadoras de algo.

3.5. Glosario de términos

- **Concienciación:** Es la capacidad que tiene el usuario de TI para poder usar las políticas de TI de la manera más consciente y racional.
- **Conducta:** Conjunto de actos que tienen los usuarios de TI, quienes están determinados y formados por la cultura, las emociones y los valores factores que les permitirá aplicar de la manera más correcta las políticas de seguridad.
- **Comportamiento:** Es la forma cómo los usuarios o encargados de las TI actúan frente a diferentes factores que se les coloca para demostrar cómo es que pueden responder a ello sin necesidad de atentar ante la las Políticas de seguridad de TI de una organización.
- **Consciente:** Los usuarios de TI deben tener un amplio conocimiento de que cada uno de sus actos ya sean correctos e incorrectos (intencionales y no intencionales) siempre tendrá una consecuencia positiva o negativa de acuerdo a sus acciones.
- **Seguridad de Información:** Término de gran significado que consiste en proteger el activo más importante de una organización (información) teniéndose en cuenta en sus tres pilares fundamentales como son: confidencialidad, integridad y disponibilidad.
- **Políticas de Seguridad de información:** Conjunto de reglas o directrices que los usuarios de TI deben tener muy claras y que consecuencias tendría si se incumplieran una de ellas, las pérdidas que se podría ocasionar y asimismo poder tener mantenimiento de cierto nivel de seguridad de la información de una organización.
- **Usuario TI:** Es la persona encargada del área de TI quien debe tener bien claro la importancia que tiene el uso correcto de las políticas de seguridad y

también saber qué consecuencias podría traer si incumpliera una de ellas encargada de usar un determinado servicio pero con limitaciones.

3.6. Técnicas para recopilar información del comportamiento

3.6.1. Estudio Etnográfico

El concepto de etnografía, compuesto de los elementos griegos ethnos (pueblo, grupo humano) y graphein (describir). Se nos muestra ya socialmente consolidado en diccionarios a partir de 1823, como aquel vocablo que designa el estudio del inventario étnico en función de las características lingüísticas de los pueblos (Petit Robert, 1983).

Una encuesta de tipo etnográfico va a tratar precisamente de captar lo más sistemáticamente posible esas diversas diferencias pertinentes que luego relaciona, por comparación o generalización y siguiendo una estructura lógico-deductiva, con otros fenómenos socioculturales, tanto en el orden de lo sincrónico como de lo diacrónico (Piaget, 1986).

Las limitaciones de empleo del método etnográfico dependen tanto del investigador como de los recursos, ya que un solo investigador no logra recaudar La información suficiente más que en un campo restringido; varios investigadores pueden reunir experiencias sectoriales cuya confrontación, análisis y sistematización comunes pueden permitir reforzar la ventaja que hemos citado hace un momento, para ofrecer interpretaciones más amplias e integradas. Además, una de las características esenciales de un razonamiento lógico, operatorio y válido, es su reversibilidad en cada una de sus etapas. En el método etnográfico esta reversibilidad consiste en el retorno permanente a la información directa sobre el terreno, que hay que confrontar dialécticamente con los grandes desarrollos lógicos o teorías. En esto se encuentra la ventaja de disponer, de acuerdo con el método de la encuesta inductiva, de numerosas informaciones, sobre las que uno puede, por medio de nuevos reagrupamientos, acceder a una reversibilidad del proceso, tal y como la plantea Piaget (1986).

3.6.2. Observación de campo

La observación es la técnica de investigación básica, sobre las que sustentan todas las demás, ya que establece la relación básica entre el sujeto que observa y el objeto que es observado, que es el inicio de toda comprensión de la realidad.

Según Bunge la observación es un procedimiento científico se caracteriza por ser:

Intencionada: porque coloca las metas y los objetivos que los seres humanos se proponen en relación con los hechos, para someterlos a una perspectiva teleológica.

Ilustrada: porque cualquier observación para ser tal está dentro de un cuerpo de conocimientos que le permite ser tal; solo se observa desde una perspectiva teórica.

Selectiva: porque necesitamos a cada paso discriminar aquello que nos interesa conocer y separarlo del cúmulo de sensaciones que nos invade cada momento.

Interpretativa: en la medida en que tratamos de describir y de explicar aquello que estamos observando. Al final de una observación científica nos dotamos de algún tipo de explicación acerca de lo que hemos captado, al colocarlo en relación con otros datos y con otros conocimientos previos.

En el proceso de observación, siempre según Bunge se distinguen cinco elementos:

Sujeto u observador: en el que se incluyen los elementos constituyentes de este, tanto los sociológicos como los culturales, además de las experiencias específicas del investigador.

Objeto de la observación: que es la realidad, pero en donde se han introducido procedimientos de selección y de discriminación, para separarlo de otras sensaciones. Los hechos en bruto de la realidad se han transformado en datos de un proceso de conocimiento concreto.

Circunstancias de la observación: son las condiciones concretas que rodean al hecho de observar y que terminan por formar parte de la propia observación.

Los medios de la observación: son los sentidos y los instrumentos desarrollados por los seres humanos para extender los sentidos o inventar nuevas formas y campos para la observación.

Cuerpo de conocimientos: es el conjunto de saberes debidamente estructurados en campos científicos que permiten que haya una observación y que los resultados de esta se integren a un cuerpo más amplio de conocimientos.

Con estos aspectos, podemos entrar a los aspectos propiamente técnicos de la observación.

3.6.3. Ventajas de la observación:

Hernández señala las siguientes ventajas de la observación:

Técnica natural: en cuanto no interviene sobre el objeto de investigación, este puede ser percibido en su ambiente natural y en sus formas de comportamiento independiente de cualquier participación externa.

Útiles para trabajar con materiales poco estructurados, porque la información fluye de la proximidad directa con el objeto de investigación.

Se puede trabajar con grande grupos y con información abundante.

Aspectos técnicos:

Un buen proceso de observación requiere que se tome en cuenta:

- Definir el punto de vista o el marco conceptual desde el que se realizará la observación.
- Elaborar una guía de observación lo más detenida y detallada posible.
- Registrar lo observado lo más pronto y lo más fielmente que sea posible.
- Interpretar lo observado a la luz de otras observaciones y de conocimiento previamente dados.

IV. MARCO METODOLOGICO

4.1. Hipótesis:

H0: La gestión de las conductas y comportamientos de los usuarios de TI no tiene un impacto positivo en la concientización para el cumplimiento de las políticas de seguridad de la información en la Universidad Nacional Pedro Ruiz Gallo.

HA: La gestión de las conductas y comportamientos de los usuarios de TI tiene un impacto positivo en la concientización para el cumplimiento de las políticas de seguridad de la información en la Universidad Nacional Pedro Ruiz Gallo.

4.2. Tipo de investigación

El presente trabajo se encuentra tipificado de la siguiente manera:

a) De acuerdo al fin que se persigue:

La presente investigación es aplicada, porque se contextualizaron las teorías utilizadas para fundamentar el planteamiento del modelo y las estrategias de gestión de conductas y el comportamiento de los usuarios de TI en la universidad Nacional Pedro Ruiz Gallo en Lambayeque.

b) De acuerdo a la metodología para demostrar la hipótesis:

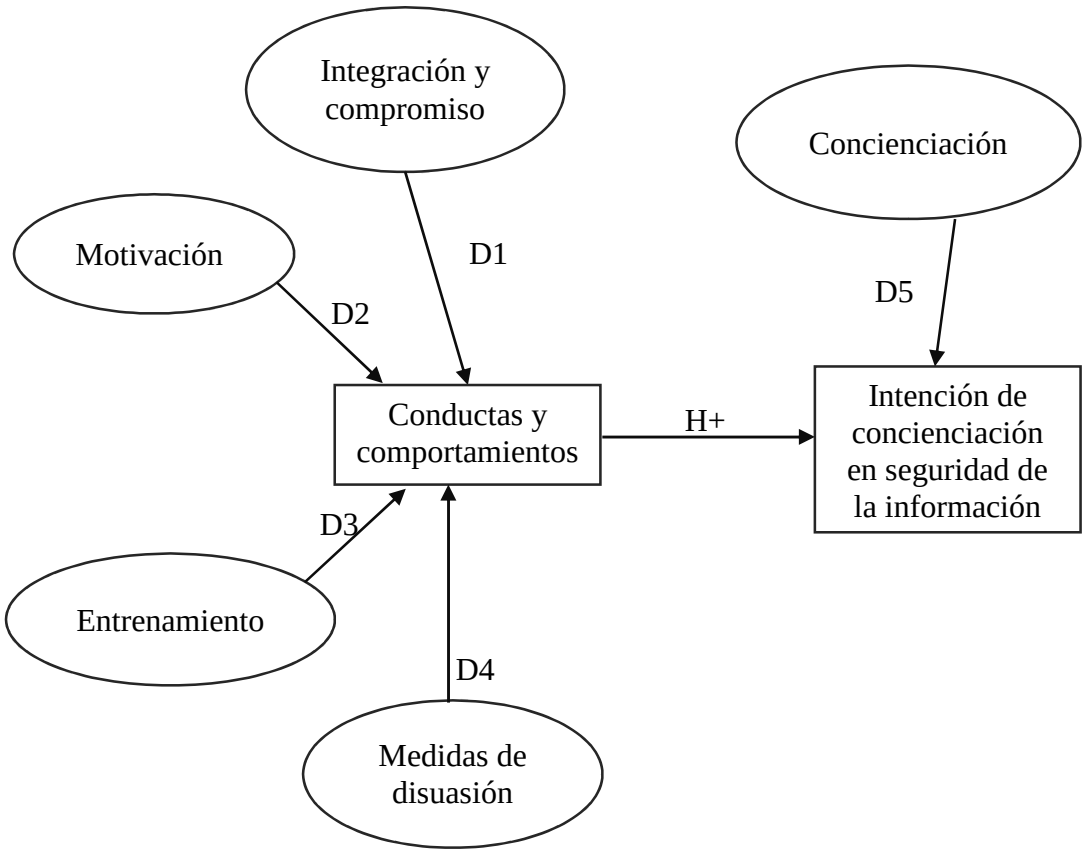
La presente investigación es de tipo relacional ya que se estableció la relación que existe entre la variable dependiente y la variable independiente, donde se buscara las relaciones estadísticas existentes al someter las variables implicadas en el estudio.

Las relaciones estadísticas que se emplearan para el estudio son: regresión lineal, análisis de varianza, covarianza.

4.3. Operacionalización de variables

El modelo conceptual planteado en la siguiente investigación se gráfica a de la siguiente manera:

Gráfica N°21. Modelo conceptual de la investigación



Fuente: Elaboración Propia

Tabla N° 01: Variables de la investigación

Variable independiente	Gestión Conductas y comportamientos de los usuarios de TI
Variable dependiente	Intención de concienciación en la seguridad de la información

Fuente: Elaboración Propia

Tabla N° 02: Relación de los factores de las teorías con sus dimensiones

TEORIAS	FACTORES DE TEORIAS	DIMENSIONES
Teoría del comportamiento planificado(TPB)	Factores relacionados con la **conducta**	Integración y compromiso
	Factores relacionados con la influencia del **entorno social**	Motivación Entrenamiento
Teoría de la Acción Razonada (TAR) / Teoría de disuasión (TD)	Factores relacionados con el **control percibido**	Medidas de Disuasión

Fuente: Elaboración propia

4.4. Diseño de contrastación de la hipótesis

Para contrastar la hipótesis se utilizará el método relacional, porque se tienen como propósito medir el grado de relación que exista entre las dos variables definidas en el contexto particular de la empresa Universidad Nacional Pedro Ruiz Gallo (UNPRG), aplicando la estrategia de evaluación y comparación de una observación a modo de Pos test, es decir, observar la reacción de una variable frente al estímulo de la otra y de esta manera comparar el después de su valores, tal como se muestra:

X O1

Dónde:

X: Grado de concientización del usuario de TI, basado en las teorías TPB y TPA.

O1: Cumplimiento de las Políticas de Seguridad de Información.

4.5. Población y muestra de estudio

Unidad de Análisis: Usuarios de los servicios de TI ofrecidos por la Dirección Universitaria de Informática y Sistemas de la UNPRG.

Población: La población de la investigación está conformada de la siguiente manera:

Tabla N° 03: Distribución de usuarios de TI en la UNPRG

Tipo de usuario/cliente	N° Personas
Personal Directivo (autoridades y responsables de jefaturas)	116
Personal Administrativo (secretarias, personal de laboratorio)	247
Total	353

Fuente: Plan Operativo Institucional de la DIUS 2015

Observación: la cantidad considerada en la tabla N° 01, considera usuarios, al personal de la UNPRG que tienen acceso y utiliza algún terminal de computador, conectado a la red telemática y que lo utiliza como parte de sus funciones diarias.

Muestra: Como la población es conocida se utilizará la fórmula de obtención de muestra para una población finita. A partir de ello, los sujetos de análisis se definirán mediante muestreo aleatorio simple.

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

Dónde:

- N = Total de la población
- Z_α = 1.96 al cuadrado (porque la seguridad es del 95%)
- p = proporción esperada (en nuestra investigación es 5%)
- q = 1-p
- d = precisión (en nuestra investigación es 5%)

$$n = \frac{353 * 1.96^2 * 0.05 * 0.95}{0.05^2 * (353-1) + 1.96^2 * 0.05 * 0.95} \approx 61$$

Interpretación:

En base a la formula previa se obtiene que el tamaño de muestra apropiado para nuestra investigación es de 61 personas. Sin embargo de las 80 encuestas aplicadas sólo se pudo obtener respuesta de 32 personas a pesar de ello, el análisis de fiabilidad indica la validez de la investigación y que no hay valores excluidos Por tanto se recomienda para una próxima investigación que la cantidad de usuarios encuestados sea como mínimo el tamaño de muestra requerida y de esa forma asegurar una mayor fiabilidad de los resultados obtenidos.

4.6. Técnicas e instrumentos de recolección de datos

Se aplicó una encuesta al total de la población indicada en la tabla N°2, la misma que se muestra en el anexo N°1.

La encuesta se realizó con la finalidad de obtener información de los procedimientos implementados sobre la gestión de los servicios de TI en la UNPRG, encuestando a los responsables de las diferentes unidades de la DUIS.Para ello se elaboró la siguiente tabla donde se muestra la relación de las preguntas planteadas en la encuesta con sus correspondientes indicadores.

Tabla Nº2. Matriz de consistencia entre los indicadores y las preguntas de la encuesta

VARIABLE		DIMENSION	INDICADOR	INDICES	TECNICA DE INSTRUMENTO
INDEPENDIENTE Gestión de las conductas y comportamientos de los usuarios de TI		**Integración y compromiso**	Nivel de percepción del compromiso con las PSI	Escala de Likert	**Encuesta**
			Nivel de percepción de la integración con las PSI	Escala de Likert	
		Entrenamiento	Nivel de formación de los usuarios en seguridad de la información	Escala de Likert	
			Percepción sobre efectividad de los programas de entrenamiento sobre seguridad de la información	Escala de Likert	
			Nivel de conocimiento de los sistemas de información	Escala de Likert	
		Motivación	Nivel de motivación para cumplir con los PSI	Escala de Likert	
		Medidas de Disuasión	Identificación y comprensión de las medidas de disuasión	Escala de Likert	
DEPENDIENTE Concienciación en la seguridad de la información		**Concienciación**	Grado de concienciación del cumplimiento de las PSI	Escala de Likert	

Fuente: Elaboración Propia

4.7. Tratamiento de los datos y discusión de resultados

Para el tratamiento de los datos, se utilizó el aplicativo SPSS v19, obteniéndose los siguientes resultados:

4.7.1. Fiabilidad del instrumento (encuesta)

Para la presente investigación se ha empleado un método de consistencia interna altamente aceptado el cual es el Alfa de Cronbach, utilizado para evaluar el nivel de fiabilidad de un instrumento (encuesta). Mientras más cerca de 1 se encuentre este estadístico, quiere decir que el instrumento mide con mayor precisión lo que pretende medir. La medida de la fiabilidad mediante el Alfa de Cronbach asume que los ítems (evaluados en escala tipo Likert) miden un mismo constructo y que están altamente correlacionados (Welch & Comer, 1988). Para avalar un Alfa de Cronbach fiable se debe obtener siempre mediante los datos de cada muestra, de esta manera se garantiza la medida fiable del constructo en la muestra concreta de investigación.

Como criterio de evaluación de los coeficientes de Alfa de Cronbach usamos la escala De Vellis (en García, 2005) tal como sigue:

- Coeficiente alfa > 0.9 es **excelente**
- Coeficiente alfa > 0.8 es **muy bueno**
- Coeficiente alfa > 0.7 es **respetable**
- Coeficiente alfa > 0.65 es **mínimamente aceptable**
- Coeficiente alfa > 0.6 es **indeseable**
- Coeficiente alfa < 0.6 es **inaceptable**

Procesados los datos se obtuvo lo siguiente:

- **Análisis de fiabilidad**

Resumen del procesamiento de los casos

		N	%
Casos	Válidos	32	100,0
	Excluidos[a]	0	,0
	Total	32	100,0

a. Eliminación por lista basada en todas las variables del procedimiento.

Estadísticos de fiabilidad

Alfa de Cronbach	N de elementos
,814	18

Interpretación de resultados:

En el cuadro de **resumen del procesamiento de los casos** tenemos los casos válidos, que en este caso N = 32, debido a que han sido 32 los usuarios de TI los que han contestado las encuestas. También se observa que no hay ningún caso excluido, es decir que las 32 encuestas han sido consideradas para el análisis de los datos.

En el cuadro de **estadísticos de fiabilidad**, podemos observar que nuestra **Alfa de Cronbach** es **0.814**, eso quiere decir que mientras el valor del Alfa de Cronbach se aproxime o sea más cercano a 1, más confiable será nuestro modelo. Si lo definimos estadísticamente el instrumento es **muy bueno**, en base a la escala propuesta por De Vellis.

4.7.2. Análisis de Regresión Múltiple

Utilizamos regresión múltiple porque nuestra hipótesis pretende estudiar la posible relación entre variables independientes (predictoras o explicativas) y la variable dependiente (criterio, explicada, respuesta). En este caso, nuestras variables son:

- **Variable Independiente (Xi):** Conductas de usuarios de TI, descrita a través de las dimensiones: Integración y compromiso (X_1), Entrenamiento (X_2), Medidas de disuasión (X_3) y Motivación (X_4).
- **Variable Dependiente (Y):** Intención de cumplimiento de las políticas de seguridad.

Por tanto, el modelo a evaluar es un modelo de regresión múltiple de la forma:

$$Y = C_0 + C_1X_1 + C_2X_2 + C_3X_3 + C_4X_4 + E$$

Esto significa que se pretende evaluar la relación existente entre la variable dependiente “Intención de cumplimiento de las políticas de seguridad” y la variable independiente “Control de conductas de los usuarios de TI”, esta última explicada por cuatro dimensiones: Integración y compromiso (X_1), Entrenamiento (X_2), Medidas de disuasión (X_3) y Motivación (X_4).

Para lograr este objetivo, se desarrolló el siguiente procedimiento:

4.7.2.1. Reducción de ítems de cada dimensión evaluada

Dado que cada una de las dimensiones tiene más de un ítem a evaluar (ver Tabla Nº20) se tuvo que reducir a un solo ítem, de la siguiente manera:

Tabla Nº 1. Matriz de reducción de ítems evaluados

DIMENSION	**ITEMS**		**ITEM REDUCIDO(Promedio Simple)**
Concienciación	Grado de intención de cumplimiento de las PSI	P18	P18
Integración y compromiso	Nivel de percepción del compromiso con las PSI	P1	Integra_Compro = (P1 + P2 + P6 + P7)/4
	Nivel de percepción de la integración con las PSI	P2	
	Nivel de percepción de la integración con las PSI	P6	
	Nivel de percepción de la integración con las PSI	P7	
Entrenamiento	Nivel de formación de los empleados en seguridad de la información	P4	Entrenamiento = (P3 + P4 + P8 + P9 + P10)/5
		P10	
	Percepción sobre efectividad de los programas de entrenamiento sobre seguridad de la información	P3	
	Nivel de conocimiento de los sistemas de información	P8	
		P9	
Medidas de Disuasión	Identificación y comprensión de las medidas de disuasión	P5	Disuasión = (P5 + P13 + P14)/3
		P13	
		P14	
Motivación	Nivel de motivación para cumplir con las PSI	P11	Motivación = (P11 + P12 + P15 + P16 + P17)/5
		P12	
		P15	
		P16	
		P17	

4.7.2.2. Aplicación de la metodología de regresión múltiple

Para nuestro análisis se aplicará la metodología de regresión múltiple jerárquica con cuatro bloques, donde se fueron tomando variable por variable independiente con las que estamos trabajando, con la finalidad de generar diferente modelos.

Los modelos que esperamos generar son los siguientes:

- **Modelo 1:** sólo con la variable Integración y compromiso (X_1)
- **Modelo 2:** sólo con las variables: Integración y compromiso (X_1) y Entrenamiento (X_2)
- **Modelo 3:** sólo con las variables: Integración y compromiso (X_1), Entrenamiento (X_2) y Medidas de disuasión (X_3)
- **Modelo 4:** con las cuatro variables: Integración y compromiso (X_1), Entrenamiento (X_2), Medidas de disuasión (X_3) y Motivación (X_4).

Esto nos permitirá identificar mayor información de las variables independientes con las que estamos trabajando; así como también nos permite identificar si alguna de esas variables independientes no aporta al modelo, por tanto puede ser excluida del modelo.

Los resultados obtenidos se muestran a continuación:

Resumen del modelo[e]

Modelo	R	R cuadrado	R cuadrado corregida	Error típ. de la estimación	Durbin-Watson
1	,512[a]	,263	,238	,429	
2	,680[b]	,462	,425	,373	
3	,688[c]	,473	,416	,376	
4	,688[d]	,473	,395	,383	1,882

a. Variables predictoras: (Constante), Integra_Compro

b. Variables predictoras: (Constante), Integra_Compro, entrena

c. Variables predictoras: (Constante), Integra_Compro, entrena, disuacion

d. Variables predictoras: (Constante), Integra_Compro, entrena, disuacion, motiva

e. Variable dependiente: P18

Del cuadro se deduce que:

- El Modelo 1 (sólo con la variable Integración y Compromiso (X_1)) explica el **26.3%** de la varianza de la variable dependiente.
- El Modelo 2 (solo con las variables Integración y Compromiso (X_1) y Entrenamiento(X_2)) explica el **46.2%** de la varianza de la variable dependiente.
- El Modelo 3 (solo con las variables Integración y Compromiso (X_1), Entrenamiento (X_2) y Disuasión (X_3)) explica el **47.3%** de la varianza de la variable dependiente.
- El Modelo 4 (con las cuatro variables Integración y Compromiso (X_1), Entrenamiento (X_2), Disuasión (X_3) y Motivación (X_4)) explica el **47.3%** de la varianza de la variable dependiente.

Resultado:

- Se aplicó el modelo de regresión múltiple jerárquica porque la pretensión es evaluar el aporte que tiene cada una de las dimensiones de manera independiente sobre el modelo, asimismo determinar cuál de ellas es la que más y menos aporte al modelo de la presente investigación.

- De los resultados obtenidos en el cuadro resumen de los 4 modelos se observa que:
  - El Modelo 1 (sólo con la variable Integración y Compromiso (X_1) explica el **26.3%** de la varianza de la variable dependiente.
  - El Modelo 2 (solo con las variables Integración y Compromiso (X_1) y Entrenamiento(X_2)) explica el **46.2%** de la varianza de la variable dependiente.

- El Modelo 3 (solo con las variables Integración y Compromiso (X_1), Entrenamiento (X_2) y Disuasión (X_3)) explica el **47.3%** de la varianza de la variable dependiente.
- El Modelo 4 (con las cuatro variables Integración y Compromiso (X_1), Entrenamiento (X_2), Disuasión (X_3) y Motivación (X_4)) explica el **47.3%** de la varianza de la variable dependiente.

- Por tanto se puede deducir que la variable del modelo 1: Integración y compromiso (X_1) aporta con un 26.3% y la variable del modelo 2: Entrenamiento (X_2) aporta con 19.9 %, ambas variables aportan significativamente al modelo; a diferencia de la variable Medidas de disuasión (X_3) del modelo 3 y; la variable Motivación (X_4) del modelo 4 que aportan con 1.1 % constituyéndose así en variables que menos aportan al presente modelo.

- De los resultados de los modelos obtenidos se observa que los modelos 3 y 4 son los que dan mayor aporte para explicar el comportamiento de la población con 47.3%. Pero por efectos de la demostración de la hipótesis seleccionamos el modelo 3 donde sólo están las 3 variables independientes (variables Integración y Compromiso (X_1), Entrenamiento (X_2) y Disuasión (X_3)).

- Por otro lado, en el mismo cuadro observamos el resultado de la prueba de Durbin-Watson que nos da un valor para determinar la independencia de errores, pero no una significancia; por lo debemos tener algunos criterios de identificación de cuando este valor es bueno o no bueno. El valor esperado de la prueba Durbin-Watson es que sea lo más cercano a 2, en este caso tenemos un valor de (1.882).

Para evaluar su idoneidad usamos la tabla de Savin y White (Anexo 3) de la manera siguiente:

- Si el estadístico de Durbin-Watson (D) es mayor al límite D_U, entonces no existe correlación.
- Si $D < D_L$, existe una correlación positiva.
- Si D se encuentra entre los dos límites, la prueba no es concluyente.

Asimismo:

- Si $(4 - D) > D_U$, entonces no existe correlación.
- Si $(4 - D) < D_L$, existe una correlación negativa.
- Si (4 - D) se encuentra entre los dos límites, la prueba no es concluyente.

En base a los datos de nuestra investigación determinamos que $\mathbf{D_L}$ es **1.24371** y $\mathbf{D_U}$ es **1.65046**; por tanto concluimos que no existe correlación y que la recogida de datos ha sido aleatoria, evitando así invalidar por completo las conclusiones del análisis estadístico (obteniendo conclusiones erróneas).

4.7.3. ANOVA

Los resultados se muestran a continuación en el siguiente cuadro:

ANOVA[a]

Modelo		Suma de cuadrados	Gl	Media cuadrática	F	Sig.
1	Regresión	1,969	1	1,969	10,683	,003[b]
	Residual	5,531	30	,184		
	Total	7,500	31			
2	Regresión	3,465	2	1,732	12,449	,000[c]
	Residual	4,035	29	,139		
	Total	7,500	31			
3	Regresión	3,547	3	1,182	8,374	,000[d]
	Residual	3,953	28	,141		
	Total	7,500	31			
4	Regresión	3,548	4	,887	6,059	,001[e]
	Residual	3,952	27	,146		
	Total	7,500	31			

a. Variables predictoras: (Constante), Integra_Compro

b. Variables predictoras: (Constante), Integra_Compro, entrena

c. Variables predictoras: (Constante), Integra_Compro, entrena, disuacion

d. Variables predictoras: (Constante), Integra_Compro, entrena, disuacion, motiva

e. Variable dependiente: P18

Interpretación:

La presente investigación está trabajando con el 95 % de fiabilidad y por lo tanto el ANOVA evalúa que el modelo está dentro del tanto del 0.05 por tanto el modelo propuesto en la investigación es aceptado, Como se observa hay una significancia menor al 0.05 (0.00 ≤ 0.05) y la interpretación en términos de hipótesis es que el modelo que estamos probando mejora significativamente la predicción de la variable **dependiente**. Por tanto queda demostrado que el modelo que se encuentra dentro del 95% de fiabilidad con un margen de error de 0.05 es el modelo 3 comprendido con las siguientes variables: Integración y Compromiso (X_1), Entrenamiento (X_2) y Disuasión (X_3)

4.7.4. Análisis de coeficiente de la ecuación de regresión

Coeficientes[a]

Modelo		Coeficientes no estandarizados		Coeficientes tipificados	T	Sig.	Estadísticos de colinealidad	
		B	Error típ.	Beta			Tolerancia	FIV
1	(Constante)	,404	,989		,408	,686		
	Integra_Compro	,900	,275	,512	3,269	,003	1,000	1,000
2	(Constante)	-,947	,953		-,994	,328		
	Integra_Compro	,435	,278	,247	1,562	,129	,740	1,352
	Entrena	,838	,256	,519	3,278	,003	,740	1,352
3	(Constante)	-,722	1,004		-,719	,478		
	Integra_Compro	,405	,283	,230	1,429	,164	,725	1,379
	Entrena	1,087	,416	,674	2,613	,014	,283	3,532
	disuasion	-,282	,370	-,180	-,763	,452	,338	2,959
4	(Constante)	-,738	1,041		-,709	,484		
	Integra_Compro	,383	,397	,218	,963	,344	,381	2,622
	Entrena	1,086	,424	,673	2,562	,016	,283	3,536
	disuasion	-,286	,380	-,183	-,754	,458	,333	3,005
	Motiva	,032	,396	,018	,080	,937	,392	2,549

a. Variable dependiente: P18

En la tabla de coeficientes siguientes se observa que nuestro modelo de regresión es:

$$\mathbf{Y = C_0 + C_1X_1 + C_2X_2 + C_3X_3 + C_4X_4 + E}$$

Pero debido a los resultados estadísticos anteriores se descartó la variable Motivación por lo que el modelo quedaría de la siguiente manera:

$$\mathbf{Y= -0.722+0.405X_1+1.087X_2-0.282X_3+E}$$

De los coeficientes obtenidos concluimos que solo la variable **Motivación** (X_4) no aporta en la explicación del modelo propuesto.

De la misma tabla, también podemos observar los valores **t** y su significancia, que son valores que nos demuestran que tanto podemos generalizar el modelo de predicción a la población, son: **t= 1.429, 2.613, -0.763**. La cual nos confirma que el modelo puede generalizarse a toda la población solo con las variables **Integración y Compromiso** (X_1), **Entrenamiento** (X_2) y **Disuasión** (X_3).

V. CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones

1. A través de las **estadísticas descriptivas** se pudo determinar que el **63%** de los usuarios de TI de la **UNPRG** presentan insatisfacción respecto a la capacitación y al nivel de preparación brindada por parte de la institución. A su vez también se determinó que el **52%** de los usuarios de TI manifiestan que nunca se utilizan medidas de seguridad para mitigar los riesgos que pueden atentar a la información.

2. Como resultado de la encuesta etnográfica se pudo determinar: que la falta de capacitación y el leve nivel de preparación a los usuarios respecto a las PSI no es lo suficiente para poder resolver, gestionar y mitigar los riesgos de Seguridad de la Información.; sin embargo con la constante capacitación y preparación los usuarios tendrían mayor conocimiento y la capacidad para poder salvaguardar la información.

3. Debido a que los marcos de referencia que gestionan riesgos de TI normalmente no tienen controles relacionados con los comportamientos de los usuarios de TI, por ello se recurrió a teorías de gestión del comportamiento.Las teorías de la gestión de los comportamientos utilizados y aplicados para la construcción del modelo conceptual de la investigación fueron: Teoría de la acción razonada, Teoría del comportamiento planificado, Teoría de la disuasión.

4. Como resultado de la prueba de análisis de fiabilidad por **Alfa de Cronbach**, se obtuvo un **81,4%,** por lo tanto afirmamos que el instrumento de recolección de datos (encuesta) de acuerdo a la escala de Vellis (2003) es bueno.

5. Se demostró la aceptación del modelo conceptual propuesto con los factores: **Integración y compromiso** (X_1), **Entrenamiento** (X_2), **Medidas de disuasión** (X_1) y **Motivación** (X_4), a través de los siguientes aspectos:

    a. El modelo de regresión lineal probado con las tres variables independientes: Integración y Compromiso (X1), Entrenamiento (X2) y Disuasión (X3) explica el 47.3% de la varianza de la variable dependiente. Descartándose la variable Motivación (X4).

    b. El puntaje de la prueba **Durbin-Watson** de **1.882** indica que hay independencia de errores, y que la recogida de la información ha sido aleatoria, evitando así invalidar las conclusiones del análisis estadístico.

    c. Los dos modelos que explican mayor cantidad de datos son el modelo 3 y el modelo 4, dado que en ambos casos tienen el mayor **R_2** igual (**0.473**), esto es que ambos modelos explican el **47.3%** de los datos hallados. Sin embargo el modelo de regresión con 3 variables independientes: **Integración y Compromiso** (X1), **Entrenamiento** (X2) y **Medidas de Disuasión** (X3), es el modelo más preciso con (**F=8.374; sig ≤ 0.05**) y que explica la mayor cantidad de datos (47.3%) obtenidos durante nuestra investigación. Este modelo es el que usaremos para predecir nuestra variable dependiente (Intención de cumplimiento de las políticas de seguridad (Y)), quedando nuestro modelo de la siguiente forma:

    Y = C0 + C1X1 + C2X2 + C3X3 + C4X4 + E

d. El ANOVA de los modelos de regresión con 3 y 4 variables independientes son las que tienen significancia más pequeña, muy cercana a 0, por tanto son los modelos de regresión más precisos a explicar los datos de nuestra investigación. Por tanto son buenos modelos de predicción de la variable dependiente, Por tanto, es un buen modelo de predicción de la variable dependiente. Se acepta la hipótesis alternativa.

6. Queda demostrado así que La gestión de las conductas y comportamientos de los usuarios de TI tiene un impacto positivo en la concientización para el cumplimiento de las políticas de seguridad de la información en la Universidad Nacional Pedro Ruiz Gallo.

5.2. Recomendaciones

- Tomar como punto de partida la presente investigación para que con la revisión de otras teorías del comportamiento, se logre encontrar otras dimensiones que puedan fortalecer y complementar la investigación realizada.
- La realización de otras investigaciones en instituciones para que se pueda reforzar y complementar la investigación realizada.
- Capacitar al personal administrativo para que se desempeñe óptimamente demostrando mayor integración y compromiso; asimismo, cumpla con las medidas de disuasión establecidas dentro de la institución.

VI. FUENTES Y REFERENCIAS

Bibliografía

Alvarez Lopez, L. (2005). Evaluación, La satisfacción laboral su medición y evaluacion.

Chen, C., Shaw, R., & Yang, S. (2006). Mitigating Information Security Risks by Increasing User Security. *Performance Journal*.

D'Arcy, J., & Tejaswini, H. (2011). "Una revision y Analisis de la teoria de disuasion en la literatura de Seguridad de SI:dando sentido a resultados dispares".

Fishbein, M., & Ajzen. (1975). Belief, attitude, intention, and behavior: An introduction to theory and research. *MA: AddisonWesley*.

French, W., & Bell, C. (1996). *Desarrollo Organizacional.* Mexico: Prentice Hall.

García, M. (2004). *"uso de nuevas Tecnologías de la Informacion en el sevicio de referencia de la biblioteca central de la universidad de Piura".* Lima_Perú.

Glenn, S., & Malagodi, E. F. (1991). Process and Content in Behavioral and Cultural Phenomena. *Behavior and Social Studies*.

Herath, T., & Rao, R. (2009). Motivacion,Protecion y disusion .

Jaik, A., Tena, J. A., & Villanueva, R. (2010). *Revista Electrónica Dialogos Educativos*.

Kreitner, & Kinicki. (1997). *Comportamiento de las Organizaciones.* Madrid: McGraw Hill.

Lee, J., & Lee, Y. (2002). A holistic model of computer abuse within organizations.A holistic model of computer abuse within organizations. *Inform. Management Comput.*

Maslow. (1954). Teoría de la jerarquía de necesidades.

Nuñez, P. (1992). *"Guia metodologica para el estudio de las necesidades de información de los usuarios o lectores".*

Quackenbush, S. (2010). "Teoria de La Disuasión:¿ Dónde estamos?".

Rodriguez, G. (2013). La presión como factor estresor en el entorno laboral Publicitario. *Poliantea*.

Sommestad, T., Hallberg, J., Lundholm , K., & Bengtsson , J. (2013). Las variables que Influyen en el cumplimineto de las politicas de seguridad de la Informacion:Una revision sistematica de los estudios cuantitativos.

Straub, D., & Welke, R. (1998). Coping With Systems Risk: Security Planning Models for Management Decision. *MIS Quarterly*.

Takemura, T. (2011). Empirical Analysis of Behavior on Information Security. International Conference on and 4th.

Theoharidou, M., Kokolakis, S., & Karyda, M. (2005). The insider threat to information systems and the effectiveness of ISO17799. *Computers & Security*.

Whitman, M., Townsend, A., & Aalberts, R. (2001). Information Systems Security and the Need for Policy. *Security Management: Global Challenges in the New Millennium .*

ANEXOS

ANEXO N° 1: **Encuesta Etnográfica**

Proyecto de investigación: La gestión de conductas y comportamientos en los u
de TI y la concienciación en seguridad de la información en la Universidad N

En la siguiente encuesta etnográfica, marque usted con un aspa (X) la respuesta que crea conveniente

Conductas				
	Siempre	**Casi siempre**	**Algunas veces**	**Nunca**
1. En caso que ocurra alguna incidencia, ¿sabe cómo actuar según las políticas de seguridad de la información de la institución donde labora?				
2. En el caso de un incidente, ¿usted realiza el registro respectivo?				
3. Si le derivaran la tarea de registrar un incidente, ¿conoce el procedimiento a realizar?				

4. ¿Si algún compañero que no pertenece a su área o departamento donde labora usted, le pidiera información, le brindaría dicha información?				
5. ¿En alguna ocasión ha tenido que brindar información a personas que no pertenece a su área por orden de su jefe?				
	Si		No	
6. ¿Siente que la capacitación que ha recibido en relación a las políticas de seguridad de la información en los últimos 6 meses le ayudan para resolver cualquier problema o incidente que se presente en su área o departamento?				
7. ¿En alguna ocasión usted ha recibido algún reconocimiento por haber alertado y registrado algún problema relacionado con las políticas de seguridad de la información?				
8. ¿Siente que el compromiso que tiene usted y sus compañeros con el cumplimiento de las políticas de la seguridad de la información es reconocido por sus superiores?				
9. ¿En los últimos 6 meses ha recibido algún reconocimiento por el buen desempeño de sus labores en relación al cumplimiento de las políticas de seguridad? Si es así, ¿qué tan satisfecho está con el reconocimiento?				

10. ¿usted y sus compañeros están satisfechos con el nivel de preparación y capacitación que le brindan sobre políticas de seguridad de la información en el departamento en el que labora?		
	Si	No
11. ¿Si usted notará que su compañero está infringido las políticas de seguridad de la información, reportaría el suceso a su superior?		
12. ¿Si alguno de sus compañeros le pidiera ayuda para registrar algún incidente usted le brindaría su ayuda?		
13. ¿sí se requiere algún tipo de información de la institución, y usted no es la persona encargada de acceder a dicha información le pediría de favor a compañero de trabajo para que le permita acceder a esos datos?		
14. ¿Para usted es tedioso que las unidades de seguridad estén capacitando o implementando nuevos controles permanentemente para velar por la seguridad de la información?		

	Siempre	Casi siempre	Algunas veces	Nunca
15. ¿Su supervisor, o alguien en el trabajo ¿verifica el cumplimiento de los controles de seguridad de la información relacionados a su puesto de trabajo?				
16. ¿En la institución donde labora se establecen las medidas necesarias para analizar, evaluar y gestionar el riesgo de que se ocasionen al incumplir las políticas de seguridad en el desarrollo de sus actividades?				
17. ¿A usted le consideran parte del grupo de personas que evalúan y realizan registro anual de los incidentes que ocurren en el departamento o área en actividades relacionadas con el cumplimiento de las políticas de seguridad de la información?				
18. ¿Usted tiene la posibilidad de plantear mejoras en relación al cumplimiento de las políticas de seguridad de la información?				
19. ¿En alguna ocasión usted ha hecho uso del registro de incidentes para dar solución a algún problema reiterativo en relación a las políticas de seguridad de la información?				

ANEXO N°2: **Encuesta general**

UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO

FACULTAD DE INGENIERIA CIVIL, DE SISTEMAS Y DE ARQUITECTURA

Cuestionario de Tesis

"La Gestión de conductas y comportamientos en los usuarios de TI y la concienciación en la seguridad de la información en la Universidad Nacional Pedro Gallo"

Marcar con un aspa (x) la respuesta que considere de acuerdo a su criterio

Para las siguientes preguntas de la siguiente encuesta, considerar las siguientes escalas:

1	2	3	4	5
Totalmente de acuerdo	**De acuerdo**	**indiferente**	**En desacuerdo**	**Totalmente en desacuerdo**

Nº	ITEMS	VALORACIÓN				
		1	2	3	4	5
INTEGRACION Y COMPROMISO						
1	¿Cuál es el nivel de aceptación que Ud. tiene respecto a los mecanismos y procedimientos planteados por la institución para velar por la seguridad de la información?					
2	¿Está Ud. de acuerdo que la misión o propósito de los lineamientos planteados por la institución donde labora, es que su compromiso se vea reflejado con el cumplimiento de las PSI?					
ENTRENAMIENTO						
3	¿Está Ud. de acuerdo con las técnicas de entrenamiento empleadas por su institución para mejorar su conocimiento respecto a las PSI?					

4	¿Considera Ud. que el nivel de entrenamiento que recibe por parte de su institución debe ser innovada cada cierto tiempo?					
MEDIDAS DE DISUASIÓN						
5	¿Cuál es el nivel de aceptación que Ud. Tiene respecto a que haya un supervisor o alguien del trabajo verifique el cumplimiento de los controles de seguridad de la información relacionados a su puesto de trabajo?					

Nº	ITEMS	VALORACIÓN				
		1	2	3	4	5
INTEGRACION Y COMPROMISO						
6	¿Esta Ud. de acuerdo que con el cumplimiento de las PSI, tiene la oportunidad de hacer mejor su trabajo en el área en el que se desempeña?					
7	¿Considera Ud. que las PSI implementados están acorde a las necesidades del rol que desempeña?					
ENTRENAMIENTO						
8	¿Ud. está de acuerdo que el conocimiento que se tiene respecto al uso de ordenadores, es suficiente para salvaguardar la información?					
9	¿Esta Ud. de acuerdo que los que laboran dentro de la institución debe tener conocimiento de las consecuencias que traen el uso incorrecto de internet como el acceso a páginas web no autorizadas, correo electrónico personal y/o herramientas donde se almacena información confidencial de la institución ?					
10	¿Está de acuerdo con los periodos de capacitaciones respecto a las PSI que recibe de parte de la institución donde labora?					
MOTIVACION						
11	¿Esta Ud. de acuerdo que en el área donde labora haya alguien que motive o aliente el cumplimiento de las PSI?					
12	¿En su opinión, esta Ud. está de acuerdo con el reconocimiento institucional en los últimos días por el cumplimiento de las PSI?					
MEDIDAS DE DISUASIÓN						

13	¿Esta Ud. de acuerdo que en la institución donde labora exista un informe anual que resuma las actividades del cumplimiento de las PSI?					
14	¿En su opinión Ud. está de acuerdo con las medidas preventivas implementadas como rutina en los programas de auditoría y control interno?					
CONCIENCIACION						
15	¿Considera Ud. que la información que recibe y el peligro que supone no cumplir las PSI es suficiente para las tareas y asignaciones diarias según su rol laboral?					
16	¿Considera Ud. que el no conocer las PSI en su rolo dentro de la institución afecta su rendimiento laboral?					
17	¿Siente Ud. que conoce el peligro que supone para la institución, el hecho que no cumpliera las PSI conforme a su rol laboral?					
18	¿Esta Ud. de acuerdo que actualmente se está dando mayor énfasis en el cumplimiento de las PSI dentro de la institución donde labora?					

ANEXO N° 3: **Tabla de Savin y White (fragmento)**

Tamaño de la muestra	**Número de términos (incluida la intersección)**	**D_L**	**D_U**
32	2	1,3734	1,5019
32	3	1,30932	1,57358
32	4	1,24371	1,65046
32	5	1,17688	1,73226
32	6	1,10916	1,81867
32	7	1,04088	1,90931
32	8	0,97239	2,00381
32	9	0,90401	2,10171
32	10	0,83609	2,20255
32	11	0,76897	2,30583
32	12	0,70299	2,41102
32	13	0,63847	2,51758
32	14	0,57573	2,62493
32	15	0,5151	2,73248
32	16	0,45685	2,83963
32	17	0,40129	2,94576
32	18	0,34866	3,05028
32	19	0,29923	3,15253
32	20	0,25319	3,25193
32	21	0,21078	3,34784