UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO
ESCUELA DE POSTGRADO

DOCTORADO EN ADMINISTRACIÓN

Tesis presentada para obtener el Grado Académico de Doctor en Administración

TÍTULO

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN EN FUNCIÓN DEL COMPORTAMIENTO DE LOS USUARIOS DE TECNOLOGÍAS DE LA INFORMACIÓN EN EL SECTOR MICROFINANCIERO DE LAMBAYEQUE

PRESENTADO POR

Ernesto Karlo Celi Arévalo
Regis Jorge Alberto Díaz Plaza

ASESOR

Dr. Juan Manuel Saavedra Tineo

LAMBAYEQUE, PERÚ

FEBRERO - 2017

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN EN FUNCIÓN DEL COMPORTAMIENTO DE LOS USUARIOS DE TECNOLOGÍAS DE LA INFORMACIÓN EN EL SECTOR MICROFINANCIERO DE LAMBAYEQUE

PRESENTADO POR:

M. Sc. ERNESTO KARLO CELI ARÉVALO
AUTOR

M.A. REGIS JORGE ALBERTO DÍAZ PLAZA
AUTOR

DR. JUAN MANUEL SAAVEDRA TINEO
ASESOR

APROBADO POR:

DR. JOSÉ BECERRA SANTA CRUZ
PRESIDENTE DEL JURADO

DR. ARTURO TORRES GALLARDO
SECRETARIO DEL JURADO

DR. IVÁN SALVADOR BRICEÑO
VOCAL DEL JURADO

Febrero, 2017

DEDICATORIA

Es justo y necesario que

después de un trabajo al que se dio tanto tiempo y dedicación,

como es esta investigación,

reconocer a quienes fueron y son la base de mis deseos de superación,

mis hijos María Fernanda, Juan Diego y Dana Rafaela

y mi esposa Ericka,

de quienes quiero reflejar sus virtudes infinitas

y sus grandes corazones que abarcan todo el amor que me brindan.

Ernesto

A mi madre Dorina

Quien siempre se alegra por mis logros

A mis hijos Paula y Gustavo

A mi esposa Mariaeloy

Quienes me brindaron su tiempo para terminar esta tesis

Regis

TABLA DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE GRÁFICOS

RESUMEN

Las entidades financieras en el Perú están obligadas, por mandato, a proteger la información que se genera, almacena y transmite en sus procesos de negocio. Estas entidades implementan sistemas de seguridad que gestionan los riesgos operativos, sobre todo los que provienen de las tecnologías de la información que dan soporte a sus procesos. Sin embargo, estos sistemas no son efectivos para identificar, evaluar y tratar los riesgos que provienen de las amenazas internas, que según las estadísticas son más del 60%, sobre todo en entidades del sector financiero. Una amenaza interna se define generalmente como un empleado, contratista u otro socio comercial actual o anterior, que autoriza o ha autorizado el acceso a la red, al sistema de información o a los datos de la organización y ha utilizado intencionalmente ese acceso para afectar negativamente la confidencialidad, integridad o disponibilidad de la información. Las amenazas internas incluyen sabotaje, robo de información, espionaje, fraude, etc., y a menudo se llevan a cabo a través del abuso de los derechos de acceso, el robo de materiales y la manipulación de dispositivos físicos.

Es vital entonces, que las entidades financieras identifiquen y evalúen los comportamientos de sus empleados, específicamente de los que utilizan algún recurso informático para cumplir con sus funciones y tareas. En este estudio se desarrolló un modelo conceptual que identifica los principales factores que influyen en los comportamientos de los usuarios de TI, ya sean éstos intencionales o no intencionales, para no cumplir con las políticas y normas de seguridad de la información en las organizaciones del sector microfinanciero en la ciudad de Lambayeque Perú. El aporte del modelo es que permite evaluar los factores que influyen en los comportamientos de los usuarios de TI, relacionados con su conducta, influencia del entorno y la percepción que tienen sobre el control instaurado, permitiéndole a los administradores de la seguridad organizacional la comprensión anticipada de tipos de personalidades y las normas de comportamiento de las personas definidas como "usuarios de

TI" lo que facilitará en la detección de desviaciones en estas normas, que generen riesgo de convertirse en una amenaza interna futuras. Para la construcción del modelo se tomó como guía a: (1) Teoría de la Conducta Planificada, (2) Teoría de la Acción Razonada y (3) Teoría de la Disuasión.

Se utilizó la técnica la encuesta para recopilar los datos y como instrumento el cuestionario que fue elaborado por los investigadores y validado a través de una prueba piloto, utilizando el estadístico alfa de Conbrach, a una muestra de 133 usuarios de TI, pertenecientes a 8 entidades microfinancieras, de las cuales 110 fueron válidas, y para el procesamiento de datos se aplicó análisis de correlación obteniéndose que los factores relacionados con el comportamiento intencional tienen un coeficiente de correlación de 0.695 con respecto al cumplimiento de las políticas de seguridad de la información, mientras que los factores relacionados con el comportamiento No intencional obtienen un coeficiente de correlación del 0.564. Pero en conjunto el modelo explica que en una institución microfinanciera los resultados del cumplimiento de las políticas de seguridad de información se debe en 63.9% al comportamiento de los usuarios de tecnología de información compuesta por comportamiento intencional y comportamiento no intencional.

ABSTRACT

Financial entities in Peru are mandated to protect the information that is generated, stored and transmitted in their business processes. These entities implement security systems that manage operational risks, especially those that come from the information technologies that support their processes. However, these systems are not effective in identifying, assessing and addressing the risks that arise from internal threats, which according to statistics are more than 60%, especially in financial sector entities. An internal threat is generally defined as an existing or former employee, contractor, or other business partner who authorizes or has authorized access to the organization's information system or data and has intentionally used such access to adversely affect Confidentiality, integrity or availability of information. Internal threats include sabotage, theft of information, espionage, fraud, etc., and are often carried out through the abuse of access rights, theft of materials and the manipulation of physical devices.

It is vital, therefore, that financial institutions identify and evaluate the behavior of their employees, specifically those who use some computer resource to fulfill their functions and tasks. This study developed a conceptual model that identifies the main factors that influence the behavior of IT users, whether intentional or unintentional, to not comply with information security policies and standards in microfinance organizations, Of the city of Lambayeque Peru. The contribution of the model is that it allows to evaluate the factors that influence the behavior of the IT users, related to their behavior, influence of the environment and the perception that they have on the established control, allowing to the administrators of the organizational security the anticipated understanding Personality types and behavioral norms defined as "IT users", which will facilitate the detection of deviations in these norms, which create the risk of becoming a future internal threat. For the construction of the model was taken

as a guide to: (1) Theory of Planned Behavior, (2) Theory of Reasoned Action and (3) Theory of Deterrence.

The survey was used to collect the data and as a tool the questionnaire that was prepared by the researchers and validated through a pilot test, using the Conbrach alpha statistic, to a sample of 133 IT users, belonging to 8 entities Microfinance institutions, of which 110 were valid, and for data processing, correlation analysis was applied, and factors related to intentional behavior had a correlation coefficient of 0.695 with respect to compliance with information security policies, while that factors related to unintentional behavior obtain a correlation coefficient of 0.564. But overall, the model explains that in a microfinance institution the results of compliance with information security policies are due in 63.9% to the behavior of users of information technology composed of intentional behavior and unintentional behavior.

INTRODUCCIÓN

Las organizaciones son cada vez más conscientes del papel que la información y sus tecnologías asociadas juegan en casi todas las funciones de organización, sobre todo en el impulso de la innovación y la generación de ventajas competitivas (Ahmad, Maynard, & Park, 2014). Sin embargo, también hay que reconocer que la incorporación de tecnologías de la información para dar soporte a los procesos de negocio y a los servicios que se generan a partir de éstos, generan entornos cambiantes para su gobierno y gestión, además de exponerlos a una variedad de riesgos de seguridad, en las que están incluidas por ejemplo, las fugas o robo de información sensible[1], la interrupción prolongada de los servicios de TI (correo electrónico, acceso a Internet, acceso a la base de datos, etc.), lo que resulta en un impacto negativo y significativo para la continuidad del negocio y la disponibilidad, integridad y confidencialidad de la información. Johnston y Warkentin (2010) corroboran esta aseveración al establecer que, dentro del clima de los negocios modernos, las organizaciones comúnmente sufren de amenazas a los datos corporativos, a la infraestructura de tecnología de la información y a la informática personal.

Para hacer frente a estos riesgos de seguridad, una organización debe implementar estrategias de seguridad de la información mediante el establecimiento de un marco global que permita el desarrollo, la institucionalización, la evaluación y la mejora de un programa de seguridad de la información. Para Susanto y Almunawar (2012) la seguridad de la información significa proteger la información y los sistemas de información del acceso, uso, divulgación, alteración, modificación, lectura, inspección, grabación o destrucción no autorizada. Por tanto, la seguridad de la información tiene un papel muy importante en el apoyo a las actividades de la organización.

[1]**Información sensible** esuno de los elementos más importantes para cualquier empresa -sea grande o micro-, ya que en ella se resguardan datos privados de clientes, proveedores y ejecutivos; datos financieros; proyectos en desarrollo; fórmulas de producción; esquemas de productos, entre otros.
Este tipo de información es lo que buscan las personas -externas e internas- que realizan robos de información, por tanto, es la que mejor debe ser protegida por usuarios y corporativos.

Pese a que las organizaciones están utilizando activamente tecnologías para la seguridad de la información, las violaciones que realizan los empleados a las políticas de seguridad de los sistemas de información (SI), es hoy en día una de las principales preocupaciones (Herath y Rao, 2009).

En el Perú, las instituciones financieras que cuentan con la autorización de la Superintendencia de Banca y Seguros (SBS), se encuentra inmersa en el cumplimiento de las normativas emitidas por este ente regulador. Una de estas normativas es la implementación de sistemas de gestión de los riesgos. Entre los riesgos a los que se enfrentan las instituciones financieras, como parte del desarrollo de sus actividades, se encuentra el riesgo operacional, el cual puede generarse por deficiencias o fallas en los procesos internos, en la tecnología de la información, en las personas o por ocurrencia de eventos externos (Ávalos, 2012).

A través de la Resolución SBS N° 37-2008 del 10 de enero de 2008 (SBS, 2008) se aprobó el Reglamento de la Gestión Integral de Riesgos, que establece que las empresas supervisadas por la SBS deben contar con una gestión integral de riesgos adecuada a su tamaño y a la complejidad de sus operaciones y servicios y, mediante la Resolución SBS N° 2116-2009 del 02 de abril del 2009 (SBS, 2008), se aprobó el Reglamento para la Gestión del Riesgo Operacional, la cual es de aplicación para todo el sistema financiero peruano.

Por ello, las empresas de este sector están incorporando procedimientos, métodos y herramientas que les permite aplicar mejores prácticas para gestionar los riesgos operacionales provenientes de la TSI[2], tomando como guía los marcos de referencia ISO/IEC

[2]TSI. Tecnologías y Sistemas de Información.

27001 e ISO/IEC 27005, así como metodologías como: MAGERIT[3], OCTAVE[4], AS/NZS 4360:1999[5], entre otras.

Estos marcos de referencia les permiten determinar niveles de exposición a los riesgos a través de valoraciones cualitativas o cuantitativas de los diferentes elementos considerados en la identificación y evaluación de los riesgos, como son los impactos y las probabilidades de ocurrencia de las amenazas que puede afectar a los activos de TI críticos y, por consiguiente, a los procesos del negocio. A partir de allí, como parte del tratamiento de los riesgos, se identifican los controles y las salvaguardas necesarias para mitigar aquellos niveles de riesgos que están fuera de sus rangos de tolerancia.

Estos procedimientos, que generalmente se plasma en una matriz de gestión de riesgos, logran niveles de efectividad aceptables en la mitigación de amenazas provenientes específicamente de la tecnología (equipos, infraestructura de comunicación, aplicaciones informáticas, base de datos, etc.) y de los procesos (gestión de cuentas de usuario, respaldos de la información, desarrollo de aplicaciones, control de cambios, etc.). Sin embargo, adolecen de técnicas y estrategias para evaluar amenazas provenientes del comportamiento de las personas, específicamente de los usuarios de las TSI, siendo este tipo de amenazas, las que tienen mayor impacto negativo y las que tienen mayor frecuencia de ocurrencia, sin importar si éstas son intencionales o no intencionales.

Si tomamos en cuenta lo sustentado por Herath y Rao (2009) quienes establecen que la eficacia de la seguridad de la información organizacional depende de tres componentes: personas, procesos y tecnología; entonces el componente “personas” no está debidamente

[3]MAGERIT es una metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica de España, muy utilizada en nuestro medio.
[4]OperationallyCriticalThreat, Asset and VulnerabilityEvaluation (OCTAVE, por sus siglas en inglés), es una metodología desarrollada por ComputerEmergency Response Team (CERT), que tiene como objetivo facilitar la evaluación de riesgos en una organización.
[5]AS/NZS 4360:1999 es el Estándar Australiano para la Administración de Riesgos utilizado en varias instituciones en el Perú

gestionado con los procedimientos y técnicas que actualmente las organizaciones del sector financiero han implementado. La regulación de la conducta de los empleados no es nunca una tarea fácil (Herath & Rao, 2009), porque las malas acciones son difíciles de detectar a través de los mecanismos de seguimiento clásicos considerados en los marcos de referencia que se utilizan actualmente en la gestión de la seguridad de la información, puesto que, según Dang-Pham, Pittayachawan& Bruno (2015), la actitud y el mal comportamiento de las personas en el desempeño de su trabajo, recibe influencia de una variedad de factores organizacionales e individuales.

Frente a este contexto, de debilidad existente en las herramientas y metodologías que se utilizan actualmente en la empresas financieras para tratar los riesgos provenientes de los comportamientos y conductas de los usuarios de las TSI, siendo éstos, la principal fuente de generación de amenazas que impactan negativamente en los activos de TI y en el negocio, y debido a la escaza literatura e investigaciones sobre el tema en nuestro medio, este trabajo de investigación se plantea el reto de desarrollar un modelo, a partir de teorías de control de conductas y comportamientos, trabajadas en campos como la psicología, sociología, antropología y en la gestión de recursos humanos, para mejorar la efectividad de los sistemas de gestión de la seguridad de la información y de la gestión de los riesgos operativos de TI.

CAPÍTULO I: EL OBJETO DE ESTUDIO

1.1 UBICACIÓN

Este estudio es una investigación transversal que se desarrolló con información recopilada de empresas microfinancieras del Departamento de Lambayeque - Perú,durante el año 2016.

1.2 DESCRIPCIÓN DEL PROBLEMA

1.2.1 LA SEGURIDAD DE LA INFORMACIÓN EN FUNCIÓN DE LA RELACIÓN NEGOCIO – TECNOLOGÍA DE INFORMACIÓN

Las TSI se han convertido en el elemento más esencial para la supervivencia de las organizaciones, ya que de ellas dependen el buen funcionamiento y la evolución de sus procesos de negocio, así como la información que necesitan para tomar todas sus decisiones operacionales, tácticas y estratégicas (Fernández & Piattini, 2012).

La presencia de las TSI se ha vuelto cada vez más importante a medida que los negocios integran sus procesos con éstas. Las TSI puede ayudar a las empresas en diversos aspectos, tales como: el almacenamiento y recuperación de información, sincronización de trabajo, formación de estrategias de negocio y la comunicación entre sus áreas.

Con el entorno cambiante y las dinámicas competitivas de la actualidad, contar con TSI no supone por sí misma una ventaja competitiva para las organizaciones. Es la gestión de esta tecnología la que puede dar una ventaja o generar un factor diferencial para el éxito de los negocios. Debido a ello, apropiarse de un modelo de gobierno y de gestión de las tecnologías de información (TI), es un elemento clave para el cumplimiento de los objetivos de la empresa.

Hay que reconocer que este mismo entorno cambiante de los escenarios para el gobierno y la gestión de la información y de las tecnologías de información, que dan soporte a

los procesos de negocio y a los servicios que se generan a partir de éstos, generan una variedad de riesgos de seguridad, en las que están incluidas por ejemplo, las fugas o robo de información sensible, la interrupción prolongada de los servicios de TI (correo electrónico, acceso a Internet, acceso a la base de datos, etc.), lo que resulta en un impacto negativo y significativo para la continuidad del negocio y la disponibilidad, integridad y confidencialidad de la información.

El robo de información, el espionaje, el sabotaje, la malversación, el soborno, la corrupción son acciones que se realizan o que involucran el uso de equipos y redes informáticas, por tanto se constituyen en algunos de los retos de la seguridad informática más apremiantes, siendo los ataques causados por los empleados internos y de los contratistas de servicios de TI, los que ocasionan mayores costosos daños (Greitzer et. al., 2010).

Hoy en día son múltiples los riesgos asociados a que equipos y sistemas de información y comunicaciones no cuenten con controles de seguridad. Las amenazas en las TI son globales, y están repartidas en distintos niveles de criticidad según sea la orientación y el ámbito de su utilización. Preocupante es para grandes, medianas y pequeñas organizaciones el espionaje industrial, los ladrones de información, la interrupción de servicios y las fallas críticas en la infraestructura y sistemas centrales de información (Burgos S. & Campos, 2014)

Así mismo, la estrategia de seguridad de la información debe ser compatible con los planes estratégicos de la organización (Ahmad, Maynard, & Park, 2011) y el grado en que los profesionales de la tecnología pueden alinear las acciones de los usuarios finales con los objetivos de seguridad de la información, determinará el nivel de éxito que tiene la organización para hacer frente a las amenazas (Straub & Welke, 1998).

Las actividades maliciosas incluyen una gama aún más amplia de exploits[6], como violaciones de derechos de autor, uso negligente de datos clasificados, el fraude, el acceso no autorizado a información sensible y comunicaciones ilícitas con receptores no autorizados, etc.

IndicanGreitzer et. al. (2010) que la amenaza interna se manifiesta cuando los comportamientos humanos salen de las políticas establecidas, sin importar si es el resultado de una mala intención o de la indiferencia hacia las políticas de seguridad. Por lo general, las conductas negativas de los empleados en relación a la seguridad de la información, está dada por indicadores como: descontento, problemas en el manejo de situaciones complejas, ira, desobediencia a la autoridad, aislamiento, comportamiento confrontacional, estrés, problemas personales, concientización, falta de compromiso e identificación, etc.

1.2.2 LA SEGURIDAD DE LA INFORMACIÓN EN EL SISTEMA FINANCIERO

El sistema financiero es parte de la infraestructura crítica de los países y puede requerir medidas de repuesta a varios niveles, desde la organización hasta la comunidad internacional (Moreno M., 2015). Se entiende al sistema financiero como el conjunto de instituciones encargadas de la circulación del flujo monetario y cuya tarea principal es canalizar el dinero de los agentes superavitarios (ofertantes de fondos) a los agentes deficitarios (demandantes de fondos quienes realizan actividades productivas) (Román R., 2012).

A raíz de los avances en las tecnologías de la información,… los sistemas financieros han aumentado en complejidad. Cada vez resulta más complicado entender el lenguaje de los expertos en finanzas, así como los instrumentos que han creado. No obstante, en esencia, el sistema financiero cumple las mismas funciones que antes (Pacheco, 2012).

[6]Un exploit es un fragmento de software, fragmento de datos o secuencia de comandos y/o acciones, utilizada con el fin de aprovechar una vulnerabilidad de seguridad de un sistema de información para conseguir un comportamiento no deseado del mismo

De acuerdo a Verizon Enterprise Solutions[7], en su *Informe de investigaciones sobre violaciones de datos de 2015* (2015 data breachinvestigationsreport[8]), las tres industrias más afectadas por incidentes de seguridad, repitiéndose los resultados de los tres años anteriores, son: Servicios Públicos, de Información y Financieros. Sin embargo, hace hincapié que ninguna industria es inmune a los fallos de seguridad. Específicamente, sobre las empresas dedicadas a servicios financieros, el informe detalla que durante el 2015 se registraron 642 incidentes en todo el mundo, de los cuales 277 implicaron pérdida de información de manera confirmada.

Uno de los aportes interesantes del *Informe de investigaciones sobre violaciones de datos del 2015* de Verizon, fue considerar el término "motivo secundario" en la explicación de los ataques de las amenazas. Esta terminología la usa para indicar que la víctima que fue blanco de un ataque informático,en realidad fue una víctima secundaria, porque fue utilizado como una forma de avanzar en un ataque diferente contra otra víctima. Por ejemplo, cuando un sitio web es hackeado para servir malware a los visitantes del sitio con la esperanza de que el verdadero objetivo se infectará, es decir, el interés no fue atacar al propietario del sitio web, sino para promover un ataque real a otra víctima. En sus estadísticas, se encuentra que casi el 70% de los ataques donde se conoce un motivo para el ataque incluyen una víctima secundaria. La mayoría de ellos son casos donde servidores se vieron comprometidos para participar en ataques de negación de servicio (DoS), malware del host o ser reutilizados para realizar phishing.

[7]Verizon Enterprise Solutions es una división de VerizonCommunications con sede en BaskingRidge, Nueva Jersey, que ofrece, entre otros, servicios y productos para los negocios y clientes gubernamentales de todo el mundo, en los que se incluye servicios de gestión de seguridad para productos en la nube y de movilidad. Estos incluyen herramientas de gestión de amenazas y servicios de protección, monitoreo, análisis, respuesta a incidentes e investigaciones forenses.

[8]Los data breachinvestigationsreport de Verizon son uno de los informes más consultados por la gran cantidad de empresas aliadas relacionadas con la seguridad de la información y las TI en el mundo para recopilar información. En su reporte 2015 incluye a Perú como uno de los 95 países donde se recopiló información sobre incidentes de seguridad.

De acuerdo al portal oficial de la compañía de seguridad informática Digiware, las instituciones financieras están experimentando un reto exigente en términos de seguridad de la información en nuestros días; la necesidad de contar con servicios especializados y seguros para sus clientes, relaciones de confianza mediante la protección de la privacidad de datos, demostrar cumplimiento de regulación y mejorar la postura en materia de seguridad en donde elementos como los portales transaccionales, la banca móvil, la masificación del crimen como servicio, la mutación del fraude transaccional y la interacción con cientos de proveedores o aliados tecnológicos no dan espera en un mundo más competitivo.

En una de sus estadísticas Digiware informó que el sector financiero pasó del segundo al primer puesto en cuanto a ciberataques en Latinoamérica. Según la empresa de seguridad, el sector financiero en el 2014 registraba el 14.34% del total de ataques en la región, por detrás del sector gobierno. En el 2015, la cifra se eleva por encima del 33,45% del total de hackeos.

La amenaza más potente para las empresas financieras que existe hoy en día se denomina los APT´s[9], estos han generado los grandes ataques de los últimos tiempos, el espionaje corporativo, el robo de información, entre otros.

La problemática de este tipo de ataques se da por la particularidad, lo complejo y su potencia, en primer lugar hace parte de los riesgos latentes y emergentes por lo que tiende ser nuevo para la industria financiera o para la compañía específica. En segundo lugar brindan un complejo reto porque guardan dos consideraciones muy relevantes, el ocultismo y la resiliencia, generando una dificultad para ser detectados, a tal punto que se puede confundir con una leyenda urbana. En tercer lugar tiende a violar fácilmente la seguridad perimetral tradicional

[9]Una amenaza persistente avanzada, también conocida por sus siglas en inglés, APT (por AdvancedPersistentThreat), es un conjunto de procesos informáticos sigilosos y continuos, a menudo orquestados por humanos, dirigidos a penetrar la seguridad informática de una entidad específica. El objetivo de estos ataques es colocar código personalizado malicioso en uno o varios ordenadores para tareas específicas y para no ser detectados durante el período más largo posible.

ya que se basa en firmas, no en comportamientos. Por último, cuando aparecen pueden llegar a afectar la confianza interna y externa, la gestión de los sistemas de información y hasta la sostenibilidad misma de la compañía (Casos como Target 2014, Sony 2012, Yahoo 2014 etc.)(Digiware SA, 2016).

En el último informe de KPMG[10] Perú, resultado de una encuesta para el sector financiero a nivel nacional entre los meses de junio y julio de 2012, se encontraron los siguientes datos: el nivel de incidencia del fraude en Perú es uno de los más altos de la región. El 63% de las personas encuestadas revelaron que sus organizaciones fueron víctimas de fraude durante los últimos 15 meses. En el 15% de los casos los daños económicos superaron los US$500.000. Adicionalmente, el 87% consideran que sus empresas podrían ser víctimas de un fraude. Los fraude cometidos por la alta dirección y gerentes suelen provocar daños económicos más relevantes. Los conflictos de intereses es el esquema de fraude más reportado entre los niveles superiores de las organizaciones (25%). La malversación de activos es el fraude más frecuente, siendo los fraudes con activos financieros los más relevantes, seguido por proveedores y empleados fantasmas. La segunda causa de fraude es la corrupción, destacándose los conflictos de intereses y los sobornos. Luego se ubican la falsificación de documentación, el robo de información confidencial y el fraude informático. **El fraude fue principalmente interno (44%), cometido tanto por los niveles superiores como por empleados de menor jerarquía.** A esto hay que sumarle **la colusión (5%), que involucra a empleados con proveedores y clientes**. Aun en los entornos gobernados por eficientes controles, dos personas en posiciones claves pueden vulnerarlos. El 62% de los encuestados piensan que sus competidores en procesos de compras y contrataciones contactan empleados de la compradora y que se pagan sobornos en su mayoría de hasta el 20% del monto del contrato. Si bien la detección en general se dio por una combinación de medios, el 46% fue detectado por denuncias internas y líneas éticas, seguido por los controles internos. En promedio, las empresas tardaron

[10]KPMG es una firma de servicios profesionales con presencia en más de 150 países. En el Perú ofrece servicios en Auditoría, Tributación & Legal y Consultoría

un año en detectar el fraude, llegando en unos casos a tardar más de 2 años (7%). Cabe destacar que una parte significativa de los empresarios no lograron establecer la duración del fraude. En los casos investigados, apenas el 33% logró identificar plenamente a los responsables y los actos cometidos. Esto pudo deberse a la falta de adecuados protocolos de investigación y a la participación en la resolución de los casos de personal sin el suficiente entrenamiento en auditoria forense(KPMG Asesores S. Civil de R.L, 2012).

En latabla N° 1 se muestran las principales categorías de fraudes que se perpetran en las empresas financieras:

Tabla N° 1. Categorías de fraudes en las empresas financieras

Categoría	Descripción
Malversación de activos	Un empleado actuando solo o en complicidad con otros empleados o terceros, se apropia o abusa de activos pertenecientes a la empresa. (por ejemplo: manipulación de compras y contrataciones, factura falsas, desvío de ventas, robo de productos terminados, efectivo y bancos).
Corrupción	Un empleado abusa de su poder de influenciar decisiones del negocio en beneficio propio y/o de terceros (por ejemplo: sobornos, conflictos de interés).
Falsificación de Informes y documentos	Un empleado oculta o falsifica información que impactan en los estados financieros y en información de gestión de la empresa (por ejemplo: contabilización de ventas falsas, subvaluación de gastos, sobrevalorización de activos, falsificación de solicitudes de crédito, falsificación de soporte documental).
Robo de información confidencial	Un empleado actuando solo, en conjunto o en complicidad con un tercero ajeno a la empresa accede a información clave del negocio con el objeto de comerciar con la misma (Por ejemplo: venta de datos de directores y alta gerencia, planes de negocios, claves, datos de clientes, secretos industriales).

Fuente: (KPMG Asesores S. Civil de R.L, 2012)

La siguiente tabla muestra la distribución de los casos de fraude reportados en la encuesta:

Tabla N° 2. Clases y tipologías de actos fraudulentos que pudieron afectar la organización

Clases y tipologías de actos fraudulentos que pudieron afectar la organización	Porcentaje
Otros fraudes de caja o bancarios	33%
Conflicto de intereses	25%
Empleados/clientes/proveedores inexistentes	24%
Mal uso de información privilegiada	21%
Sobornos y/o retornos	21%
Malversación de activos	18%
Sustracciones en fondos fijos	15%
Compras para uso personal	12%
Cheques falsos o falsificados	10%
Sobrecuentas de gastos	9%
Espionaje industrial y/o comercia	4%
Otros	7%

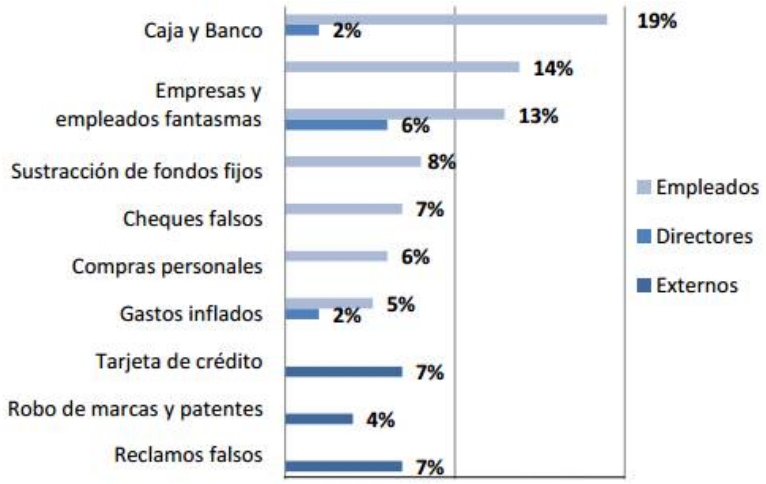
Fuente: (KPMG Asesores S. Civil de R.L, 2012)

A continuación se muestra una serie de gráficos que muestran las estadísticas de los diferentes tipos de fraudes, según el tipo de actor que lo perpetra:

a. Malversación de Activos

En esta categoría se destacan los fraudes que involucran la administración de fondos representando el 29% de los incidentes en caja, bancos y fondos fijos. Lo siguen los casos reportados de empresas y empleados fantasmas. Si bien los casos de piratería y de robo de patentes son menos en cantidad, su impacto suele ser importante

Gráfico N° 1. Actos fraudulentos de malversación de activos en entidades financieras según el tipo de atacante, durante el 2012

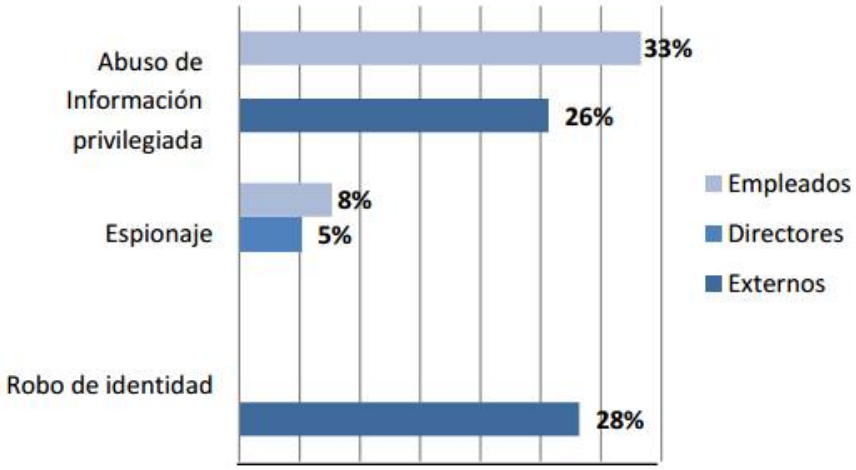


Fuente: (KPMG Asesores S. Civil de R.L, 2012)

b. Robo de información confidencial

Los ejecutivos encuestados también permitieron determinar que el abuso de información privilegiada es un problema en Perú.

Gráfico N° 2. Actos fraudulentos de robo de información confidencial en entidades financieras según el tipo de atacante, durante el 2012

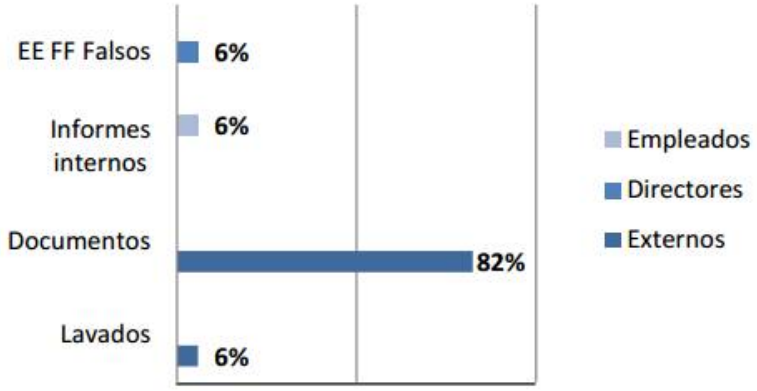


Fuente: (KPMG Asesores S. Civil de R.L, 2012)

c. Falsificación de información y documentación

Los casos de falsificación de documentación lideran este tipo de fraudes. Es de notar que la falsificación de documentación es generalmente un medio para alterar estados financieros, solicitar un crédito, manipular un proceso de compras, presentar reclamos falsos, entre otros. Adicionalmente, observamos el reporte de ciertos casos de falsificación de estados financieros cometidos por directores y gerentes. Esto responde a que por su posición en la organización son los que tienen la posibilidad de cometer este tipo de fraude. Si bien, en cantidad de incidentes el indicador puede ser bajo, cada incidente de estados financieros falsos acarrea serias consecuencias económicas, reputacionales y judiciales para la empresa y sus directivos.

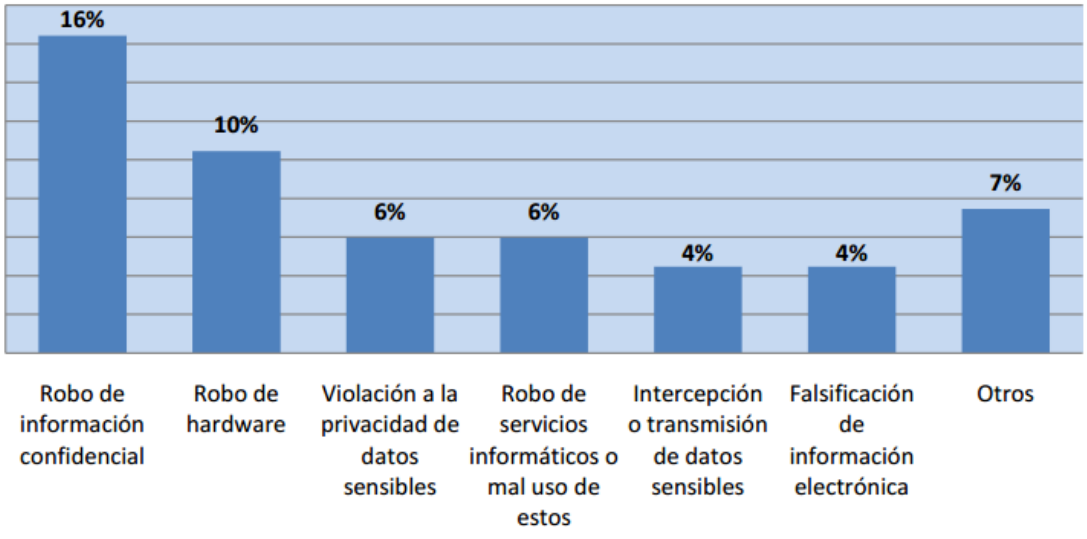
Gráfico N° 3. Actos fraudulentos de falsificación de información y documentación en entidades financieras según el tipo de atacante, durante el 2012



Fuente: (KPMG Asesores S. Civil de R.L, 2012)

Con la mayor dependencia de la tecnología para la administración de los negocios, se incrementa el riesgo de que a través de la manipulación de datos o programas informáticos se busque defraudar a una compañía. El siguiente gráfico refleja que tanto los encuestados saben sobre si su empresa fue víctima de un fraude informático y las modalidades detectadas:

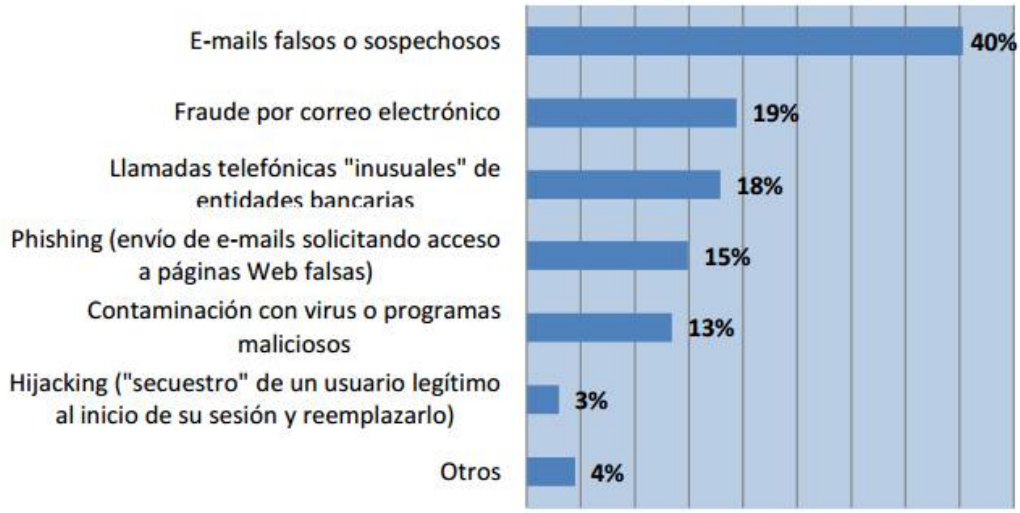
Gráfico N° 4. Modalidades de los delitos informáticos



Fuente: (KPMG Asesores S. Civil de R.L, 2012)

Acerca si los encuestados fueron víctimas de alguna modalidad de delito informático, el 40% confirma haber recibido emails falsos o sospechosos:

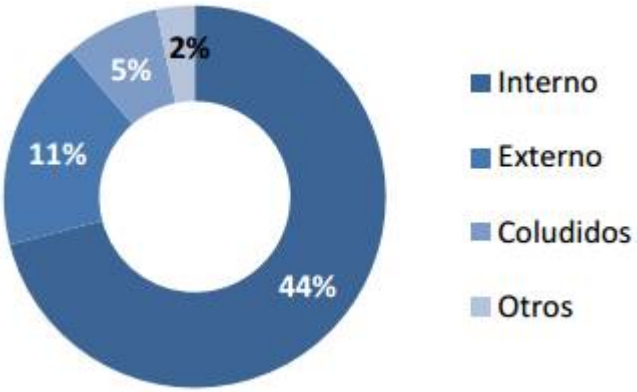
Gráfico N° 5. Formas de ataque para cometer delitos informáticos en entidades financieras



Fuente: (KPMG Asesores S. Civil de R.L, 2012)

Cuestionados sobre la identificación de los responsables, el 62% respondió que sí pudieron determinar si los responsables eran internos, externos, coludidos y otros:

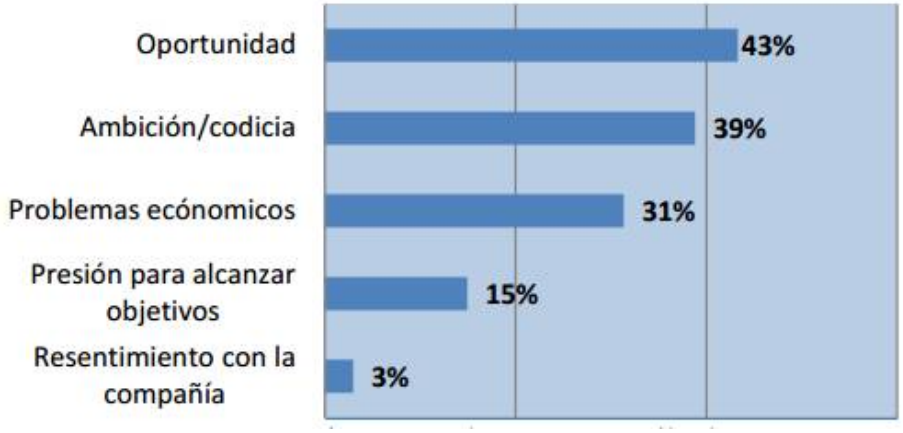
Gráfico N° 6. Responsables de los fraudes en entidades financieras



Fuente: (KPMG Asesores S. Civil de R.L, 2012)

La presión o la motivación no actúan en forma aislada. Un individuo bajo presión necesita una oportunidad real o percibida. Usualmente, los individuos conocen bien el funcionamiento y las debilidades de los sistemas de control interno y pretenden vulnerarlo. Precisamente, en los casos bajo estudio, los encuestados han identificado las oportunidades ofrecidas por las debilidades en los sistemas de control, como el principal motivo por el cual el fraude fue cometido (43%).

Gráfico N° 7. Motivos para cometer el delito en entidades financieras



Fuente: (KPMG Asesores S. Civil de R.L, 2012)

1.2.3 LA GESTIÓN DE RIESGOS DE TI EN LAS ENTIDADES MICROFINANCIERAS PERUANAS

Las microfinancieras han sido un componente clave para la inclusión financiera en los países emergentes como el Perú. Y es que, desde su creación, se han caracterizado por atender a los segmentos de ingresos medios-bajos, principalmente del interior del país.

La industria microfinanciera es más que simples oficinas de coordinación y no sólo debería representar préstamos al sector de la pequeña y micro empresa. Tiene que ver con los diversos tipos de tecnología crediticia, facilidad en el acceso al crédito, rapidez en el servicio

al cliente, financiamiento de capital de trabajo, relación financiera a largo plazo, garantías, redes empresariales, asociatividad empresarial, adecuados controles internos y administración de riesgos empresariales (Martínez S., 2009).

Según el Comité de Basilea[11], las crisis económicas y financieras de los últimos años unidas al desarrollo, la evolución y la innovación de las operaciones y de las instituciones bancarias y financieras, dieron lugar a riesgos más complejos, por lo que se requería un nuevo marco de adecuación de capital, ya que Basilea I no era suficientemente sensible a los riesgos (Cruz M. & Alarcón A., 2015).

En tal virtud, los gobernadores de bancos centrales y las autoridades de supervisión bancaria del Grupo de los Diez (G-10) se reunieron y aprobaron la publicación del nuevo marco para la adecuación del capital, conocido como Basilea II[12].

El Nuevo Acuerdo de Capital o Basilea II es una serie de principios y recomendaciones del Comité de Basilea sobre Supervisión Bancaria cuyo objetivo es propiciar la convergencia regulatoria hacia los estándares más eficaces y avanzados sobre medición y gestión de los principales riesgos en la industria bancaria.

En abril de 2003, la SBS decidió asumir el reto de la implementación y adecuación de lo propuesto por el comité de Basilea y estableció el Comité Especial Basilea II (CEB), en el cual se encuentran representadas las diversas áreas de la Superintendencia involucradas.

[11]El Comité de Basilea es la denominación usual con la que se conoce al Comité de Supervisión Bancaria de Basilea (BCBS, sigla de BaselCommitteeonBankingSupervision en inglés), la organización mundial que reúne a las autoridades de supervisión bancaria, cuya función es fortalecer la solidez de los sistemas financieros.

[12]El propósito de Basilea II, publicado inicialmente en junio de 2004, es la creación de un estándar internacional que sirva de referencia a los reguladores bancarios, con objeto de establecer los requerimientos de capital necesarios para asegurar la protección de las entidades frente a los riesgos financieros y operativos.

La SBS con la finalidad de establecer criterios mínimos ha considerado conveniente establecer las siguientes disposiciones(SBS, 2008)(SBS, 2009):

1. Resolución SBS N° 37-2008 del 10 de enero de 2008, donde se aprueba el Reglamento de la Gestión Integral de Riesgos, que establece que las empresas supervisadas deben contar con una gestión integral de riesgos adecuada a su tamaño y a la complejidad de sus operaciones y servicios y

2. Resolución SBS N° 2116-2009 del 02 de abril del 2009, se aprueba el Reglamento para la Gestión del Riesgo Operacional, la cual es de aplicación para todo el sistema financiero peruano.

3. Circular N° G-139-2009-Gestión de la continuidad del negocio, se establecen los criterios mínimos para la gestión de la continuidad del negocio, que forma parte de una adecuada gestión del riesgo operacional que enfrentan las empresas del sector financiero. la SBS considera establecer una serie de disposiciones, las cuales toman como referencia estándares internacionales como el BS-25999[13].

4. Circular N° G-140-2009- Gestión de la seguridad de la información, en ella se establecen los criterios mínimos para una adecuada gestión de la seguridad de la información. la SBS considera conveniente establecer una serie disposiciones, las cuales toman como referencia estándares internacionales como el ISO 17799 e ISO 27001[14].

Para ello, las empresas financieras deben aplicar las disposiciones que se establezcan en las normas específicas sobre estos temas.

[13]BS-25999: en la actualidad la BS-25999 ya no es vigente, porque la que rige hoy en día sobre continuidad del negocio es la ISO 22301.
[14]ISO 17799: Esta norma todavía es vigente en Perú por la norma técnica peruana, pero es reemplazada por la norma ISO 27002.

Debido a esta estricta regulación, estas instituciones deben integrar todos sus sistemas para otorgar a los clientes un servicio de seguridad en el manejo de su dinero. Se les exige implementar controles para el aseguramiento de la fiabilidad, confidencialidad y disponibilidad de la información de sus clientes; así como de la continuidad de sus procesos críticos, como créditos, operaciones, recuperaciones, etc.

Estas entidades implementan sistemas de gestión de riesgos de TI, que es uno de los tipos de riesgo operacional, que permiten identificar brechas de seguridad de la información a través del cálculo de los niveles de riesgo inherente (antes de la implementación de controles) y residual (después de la implementación de controles), que están relacionadas más con los activos de TI que se tienen que proteger para cumplir con las exigencias de la SBS.

Sin embargo, la mayor cantidad de amenazas (aproximadamente el 70%) provienen de los usuarios internos de la organización, los cuáles no son contemplados ni evaluados en los sistemas descritos anteriormente.

1.3 FORMULACIÓN DEL PROBLEMA

En base al problema descrito, formulamos el siguiente problema de investigación:¿Cómo mejorar el cumplimiento de las políticas de seguridad de tecnologías de información a través de la gestión del comportamiento de los usuarios de TI en las organizaciones del sector microfinanciero de la ciudad de Lambayeque, Perú?

1.4 JUSTIFICACIÓN E IMPORTANCIA DEL ESTUDIO

La presente investigación se justifica desde las siguientes perspectivas:

Relevancia social

De acuerdo a las normativas impuestas por la SBS en Perú, las entidades financieras tienen que garantizar a sus usuarios y clientes la disponibilidad, integridad y confidencialidad de la información relacionada con los activos y las transacciones de sus los ahorros y créditos, y a su vez la continuidad de los procesos de la entidad.

Las técnicas que aplican para ello, de acuerdo a la problemática descrita, solo evalúan y miden las exposiciones a los riesgos, en base a información de los registros de incidencias o informes de la evaluación de sus controles. En el caso específico de los riesgos operacionales de tecnologías de información, evalúan y miden la exposición al riesgo de las fuentes de amenazas y las actuaciones de las mismas, relacionadas con los sistemas informáticos, infraestructura tecnológica, desastres naturales, malos diseños o planificaciones, etc. Sin embargo, tienen debilidades para medir las amenazas provenientes de los comportamientos y conductas de los usuarios internos de TI.

Esta investigación tiene relevancia social porque sus resultados servirán como guía de referencia para que los responsables diseñen sus procedimientos de gestión de riesgos de TI, con la inclusión de estrategias, técnicas y controles para la gestión de las amenazas provienen de los comportamientos de los usuarios finales de las TSI.

Aporte teórico

Las investigaciones relacionadas con el comportamiento intencional y no intencional de los usuarios de las TSI y su influencia en el cumplimiento de normas de

seguridad, han sido poco estudiadas por lo que genera una expectativa por la validación de un modelo en el sector financiero.

El aporte teórico de esta investigación es la elaboración de constructos teóricos que identifican y explican factores que contribuyen a explicar el comportamiento no intencional y mal intencionado de los trabajadores que hacen uso de las TSI, cumpliendo alguna función operativa, en las empresas microfinancieras; distinguiendo los factores que motivano inhibendichos comportamientos.

Estos constructos teóricos se desarrollarán en base al cuerpo de las teorías revisadas, como son: Teoría de la Elección Racional (TER), Teoría de la Conducta Planificada (TCP) y Teoría General de la Disuasión (TGD).

CAPÍTULO II: MARCO TEÓRICO

1.1. ANTECEDENTES A LA INVESTIGACIÓN

1.1.1. ANTECEDENTES RELACIONADOS CON EL SECTOR MICROFINANCIERO EN EL PERÚ Y LAMBAYEQUE

La pretensión de esta revisión de antecedentes es identificar cuál es el marco normativo que rige o determina las formas, responsabilidades y obligaciones de las empresas del sector financiero en el Perú en relación a la seguridad de la información y a la gestión de los riesgos operativos de TI.

a. Basilea I (1998)

El Comité de Basilea forma parte del Banco Internacional de Pagos (BIS por sus siglas en inglés) y fue creado por acuerdo de los representantes de los Bancos Centrales de los 10 países más industrializados con el propósito de formular una serie principios y estándares de supervisión bancaria, los que han sido acogidos no solamente por los países miembros, sino por la mayoría de países en el mundo.

Las normas de Basilea I son recomendaciones elaboradas por el Comité de Basilea, para establecer las condiciones mínimas que una entidad bancaria debería tener para asegurar su estabilidad. Establecía que el principal riesgo era el riesgo de crédito, y se calculaba agrupando las exposiciones de riesgo en 5 categorías según la contraparte y asignándole una «ponderación» diferente a cada categoría (0%, 10%, 20%, 50%, 100%), la suma de los riesgos ponderados formaba los activos de riesgo.

Su principal recomendación se trataba de un conjunto de recomendaciones para establecer un capital mínimo que debía tener una entidad bancaria en función de los riesgos que afrontaba.

b. Basilea II (2004)

Su principal aporte es la creación de un estándar internacional que sirva de referencia a los reguladores bancarios, con objeto de establecer los requerimientos de capital necesarios para asegurar la protección de las entidades frente a los riesgos financieros y operativos. Basilea II es un marco de referencia para la gestión de riesgos.

Los objetivos de Basilea II más destacados son:

- Promover seguridad en el sistema financiero.
- Construir una aproximación más completa hacia el cálculo de riesgo.
- Plantear métodos más sensibles al riesgo.

Basilea II reconoce que dentro de los tipos de riesgos en una organización, los riesgos tecnológicos son los que ocurren con mayor frecuencia y los que causan más daño.

c. Basilea II en el Perú

El Perú, por medio de la SBS, es consciente de las ventajas en seguridad y estabilidad que genera un esquema como el propuesto en Basilea II y no está al margen de esta reforma internacional de la regulación bancaria. El cronograma de implementación seguido en Perú se inició en el año 2007 con los estudios de impacto y la emisión de la normativa necesaria para la implementación del NAC[15]. Esta primera fase duró hasta junio del 2009 y a partir de julio del 2009 entró en vigencia del método estandarizado para riesgo de crédito y riesgo de mercado, y el método básico y estándar alternativo para riesgo operacional. Asimismo, es a partir de esta fecha que las empresas pueden postular para el uso de modelos internos.

A raíz de la crisis financiera internacional del 2008, que evidenció la necesidad de fortalecer la regulación, supervisión y gestión de riesgos del sector bancario, el Comité de

[15]NAC (Nuevo Acuerdo de Capital): propone adecuar la forma de calcular el capital regulatorio a una forma más acorde con los estándares actuales en el manejo del riesgo.

Basilea inició en el 2009 la reforma de Basilea II, actualmente llamada Basilea III. En este sentido, la SBS actualmente está evaluando la implementación de estos cambios de acuerdo a la realidad peruana.

d. Basilea III

Basilea III es un conjunto integral de reformas elaborado por el Comité de Supervisión Bancaria de Basilea para fortalecer la regulación, supervisión y gestión de riesgos del sector bancario. Estas medidas persiguen:

- Mejorar la capacidad del sector bancario para afrontar perturbaciones ocasionadas por tensiones financieras o económicas de cualquier tipo.
- Mejorar la gestión de riesgos y el buen gobierno en los bancos.
- Reforzar la transparencia y la divulgación de información de los bancos.

e. Ley 26702

Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros.

Las empresas que componen los componentes son bancos, financieras, cajas municipales de ahorro, cajas de ahorro y crédito, cajas municipales de ahorro y crédito, cooperativas de ahorro y EDPYMES. La presente ley no alcanza al Banco Central.

f. Resolución SBS 0037-2008 Reglamento de la Gestión Integral de Riesgos

La gestión integral de riesgos es un proceso, efectuado por el Directorio, la Gerencia y el personal aplicado en toda la empresa y en la definición de su estrategia, diseñado

para identificar potenciales eventos que pueden afectarla, gestionarlos de acuerdo a su apetito por el riesgo y proveer una seguridad razonable en el logro de sus objetivos.

La Gestión Integral de Riesgos considera las siguientes categorías de objetivos:

- Estrategia: Son objetivos de alto nivel, vinculados a la visión y misión empresarial.
- Operaciones: Son objetivos vinculados al uso eficaz y eficiente de los recursos.
- Información: Son objetivos vinculados a la confiabilidad de la información suministrada.
- Cumplimiento: Son objetivos vinculados al cumplimiento de las leyes y regulaciones aplicables.

Las empresas deben efectuar una gestión integral de riesgos adecuada a su tamaño y a la complejidad de sus operaciones y servicios.

g. Resolución SBS 2116 - 2009 Reglamento para la gestión de riesgo de operación

Como parte de una adecuada gestión del riesgo operacional, las empresas deben implementar un sistema de gestión de la continuidad del negocio que tendrá como objetivo implementar respuestas efectivas para que la operatividad del negocio de la empresa continúe de una manera razonable, ante la ocurrencia de eventos que pueden crear una interrupción o inestabilidad en las operaciones de la empresa.

Asimismo, las empresas deben contar con un sistema de gestión de la seguridad de la información, orientado a garantizar la integridad, confidencialidad y disponibilidad de la información.

Para ello, las empresas deberán aplicar las disposiciones que se establezcan en las normas específicas sobre estos temas.

h. Circular N° G-139-2009 Gestión de la continuidad del negocio

Con la finalidad de establecer criterios mínimos para la gestión de la continuidad del negocio, que forma parte de una adecuada gestión del riesgo operacional que enfrentan las empresas del sector financiero, la SBS considera establecer una serie de disposiciones, las cuales toman como referencia estándares internacionales como el BS-25999[16].

Según el artículo 3°"la gestión de la continuidad del negocio es un proceso, efectuado por el Directorio, la Gerencia y el personal, que implementa respuestas efectivas para que la operatividad del negocio de una empresa continúe de una manera razonable, con el fin de salvaguardar los intereses de los principales grupos de interés, ante la ocurrencia de eventos que pueden crear una interrupción o inestabilidad en las operaciones de la empresa".

Las empresas deben realizar una gestión de la continuidad del negocio adecuada a su tamaño y a la complejidad de sus operaciones y servicios.

i. Circular N° G-140-2009 Gestión de la seguridad de la información

Con la finalidad de establecer criterios mínimos para una adecuada gestión de la seguridad de la información, la SBS considera conveniente establecer una serie disposiciones, las cuales toman como referencia estándares internacionales como el ISO 17799 e ISO 27001[17].

Según el artículo 3° "las empresas deberán establecer, mantener y documentar un sistema de gestión de la seguridad de la información (SGSI)".

[16]BS-25999: en la actualidad la BS-25999 ya no es vigente, porque la que rige hoy en día sobre continuidad del negocio es la ISO 22301.
[17]ISO 17799: Esta norma todavía es vigente en Perú por la norma técnica peruana, pero es reemplazada por la norma ISO 27002.

Las actividades mínimas que deben desarrollarse para implementar el SGSI, son las siguientes:

- Definición de una política de seguridad de información aprobada por el Directorio.
- Definición e implementación de una metodología de gestión de riesgos, que guarde consistencia con la gestión de riesgos operacionales de la empresa.
- Mantenimiento de registros adecuados que permitan verificar el cumplimiento de las normas, estándares, políticas, procedimientos y otros definidos por la empresa, así como mantener pistas adecuadas de auditoría.

Podemos destacar de que en este marco normativo que rige en Perú, no se hace referencia a los controles relacionados con el comportamiento de los usuarios de TI.

1.1.2. ANTECEDENTES RELACIONADOS CON LA GESTIÓN DEL COMPORTAMIENTO EN SEGURIDAD DE LA INFORMACIÓN

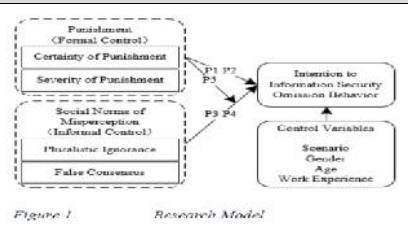
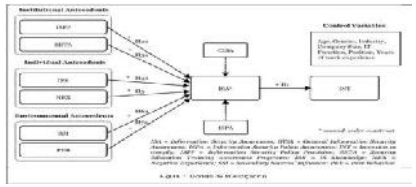
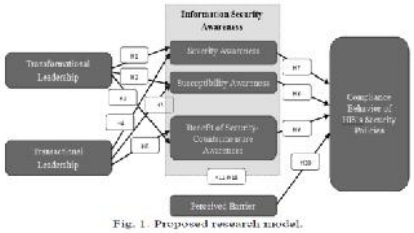
Aunque el interés por la seguridad de SI ha aumentado en los últimos años, poca investigación empírica ha examinado este problema (Vance, 2010). Sin embargo, muy recientemente, los profesionales y académicos han comenzado a darse cuenta de que la seguridad de información no se puede lograr sólo a través de herramientas tecnológicas, pues la eficacia de la seguridad de la información organizacional depende de tres componentes: personas, procesos y tecnología (Herath & Rao, 2009).

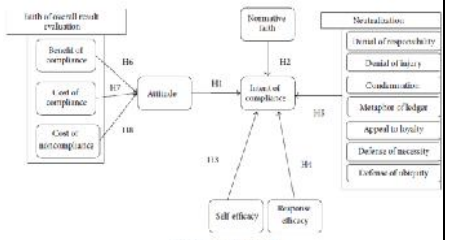
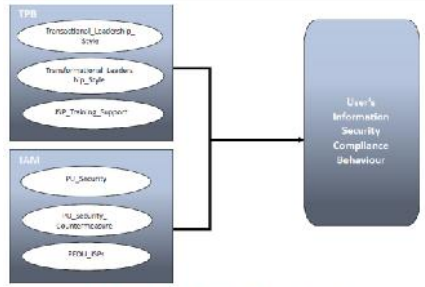
Con los avances en las tecnologías de seguridad, muchos de los comportamientos de computación, tales como la gestión de parches y actualizaciones de antivirus están siendo automatizados para reducir los conocimientos y los tiempos de las tareas de los usuarios finales. Sin embargo, los comportamientos como el uso adecuado de los recursos informáticos y de red, los hábitos de contraseñas adecuadas, etc., que no puede ser abordado por las tecnologías de seguridad a menudo se tratan a través de programas de concientización en

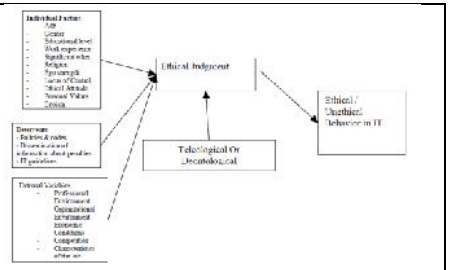
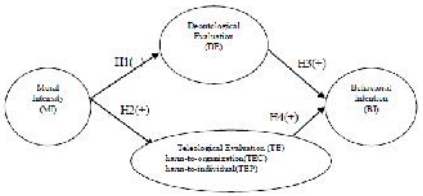
seguridad de la información. Sin embargo, la investigación empírica sobre las conductas de seguridad de los usuarios finales y los factores que influyen en ellas todavía está en su infancia (Cheng&Hsu, 2013).

Para ahondar sobre los fundamentos teóricos que sustentan los pocos trabajos sobre comportamientos de los usuarios de las tecnologías de la información en relación al cumplimiento de las políticas de seguridad, se realizó una exploración de trabajos de investigación relacionados con el tema, con la finalidad de analizar sus aportes, sus resultados, los instrumentos de recopilación aplicados y las pruebas de sus hipótesis, los mismos que se resumen a continuación:

Tabla N° 3. Catálogo de antecedentes de la investigación

Título de la fuente revisada	Fundamento teórico	Aporte	Modelo Estadístico	Cuestionario	Modelo conceptual de la investigación
Understanding organization employee`s information security omission behavior an integrated model of social norm and deterrence(Yayla, 2011)	- Teoría de control de la organización - Teoría general de la disuasión - Teoría de la norma social	- Identifica determinantes potenciales de la intención en la conducta de los empleados sobre la omisión de la seguridad de la información en relación a la implementación de controles formales e informales - Construye un modelo que integra la Teoría de la disuasión y la Teoría de la Norma Social	No cuantifica sus resultados	No aplica	
Information security awareness: its antecedents and mediating effects on security compliant behavior(Haeussinger & Kranz, 2013)	- Conciencia en seguridad de la información	Realiza una evaluación de los antecedentes relacionados con los empleados de una organización, desde tres perspectivas: institucional, individual y del entorno, en relación a la influencia en su comportamiento	Aplica un modelo de ecuaciones estructurales para cuantificar sus resultados	Si aplica	
Leadership Styles and Information Security Compliance Behavior. The Mediator Effect of Information Security Awareness(Humaidi & Balakrishnan, 2015)	- Teoría del liderazgo	Modelo empírico de aplicación de la Teoría de Liderazgo para determinar el impacto de la concienciación en seguridad de la información sobre el comportamiento de cumplimiento de las políticas de seguridad de la información	Aplica Modelo BIAS para estimar tendencias o sesgos	No aplica	
Towards a complete understanding of information security misbehaviours: a proposal for future research with social network approach(Dang-Pham, Pittayachawan, & Bruno, 2014)	- Teoría de la disuasión - Teoría del razonamiento causal - Teoría de la vinculación social - Ciclo de acción de la seguridad	- Identifica factores intrínsecos y extrínsecos que determinan el mal comportamiento de los empleados en relación al cumplimiento de las políticas de seguridad	Es una investigación exploratoria	No aplica	No aplica a este tipo de investigación

Cultural Values, Information Sources, and Perceptions of Security(Mason & Dupuis, 2014)	- Valores culturales - Fuentes de información sobre un evento actual - Percepción de la seguridad nacional: Caso Edward Snowden	- Aplicación de las medidas de los valores culturales de Hofstedepara estimar la distancia de poder y la individualidad	Es una investigación exploratoria	Si aplica	No aplica a este tipo de investigación
An Integrative Behavioral Model of Information Security Policy Compliance(Kim, Yang, & Park, 2014)	- Teoría de la neutralización - Teoría de la conducta planificada - Teoría protección - motivación	- El estudio desarrolla un enfoque interdisciplinario combinando la psicología y la investigación de seguridad del sistema de información - Se sugieren definiciones operativas concretas para influir en los factores para el cumplimiento de la política de seguridad de la información a través de las teoríasque aplica. - Proporcionauna guía para apoyar la ejecución exitosa del establecimiento estratégico para la implementación de políticas de seguridad de sistemas de información en las organizaciones - Demuestra que los programas de educación y formación suprimen o neutralizan la intención de los miembros para violar la política de seguridad de la información	Aplica un modelo de ecuaciones estructurales para cuantificar sus resultados	Aplica, pero no lo brinda	 Figure 1: Research Model.
Exploratory Factor Analysis of User's Compliance Behaviour towards Health Information System's Security (Humaidi & Balakrishnan, 2013)	- Teoría general de la disuasión - Modelo del modelo de aceptación	Realiza un estudio preliminar para identificar los posibles factores que pueden afectar el comportamiento de cumplimiento del usuario hacia la seguridad de la información en términos de dos aspectos: apoyo a la gestión y la tecnología de seguridad. Se aplica básicamente dos teorías: Teoría del Comportamiento Planeado y la Teoría del Modelo de Aceptación.	Aplica Alfa de Cronbach Análisis de componentes principales con rotación Promax Análisis factorial	Aplica el test de Kaiser-Mayer-Olkin (KMO) y las Pruebas de Bartlett	 Figure 1: The Integrated Research Framework.

Evaluation of Ethical Issues in the Knowledge Age- An Exploratory Study(Bethune & McCarthy, 2013)	- Teoría general de la disuasión	- Propone un modelo integral de la conducta ética de los trabajadores del conocimiento integrando factores individuales, factores de disuasión y las variables externas - Desarrolla estrategias de afrontamiento para manejar las cuestiones éticas en la era del conocimiento			
How Did Ethical Evaluation Work As a Mediator between Moral Intensity and Decision Making(Su, 2013)	- Intensión moral - Modelo de decisión ética - Evaluación deontológica - Evaluación teleológica	Desarrolla una evaluación deontológica y teleológica de la intensión ética y la intensidad ética de los profesionales que desarrollan tecnologías de información	Medición de confiabilidad con Alfa de Cronbach Multicolinealidad	Aplica un cuestionario para evaluar 3 escenarios relacionados a la investigación ética: propiedad, privacidad y precisión, utilizando una escala Likert de 7 puntos	

Antecedente n° 1

Título	Controlando las amenazas internas con las políticas de seguridad de la información
Entidad	Universidad Binghamton - Suny
Fecha	2011
Responsable	YaylaAliAlper
Logros y/o resultados obtenidos	En este trabajo se presenta un marco de referencia que tiene como objetivo controlar las amenazas internas intencionales, donde se usa mecanismos de control social y de comportamiento, medidas de disuasión donde se proponen como posibles medidas para controlar las amenazas intencionales.
Análisis de relación con la presente investigación	La relación con la investigación es que este trabajo propone un marco para el control de las amenazas internas a la seguridad de la información que nos permitirá identificar dimensiones que evaluarán conductas de los usuarios.

Antecedente n° 2

Título	Eficacia de los métodos de sensibilización seguridad de información, métodos basados en las teorías psicológicas
Entidad	Universidad Rey Saud, Arabia Saudita
Fecha	2011
Responsable	Bilal Khan, Khaled S. Alghathbar, Syed IrfanNabiand Muhammad Khurram Khan
Resumen	Esta investigación es un estudio teórico de la conciencia de seguridad de la información basado en la teoría del comportamiento planificado y la teoría de la acción razonada. El estudio muestra que las teorías tratadas pueden usarse para hacer métodos de conciencia de seguridad de información más eficaces.
Análisis de relación con la presente investigación	La relación con la investigación es que nos permitirá realizar un modelo que integra al modelo (KAB)[18] y la teoría del comportamiento planificado para lograr el deseado cambio en el comportamiento.

[18]Modelo (KAB): modelo de conocimiento, actitud y conocimiento.

Antecedente n° 3

Título	Modelo de comportamiento integral de información sobre el cumplimiento de políticas de seguridad
Entidad	Universidad Kwangwoon - China
Fecha	2014
Responsables	Sang Hoon Kim, Kyung Hoon Yang, Sunyoung Park
Resumen	En esta investigación, los autores plantean factores de comportamiento que influyen en el cumplimiento de los miembros de la organización, donde se utilizan diversas teorías como: Teoría de la neutralización, Teoría de la acción planeada, Teoría del comportamiento planificado, Teoría de motivación de la protección y la Teoría de la elección racional. El estudio sugirió definiciones operacionales concretas de factores que influyen en la seguridad de la información y el cumplimiento de la política a través de una exhaustiva revisión teórica.
Análisis de relación con la presente investigación	La relación con esta investigación nos proporciona una guía para establecer estratégicamente políticas de seguridad de la información.

Antecedente n° 4

Título	Concienciación en seguridad de la Información, antecedentes para medir efectos sobre la seguridad compatible con el comportamiento
Entidad	Universidad de Goettingen
Fecha	2013
Responsable	Haeussinger, Kranz
Logros y/o resultados obtenidos	Este estudio está fundamentado en conciencia en seguridad de la información. Se realizó una evaluación a través de un cuestionario para saber los antecedentes relacionados con los empleados de una organización, bajo tres perspectivas: institucional, individual y del entorno, en relación a la influencia en su comportamiento. También se aplicó un modelo de ecuaciones estructurales para cuantificar sus resultados
Análisis de relación con la presente investigación	La relación con la investigación es que podríamos utilizar ciertas preguntas del cuestionario para evaluar a los usuarios de TI de sectormicrofinanciero y encontrar las influencias en su comportamiento bajo las 3 perspectivas mencionadas.

Antecedente n° 5

Título	Conciencia de seguridad de información. Herramientas de marketing para procesos de negocio en empresas.
Entidad	Universidad de Brunei
Fecha	2012
Responsable	HeruSusanto, Mohammad Nabil Almunawar
Resumen	Este estudio está fundamentado en conciencia de seguridad de la información con uso de herramientas de marketing para procesos de negocio, donde se discuten temas de tecnología de la información, apoyo a la comercialización para el entorno empresarial con un impacto en los procesos de negocios en el entorno empresarial. Aquí se desarrolló un software de medición en el entorno empresarial, a la protección de la información y sistemas de información.
Análisis de relación con la presente investigación	Esta investigación es muy útil porque nos permite usar un modelo con herramientas integrales de la conducta ética, para las mejoras en el control de las conductas de los usuarios de TI en el cumplimiento de las políticas de seguridad en las empresas del sector microfinanciero.

Antecedente n° 6

Título	Impacto de medidas preventivas de seguridad en convergencia de información organizativa
Entidad	Universidad de Indiana
Fecha	2012
Responsable	NeamenBerhanu, IvyTech
Resumen	Este estudio usa la Teoría de la disuasión general para explorar como las contramedidas de seguridad impactan e influyen en una organización, y a su vez cómo afectan el desempeño de la conciencia de seguridad.
Análisis de relación con la presente investigación	La relación con la investigación es que nos sirve de ayuda ya que nos permite ver como la teoría de disuasión tiene impacto sobre el desempeño de un usuario de TI en una organización.

Antecedente n° 7

Título	Apelaciones de temor y comportamiento de seguridad de la información. Un estudio empírico
Entidad	Universidad de Alabama en Birmingham
Fecha	2010
Responsable	Allen C. Johnston
Resumen	Esta investigación plantea el modelo de infusión del comportamiento que ve la influencia de las apelaciones de miedo en el cumplimiento de los usuarios finales con las recomendaciones para promulgar medidas específicas de seguridad informática individuales hacia la mitigación de amenazas.
Análisis de relación con la presente investigación	Este trabajo de investigación nos ayuda con la construcción de un modelo conceptual que representa la infusión de comportamiento de adopción de la tecnología. Donde desarrollamos estrategias de afrontamiento para manejar las cuestiones éticas del comportamiento.

Antecedente n° 8

Título	Evaluación de aspectos éticos en la era del conocimiento: Un estudio exploratorio
Entidad	Universidad de Quinnipiac
Fecha	2013
Responsable	Berthune, Richard V. McCarthy
Resumen	Esta investigación explora la percepción ética del conocimiento, también examina los efectos de los elementos de la teoría de disuasión que determinan las diferencias en las percepciones éticas que pueden explicarse con variables.
Análisis de relación con la presente investigación	Este trabajo de investigación es muy útil porque nos permite usar un modelo integral de la conducta ética de los empleados integrando la disuasión con el afrontamiento para mejorar las cuestiones éticas en la era del conocimiento.

Antecedente n° 9

Título	Delitos informáticos y encuesta de seguridad
Entidad	
Fecha	2008
Responsable	Robert Richardson
Resumen	En esta investigación se han realizo diversas muestras correspondientes a la seguridad informática que muestran los resultados de las empresas que sufren ataques debido a los delitos informáticos donde se hace uso de controles concernientes a conductas de los usuarios de TI para el cumplimiento de las políticas de seguridad.
Análisis de relación con la presente investigación	La relación con esta investigación nos ayuda a proporcionar una guía para establecer las políticas de seguridad de la información, donde podemos desarrollar estrategias de afrontamiento para manejar las cuestiones éticas de los controles de comportamiento.

Antecedente n° 10

Título	Apelaciones de temor y comportamiento de seguridad de la información. Un estudio empírico
Entidad	Universidad de Alabama en Birmingham
Fecha	2010
Responsable	Allen C. Johnston
Resumen	Esta investigación ayuda a mejorar las conductas de los usuarios de TI para el cumplimiento de las políticas de seguridad en las empresas micro financieras que están siendo afectados por ciertos tipos de daños o pérdidas que se conoce como "riesgo de sistemas", aquí se muestra una amplia gama de controles disponibles para implementar los controles más eficaces haciendo de estudios cualitativos comparativos. Este programa de seguridad que se basa en la teoría incluye el uso de un modelo de planificación de riesgos de seguridad, la educación / formación en la conciencia de seguridad, y el análisis de la matriz de contramedidas.
Análisis de relación con la presente investigación	Este trabajo de investigación es muy útil porque nos permite usar un modelo de planificación de la conducta ética sobre los usuarios para mejorar las cuestiones éticas en la era del conocimiento.

De los antecedentes revisados podemos afirmar que aunque muchas organizaciones enfocan sus esfuerzos de seguridad en los límites de la red, son los usuarios internos los que ofrecen mayor riesgo para la seguridad informática. Desde ejecutivos, administradores de TI y socios, muchas personas tienen acceso a información confidencial que, si se expone públicamente, podría causar consecuencias significativas para el negocio de una organización, o incluso para su existencia.

Por lo general, la seguridad informática se entiende como un campo técnico, con defensores altamente calificados que buscan superar a los atacantes en un concurso de intelecto y determinación. A pesar de que hay algo de verdad en esta caracterización, omite lo que quizás represente el aspecto más importante de la seguridad: el elemento humano. Las personas tienden a creer en aquellos que conocen, lo cual los lleva a compartir contraseñas u otros datos que no deberían compartir.

La confianza es un elemento esencial para operar cualquier tipo de organización. Las personas necesitan acceso a información confidencial y sistemas críticos por distintos motivos y un nivel de confianza debe estar asociado con ese acceso. Comprender y manejar esa confianza es el desafío más importante, y difícil, al momento de tratar con las amenazas internas.

“Confianza” no significa darles a los empleados acceso no restringido e innecesario a la información. Con los controles de seguridad adecuados, las organizaciones pueden reducir significativamente la exposición al riesgo de amenazas internas. Es fundamental encontrar el balance adecuado entre los controles y las habilitaciones que tiene el empleado, y la responsabilidad de los empleados por sus acciones. Esto requiere un enfoque amplio que le permita a las organizaciones administrar cuidadosamente sus identidades, accesos y datos desde la administración de identidades hasta la gobernanza, la administración de identidades con privilegios y la protección de datos.

1.2. LITERATURA REVISADA Y FUNDAMENTOS TEÓRICOS

1.2.1. DELITOS INFORMÁTICOS

Las nuevas herramientas que ponen las TI C al servicio del hombre están relacionadas con la transmisión, procesamiento y almacenamiento digitalizado de información, así como un conjunto de procesos y productos que simplifican la comunicación, y hacen más viables la interacción entre las personas.

De acuerdo a Villavicencio T. (2014), las aplicaciones de las TIC a partir de internet (entre ellas cibergobierno, cibereducación y cibersalud) se consideran habilitantes para el desarrollo social, puesto que proporcionan un canal eficaz para distribuir una amplia gama de servicios básicos en zonas remotas y rurales, pues estas aplicaciones facilitan el logro de los objetivos de desarrollo prospectivo, mejoras en las condiciones sanitarias y medioambientales.

Si bien los diversos ámbitos de interacción se ven favorecidos por la fluidez que le brinda esta nueva alternativa tecnológica, no obstante, crecen los riesgos relacionados al uso de las tecnologías informáticas y de comunicación. El desarrollo de la tecnología también ha traído consigo nuevas formas delictuales que tienen por medio y/o finalidad los sistemas informáticos e internet.

Las principales características de vulnerabilidad que presenta el mundo informático son las siguientes:

a. La falta de jerarquía en la red, que permite establecer sistemas de control, lo que dificulta la verificación de la información que circula por este medio.
b. E l creciente número de usuarios, y la facilidad de acceso al medio tecnológico.
c. E l anonimato de los cibernautas que dificulta su persecución tras la comisión de un delito a través de este medio.
d. La facilidad de acceso a la información para alterar datos, destruir sistemas informáticos.

e. Otro factor determinante es la rápida difusión de información a través de este medio tecnológico a muy bajo costo que permite a las organizaciones delictivas perpetrar delitos con mayor facilidad.

Conforme al informe del doceavo Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, estos adelantos tecnológicos posibilitan una nueva modalidad de cometer los delitos tradicionales como el fraude y la distribución de pornografía infantil, y a su vez facilita la comisión de nuevos delitos como la penetración en redes informáticas, el envío de correo basura, la pesca de los datos pishing, la piratería digital, la propagación maliciosa de virus y otros ataques contra las infraestructuras de información esenciales (Naciones Unidas, 2010).

Los delitos informáticos[19] se vinculan con la idea de la comisión del crimen a través del empleo de la computadora, internet, etcétera; sin embargo, esta forma de criminalidad no solo se comete a través de estos medios, pues éstos solo son instrumentos que facilitan pero no determinan la comisión de estos delitos. Esta denominación es poco usada en las legislaciones penales; no obstante, bajo ella se describe una nueva forma de criminalidad desarrollada a partir del elevado uso de la tecnología informática.

Para Mühlen citado en Mazuelos C. (s/a)el delito informático ha de comprender todo comportamiento delictivo en el que la computadora es el instrumento el objetivo del hecho. Concibe el delito informativo como aquella forma de criminalidad que se encuentra directa o indirectamente en relación con el procesamiento electrónico de datos y se comete con la presencia de un equipo de procesamiento electrónico de datos.

[19]Debido al desarrollo de la tecnología, entre ellas la computadora, y dado la nueva forma de comisión de delitos a través de las tecnologías es que se ha optado por denominar indistintamente a este tipo de delitos como delitos de abuso de computadoras, delitos bajo la influencia de la computadora, criminalidad de la información y la comunicación, criminalidad de Internet, criminalidad multimedia. En el Perú se los denomina delitos informáticos. Todas estas denominaciones identifican de manera general la problemática de la delincuencia mediante las computadoras y el empleo de las comunicaciones; sin embargo, para efectos didácticos en la doctrina se prefiere la denominación de delitos informáticos para identificar la criminalidad vinculada a la tecnología.

Para efectos de esta investigación, tomaremos el concepto de criminalidad informática de Miró Llinares (2013) como aquellas conductas dirigidas a burlar los sistemas de dispositivos de seguridad, esto es, invasiones a computadoras, correos o sistemas de datas mediante una clave de acceso; conductas típicas que únicamente pueden ser cometidas a través de la tecnología. En un sentido amplio, comprende a todas aquellas conductas en las que las TI C son el objetivo, el medio o el lugar de ejecución, aunque afecten a bienes jurídicos diversos; y que plantea problemas criminológicos y penales, originados por las características propias del lugar de comisión.

Es necesario determinar que conductas pueden ser clasificadas como delitos informáticos y cuáles no, a pesar de su vinculación con una computadora, un procesador de datos o la red de información. Al respecto, uno de los criterios a utilizar seria que un delito, para ser clasificado dentro de los delitos informáticos, no sea posible de realizarse sin la intervención de la informática, porque es el medio informático lo que va caracterizar este delito (Mazuelos Coello, 2001); por ejemplo el difamar a una persona a través de los medios de comunicación (sea por correo electrónico, facebook o twitter), no puede constituirse como un delito informático por el solo hecho de emplear la tecnología informática como medio, pues este delito puede realizarse a través de otros medios como son verbal, escrito, etcétera. Sin embargo, los delitos de ingresar sin autorización a un sistema de datos o sabotear una base de datos sí se clasifican dentro de los delitos informativos, porque no es posible la comisión de estos delitos sin la intervención de la informática.

Las nociones tradicionales de ciberseguridad hacen hincapié en la protección contra los ataques que surgen de amenazas externas. Sin embargo, cada vez es más evidente que la mayor amenaza a la seguridad de una organización puede estar dentro de ella, como lo demuestran muchas encuestas recientes. Para subrayar Nurse y otros (2014) indica que en un estudio reciente de Clearswift[20] informa que el 58% de los incidentes de seguridad reportados fueron como resultado de una amenaza interna. Este punto se apoya además en varios casos recientes de alto perfil y muy

[20]Clearswift. (2013) The enemy within. [Online]. Available: http://www.clearswift.com/sites/default/files/images/blog/enemy-within.pdf

divulgados de filtración de datos y denuncias; Por ejemplo Edward Snowden[21], Xiang Dong Yu[22] y Michael Woodford[23]. Estos informes probablemente sólo presentan un pequeño porcentaje de los casos de amenaza de información privilegiada. Es ampliamente aceptado que hay una miríada de incidentes de información privilegiada que no serán denunciados (por miedo a dañar la reputación de la compañía, por ejemplo) o que pasarán desapercibidos ya que los ataques simplemente evitarán la detección.

Respecto de los delitos informativos, Krutisch referenciado en Villavicencio T. (2014), identifica tres tipos de categorías: manipulación informática, sabotaje informático y acceso no autorizado a datos o sistema computarizados, pero no son categorías de delitos, sino modos de cometer los delitos informativos.

En el Perú, la Ley de delitos informáticos (Ley N° 30096, 2013)establece en su artículo N° 1, que la finalidad de la ley es prevenir y sancionar las conductas ilícitas que afectan los sistemas, las datas informáticos, el secreto de las comunicaciones; y otros bienes jurídicos de relevancia penal (como el patrimonio, la fe pública, la libertad sexual, etc.) que puedan ser afectados mediante la utilización delas TIC, con la finalidad de garantizar las condiciones mínimas para que las personas gocen del derecho a la libertad y al desarrollo. Con esta ley se intenta garantizar la lucha eficaz contra la ciberdelincuencia.

Esta Ley no responde solo a la necesidad de ejercer la función punitiva del Estado enfocada en la **protección de la información**; sino que tiene como principal objetivo la estandarización dela ley penal peruana con el ordenamiento penal internacional, principalmente por la Convenio contra la cibercriminalidad del Consejo Europeo (CETS 185), denominado Convenio de Budapest (Villavicencio T., 2014).

[21]http://www.bbc.com/news/world-us-canada-22837100
[22]http://www.reuters.com/article/2011/04/13/us-djc-ford-tradesecrets-idUSTRE73C3FG20110413
[23]http://www.bbc.co.uk/news/15742048

Por tanto, el bien jurídico tutelado en los delitos informáticos por la Ley son: la información de manera general (información almacenada, tratada y transmitida mediante los sistemas de tratamiento automatizado de datos), y en el segundo plano, los demás bienes afectados a través de este tipo de delitos como son la indemnidad sexual, intimidad, etc. Respecto de la información debe ser entendido como el contenido de las bases y/o banco de datos o el producto delos procesos informáticos automatizados; por lo tanto se constituye en un bien autónomo de valor económico. Y es la importancia del valor económico de la información lo que ha hecho que se incorpore como bien jurídico tutelado (Gutierrez F., 1994).

Sin embargo, la información se debe considerar de diferentes formas, y no solo como un valor económico, sino como un valor intrínseco por los sistemas que lo procesan o automatizan, los mismos que se equiparan a los bienes protegidos tradicionalmente, tales como el patrimonio (fraude informático), la reserva, la intimidad y confidencialidad de los datos(agresiones informáticas a la esfera de la intimidad), la seguridad o fiabilidad del trafico jurídico probatorio (falsificación de datos o documentos probatorios), etc. (Villavicencio T., 2014).

Por tanto, en este tipo de delitos no se puede establecer a la información como el único bien jurídico afectado, por ser el principal y el más importante; sino a un conjunto de bienes que son afectados, debido a la característica de la conducta típica en esta modalidad delictiva que colisiona con diversos intereses colectivos.

1.2.2. 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 (Whitman, 2001). 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 y 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 (Forcht 1994, Straub y Welke 1998). Straub y 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 et al. 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. Muchos de los investigadores y los profesionales recomiendan varias medidas que pueden ser utilizados para el combate el mal uso de las PSI (Dhillon 1999, Parker 1998, Straub&Welke 1998).

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, InformationWeek 2005), a menudo perpetrados por empleados descontentos (Standage 2002). Debido a que sólo una fracción de incidentes de seguridad es en realidad descubiertos (Hoffer y Straub 1989, Whitman 2003), las estadísticas reportadas probablemente subestiman el problema. 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).

1.2.3. TIPIFICACIÓN Y CARACTERIZACIÓN DE LAS AMENAZAS INTERNAS

Para poder caracterizar y tipificar las amenazas internas se tuvo que caracterizar a los actores, los ataques y el tipo de organización donde ocurren los hechos.

Comenzamos con los aspectos conductuales y psicológicos relacionados con el actor. Estos pueden ser vistos como los antecedentes o factores iniciales clave para comprender la propensión de un individuo a atacar. Basándonos en nuestra investigación en artículos y los datos recogidos, identificamos ocho elementos que pueden ser útiles para modelar y analizar este aspecto de las amenazas internas.

a. El evento iniciador

   De acuerdo con Moore, Cappelli y Trzeciak (2008), es el evento clave o catalizador que tiene el potencial de convertir a un empleado interno en una amenaza para su empleador. Ejemplos de estos eventos incluyen despido de empleados, disputas con empleadores (por ejemplo, con respecto a los derechos de propiedad intelectual), injusticias percibidas, actos negativos de la empresa (por ejemplo, despidos intempestivos), problemas familiares (divorcio, custodia

de niños, problemas de salud), oferta de trabajo de una empresa competidora, o incluso falta de entrenamiento en el caso de ataques accidentales.

b. Las características de la personalidad

Incluye los rasgos psicológicos y las capacidades y destrezas de las personas. Captan las características de la personalidad de un actor basándose tanto en su yo innato (los aspectos estáticos) como en sus experiencias de vida (los aspectos más dinámicos y responsivos). Los rasgos generales de personalidad pueden incluir su OCECN (Openness, Consciousness, Extroversion, Convenience, Neuroticism - Apertura, Conciencia, Extroversión, Conveniencia, Neuroticismo)(Digman, 1996), la Tríada Oscura (Maquiavelismo, Narcisismo y Psicopatía) (Furnham, Richards, & Paulhus, 2013) y otras características como: madurez, agresividad, problemas de habilidades sociales, superficialidad, (falta de) autoestima e integridad personal.

Sin embargo, es importante entender que, aunque algunas características de la personalidad son dignas de mención, no son suficientes, aisladamente, para identificar a un atacante potencial, sino que necesitamos evaluar los grupos de características de la personalidad junto con los catalizadores (eventos precipitantes) e incluso el individuo ambiente.

c. Comportamiento histórico

Documenta los tipos de actividades que el actor ha realizado durante el pasado y, como con la mayoría de los comportamientos, es probable que se vean influidos por sus características de personalidad. Incluye prácticas adictivas (por ejemplo, juegos de azar o abuso de alcohol), violaciones de reglas anteriores (por ejemplo, acoso o violación de la política de la empresa), antecedentes penales o antecedentes de problemas mentales graves. Por supuesto, cuando se considera

aisladamente, esto de nuevo no es solo indicativo de un individuo que se convierte en una amenaza interna(Liginlal, Sim, & Khansa, 2009).

d. Estado psicológico

Representa el estado psicológico y emocional del actor (por ejemplo: feliz, deprimido, estresado o ansioso). Esto puede ser, en parte, debido a su situación psicológica(por ejemplo, tener depresión clínica), o como resultado de su ambiente de trabajo (por ejemplo, un evento estresante, como la transferencia forzada de trabajo, que conduce a la depresión), lo que explica las relaciones con las características de la personalidad y el evento precipitante respectivamente.

En la literatura de amenazas internas, es comúnmente encontrar como ejemplo que un empleado descontento es responsable potencial de los ataques. Pero el descontento es sólo uno de un conjunto de estados encontrados para ser un precursor convincente de motivo de ataque, como: el estrés, el temor (por ejemplo, el despido o la exclusión de grupo), la falta de reconocimiento, el sentimiento de derecho (a los datos de contacto del cliente, por ejemplo), el sentimiento de oportunismo o, desde una perspectiva de amenaza accidental, descuido, aburrimiento o insatisfacción.

e. Motivación para atacar

Se refiere a la razón por la que un actor podría desear atacar a la empresa. La noción de motivación de ataque sirve mucho para la evaluación de amenazas. Las motivaciones pueden ser: financieras, políticas, por venganza, curiosidad o diversión, poder, ventaja competitiva o reconocimiento de pares (Martinko, Gundlach, & Douglas, 2002).

Consideramos que el estado psicológico actual de un actor es una influencia significativa en su motivación al ataque. Por ejemplo, el descontento de un contratista por maltrato puede dar lugar a algunos deseos de venganza; o el temor a ser excluidos de la oficina o de la lealtad de los amigos/familia puede motivar a un empleado a participar en un ataque. Otro ejemplo, si un empleado fue constantemente pasado por alto para una promoción, por lo tanto, posiblemente puede sentirse agraviado (estado psicológico), podría sentir que su compromiso con su empleador (actitud) se ha perdido, y por lo tanto muy motivado para atacar.

f. Las habilidades del actor

Se refiere a la capacidad del actor o las habilidades necesarias para realizar un ataque (Jones & Ashenden, 2005). Entonces se puede establecer el vínculo razonable entre el rol que un actor desempeña dentro de una empresa y el conjunto de habilidades que poseen. Por ejemplo, un desarrollador de software de una organización que está enojado por la falta de bonos de la empresa, inserta código malicioso en el principal sistema de la empresa. En este caso la habilidad para desarrollar software del empleado y su función que cumple dentro de la empresa le permitió iniciar y llevar a cabo el ataque.

En general, las personas que exhiben características, como:

- Introversión,
- Avaricia / necesidad financiera,
- Vulnerabilidad al chantaje,
- Comportamiento compulsivo y destructivo,
- Rebelde, pasivo agresivo
- La "flexibilidad" ética
- Lealtad reducida

- Derecho - narcisismo (ego / auto-imagen)
- Minimizar sus errores o faltas
- Incapacidad para asumir la responsabilidad de sus acciones
- Intolerancia de la crítica
- El valor de autopercepción excede el rendimiento
- Falta de empatía
- Predisposición a la aplicación de la ley
- Patrón de frustración y decepción
- Historia de la gestión de las crisis ineficaz,
- Etc.

pueden llegar a un punto en el que llevan a cabo actividades maliciosas contra la organización. Una de las mejores medidas de prevención es capacitar a los empleados para reconocer y reportar indicadores de comportamiento exhibidos por compañeros o socios comerciales.

Algunos de los indicadores de comportamiento de actividad de amenaza maliciosa, pueden ser (CERT, 2013):

- Accede de forma remota a la red mientras está de vacaciones, enfermo o en momentos extraños
- Trabaja horas sin autorización
- Notable entusiasmo por las horas extras, los fines de semana o los horarios de trabajo inusuales
- Copia innecesariamente el material, especialmente si es propietario o clasificado
- Intereses en asuntos fuera del alcance de sus funciones
- Las señales de vulnerabilidad, como abuso de drogas o alcohol, dificultades financieras, juegos de azar, actividades ilegales, mala salud mental o comportamiento hostil, deberían despertar preocupación. Por eso se debe estar

atento a las señales tales como la adquisición de riqueza inesperada, viajes inusuales en el extranjero, horas de trabajo irregulares o ausencias inesperadas.

Los usuarios internos pueden robar, borrar o exponer información confidencial de forma malintencionada o inconsciente por diversas razones. Al mismo tiempo, los usuarios internos deben tener cierto nivel de acceso para que funcione el negocio o para que la organización opere. Puede ser considerado como un individuo que es un empleado (pasado o presente), contratista u otro tercero de confianza, que tiene acceso privilegiado a las redes, sistemas o datos de una organización(Nurse, y otros, 2014). Es fundamental comprender las amenazas internas en sus diversos niveles, desde las motivaciones a los ejemplos de daños hasta comprender cómo evolucionaron las amenazas, para abordar de forma inteligente las estrategias de mitigación de riesgos.

Una amenaza interna maliciosa se caracteriza porque el atacante utiliza su acceso privilegiado para causar intencionalmente un impacto negativo a la confidencialidad, integridad o disponibilidad de la información, sistemas o infraestructura de la organización. Normalmente se entiende que un miembro de la red maliciosa tratará de explotar su acceso privilegiado por algún beneficio inapropiado, ya sea personal, financiero o por venganza(Nurse, y otros, 2014).

De la misma forma Nurse y otros (2014) define a la segunda forma de amenaza como aquella ejecutada por un personal interno de manera accidental o no maliciosa y que causa un daño futuro a la confidencialidad, integridad o disponibilidad de los activos o recursos de la organización (por ejemplo, información o sistemas); y es considerada como el tipo más común de amenaza. Esto por lo tanto, cubre errores humanos y otros errores y percances que pueden comprometer la organización, relacionados por un mal diseño del sistema tanto o por la negligencia de las personas. Se incluyen a los empleados que pierden sus dispositivos de trabajo, filtrando accidentalmente la información sensible de la compañía en redes sociales, y cayendo en el phishing y otros ataques maliciosos disfrazados.

En el caso específico de las acciones intencionales, el perfil del "delincuente" (sujeto activo) en esta modalidad delictual requiere que este posea ciertas habilidades y conocimientos detallados en el manejo del sistema informático. Es en razón a esas cualidades que se les ha calificado a los sujetos activos como delincuentes de cuello blanco, que tienen como características(Azaola Calderón, 2010):

a. Poseer importantes conocimientos informáticos.
b. Ocupar lugares estratégicos en su centro laboral, en los que se maneja información de carácter sensible (se denominan delitos ocupacionales, ya que se comenten por la ocupación que se tiene y el acceso al sistema).

Las personas que cometen los delitos informáticos son aquellas que poseen ciertas características que no presentan el denominador común, esto es, habilidades para el manejo delos sistemas informáticos y que por su situación laboran en puestos estratégicos donde se maneja información sensible.Camacho Losa (2007) considera que el perfil de estas personas no coincide con el de un delincuente marginal, y caracteriza a los autores de estas infracciones como empleados de confianza de las empresas afectadas.

Sin embargo, desde nuestra perspectiva el autordel delito informático puede serlo cualquiera, no precisando el mismo de determinadosrequisitos personales o conocimientostécnicos cualificados. El sujeto activo puedeser cualquier persona con conocimientosy habilidades en informática, ocupe o no un puesto laboral que le permitaacceder a información sensible. Lo que necesita son ciertas habilidades y conocimientossobre la informática y los conocemos como: hackers[24] o crackers[25].

[24]Son personas dedicadas, por afición u otro interés, a violar programas y sistemas supuestamente impenetrables
[25]Son personas que se introducen en sistemas remotos con la intención de destruir datos, denegar el servicio a usuarios legítimos y, en general, a causar problemas a los sistemas, procesadores o redes informáticas, conocidos como piratas electrónicos

Los tipos de amenazas internas no son todas iguales. 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 (Miller & Maxim, 2013).

a. Los usuarios internos malintencionados son el tipo menos frecuente, pero tienen el potencial de ocasionar daños considerables por su capacidad de acceso interno. Los administradores que tienen identidades con privilegios son particularmente riesgosos. De acuerdo con Ponemon Institute[26], las violaciones a la información que son consecuencia de ataques malintencionados son las más costosas.

   Una amenaza interna malintencionada para una organización es un empleado actual, un ex empleado, un contratista u otro socio de negocios que tiene o tuvo acceso autorizado a los datos, los sistemas o las redes de una organización y que abusó o hizo un uso inadecuado de dicho acceso de manera voluntaria de modo tal que afectó negativamente la confidencialidad, la integridad o la disponibilidad de la información o de los sistemas de información de la organización.

b. Los usuarios internos explotados pueden ser "engañados" por partes externas para proporcionar datos o contraseñas que no deberían compartir.

c. Por último, un usuario interno descuidado puede simplemente presionar la tecla equivocada y borrar o modificar información esencial de manera no intencional.

[26]PonemonInstitutees una empresa reconocida mundialmente que realiza investigaciones independientes sobre privacidad, protección de datos y política de seguridad de la información.

Las amenazas internas también pueden provenir de usuarios con privilegios (administradores) o de usuarios comunes con acceso a información confidencial. Por lo general, los administradores poseen privilegios completos para realizar esencialmente cualquier operación en los sistemas importantes. Por lo general, personas de todo tipo han acumulado más derechos de los necesarios para sus trabajos actuales, lo cual lleva a un aumento del riesgo que es absolutamente evitable.

1.2.4. FACTORES DE RIESGO DE LOS USUARIOS INTERNOS

Todas las organizaciones enfrentan desafíos comunes cuando intentar reducir los riesgos a infracciones de seguridad internas. Para ello deben conocer los factores que generan los riesgos que provienen de amenazas internas, las cuales las podemos clasificar de la siguiente manera (Miller, El costado cambiante de los ataques ciberneticos, 2013), (Miller & Maxim, Tengo que confiar en alguién, ¿cierto?. Cómo tratar las amenazas internas a la ciberseguridad, 2013), (Silowash, Cappelli, Moore, Trzeciak, Shimeall, & Flynn, 2012), (National Cybersecurity and Communications Integration Center, 2014), (Nurse, y otros, 2014), (Kont, Pihelgas, Wojtkowiak, Trinberg, & Osula, 2014):

a. **Administración ineficaz de usuarios con privilegios**. En todos los entornos de TI, existen usuarios con privilegios (administradores, usuarios raíz) que tienen acceso total a los sistemas, las aplicaciones y la información clave.

   Esto no solo es un riesgo de seguridad, sino que también puede dificultar mucho más el cumplimiento de los protocolos de seguridad. El uso compartido de contraseñas de administrador es otro problema común que podría dar lugar al acceso inapropiado a sus sistemas y datos, y a la incapacidad de identificar específicamente quién realizó cuál acción en cada sistema.

b. **Asignación inapropiada de roles y derechos**. La administración de roles y derechos de usuarios es uno de los principales desafíos que muchas organizaciones de TI enfrentan. Los roles superpuestos o los derechos duplicados incoherentes son problemas comunes que pueden dar lugar a la obtención y el uso inapropiados de información confidencial. Además, la falta de un control automático puede generar derechos excesivos o cuentas huérfanas, lo que puede proporcionar fisuras a través de las cuales los usuarios internos insatisfechos pueden lanzar un ataque.

c. **Gobernanza general de identidades inadecuada**. La protección eficaz contra el acceso inapropiado a la información, o el uso inapropiado de esta, requiere de un fuerte control de las identidades de usuarios, el acceso y el uso de la información. La mayoría de las organizaciones tienen algunos controles en estas áreas, pero no cuentan con un enfoque unificado y sólido para proteger verdaderamente sus activos de información.

d. **Deficiente clasificación de la información y cumplimiento de políticas**. Muchas organizaciones ni siquiera saben dónde se encuentra toda su información confidencial y, por lo general, tienen políticas inadecuadamente definidas y comunicadas acerca de cómo se debe manejar la información confidencial. Sin embargo, lo que es más importante, muchas organizaciones no disponen de controles para detectar y prevenir la transmisión o divulgación inapropiada de información confidencial.

e. **Auditorías y análisis inadecuados**. Muchas empresas no tienen forma de auditar continuamente el acceso para asegurarse de que solo las personas debidamente autorizadas obtengan acceso, y que su uso de la información cumpla con la política establecida. Además, aunque tengan herramientas de auditoría, el mero

volumen de los datos de registro generados hace que sea muy difícil para las organizaciones examinar los datos e identificar infracciones o amenazas.

f. **Complejidad del registro de auditoría.** El mero volumen de los datos de auditoría y registro dificulta la detección y la investigación forenses. Registrar toda la actividad de TI es un primer paso importante para combatir los ataques internos, y los complejos y altamente distribuidos entornos actuales de TI generan volúmenes masivos de datos de registro, pero es muy difícil administrar el volumen total de datos.

g. **Respuestas solo reactivas**. La mayoría de los enfoques actuales para abordar las amenazas internas son reactivos, no predictivos. A pesar de que esto puede ayudar muchísimo en las investigaciones forenses, el problema es que el ataque o robo ya se produjo. Por lo tanto, las organizaciones deben buscar soluciones que puedan ofrecer más capacidades analíticas y predictivas que, aunque no puedan evitar los ataques internos, puedan igualmente identificar a los "usuarios internos de riesgo", y luego implementar un registro más detallado sobre estos individuos.

h. **Ausencia de políticas de uso aceptable que sean integrales y por escrito**. Todas las organizaciones deben tener políticas de uso aceptable detalladas para todos los empleados, y deben exigir a los empleados que revisen y firmen la política una vez por año. Es una medida básica, pero las organizaciones a menudo la pasan por alto. Tener una política de seguridad por escrito no evitará necesariamente los ataques internos, pero puede resultar útil para proporcionar a toda la organización un punto de referencia acerca de lo que es el uso aceptable y de los métodos adecuados para administrar los datos confidenciales.

1.2.5. TEORÍAS DE LA PREDICCIÓN DEL COMPORTAMIENTO

Identificar indicadores de comportamiento puede ser difícil, especialmente si no ocurren durante un largo período de tiempo y por lo tanto no establecen un patrón. Por lo tanto, una buena comprensión de las características de riesgo y eventos que pueden desencadenar esas características es esencial. Los individuos plantean amenazas por una variedad de razones. Algunas teorías de la predicción del comportamiento a considerar son:

Tabla N° 4. Teorías de la predicción del comportamiento

Teoría	Fundamento básico de la teoría
Teoría general de la disuasión (TGD) General DeterrenceTheory (GDT)	La persona comete delito si el beneficio esperado supera el costo de la acción
Teoría del enlace social (TES) Social Bond Theory (SBT)	La persona comete delito si los lazos sociales de apego, compromiso, participación y creencia son débiles
Teoría del Aprendizaje Social (TAS) Social Learning Theory (SLT)	La persona comete delito si se asocia con compañeros delincuentes
Teoría del comportamiento planeado (TCP) Theory of Planned Behavior (TPB)	La intención de la persona (actitud, normas subjetivas y control de la conducta percibida) hacia el crimen factor clave en la predicción del comportamiento
Prevención Situacional de la Delincuencia (TSD) Situational Crime Prevention (SCP)	La delincuencia ocurre cuando existe un motivo y una oportunidad

Fuente: (CERT, 2013)

De acuerdo al objetivo de la presente investigación y al sector a las que pertenecen las organizaciones, donde se aplicará el estudio, las teorías seleccionadas son: Teoría del comportamiento planeado y la Teoría general de la disuasión

a. La Teoría del Comportamiento Planificado (TCP)

La TCP es una teoría diseñada para predecir y explicar el comportamiento humano en contextos específicos (Ajzen, 1991). La teoría propone un modelo que puede medir cómo las acciones humanas son guiadas. Se predice la ocurrencia de una conducta en particular, siempre que la conducta es intencional (Ajzen, 1985).

El factor central en la teoría es la intención de conducta de la persona para realizar un comportamiento determinada. Las intenciones permiten identificar los factores motivacionales que influyen en un comportamiento; son indicadores de cómo personas cerradas están dispuestas a probar o tratar, de cuánto esfuerzo se está planeando ejercer, con el fin de lograr la conducta deseada. Como regla general, la fuerza de la intención de conducta para lograr un comportamiento, se refleja, más probable, en el rendimiento. Debe quedar claro, sin embargo, que una intención de conducta puede encontrar expresión en el comportamiento, sólo si el comportamiento en cuestión, está bajo control volitivo, es decir, si la persona puede decidir a voluntad, realizar o no realizar la conducta. Aunque algunos comportamientos pueden, de hecho, cumplir con este requisito bastante bien, el desempeño de la mayoría depende, al menos en cierta medida, de factores no motivacionales como la disponibilidad de oportunidades y recursos necesarios (por ejemplo, tiempo, dinero, habilidades, la cooperación de los demás). En conjunto, estos factores representan el control real de las personas sobre el comportamiento. En la medida en que una persona tiene las oportunidades y los recursos necesarios, y tiene la intención de realizar la conducta, él o ella deben tener éxito en hacerlo (Ajzen, 1991).

De acuerdo con la TCP, el control del comportamiento percibido, junto con la intención de conducta, se puede utilizar directamente para predecir el rendimiento conductual. Al menos dos razones pueden sustentar esta hipótesis. En primer lugar, la intención constante, el esfuerzo realizado para llevar un curso de comportamiento a una conclusión exitosa, es probable que aumente con el control conductual percibido. Por ejemplo, si dos personas tienen intenciones igualmente fuertes para aprender a esquiar, y ambos tratan de hacerlo, la persona que está convencido de que puede dominar esta actividad, es más probable que lo logre que la persona que duda de su capacidad. La segunda razón que permite una relación

directa entre el control conductual percibido y el logro de un comportamiento, es que el control del comportamiento percibido a menudo puede ser utilizado como un sustituto de una medida de control real (Ajzen I. , 1991).

Para que una medida de control del comportamiento percibido pueda sustituir a una medida de control real depende de la exactitud de las percepciones. El control del comportamiento percibido puede no ser realista cuando la persona tiene poca información sobre el comportamiento, cuando los requerimientos o recursos disponibles han cambiado, o cuando nuevos y desconocidos elementos aparecen. En esas condiciones, una medida de control del comportamiento percibido puede añadir poco a la precisión de la predicción del comportamiento. Sin embargo, en la medida en que el control percibido es realista, puede ser utilizado para predecir la probabilidad de un intento exitoso de comportamiento (Ajzen, 1985).

La importancia relativa de las intenciones y el control del comportamiento percibido en la predicción de un comportamiento se espere que varíe según las situaciones y los diferentes comportamientos esperados. Cuando el comportamiento/situación permite a una persona el control completo sobre el rendimiento de comportamiento, las intenciones por sí solas deberían ser suficientes para predecir el comportamiento(Ajzen, 1991).

La TCP postula tres determinantes conceptualmente independientes de intención. La primera es la actitud hacia el comportamiento y se refiere al grado en que una persona tiene una evaluación o valoración favorable o desfavorable de la conducta en cuestión. El segundo predictor es un factor social, denominado norma subjetiva; se refiere a la presión social percibida para realizar o no realizar el comportamiento. El tercer antecedente de intención es el grado de control del comportamiento percibido que, como hemos visto anteriormente, se refiere a la

facilidad o dificultad de realizar el comportamiento percibido y se supone para reflejar la experiencia del pasado, así como los impedimentos y obstáculos previstos. Como regla general, más favorable será la actitud y la norma subjetiva con respecto a un comportamiento, y a mayor el control conductual percibido, más fuerte debe ser la intención de una persona para realizar el comportamiento en cuestión (Ajzen, 1991).

Se espera que la importancia relativa de actitud, la norma subjetiva y el control percibido en la predicción de la intención de un comportamiento varíe en situaciones distintas. Así, en algunas aplicaciones puede que sólo las actitudes tengan un impacto significativo en las intenciones, en otros casos, las actitudes y el control percibido son suficientes para dar cuenta de las intenciones de comportamiento, y en otros los tres predictores hacen contribuciones independientes (Ajzen, 1991).

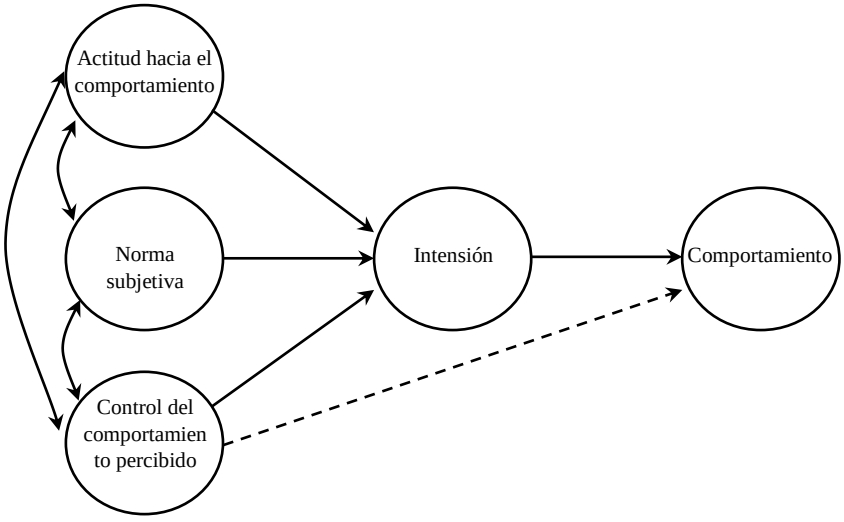


Gráfico N° 8. Modelo conceptual de la Teoría del ComportamientoPlanificado

Fuente: (Ajzen, 1991)

b. Teoría General de la Disuasión (TGD)

La TGD se puede remontar a los primeros trabajos de filósofos clásicos como Thomas Hobbes (1588-1678), Cesare Beccaria (1738-1794), y Jeremy Bentham (1748-1832). Postula que los individuos sopesan los costos y los beneficios al momento de decidir si procede o no a cometer un delito, y eligen el crimen cuando éste paga (Vance, 2010). Para ser más precisos, si una persona considera que el riesgo de ser descubierto es alta (certeza de sanciones) y que se le aplicarán severas sanciones en el caso de que sea atrapado (severidad de las sanciones), entonces la teoría de la disuasión postula que las personas no van a cometer delitos.

Los defensores de la disuasión creen que las personas optan por obedecer o violar la ley después de calcular las ganancias y las consecuencias de sus acciones.

En Zagrare (2004) se planteó que la TGD es lógicamente inconsistente, empíricamente imprecisa y deficiente como teoría. En lugar de la disuasión clásica, los estudiosos de la elección racional han argumentado a favor de la disuasión perfecta, que supone que los estados pueden variar en sus características internas y sobre todo en la credibilidad de sus amenazas de represalias.

1.2.6. FACTORES DEL COMPORTAMIENTO ASOCIADOS CON LAS TEORÍAS UTILIZADAS

De acuerdo a la Teoría de la Conducta Planificada, los factores que influyen en el comportamiento deben ser clasificados en:

a. Factores asociados a la actitud
b. Factores asociados a la norma subjetiva, entendida como la influencia del entorno
c. Factores asociados al control percibido

De la Teoría General de Disuasión tomamos que el factor que influye en el comportamiento es:

d. Factores relacionados a la certeza y severidad de la sanción

Tomando como base esta clasificación de factores que influyen en el comportamiento y de los fundamentos teóricos relacionados con las amenazas internas, consideramos como factores a ser incluidos en la construcción del modelo propuesto a los siguientes:

Tabla N° 5. Identificación de los tipos de intensión de comportamiento de acuerdo al factor y tipo de factor generadora de amenazas

Tipo de factor	Factor	Intensión de comportamiento asociado
Relacionado con la actitud	Integración y compromiso	Comportamiento intencional
	Concienciación	Comportamiento no intencional
Relacionado con la influencia del entorno	Motivación	Comportamiento no intencional
	Entrenamiento	Comportamiento no intencional
Relacionado con el control percibido	Tecnologías basadas en el control	Comportamiento intencional
	Usabilidad de herramientas de seguridad	Comportamiento no intencional
Relacionado con la certeza y severidad de la sanción	Medidas de disuasión	Comportamiento intencional
	Presión del tiempo y carga del trabajo	Comportamiento no intencional

1.2.6.1. FACTORES DEL COMPORTAMIENTO ASOCIADOS CON LA ACTITUD

a. Integración y compromiso

La perspectiva para considerar este factor es evaluar que tanto influye la percepción que tiene el individuo de sentirse integrado con el sistema de seguridad de la organización con la finalidad de que cumpla con las políticas de seguridad de la información.

Definimos integración como el proceso de inserción y adaptación del individuo a la organización (Fernández Losa, 2007) y, en este caso específico, al sistema de seguridad de la información de una empresa microfinanciera.

Consideramos que la atención y programación adecuada del ingreso de nuevos empleados puede ser crucial tanto para la empresa como para el empleado. Los beneficios pueden expresarse en la reducción de las tasas de abandono y rotación y, por tanto, en la disminución de los costes de selección, formación, cumplimiento de nomas, etc. Así mismo, una integración adecuada en la empresa puede considerarse como un factor motivador y gratificante para el trabajador (Palací y Peiró, 1995).

La empresa espera que la persona recién incorporada responda de una manera prevista y el empleado desea integrarse adecuadamente en la organización y obtener unas compensaciones justas por su trabajo. Se espera, en definitiva, que no haya una ruptura en el contrato psicológico entre el individuo y la organización. Los principales fines de la integración y socialización de los empleados son: reducir los costes de puesta en marcha, reducir el estrés y la ansiedad, reducir la rotación de personal y ahorrar tiempo a los supervisores y compañeros de trabajo (Dolan, Valle Cabrera, & Jackson, 2003).

Cuando el nuevo miembro se percibe capaz de abordar las demandas de la organización, interpreta éstas como desafíos, los cuales estimulan al individuo, con la finalidad de adecuar las circunstancias a las necesidades individuales. De esta manera, desarrolla estrategias activas y actitudes consecuentes que favorezcan el ajuste y la integración, como bajo nivel de estrés, alta satisfacción laboral, compromiso con las metas de la organización y deseo de permanencia en ella (Fernández Losa, 2007).

Las actitudes del empleado hacia su trabajo y la organización y su comportamiento nos indicarán su grado de integración. El grupo de trabajo y el supervisor también nos pueden dar información acerca de si el nuevo empleado está plenamente integrado. Finalmente, desde el punto de vista de la organización, se puede tratar de determinar si el nuevo empleado está respondiendo tal y como ésta esperaba.

Por otro lado el compromiso es una decisión personal (de cada empleado) que va más allá de cumplir la obligación laboral. El compromiso nace del interior y aporta un extra que conduce a la excelencia, pues implica poner en juego todas las capacidades y hacer más de lo esperado.

Un empleado comprometido proyecta sus energías para conseguir su propósito, aquello que tiene significado para él. Las personas comprometidas son generosas, ayudan a los demás y contribuyen a crear un clima positivo. Promueven el compromiso de otros.

Algunos estudios indican que el compromiso es un comportamiento cíclico. Se trata de una curva que varía en determinados momentos de la vida laboral. Depende a veces de la trayectoria de cada persona en la empresa. Al comienzo los niveles de compromiso suelen ser mayores y van decayendo con el tiempo. Por eso para la empresa es esencial mantenerse vigilante, medir todo el tiempo y actuar antes de que sea demasiado tarde.

b. Concienciación

Una de las principales tareas del sistema de seguridad en el trabajo es formar conciencia de seguridad como una manera eficiente para evitar riesgos.

Conciencia de seguridad se define como la facilidad para pensar habitualmente, en como eliminar riesgos producto del trabajo que se encuentran presentes en las tareas que normalmente realizamos. Conciencia de seguridad es detenerse un instante a pensar o programar una tarea, para efectuarla eficientemente y en condiciones seguras encuadradas dentro de la normativa de seguridad en el trabajo.

El concepto de conciencia de seguridad de información se toma en la literatura en el sentido de que los usuarios deben ser conscientes de los objetivos de seguridad (y más comprometido con ellos). Las dimensiones de la conciencia de seguridad se basan en la creencia de que la conciencia es un tema que todo aquel que usa alguna forma de servicios de TI, ya sea directa o indirectamente, en

particular en un entorno de Internet, debe tener en cuenta (Siponen, 2001). Por otra parte, la participación pasiva del individuo y el aumento de interés hacia ciertos temas, se considera uno de los componentes clave de concienciación siendo el otro la acción (Namjoo, 2008).

El personal de la organización es la medida más rentable contra violaciones de seguridad. Por lo general son los primeros en ser afectados por los incidentes de seguridad, y su conformidad con la política de seguridad pueden hacer o deshacer un programa de seguridad. Un personal que está al tanto de los problemas de seguridad puede prevenir incidentes y mitigar los daños cuando ocurren incidentes. Dada la importancia del personal como un control de seguridad, por lo tanto, la conciencia es la parte más importante del programa de seguridad de una organización (Rudolph, Warshawsky, & Numkin, 2001).

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.

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. El factor humano en la seguridad es más importante que la tecnología (Desman, 2003).

Según Chen, Shaw y 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.

En muchos de los problemas recientes en seguridad de la información, soluciones de gestión se han aplicado en lugar de soluciones técnicas (Thomson, 1998; Schultz, 2005). 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 se 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.

La negligencia del usuario es un factor crítico en el contexto de seguridad de la información (Yayla, 2012) y esto aumenta si se tiene que los usuarios finales varían extensamente en su nivel de conciencia y conocimiento de cómo controlar las amenazas en sus respectivas instalaciones de computación (Siponen, 2001).

Una forma de luchar con la negligencia es creando conciencia entre los usuarios (Spurling, 1995).El aumento de la concienciación de los usuarios acerca de las amenazas de seguridad y los controles basados en computadoras como autenticaciones y sistemas antivirus les ayudará a comprender la gravedad de las amenazas y también aumentar la utilización de estos mecanismos de control(Richardson, 2009). Los programas de sensibilización tienen dos objetivos principales; a) hacer que los empleados conozcan los procedimientos, normas y regulaciones establecidas en la política de seguridad, y b) hacer que los empleados tomen conciencia de los problemas de seguridad (Yayla,

2012). Además, la gran diferencia entre los usuarios finales en términos de privilegios de acceso, prioridad, motivación complica aún más los esfuerzos de cumplimiento (Siponen, 2001).

Muchas organizaciones han establecido programas de sensibilización sobre la seguridad de la información para asegurarse de que sus empleados estén informados y conscientes de los riesgos de seguridad, de la forma cómo protegerse a sí mismos y de la rentabilidad de la información(Yayla, 2012). Para que un programa de concienciación sobre la seguridad genere valor agregado a la organización y al mismo tiempo hacer una contribución a la seguridad de la información, es necesario contar con un conjunto de métodos para estudiar y medir su efecto (Richardson, 2009).

El crecimiento continuo de las TI y la informatización, hace hincapié en la importancia de la seguridad información y la conciencia individual de todo esto. En un intento por formalizar el tema de dimensiones de la conciencia de seguridad de TI, en Siponen (2001) se desarrolla una clasificación de la siguiente manera:

- La dimensión organizativa.
- La dimensión “público en general”.
- La dimensión “Socio política”.
- La dimensión “Computación ética”.
- La dimensiónde la “Educación institucional”.

1.2.6.2. FACTORES DEL COMPORTAMIENTO ASOCIADOS CON LA INFLUENCIA DEL ENTORNO

c. Motivación

La motivación está constituida por todos los factores capaces de provocar, mantener y dirigir la conducta hacia un objetivo.

La motivación también es considerada como el impulso que conduce a una persona a elegir y realizar una acción entre aquellas alternativas que se presentan en una determinada situación. En efecto, la motivación está relacionada con el impulso, porque éste provee eficacia al esfuerzo colectivo orientado a conseguir los objetivos de la empresa, por ejemplo, y empuja al individuo a la búsqueda continua de mejores situaciones a fin de realizarse profesional y personalmente, integrándolo así en la comunidad donde su acción cobra significado.

Para mantener tal grado de compromiso y esfuerzo, las organizaciones tienen que valorar adecuadamente la cooperación de sus miembros, estableciendo mecanismos que permitan disponer de una fuerza de trabajo suficientemente motivada para un desempeño eficiente y eficaz, que conduzca al logro de los objetivos y las metas de la organización y al mismo tiempo se logre satisfacer las expectativas y aspiraciones de sus integrantes.

En resumen, el estudio de la motivación y su influencia en el ámbito laboral, no es otra cosa que el intento de averiguar, desde el punto de vista de la psicología, a qué obedecen todas esas necesidades, deseos y actividades dentro del trabajo, es decir, investiga la explicación de las propias acciones humanas y su entorno laboral: ¿Qué es lo que motiva a alguien a hacer algo? ¿Cuáles son los determinantes que incitan?. Cuando se produce un comportamiento extraordinario de algún individuo siempre nos parece sospechoso. Frecuentemente intentamos explicar el patrón diferente haciendo referencia a los motivos.

d. Entrenamiento

El entrenamiento es un proceso educativo a corto plazo, aplicado de manera sistemática y organizada, mediante el cual las personas aprenden conocimientos, actitudes y habilidades, en función de objetivos definidos.

El entrenamiento implica la transmisión de conocimientos específicos relativos al trabajo, actitudes frente a aspectos de la organización, de la tarea y del ambiente, y desarrollo de habilidades.

Cualquier tarea, ya sea compleja o sencilla, implica necesariamente estos tres aspectos. Según Flippo, dentro de una concepción más limitada, "el entrenamiento es el acto de aumentar el conocimiento y la pericia de un empleado para el desarrollo de determinado cargo o trabajo:". McGehee señala que "el entrenamiento significa educación especializada. Abarca todas las actividades que van desde la adquisición de habilidad motora hasta la obtención de conocimientos técnicos, el desarrollo de aptitudes administrativas y actitudes referentes a problemas sociales".

Según la National Industrial Conference Board, el propósito del entrenamiento es ayudar a alcanzar los objetivos de la empresa, proporcionando oportunidades a los empleados de todos los niveles para obtener el conocimiento, la práctica y la conducta requeridos por la organización. Algunos autores, como Hoyler ', van más allá, al considerar que el entrenamiento es "una inversión empresarial destinada a capacitar un equipo de trabajo para reducir o eliminar la diferencia entre el desempeño actual y los objetivos y las realizaciones propuestos. En un sentido más amplio, el entrenamiento es un esfuerzo dirigido hacia el equipo, con la finalidad de que el mismo alcance los objetivos de la empresa de la manera más económica posible".

En este sentido, el entrenamiento no es un gasto, sino una inversión cuyo retorno es bastante compensatorio para la organización. El contenido del entrenamiento puede incluir cuatro tipos de cambio de comportamiento:

1. Transmisión de información. El elemento esencial en muchos programas de entrenamiento es el contenido: distribuir información entre los entrenados como un cuerpo de conocimientos. A menudo, la información es genérica y referente al trabajo: información acerca de la empresa, sus productos, sus servicios, su organización, su política, sus reglamentos, etc. Puede cobijar también la transmisión de nuevos conocimientos

2. Desarrollo de habilidades. Sobre todo aquellas destrezas y conocimientos relacionados directamente con el desempeño del cargo actual o de posibles

ocupaciones futuras. Es un entrenamiento orientado de manera directa a las tareas y operaciones que van a ejecutarse.

3. Desarrollo o modificación de actitudes. En general, se refiere al cambio de actitudes negativas por actitudes más favorables entre los trabajadores, aumento de la motivación, desarrollo de la sensibilidad del personal de gerencia y de supervisión, en cuanto a los sentimientos y reacciones de las demás personas. También puede implicar adquisición de nuevos hábitos y actitudes, ante todo, relacionados con los clientes o usuarios (como en el caso de entrenamiento de vendedores, promotores, etc.), o técnicas de ventas.

4. Desarrollo de conceptos. El entrenamiento puede estar dirigido a elevar el nivel de abstracción y conceptualización de ideas y pensamientos, ya sea para facilitar la aplicación de conceptos en la práctica administrativa o para elevar el nivel de generalización, capacitando gerentes que puedan pensar en términos globales y amplios. Estos cuatro tipos de contenido del entrenamiento pueden utilizarse por separado o en conjunto. Por ejemplo, en algunos programas de entrenamiento de vendedores, se incluyen la transmisión de información (acerca de la empresa, los productos, los clientes, el mercado etc), el desarrollo de habilidades (cubrimiento de pedidos, cálculos de precios, etc), y el desarrollo de actitudes (cómo tratar al cliente, cómo comportarse, cómo conducir el proceso de venta, argumentar y afrontar las negativas del cliente, etc) y el desarrollo de conceptos (relacionados con la filosofía de la empresa y la ética profesional).

Uno de los objetivos del entrenamiento es cambiar la actitud de las personas, bien sea para crear un clima más satisfactorio entre los empleados, aumentar su motivación o hacerlos más receptivos a las técnicas de supervisión y gerencia.

1.2.6.3. FACTORES DEL COMPORTAMIENTO ASOCIADOS CON LA PERCEPCIÓN DEL CONTROL

e. Tecnologías basadas en el control

La tecnología (o sistema) de control es cualquier tecnología que permite controlar, generalmente de forma automática (aunque no necesariamente) un ambiente, una máquina, etc.

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. El operario manipula solamente las magnitudes de salida deseadas de ese sistema, llamadas las consignas, y el sistema de control se encarga de gobernarlas por medio de los accionamientos o actuadores correspondientes.

La decisión de que los procesos funcionen en base a regulaciones o parámetro establecidos no disminuyan frente a las nuevas tecnologías de almacenamiento y reproducción de la información, obliga a la entidades a generar opciones tecnológicas que contemplen el control del acceso a la información por parte de los usuarios.

f. Usabilidad de herramientas de seguridad

La usabilidad se refiere a la capacidad de un software o sistema interactivo de ser comprendido, aprehendido, usado fácilmente y atractivo para un usuario, en condiciones específicas de uso. También es la efectividad, eficiencia y satisfacción con la que un sistema informático permite alcanzar sus objetivos específicos.

Esta característica se subdivide a su vez en las siguientes subcaracterísticas (ISO/IEC 2011, 2011):

- Capacidad para reconocer su adecuación. Capacidad del producto que permite al usuario entender si el software es adecuado para sus necesidades.

- Capacidad de aprendizaje. Capacidad del producto que permite al usuario aprender su aplicación.
- Capacidad para ser usado. Capacidad del producto que permite al usuario operarlo y controlarlo con facilidad.
- Protección contra errores de usuario. Capacidad del sistema para proteger a los usuarios de hacer errores.
- Estética de la interfaz de usuario. Capacidad de la interfaz de usuario de agradar y satisfacer la interacción con el usuario.
- Accesibilidad. Capacidad del producto que permite que sea utilizado por usuarios con determinadas características y discapacidades.

1.2.6.4. FACTORES DEL COMPORTAMIENTO ASOCIADOS CON LA CON LA CERTEZA Y SEVERIDAD DE LA SANCIÓN

g. Medidas de disuasión

La disuasión es la acción y efecto de disuadir, y disuadir significa inducir, mover a alguien con razones a mudar de dictamen o a desistir de un propósito; básicamente, la disuasión consiste en convencer a alguien, de una u otra forma, para que cambie su manera de actuar.

Cuando hablamos de seguridad, las medidas de disuasión son las que tratan de "convencer" a alguien hostil para que cese su actitud -al menos ante nosotros-; en muchos casos, son el efecto colateral de salvaguardas reales, pero en ocasiones se utilizan de forma pura, sin ningún otro mecanismo de seguridad real más allá de la intención de "convencer" a un delincuente de que nos deje tranquilos.

Desde siempre, la disuasión ha sido uno de los pilares básicos de la seguridad, junto aspectos como la prevención, la canalización o la detección.

La efectividad de una medida estrictamente disuasoria es cuestionable: por ejemplo, si un potencial atacante descubre que las cámaras son falsas, tendrá el camino libre hacia su objetivo; así, llegado este punto, la disuasión pura habrá dejado de funcionar y deberán entrar en juego otro tipo de salvaguardas más eficaces… Adicionalmente, otro aspecto de las medidas de disuasión puras es el efecto negativo que pueden llegar a tener; si nuestra casa está plagada de controles de acceso, carteles, etc. puede llegar a convertirse, con o sin razón, en un buen reclamo para un potencial atacante, y en ese caso deberemos disponer de más medidas de seguridad para frenar el ataque. Por tanto, el uso excesivo de medidas disuasorias puede ser, en ocasiones, contraproducente.

Bajo mi punto de vista, para que una medida estrictamente disuasoria funcione deben cumplirse dos principios (aparte de aspectos obvios como que la disuasión sea creíble y demás), o al menos una combinación de ambos: percepción de riesgo y direccionalidad del ataque. Con respecto a la percepción del riesgo, el atacante debe percibir -correcta o incorrectamente- un riesgo elevado frente al beneficio que puede obtener con sus actividades. ¿Para qué arriesgar más de lo necesario permitiendo que se grabe su imagen?

Desde el punto de vista de la direccionalidad, las medidas disuasorias pueden ser efectivas frente a ataques no dirigidos, en los que no importa la víctima, pero los ataques dirigidos rara vez se detienen por una medida puramente disuasoria.

La disuasión previene una buena parte de los delitos. Sin embargo, los delincuentes más preparados y determinados verán oportunidades en las medidas disuasorias. Especialmente si las medidas disuasorias son meramente disuasorias, porque no cumplen la función de obstaculizar el delito porque, por ejemplo, estén mal planteadas. El atacante buscará los fallos en las medidas de seguridad.

h. Presión del tiempo y carga del trabajo

La presión el tiempo y de trabajo es una situación en la que se percibe que algo importante depende del resultado de su desempeño. La presión implica sentimientos de ansiedad y a veces temor, que se relacionan con situación que consideramos de “vida o muerte”. En otras palabras, cuando solo tiene una oportunidad para conseguir algo. Es común sentir presión durante una presentación ante un cliente o en una entrevista de trabajo.

El trabajo bajo presión puede ser entendido como aquel trabajo que se realiza bajo condiciones adversas de tiempo o de sobrecarga de tareas, y que demanda mantener la eficiencia y no cometer más errores de lo habitual

.

La exigencia de ser capaz de trabajar bajo presión se ha producido por varias razones.

1. En primer lugar porque el nivel de exigencia de las empresas ha aumentado. En efecto, en un mundo tan competitivo, las empresas deben esforzarse para sobrevivir y desarrollarse, y esto significa recargar con más trabajo a sus empleados para ahorrar en personal y mostrar mejores cifras. Lo mismo puede decirse del aumento de los estándares de calidad, a través de las diversas certificaciones (ISO y otras), que obligan a utilizar procedimientos y controles que anteriormente no existían, y que demandan mayor tiempo.

2. Otro factor que podrían citarse como responsable del trabajo bajo presión es la polifuncionalidad, que se ha transformado en algo común. Es decir, nadie hace solamente una tarea o función, sino varias, y esto desde luego aumenta la carga de trabajo. También la cultura de la respuesta rápida, en el sentido de responder lo mejor y más rápido posible a los clientes, ha estimulado el trabajo bajo presión, ya que por ejemplo, una cotización hay que enviarla "ya", pues de lo contrario los competidores podrían adelantarse y se perdería un negocio.

Lo cierto es que no todos pueden resistir bien el trabajo bajo presión. Hay personas que se abruman con rapidez, y tarde o temprano deben buscar empleos de menor presión, por la amenaza de sufrir un cuadro de estrés.

En efecto, el trabajo bajo presión puede fácilmente producir estrés si la persona no está preparada o no sabe manejar bien el estrés. Lo importante es que cada cual sepa hasta dónde "apretar el acelerador". Cada trabajo tiene un nivel óptimo de estrés. Bajo condiciones de trabajo muy relajado, el rendimiento disminuye, pero paradojalmente, bajo condiciones de mucha presión, también disminuye. El óptimo es un nivel medio de estrés, como han señalado diversos estudios. La mejor manera de lograr un buen ajuste al trabajo bajo presión es organizar muy bien el tiempo; sin embargo esto no siempre es posible, porque las múltiples funcionen desconectan al empleado de lo que estaba haciendo y lo desconcentran. De ahí que mucha gente dice que la hora más productiva de su trabajo es en la mañana, antes de que empiece a sonar el teléfono y las interrupciones.

Otro factor que ayuda es la capacidad de clarificar qué es lo importante y lo urgente, pues a veces las urgencias no requieren realmente de una respuesta tan rápida. Como sea, aprender a trabajar bajo presión es una demanda creciente del mercado laboral, y cada cual debe aprender técnicas que le permitan sortear con éxito esta nueva exigencia.

CAPÍTULO III: METODOLOGÍA DE LA INVESTIGACIÓN

3.1. OBJETIVO GENERAL

El desarrollo de la investigación cumplió con el siguiente objetivo general: Se evaluó los factores que influyen en el comportamiento de los usuarios de TI en relación al cumplimiento de las políticas de seguridad de las tecnologías de la información en las organizaciones del sector microfinanciero de la ciudad de Lambayeque – Perú, con la finalidad de comprender estos comportamientos e indicadores, ya sean detectados a través de la tecnología o por técnicas de observancia humana destinadas a detectar acciones maliciosa o errores, para que posteriormente, se pueda crear ambientes de trabajo productivos, saludables y controlados anticipadamente, que ayude a a reducir las amenazas internas.

3.2. OBJETIVOS ESPECÍFICOS

El desarrollo de la investigación cumplió con los siguientes objetivos específicos:

1. Se evaluó la integración y el compromiso de los usuarios internos de TI como un factor relacionado a la generación de amenazas intencionales sobre el cumplimiento de las políticas de seguridad de la información.

2. Se evaluó el efecto de las medidas de disuasión implementadas por la organización sobre los usuarios internos de TI como un factor de mitigación de amenazas intencionales sobre el cumplimiento de las políticas de seguridad de la información.

3. Se evaluó el efecto de la utilización de tecnologías de control por parte de los usuarios internos de TI como un factor de mitigación de amenazas intencionales en relación al cumplimiento de las políticas de seguridad de la información.

4. Se evaluó la motivación de los usuarios internos de TI como una estrategia de gestión de amenazas no intencionales en relación al cumplimiento de las políticas de seguridad de la información.

5. Se evaluó el entrenamiento de los usuarios internos de TI como una estrategia de gestión de amenazas no intencionales en relación al cumplimiento de las políticas de seguridad de la información.

6. Se evaluó la usabilidad de herramientas de seguridad de la información por parte de los usuarios internos de TI como un factor relacionado a la mitigación de amenazas no intencionales en relación al cumplimiento de las políticas de seguridad de la información.

7. Se evaluó la presión del tiempo y la carga de trabajo en los usuarios internos de TI como un factor que genera amenazas no intencionales en relación al cumplimiento de las políticas de seguridad de la información.

8. Se evaluó la concienciación en seguridad de la información de los usuarios internos de TI como un factor de mitigación de amenazas no intencionales en relación al cumplimiento de las políticas de seguridad de la información.

3.3. DISEÑO DE LA INVESTIGACIÓN

Se tipificó la investigación de la siguiente manera:

a. Por el tipo de estudió, se procedió como una investigación no experimental porque no se manipularon ninguna de las variables estudiadas y éstas fueron analizadas en su contexto natural. No se construyó ninguna situación causal para evaluar sus

efectos. Los sujetos, considerados como unidades de análisis, ya pertenecían a los grupos estudiados (empresas microfinancieras).

b. Por el fin que se persiguió, se procedió como investigación básica, porque no está dirigido hacia un objetivo de aplicación inmediata el modelo propuesto.

c. Por la naturaleza de la investigación, se procedió como una investigación teórica empírica, porque se logró una explicación racional de las teorías aplicadas, fundada en evidencia objetiva.

d. De acuerdo al alcance de la investigación, se procedió como una investigación relacional porque se evaluó el modelo conceptual a través de la asociación entre las variables independientes y la variable dependiente.

e. Por el diseño de la investigación, se procedió como una investigación cuantitativa aplicando la encuesta como técnica e recopilación de información.

3.4. ASPECTOS ÉTICOS Y DE RIGOR CIENTÍFICO

Los criterios éticos que se tomaron en cuenta y las acciones que se realizaron para garantizarlos fueron los siguientes:

Tabla N° 6. Criterios éticos aplicados en la investigación

Criterio	Características éticas del criterio
Consentimiento informado	Los participantes estuvieron de acuerdo con ser informantes y conocer sus derechos y responsabilidades
Confidencialidad	Se aseguró la protección de la identidad de las personas que participaron como informantes de la investigación
Manejo de riesgos	Establecimos principios de no maleficencia y beneficencia para hacer investigación con las personas participantes.
Observación participante	La incursión de los investigadores en el campo (empresas financieras) exigió una responsabilidad ética por los efectos y las consecuencias que pueden derivarse de la interacción establecida con los sujetos participantes de este estudio
Entrevistas	En la interacción social se trató de no provocar actitudes que no condicionen las respuestas de los participantes

Fuente: Adaptación de Noreña, Alcaraz-Moreno, Rojas y Rebolledo-Malpica (2012)

Los criterios de rigor científico que se tomaron en cuenta y las acciones o estrategias se realizaron para garantizarlos fueron los siguientes:

Tabla N° 7. Criterios de rigor científico aplicados a la investigación

Criterio	Características éticas del criterio	Procedimientos
Credibilidad Valor de la verdad/ autenticidad	Aproximación de los resultados de la investigación frente a las observaciones realizadas	– Los resultados fueron reconocidos como "verdaderos" por los participantes – Se realizó observación continua y prolongada delos comportamientos de los usuarios – Triangulación con otras técnicas para corroborar los resultados
Transferibilidad Aplicabilidad	Los resultados derivados de la investigación cualitativa deben ser transferibles y no generalizables	– Realizamos una descripción detallada del contexto y de los participantes – Aplicamos técnicas de muestreo teórico – Realizamos recogida exhaustiva de datos
Consistencia Dependencia/réplica bilidad	Como parte de la investigación cualitativa, la complejidad de ésta dificultó la estabilidad de los datos. Tampoco será posible la replicabilidad exacta del estudio	– Triangulación con otras técnicas para corroborar los resultados – Se realizó una descripción detallada del proceso de recogida, análisis e interpretación de los datos.
Confirmabilidad o reflexividad Neutralidad/ objetividad	Los resultados de la investigación garantizarán la veracidad de las descripciones realizadas por los participantes.	– Contrastación de los resultados con la literatura existente – Revisión de hallazgos por otras investigaciones tomadas como antecedentes – Para el desarrollo de la investigación, se realizó la identificación y descripción de las limitaciones y alcances de la investigación
Relevancia	Los resultados de esta investigación permitirán evaluar el logro de los objetivos planteados y saber si se obtuvo un mejor conocimiento del objeto de estudio	– Se trató en lo posible describir la comprensión amplia delos comportamientos de los usuarios en las empresas tomadas como casos de estudio fenómeno – Existió correspondencia entre la justificación y los resultados obtenidos
Adecuación teórico-epistemológica	Habrá correspondencia adecuada del problema investigado con la teoría existente	– Contrastación de la pregunta con los métodos – Sólo en caso de que sea necesario, se realizarán ajustes de las teorías utilizadas durante el diseño de la propuesta

Fuente: Adaptación de (Noreña, Alcaraz-Moreno, Rojas, & Rebolledo-Malpica, 2012)

3.5. APLICACIÓN DEL INSTRUMENTO DE RECOLECCIÓN DE DATOS

3.5.1. SELECCIÓN DE LA MUESTRA

Para la obtención de la muestra se identificaron 24 entidades financieras con participación en el mercado regional, de las cuales se seleccionaron 8 entidades, por corresponder al sector de aplicación el presente estudio, como es el sector microfinanciero. Se distribuyeron 365 cuestionarios obteniendo una tasa de respuesta del 36.44% (133). Se eliminaron 23 casos por estar incompletos. Finalmente el tamaño de la muestra fue de 110 casos consistentes.

Dado que nuestra unidad de análisis son los usuarios de TI, en cada entidad financiera, éstos cumplen diferentes funciones o tipo de trabajo, se tuvo que identificar las denominaciones para esta variable. La tabla siguiente muestra la distribución de los tipos de trabajo de los usuarios que respondieron a las encuestas de manera consistente.

Tabla N° 8. Denominaciones de trabajo clasificado por tipo de trabajo

Tipo de trabajo	Estandarización de Tipo de trabajo					
	Créditos	**Funcionario**	**Operaciones**	**Plataforma**	**Riesgos**	**Total general**
Administrador de agencias		2				2
Analista de organización y métodos					2	2
Analista de riesgo crediticio					4	4
Analista de crédito	2					2
Analista de créditos master	2					2
Analista de riesgos					2	2
Analista financiero	2					2
Analista senior	2					2
Asesor de créditos	2					2
Asesor	2					2
Asesor comercial	4					4
Asesor comercial master	2					2
Asesor de créditos	2					2
Asesor de finanzas empresariales	6					6
Asesor microfinanzas junior	2					2
Asesor negocios senior	2					2
Asesor ejecutivo	2					2
Asistente de riesgo operacional					2	2
Asistente de servicios	2					2
Control					2	2
Coordinador de créditos	2					2
Créditos	8					8
Directivo		2				2
Funcionario		4				4
Jefe base de datos		2				2
Jefe cobranzas y riesgos		2				2
Jefe comercial		2				2
Jefe créditos		2				2
Jefe de operaciones		2				2
Jefe de organización y métodos		2				2
Operaciones			2			2
Operativo			6			6
Plataforma servicio				2		2
Procurador					1	1
Promotor de servicios			14			14
Representante financiero	8					8
Riesgos					1	1
Total general	**52**	**20**	**22**	**2**	**14**	**110**

Fuente: desarrollo propio

Como se puede observar la dispersión de los tipos de trabajo es significativa, se tuvo que estandarizarlo de la forma como se muestra en la tabla siguiente:

Tabla N° 9. Estandarización de los diferentes tipos de trabajo en las entidades financieras

Tipo	Descripción
Plataforma	Personal que ofrece información a los clientes de los servicios de la entidad financiera, apertura cuentas, etc.
Operaciones	Personal que trabaja entregando o recibiendo dinero a los clientes por sus transacciones.
Créditos	Personal que trabaja ofreciendo el servicio de crédito en diversas modalidades
Riesgos	Personal que trabaja en el área que procura la salvaguarda de los activos de la entidad financiera
Funcionario	Cualquier tipo de jefe a diferente nivel

Fuente: desarrollo propio

Tomando como referencia, la estandarización mostrada en la tabla N° 8, la frecuencia por tipo de trabajo de los usuarios de TI que respondieron consistentemente las encuestas se muestra en la tabla siguiente.

Tabla N° 10. Frecuencia de los tipos de trabajo

Tipo de trabajo	Cantidad	Frecuencia
Créditos	52	47.27%
Operaciones	22	20.00%
Funcionario	20	18.18%
Riesgos	14	12.73%
Plataforma	2	1.82%
Total general	**110**	**100.00%**

Fuente: desarrollo propio

Se utilizó la técnica encuesta y como instrumento un cuestionario elaborado por los investigadores para la recolección de datos (ver anexo N° 1). Este instrumento fue validado a través de una prueba piloto, utilizando el estadístico alfa de Conbrach.

Para la recolección de datos se solicitó el permiso a cada una de las entidades microfinancieras, aplicándose esta actividad en horarios disponibles por los trabajadores, que generalmente se realizó en la primera semana de los meses agosto, setiembre y octubre del 2016.

3.5.2. ANÁLISIS DE DATOS

Para el análisis de datos se realizaron los siguientes estudios:

a. un estudio univariado para medir cada una de las variables y dimensiones consideradas en el modelo propuesto, utilizando medidas de tendencia central y medidas de dispersión y distribución de frecuencias.

b. un estudio bivariado porque se midió la relación causal entre las variables y dimensiones consideradas en el modelo propuesto. Primero se realizó la prueba de cada una de las hipótesis a través de p valor y luego se determinó el coeficiente de correlación como estimador puntual para determinar la fuerza de correlación de cada una de las relaciones entre las variables definidas en el modelo propuesto.

Para esta tarea se utilizaron las herramientas informáticas para análisis estadístico de datos: SPSS, Ms Excel y Minitab.

CAPÍTULO IV: MODELO TEÓRICO Y RESULTADOS

4.1. MODELO CONCEPTUAL Y FORMULACIÓN DE HIPÓTESIS

Considerando el marco teórico se propone el modelo conceptual que relacionó las variables de las investigaciones y las dimensiones que se analizaron y evaluaron en la misma.

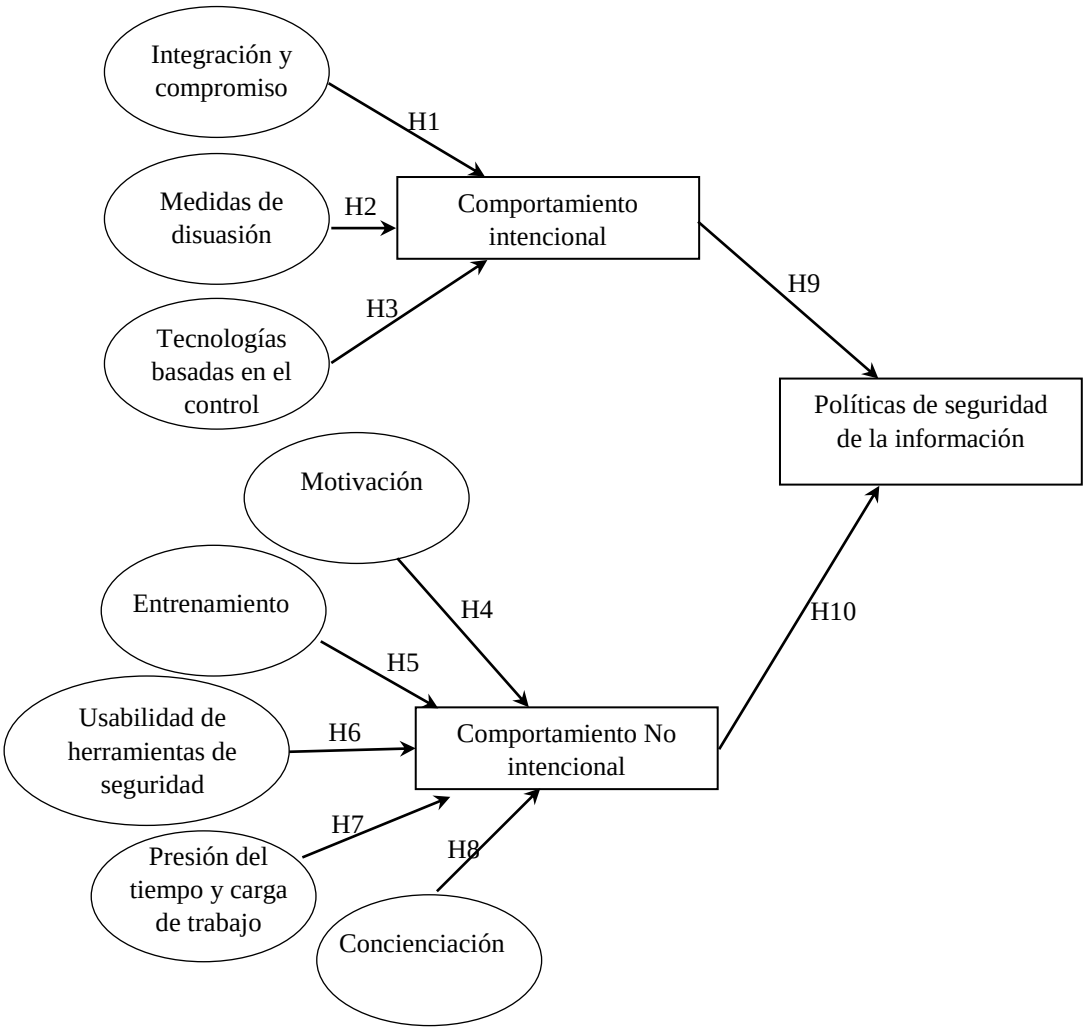


Gráfico N° 9. Modelo conceptual de la investigación

Fuente: Elaboración Propia

Del modelo conceptual se formularon las siguientes hipótesis

4.1.1. HIPÓTESIS GENERALES

H9: La disminución de las amenazas internas provenientes de los comportamientos intencionales aumentará el cumplimiento de las políticas de seguridad de la información.

H10: Disminuir las amenazas internas provenientes de los comportamientos no intencionales aumentará el cumplimiento de las políticas de seguridad de la información.

4.1.2. HIPÓTESIS ESPECÍFICAS

Sobre amenazas internas intencionales a seguridad de la información

Integración y compromiso

H1: Los altos niveles de integración y compromiso de los empleados a su organización reducirán las amenazas internas a la seguridad de la información provenientes del comportamiento intencional

Sobre Medidas de disuasión

H2: Las medidas de disuasión que se refuerzan con acciones disciplinarias reducirán las amenazas internas a la seguridad de la información provenientes del comportamiento intencional.

Tecnología basada en el control

H3: Los mecanismos de control basados en tecnología reducirán las amenazas internas a la seguridad de la información provenientes del comportamiento intencional.

Sobre amenazas internas no intencionales a la Seguridad de la Información

Motivación

H4: El aumento de la motivación intrínseca del usuario reducirá las amenazas internas a la seguridad de la información provenientes del comportamiento no intencional

Entrenamiento

H5: El entrenamiento de los usuarios de herramientas de seguridad reducirá las amenazas internas a la seguridad de la información provenientes del comportamiento no intencional

Usabilidad de Herramientas de Seguridad

H6: Los altos niveles de capacidad de uso de las herramientas de seguridad reducirán las amenazas internas a la seguridad de la información provenientes del comportamiento no intencional

Presión del tiempo y carga de trabajo

H7: La reducción de los niveles de estrés y fatiga relacionados con el trabajo mediante el ajuste de la presión del tiempo y la carga de trabajo reducirá las amenazas internas a la seguridad de la información provenientes del comportamiento no intencional

Concienciación

H8: Aumentar el conocimiento del usuario reducirá las amenazas internas a la seguridad de la información provenientes del comportamiento no intencional

4.2. DEFINICIÓN DE VARIABLES

Variables Independientes:

- Comportamiento intencional de los usuarios de tecnología de información.
- Comportamiento no intencional de los usuarios de tecnología de información.

Variable Dependiente:

– Cumplimiento de las políticas de seguridad de la información.

4.3. OPERACIONALIZACIÓN DE LAS VARIABLES

Tabla N° 11. Operacionalización de variables de la investigación

Variables		Dimensión	Tipo de variable	Escala de variable	Escala por pregunta
Dependiente	Políticas de seguridad de la información.		Discreta	Intervalo	Likert
Independiente	Comportamiento intencional	Integración y compromiso	Discreta	Intervalo	Likert
		Medidas de disuasión	Discreta	Intervalo	Likert
		Tecnologías basadas en el control	Discreta	Intervalo	Likert
	Comportamiento no intencional	Motivación	Discreta	Intervalo	Likert
		Entrenamiento	Discreta	Intervalo	Likert
		Usabilidad de herramientas de seguridad	Discreta	Intervalo	Likert
		Presión del tiempo y carga de trabajo	Discreta	Intervalo	Likert
		Concienciación	Discreta	Intervalo	Likert

Se describe las variables a través de las dimensiones, se ha identificado el tipo de variable, la escala de variable y la escala por pregunta.

4.4. ANÁLISIS Y DISCUSIÓN DE LOS RESULTADOS

En la investigación se diseñó un instrumento que permitió determinar dos variables intervinientes género y tipo de trabajo tipo categórica estandarizándose sus categorías, se realizó la prueba de fiabilidad del instrumento, para determinar el tipo de estudio se realizaron las pruebas de normalidad que determinaron el tipo de estudio a realizar paramétrico o no paramétrico, y dependiendo del tipo de estudio se realizó la prueba de homocedastacidad para determinar igualdad o

diferencia de varianza. Posteriormente se realizaron los contrastes de hipótesis y la evaluación del modelo conceptual.

4.4.1. ESTANDARIZACIÓN DE LAS VARIABLES DE ESCALA CATEGÓRICA

Antes de iniciar el análisis de las observaciones se estandarizaron variables intervinientes que se identificaron en el momento de la aplicación del instrumento en la encuesta, se identificaronlas variables género y tipo de trabajo.

A. Estandarización de la variable Género

Se definió como tipo cuantitativa y escala categórica, las categorías: Femenino y Masculino.

B. Estandarización de la variable de Tipo de trabajo

Se encontró que en las diferentes entidades financieras existen numerosas denominaciones para el mismo tipo de trabajo, se estableció una estandarización para caracterizarlos, como se muestran en las tablas N° 8 y 9. Por tanto, se realizó el estudio considerando solamente a las categorías: créditos, operaciones, funcionario y riesgos.

4.4.2. PRUEBA FIABILIDAD ALFA DE CRONBACH

Se determinó la consistencia interna que permite estimar la fiabilidad del instrumento que se diseñó a través de ítems que midieron el mismo constructo o dimensión teórica. La fiabilidad de la consistencia interna del instrumento se puede estimar con el alfa de Cronbach. La medida de la fiabilidad mediante el alfa de Cronbach asume que los ítems (medidos en escala tipo Likert) miden un mismo constructo y que están altamente relacionados (Welch & Comer, 1988).

Se ha considerado el criterio propuesto por George y Mallery (2003) que las recomendaciones siguientes para evaluar los coeficientes de alfa de Cronbach:

- Coeficiente alfa >0,9 es excelente
- Coeficiente alfa >0,8 es bueno
- Coeficiente alfa >0,7 es aceptable
- Coeficiente alfa >0,6 es cuestionable
- Coeficiente alfa >0,5 es pobre
- Coeficiente alfa <0,5 es inaceptable

El resultado fue el siguiente:

Tabla N° 12. Estadísticos de fiabilidad del instrumento

Alfa de Cronbach	Alfa de Cronbach basada en los elementos tipificados	N de elementos
0,753	0,784	21

Se obtuvo0,753 del estadístico alfa de Cronbach, por lo tanto, se validó la fiabilidad del instrumento con una condición de aceptable.

4.4.3. PRUEBA DE NORMALIDAD DE LOS ÍTEMS DEL INSTRUMENTO

Por el tamaño de observaciones igual a 110 se realizó el test de Kolmogorox-Smirnov para confirmar los resultados.

Para los casos se enunciaron las hipótesis siguientes:

H_0: La distribución de los ítems tiene una distribución aproximada a la distribución normal.

H_1: La distribución de ítems tiene una distribución diferente a la distribución normal.

El criterio de aceptación es aceptar H_0 si p-valor es mayor o igual a 0.05 y rechazar H_0 si p-valor es menor a 0.05.

Tabla N° 13. Resultado de prueba de normalidad Kolmogorov-Smirnov por ítems del instrumento

Ítem	Kolmogorov-Smirnov	Criterio	Descripción	Tipo de test aplicar
P1	0,00	Rechazar H_0	No sigue distribución normal	No Paramétrico
P2	0,00	Rechazar H_0	No sigue distribución normal	No Paramétrico
P3	0,00	Rechazar H_0	No sigue distribución normal	No Paramétrico
P4	0,00	Rechazar H_0	No sigue distribución normal	No Paramétrico
P5	0,00	Rechazar H_0	No sigue distribución normal	No Paramétrico
P6	0,00	Rechazar H_0	No sigue distribución normal	No Paramétrico
P7	0,01	Rechazar H_0	No sigue distribución normal	No Paramétrico
P8	0,00	Rechazar H_0	No sigue distribución normal	No Paramétrico
P9	0,00	Rechazar H_0	No sigue distribución normal	No Paramétrico
P10	0,04	Rechazar H_0	No sigue distribución normal	No Paramétrico
P11	0,00	Rechazar H_0	No sigue distribución normal	No Paramétrico
P12	0,01	Rechazar H_0	No sigue distribución normal	No Paramétrico
P13	0,03	Rechazar H_0	No sigue distribución normal	No Paramétrico
P14	0,00	Rechazar H_0	No sigue distribución normal	No Paramétrico
P15	0,00	Rechazar H_0	No sigue distribución normal	No Paramétrico
P16	0,00	Rechazar H_0	No sigue distribución normal	No Paramétrico
P17	0,00	Rechazar H_0	No sigue distribución normal	No Paramétrico
P18	0,01	Rechazar H_0	No sigue distribución normal	No Paramétrico
P19	0,00	Rechazar H_0	No sigue distribución normal	No Paramétrico
P20	0,012	Rechazar H_0	No sigue distribución normal	No Paramétrico
P21	0,00	Rechazar H_0	No sigue distribución normal	No Paramétrico

Fuente: Elaboración propia

Considerando los resultados de prueba de normalidad y su representación gráfica, se realizaron los contrastes de acuerdo al resultado de test no paramétrico.

4.4.4. PRUEBA DE NORMALIDAD DE LAS DIMENSIONES

Se representaron gráficamente los histogramas de frecuencia de cada una de las dimensiones para tener un indicio de tipo de test a realizar, luego por el tamaño de observaciones igual a 110 se realizó el test de Kolmogorox-Smirnov para confirmar los resultados.

Para los casos se enunciaron las hipótesis siguientes:

H_0: La distribución de las dimensiones tiene una distribución aproximada a la distribución normal.

H_1: La distribución de las dimensiones tiene una distribución diferente a la distribución normal.

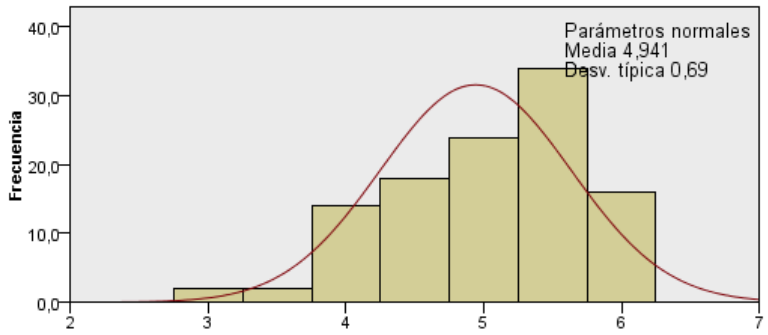


Gráfico N° 10. Histograma y distribución de la dimensión Integración y Compromiso
Fuente: Elaboración propia elaborado con software SPSS

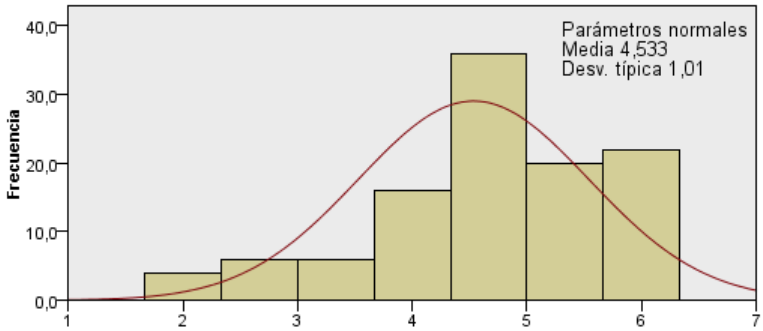


Gráfico N° 11. Histograma y distribución de la dimensión Medidas de disuasión
Fuente: Elaboración propia elaborado con software SPSS

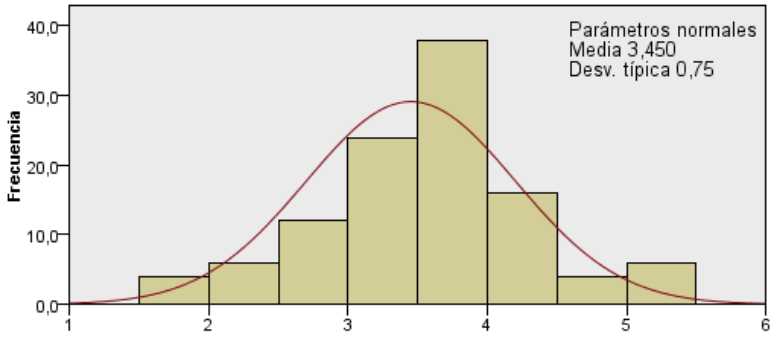


Gráfico N° 12. Histograma y distribución de la dimensión Tecnologías basadas en el control
Fuente: Elaboración propia elaborado con software SPSS

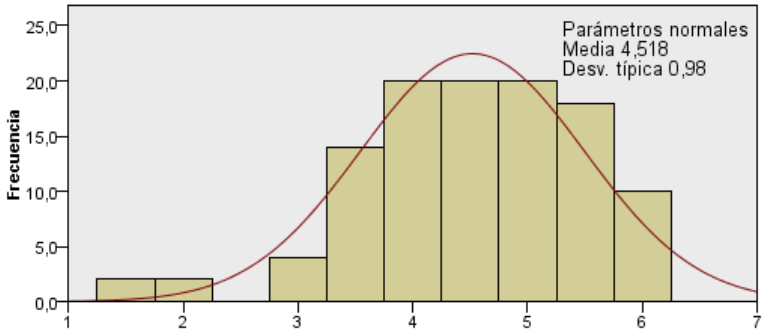


Gráfico N° 13. Histograma y distribución de la dimensión Motivación
Fuente: Elaboración propia elaborado con software SPSS

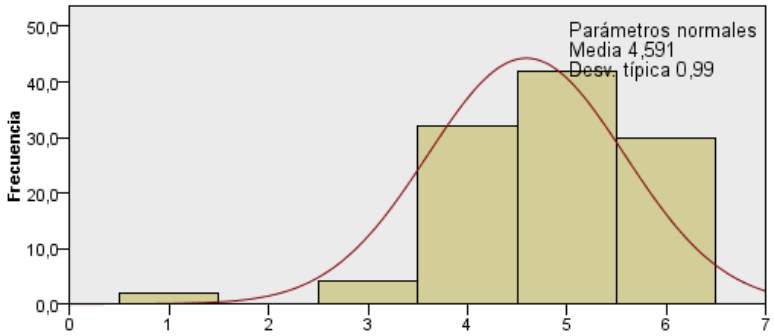


Gráfico N° 14. Histograma y distribución de la dimensión Entrenamiento
Fuente: Elaboración propia elaborado con software SPSS

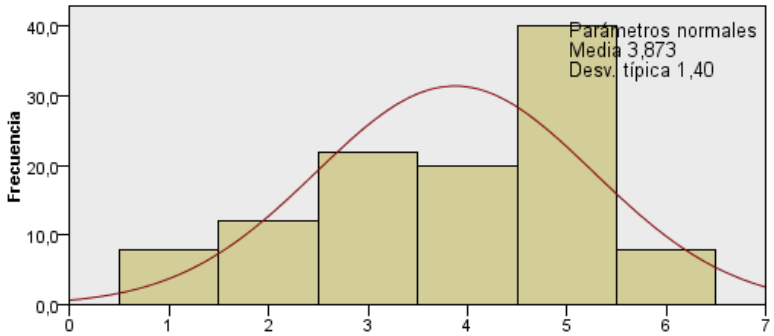


Gráfico N° 15. Histograma y distribución de la dimensión Usabilidad de herramientas de seguridad
Fuente: Elaboración propia elaborado con software SPSS

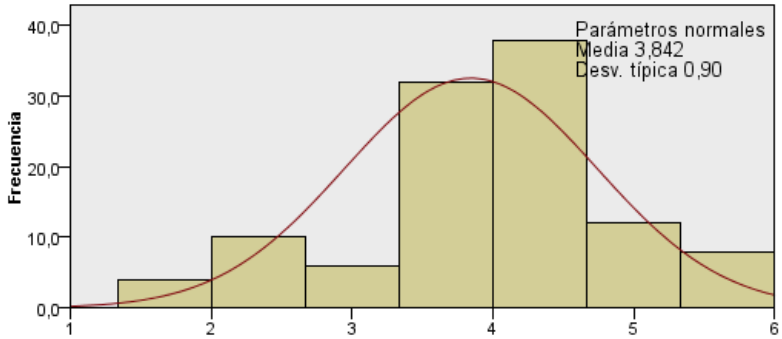


Gráfico N° 16. Histograma y distribución de la dimensión Presión del tiempo y carga del trabajo
Fuente: Elaboración propia elaborado con software SPSS

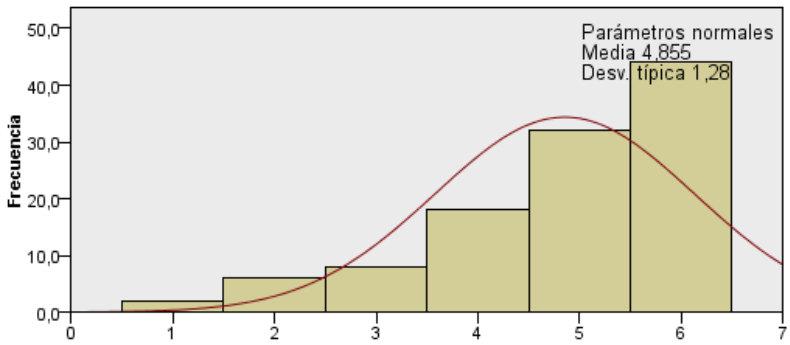


Gráfico N° 17. Histograma y distribución de la dimensión Concienciación
Fuente: Elaboración propia elaborado con software SPSS

Tabla N° 14. Resultado de prueba de normalidad Kolmogorov-Smirnov por dimensiones

Tipo	Dimensión	Kolmogorov-smirnov		Criterio	Descripción	Tipo de test aplicar
		Hipótesis	Sig.			
Dimensiones	Integración y compromiso	La distribución es normal con la media 4,941 y la desviación típica 0,69.	**0,012**	Rechazar H_0	No sigue distribución normal	No Paramétrico
	Medidas de disuasión	La distribución es normal con la media 4,533 y la desviación típica 1,01	**0,048**	Rechazar H_0	No sigue distribución normal	No Paramétrico
	Tecnologías basadas en el control	La distribución es normal con la media 3,450 y la desviación típica 0,75	**0,144**	Aceptar H_0	Sigue distribución normal	Paramétrico
	Motivación	La distribución es normal con la media 4,518 y la desviación típica 0,98.	**0,063**	Aceptar H_0	Sigue distribución normal	Paramétrico
	Entrenamiento	La distribución es normal con la media 4,591 y la desviación típica 0,99.	**0,016**	Rechazar H_0	No sigue distribución normal	No Paramétrico
	Usabilidad de herramientas de seguridad	La distribución es normal con la media 3,873 y la desviación típica 1,40.	**0,000**	Rechazar H_0	No sigue distribución normal	No Paramétrico
	Presión del tiempo y carga de trabajo	La distribución es normal con la media 3,842 y la desviación típica 0,90.	**0,118**	Aceptar H_0	Sigue distribución normal	Paramétrico
	Concienciación	La distribución es normal con la media 4,855 y la desviación típica 1,28.	**0,000**	Rechazar H_0	No sigue distribución normal	No Paramétrico

Fuente: Elaboración propia

4.4.5. PRUEBA DE NORMALIDAD DE LAS VARIABLES

Se representaron gráficamente los histogramas de frecuencia de cada una de las variables para tener un indicio de tipo de test a realizar, luego por el tamaño de observaciones igual a 110 se realizó el test de Kolmogorox-Smirnov para confirmar los resultados.

Para los casos se enunciaron las hipótesis siguientes:

H_0: La distribución de las dimensiones tiene una distribución aproximada a la distribución normal.

H_1: La distribución de las dimensiones tiene una distribución diferente a la distribución normal.

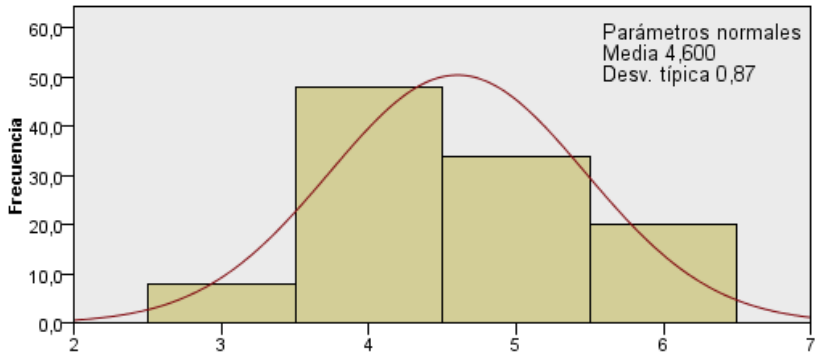


Gráfico N° 18. Histograma y distribución de la variable independiente Comportamiento intencional de los usuarios de tecnología de información

Fuente: Elaboración propia elaborado con software SPSS

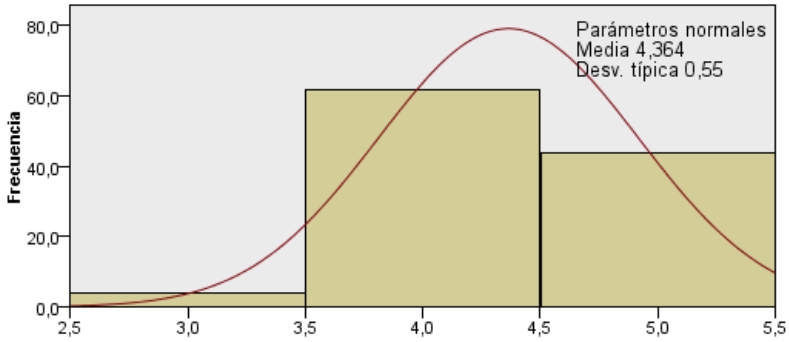


Gráfico N° 19. Histograma y distribución de la variable independiente Comportamiento No intencional de los usuarios de tecnología de información
Fuente: Elaboración propia elaborado con software SPSS

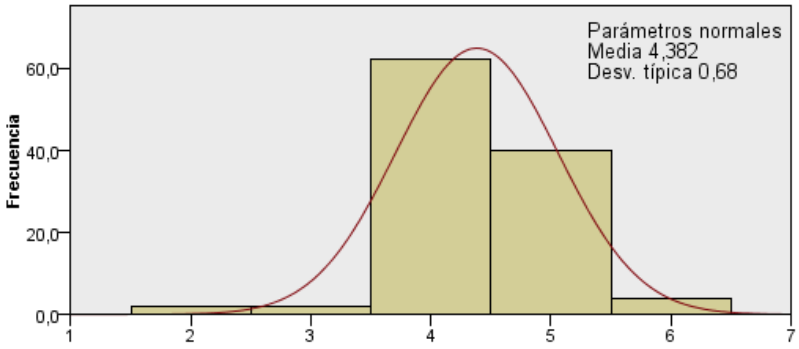


Gráfico N° 20. Histograma y distribución de la variable dependiente Políticas de seguridad de la información
Fuente: Elaboración propia elaborado con software SPSS

Tabla N° 15.Resultado de prueba de normalidad Kolmogorov-Smirnov por dimensiones

Tipo	Dimensión	Kolmogorov-smirnov		Criterio	Descripción	Tipo de test aplicar
		Hipótesis	Sig.			
Variable Independiente	Comportamiento intencional	La distribución es normal con la media 4,6 y la desviación típica 0,87.	**0,000**	Aceptar H_0	No sigue distribución normal	No Paramétrico
	Comportamiento intencional	La distribución es normal con la media 4,364 y la desviación típica 0,55	**0,000**	Aceptar H_0	No sigue distribución normal	No Paramétrico
Dependiente	Políticas de seguridad	La distribución es normal con la media 4,382 y la desviación típica 0,68.	**0,000**	Rechazar H_0	No sigue distribución normal	No Paramétrico

Fuente: Elaboración propia

4.4.5.1. PRUEBA DE NORMALIDAD DETALLADA POR VARIABLE GÉNERO

Se analizó las dimensiones según la categoría del género y por el número de las observaciones, se utilizó el estadístico Kolmogorov-Smirnov cuando las observacionesfueron mayores de 50 y de Shapiro-Wilk cuando las observaciones fueron menores de 50.

Tabla N° 16. Resultado de la prueba de normalidad por género según las dimensiones

Variable	Dimensión	Género	Kolmogorov-Smirnov[a]			Shapiro-Wilk			Criterio	Descripción	Tipo de test aplicar por categoría de genero	Tipo de test aplicar por dimensión
			Estadístico	gl	Sig.	Estadístico	gl	Sig.				
Variable Independiente Comportamiento intencional	Integración y compromiso	Femenino	0,181	46	0,001	0,912	46	**0,002**	Rechazar H_0	No sigue D.N.	No paramétrico	No paramétrico
		Masculino	0,138	64	**0,004**	0,950	64	0,012	Rechazar H_0	No sigue D.N.	No paramétrico	
	Medidas de disuasión	Femenino	0,158	46	0,006	0,920	46	**0,004**	Rechazar H_0	No sigue D.N.	No paramétrico	No paramétrico
		Masculino	0,199	64	**0,000**	0,916	64	0,000	Rechazar H_0	No sigue D.N.	No paramétrico	
	Tecnologías basadas en el control	Femenino	0,168	46	0,002	0,932	46	**0,010**	Rechazar H_0	No sigue D.N.	No paramétrico	No paramétrico
		Masculino	0,153	64	**0,001**	0,943	64	0,005	Rechazar H_0	No sigue D.N.	No paramétrico	
Variable Independiente Comportamiento intencional	Motivación	Femenino	0,152	46	0,009	0,882	46	**0,000**	Rechazar H_0	No sigue D.N.	No paramétrico	No paramétrico
		Masculino	0,130	64	**0,009**	0,955	64	0,020	Rechazar H_0	No sigue D.N.	No paramétrico	
	Entrenamiento	Femenino	0,140	46	0,024	0,942	46	**0,024**	Rechazar H_0	No sigue D.N.	No paramétrico	No paramétrico
		Masculino	0,205	64	**0,000**	0,865	64	0,000	Rechazar H_0	No sigue D.N.	No paramétrico	
	Usabilidad de herramientas de seguridad	Femenino	0,284	46	0,000	0,852	46	**0,000**	Rechazar H_0	No sigue D.N.	No paramétrico	No paramétrico
		Masculino	0,190	64	**0,000**	0,920	64	0,000	Rechazar H_0	No sigue D.N.	No paramétrico	
	Presión del tiempo y carga de trabajo	Femenino	0,163	46	0,004	0,936	46	**0,014**	Rechazar H_0	No sigue D.N.	No paramétrico	No paramétrico
		Masculino	0,149	64	**0,001**	0,954	64	0,018	Rechazar H_0	No sigue D.N.	No paramétrico	
	Presión del tiempo y carga de trabajo	Femenino	0,271	46	0,000	0,783	46	**0,000**	Rechazar H_0	No sigue D.N.	No paramétrico	No paramétrico
		Masculino	0,247	64	**0,000**	0,825	64	0,000	Rechazar H_0	No sigue D.N.	No paramétrico	
Variable Dependiente Políticas de seguridad		Femenino	0,298	46	0,000	0,813	46	**0,000**	Rechazar H_0	No sigue D.N.	No paramétrico	No paramétrico
		Masculino	0,238	64	**0,000**	0,869	64	0,000	Rechazar H_0	No sigue D.N.	No paramétrico	

Por lo tanto las pruebas de contrastes relacionadas conla variable género fueron realizados con un tipo de test no paramétrico, es decir, las distribuciones de las categorías de género por dimensión no siguen una distribución normal.

4.4.5.2. PRUEBA DE NORMALIDAD DETALLADA POR VARIABLE TIPO DE TRABAJO

Tabla N° 17. Resultado de la prueba de normalidad por tipo de trabajo

Variable	Dimensión	Tipo de trabajo	Kolmogorov-Smirnov			Shapiro-Wilk			Criterio	Descripción	Tipo de test aplicar por categoría de trabajo
			Estadístico	gl	Sig.	Estadístico	gl	Sig.			
Variable Independiente Comportamiento intencional	Integración y compromiso	Créditos	0,171	52	**0,001**	0,914	52	0,001	Rechazar H_0	No sigue D.N.	No paramétrico
		Operaciones	0,163	22	0,134	0,909	22	**0,045**	Rechazar H_0	No sigue D.N.	
		Riesgos	0,259	14	0,011	0,884	14	0,067	Aceptar H_0	D.N.	
		Funcionario	0,168	20	0,143	0,919	20	0,096	Aceptar H_0	D.N.	
	Medidas de disuasión	Créditos	0,090	52	**0,200**	0,948	52	0,025	Rechazar H_0	No sigue D.N.	No paramétrico
		Operaciones	0,227	22	0,005	0,859	22	**0,005**	Rechazar H_0	No sigue D.N.	
		Riesgos	0,159	14	0,200	0,917	14	0,199	Aceptar H_0	D.N.	
		Funcionario	0,259	20	0,001	0,786	20	**0,001**	Rechazar H_0	No sigue D.N.	
	Tecnologías basadas en el control	Créditos	0,166	52	**0,001**	0,930	52	0,004	Rechazar H_0	No sigue D.N.	No paramétrico
		Operaciones	0,131	22	0,200	0,950	22	0,314	Aceptar H_0	D.N.	
		Riesgos	0,239	14	0,029	0,801	14	**0,005**	Rechazar H_0	No sigue D.N.	
		Funcionario	0,160	20	0,195	0,871	20	**0,012**	Rechazar H_0	No sigue D.N.	
Variable Independiente Comportamiento intencional	Motivación	Créditos	0,178	52	**0,000**	0,897	52	0,000	Rechazar H_0	No sigue D.N.	No paramétrico
		Operaciones	0,202	22	0,020	0,864	22	**0,006**	Rechazar H_0	No sigue D.N.	
		Riesgos	0,224	14	0,054	0,876	14	0,052	Aceptar H_0	D.N.	
		Funcionario	0,164	20	0,162	0,895	20	**0,033**	Rechazar H_0	No sigue D.N.	
	Entrenamiento	Créditos	0,158	52	**0,002**	0,900	52	0,000	Rechazar H_0	No sigue D.N.	No paramétrico
		Operaciones	0,175	22	0,077	0,901	22	**0,032**	Rechazar H_0	No sigue D.N.	
		Riesgos	0,214	14	0,081	0,823	14	**0,010**	Rechazar H_0	No sigue D.N.	
		Funcionario	0,271	20	0,000	0,827	20	**0,002**	Rechazar H_0	No sigue D.N.	
	Usabilidad de herramientas de seguridad	Créditos	0,258	52	**0,000**	0,794	52	0,000	Rechazar H_0	No sigue D.N.	No paramétrico
		Operaciones	0,275	22	0,000	0,819	22	**0,001**	Rechazar H_0	No sigue D.N.	
		Riesgos	0,393	14	0,000	0,718	14	**0,001**	Rechazar H_0	No sigue D.N.	
		Funcionario	0,214	20	0,017	0,860	20	**0,008**	Rechazar H_0	No sigue D.N.	
	Presión del tiempo y carga de trabajo	Créditos	0,189	52	**0,000**	0,900	52	0,000	Rechazar H_0	No sigue D.N.	No paramétrico
		Operaciones	0,102	22	0,200	0,957	22	0,437	Aceptar H_0	D.N.	
		Riesgos	0,224	14	0,054	0,866	14	**0,037**	Rechazar H_0	No sigue D.N.	
		Funcionario	0,173	20	0,120	0,923	20	0,112	Aceptar H_0	D.N.	
	Concienciación	Créditos	0,206	52	**0,000**	0,866	52	0,000	Rechazar H_0	No sigue D.N.	No paramétrico
		Operaciones	0,258	22	0,001	0,800	22	**0,001**	Rechazar H_0	No sigue D.N.	
		Riesgos	0,302	14	0,001	0,744	14	**0,001**	Rechazar H_0	No sigue D.N.	
		Funcionario	0,351	20	0,000	0,710	20	**0,000**	Rechazar H_0	No sigue D.N.	
Variable Dependiente Políticas de seguridad		Créditos	0,256	52	**0,000**	0,862	52	0,000	Rechazar H_0	No sigue D.N.	No paramétrico
		Operaciones	0,283	22	0,000	0,839	22	**0,002**	Rechazar H_0	No sigue D.N.	
		Riesgos	0,429	14	0,000	0,616	14	**0,000**	Rechazar H_0	No sigue D.N.	
		Funcionario	0,287	20	0,000	0,863	20	**0,009**	Rechazar H_0	No sigue D.N.	

4.5. ANÁLISIS UNIVARIADO

Se realizó el análisis univariado de las dimensiones de las variables con el objeto de describir, analizar y representar su comportamiento.

4.5.1. DATOS DESCRIPTIVOS

Las medidas descriptivas que se utilizaron en esta investigación fueron las medidas de tendencia central media, mediana y moda, las medidas de dispersión como desviación estándar y varianza, y las medidas de distribución la curtosis y asimetría.

a. Dimensión Integración y compromiso

Tabla N° 18. Estadística descriptiva de la dimensión Integración y compromiso

Estadístico	Valor
Media	4.94
Mediana	5.00
Moda	5.50
Desviación estándar	0.69
Varianza de la muestra	0.48
Rango	3.00
Mínimo	3.00
Máximo	6.00
Error típico	0.07
Coeficiente de asimetría	-0.61
Curtosis	-0.04

Se determinó que la dimensión Integración y compromiso es platicúrtica, asimétrica a la derecha y no sigue una distribución normal.

b. Dimensión Disuasión

Tabla N° 19. Estadística descriptiva de la dimensión Medidas de disuasión

Estadístico	Valor
Media	4,53
Mediana	4,67
Moda	4,67
Desviación estándar	1,01
Varianza de la muestra	1,01
Rango	4,00
Mínimo	2,00
Máximo	6.00
Error típico	0.10
Coeficiente de asimetría	-0.61
Curtosis	0,12

Se determinó que la dimensión Disuasión es leptocúrtica, asimétrica a la derecha y no sigue una distribución normal.

c. Dimensión Tecnologías basadas en el control

Tabla N° 20. Estadística descriptiva de la dimensión Tecnologías Basadas en el control

Estadístico	Valor
Media	3,45
Mediana	3,50
Moda	3,75
Desviación estándar	0,75
Varianza de la muestra	0,57
Rango	3,25
Mínimo	1,75
Máximo	5,00
Error típico	0.10
Coeficiente de asimetría	0.23
Curtosis	-0,23

Se determinó que la dimensión Tecnologías basadas en el control es leptocúrtica, asimétrica a la derecha y no sigue una distribución normal.

d. Dimensión Motivación

Tabla N° 21. Estadística descriptiva de la dimensión Motivación

Estadístico	Valor
Media	4,52
Mediana	4,50
Moda	4,50
Desviación estándar	0,98
Varianza de la muestra	0,95
Rango	4,50
Mínimo	1,50
Máximo	6,00
Error típico	0.09
Coeficiente de asimetría	0.23
Curtosis	-0,23

Se determinó que la dimensión Motivación es leptocúrtica, asimétrica a la derecha y no sigue una distribución normal.

e. Dimensión Entrenamiento

Tabla N° 22. Estadística descriptiva de la dimensión Entrenamiento

Estadístico	Valor
Media	4,59
Mediana	4,50
Moda	4,50
Desviación estándar	0,99
Varianza de la muestra	0,98
Rango	5,00
Mínimo	1,00
Máximo	6,00
Error típico	0.09
Coeficiente de asimetría	-0,85
Curtosis	1,90

Se determinó que la dimensión Motivación es leptocúrtica, asimétrica a la derecha y no sigue una distribución normal.

f. Dimensión Herramientas de seguridad

Tabla N° 23. Estadística descriptiva de la dimensión Herramientas de seguridad

Estadístico	Valor
Media	3,87
Mediana	4,00
Moda	5,00
Desviación estándar	1,40
Varianza de la muestra	1,95
Rango	5,00
Mínimo	1,00
Máximo	6,00
Error típico	0.13
Coeficiente de asimetría	-0,51
Curtosis	-0,70

Se determinó que la dimensión Usabilidad de herramientas de seguridad es platicúrtica, asimétrica a la derecha y no sigue una distribución normal.

g. Dimensión Presión del tiempo y carga del trabajo

Tabla N° 24. Estadística descriptiva de la dimensión Presión del tiempo y carga del trabajo

Estadístico	Valor
Media	3,84
Mediana	4,00
Moda	4,33
Desviación estándar	0,90
Varianza de la muestra	0,81
Rango	4,00
Mínimo	1,67
Máximo	5,67
Error típico	0.09
Coeficiente de asimetría	-0,39
Curtosis	0,11

Se determinó que la dimensión Presión del tiempo y carga del trabajo es leptoticúrtica, asimétrica a la derecha y no sigue una distribución normal.

h. Dimensión Concienciación

Tabla N° 25. Estadística descriptiva de la dimensión Concienciación

Estadístico	Valor
Media	4,85
Mediana	5,00
Moda	6,00
Desviación estándar	1,28
Varianza de la muestra	1,63
Rango	5,00
Mínimo	1,00
Máximo	6,00
Error típico	0,12
Coeficiente de asimetría	-0,12
Curtosis	0,64

Se determinó que la dimensión Concienciación es leptoticúrtica, asimétrica a la derecha y no sigue una distribución normal.

i. Variable Políticas de seguridad

Tabla N° 26. Estadística descriptiva de la variable Políticas de seguridad

Estadístico	Valor
Media	4,60
Mediana	4,00
Moda	4,00
Desviación estándar	0,87
Varianza de la muestra	0,76
Rango	3,00
Mínimo	3,00
Máximo	6,00
Error típico	0,08
Coeficiente de asimetría	0,20
Curtosis	-0,77

Se determinó que la dimensión Concienciación es platicúrtica, asimétrica a la izquierda y no sigue una distribución normal.

4.5.2. DESCRIPCION DE LA VARIABLE GÉNERO

Tabla N° 27. Número de observaciones por género

Género	Cantidad	Porcentaje %
Masculino	64	58.18
Femenino	46	41.82
Total	110	100.00

4.5.3. DESCRIPCION DE LA VARIABLE TIPO DE TRABAJO

Tabla N° 28. Frecuencia de los tipos de trabajo

Tipo de trabajo	Cantidad	Frecuencia
Créditos	52	47.27%
Operaciones	22	20.00%
Funcionario	20	18.18%
Riesgos	14	12.73%
Plataforma	2	1.82%
Total general	**110**	100.00%

4.5.4. CONTRASTE DE GENERO POR DIMENSIONES

Se aplicó la prueba de U de Mann-Whitney por que las dimensiones están definidas en una escala de intervalo, el requisito mínimo es una escala ordinal, la variable género es de tipo categórica y tiene solamente dos categorías (dicotómica), las observaciones de ambas categorías es independiente, es un estudio transversal, de alcance correlacional o estudio relacional. Por lo tanto se plantea que las observaciones tienen las mismas características de la población.

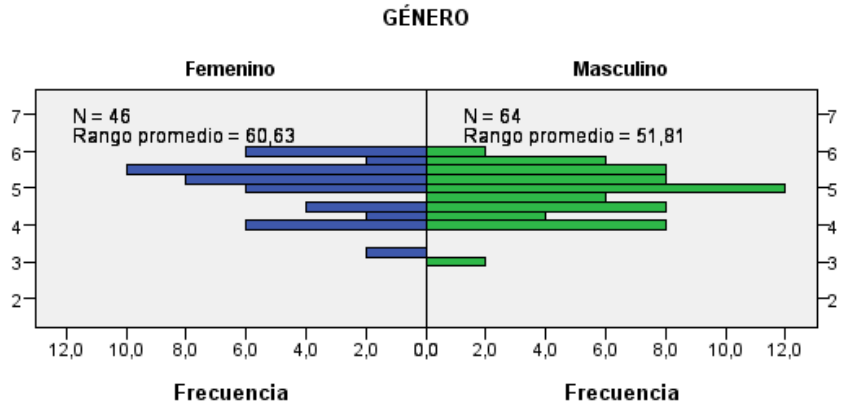


Gráfico N° 21. Contraste de la dimensión Integración y compromiso por género
Fuente: Elaboración propia elaborado con software SPSS

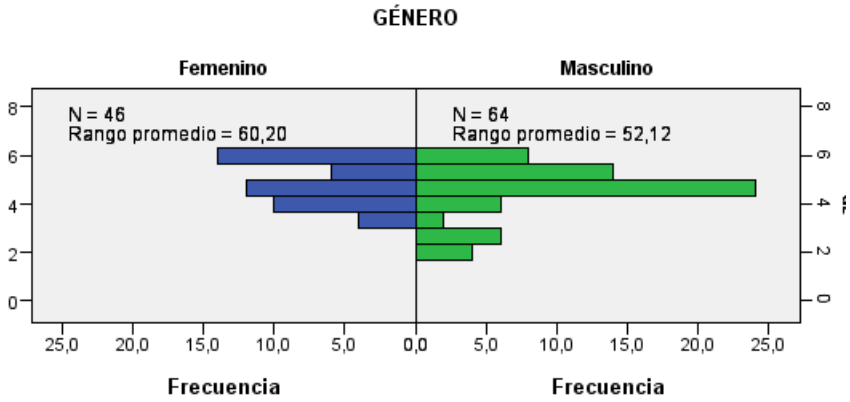


Gráfico N° 22. Contraste de la dimensión Medidas de disuasión por género
Fuente: Elaboración propia elaborado con software SPSS

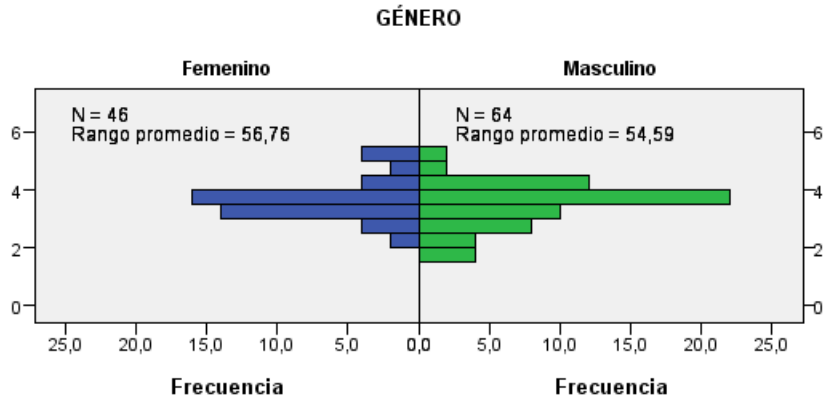


Gráfico N° 23. Contraste de la dimensión Tecnologías basadas en el control por género
Fuente: Elaboración propia elaborado con software SPSS

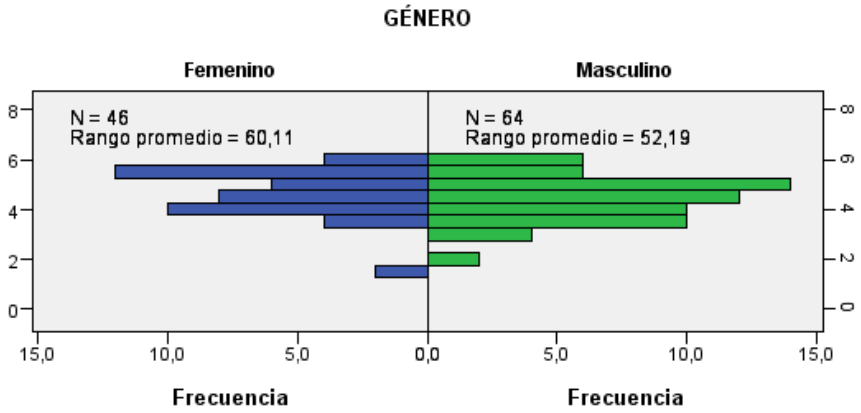


Gráfico N° 24. Contraste de la dimensión Motivación por género
Fuente: Elaboración propia elaborado con software SPSS

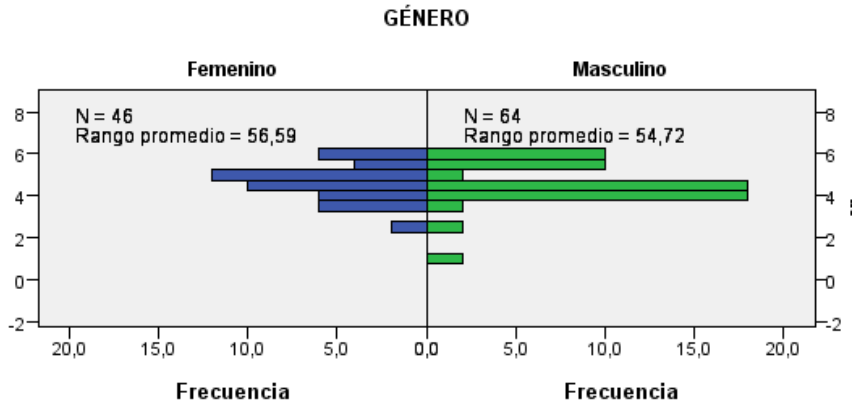


Gráfico N° 25. Contraste de la dimensión Entrenamiento por género
Fuente: Elaboración propia elaborado con software SPSS

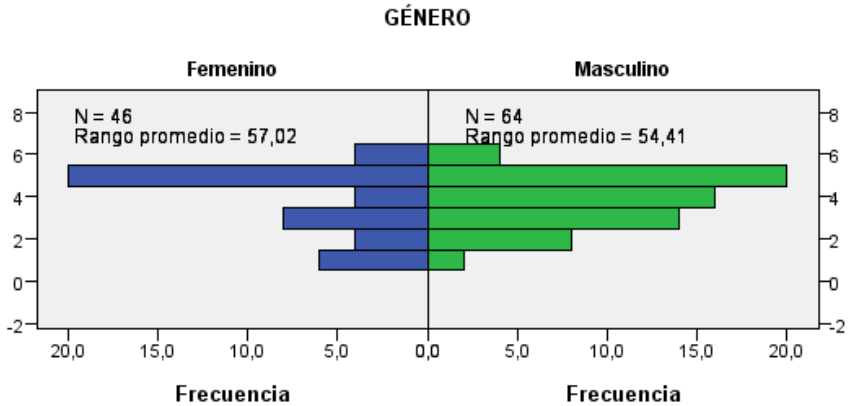


Gráfico N° 26. Contraste de la dimensión Usabilidad de herramientas de seguridad por género
Fuente: Elaboración propia elaborado con software SPSS.

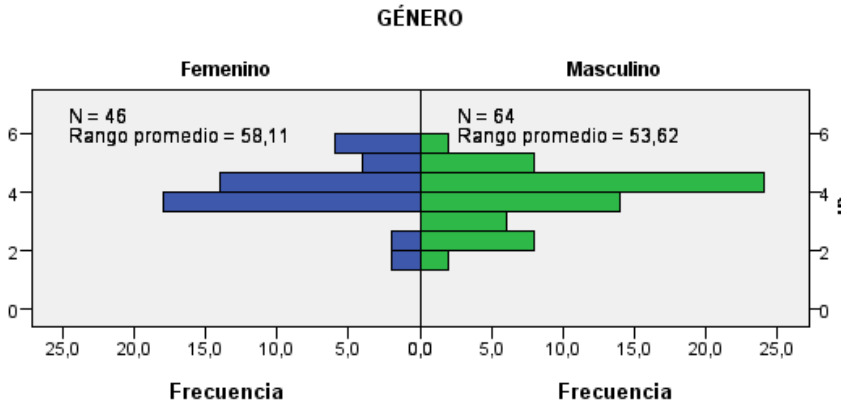


Gráfico N° 27. Contraste de la dimensión Presión del tiempo y carga del trabajo por género
Fuente: Elaboración propia elaborado con software SPSS

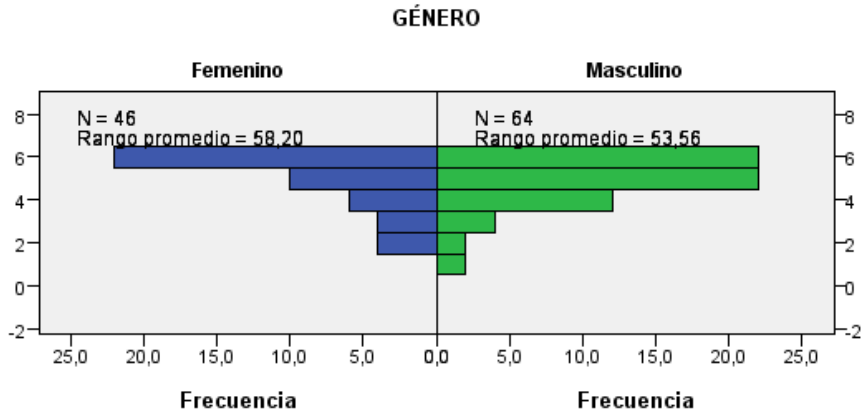


Gráfico N° 28. Contraste de la dimensión Concienciación por género
Fuente: Elaboración propia elaborado con software SPSS

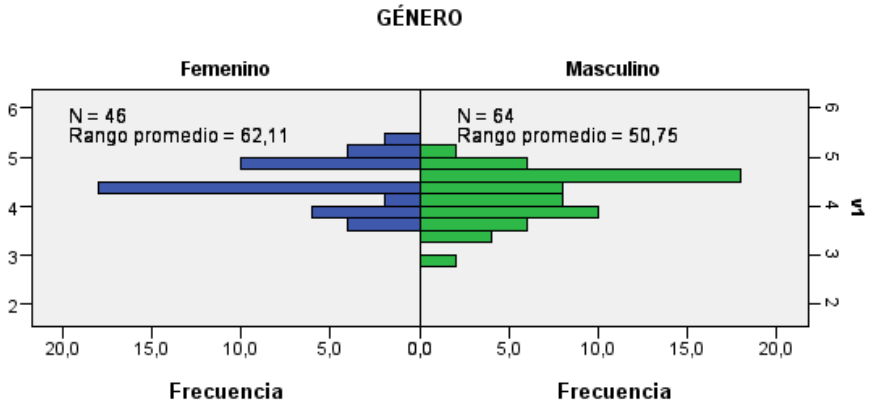


Gráfico N° 29. Contraste de la variable Independiente comportamiento intencional por género
Fuente: Elaboración propia elaborado con software SPSS

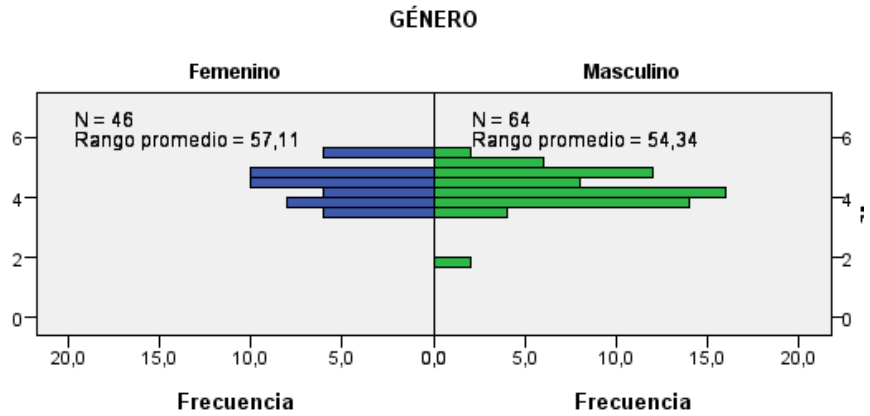


Gráfico N° 30. Contraste de la variable independiente comportamiento No intencional por género

Fuente: Elaboración propia elaborado con software SPSS

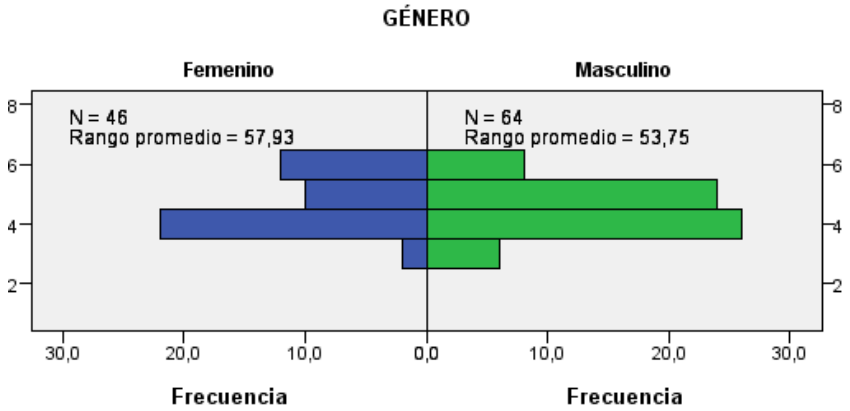


Gráfico N° 31. Contraste de la variable dependiente Políticas de seguridad por género

Fuente: Elaboración propia elaborado con software SPSS

Para la contrastación se formularon las siguientes hipótesis para cada dimensión y variable:

H_0: La distribución es la misma entre las categorías de género.

H_1: La distribución es diferente entre las categorías de género.

Tabla N° 29. Resultado de la prueba de U de Mann-Whitney por dimensiones por género

Variable/ Dimensión		Hipótesis nula	U de Mann-Whitney	W de Wilcoxon	Z	Significancia asintótica (bilateral)	Decisión
Dimensiones	Integración y compromiso	La distribución es la misma entre las categorías de género.	1236,000	3316,000	-1,442	0,149	Aceptar H_0
	Medidas de disuasión	La distribución es la misma entre las categorías de género.	1256,000	3336,000	-1,318	0,187	Aceptar H_0
	Tecnologías basadas en el control	La distribución es la misma entre las categorías de género.	1414,000	3494,000	-,355	0,723	Aceptar H_0
	Motivación	La distribución es la misma entre las categorías de género.	1260,000	3340,000	-1,301	0,193	Aceptar H_0
	Entrenamiento	La distribución es la misma entre las categorías de género.	1422,000	3502,000	-,308	0,758	Aceptar H_0
	Usabilidad de herramientas de seguridad	La distribución es la misma entre las categorías de género.	1402,000	3482,000	-,438	0,661	Aceptar H_0
	Presión del tiempo y carga de trabajo	La distribución es la misma entre las categorías de género.	1352,000	3432,000	-,734	0,463	Aceptar H_0
	Presión del tiempo y carga de trabajo	La distribución es la misma entre las categorías de género.	1348,000	3428,000	-,789	0,430	Aceptar H_0
Variable Independiente	Comportamiento intencional	La distribución es la misma entre las categorías de género.	1453,000	2534,000	-0,132	0,895	Aceptar H_0
	Comportamiento intencional	La distribución es la misma entre las categorías de género.	1450,000	3530,000	-0,152	0,879	Aceptar H_0
Variable Dependiente	Políticas de seguridad	La distribución es la misma entre las categorías de género.	1360,000	3440,000	-0,723	0,470	Aceptar H_0

Se muestran las significancias asintóticas. El nivel de significancia es ,05.

Se determinó que no existe diferencia significativa originada por el género entre las observaciones de cada dimensión por lo tanto el género no debería influenciar en el modelo conceptual propuesto.

4.5.5. CONTRASTE DE TIPO DE TRABAJO POR DIMENSIONES

Se aplicó la prueba de H Kruskal-Wallis por que las dimensiones están definidas en una escala de intervalo, el requisito mínimo una escala ordinal, la variable género es de tipo categórica y tiene más de dos categorías, las observaciones de ambas categorías es independiente, es un estudio transversal, de alcance correlacional o estudio relacional. Por lo tanto, se plantea que las observaciones tienen las mismas características de la población.

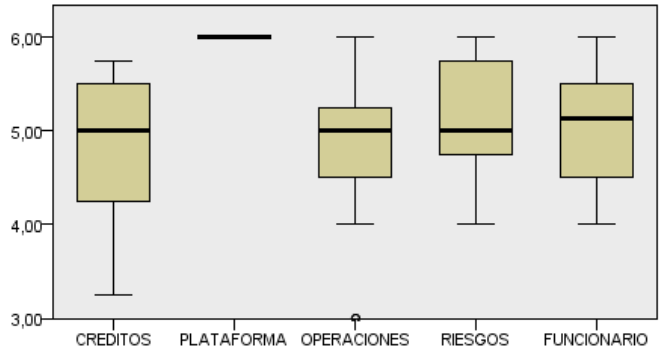


Gráfico N° 32. Diagrama de caja de la dimensión Integración y compromiso
Fuente: Elaboración propia elaborado con software SPSS

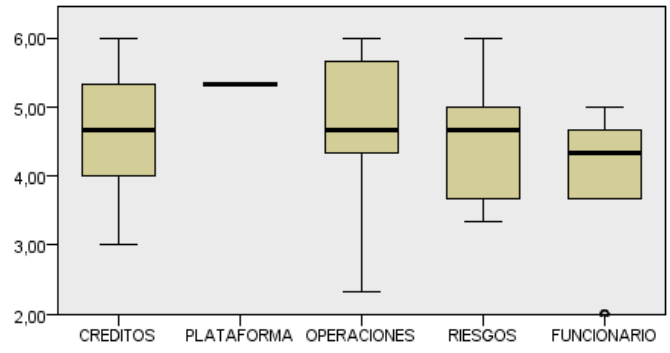


Gráfico N° 33. Diagrama de caja de la dimensión Métodos de disuasión
Fuente: Elaboración propia elaborado con software SPSS

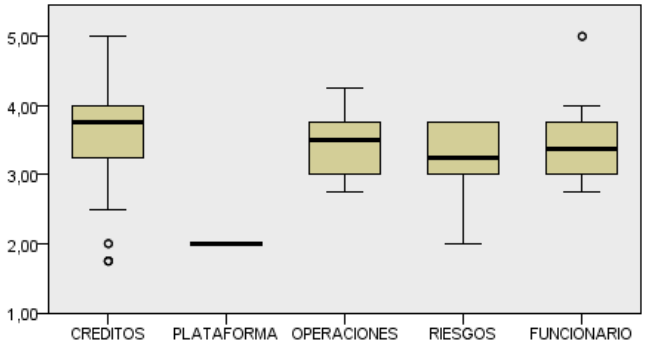


Gráfico N° 34. Diagrama de caja de la dimensión Tecnologías basadas en el control
Fuente: Elaboración propia elaborado con software SPSS

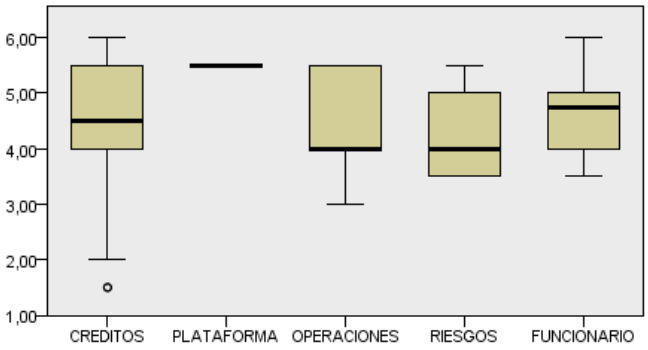


Gráfico N° 35. Diagrama de caja de la dimensión Motivación
Fuente: Elaboración propia elaborado con software SPSS

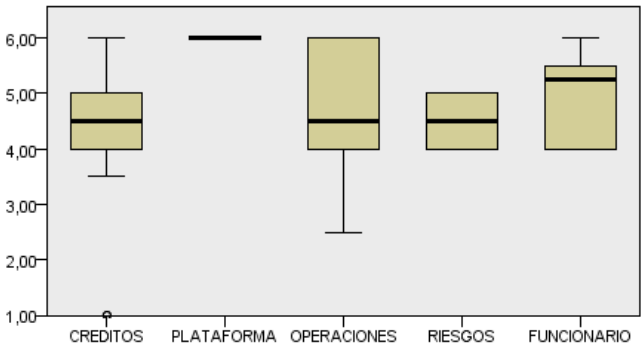


Gráfico N° 36. Diagrama de caja de la dimensión Entrenamiento
Fuente: Elaboración propia elaborado con software SPSS

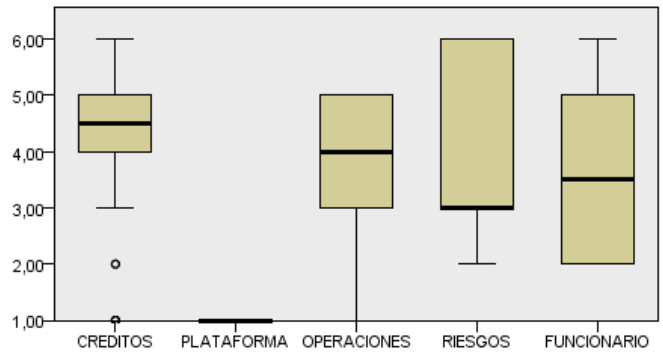


Gráfico N° 37. Diagrama de caja de la dimensión Usabilidad de herramientas de seguridad
Fuente: Elaboración propia elaborado con software SPSS

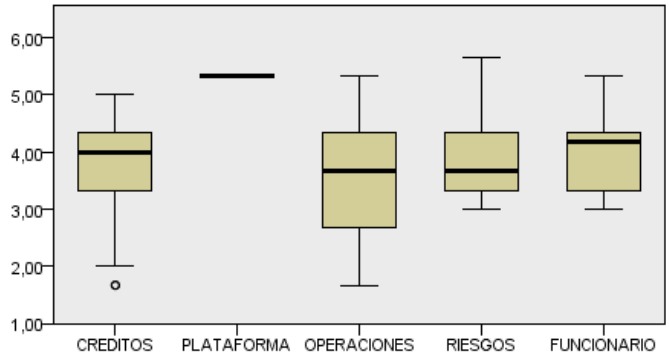


Gráfico N° 38. Diagrama de caja de la dimensión Presión del tiempo y carga del trabajo
Fuente: Elaboración propia elaborado con software SPSS.

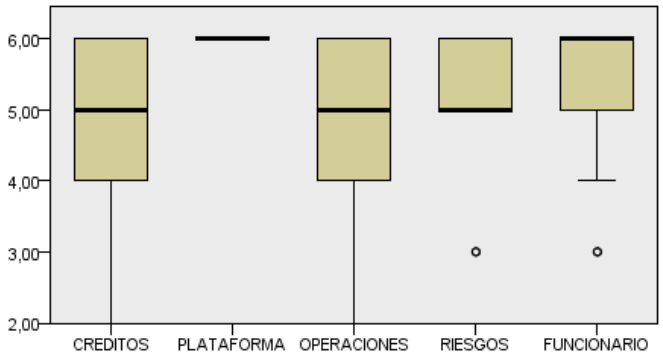


Gráfico N° 39. Diagrama de caja de la dimensión Concienciación
Fuente: Elaboración propia elaborado con software SPSS.

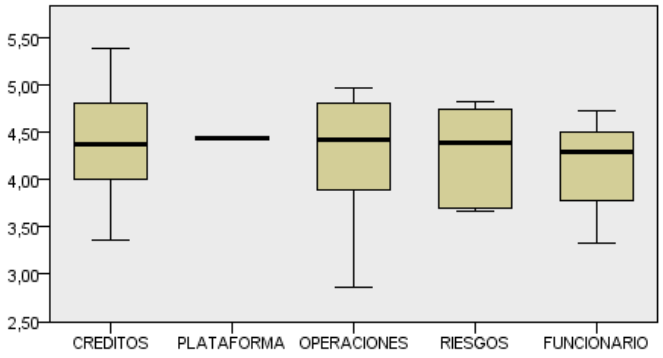


Gráfico N° 40. Diagrama de caja de la variable independiente Comportamiento intencional
Fuente: Elaboración propia elaborado con software SPSS

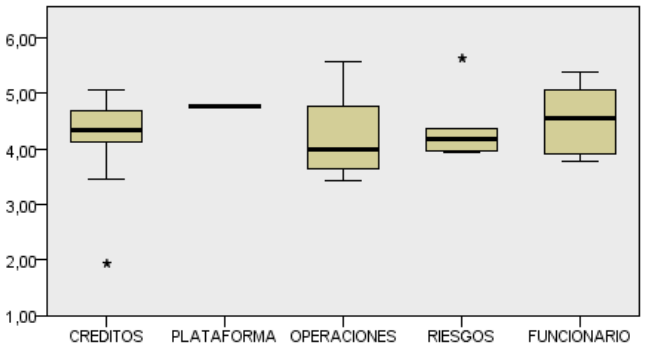


Gráfico N° 41. Diagrama de caja de la variable independiente Comportamiento No intencional
Fuente: Elaboración propia elaborado con software SPSS

Gráfico N° 42. Diagrama de caja de la variable dependiente Políticas de seguridad
Fuente: Elaboración propia elaborado con software SPSS

Para la contrastación se formularon las siguientes hipótesis para cada dimensión y variable:

H_0: La distribución es la misma entre las categorías de tipo de trabajo.

H_1: La distribución es diferente entre las categorías de tipo de trabajo.

Tabla N° 30. Resultado de la prueba de H Kruskal-Wallis por dimensiones por tipo de trabajo

Variable/Dimensión		Hipótesis nula	Chi-cuadrado	Sig.	Decisión
Dimensiones	Integración y compromiso	La distribución es la misma entre las categorías de tipo de trabajo.	6,478	0,166	Aceptar hipótesis nula.
	Medidas de disuasión	La distribución es la misma entre las categorías de tipo de trabajo.	9,973	0,041	Rechazar hipótesis nula.
	Tecnologías basadas en el control	La distribución es la misma entre las categorías de tipo de trabajo.	8,739	0,068	Aceptar hipótesis nula.
	Motivación	La distribución es la misma entre las categorías de tipo de trabajo.	5,818	0,213	Aceptar hipótesis nula.
	Entrenamiento	La distribución es la misma entre las categorías de tipo de trabajo.	7,974	0,093	Aceptar hipótesis nula.
	Usabilidad de herramientas de seguridad	La distribución es la misma entre las categorías de tipo de trabajo.	8,464	0,076	Aceptar hipótesis nula.
	Presión del tiempo y carga de trabajo	La distribución es la misma entre las categorías de tipo de trabajo.	8,545	0,074	Aceptar hipótesis nula.
	Concienciación	La distribución es la misma entre las categorías de tipo de trabajo.	8,793	0,066	Aceptar hipótesis nula.
Variable Independiente	Comportamiento intencional	La distribución es la misma entre las categorías de tipo de trabajo.	1,657	0,799	Aceptar hipótesis nula.
	Comportamiento intencional	La distribución es la misma entre las categorías de tipo de trabajo.	4,967	0,291	Aceptar hipótesis nula.
Variable Dependiente	Políticas de seguridad	La distribución es la misma entre las categorías de tipo de trabajo.	5,005	0,287	Aceptar hipótesis nula.
Se muestran las significancias asintóticas. El nivel de significancia es ,05.					

Se determinó que no existe diferencia significativa originada por el tipo de trabajo entre las observaciones de cada dimensión por lo tanto el tipo de trabajo no debería influenciar en el modelo conceptual propuesto.

4.6. ANÁLISIS BIVARIADO

4.6.1. ANALISIS DE COMPORTAMIENTO INTENCIONAL

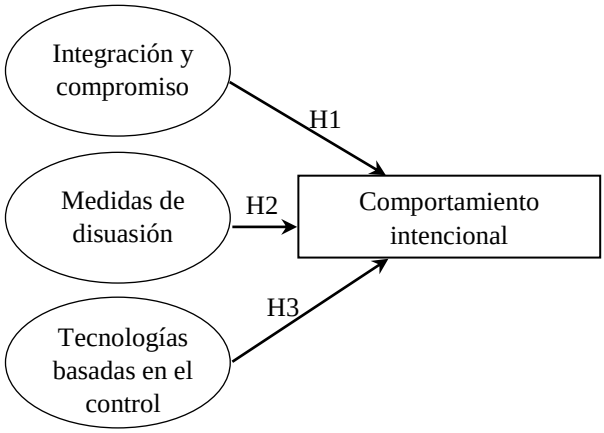


Gráfico N° 43. Dimensiones del Comportamiento intencional
Fuente: Elaboración propia

4.6.1.1. CONTRASTACIÓN DE HIPÓTESIS DE LA VARIABLE COMPORTAMIENTO INTENCIONAL

Se realizó teniendo considerando que las distribuciones no son normales y por lo tanto se realizó un estudio no paramétrico.

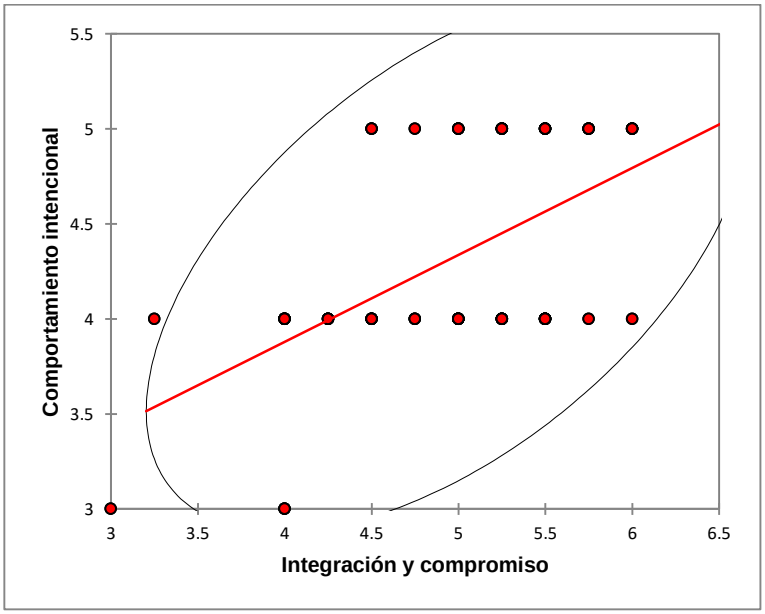


Gráfico N° 44. Gráfico de dispersión entre la dimensión Integración y compromiso yla variable comportamiento intencional

Fuente: Elaboración propia elaborado con software XLSTAT

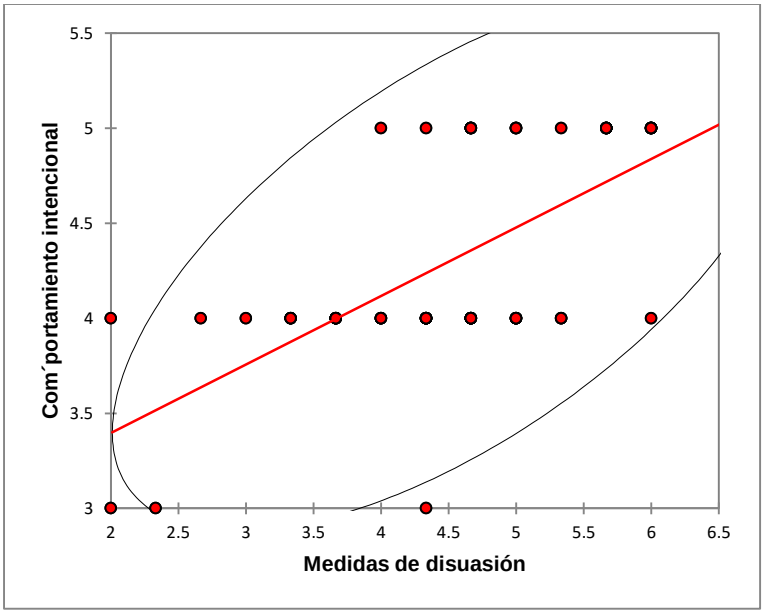


Gráfico N° 45. Gráfico de dispersión entre la dimensión Medidas de disuasión y la variable comportamiento intencional

Fuente: Elaboración propia elaborado con software XLSTAT

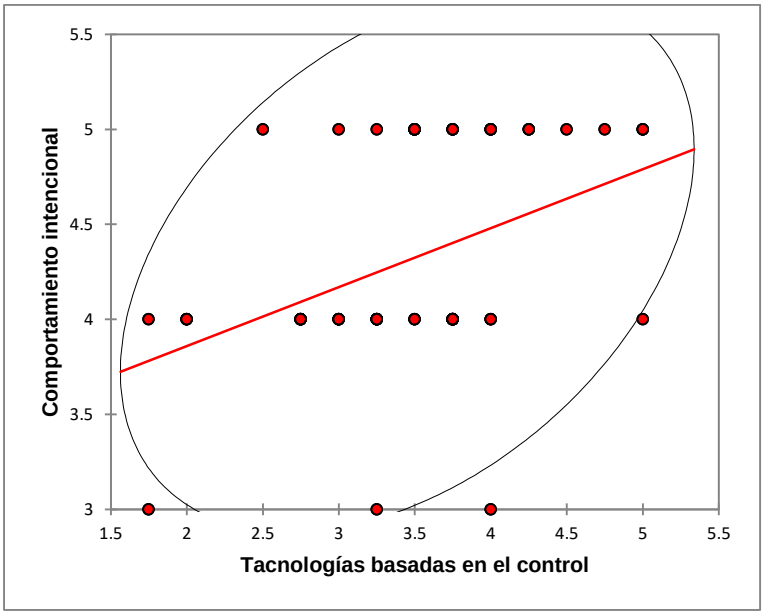


Gráfico N° 46. Gráfico de dispersión entre la dimensión Tecnologías basadas en el control y la variable comportamiento intencional

Fuente: Elaboración propia elaborado con software XLSTAT

Tabla N° 31. Matriz de correlación (Pearson) de las dimensiones del comportamiento intencional

Variable /Dimensión	Integración y compromiso	Medidas de disuasión	Tecnologías basadas en el control	Comportamiento intencional
Integración y compromiso	1.000			
Medidas de disuasión	0.348	1.000		
Tecnologías basadas en el control	-0.023	-0.077	1.000	
Comportamiento intencional	**0.556 valor-p: < 0.0001**	**0.637 valor-p: < 0.0001**	**0.410 valor-p: < 0.0001**	1.000

Fuente: Elaboración propia elaborado con software XLSTAT
Nota 1. Los valores en negrita son diferentes de 0 con un nivel de significación alfa=0.05

Para la contrastación estadísticas se formularon las siguientes hipótesis para validar la correlación entre las unidades de las variables:

H_0: Las unidades de la variable independiente no se correlacionan con las unidades de la variable dependiente.

H_1: Las unidades de una variable independiente se correlacionan con las unidades de la variable dependiente.

Para Integración y compromiso

H1: Los altos niveles de integración y compromiso de los empleados a su organización reducirán las amenazas internas a la seguridad de la información provenientes del comportamiento intencional.

Considerando una probabilidad de error menor a 0,01% que está por debajo de nivel significancia del 5%, se rechaza la hipótesis que no se correlacionan y se acepta que la dimensión Integración y compromiso está correlacionada con el Comportamiento intencional.

Por lo tanto, se validó H2: *Las medidas de integración y compromiso que se refuerzan con acciones disciplinarias reducirán las amenazas internas a la seguridad de la información provenientes del comportamiento intencional.*

Para Medidas de disuasión

H2: Las medidas de disuasión que se refuerzan con acciones disciplinarias reducirán las amenazas internas a la seguridad de la información provenientes del comportamiento intencional.

Considerando una probabilidad de error menor a 0,01% que está por debajo de nivel significancia del 5%, se rechaza la hipótesis que no se correlacionan y se acepta que la dimensión Medidas de disuasión está correlacionada con el Comportamiento intencional.

Por lo tanto, se validó H2: *Las medidas de disuasión que se refuerzan con acciones disciplinarias reducirán las amenazas internas a la seguridad de la información provenientes del comportamiento intencional.*

Para Mecanismos de control basados en tecnología

H3: Los mecanismos de control basados en tecnología reducirán las amenazas internas a la seguridad de la información provenientes del comportamiento intencional.

Considerando una probabilidad de error menor a 0,01% que está por debajo de nivel significancia del 5%, se rechaza la hipótesis que no se correlacionan y se acepta que la dimensión Mecanismos de control basados en tecnología está correlacionada con el Comportamiento intencional.

Por lo tanto, se validó H3: *Los mecanismos de control basados en tecnología reducirán las amenazas internas a la seguridad de la información provenientes del comportamiento intencional.*

4.6.1.2. EVALUACIÓN DEL MODELO CORRESPONDIENTE A LA VARIABLE COMPORTAMIENTO INTENCIONAL

La evaluación del modelo se realizó con la regresión no paramétrica utilizando el método Lowess.

Tabla N° 32. Matriz de coeficientes de determinación de las dimensiones del comportamiento intencional

Dimensión-Variable	**Integración y compromiso**	**Medidas de disuasión**	**Tecnologías basadas en el control**	**Comportamiento intencional**
Integración y compromiso	**1**			
Medidas de disuasión	0.121	**1**		
Tecnologías basadas en el control	0.001	0.006	**1**	
Comportamiento intencional	**0.309**	**0.405**	**0.168**	**1**

La matriz de coeficientes de determinación nos indica la influencia que tiene las dimensiones sobre el comportamiento intencional. El resultado del comportamiento intencional puede ser explicado hasta un 30.9% por la influencia de la dimensión Integración y compromiso, hasta un 40.5% por la influencia de la dimensión Medidas de la disuasión y hasta un 16.8% por la influencia de la dimensión Tecnologías basadas en el control.

La regresión no paramétrica permitió evaluar el modelo obteniendo coeficiente de determinación r^2 de 81,3%, el cual explica el porcentaje en que las dimensiones integración y compromiso, medidas de disuasión y tecnologías basadas en el control son responsables del comportamiento de la variable Comportamiento intencional. La SEC (suma de errores cuadráticos) es de 6,63 y el MEC (error medio cuadrático) es 6,00.

4.6.2. ANALISIS DE COMPORTAMIENTO NO INTENCIONAL

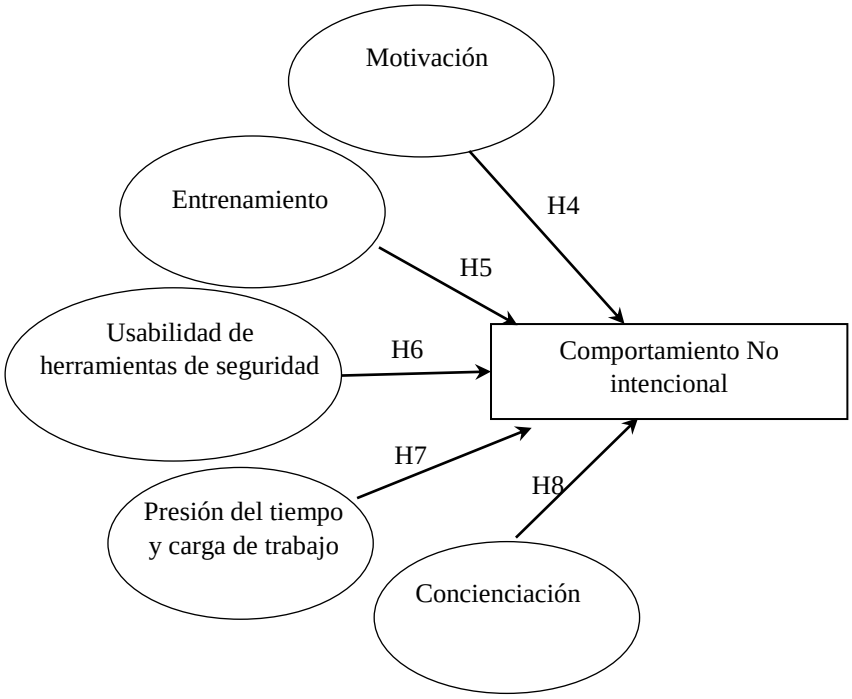


Tabla N° 33. Dimensiones del Comportamiento No intencional
Fuente: Elaboración propia.

4.6.2.1. CONTRASTACIÓN DE HIPÓTESIS DE LA VARIABLE COMPORTAMIENTO NO INTENCIONAL

Se realizó teniendo considerando que las distribuciones no son normales y por lo tanto se realizó un estudio no paramétrico.

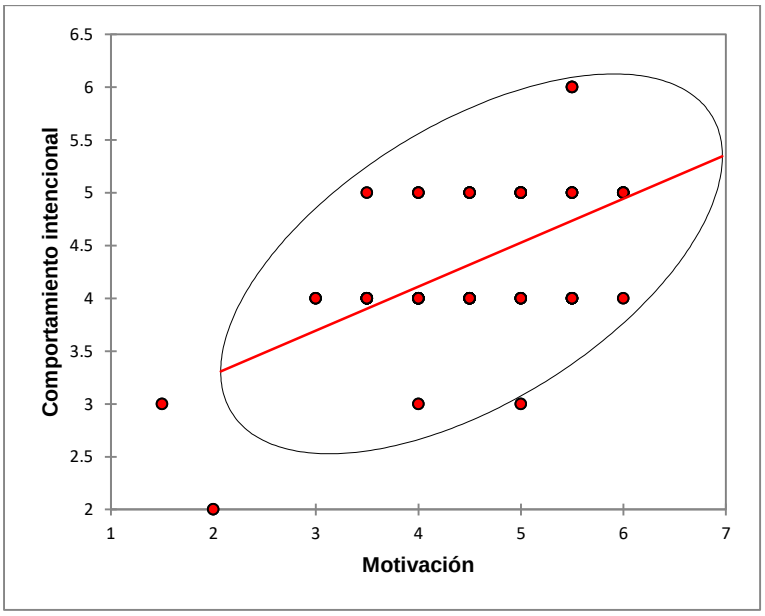


Gráfico N° 47Gráfico de dispersión entre la dimensión Motivación y la variable comportamiento no intencional
Fuente: Elaboración propia elaborado con software XLSTAT

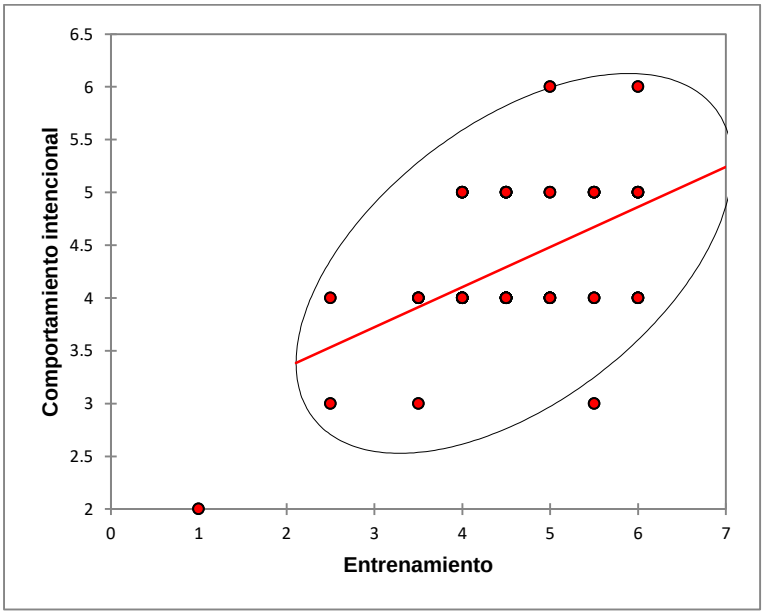


Gráfico N° 48. Gráfico de dispersión entre la dimensión Entrenamiento y la variable comportamiento no intencional
Fuente: Elaboración propia elaborado con software XLSTAT

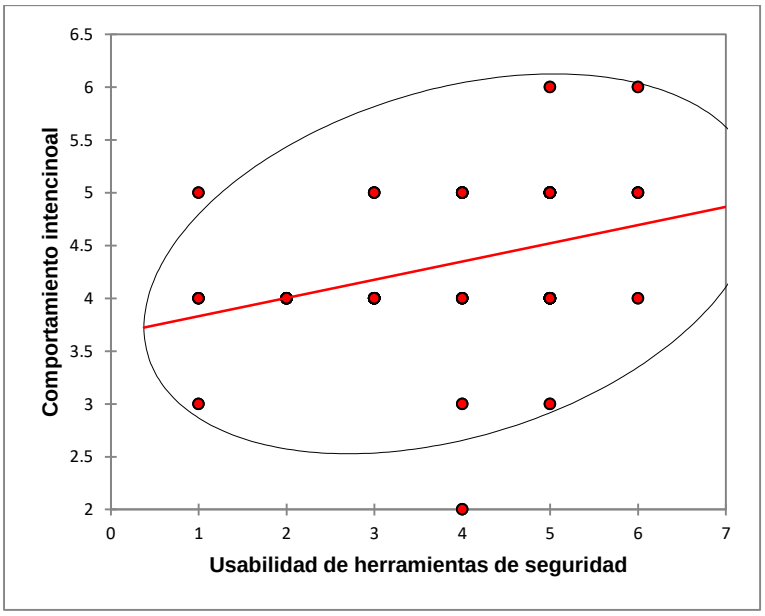


Gráfico N° 49. Gráfico de dispersión entre la dimensión Usabilidad de herramientas de seguridad y la variable comportamiento no intencional
Fuente: Elaboración propia elaborado con software XLSTAT

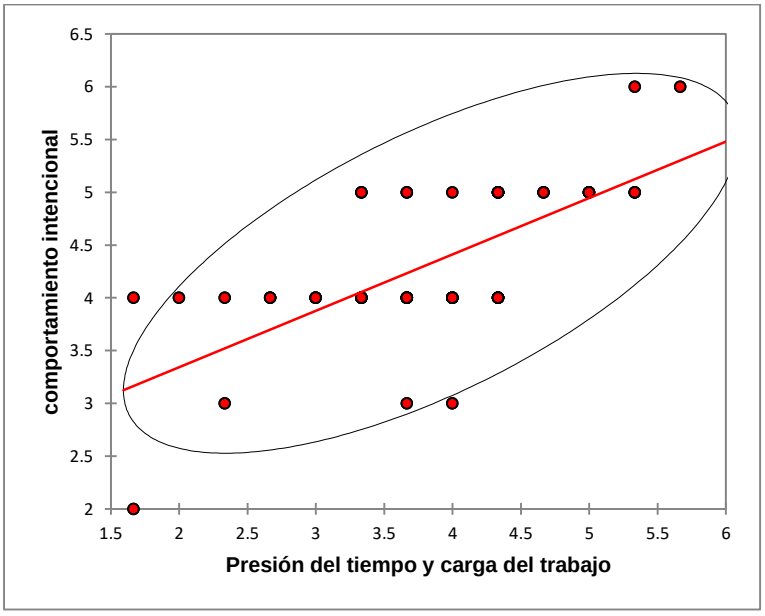


Gráfico N° 50. Gráfico de dispersión entre la dimensión Presión del tiempo y carga del trabajo y la variable comportamiento no intencional
Fuente: Elaboración propia elaborado con software XLSTAT

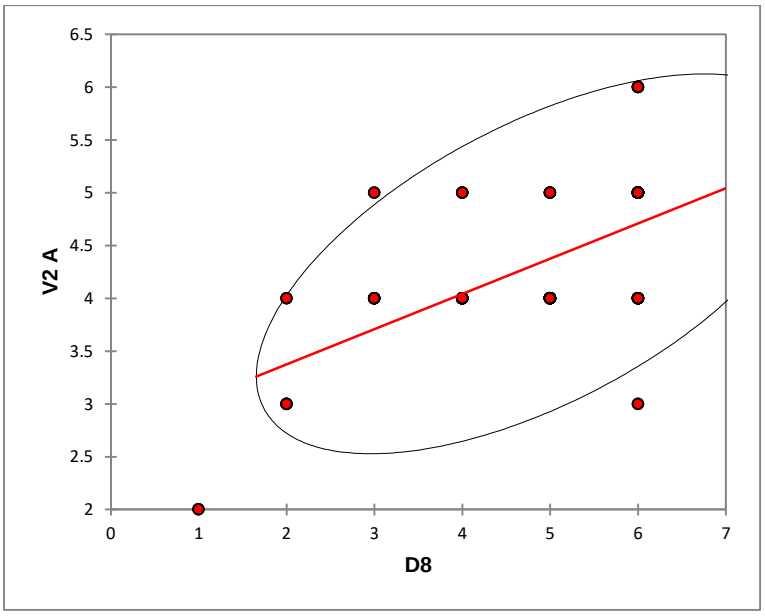


Gráfico N° 51. Gráfico de dispersión entre la dimensión Concienciación y la variable comportamiento no intencional
Fuente: Elaboración propia elaborado con software XLSTAT

Tabla N° 34. Matriz de correlación (Pearson) de las dimensiones del comportamiento no intencional

Variable /Dimensión	Motivación	Entrenamiento	Usabilidad de herramientas de trabajo	Presión del tiempo y carga del trabajo	Concienciación	Comportamiento no intencional
Motivación	1					
Entrenamiento	0.529	1				
Usabilidad de herramientas de trabajo	-0.039	-0.184	1			
Presión del tiempo y carga del trabajo	0.498	0.415	-0.026	1		
Concienciación	0.120	0.170	0.010	0.359	1	
Comportamiento no intencional	**0.567 valor-p: < 0.0001**	**0.525 valor-p: < 0.0001**	**0.335 valor-p: < 0.0001**	**0.669 valor-p: < 0.0001**	**0.593 valor-p: < 0.0001**	1

Fuente: Elaboración propia elaborado con software XLSTAT
Nota 1. Los valores en negrita son diferentes de 0 con un nivel de significación alfa=0.05

Para la contrastación estadísticas se formularon las siguientes hipótesis para validar la correlación entre las unidades de las variables:

H_0: Las unidades de la variable independiente no se correlacionan con las unidades de la variable dependiente.

H_1: Las unidades de una variable independiente se correlacionan con las unidades de la variable dependiente.

Para Motivación

H4: El aumento de la motivación intrínseca del usuario reducirá las amenazas internas a la seguridad de la información provenientes del comportamiento no intencional.

Considerando una probabilidad de error menor a 0,01% que está por debajo de nivel significancia del 5%, se rechaza la hipótesis que no se correlacionan y se acepta que la dimensión Motivación está correlacionada con el Comportamiento no intencional.

Por lo tanto, se validó H4: *El aumento de la motivación intrínseca del usuario reducirá las amenazas internas a la seguridad de la información provenientes del comportamiento no intencional.*

Para Entrenamiento

H5: El entrenamiento de los usuarios de herramientas de seguridad reducirá las amenazas internas a la seguridad de la información provenientes del comportamiento no intencional.

Considerando una probabilidad de error menor a 0,01% que está por debajo de nivel significancia del 5%, se rechaza la hipótesis que no se correlacionan y se acepta que la dimensión Entrenamiento está correlacionada con el Comportamiento no intencional.

Por lo tanto, se validó H5: *El entrenamiento de los usuarios de herramientas de seguridad reducirá las amenazas internas a la seguridad de la información provenientes del comportamiento no intencional.*

Para Usabilidad de herramientas de seguridad

H6: Los altos niveles de capacidad de uso de las herramientas de seguridad reducirán las amenazas internas a la seguridad de la información provenientes del comportamiento no intencional.

Considerando una probabilidad de error menor a 0,01% que está por debajo de nivel significancia del 5%, se rechaza la hipótesis que no se correlacionan y se acepta que la dimensión Usabilidad de herramientas de seguridad está correlacionada con el Comportamiento no intencional.

Por lo tanto, se validó *H6: Los altos niveles de capacidad de uso de las herramientas de seguridad reducirán las amenazas internas a la seguridad de la información provenientes del comportamiento no intencional.*

Para Presión del tiempo y carga del trabajo

H7: La reducción de los niveles de estrés y fatiga relacionados con el trabajo mediante el ajuste de la presión del tiempo y la carga de trabajo reducirá las amenazas internas a la seguridad de la información provenientes del comportamiento no intencional.

Considerando una probabilidad de error menor a 0,01% que está por debajo de nivel significancia del 5%, se rechaza la hipótesis que no se correlacionan y se acepta que la dimensión Presión del tiempo y carga del trabajo está correlacionada con el Comportamiento no intencional.

Por lo tanto, se validó *H7: La reducción de los niveles de estrés y fatiga relacionados con el trabajo mediante el ajuste de la presión del tiempo y la carga de trabajo reducirá las amenazas internas a la seguridad de la información provenientes del comportamiento no intencional*.

Para Concienciación

H8: Aumentar el conocimiento del usuario reducirá las amenazas internas a la seguridad de la información provenientes del comportamiento no intencional.

Considerando una probabilidad de error menor a 0,01% que está por debajo de nivel significancia del 5%, se rechaza la hipótesis que no se correlacionan y se acepta que la dimensión Concienciación está correlacionada con el Comportamiento no intencional.

Por lo tanto, se validó *H8: Aumentar el conocimiento del usuario reducirá las amenazas internas a la seguridad de la información provenientes del comportamiento no intencional.*

4.6.2.2. EVALUACIÓN DEL MODELO CORRESPONDIENTE A LA VARIABLE COMPORTAMIENTO NO INTENCIONAL

La evaluación del modelo se realizó con la regresión no paramétrica utilizando el método Lowess.

Tabla N° 35. Matriz de coeficientes de determinación de las dimensiones del comportamiento no intencional

Variable /Dimensión	**Motivación**	**Entrenamiento**	**Usabilidad de herramientas de trabajo**	**Presión del tiempo y carga del trabajo**	**Conciencia ción**	**Comportamien to intencional**
Motivación	1					
Entrenamiento	0.280	1				
Usabilidad de herramientas de trabajo	0.001	0.034	1			
Presión del tiempo y carga del trabajo	0.248	0.172	0.001	1		
Concienciación	0.014	0.029	0.000	0.129	1	
Comportamiento intencional	**0.321**	**0.276**	**0.112**	**0.447**	**0.351**	1

La matriz de coeficientes de determinación nos indica la influencia que tiene las dimensiones sobre el comportamiento no intencional. El resultado del comportamiento no intencional puede ser explicado hasta un 32,1% por la influencia de la dimensión Motivación, hasta un 27.6% por la influencia de la dimensión entrenamiento, hasta 11,2% por la influencia de la dimensión Presión del tiempo y carga del trabajo, hasta un 44,7% por la influencia de la dimensión Concienciación y hasta un 35,1% por la influencia de la dimensión Concienciación.

La regresión no paramétrica permitió evaluar el modelo obteniendo coeficiente de determinación r^2 de 90,5%, el cual explica el porcentaje en que las dimensiones Motivación, Entrenamiento, Usabilidad de las herramientas de seguridad, Presión del tiempo y carga del trabajo, y Concienciación son responsable del comportamiento de la variable Comportamiento no intencional. La SEC (suma de errores cuadráticos) es de 5,35 y el MEC (error medio cuadrático) es 5.35.

4.6.3. ANALISIS DE LAS VARIABLES DEL MODELO CONCEPTUAL

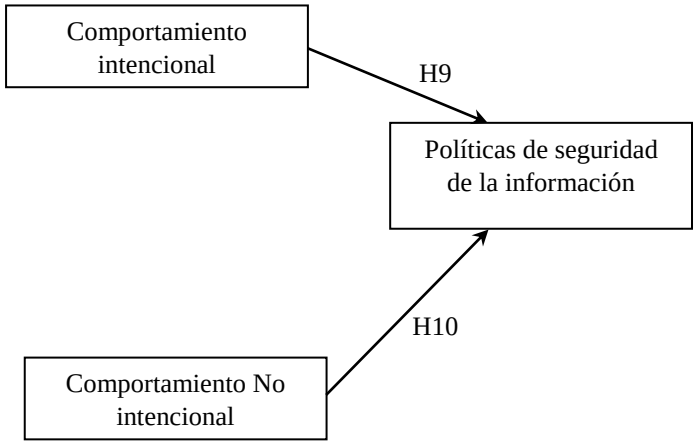


Gráfico N° 52. Variables del modelo propuesto
Fuente: Elaboración propia.

4.6.3.1. CONTRASTACIÓN DE HIPÓTESIS

Se realizó teniendo considerando que las distribuciones no son normales y por lo tanto se realizó un estudio no paramétrico.

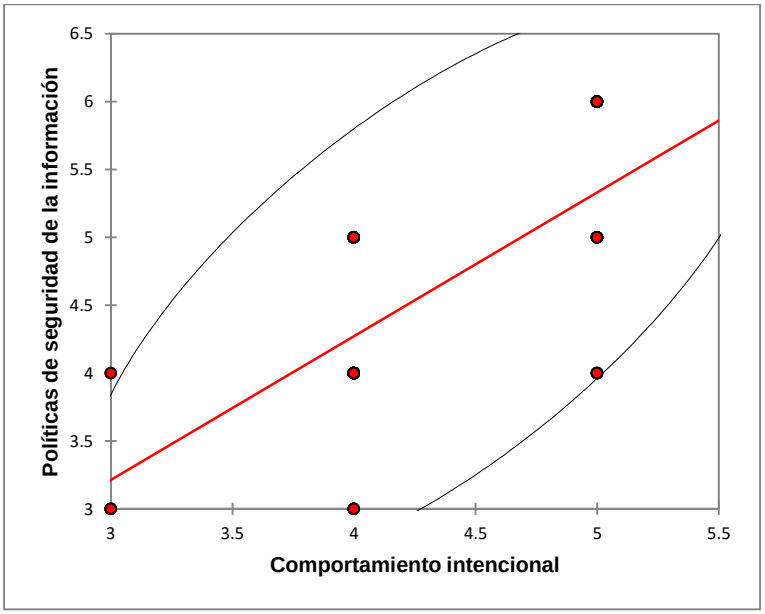


Gráfico N° 53. Gráfico de dispersión entre la variable Comportamiento intencional y la variable Políticas de seguridad
Fuente: Elaboración propia elaborado con software XLSTAT

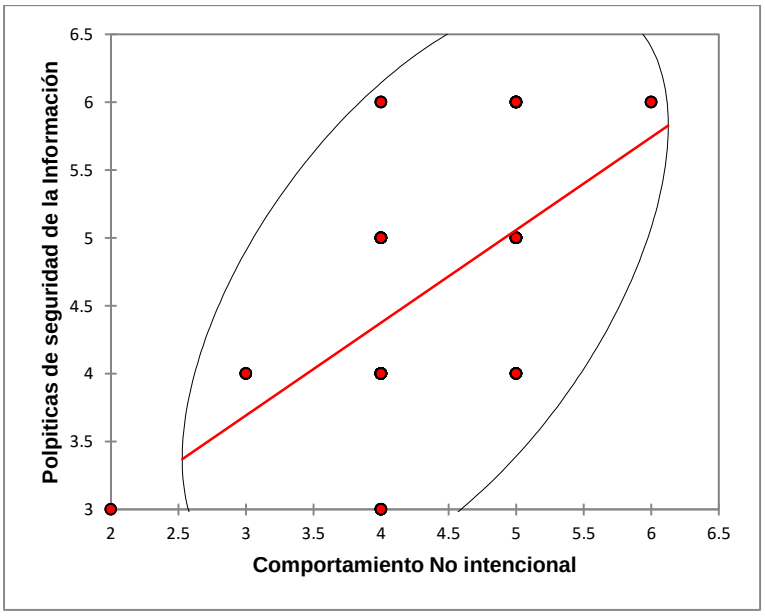


Gráfico N° 54. Gráfico de dispersión entre la variable Comportamiento no intencional y la variable Políticas de seguridad
Fuente: Elaboración propia elaborado con software XLSTAT.

Tabla N° 36. Matriz de correlación (Pearson) de las dimensiones del comportamiento no intencional

Variable /Dimensión	Comportamiento Intencional	Comportamiento No Intencional	Políticas de seguridad
Comportamiento Intencional	1		
Comportamiento No Intencional	0.253	1	
Políticas de seguridad	**0.695 valor-p: < 0.0001**	**0.564 valor-p: < 0.0001**	1

Nota 1. Los valores en negrita son diferentes de 0 con un nivel de significación alfa=0.05

Para la contrastación estadísticas se formularon las siguientes hipótesis para validar la correlación entre las unidades de las variables:

H_0: Las unidades de la variable independiente no se correlacionan con las unidades de la variable dependiente.

H_1: Las unidades de una variable independiente se correlacionan con las unidades de la variable dependiente.

Para Comportamiento Intencional

H9: La disminución de las amenazas internas provenientes de los comportamientos intencionales aumentará el cumplimiento de las políticas de seguridad de la información.

Considerando una probabilidad de error menor a 0,01% que está por debajo de nivel significancia del 5%, se rechaza la hipótesis que no se correlacionan y se acepta que la variable Comportamiento Intencional está correlacionada con las Políticas de seguridad de la información.

Por lo tanto, se validó *H9: La disminución de las amenazas internas provenientes de los comportamientos intencionales aumentará el cumplimiento de las políticas de seguridad de la información.*

Para Comportamiento No Intencional

H10: Disminuir las amenazas internas provenientes de los comportamientos no intencionales aumentará el cumplimiento de las políticas de seguridad de la información.

Considerando una probabilidad de error menor a 0,01% que está por debajo de nivel significancia del 5%, se rechaza la hipótesis que no se correlacionan y se acepta que la variable Comportamiento No Intencional está correlacionada con las Políticas de seguridad de la información.

Por lo tanto, se validó *H10: Disminuir las amenazas internas provenientes de los comportamientos no intencionales aumentará el cumplimiento de las políticas de seguridad de la información.*

4.6.3.2. VALIDACIÓN DEL MODELO CONCEPTUAL GENERAL PROPUESTO

La evaluación del modelo se realizó con la regresión no paramétrica utilizando el método Lowess.

Tabla N° 37. Matriz de coeficientes de determinación del modelo conceptual

Variable /Dimensión	Comportamiento Intencional	Comportamiento No Intencional	Políticas de seguridad
Comportamiento Intencional	1		
Comportamiento No Intencional	0.059	1	
Políticas de seguridad	**0.483**	**0.318**	1

La matriz de coeficientes de determinación nos indica la influencia que tiene las variables Comportamiento Intencional y Comportamiento No Intencional sobre las Políticas de Seguridad de la Información, comportamiento no intencional. El resultado de las Políticas de Seguridad puede ser explicado hasta un 48,3% por la el Comportamiento Intencional y hasta el 31.8% por el Comportamiento No Intencional.

La regresión no paramétrica permitió evaluar el modelo obteniendo coeficiente de determinación r^2 de 63,9%, el cual explica el porcentaje en que las variables Comportamiento Intencional y Comportamiento No Intencional son responsables de las Políticas de Seguridad. La SEC (suma de errores cuadráticos) es de 29,765 y el MEC (error medio cuadrático) es 0,271.

4.7. EVALUACIÓN DEL MODELO

4.7.1. EVALUACIÓN DEL INSTRUMENTO DE RECOLECCIÓN DE DATOS

El instrumento de recolección de datos fue diseñado considerando las recomendaciones de Ajzen en su publicación "Constructing a Theory of Planned Behavior Questionnaire". La fiabilidad del instrumento se realizó mediante el coeficiente de Alfa de Cronbach logrando un valor de 78.4%, que en la escala de George y Mallery (2003) es calificada como buena. Por tanto, el instrumento diseñado puede ser utilizado para la evaluación del comportamiento de los usuarios de tecnologías de información para cumplir con las políticas de seguridad de la información.

La tabla siguiente muestra las especificaciones a tomar en cuenta para la aplicación del instrumento utilizado en la presente investigación.

Tabla N° 38. Especificaciones para la elaboración de la encuesta como instrumento validado en la investigación del comportamiento de los usuarios de tecnologías de información para cumplir con las políticas de seguridad de la información

VARIABLE	DIMENSIÒN	INTERROGANTE	ESCALA	Tratamiento
Políticas de seguridad de la información		1. Usted considera que las políticas de seguridad de la información de su empresa se cumplen o serán cumplidas.	De 1 a 6 1. Más bajo 6. Más alto	
Comportamiento intencional	Integración y Compromiso	1 El propósito o finalidad de las políticas de seguridad de información está muy relacionada con las características de su personalidad	De 1 a 6 1. Más bajo 6. Más alto	
		2 Si usted identifica una situación en la cual debe realizarse una mejora en las políticas de seguridad de información. ¿Qué tan importante es para usted comunicar que debe realizarse dicha mejora?	De 1 a 6 1. Más bajo 6. Más alto	
		3 Siente que está (o estará de acuerdo) a cumplir al cien por ciento con las políticas de seguridad de información de su empresa.	De 1 a 6 1. Más bajo 6. Más alto	
		4 Respecto a la siguiente afirmación: "el respeto a la institucionalidad es muy importante en el logro de sus objetivos", de acuerdo a su experiencia usted se identifica	De 1 a 6 1. Más bajo 6. Más alto	
	Medidas de disuasión	5 Usted cumple con las políticas de seguridad de información porque conoce las medidas disciplinarias	De 1 a 6 1. Más bajo 6. Más alto	
		6 Tiene temor a un mal manejo de la información por las sanciones impuestas.	De 1 a 6 1. Más bajo 6. Más alto	
		7 El conocimiento de las acciones disciplinarias, le han permitido tener cuidado con el manejo de la información.	De 1 a 6 1. Más bajo 6. Más alto	

	Tecnologías basadas en el control	8	Ha tenido incidentes de seguridad de la información (robo de información, accedieron a su equipo o sistema sin su permiso, virus, etc.) pero fueron detectados rápidamente.	De 1 a 6 1. Más bajo 6. Más alto	Invertir
		9	Para verificar que su equipo y sistemas son confiables, alguna vez ha puesto en prueba los controles de seguridad (ingreso con clave errónea, mal ingreso de datos, etc.).	De 1 a 6 1. Más bajo 6. Más alto	Invertir
		10	Sobre los controles instalados en su equipo y sisteMás, ¿considera usted que le han ayudado a no cometer errores de ingreso de información?	De 1 a 6 1. Más bajo 6. Más alto	Invertir
		11	Usted conoce que el ingreso de toda la información desde su equipo es registrado y monitoreado en un proceso de evaluación y auditoría, con respecto a esto, ¿qué nivel de confianza le asigna al equipo (computadora, impresora, etc.) y sistemas informáticos que tiene acceso?	De 1 a 6 1. Más bajo 6. Más alto	Invertir
Comportamiento No Intencional	Motivación	12	Por el buen desempeño de sus labores en relación al cumplimiento de las políticas de seguridad, ¿están claramente establecidos los reconocimientos en la empresa?	De 1 a 6 1. Más bajo 6. Más alto	
		13	Considerando a su empresa ¿Tiene usted la voluntad de hacer el mayor esfuerzo, más allá de lo normalmente esperado, para cumplir y usar adecuadamente las políticas de seguridad de la información?	De 1 a 6 1. Más bajo 6. Más alto	
	Entrenamiento	14	En caso que ocurra alguna incidencia, ¿sabe cómo actuar según las políticas de seguridad de la información de la institución donde labora?	De 1 a 6 1. Más bajo 6. Más alto	
		15	¿Siente que la capacitación o entrenamiento que ha recibido en relación a las políticas de seguridad de la información le ha ayudado para resolver cualquier problema o incidente que se ha presentado?	De 1 a 6 1. Más bajo 6. Más alto	
	Usabilidad de herramientas de seguridad	16	Considera usted que los sistemas son de difícil acceso.	De 1 a 6 1. Más bajo 6. Más alto	Invertir
	Presión del tiempo y carga de trabajo	17	Se dice que en su trabajo "se trabaja bajo objetivos y presión". ¿Considera usted que puede lograrse un trabajo sin errores bajo estas condiciones?	De 1 a 6 1. Más bajo 6. Más alto	
		18	En su trabajo, ¿con qué frecuencia a cometido errores de seguridad de información (registro de datos, errores de cálculo, etc.) debido a la presión y carga de trabajo?	De 1 a 6 1. Más bajo 6. Más alto	Invertir
		19	Considera que la empresa ha implementado políticas para el manejo del tiempo y carga de trabajo han logrado su objetivo	De 1 a 6 1. Más bajo 6. Más alto	
	Concienciación	20	Cuántos errores relacionados con sisteMás de información usted ha cometido por falta de conocimiento de las políticas de seguridad de la información.	De 1 a 6 1. Más bajo 6. Más alto	Invertir

Fuente: Elaboración propia

4.7.2. SIGNIFICADO DE LOS RESULTADOS OBTENIDOS CON EL MODELO PROPUESTO EN EL ANÁLISIS DE CORRELACION

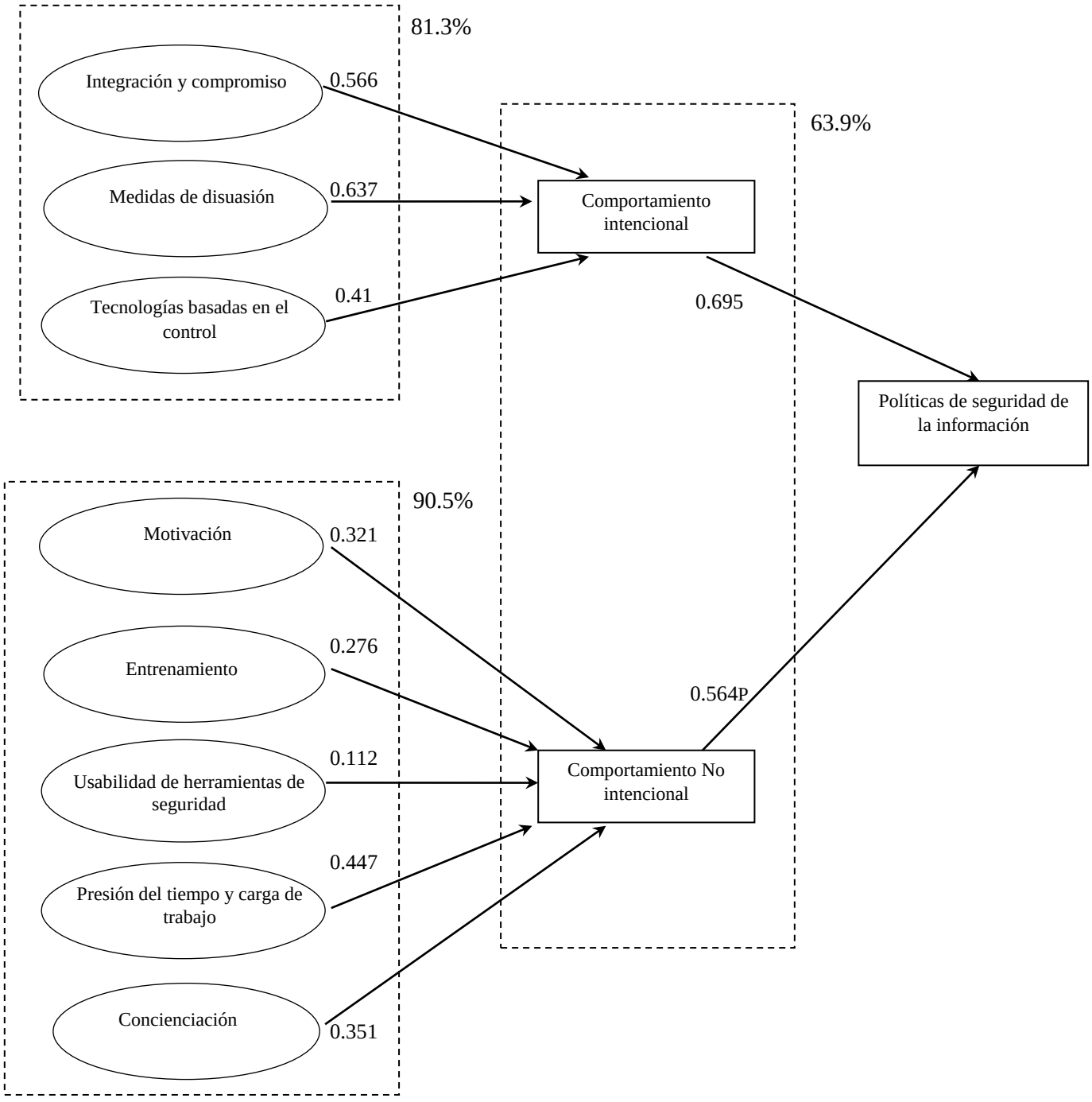


Gráfico N° 55. Modelo conceptual de la investigación
Fuente: Elaboración propia elaborado con software XLSTAT.

El modelo permite predecir el grado de relación entre las variables "comportamiento de los usuarios de tecnologías de información" y el "cumplimiento de las políticas de seguridad de la información" en entidades del sector microfinanciero. Esto se logra a través del Coeficiente de Determinación, que es el cuadrado del coeficiente de correlación de Pearson, y el modelo nos arroja la proporción de variación de la variable "cumplimiento de las políticas de seguridad de la información" que es explicada por la variable "comportamiento de los usuarios de tecnologías de información" (variable predictora o explicativa), que en este caso logró un porcentaje alto de 63.9%.

Tabla N° 39. Evaluación de la correlación de las variables independiente con la variable dependiente

Variables	Coeficiente de Correlación	Coeficiente de Determinación por dimensión	Interpretación	Coeficiente de determinación del modelo
Comportamiento Intencional	0.695	0.483	Alta	63.9%
Comportamiento No Intencional	0.564	0.318	Moderada	

Fuente: Elaboración propia

El modelo explica que en una institución microfinanciera los resultados del cumplimiento de las políticas de seguridad de información se debe en 63.9% al comportamiento de los usuarios de tecnología de información compuesta por comportamiento intencional y comportamiento no intencional. La institución debe considerar que la correlación Alta del comportamiento intencional implica un mayor énfasis en al análisis, pero recomendamos no descartar al comportamiento no intencional por su correlación moderada.

Además, el modelo predice que la fuerza de correlación que existe entre los factores que consideramos agrupados bajo la dimensión "amenazas intencionales" alcanza un 81.3% de explicación del cumplimiento de las políticas de seguridad en las empresas microfinancieras, y un 90.5% con los factores que consideramos agrupados como "amenazas no intencionales".

Tabla N° 40. Evaluación de la correlación de las dimensiones de la variable independiente Comportamiento intencional

Dimensiones de la variable Comportamiento Intencional	Coeficiente de Correlación	Coeficiente de Determinación por dimensión	Interpretación	Coeficiente de determinación del modelo
Integración y compromiso	0.556	0.309	Moderada	81.3%
Medidas de disuasión	0.637	0.405	Alta	
Tecnologías basadas en el control	0.41	0.168	Moderada	

Fuente: Elaboración propia

Los coeficientes de correlación indican que las dimensiones Integración y Compromiso, y Tecnologías basadas en el control tienen una correlación Moderada, y la dimensión Medidas de disuasión una correlación Alta. Considerar a las tres dimensiones en la evaluación del Comportamiento Intencional para el cumplimiento de las Políticas de Seguridad de Información implica un explicación del 81.3% de los posibles resultados, considerándose un alto coeficiente de determinación.

Tabla N° 41. Evaluación de la correlación de las dimensiones de la variable independiente Comportamiento No Intencional

Dimensiones de la variable Comportamiento No Intencional	Coeficiente de Correlación	Coeficiente de Determinación por dimensión	Interpretación	Coeficiente de determinación del modelo
Motivación	0.567	0.321	Moderado	90.5%
Entrenamiento	0.525	0.276	Moderado	
Usabilidad de herramientas de seguridad	0.335	0.112	Baja	
Presión del tiempo y carga de trabajo	0.669	0.447	Alta	
Concienciación	0.593	0.351	Moderado	

Fuente: Elaboración propia

Los coeficientes de correlación indican que las dimensiones Motivación, Entrenamiento y Concienciación tienen una correlación Moderada, la dimensión Presión del tiempo y carga del trabajo una correlación Alta, sin embargo la Usabilidad de herramientas de seguridad tienen una correlación Baja. Considerar a las cinco dimensiones en la evaluación del Comportamiento No Intencional para el cumplimiento de las Políticas de Seguridad de Información implica un explicación del 90.5% de los posibles resultados, considerándose un alto coeficiente de determinación. Sin embargo, no se descarta la posibilidad de omitir a la dimensión Usabilidad de herramientas de seguridad por tener un coeficiente bajo.

Con estos resultados, podemos confirmar que en este modelo, las dos variables de la investigación covarían fuertemente, y se pueden hacer realizar predicciones válidas. Sin embargo, consideramos que independientemente hay algunos factores que hemos considerado en el modelo que no aportan mucho a la explicación de la variable dependiente, por lo que hay que disponer de alguna medida de la capacidad de la ecuación de regresión para obtener mejores predicciones (en el sentido de que sean lo menos erróneas posible).

CONCLUSIONES

En relación a los fundamentos teóricos aplicados

1. Esta investigación ha propuesto un nuevo enfoque para la predicción y detección de ataques internos. La premisa básica subyacente a este marco es que, a diferencia de la detección de ataques iniciados externamente, ninguna pista es suficiente para predecir y detectar ataques internos. Por ello, es que consideramos que el primer paso para enfrentar las amenazas internas es identificar y evaluar, de manera contextualizada, los factores que pueden influir en las intenciones de comportamiento de los "atacantes", antes de enfrentar en sí al ataque iniciado o por iniciarse.

2. Las intenciones de comportamiento están en función de los factores que influyen en ellos; y éstos a su vez, dependen del contexto en el cual se pueden tangibilizar. El contexto interno y externo en el cual se desarrollan las organizaciones hacen que los factores que influyen en los comportamientos sean distintos. En la gestión de los recursos humanos, las etapas de selección y contratación, formación de los empleados y el de finalización o cambio de puesto de trabajo, tienen diferentes formas de gestionarse y valorarse de acuerdo al tipo de organización, su forma de administración, su rubro o giro de negocio, etc. En base a ello, los factores que se han identificado y evaluado para determinar las intenciones de comportamiento en relación al cumplimiento de las políticas de seguridad, ha sido el producto de contextualizar a las empresas del sector microfinanciero de la ciudad de Lambayeque – Perú, razón por el cual, se han evaluado los 8 factores siguientes: Integración y compromiso, Medidas de disuasión, Tecnología orientadas al control, Motivación, Entrenamiento, Usabilidad de Herramientas de Seguridad, Presión del tiempo y carga de trabajo y Concienciación.

3. La necesidad de una mejor predicción y detección de ataques internos es grande dada la magnitud de la amenaza interna en las empresas del sector financiero. El modelo presentado en esta investigación es prometedor en el sentido de que sintetiza los factores que influyen en el comportamiento de los usuarios de TI de las empresas microfinancieras y que han sido identificadosen base a la aplicación deteorías de la predicción del comportamiento, como son: la

Teoría del comportamiento planeado y la Teoría general de la disuasión. Ambas teorías han resultado muy útiles para poder identificar los 8 factores de comportamiento evaluados. Las teorías aplicadas, nos ha permitido comprender que las intenciones de comportamiento están influenciadas por factores de tres tipos: los que provienen de la conducta individual, los que resultan de la influencia del entorno y los que se originan de la percepción que tienen los usuarios de TI de los mecanismos de control y disuasión que las organizaciones donde se desarrolló este estudio, han implementado.

En relación a los resultados obtenidos

4. Se realizó la investigación en un escenario donde se tuvo escasa o nulo control sobre las variables, sin posibilidad de manipularla, replica baja o nula pero que permitió la selección de grupo más real. Este escenario no fue impedimento, aunque si difícil de administrar, para desarrollar la investigación caracterizándola como básica, teórica empírica, explicativa y cuantitativa, evidenciándose en los cuestionarios respondidos con éxito; 110 de 365 distribuidos.

5. El diseño de un instrumento fundamentado en los marcos teóricos fue aceptable con un indicador Alfa de Cronbach de 78.4% permitiendo una propuesta de medición para el modelo conceptual; consideramos esta propuesta de instrumento como un aporte importante para las investigaciones relacionadas con el comportamiento en el sector financiero.

6. El comportamiento no normal de los ítems del instrumento, dimensiones y de las variables permitió seleccionar test no paramétricos para someter a pruebas estadísticas que permitieron determinar que las variables género tipo de trabajo no influyen en las relaciones entre las dimensiones y entre las variables, es decir, no existe diferencia en el comportamiento entre hombre y mujeres; y entre los trabajadores de créditos, plataforma, operaciones, riesgos y funcionario.

7. Las dimensiones integración y compromiso, medidas de disuasión y tecnologías basadas en el control tienen influencia sobre el comportamiento intencional que conjunto explican en un 81.3% este comportamiento. Las dimensiones motivación, entrenamiento, usabilidad de herramientas de seguridad, presión del tiempo y carga del trabajo, y concienciación tienen influencia sobre el comportamiento no intencional que en conjunto explican en un 90.5% este comportamiento.

   El comportamiento no intencional y el comportamiento intencional tienen influencia sobre las políticas de seguridad que en conjunto explican en un 63.9% este cumplimiento.

RECOMENDACIONES

1. Identificar indicadores de comportamiento puede ser difícil, especialmente si no ocurren durante un largo período de tiempo y por lo tanto no establecen un patrón. Desafortunadamente, el modelo propuesto no está probado empíricamente. Un siguiente paso lógico es realizar pruebas de validación del modelo recopilando un gran número de estudios de casos y analizando cada uno de ellos para determinar la presencia y la cantidad de cada uno de los indicadores o factores (y posiblemente otros también) discutidos en esta investigación.

2. Los 8 factores de comportamiento evaluados son fáciles de monitorear y registrar regularmente. Prevemos que estos factores sean registrados por los responsables de la gestión de la seguridad o de RRHH, ya que los comportamientos se observan a lo largo plazo.Los factores de comportamiento propuestos tienen su propio peso predictivo diferencial y las combinaciones de éstos no aumentan automáticamente el riesgo. Así, consideramos que para mejorar el modelo se necesita pesar cada indicador por separado y combinar inteligentemente los indicadores

3. Creemos que si el modelo desarrollado se incorpora en las empresas microfinancieras para monitorear a los usuarios de TI con un registro adecuado de los factores de comportamiento, y combinado con la detección y clasificación de los datos del uso de computadoras y las redes de por parte de los empleados, facilitará la detección y prevención de delitos informáticos.

En relación a los resultados obtenidos

4. Los escenarios de desarrollo de investigación son muy variados, aunque en forma preliminar el investigador tipifica las características de la investigación en el devenir del desarrollo estas pueden precisadas con mayor certeza. El investigador deberá observar la dinámica del escenario y reaccionar con prontitud para no perder la dirección de la investigación.

5. Un modelo conceptual nuevo propuesto a partir de otras investigaciones, como el que proponemos, debe ser factible de poder desarrollar instrumentos de medición pertinente al modelo, y que pueda se adaptable a otros escenario similares.

6. Los comportamientos no siempre seguirán una distribución normal y en esos escenarios deberán realizarse los estudios sobre comportamiento expandiendo las investigaciones con otras variables intervinientes o moderadora.

7. El resultado obtenido de la explicación del comportamiento intencional y del comportamiento no intencional en base a sus respectivas dimensiones, y del cumplimiento de las políticas de seguridad en base a los comportamiento intencional y no intencional permiten establecer un nuevo marco conceptual que puede ser utilizado para posteriores investigaciones.

REFERENCIAS DE CONSULTA

1. KPMG Asesores S. Civil de R.L. (2012). *Informe del fraude en el Perú 2012.* Lima, Perú.
2. Ley No 26702. (1996). *Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia*. Perú.
3. Ley N° 30096. (2013). *Ley de delitos informáticos*.
4. Ahmad, A., Maynard, S., & Park, S. (2011). Information Security Strategies. Towards an Organizational Multi-Strategy Perspective. pp. 11-34.
5. Ahmad, A., Maynard, S., & Park, S. (2014). Information security strategies: Towards an organizational multi-strategy perspective. *Journal of Intelligent Manufacturing, 25*(2), 257-370.
6. Ajzen, I. (1991). Teoría del Comportamiento Planificado. *Comportamiento Organización y Procesos Decisión Humana*, 179-211.
7. Ajzen, I. (s.f.). Constructing a Theory of Planned Behavior Questionnaire. *TPB Questionnaire Construction*.
8. Avalos Ruiz, C. (2012). *Análisis, diseño e implementación del sistema de riesgo operacional para entidades financieras - SIRO.* PUCP. Lima: PUCP Ed.
9. Azaola Calderón, L. (2010). *Delitos informáticos y Derecho penal.* México D.F.. México: Ubijus Editorial.
10. Bethune, L., & McCarthy, R. (2013). Evaluation of Ethical Issues in the Knowledge Age: An Exploratory Study. *Issues in Information Systems, 14*(1), pp.106-112.
11. Burgos S., J., & Campos, P. (2014). Modelo para seguridad de la información en TIC. *2do Encuentro Informática y Gestión*, (págs. 234 - 253 pp). Temuco, Chile.
12. Camacho Losa, L. (2007). *Delito informático.* Madrid: Gráficas Condor.
13. CERT. (2013). Combating the Insider Threat. *National Cibersecurity and Communications Integration Center*.
14. Chen, H., & Li, W. (2014). Understanding organization employee`s information security omission behavior an integrated model of social norm and deterrence.
15. Cruz M., A., & Alarcón A., A. (2015). El capital económico por riesgo operacional: un oportuno acercamiento teórico para el sistema bancario cubano. *EKOTEMAS - Revista cubana de ciencias económicas, 1*(2), 1 - 11 pp.
16. Dang-Pham, D., Pittayachawan, S., & Bruno, V. (2014). Towards a complete understanding of information security misbehaviours: a proposal for future research with social network approach. *25th Australasian Conference on Information Systems*, pp. 1-10.
17. Dang-Pham, D., Pittayachawan, S., & Bruno, V. (Diciembre de 2014). Towards a complete understanding of information security misbehaviours: a proposal for future research with social network approach. *25th Australasian Conference on Information Systems*, pp. 1-10.
18. D'Arcy, J., & Hovav, A. (2004). El rol de las características individuales en a efectividad de contramedidas de seguridad de SI. *Décima Conferencia de América en Sistema de Información.* New York.

19. Digiware SA. (2016). *Estrategia prevención de ataques*. Recuperado el Diciembre del 2016, de Digiware, su aliado en seguridad de la información: http://www.digiware.net/?q=node/54

20. Digman, J. (1996). Personality structure_Emergence of de Five - Factor Model. *Annual Reviews Psychol*, 417 - 440 pp.

21. Dolan, S., Valle Cabrera, R., & Jackson, S. (2003). *La gestión de los recursos humanos* (2ª ed. ed.). Madrid: McGraw Hill.

22. Fernández Losa, N. (2007). Integración laboral - estrategias organizacionales y enfoque de contenidos. 1 - 7 pp.

23. Fernández, C., & Piattini, M. (2012). *Modelo para el gobierno de las TIC basado en las normas ISO.* (A. e. normalización, Ed.) Madrid: AENOR Ediciones.

24. Fishbein, M., & Ajzen, I. (1980). Teoría de la Acción Razonada. *Revista de psicologíaexperimental y social*, 453-474.

25. Furnham, A., Richards, S., & Paulhus, D. (2013). The Dark Triad of Personality- A 10 Year Review. *Social and Personality Psychology Compass*, 199 - 216 pp.

26. George, D., & Mallery, P. (2003). *SPSS/PC+step by step: a simple guide and reference.* California - USA: Wadsworth Publishing Co. Belmont.

27. Gobierno de España. (2016). *Portal Administración Electrónica - MAGERIT*. Recuperado el 2 de 2016 de Noviembre, de https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.WBjW8y3hB6o

28. Greitzer et. al., F. L. (2010). *Identifying at-Risk Employees: A Behavioral Model for Predicting Potential Insider Threats.* Pacific Northwest National Laboratory.

29. Gutierrez F., M. (1994). Notas sobre la delincuencia informática: atentados contra la 'información' como valor económico de empresa. (E. U.-L. Mancha, Ed.) *Estudios de Derecho Penal Económico*.

30. Haeussinger, F. J., & Kranz, J. J. (2013). Information security awareness: its antecedents and mediating effects on security compliant behavior. *International Conference on Information Systems*, 1-16.

31. Haeussinger, F., & Kranz, J. (2013). Information Security Awareness: Its Antecedents and Mediating Effects on Security Compliant Behavior. *International Conference on Information Systems*, pp. 1-16.

32. Herath, T., & Rao, H. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, pp. 154-165.

33. Humaidi, N., & Balakrishnan, V. (2013). Exploratory Factor Analysis of User's Compliance Behaviour towards Health Information System's Security. *Health & Medical Informatic*, pp. 1-8.

34. ISO/IEC. (2005). *27001:2005.* Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI).

35. ISO/IEC. (2008). *27005:2008.* Tecnología de la información. Técnicas de seguridad. Gestión de riesgos de Seguridad de la información.

36. ISO/IEC 2011. (2011). ISO/IEC 25010:2011. *Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — System and software quality models*.

37. Johnston, A., & Warkentin, M. (September de 2010). Fear appeals and information security behaviors: an empirical study. *Vol. 34*(N°. 10), pp. 549-566.

38. Jones, A., & Ashenden, D. (2005). *Risk management for computer security* (1st Edition ed.). Butterworth-Heinemann.

39. Kim, S., Yang, K., & Park, S. (2014). An Integrative Behavioral Model of Information Security Policy Compliance. *The Scientific World Journal*, 12 p.

40. Kont, M., Pihelgas, M., Wojtkowiak, J., Trinberg, L., & Osula, A.-M. (2014). Insider Threat Detection Study. (N. C. Excellence, Ed.) Tallinn, Estonia.

41. Liginlal, D., Sim, I., & Khansa, L. (2009). How significant is human error as a cause of privacy breaches? An empirical study and a framework for error management. *Computers & Security*, 215–228 pp.

42. Martínez S., C. (24 de Agosto de 2009). *Microfinanzas en el Perú*. Obtenido de http://www.gestiopolis.com/microfinanzas-en-el-peru/

43. Martinko, M., Gundlach, M., & Douglas, S. (2002). Toward an integrative theory of counterproductive workplace behavior: A causal reasoning perspective. *International Journal of Selection and Assessment*, 36–50 pp.

44. Mason, R., & Dupuis, M. (2014). Cultural Values, Information Sources, and Perceptions of Security. *iConference 2014 Proceedings*, pp. 778–783.

45. Mazuelos C. (s/a). Modelos de imputación en el derecho penal informático.

46. Mazuelos Coello, J. (2001). *Delitos informativos: una aproximación a la regulación del código penal peruano.* Lima.

47. Medina, E. D. (14 de Julio de 2004). *Herramientas tecnológicas en los servicios financieros*. Obtenido de http://www.gestiopolis.com/herramientas-tecnologicas-servicios-financieros/

48. Miller, R. (2013). *El costado cambiante de los ataques ciberneticos.* Informe sobre protección contra amenaZas internas y ataques externos, CA Technologies (NASDAQ: CA).

49. Miller, R., & Maxim, M. (2013). *Tengo que confiar en alguién, ¿cierto?. Cómo tratar las amenazas internas a la ciberseguridad.* CA Technologies (NASDAQ: CA).

50. Miró Llinares, F. (2013). *El cibercrimen - Fenomenología y criminología de la delincuencia en el ciberespacio* (Primera ed.). (S. Marcial Pons Ediciones Jurídicas y Sociales, Ed.)

51. Moore, A., Cappelli, D., & Trzeciak, R. (2008). *The "Big Picture" of Insider IT Sabotage Across U.S. Critical Infrastructures.* Technical Report, CMU-CERT.

52. Moreno M., A. (15 de Octubre de 2015). Seguridad Bancaria bajo el enfoque de riesgos. *XXX Congreso Latinoamericano de Seguridad Bancaria - CELAES 2015.* Panamá.

53. Naciones Unidas. (2010). *Informe del 12º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal.* Salvador.

54. National Cybersecurity and Communications Integration Center. (2014). Combating the Insider Threat.

55. Noreña, A., Alcaraz-Moreno, N., Rojas, J., & Rebolledo-Malpica, D. (2012). Aplicabilidad de los criterios de rigor y éticos en la investigación cualitativa. *Aquichan*, 263-274 pp.

56. Nurse, J., Buckley, O., Legg, P., Goldsmith, M., Creese, S., Wright, G., y otros. (2014). Understanding Insider Threat - A Framework for Characterising Attacks. (I. C. Society, Ed.) *2014 IEEE Security and Privacy Workshops*, 214 - 228 pp.

57. Pacheco, F. (2012). *ISO 2700.es*. Recuperado el Consultado en setiembre del 2016, de El portal de ISO 27001 en español: http://www.iso27000.es/sgsi.html

58. Paramio, L. (enero-abri de 2005). Teorías de la decisión racional y de la acción colectiva. *Sociológica, vol. 20*(núm. 57), pp. 13-34.

59. Parodi, C. (22 de Marzo de 2013). *Gestión*. Obtenido de http://blogs.gestion.pe/economiaparatodos/2013/03/que-es-un-sistema-financiero.html

60. Richardson, R. (2009). *2008 CSI Computer Crime & Security* . Computer Security Institute.

61. Román R., K. (Octubre de 2012). Sistema financiero peruano. *Actualidad Empresarial*. Lima, Perú.

62. Rudolph, K., Warshawsky, G., & Numkin, L. (2001). Security Awareness. En S. Bosworth, *Computer Security Handbook* (4th Edition ed.).

63. Sang Hoon, K., Kyung Hoon, Y., & Sunyong, P. (2014). An Integrative Behavioral Model of Information Security Policy Compliance. *Hindawi*, 1-12.

64. SBS. (2008). Resolución SBS N° 37-2008. *Reglamento de la gestión integral de riesgos*. Lima, Perú.

65. SBS. (2009). Resolución S.B.S.N° 2116 -2009. *Reglamento para la Gestión del Riesgo Operacional*. Lima, Perú.

66. Silowash, G., Cappelli, D., Moore, A., Trzeciak, R., Shimeall, T., & Flynn, L. (2012). *Common Sense Guide to Mitigating Insider Threats.* Informe técnico, Carnegie Mellon University.

67. Siponen, M. T. (2001). Five Dimensions of Information Security Awareness. *Computers and Society*, pp. 24-29.

68. Spurling, P. (1995). Promoting security awareness and commitment. *Information Management and Computer Security*, pp. 20-26.

69. Straub, D., & Welke, R. (1998). Coping with Systems Risk: Security Planning Models for Management Decision Making. *MIS Quarterly*, pp. 441-469.

70. Su, W.-J. (2013). How Did Ethical Evaluation Work As a Mediator between Moral Intensity and Decision Making? *International Journal of Business, Humanities and Technology, 3*(1), pp. 58-68.

71. Susanto, H., & Almunawar, M. (2012). Information Security Awareness: A Marketing Tools for Corporate's Business Processes.

72. Vance, A. (2010). Why do employees violate is security policies?. Insights from multiple theoretical perspectives. *Facu* (pág. 162). lty of Science, Department of Information Processing Science, University of Oulu, Finland.

73. Vidal de la Rosa, G. (2008). La Teoría de la Elección Racional en las ciencias sociales. *Sociología, 23*(67), pp. 221-236.

74. Villavicencio T., F. (2014). Delitos informáticos. *IUS ET Veritas*(24), 284 - 304 pp.

75. Welch, S., & Comer, J. (1988). *Quantitative Methods for Public Administration: Techniques And Applications.* USA: Books/Cole Publishing Co. ISBN.

76. Yayla, A. A. (2012). Controlling insider threats with information security policies.

77. Zambrano, F. (15 de Septiembre de 2015). *El Comercio.* Obtenido de http://elcomercio.pe/tecnologia/actualidad/hackeos-se-incrementaron-19-sector-financiero-2015-noticia-1841075

ANEXOS

ANEXO 01ENCUESTA APLICADA

CARTA DE PRESENTACIÓN

Chiclayo, 2016

Estimado Sr. (a) (ita):

Le presentamos nuestro saludo y a la vez solicitarle su apoyo respondiendo la presente encuesta que permitirá realizar el trabajo de campo de nuestra investigación doctoral relacionada con el sector financiero.

Le indicamos que es un cuestionario diseñado estrictamente con los parámetros de investigación, por lo tanto, respetando los principios de la investigación científica los datos consignados en cada encuesta son de absoluta reserva.

Las interrogantes han sido diseñadas para que usted marque con una "X" el nivel de intensidad según considere por interrogante, aquí presentamos un ejemplo:

PREGUNTA	NIVEL DE INTESIDAD
1. Usted considera que la capacitación es muy importante.	

Poca 1	2	3	4	5	Mucha 6
				X	

MUY IMPORTANTE *es que todas las preguntas deben ser respondidas, caso contrario invalidaría la encuesta.*

Agradecidos por la atención nos despedimos de usted.

Atentamente;

Msc. Ing. Ernesto K. Celi Arévalo

Ma. Ing. Regis J. A. Díaz Plaza

Universidad Nacional Pedro Ruiz Gallo
ESCUELA DE POSTGRADO
DOCTORADO DE ADMINISTRACION

IMPORTANTE: CONTESTAR TODAS LAS PREGUNTAS, DEJAR UNA DE ELLAS SIN CONTESTAR INVALIDA LA ENCUESTA

CARGO / NIVEL : _____

GÉNERO : M___ / F____

PREGUNTA	NIVEL DE INTESIDAD
1. Usted considera que las políticas de seguridad de la información de su empresa se cumplen o serán cumplidas.	Nunca 1 | 2 | 3 | 4 | 5 | Siempre 6
2. El propósito o finalidad de las políticas de seguridad de información está muy relacionada con las características de su personalidad	Nada 1 | 2 | 3 | 4 | 5 | Mucho 6
3. Si usted identifica una situación en la cual debe realizarse una mejora en las políticas de seguridad de información. ¿Qué tan importante es para usted comunicar que debe realizarse dicha mejora?	Nada 1 | 2 | 3 | 4 | 5 | Mucho 6
4. Siente que está (o estará de acuerdo) a cumplir al cien por ciento con las políticas de seguridad de información de su empresa.	Poco 1 | 2 | 3 | 4 | 5 | Mucho 6
5. Respecto a la siguiente afirmación: "el respeto a la institucionalidad es muy	

importante en el logro de sus objetivos", de acuerdo a su experiencia usted se identifica	Poco 1 | 2 | 3 | 4 | 5 | Mucho 6
6. Usted cumple con las políticas de seguridad de información porque conoce las medidas disciplinarias	Nada 1 | 2 | 3 | 4 | 5 | Mucho 6
7. Tiene temor a un mal manejo de la información por las sanciones impuestas.	Nada 1 | 2 | 3 | 4 | 5 | Mucho 6
8. El conocimiento de las acciones disciplinarias, le han permitido tener cuidado con el manejo de la información.	Nada 1 | 2 | 3 | 4 | 5 | Mucho 6
9. Ha tenido incidentes de seguridad de la información (robo de información, accedieron a su equipo o sistema sin su permiso, virus, etc.) pero fueron detectados rápidamente.	Nunca 1 | 2 | 3 | 4 | 5 | Siempre 6
10. Para verificar que su equipo y sistemas son confiables, alguna vez ha puesto en prueba los controles de seguridad (ingreso con clave errónea, mal ingreso de datos, etc.).	Nunca 1 | 2 | 3 | 4 | 5 | Siempre 6
11. Sobre los controles instalados en su equipo y sistemas, ¿considera usted que le han ayudado a no cometer errores de ingreso	Nada 1 | 2 | 3 | 4 | 5 | Mucho

de información?	1 2 3 4 5 6
12. Usted conoce que el ingreso de toda la información desde su equipo es registrado y monitoreado en un proceso de evaluación y auditoría, con respecto a esto, ¿qué nivel de confianza le asigna al equipo (computadora, impresora, etc.) y sistemas informáticos que tiene acceso?	Poco 1 2 3 4 5 Mucho 6
13. Por el buen desempeño de sus labores en relación al cumplimiento de las políticas de seguridad, ¿están claramente establecidos los reconocimientos en la empresa?	Nada 1 2 3 4 5 Mucho 6
14. Considerando a su empresa ¿Tiene usted la voluntad de hacer el mayor esfuerzo, más allá de lo normalmente esperado, para cumplir y usar adecuadamente las políticas de seguridad de la información?	Poca 1 2 3 4 5 Mucha 6
15. En caso que ocurra alguna incidencia, ¿sabe cómo actuar según las políticas de seguridad de la información de la institución donde labora?	Nunca 1 2 3 4 5 Siempre 6
16. ¿Siente que la capacitación o entrenamiento que ha recibido en relación a las políticas de seguridad de la información le ha ayudado para resolver cualquier problema o incidente que se ha presentado?	Nunca 1 2 3 4 5 Siempre 6
17. Considera usted que los sistemas son de difícil acceso.	Nunca 1 2 3 4 5 Siempre

	6
18. Se dice que en su trabajo “se trabaja bajo objetivos y presión”. ¿Considera usted que puede lograrse un trabajo sin errores bajo estas condiciones?	Nunca se logra 1 | 2 | 3 | 4 | 5 | Siempre se logra 6
19. En su trabajo, ¿con qué frecuencia a cometido errores de seguridad de información (registro de datos, errores de cálculo, etc.) debido a la presión y carga de trabajo?	Poca 1 | 2 | 3 | 4 | 5 | Mucha 6
20. Considera que la empresa ha implementado políticas para el manejo del tiempo y carga de trabajo han logrado su objetivo	Poco 1 | 2 | 3 | 4 | 5 | Mucho 6
21. Cuántos errores relacionados con sistemas de información usted ha cometido por falta de conocimiento de las políticas de seguridad de la información.	Pocos 1 | 2 | 3 | 4 | 5 | Muchos 6