FACULTAD DE INGENIERÍA
DEPARTAMENTO DE INDUSTRIA Y NEGOCIOS

INFLUENCIA DE LAS CREENCIAS EN CIBERSEGURIDAD EN EL COMPORTAMIENTO DE LOS TRABAJADORES DE PUNTA DEL COBRE

Trabajo de titulación presentado en conformidad a los requisitos para obtener el título de Ingeniero Civil Industrial

Profesor guía: Carlos Galleguillos Cortés

Bárbara Letelier Díaz
Camila Juárez Ibaceta

Copiapó, Chile 2021

FACULTAD DE INGENIERÍA
DEPARTAMENTO DE INDUSTRIA Y NEGOCIOS

INFLUENCIA DE LAS CREENCIAS EN CIBERSEGURIDAD EN EL COMPORTAMIENTO DE LOS TRABAJADORES DE PUNTA DEL COBRE

Profesor guía: Carlos Galleguillos Cortés

Bárbara Letelier Díaz
Camila Juárez Ibaceta
Copiapó, Chile 2021

AGRADECIMIENTOS

En primer lugar, agradecer a mis compañeras, qué me acompañaron desde el primer año de universidad, apoyándonos siempre, confiaron en mí, y me aguantaron todo este tiempo. A mi compañera de tesis, a pesar que en un principio dudamos del tema, fuimos capaces de lograrlo y aquí estamos, dándolo todo. A mi mami, a pesar de que no me pudo ver en esta última etapa, siempre me motivó a todo lo que quise hacer y lograr hacerlo. Agradecer a mi familia y a todos los que me ayudaron en el último empujón para terminar este trabajo completo y bien hecho. Y por último lo más importante a Mí, a mi esfuerzo, a mis desvelos y a mis metas. Yo del futuro te espera una vida de buen augurio.

Camila Juárez Ibaceta.

Agradecer a mi familia por el constante apoyo, aguante y comprensión en todo mi proceso educativo, ya que sin ellos no hubiese podido lograr ni la mitad de lo que soy hoy. A mis amigos que hicieron mi tiempo dentro y fuera de la universidad más amigables. Y a mi profesor guía por su excelente disposición cuando lo requería. De todos ustedes obtuve un aprendizaje, los llevaré guardados en un rincón de mi corazón, gracias totales. Life Goes On.

Bárbara Letelier Díaz.

Índice de contenidos

Índice de Tablas

Índice de ilustraciones

Resumen

Teniendo como precedente el creciente aumento de tecnologías, el uso exponencial del internet y paralelamente los ataques cibernéticos, se realiza una investigación que busque encontrar la relación entre 4 variables que pueden influenciar el comportamiento humano frente a la seguridad digital. Utilizando la teoría extendida del comportamiento planificado (TPB), se desarrolló y probó un modelo teórico para investigar la relación entre variables como la actitud, la norma subjetiva, y el control conductual percibido, y el impacto que tienen estas en la intención. El estudio en cuestión se realiza en base a un modelo de ecuaciones estructurales siendo complementado con un análisis factorial. La muestra cuenta con 201 trabajadores que respondieron una encuesta mediante la plataforma Microsoft Forms. El estudio fue realizado en la minería PUCOBRE, ubicada en la comuna de Copiapó, Chile. Utilizando el programa Stata-14, los resultados han demostrado que la actitud y el control conductual percibido, se asocia positivamente con la intención, la norma subjetiva en cambio se mantiene neutral; y la intención se asocia positivamente con el comportamiento frente a la seguridad digital de los trabajadores.

Palabras Claves: Ciberseguridad, Comportamiento Planificado, Minería, PUCOBRE

Abstract

Taking as a precedent the growing increase of technologies, the exponential use of the Internet and parallel cyber attacks, research is conducted to find the relationship between 4 variables that can influence human behavior towards digital security. Using the extended theory of planned behavior (TPB), a theoretical model was developed and tested to investigate the relationship between variables such as attitude, subjective norm, and perceived behavioral control, and the impact they have on intention. The study in question is based on a structural equation model complemented by a factor analysis. The sample consisted of 201 workers who responded to a survey using the Microsoft Forms platform. The study was carried out in the PUCOBRE mining company, located in the commune of Copiapó, Chile. Using the Stata-14 program, the results have shown that attitude and perceived behavioral control are positively associated with the intention, the subjective norm remains neutral, and the intention is positively associated with the digital security behavior of workers.

Keywords: Ciberseguridad, Comportamiento Planificado, Minería, PUCOBRE

CAPÍTULO 1. Introducción.

Con el creciente avance del Covid-19, la gente ha presentado mayor presencia en actividades on-line. Entre las actividades en línea más populares se encuentran las compras, el uso del correo electrónico, uso de comunicación y las redes sociales. Estas actividades son atractivas para los ciberdelincuentes, haciendo propicio realizar ataques de correos electrónicos, amenazando la privacidad del individuo, y a su vez a la empresa a la cual pertenece, provocando así una inquietud de inseguridad para los usuarios en línea (Halevi et al., 2013).

1.2 Ministerio de Minería de Chile.

Dentro de las principales conclusiones de la conferencia virtual "Ciberseguridad en la minería 4.0", actividad inaugurada por el Ministro de Minería, Baldo Prokurica, se relevó que las nuevas demandas del actual marco de automatización, remotización y digitalización, propio de esta era, tiene impactos de incidencia directa, no solo en la producción, sino también en la seguridad de los trabajadores, dado a que a mayor eficiencia e integración que han traído los nuevos avances tecnológicos, existe un creciente número de riesgos inherentes a los ciberataques, los cuales pueden traducirse en peligros o daños tangibles sobre otros sectores productivos. Es por esto que se sostuvo que un eventual ciberataque puede amagar diferentes áreas de las compañías del rubro minero, lesionando su continuidad operacional, ya sea a nivel del proceso de extracción, procesamiento o refinamiento de metales; a la provisión de insumos elementales, como el agua; o a la contabilidad de las empresas. Paralelamente, estas incursiones tienen el poder de ocasionar consecuencias adversas en la salud y seguridad de los trabajadores, el medio ambiente y la propia comunidad, lo mismo que la interrupción de las faenas, con el consiguiente detrimento financiero que ello significa. A causa de estas amenazas, la autoridad estimó que es el momento de que el Estado de Chile avance de manera más rápida en el campo de la ciberseguridad de las empresas mineras, teniendo en cuenta el gran impacto del rubro en el Producto Interno Bruto (PIB) y los ingresos fiscales del país. A su vez, Soledad Bastías, directora de Ciberseguridad IT/OT, de la Corporación Nacional del Cobre (CODELCO), manifestó que no todo se remite al control tecnológico, pues tanto o más importante en este ámbito, es el factor humano y la psicología humana.

1.3 Antecedentes del problema.

El comportamiento de la seguridad individual ha sido un desafío para las organizaciones. Si bien estudios han reconocido a las personas como un elemento importante para lograr la seguridad, también se las ha descrito como el eslabón más débil, porque a menudo no cumplen con las mejores prácticas de seguridad. En consecuencia, no es sorprendente que el compromiso de seguridad individual se haya convertido en un tema de gestión clave para las entidades.

El uso de tecnologías digitales en la actualidad es cada vez más necesario para mejorar la productividad y sustentabilidad en la gran minería 4.0. Las oportunidades que estas tecnologías ofrecen a la industria ayudan en muchos ámbitos, por ejemplo, disminuir etapas de algún proceso de producción, aumentar la adaptación eficaz frente a una adversidad en la mina, mejorar la toma de decisión frente a un proyecto que se quiera realizar técnicamente más complejo, disminuir las leyes de mineral, e inclusive incluir aún más la seguridad digital de las operaciones.

A pesar de los mayores esfuerzos para mejorar la dicha seguridad, las estadísticas de la industria identifican las acciones maliciosas, negligentes o inadvertidas de las personas que son parte de la organización, como la principal causa de incidentes de seguridad (Donalds & Osei-Bryson, 2020). En el caso de Chile, la evidencia muestra que si bien el país cuenta con la tecnología y equipamiento similar que el de otras partes del mundo que aprovechan las tecnologías 4.0, hoy en día las faenas no hacen uso intensivo de ellas.

Se entiende también que este proceso de cambio, al estar sumergido en un ambiente de alta incertidumbre, es complejo de analizar, tanto desde la perspectiva cultural, como tecnológica. Es por lo anterior, que la minería está tendiendo a mejorar sus tecnologías con el paso del tiempo, para esto, se creó una hoja de ruta para potenciar la innovación tecnológica en la industria minera de Chile, en el cual participaron más de 100 representantes por parte del Consejo Minero, Fundación Chile y Corporación Alta Ley con el apoyo de Corfo y la asesoría técnica del programa Interop (Consejo Minero, Fundación Chile y Corporación Alta Ley, Corfo, 2018). Este modelo tiene como base 4 núcleos que consideran el desarrollo de una minería inteligente a través de elementos como la digitalización, la ciberseguridad, el desarrollo de capital humano, y la existencia

de una licencia social y política para innovar. Teniendo en cuenta que debido a la actual pandemia por Covid-19, el uso tecnológico ha aumentado exponencialmente y del mismo modo los ciberataques.

1.4. Definición del Problema.

Es por esto que los investigadores señalan que las soluciones tecnológicas deberían combinarse idealmente con un comportamiento de seguridad individual por parte de los trabajadores (Donalds & Osei-Bryson, 2020). En este sentido se sabe poco sobre el comportamiento de seguridad informática en trabajadores de la industria minera.

1.5. Alcance y Justificación.

Siguiendo con este razonamiento, en esta investigación se evaluará el comportamiento de los trabajadores frente a la ciberseguridad que tiene la mina Punta del Cobre. En particular, la necesidad de solucionar este problema surge debido a que los trabajadores de Punta del Cobre no manejan información sobre este tema, por lo cual son más susceptibles a posibles ataques cibernéticos tanto en sus máquinas como en la base de datos de la empresa.

Punta del Cobre al ser mediana minería está expuesta ante los posibles ciberataques, ya que recientemente a principios de este año se tomaron acciones para que sus trabajadores posean información sobre seguridad cibernética y así conocer sus comportamientos con respecto a la seguridad. Por otro lado, una parte de sus trabajadores (Supervisión, administrativos, técnicos y algunos operadores) cuentan con un correo de la empresa, donde acceden a información confidencial de la base de datos, si un cracker vulnera al menos uno de estos correos puede provocar enormes daños financieros u operativos de la empresa.

1.6. Objetivos

1.6.1. Objetivo General.

Determinar cómo las creencias de los trabajadores de la mina Punta del Cobre influyen en el comportamiento frente a la seguridad cibernética.

1.6.2. Objetivos Específicos.

- Determinar la relación entre la intención con el comportamiento de los trabajadores frente a la seguridad cibernética.

- Determinar la relación entre la intención con las actitudes de los trabajadores.

- Determinar la relación entre la intención con las normas subjetivas de los trabajadores.

- Determinar la relación entre la intención con el control de conducta percibida de los trabajadores.

CAPÍTULO 2. Marco Teórico.

2.1. Minería en Chile

La minería ha estado en la historia de Chile desde siempre y forma parte de nuestra identidad como nación. Mucho antes de que los españoles llegaran a América, los indígenas que habitaban estas tierras sacaban el mineral de cobre de la cordillera de Los Andes y lo utilizaban para fabricar herramientas y adornos. Luego, durante los primeros 200 años de la Conquista, el cobre fue una industria pequeña que se realizaba básicamente en la zona norte del país. Recién en 1820 comenzó la expansión de la producción, que abarcó desde la Región de Atacama hasta la Región del Aconcagua. Durante los siglos XIX y XX, Chile se posicionó como importante productor de cobre a nivel mundial. Adelantos como el uso de carbón mineral, la construcción de ferrocarriles y nuevas fundiciones dieron un gran impulso a la minería nacional, pero particularmente las fundiciones de cobre, han llegado a ser el sector más activo en el desarrollo de la economía nacional debido al monto de sus inversionistas y la magnitud alcanzada en la producción.

2.1.1 Historia de la ciberseguridad en la Industria Minera.

Históricamente la minería ha sido una industria que ha sido bastante conservadora al momento de adoptar nuevas tecnologías. Sin embargo, ante las nuevas exigencias ambientales y sociales que enfrenta el sector, así también como el imperativo de mejorar la productividad, la incorporación de estas tecnologías facilita el cumplimiento de la demanda social que enfrentamos hoy. Algunas estimaciones internacionales que hablan de los potenciales beneficios de implementar estas tecnologías en la industria minera entre 2016 y 2025, consideran beneficios económicos del orden de USD $189 billones en la industria minera mundial, y USD$ 130 billones en los metales (CESCO, 2020). Hay otros beneficios no económicos asociados, como la reducción de CO_2 o una mayor seguridad para los trabajadores en la operación.

La Minería Inteligente depende en primera medida de la digitalización de sus procesos, por lo que su modelo debe tener en cuenta, los profundos impactos que la tecnología disruptiva tendrá en cuanto a la toma de decisiones, el requerimiento de nuevas competencias y habilidades para la implementación de dichas aplicaciones.

2.1.2 Sociedad Punta del Cobre S.A

PUCOBRE es una empresa especializada en la explotación de yacimientos de cobre de mediana minería, y que agrega valor a los minerales obtenidos mediante su procesamiento en plantas propias. En dichas plantas se obtienen dos productos diferentes: Concentrados de cobre para las fundiciones y cátodos de cobre destinados a la exportación. La compañía desarrolla sus operaciones en la Región de Atacama y sus oficinas generales están localizadas en la ciudad de Copiapó, distante a 805 km al norte de Santiago de Chile (también cuenta con oficinas en Santiago). Las minas Punta del Cobre, Mantos de Cobre y Granate, ubicadas a 20 km de distancia de las oficinas generales, son los yacimientos que abastecen de minerales a la Planta San José de la compañía, la cual se encuentra aproximadamente a 5 km. de las minas y obtiene como producto final concentrados de cobre. La compañía también opera la Planta Biocobre, ubicada a 13 km de Copiapó por el Camino Internacional a Argentina, unidad que se abastece de minerales provenientes de la Mina Venado Sur, ubicada a 35 km. de Biocobre, por el mismo Camino Internacional. PUCOBRE actualmente desarrolla dos proyectos para la explotación de cobre, El Espino y Tovaku, ambos yacimientos de mediana minería. Están ubicados en la Región de Coquimbo y en la Región de Antofagasta, respectivamente.

2.1.3. Descripción de las principales actividades realizadas en la mina PUCOBRE

PUCOBRE se encuentra en un proceso de formación para que todos sus trabajadores conozcan conceptos asociados a ciberseguridad, para que protejan sus datos tanto en el contexto laboral como personal. Desde comienzos de este año 2021 se han realizado 4 etapas principales, donde la primera etapa consiste en la difusión inicial, esto con el motivo de que los trabajadores tengan un mínimo conocimiento acerca de que es la ciberseguridad. La segunda etapa comprende la capacitación en la plataforma de academia que la empresa entrega a disposición para sus trabajadores, en el cual estos mismos realizan un auto-aprendizaje con la ayuda de videos digitales explicativos que luego son evaluados. Posteriormente, en la tercera etapa se realizan reuniones donde se vuelve a explicar todo el contexto de ciberseguridad, las problemáticas y los pactos asociados a no seguir las políticas de ciberseguridad. Finalmente, en la cuarta etapa, el equipo de informática de PUCOBRE, realiza pruebas de prácticas con el método de phishing

(correos maliciosos), para conocer quiénes de sus trabajadores fallan en esta última prueba.

2.2. Concepto de Ciberseguridad

La ciberseguridad es la práctica de proteger sistemas, redes y programas de ataques digitales. Por lo general, estos ciberataques apuntan a acceder, modificar o destruir la información confidencial, extorsionar a los usuarios o interrumpir la continuidad del negocio. Actualmente, la implementación de medidas de seguridad digital se debe a que hay más dispositivos conectados que personas, y los atacantes son cada vez más creativos como por ejemplo utilizando la práctica del phishing.

Digitalización: La digitalización es el proceso de transformar procesos analógicos y objetos físicos en digitales. Considera cómo el escaneo de documentos de papel o el uso del almacenamiento en la nube para guardar todos tus archivos importantes eliminando la necesidad de archivadores.

Phishing: La suplantación de identidad (phishing), el cual ha ido en aumento estos últimos años (Halevi et al., 2013), es la práctica de enviar correos electrónicos fraudulentos que se asemejan a correos electrónicos de fuentes de buena reputación. El objetivo es robar datos sensibles, como números de tarjetas de crédito e información de inicio de sesión. Es el tipo más común de ciberataque. Puede protegerse mediante la educación o una solución tecnológica que filtre los correos electrónicos maliciosos.

Pharming: es una evolución del phishing y consiste en redirigir las solicitudes de un usuario a sitios web fraudulentos. Para alojarlos, los atacantes operan enormes “granjas de servidores” o server farm en inglés, de donde procede el nombre que se ha dado a esta modalidad de fraude.

Hackers: es quien usa sus conocimientos para descubrir vulnerabilidades en sistemas informáticos. Por el contrario, un cracker, es quien se dedica a vulnerar sistemas informáticos para cometer operaciones ilícitas, como publicar información confidencial o dañar una plataforma virtual.

Malware: (del inglés malicious software), también llamado badware, es cualquier programa o código malicioso, que tiene como objetivo infiltrarse o dañar una computadora o Sistema de información sin el consentimiento de su propietario. Por otro lado, el software se considera malware en función de los efectos que, pensados por el creador, provoque en un computador. Malware no es lo mismo que software defectuoso, este último contiene bugs peligrosos, pero no de forma intencionada.

Virus informático: Es un malware que tiene por objeto alterar el normal funcionamiento de la computadora, sin el permiso o el conocimiento del usuario. Los virus, habitualmente, reemplazan archivos ejecutables por otros infectados con el código de este. Los virus pueden destruir, de manera intencionada, los datos almacenados en una computadora, aunque también existen otros más inofensivos, que solo se caracterizan por ser molestos.

Firewall: Elemento de protección que sirve para filtrar paquetes (entrada o salida) de un sistema conectado a una red, que puede ser internet o una intranet. Existen firewall de software o hardware. Este filtrado se hace a través de reglas, donde es posible bloquear direcciones (URL), puertos, protocolos, entre otros.

Anti-virus: Programa capaz de detectar, controlar y eliminar virus informáticos y algunos códigos maliciosos.

Anti-spam: Programas capaz de detectar, controlar y eliminar correos spam.

Criptografía: Es el arte cifrar y descifrar información con claves secretas, donde los mensajes o archivos sólo puedan ser leídos por las personas a quienes van dirigidos, evitando la interceptación de éstos. (Kuss et al., 2013)

2.2.1. Factores determinantes en la seguridad digital

La pandemia por el coronavirus ha potenciado el trabajo en línea con el objetivo de evitar mayores contagios por contacto físico. Como consecuencia de ello, distintas empresas han implementado equipos de ciberseguridad para prevenir potenciales riesgos en el mundo digital, algunos de los factores a tener en cuenta son:

1.- En cualquier tipo de negocio los datos son objeto de protección y, por tanto, los sistemas que los albergan resultan vulnerables ante los ciberataques. La transformación

digital de las empresas implica acceder a los datos desde cualquier punto, para ser más productivos, accediendo a la información del trabajo, donde se comparte con clientes o proveedores. Este intercambio, al poder realizarse fuera de la empresa, presenta otro nivel de dificultad para la seguridad de la misma. Como, por ejemplo: robo de dispositivos, pérdida o robo de información confidencial, conexión no segura, robo de credenciales.

2.- En la transmisión de datos, desactivar la sincronización automática de las aplicaciones tiene relevancia cuando el dispositivo personal es el que hace enlace entre la información que se obtiene del trabajo y la que se transmite. En muchas de las redes inalámbricas que utilizan los trabajadores fuera del entorno empresarial, no existe protección alguna. A veces la información confidencial de la empresa puede transmitirse a través de comunicaciones inalámbricas que no están bajo control. Cuando esto ocurre, es importante que los datos que enviemos estén debidamente protegidos.

3.- El Almacenamiento, en la actualidad la información empieza a necesitar infraestructuras de almacenamiento flexibles que se adapten rápidamente a cualquier cambio en la empresa o el mercado. Hay distintos tipos de almacenamiento; local, en red, dispositivos externos y en la nube.

Las copias de seguridad son el respaldo que hará que la información que se considere importante esté a salvo, de esta forma, si cualquiera de los tipos de almacenamiento de los que disponemos se ve vulnerado ante un ataque, quedará una copia de seguridad.

4.- El factor humano, es otro punto a considerar, ya que, si bien los académicos y profesionales han reconocido a las personas como un elemento importante para lograr la seguridad, también se las ha descrito como el eslabón más débil de la cadena, porque a menudo no cumplen con las mejores prácticas de seguridad como, por ejemplo:

- Utilizar contraseñas fuertes y distintas para cada servicio, apoyándose en gestores de contraseñas que permiten generar contraseñas complicadas para establecer diferentes credenciales.

- Mantener los dispositivos actualizados ya que los desarrolladores de los sistemas operativos continuamente emiten parches de seguridad que corrigen y tapan las fugas de seguridad, pues los virus y el malware se crean todo el tiempo y atacan a equipos que todavía no han aplicado la siguiente actualización de seguridad.

- No abrir enlaces sospechosos, desconfiando de los enlaces en mensajería instantánea, correo electrónico o incluso de los que se puede hallar en las redes sociales, pues nunca se sabe cuándo un enlace puede llevar a una web fraudulenta que pretenda utilizar datos confidenciales. Lo mismo ocurre con los archivos adjuntos de e-mails que se desconoce, pues pueden tratarse de virus.

2.3 Comportamiento organizacional.

El comportamiento organizacional (conocido también con la abreviatura CO) es un campo de estudio que investiga el efecto que los individuos, grupos y organización, tienen sobre el comportamiento dentro de las empresas, con el propósito de mejorar la efectividad de las organizaciones.

El CO es una doctrina que logra reunir aportaciones, de diversas disciplinas, que tienen como base el comportamiento, como la psicología, antropología, sociología, ciencias políticas, entre otras. Dentro del estudio del CO, se consideran las siguientes variables dependientes:

Por otro lado, en el estudio de CO, también se encuentran variables independientes:

- A nivel individual: Son todos los valores, actitudes, personalidades y habilidades de la persona, que lo han acompañado desde su nacimiento, son posiblemente modificables por la empresa y que influyen en su comportamiento dentro de la misma.

- A nivel grupal: el comportamiento que tienen las personas al estar en contacto con otras, va a variar de acuerdo al obtenido de manera individual.

- A nivel organizacional: los individuos y los grupos conforman la organización, en consecuencia, los procesos de trabajo, las políticas y las prácticas que se realizan dentro de dicha organización.

- Dado a lo anterior, la organización debe buscar adaptarse a sus trabajadores, ya que el aspecto humano es factor determinante, dentro de la posibilidad de alcanzar los logros de la organización.

2.4. Teoría del comportamiento planificado.

Se puede entender que de esta investigación se quiere comprender las motivaciones de las personas y cuáles son los factores que influyen en sus decisiones frente a la ciberseguridad en la empresa PUCOBRE, basándonos en la teoría del comportamiento planificado. Esta teoría creada en 1985 por Icek Ajzen, profesor de psicología de la universidad de Massachusetts, predice y explica el comportamiento premeditado en específicos contextos. La teoría (TCP) contiene cinco variables donde se incluye la actitud, la norma subjetiva y el locus de control (posible equivalente de la auto-eficacia) el cual se refiere a las percepciones de una persona sobre la presencia o ausencia de recursos y oportunidades requeridos, lo cual lleva a la persona a una evaluación de la situación como que tan probable es que con sus recursos pueda realizar su conducta, esto además de los factores externos de los cuales el sujeto no tiene control absoluto. Dichas variables tienen una influencia en la intención de llevar a cabo una conducta, por lo que a mayor intención, mayor probabilidad de que la conducta sea realizada.

Variables: Según la teoría del comportamiento planeado, las intenciones y los comportamientos son una función de tres determinantes básicos, uno de naturaleza personal, otro que refleja la influencia social, y el último que trata con temas de control.

De acuerdo con Ajzen, hay tres tipos de creencias relacionadas con los constructos de la teoría del comportamiento planeado que son:

- Actitud: La valoración personal que hace un individuo de una conducta, si la valoración es positiva la intención es mayor. La actitud es referida como el

grado en el cual una persona tiene una evaluación o apreciación favorable o desfavorable del comportamiento en cuestión (Ajzen, 1991). Las creencias de los individuos acerca de las consecuencias de cierto comportamiento determinan la actitud con respecto a este comportamiento. Las actitudes se componen de 3 elementos principales: Cognitivo, Afectivo y Conativo. (Shiffman, Leon G; Kanuk, 2010)

- ❖ Componente Cognitivo: Está compuesto por las cogniciones del individuo. Es toda la información proveniente de distintas fuentes, estos pueden ser las creencias, experiencia propia o ajena, que maneja el individuo racional con respecto a un objetivo en concreto.

- ❖ Componente Afectivo: Es el componente que tiene relación con las emociones. Son todas aquellas percepciones guiadas por el sentimentalismo o sensaciones subjetivas que influencian la actitud de un individuo.

- ❖ Componente Conativo: Es el componente que representa la facilidad o probabilidad de asociación que percibe el individuo con respecto a lograr un objetivo o comportamiento. Está compuesto por las intenciones, disposición o tendencia hacia un objeto. Por lo tanto, es la variable observable de la actitud, esto es, el cómo actúa la persona ante el objeto. La conducta está mediatizada por la situación. Muchas veces la presión social puede impedir o facilitar la expresión conductual de la actitud.

- Norma Subjetiva: La norma subjetiva es un factor social asociado a la percepción del individuo con respecto a la presión social acerca de realizar o no un determinado comportamiento (Ajzen, 1991). También es considerada como la percepción que tienen los individuos acerca de las personas que conforman su círculo más cercano, y lo que estos piensan que haría o no el individuo con respecto a realizar cierto comportamiento.

- Control del Comportamiento Percibido (PBC): Grado de percepción acerca del comportamiento en duda, con respecto a la facilidad o dificultad para llevar a cabo el comportamiento, el cual puede ser un reflejo de las experiencias pasadas del individuo para medir los riesgos u obstáculos involucrados (Ajzen, 1991). En resumen, el PBC es descrito como la percepción que tiene el individuo acerca de la dificultad que conlleva realizar cierto tipo de acción, y de su disponibilidad de recursos para llevar a cabo la acción en específico.

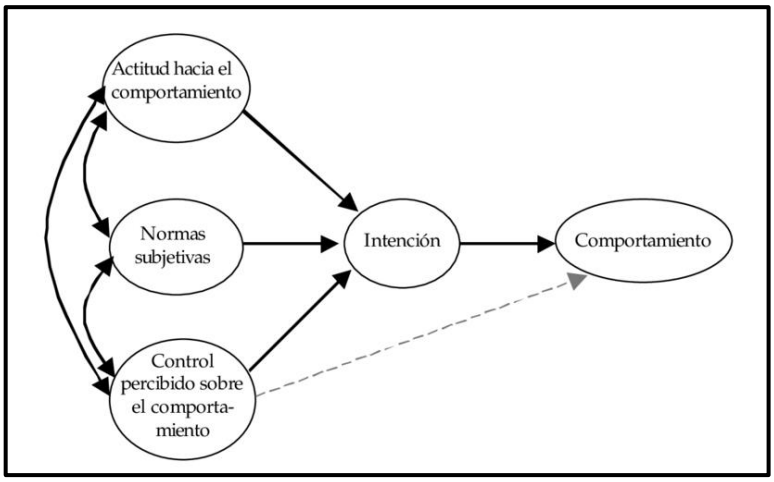


Ilustración 2.1 Teoría del Comportamiento Planificado

Fuente: Icek Ajzen, 1991

Las variables mencionadas anteriormente tienen una influencia en la intención de llevar a cabo una conducta, por lo que, a mayor intención, mayor probabilidad de que la conducta sea realizada. Las intenciones tienen una importancia capital en esta teoría, actuando como mediadora. En esos términos, el comportamiento es predicho por la intención al realizar un comportamiento que por su parte es predicho por las actitudes. La intención se considera para percibir los factores motivacionales que influyen en el comportamiento. Son indicaciones de que tanto esfuerzo están dispuesto a ejercer con el fin de realizar la conducta. Pero esta intención será productiva siempre y cuando la persona tenga un control voluntario de su comportamiento (Ajzen, 1991).

En resumen, las creencias de comportamiento producen una actitud favorable o desfavorable sobre el comportamiento, las creencias normativas resultan en la presión social percibida o la norma subjetiva. Las creencias de control dan lugar al control del comportamiento percibido. En combinación, la actitud hacia el comportamiento, la norma subjetiva y la percepción de comportamiento controlado, conducen a la formación de un comportamiento intencional. Como regla general, si la actitud y la norma subjetiva son más favorables, el control percibido será mayor, y la intención de la persona a realizar un comportamiento en particular será más fuerte. Por lo tanto, estos tres factores son los que crean la intención de acción de las personas y entregan como consecuencia el comportamiento de las personas.

CAPÍTULO 3. Metodología Aplicada

En la siguiente sección, se presenta la metodología utilizada, el tipo y diseño de investigación, la muestra estudiada y el procedimiento de ejecución de la investigación.

3.1. Etapas de la investigación

En la primera etapa de la investigación se explica la introducción al problema, se identifica su alcance, justificación y los objetivos que se quieren lograr, en la siguiente etapa se investiga la parte bibliográfica de la investigación para construir el marco teórico con el fin de poder contextualizar la investigación y así entender la teoría del comportamiento planificado y sus aspectos generales con respecto a la ciberseguridad, además de la selección del modelo a utilizar. En la tercera etapa se presenta la metodología utilizada para una posterior formulación de hipótesis, se escoge la herramienta de medición para finalmente recopilar, validar e interpretar los resultados obtenidos.

3.2. Diseño de la investigación

El diseño en esta investigación corresponde al modelo hipotético deductivo debido a que la investigación presenta una teoría de la cual se manipulan variables como las actitudes, normas subjetivas, control del comportamiento percibido e intención, las cuales están sujetas a verificación hipotética de carácter cuantitativo.

3.3. Método de recolección de datos

Luego de escoger el modelo para llevar a cabo el estudio se procedió a crear la encuesta, que medirá las distintas variables que se desean estudiar. En este caso la encuesta es obtenida del trabajo original de la Teoría del comportamiento, traducida y adaptada para ser aplicada. La encuesta es transcrita a Microsoft Forms, para luego ser difundida el 24/07/2021 en la mina PUCOBRE, lamentablemente por temas administrativos y de seguridad, la encuesta fue finalmente difundida el día 04/10/2021. Durante la primera semana se obtuvieron 100 respuestas, es decir un 50% del mínimo necesario para la investigación, luego a la semana siguiente se obtuvieron 40 respuestas más, aumentando en un total de 70% de avance del método de recolección de datos, y por último, a fines de Noviembre se obtuvo un total de 201 respuestas.

3.3.1 Diseño de encuesta

El cuestionario cuenta con un total de 31 preguntas, de las cuales 20 hacen referencia al estudio del comportamiento de los trabajadores frente a la seguridad digital, tres preguntas corresponden al ítem demográfico que mide la edad, sexo y el área al que pertenece dentro de la empresa y las 8 preguntas restantes son de interés de la empresa frente a la ciberseguridad. En las 23 preguntas correspondientes al cuestionario original se estudian 5 dimensiones: Comportamiento, Intención de Comportamiento, Actitud, Norma Subjetiva y Control Conductual Percibido. Sin contar las preguntas demográficas, las respuestas están basadas en la escala de Likert de 1-5, en cada una de las preguntas se muestra los extremos de la escala, donde 1 corresponde a totalmente en desacuerdo y 5 totalmente de acuerdo. La encuesta es distribuida de forma online por medio de Microsoft Forms, a trabajadores que pertenecen a PUCOBRE. Cabe destacar que todas las preguntas realizadas se validaron con el estudio "Development of the Cybersecurity Attitudes Scale and Modeling Cybersecurity Behavior and its Antecedents" (Howard, 2018).

A continuación, se desarrollará cada una de las preguntas de la encuesta y lo que miden (Las preguntas serán explicadas en el mismo orden de aparición de la encuesta real, en los anexos se puede observar la encuesta online).

Preguntas Demográficas de los Trabajadores en PUCOBRE:

Estas Preguntas (Tabla 3.1) se utilizan para contextualizar la muestra.

P1	Indique su edad (N°)
P2	¿Con qué género se identifica? (Hombre/Mujer)
P3	Seleccione el área a la que pertenece (Técnicos, Administrativos, Operadores, Supervisores, Otro)

Tabla 3.1 Preguntas 1 a 3, demográficas generales.

Preguntas que miden la Actitud de los Trabajadores en PUCOBRE

Según lo visto en el capítulo anterior, la actitud es aprendida, es el resultado de la experiencia directa de los individuos frente a diversas situaciones. Para este estudio en específico, basado en la Teoría del Comportamiento Planificado, la actitud del individuo hacia un comportamiento específico (seguridad digital), será la suma de las creencias y percepciones consecuentes con el desarrollo del mismo y las evaluaciones subjetivas de otras personas sobre las creencias y consecuencias. Por lo que las preguntas de esta sección (Tabla 3.2) estudian la actitud que tiene el individuo frente a la seguridad digital, buscando solo la opinión personal.

P4	Creo que es necesario utilizar contraseñas seguras para los accesos a las herramientas de trabajo
P5	Creo que es oportuno tener diferentes contraseñas en el trabajo y/o vida personal en diferentes aplicaciones
P6	Creo que es probable que participe en programas de capacitación sobre las características generales de prácticas de ciberseguridad.

Tabla 3.2 Preguntas 4 a 6 Miden la Actitud

Preguntas que miden la Norma Subjetiva de los Trabajadores en PUCOBRE

Esta variable estudia el modo o la percepción que tiene el sujeto frente a la opinión de personas o grupos que considera relevantes acerca de lo que deberían hacer respecto a la seguridad digital. El qué dirán o lo que opinan los demás es un factor que puede afectar en la toma de decisiones, por lo que estas preguntas (Tabla 3.3) medirán qué tan importantes son los agentes externos en la toma de decisiones.

P7	Las personas que me rodean (jefe directo) piensan que está bien que tenga buenas prácticas de ciberseguridad (contraseñas fuertes, cambios de contraseñas, no abrir enlaces sospechosos)
P8	Las personas que me rodean (mis compañeros de trabajo) piensan que está bien que tenga buenas prácticas de ciberseguridad (contraseñas fuertes, cambios de contraseñas, no abrir enlaces sospechosos)
P9	Las personas que me rodean (mis amigos dentro del trabajo) piensan que está bien que tenga buenas prácticas de ciberseguridad (contraseñas fuertes, cambios de contraseñas, no abrir enlaces sospechosos)
P10	Considero que la empresa utiliza un programa seguro de protección digital
P11	Creo que es importante seguir las políticas de ciberseguridad de la empresa
P12	Creo que es importante nunca violar intencionalmente las políticas de ciberseguridad en mi organización

Tabla 3.3 Preguntas 7 a 12, Miden la Norma Subjetiva.

Preguntas que miden el Control Conductual de los Trabajadores en PUCOBRE

Esto refleja la creencia de los individuos con respecto al control o capacidad sobre los factores que pudieron facilitar o impedir una determinada conducta. Este factor mide si existe autonomía o no del comportamiento, buscando saber si es que está en su control o no, la decisión de realizar un acto de seguridad digital o depende de un tercero (Tabla 3.4).

P13	Estoy seguro que los archivos adjuntos que recibo por parte de la empresa (ya sea WhatsApp o correo) son seguros para descargar

P14	Creo que es poco probable que sea víctima de un ciberataque en el trabajo
P15	Creo que no soy vulnerable al robo de información personal en un ciberataque en la empresa que pertenezco
P16	Creo tener las herramientas adecuadas para evitar un ciberataque

Tabla 3.4 Preguntas 13 a 16, Miden el Control Conductual Percibido

Preguntas que miden la Intención del Comportamiento de los Trabajadores en PUCOBRE

La intención se considera para percibir los factores motivacionales que influyen en el comportamiento. La teoría sostiene que la conducta humana es voluntaria y está determinada por la intención conductual, la cual a su vez se construye a partir de tres procesos principales o constructos: Actitud, Norma Subjetiva y Control Conductual Percibido (Ajzen, 1991). Si bien la Intención se crea a partir de otras variables, con estas preguntas (Tabla 3.5) se buscará explícitamente si es que existe una intención de realizar un acto de seguridad digital.

P17	Tengo la intención de realizar capacitaciones sobre ciberseguridad como fuente de seguridad para la empresa
P18	Tengo la intención de no ingresar a enlaces sospechosos.
P19	Tengo la intención a menudo, de realizar copias de seguridad de datos importantes para la empresa.
P20	Tengo la intención de cambiar mis contraseñas con responsabilidad.

Tabla 3.5 Preguntas 17 a 20, Miden la Intención del comportamiento

Preguntas que miden el Comportamiento de los Trabajadores en PUCOBRE

El comportamiento es el conjunto de respuestas motoras frente a estímulos tanto internos como externos. Este lo consideramos como el más importante para nuestra investigación, ya que es el resultado de todas las influencias de las variables estudiadas. Con estas preguntas (Tabla 3.6) se estudiará el comportamiento concreto de los individuos al realizar un acto de seguridad digital.

P21	He sido capaz de cambiar mis contraseñas con responsabilidad en los últimos tres meses.
P22	He sido capaz de no ingresar a enlaces sospechosos en los últimos tres meses.
P23	He sido capaz de realizar copias de seguridad de la información que considero importante de la empresa en los últimos tres meses.

Tabla 3.6 Preguntas 21 a 23, Miden el Comportamiento

3.4. Muestra

Este es uno de los puntos donde hay menor consenso, (Kline, 2016) propone que haya entre 10 a 20 participantes por parámetro estimado (MacCallum et al., 1996), que depende del poder estadístico buscado y según la complejidad del modelo, por lo que a mayor complejidad mayor será la muestra. (Campo-Arias & Oviedo, 2008) proponen un mínimo de 100 mientras que (Jackson, 2003) postula que el tamaño mínimo recomendable es de 200 sujetos para cualquier SEM.

3.5. Diseño de Muestra

En primera instancia se decide la población objetivo de este estudio, la que corresponde a personas trabajadoras de la mina Punta del Cobre residentes de la comuna de Copiapó, Región Atacama. Se escogió esta muestra debido a los intereses u objetivos personales de los investigadores, dado que el estudio puede ser aplicado a cualquier tipo de muestra de personas naturales, siempre y cuando la muestra resultante sea representativa del lugar. Además, otra razón de utilizar esta población, es que

continuamente existe una preocupación por el creciente avance tecnológico y ataques cibernéticos.

3.5.1 Tamaño de Muestra

Para el cálculo de la muestra se utilizó la siguiente fórmula:

$$n = \frac{N * Z^2 * p * (1 - p)}{(N - 1) * e^2 + Z^2 * p * (1 - p)}$$

Donde:

n = Tamaño de la muestra (número de encuestas).

N = Tamaño de la población.

Z = Valor Z que obtenido mediante un alfa de confianza determinada (suele ser 95%).

p = Proporción de individuos que poseen en la población la característica de estudio. Es un número entre 0 y 1. Se suele utilizar 0.5.

e = Límite aceptable de error muestral.

3.6. Formulación de hipótesis

• H1: La actitud está relacionada positivamente con la intención de los trabajadores.

• H2: Las normas subjetivas están relacionadas positivamente con la intención de los trabajadores

• H3: El control conductual percibido está relacionada positivamente con la intención de los trabajadores.

• H4: La intención está relacionada positivamente con el comportamiento de los trabajadores frente a la seguridad cibernética.

3.7 Herramientas Matemáticas

3.7.1 Modelo de Ecuaciones Estructurales

Existe una gran variedad de técnicas multivariadas que permiten el estudio de fenómenos psicológicos, entre las más usadas están: la regresión múltiple, el análisis factorial, el análisis multivariante de la varianza y el análisis discriminante. Todas estas tienen en común la limitación de poder examinar sólo una relación al mismo tiempo, ya sea de dependientes, independientes o entre ellas (Hair et al., 1999)

Una versión más completa y formal son los modelos de ecuaciones estructurales que establecen la relación de dependencia entre las variables. La técnica de SEM se considera una extensión de varias técnicas multivariantes de regresión múltiple, el análisis factorial principalmente y el análisis de senderos abarcando varios modelos conocidos como el análisis de la variable latente y el análisis de la estructura de covarianza. Es el grado en que las variables se pueden medir. Trata de integrar una serie de ecuaciones lineales y establecer cuáles de ellas son dependientes o independientes de otras, ya que dentro del mismo modelo las variables que pueden ser independientes en una relación pueden ser dependientes en otras, por lo que se vuelve una herramienta útil (Escobedo Portillo et al., 2016).

Combina y confronta el conocimiento a priori e hipótesis con datos empíricos, por lo que los modelos de ecuaciones estructurales son más confirmatorios que exploratorios. Los modelos de ecuaciones estructurales se caracterizan por dos elementos principales:

- Evaluar relaciones múltiples y de dependencia cruzada.
- La medida en que los conceptos no observados están representados en estas relaciones y el error de medición se tiene que tener en cuenta en el proceso de estimación.

El sistema de ecuaciones estructurales tiene una ventaja sobre otros sistemas y técnicas multivariables en el análisis de las relaciones de cada subconjunto de variables, y al mismo

tiempo permite crear correlaciones entre variables pertenecientes a diferentes grupos, dependiendo del propósito del estudio.

El modelo SEM general puede descomponerse en dos submodelos:

El modelo de medida, representa la relación entre variables observadas (Experimental o Índice) y no observadas (Latentes o Constructivas). En otras palabras, el modelo de medición es el modelo CFA que se describe más adelante. El objetivo de este modelo es validar la idoneidad de los índices seleccionados en la medición de las estructuras de interés, ayuda a evaluar la correlación de las variables observadas (Cupani, 2012). Si los indicadores propuestos están débilmente correlacionados entre sí, esto puede implicar que el modelo está mal definido o que existen errores en la hipótesis sobre la relación entre las variables (Weston & Gore, 2006). Finalmente, debemos considerar que los mejores indicadores serían la escala con alto índice de confiabilidad ($\alpha \geq 0{,}80$) (Cupani, 2012). En la Figura 2 se muestra un ejemplo de un modelo de medición, que consta de tres variables latentes y nueve indicadores.

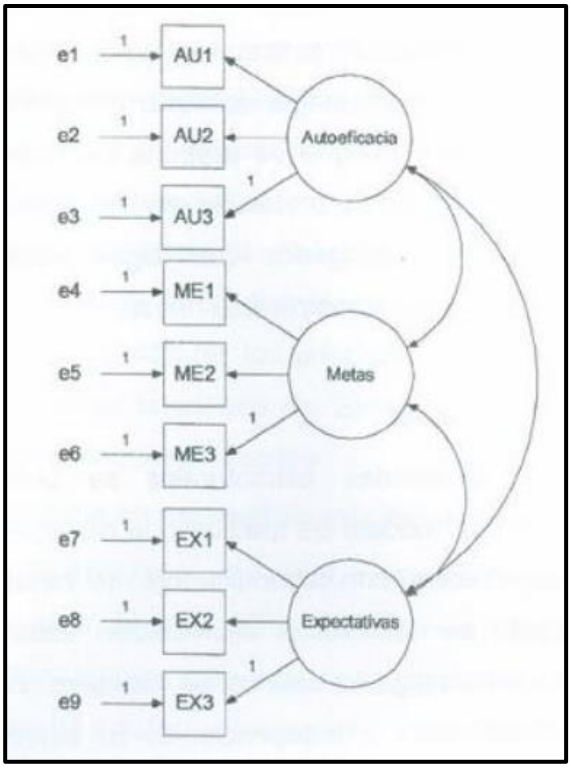


Ilustración 3.1 Ejemplo Análisis Factorial Confirmatorio de Tres Mediciones

Fuente: Cupani, 2012

Los modelos estructurales definen relaciones entre variables no observadas (latentes o constructos), especificando la forma en que una variable latente directa o indirectamente ("causa un cambio") afecta los valores de las otras variables latentes del modelo, es decir, le ayuda a distinguir qué variable independiente predice cada variable dependiente (Cupani, 2012).

3.7.1.1 Simbología del Diagrama

Los modelos de ecuaciones estructurales se representan esquemáticamente utilizando configuraciones particulares de cuatro símbolos geométricos:

- Círculo o elipse (O): Representan factores latentes no observados.
- Cuadrado o rectángulo (☐): Representan variables observadas.
- Flechas de un sentido (→): Representan el impacto de una variable en otra.
- Flechas de doble sentido (↔): Representan covarianzas o correlaciones entre pares de variables.

Al construir un modelo, se utilizan estos símbolos con cuatro configuraciones básicas, cada una de las cuales representa un componente importante en el proceso analítico:

- Coeficiente de trayectoria para la regresión de una variable observada sobre una variable (o factor) latente no observada. (O→☐)
- Coeficiente de trayectoria para la regresión de un factor a otro factor. (O→O)
- Error de medición asociado a una variable observada. (→ ☐)
- Error residual en la predicción de un factor no observado. (→O)

3.7.1.2 Etapas del modelo SEM

Los principales especialistas en el SEM consideran 6 pasos a seguir para aplicar esta técnica, estos son:

1) Especificación del modelo: En esta fase el investigador aplica sus conocimientos teóricos del fenómeno estudiado al planteamiento de las ecuaciones matemáticas relativas a los efectos causales de las variables latentes y a las expresiones que las relacionan con los indicadores o variables observables. Esta distinción es importante porque cualquier relación entre variables, sin especificar por el investigador, se asume que es igual a cero. Además, en esta etapa, se formulan enunciados sobre el conjunto de parámetros, decidiendo entre los que serán libres para ser estimados o fijos, a los que se les asignará un valor dado, normalmente cero. Asimismo, se especifican los supuestos estadísticos sobre las fuentes de variación y en concreto sobre la forma de distribución conjunta, que en la mayoría de las técnicas empleadas se considera normalidad multivariante. La claridad del modelo viene determinada por el grado de conocimiento teórico que posea el investigador sobre el tema de estudio. En efecto, si la información es poco exhaustiva o detallada, la asignación de los parámetros será confusa a priori, por lo que el investigador deberá realizar luego diversas modificaciones, contemplando principalmente los aspectos teóricos.

2) Identificación del Modelo: A continuación, se procede asegurando que todos los parámetros del modelo pueden ser estimados. El modelo estará identificado si todos los parámetros lo están. Este paso debe realizarse antes de la recolección de datos. Una forma de saber si está identificado o no el modelo, es mediante la regla de los grados de libertad (gl), que se calcula de la siguiente forma:

$$gl = \frac{(n^{\circ}\ variables\ observadas \bullet [n^{\circ}\ variables\ + 1])}{2} - (Parmetros\ a\ estimar)$$

Se pueden obtener tres posibles resultados a esta regla:

- Modelo Identificado es cuando gl = 0, siendo que esto corresponde a ser un ajuste perfecto, este no tiene interés alguno ya que este modelo no podrá ser generalizado.

- Modelo Sobreidentificado estos son los modelos que se espera obtener al trabajar con SEM, ya que se busca que el modelo sea tan generalizable como sea posible, para esto es necesario que gl > 0.

- Modelo Infraidentificado es cuando gl < 0, lo que significa que se está intentando estimar más parámetros de los que permite la información disponible.

En conclusión, a mayor cantidad de gl, el modelo será más parsimonioso, es decir, que el modelo se ajusta bien a los datos, por lo que se puede demostrar que las asociaciones entre variables latentes y observadas son más importantes.

3) Evaluación de resultados: La interpretación de datos ayuda a establecer el modelo correcto y a aceptar o rechazar las hipótesis, concluyendo la investigación. Previo al análisis, es recomendable examinar todas las variables con la finalidad de evaluar la calidad de la base de datos.

- El primer tema a tratar es el tamaño de la muestra, ya qué es uno de los aspectos donde menos consenso hay entre los especialistas.

- Otro aspecto a tener en cuenta es la multicolinealidad entre las variables, donde variables altamente correlacionadas son consideradas redundantes. Una pauta para verificar si existe multicolineidad entre las variables es mediante una correlación y bivariada, donde valores superiores a r = 0,85 pueden señalar potenciales problemas, por otro lado, las variables altamente correlacionadas ($\rho > 0, 85$) son consideradas redundantes (Kline, 2016). Cuando se observa que dos variables

están altamente correlacionadas, la solución más práctica es retirar una de ellas del modelo.

- Datos Atípicos o Outliers: es cuando existen datos extremos de un sujeto, si es en solo una variable se denomina casos atípicos univariados, mientras que, si se presentan puntajes extremos en más de una variable, se denominan casos atípicos multivariados.

- Distribución Normal Multivariada: Los estadísticos utilizados en SEM, asumen que la distribución multivariada es normal, violar esta suposición es problemático y afecta la precisión de las pruebas estadísticas. Sin embargo, evaluar la distribución normal multivariada generalmente es poco práctico, ya que esto implica el examen de un número infinito de combinaciones lineales. Una solución a este problema es examinar la distribución de cada variable observada.

  Para determinar si existe normalidad univariada, se debe examinar la asimetría y curstosis de cada variable observada, donde valores entre +1.00 y -1.00 se considerarán excelentes, mientras que valores inferiores a 1.60, adecuados (George & Mallery, 2003). Sin embargo, un método que incrementa la distribución de la normalidad es la transformación de los datos. Los métodos más comunes de transformación son la raíz cuadrada, el logaritmo, y el inverso. Eliminar o transformar los casos atípicos univariados o multivariados aumenta la distribución normal de los datos.

4) Estimación de parámetros: Se determinan los valores de los parámetros desconocidos, los investigadores utilizan programas especiales para el SEM, existen software altamente reconocidos y en uso actualmente como, por ejemplo:

- LISREL (Linear Estructural Relations): Permite establecer y analizar estructuras de covarianza.

- EQS (Structural Equation Modeling Software): Desarrollado por (Bentler, 2006) este presenta planteamientos y símbolos para comprender el modelo más fácilmente.

- AMOS (Analysis of Moment Structures): Logra que el usuario pueda especificar, ver y modificar el modelo estructural gráficamente por medio del uso de herramientas gráficas sencillas.

Una de las técnicas ampliamente empleada en la mayoría de los programas informáticos para la estimación de modelos estructurales, es el de máxima verosimilitud (MV), que es eficiente y no sesgada cuando se cumplen los supuestos de normalidad multivariada. La sensibilidad de este método de estimación a la no normalidad, genera la necesidad de técnicas de estimación alternativas, como el método mínimos cuadrados ponderados (WLS), mínimos cuadrados generalizados (GLS) y asintóticamente libre de distribución (AGL).

El principal impulsor del uso de estos modelos y las técnicas multivariadas, fueron en el desarrollo del área de la computación, ya que al crear software logran que el análisis sea cada vez más poderoso y sofisticado.

5) Evaluación de ajuste e interpretación: la relevancia o ajuste se refiere a la precisión de los datos del modelo para determinar si son correctos, y si sirve como aproximación al fenómeno real, precisando así su poder de predicción. Las medidas de bondad de ajuste pueden ser de tres tipos: (1) medidas de ajuste absoluto para evaluar el ajuste general del modelo, (2) medidas de aptitud incrementales para comparar el modelo propuesto con otros modelos especificados por el investigador, o (3) medidas del ajuste de parsimonia, que ajustan las medidas de ajuste para brindar comparaciones entre modelos con una gran cantidad de coeficientes estimados que varían, su propósito es determinar la cantidad de ajuste obtenido para cada coeficiente estimado. La literatura recomienda emplear múltiples indicadores para evaluar el ajuste del modelo (Bentler, 2006).

Existe una gran variedad de indicadores del ajuste por lo que se mencionan los más utilizados:

- Chi-Cuadrado (CMIN = $\chi 2$): Este debe ser no significativo, para que el modelo presente un buen ajuste. Esto es así porque un valor significativo de $\chi 2$ implica que la estructura del modelo teórico propuesto es significativamente diferente de la indicada por la matriz de covarianza de los datos. No obstante, este último estadístico es sensible al tamaño muestral y debe interpretarse con precaución.

- Razón de Chi-cuadrado Sobre los Grados de Libertad (CMIN/DF): En este caso se considera un buen ajuste para valores inferiores a 2.

$$\frac{\chi^2}{gl} < 2 \qquad (Buen\ Ajuste)$$

- Cambio en Chi-cuadrado Entre Modelos Alternativo ($\Delta\chi 2$): Se comparan diferentes modelos teóricos, si existe una reducción significativa del estadístico de un modelo respecto a otro, se entiende que tienen un ajuste más adecuado a los datos (Tabachnick & Fidell, 2020). ($\downarrow\chi 2$)

- Error Cuadrático Medio de Aproximación (RMSEA): Se considerará óptimo el ajuste si es que RMSEA < 0, 06 (Bentler, 2006).

- PCLOSE, denominada también por LISREL como P-Value for Test of Close Fit, prueba la hipótesis nula de que RMSEA no es mayor a 0.05. Si PCLOSE es menor a 0.05, se rechaza la hipótesis nula y concluye que RMSEA es mayor a 0.05, indicando un bajo ajuste.

- Índice de Ajuste Comparativo (CIF): Los valores que puede tomar este índice varían generalmente entre 0 y 1, siendo 1 el ajuste perfecto. Entonces se considera

un ajuste satisfactorio entre el modelo teórico y los datos de la muestra, para valores superiores a 0,9 y se considera óptimo para valores igual o superior a 0,95.

- *Índice de Tucker-Lewis (TLI):* compara el ajuste por grados de libertad del modelo propuesto y nulo (modelo de ausencia de relación entre las variables). Este índice tiende a 1 para modelos con muy buen ajuste, considerándose aceptables valores superiores a 0.90, aunque lo ideal sería valores mayores a 0.95.

- Índice de Bondad de Ajuste (GFI): Este se mide de igual manera que el anterior, GFI > 0, 95 ajuste óptimo.

Por último, es necesario que se evalúe la significancia de los parámetros estimados, que se realiza de forma análoga a los coeficientes de regresión Al igual que en el análisis de regresión, un modelo que se ajusta bien a los datos, pero que posee pocos coeficientes significativos, no tendría mucho sentido.

6) Re-especificación del modelo: La re-especificación ayuda a conocer si el primer modelo obtenido es el mejor, para lo que es necesario buscar métodos para mejorar el ajuste de este añadiendo o eliminando los parámetros estimados del modelo original, con sus justificaciones correspondientes. Para realizar una reespecificación se deben examinar los índices de modificación.

- El valor del índice de modificación corresponde aproximadamente a la reducción en el chi-cuadrado que se produciría si el coeficiente fuera estimado, un valor de 3,84 o superior sugiere que se obtiene una reducción estadísticamente significativa en el chi-cuadrado cuando se estima el coeficiente (Hair et al., 1999).

- La matriz residual de la matriz de las predicciones de la covarianza y correlación, donde los valores residuales mayores que 2,58 se consideran estadísticamente

significativos a nivel de 0,05, estos residuos significativos indican un error de predicción sustancial para un par de indicadores.

3.7.1.2 Análisis Factorial

El análisis factorial se utiliza para reducir y resumir los datos que se analizan eliminando factores dependientes o independientes de los datos. Para obtener la información necesaria, es necesario calcular un conjunto de dimensiones latentes llamadas factores con estas relaciones explicadas. Por tanto, el análisis factorial utiliza una técnica de reducción de datos mediante la cual se pueden probar las hipótesis planteadas.

Para realizar el análisis factorial se deben seguir una serie de pasos como explica Malhotra, en los que primero se debe construir la fórmula del problema para el análisis matricial de correlaciones. Se debe determinar el número de factores luego rotarlos y extraerlos para interpretar. El análisis factorial puede ser de dos tipos:

- Análisis factorial exploratorio (AFE): Este permite la creación de construcciones de modelos hipotéticos y teóricos que pueden compararse empíricamente sin especificaciones previas del modelo o sin considerar tanto el número de factores como las relaciones entre ellos. La técnica utilizada por el análisis factorial exploratorio incluye la extracción de factores con ciertos criterios estadísticos obteniendo la estructura factorial más simple para una interpretación más sencilla y significativa (Escobedo Portillo et al., 2016).

- Análisis Factorial Confirmatorio (CFA): El CFA permite corregir o corroborar. si es necesario, las deficiencias del AFE resultando en un mayor contraste de las hipótesis especificadas; asimismo analiza la matriz de covarianzas en lugar de la matriz de correlaciones, que establece si los índices son equivalentes. AFC está representado por un diagrama de ruta de acuerdo con sus especificaciones específicas. Los rectángulos representan elementos y las elipses representan

elementos comunes. Las flechas unidireccionales entre factores e ítems comunes representan la saturación y las flechas bidireccionales indican correlaciones entre factores comunes o únicos (Escobedo Portillo et al., 2016). El análisis factorial confirmatorio (CFA) se utiliza apropiadamente cuando el investigador tiene algún conocimiento de la estructura de la variable latente subyacente (Zhang, Hong, 1999). Basándose en el conocimiento de la teoría, de la investigación empírica, o de ambos. Postula relaciones a priori entre las medidas observadas y los factores subyacentes y luego prueba esta estructura hipotética estadísticamente.

En resumen, el modelo analítico de factores (EFA o CFA) se centra únicamente en cómo y en qué medida, las variables observadas están vinculadas a sus factores latentes subyacentes. Aunque las relaciones entre variables latentes son de interés, no se considera ninguna estructura de regresión entre ellas en el modelo analítico factorial. Debido a que el modelo CFA se centra únicamente en el vínculo entre factores y sus variables medidas, dentro del marco de SEM, representa lo que se ha denominado un modelo de medición.

3.7.2 Regresión Lineal

De un modo general se dice que existe regresión de los valores de una variable con respecto a los de la otra cuando hay alguna línea, denominada línea de regresión, que se ajusta más o menos claramente a los valores observados. La regresión se usa para la identificación de relaciones potencialmente causales o bien, cuando no existen dudas sobre su relación causal, para predecir una variable a partir de la otra (Dagnino S., 2014). La regresión lineal nos permite predecir el comportamiento de una variable (dependiente o predicha) a partir de otra (independiente o predictora). La ecuación requerida para calcular dicha regresión es la siguiente:

$$\gamma = \alpha \pm \beta x + \varepsilon i$$

Donde:

γ = Variable dependiente.

α = Intersección o constante.

β = Coeficiente angular de la regresión.

x = Variable independiente.

εi = Error.

3.7.3 Coeficiente de Pearson.

El coeficiente de correlación de Pearson es una prueba que mide la relación estadística entre dos variables continuas. Si la asociación entre los elementos no es lineal, entonces el coeficiente no se encuentra representado adecuadamente.

El coeficiente de correlación puede tomar un rango de valores de +1 a -1. Un valor de 0 indica que no hay asociación entre las dos variables. Un valor mayor que 0 indica una asociación positiva. Es decir, a medida que aumenta el valor de una variable, también lo hace el valor de la otra. Un valor menor que 0 indica una asociación negativa; es decir, a medida que aumenta el valor de una variable, el valor de la otra disminuye.
Para llevar a cabo la correlación de Pearson es necesario cumplir lo siguiente:

- La escala de medida debe ser una escala de intervalo o relación.
- Las variables deben estar distribuida de forma aproximada.
- La asociación debe ser lineal.
- No debe haber valores atípicos en los datos.

Para el cálculo de correlación de Pearson se utiliza la siguiente fórmula:

$$r_{xy} = \frac{\sum z_x z_y}{N}$$

Donde:

x = variable número uno

y = variable número dos

zx = desviación estándar de la variable uno

zy = desviación estándar de la variable dos

N = número de datos

3.7.4 Coeficiente de Determinación

El coeficiente de determinación es la proporción de la varianza total de la variable explicada por la regresión. Este coeficiente, también llamado R cuadrado, refleja la bondad del ajuste de un modelo a la variable que pretender explicar. Los valores del coeficiente de determinación oscilan entre 0 y 1. Cuanto más cerca de 1 se sitúe su valor, mayor será el ajuste del modelo a la variable que estamos intentando explicar. De forma inversa, cuanto más cerca de cero, menos ajustado estará el modelo y, por tanto, menos fiable será.

El cálculo del coeficiente de correlación se calcula como:

$$R^2 = \frac{Sumas\ de\ cuadrados\ Regresión}{Suma\ de\ cuadrados\ total} = \frac{SCR_{eg}}{SCT}$$

Ó

$$= 1 - \frac{Sumas\ de\ cuadrados\ Residual}{Suma\ de\ cuadrados\ total} = 1 - \frac{SCR}{SCT}$$

3.7.5 Tratamiento de encuestas

3.7.5.1 Alfa de Cronbach (CA)

Este coeficiente se forma como la media de las correlaciones entre las variables que forman parte de la escala y se puede calcular de dos formas: a partir de la varianza (alfa de Cronbach) o de la correlación de los ítems (alfa de Cronbach estandarizado).

La fiabilidad es un tema constante en todos los instrumentos de medición. Su estudio intenta establecer la precisión con la que se mide cualquier instrumento de medida en general y tests en particular. Cuanto más confiable sea un test, más precisa será la medición y, por lo tanto, menor será el error de medición.

El Alfa de Cronbach es un método para calcular los coeficientes de fiabilidad, determinando la fiabilidad como consistencia interna. Se llama así porque analiza hasta qué punto las mediciones parciales obtenidas con diferentes ítems son "consistentes" entre sí y, por lo tanto, representan el posible universo de elementos medibles. La ratio aceptable para el alfa de Cronbach debe ser 0.7 o mayor.

3.7.6 Escala de Likert.

La escala Likert es una herramienta de medición o recopilación de datos cuantitativos que se utiliza en la investigación. Es una especie de escala aditiva correspondiente a la medida ordinal; Consiste en una serie de ítems o enunciados según los cuales se solicita previamente la respuesta del sujeto. El estímulo (ítem o juicio) que se le presenta al sujeto representa la característica que el investigador desea medir, y se requieren respuestas según el grado de acuerdo o desacuerdo que tenga el sujeto con la frase particular. Hay cinco opciones de respuesta más utilizadas, donde a cada categoría se le asigna un valor numérico que llevará al sujeto a una puntuación total producto de las puntuaciones de todos los ítems. Esta puntuación final indica la posición del sujeto en la escala.

Las actitudes son lo que principalmente se pueden medir con una escala tipo Likert (Maldonado Luna, 2012). Los pasos que se requieren seguir en la elaboración de una escala Likert son los siguientes:

- Conocer la actitud o variable a medir.
- Elaborar ítems relacionados con la actitud o variable que se quiere medir.
- Administrar la escala a una muestra de sujetos que van a actuar como jueces.
- Asignar los puntajes a los ítems según su posición positiva o negativa.
- Asignar los puntajes totales a los sujetos de acuerdo con el tipo de respuesta en cada ítem.
- Efectuar el análisis de ítems (validación y confiabilidad).
- Construir con base en los ítems seleccionados la escala final.
- Aplicar la escala final a la población en la cual se validó el instrumento.

3.7.7 Composite Reliability (CR)

El uso de medidas tradicionales de confiabilidad interna como el α de Cronbach ha sido criticado en el contexto de que los modelos de variables latentes tienden a sobreestimar o subestimar la confiabilidad de la escala. Para proporcionar una evaluación más rigurosa de la confiabilidad interna, se puede utilizar la confiabilidad compuesta (CR) de las características de medición de la escala (Hyland et al., 2013). La fiabilidad compuesta se calcula de acuerdo con la siguiente fórmula:

$$pc = \frac{(\sum_{i=1}^{m} \lambda i)^2}{(\sum_{i=1}^{m} \lambda i)^2 + (\sum_{i=1}^{m} (\theta i))}$$

Donde:

pc =es la confiabilidad de la escala.

λi =carga factorial estandarizada

θi = varianza del error estandarizado

m= Número de factores.

Una ratio aceptable para el CR es de 0.6 o mayor.

3.7.8 Average Variance Extracted (AVE).

La varianza media extraída (AVE) se usa comúnmente para evaluar la validez discriminante con base en la siguiente 'regla empírica': la raíz cuadrada positiva del AVE para cada variable latente debe ser mayor que la alta correlación con cualquier otra variable latente (David Alarcón & José A. Sanchez, 2015). Se calcula utilizando la siguiente fórmula:

$$AVE\varepsilon_j = \frac{\sum_{k=1}^{k_j} \lambda_{jk}^2}{\left(\sum_{k=1}^{k_j} \lambda_{jk}^2\right) + \theta_{jk}}$$

Donde:

j = Número de variable

λi = carga factorial estandarizada

θi = varianza del error estandarizado

k = Número de factores.

Una ratio aceptable para AVE es de 0.5 o mayor.

CAPÍTULO 4. Resultados

4.1. Recopilación de Información

La muestra total corresponde a 201 encuestados, del total de estas todas son respuestas válidas. Como se dijo anteriormente la encuesta fue llevada a cabo por medio de los formularios de Microsoft, y fue distribuida mediante el departamento de informática de la empresa hasta poder cumplir con el mínimo de individuos necesarios para realizar el estudio. Del total de respuestas el 16.92 % fueron mujeres y 83.08 % hombres como se entrega en la tabla que se visualizará más adelante. Respecto al rango etario corresponden a personas entre los 23 años y 65 años. A continuación, se puede encontrar el resumen de la estadística descriptiva de la muestra:

¿Con qué género se identifica?	Freq.	Percent	Cum.
Hombre	167	83.08	83.08
Mujer	34	16.92	100.00
Total	201	100.00	

Tabla 4.1 Cantidad de Trabajadores por Género

Fuente: Elaboración Propia

Seleccione el área al que pertenece	Freq.	Percent	Cum.
Administrativos	18	8.96	8.96
Ejecutivo	8	3.98	12.94
Operadores	42	20.90	33.83
Supervisión	109	54.23	88.06
TAO	1	0.50	88.56
Técnicos	23	11.44	100.00
Total	201	100.00	

Tabla 4.2 Cantidad por Área de Trabajadores en Punta del Cobre

La siguiente tabla nos muestra especificación de la tabla 4.3, en este caso, la cantidad de personas (hombres y mujeres) que participaron del estudio segmentado por área de trabajo en la mina Punta del Cobre:

Seleccione el área al que pertenece	¿Con qué género se identifica? Hombre	Mujer	Total
Administrativos	10	8	18
Ejecutivo	6	2	8
Operadores	39	3	42
Supervisión	90	19	109
TAO	0	1	1
Técnicos	22	1	23
Total	167	34	201

Tabla 4.3 Cantidad de Personal, Área de Trabajo v/s Género

Fuente: Elaboración Propia.

Como se explicó en la teoría, la carga factorial indica cuan pesada es la variable en términos de aporte al modelo, siendo una ratio aceptable de 0.7 o mayor. Los resultados para las preguntas se encuentran en la siguiente tabla:

Pregunta	*Media*	*Des. Estándar*	*Mín.*	*Máx.*	*Carga Factorial*	*Cronbach's Alpha*
P4	4,631	0,873	1	5	0,5609	
P5	4,223	1,142	1	5	0,6035	0.6853
P6	4,398	0,938	1	5	0,5673	
P7	4,472	0,985	1	5	0,7704	
P8	4,383	0,963	1	5	0,8036	0.9285
P9	4,378	0,952	1	5	0,7501	
P13	4,194	0,962	1	5	0,3746	
P14	3,597	1,140	1	5	0,2793	0.7036
P15	3,552	1,156	1	5	0,2892	
P16	3,840	1,046	1	5	0,4806	
P17	4,144	1,050	1	5	0,5925	
P18	4,716	0,802	1	5	0,6463	0.7258
P19	3,691	1,316	1	5	0,5485	
P20	4,383	1,094	1	5	0,6928	
P21	4,253	1,183	1	5	0,4796	
P22	4,467	0,948	1	5	0,4749	0.6203
P23	3,577	1,405	1	5	0,5375	

Tabla 4.4 Resumen de Resultados de Preguntas Realizadas

4.2 Interpretación de Datos

Al igual que se obtuvieron resultados de la carga de cada pregunta, cabe destacar que en los resultados entregados por el Alfa de Cronbach rondan el valor aceptable según la teoría de 0.7, esto es, que la fiabilidad de las preguntas se considera buenas para el modelo.

	OIM Coef.	Std. Err.	z	P>|z|	[95% Conf.	Interval]
Structural						
INT <-						
A	.2229014	.0882515	2.53	0.012	.0499316	.3958712
NS	.1811415	.0607371	2.98	0.003	.062099	.300184
PBC	.2559607	.0996035	2.57	0.010	.0607414	.45118
COMP <-						
INT	1.608509	.2579708	6.24	0.000	1.102895	2.114122

Tabla 4.5 Ecuaciones estructurales sin correlaciones entre variables.

Los resultados mostrados en el recuadro marcado con rojo, nos indican que en primera instancia las ecuaciones estructurales están bien hechas, ya que todos los valores resultaron menores a 0.05, al igual que el ajuste de la variable de la intención respecto al comportamiento que nos entrega un ajuste perfecto. Sin embargo, si nos dirigimos al análisis del modelo en general, obtenemos los siguientes números:

Fit statistic	Value	Description
Likelihood ratio		
chi2_ms(115)	495.049	model vs. saturated
p > chi2	0.000	
chi2_bs(136)	1754.233	baseline vs. saturated
p > chi2	0.000	
Population error		
RMSEA	0.128	Root mean squared error of approximation
90% CI, lower bound	0.117	
upper bound	0.140	
pclose	0.000	Probability RMSEA <= 0.05
Information criteria		
AIC	8840.004	Akaike's information criterion
BIC	9021.685	Bayesian information criterion
Baseline comparison		
CFI	0.765	Comparative fit index
TLI	0.722	Tucker-Lewis index
Size of residuals		
SRMR	0.178	Standardized root mean squared residual
CD	0.998	Coefficient of determination

Tabla 4.6 Ajuste estadístico del modelo sin correlaciones entre variables.

Algunos Índices a considerar de los resultados entregados:

- TLI = 0.722 < 0,95 → El ajuste es deficiente.
- RMSEA = 0.128 > 0.06 → El ajuste no se considera como óptimo, ya que existe un ajuste lejano a los datos de la realidad.
- PClOSE = 0.000 < 0.05 → Se rechaza la hipótesis nula y concluye que RMSEA es mayor a 0.05, indicando un bajo ajuste.
- CFI = 0.75 < 0.95 → No se considera un modelo óptimo.
- SRMR (residuo cuadrático medio de la raíz estandarizada) 0.178 ≈ 17.8% > 0.05 → No se cumpla el modelo.

Debido a que el índice SRMR es el único que considera la distribución multinormal de los datos, se analiza con mayor profundidad. Dicho lo anterior, el modelo tiene un buen ajuste global a los datos, dado que, el acercamiento de errores es de un 82.2%, considerado para ciencias sociales como una probabilidad baja de ajuste, ya que debiese resultar por lo menos en un 95%, por tanto, lo que se busca es poder disminuir el valor de SRMR. Para ello, si regresamos a la teoría, Azjen indica que dentro de las variables independientes se

producen problemas de correlación, para esto, una forma de mejorar el modelo, es utilizar el análisis factorial o establecer correlaciones en el modelo de las variables mismas mencionadas anteriormente. Por lo tanto, se procedió a la re-especificación del modelo.

Las correlaciones ajustadas fueron las siguientes:

1. Actitud → Norma Subjetiva
2. Norma Subjetiva → PBC
3. Actitud → PBC

Una vez hecha las correlaciones obtenemos una nueva tabla del ajuste estadístico y una tabla del modelo de ecuaciones estructurales respectivamente.

Fit statistic	Value	Description
Likelihood ratio		
chi2_ms(112)	370.802	model vs. saturated
p > chi2	0.000	
chi2_bs(136)	1754.233	baseline vs. saturated
p > chi2	0.000	
Population error		
RMSEA	0.107	Root mean squared error of approximation
90% CI, lower bound	0.095	
upper bound	0.119	
pclose	0.000	Probability RMSEA <= 0.05
Information criteria		
AIC	8721.757	Akaike's information criterion
BIC	8913.348	Bayesian information criterion
Baseline comparison		
CFI	0.840	Comparative fit index
TLI	0.806	Tucker-Lewis index
Size of residuals		
SRMR	0.085	Standardized root mean squared residual
CD	0.993	Coefficient of determination

Tabla 4.7 Ajuste estadístico del modelo con correlaciones entre variables

Como se puede observar en la tabla 4.7, el valor del residuo cuadrático medio de la raíz estandarizada (SRMR) disminuyó considerablemente con respecto al modelo sin correlaciones, de 0.178 → 0.085, esto quiere decir que la probabilidad de que ocurra el modelo aumentó, sin embargo, para efecto de ciencia según investigadores sigue siendo un modelo no óptimo.

Con respecto a las nuevas ecuaciones estructurales tenemos:

	OIM Coef.	Std. Err.	z	P>|z|	[95% Conf.	Interval]
Structural						
INT <-						
A	.3473759	.1686924	2.06	0.039	.0167448	.6780069
NS	.0652047	.0967415	0.67	0.500	-.1244051	.2548146
PBC	.2403582	.0970253	2.48	0.013	.0501921	.4305243
COMP <-						
INT	1.595575	.2550019	6.26	0.000	1.095781	2.09537

Tabla 4.8 Ecuaciones estructurales del modelo con correlaciones

Al visualizar la tabla anterior, se visualiza que, en la variable nombrada como norma subjetiva, el "P > |z|" nos entrega un valor de 0.500 > 0.05, lo que se traduce en un 50%, esto significa, que la variable nombrada con anterioridad no es significativa para el estudio. En otras palabras, la probabilidad de que los trabajadores cambien su comportamiento producto de que otras personas de su círculo les comenten sobre cómo deben comportarse frente a la ciberseguridad, no tiene relevancia en el comportamiento del sujeto de estudio.

Ahora bien, se analiza directamente las variables entre ellas en la tabla 4.9, sin contar el comportamiento (ya que es el objetivo a estudiar), se puede notar que existen asociaciones positivas, pero imperfectas entre todas las variables, obteniendo una mayor relevancia con un valor de 0.6802 en la norma subjuntiva con la actitud, demostrando que si una de estas variables aumenta, la otra aumentará en cierto porcentaje con mayor intensidad que la relación que se encuentra entre las variables del control conductual percibido con la actitud, debido a que el resultado entregado es 0.2654.

A continuación, la tabla de valores de las correlaciones entre las variables promedio:

	ActProm	NSProm	PBCProm	IntenP~m
ActProm	1.0000			
NSProm	0.6802	1.0000		
PBCProm	0.2654	0.2882	1.0000	
IntenProm	0.5177	0.5400	0.3682	1.0000

Tabla 4.9 Correlación Entre Variables

Finalmente, para el análisis del diagrama de modelo de ecuaciones estructurales, se verifican las relaciones existentes entre las variables latentes (5 variables) y las observables. En ella se evidencia 17 variables observadas, así también 153 elementos conocidos en la matriz de covarianza, ((17 x [17+1]) / 2 = 153) y 136 grados de libertad, (153 – 17 = 136). En consecuencia, de los grados de libertad obtenidos, el modelo conceptual se ajusta bien a los datos sobre el comportamiento de ciberseguridad, es decir, en cuanto mayor sean la actitud, el control de la conducta percibida, y la intención de tener buenas prácticas de seguridad digital, mejor será el comportamiento frente la seguridad cibernética.

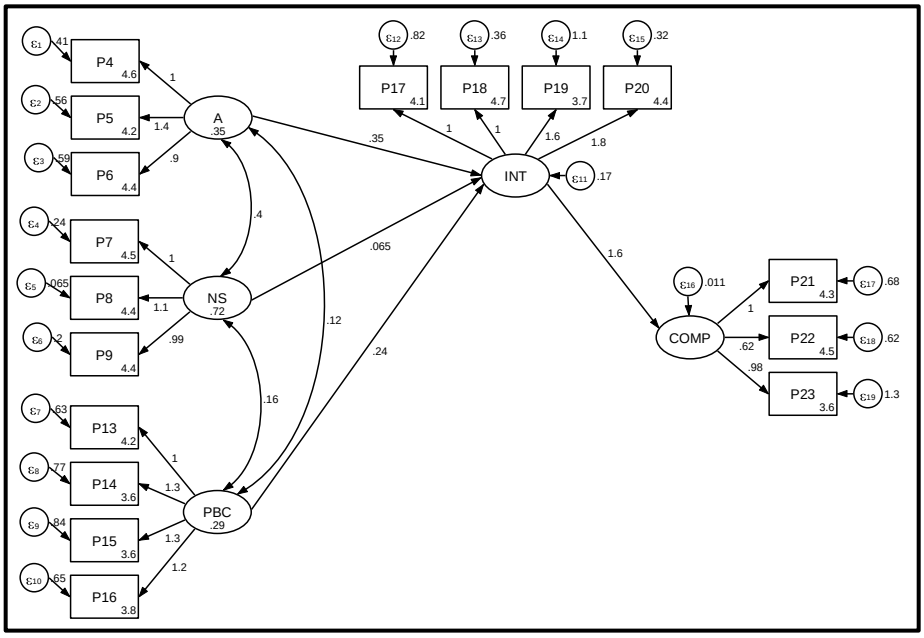


Ilustración 4.1 Modelo de la teoría del comportamiento planificado frente a la ciberseguridad con correlaciones.

4.3 Discusión Final

Con los resultados obtenidos, se confirman la mayoría de las hipótesis planteadas, es decir, las creencias individuales (A) y motivaciones (PCB), tienen una relación positiva con las intenciones (INT) previas; y la intención (INT), tiene una relación positiva con el comportamiento de seguridad digital. Lo anterior se puede respaldar con resultados similares encontrados en la investigación "Development of the Cybersecurity Attitudes Scale and Modeling Cybersecurity Behavior and its Antecedents" (Howard, 2018).

A pesar de ser probadas las hipótesis positivamente, se sugiere realizar un seguimiento de los resultados, pues los datos son obtenidos de manera auto reportadas por parte de los encuestados, los cuales no son de carácter objetivo en su totalidad. Añadiendo a esto, la percepción acerca de la ciberseguridad en general podría variar bastante entre los distintos individuos participantes del estudio, pues el 55% tiene un rango de edad entre los 41 y 65 años de edad y el resto se sitúa entre los 21 y 40 años de edad, lo que podría generar una brecha en conocimientos con respecto a la seguridad digital, aludiendo a que las personas de mayor edad tienen una menor habilidad con respecto a las tecnologías (David Alarcón & José A. Sanchez, 2015) y por tanto, en su comportamiento frente a este.

Finalmente, cabe destacar que la variable que obtuvo la mayor relación positiva respecto a la intención, resultó ser la actitud (A = 0.3473), señalando que la percepción individual de los trabajadores con respecto a la seguridad digital tiene mayor valoración positiva que la valoración a nivel grupal. Por otro lado, la intención de la persona a realizar un buen comportamiento en particular es mayor (INT = 1.5955), una de las razones que podrían explicar dicha situación, sería el avance exponencial de la tecnología, ya que del mismo modo aumentan los riesgos cibernéticos, provocando en las personas un mayor interés en cuidar sus datos digitales. En cuanto a la variable de control conductual percibido en este estudio, es positiva en relación con la intención.

CAPÍTULO 5. Conclusión, Recomendaciones y Limitaciones

5.1. Conclusión

Dado los resultados demostrados, su análisis y su previa discusión, se pueden extraer las siguientes conclusiones sobre la influencia de las creencias del comportamiento en ciberseguridad.

5.2 Conclusiones en función de los objetivos

El objetivo general del estudio, era determinar cómo las creencias de los individuos influyen en el comportamiento frente a la seguridad cibernética, para poder llegar al cumplimiento de este objetivo, se obtuvieron los siguientes análisis de los objetivos específicos:

- Se determina la relación entre la intención con el comportamiento de los trabajadores frente a la seguridad cibernética.

- Se determina la relación entre la intención con las actitudes de los trabajadores.

- Se determina la relación entre la intención con las normas subjetivas de los trabajadores.

- Se determina la relación entre la intención con el control de conducta percibida de los trabajadores.

5.3 Conclusiones en función de validación de hipótesis

Se comprueba que, para la Hipótesis 1 (H1) la actitud si está relacionada positivamente con la intención de los trabajadores, ya que, fue la que obtuvo un mayor valor numérico en el coeficiente entre las variables, dicho, en otros términos, la actitud que tendrá cada uno de los trabajadores de acuerdo a cómo quieren enfrentarse a la ciberseguridad, tendrá más importancia en la intención de un buen manejo cibernético.

Para la hipótesis 2 (H2) se demuestra que las normas subjetivas no están relacionadas positivamente con la intención de los trabajadores, ya que se pudo demostrar que existe un bajo interés en las opiniones de terceros sobre el tema por lo que no es un factor decisivo, tal como se presenta en los resultados extraídos con el software STATA-14, el cual presenta un valor bajo y no significativo. En otras palabras, la probabilidad de que los trabajadores cambien su comportamiento producto de que otras personas de su círculo les comenten sobre cómo deben comportarse frente a la ciberseguridad, no tienen relevancia en el comportamiento del sujeto de estudio.

Con respecto a la hipótesis 3 (H3) el control conductual percibido, sí está relacionado positivamente con la intención de los trabajadores, esto quiere decir que, la percepción que tiene un trabajador de PUCOBRE acerca de seguridad digital y de su disponibilidad de recursos para llevar a cabo una buena administración de su información digital, se complementará con la intención de un buen comportamiento.

Finalmente, para la hipótesis 4 (H4) la intención está relacionada directamente con el comportamiento de los trabajadores frente a la seguridad cibernética, otro modo de decir, es que ambas se complementan para que los trabajadores aporten con seguridad individual a PUCOBRE, ya que si no existe una intención verídica de un buen comportamiento no se llevará a cabo dicha conducta.

El estudio demostró que las personas, producto de sus creencias, actitudes, y motivaciones internas, actúan a favor de la ciberseguridad. En otras palabras, la gente

está preparada con voluntad (intención), para tener un comportamiento positivo frente a la seguridad digital, a la luz de los resultados y como lo mencionamos antes, los trabajadores poseían conocimiento previo, y esto se puede ratificar con PUCOBRE, quienes a principio de año realizaban capacitaciones a sus trabajadores.

5.5 Recomendación

- Una vez vista la observación qué se desprende de la variable actitud, encontramos que; "Los trabajadores tienen conocimiento acerca de la ciberseguridad", sin embargo, el comportamiento puede verse mejorado si se realizan capacitaciones al respecto, con el fin de potenciar aún más la actitud. Frente a esto, se le recomienda a la empresa PUCOBRE realizar capacitaciones.
- Aplicar el estudio en otros rubros para obtener un mayor conocimiento acerca de los comportamientos de los individuos de estudio frente a la ciberseguridad.
- Como los datos son obtenidos en un determinado tiempo, se sugiere realizar un estudio longitudinal para dar seguimiento a los resultados, con el fin de ser proyectable.
- Estudiar la ambivalencia que existe entre las creencias y el comportamiento.

5.6 Limitaciones de la investigación

- Se aplicó el estudio en el rubro de la minería en una única empresa, por tanto, no se sabe cómo resultará la investigación en otras organizaciones y con mayor razón en otro rubro.
- El estudio es de tipo transversal, ya que este analiza datos en un periodo de tiempo. Al no ser un estudio longitudinal, no es proyectable.
- No se estudia acerca de la ambivalencia que tienen los sujetos de la investigación.

CAPÍTULO 6. Bibliografía

[1] Ajzen, I. (1991). The Theory of Planned Behavior. *Organizational Behavior and HumanDecisionProcesses*,*50*(2),179–211. https://doi.org/10.1080/10410236.2018.1493416

[2] Bentler, P. M. (2006). EQS 6 structural equations program manual. In *Los Angeles: BMDPStatisticSoftware*(Issue818). http://www.econ.upf.edu/~satorra/CourseSEMVienna2010/EQSManual.pdf

[3] Campo-Arias, A., & Oviedo, H. C. (2008). Propiedades psicométricas de una escala: La consistencia interna. *Revista de Salud Publica*, *10*(5), 831–839. https://doi.org/10.1590/s0124-00642008000500015

[4] CESCO. (2020). *Hacia una minería 4.0*. 1–61. www.cesco.cl

[5] Consejo Minero, Fundación Chile y Corporación Alta Ley, Corfo, I. (2018). *Roadmap: Digitalización para una minería 4.0*.

[6] Cupani, M. (2012). Revista Tesis 2012, Nº 1. pp. 186-199 Cupani, M . *Revista Tesis*, *1*,186–199. http://www.revistas.unc.edu.ar/index.php/tesis/article/download/2884/2750

[7] Dagnino S., J. (2014). Regresión Lineal. *Revista Chilena de Anestesia*, *43*(2), 143–149. https://doi.org/10.25237/revchilanestv43n02.14

[8] David Alarcón & José A. Sanchez. (2015). *Assessing convergent and discriminant validity in the ADHD-R IV rating scale*. 1–39.

[9] Donalds, C., & Osei-Bryson, K. M. (2020). Cybersecurity compliance behavior: Exploring the influences of individual decision style and other antecedents. *International Journal of Information Management*, *51*(November 2018), 102056. https://doi.org/10.1016/j.ijinfomgt.2019.102056

[10] Escobedo Portillo, M. T., Hernández Gómez, J. A., Estebané Ortega, V., & Martínez Moreno, G. (2016). Modelos de Ecuaciones Estructurales: Características, Fases, Construcción, Aplicación y Resultados structural equation modeling: features, phases, construction, implementation and results. *Revista Ciencia y*

Trabajo,*18*(55),16–22. https://scielo.conicyt.cl/scielo.php?script=sci_arttext&pid=S0718-24492016000100004

[11] George, D., & Mallery, P. (2003). *SPSS for Windows step by step: A simple guide and reference. Fourth Edition (11.0 update)*.

[12] Hair, J., Anderson, R., Tatham, R., & Black, W. (1999). *ANALISIS MULTIVARIANTE* (pp. 1–814).

[13] Halevi, T., Lewis, J., & Memon, N. (2013). A pilot study of cyber security and privacy related behavior and personality traits. *WWW 2013 Companion - Proceedings of the 22nd International Conference on World Wide Web*, 737–744. https://doi.org/10.1145/2487788.2488034

[14] Howard, D. J. (2018). *Development of the Cybersecurity Attitudes Scale and Modeling Cybersecurity Behavior and its Antecedents*. *June*, 1–77. https://scholarcommons.usf.edu/etd/7306/

[15] Hyland, P., Shevlin, M., Adamson, G., & Boduszek, D. (2013). The factor structure and composite reliability of the Profile of Emotional Distress. *Cognitive Behaviour Therapist*, *6*. https://doi.org/10.1017/S1754470X13000214

[16] Jackson, D. L. (2003). Structural Equation Modeling : A Adding Missing-Data-Relevant Variables to FIML-Based Structural Equation Models. *A*, *10*(July 2013), 128–141. https://doi.org/10.1207/S15328007SEM1001

[17] Kline, R. B. (2016). Principles and practices of structural equation modelling 4th edition. In *Methodology in the social sciences*.

[18] Kuss, D. J., Griffiths, M. D., Binder, J. F., & Street, B. (2013). *ANÁLISIS DE LOS FACTORES DE SEGURIDAD DE UN SITIO WEB*. 1–19.

[19] MacCallum, R. C., Browne, M. W., & Sugawara, H. M. (1996). Power analysis and determination of sample size for covariance structure modeling. *Psychological Methods*, *1*(2), 130–149. https://doi.org/10.1037/1082-989X.1.2.130

[20] Maldonado Luna, S. M. (2012). Manual Práctico Para El Diseño De La Escala Likert. *Xihmai*, *2*(4), 6–8. https://doi.org/10.37646/xihmai.v2i4.101

[21] Shiffman, Leon G; Kanuk, L. (2010). Comportamiento del Consumidor. In *Pearson* (Vol.10,Issue20). https://www.pearsoneducacion.net/mexico/Inicio/comportamiento-consumidor-schiffman-8ed-ebook1

[22] Tabachnick, B. G., & Fidell, L. S. (2020). Using Multivariate Statistics. *Essentials Of Political Research*, 173–208. https://doi.org/10.4324/9780429500749-17

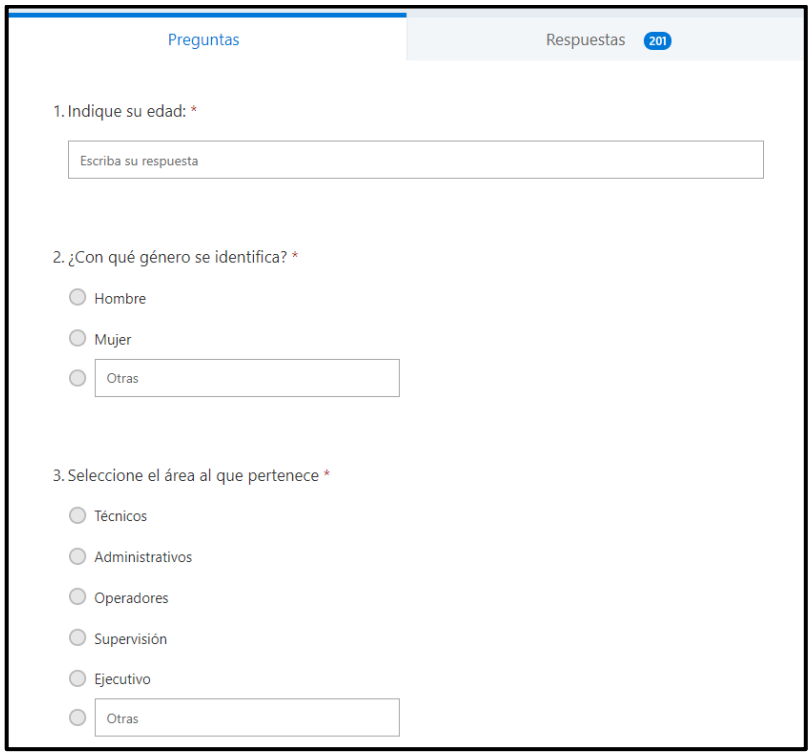
[23] Weston, R., & Gore, P. A. (2006). A Brief Guide to Structural Equation Modeling. *TheCounselingPsychologist*,*34*(5),719–751. https://doi.org/10.1177/0011000006286345

CAPÍTULO 7. Anexos

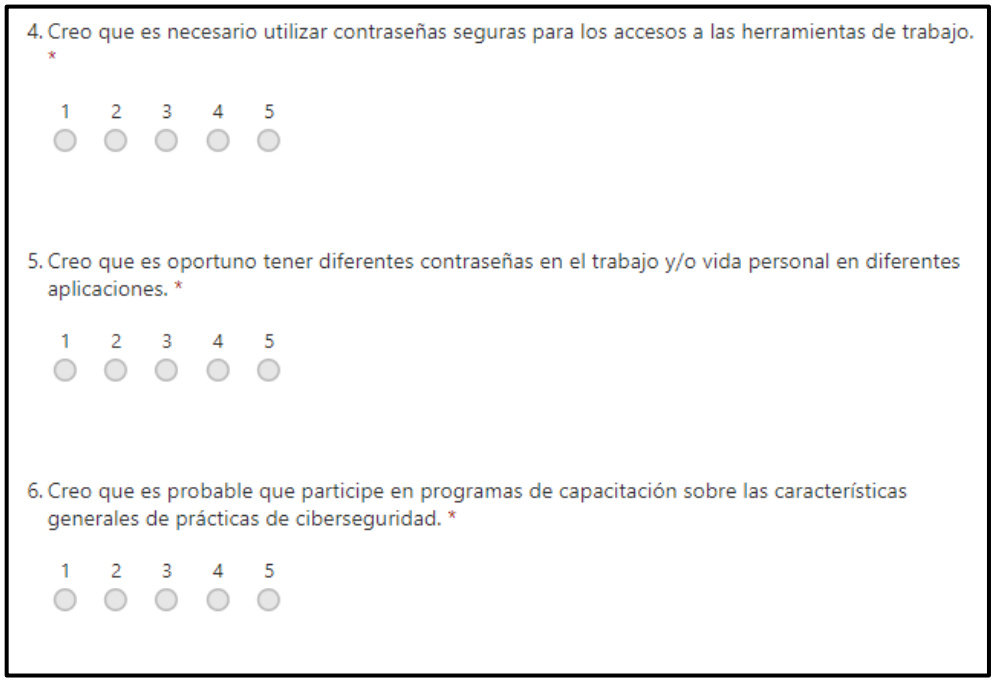
7.1 Encuesta realizada

Para Revisar la Encuesta Online, puede hacerlo con el siguiente link: https://docs.google.com/forms/d/e/1FAIpQLSc7U37eUbWmTGRUY5u-ayA3-WkPQeqrR5vMfGBbdeAGQl9AJw/viewform?usp=sf_link

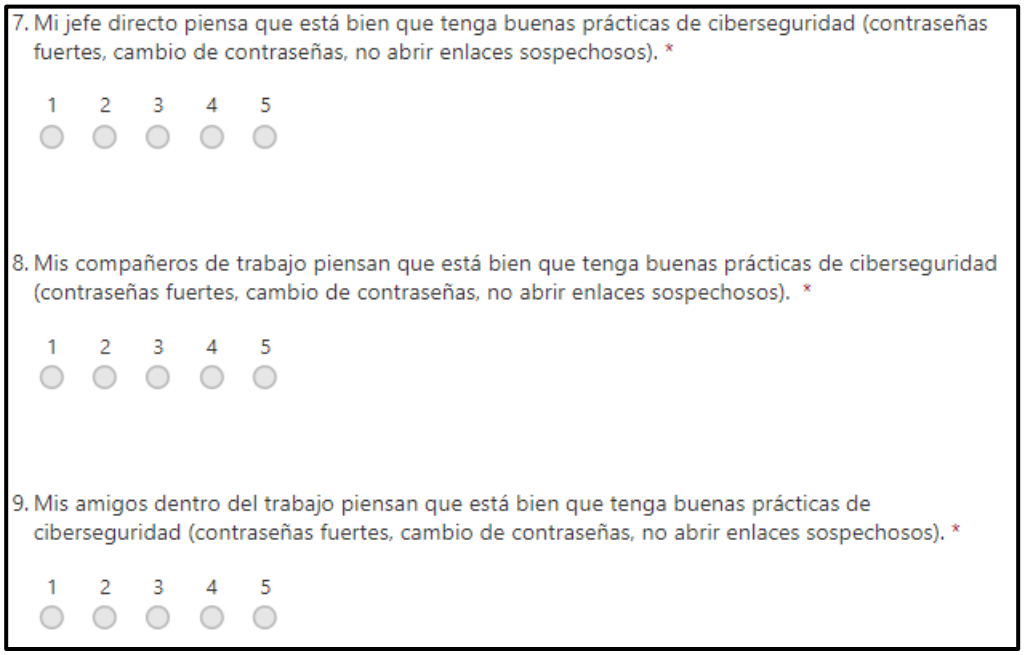
- Preguntas de características de la muestra (Pregunta 1, Pregunta 2 y Pregunta 3)



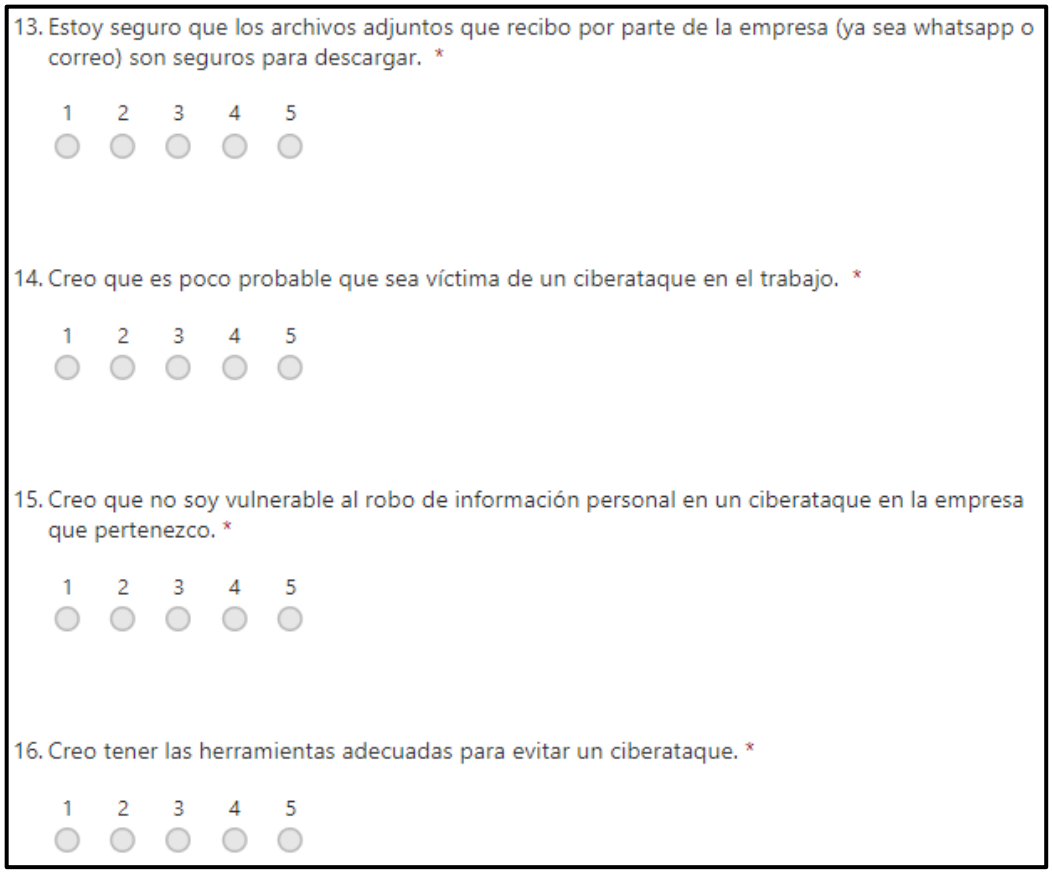
- Preguntas para evaluar la variable actitud (Pregunta 4, Pregunta 5 y Pregunta 6)



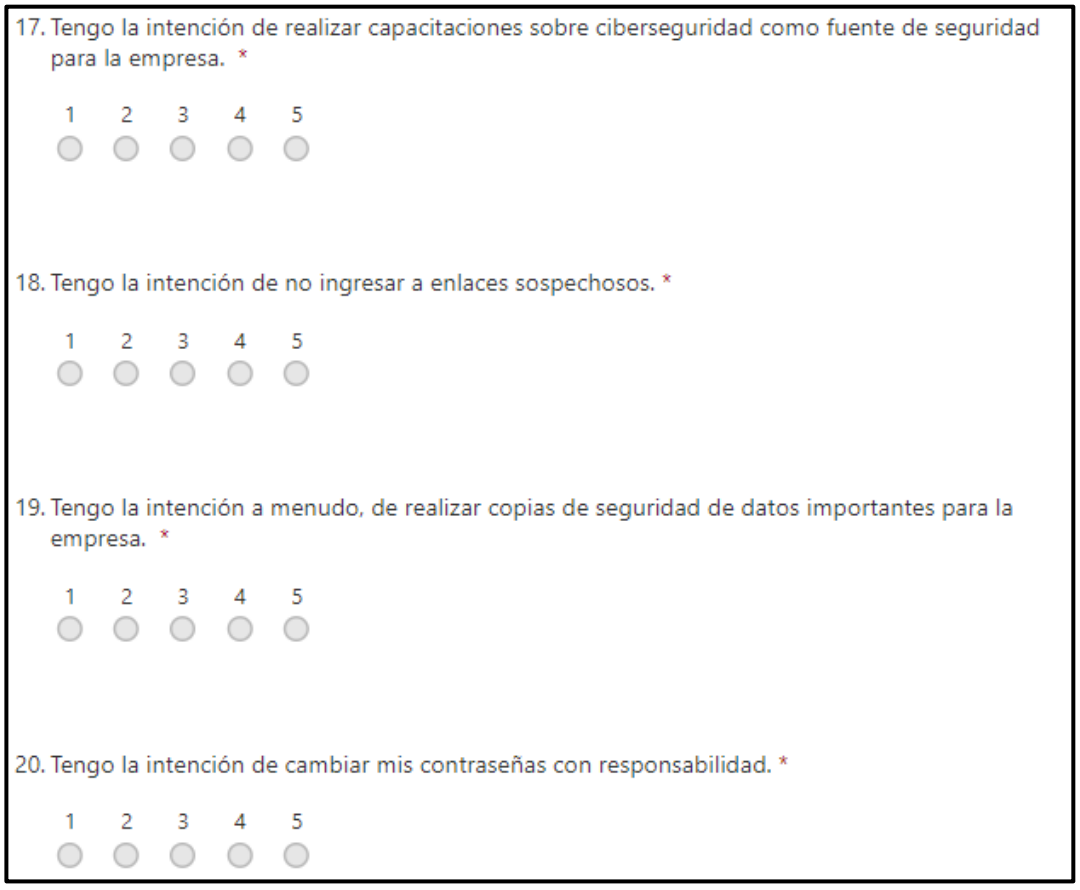
- Preguntas para evaluar la Norma Subjuntiva (Pregunta 7, Pregunta 8 y Pregunta 9)



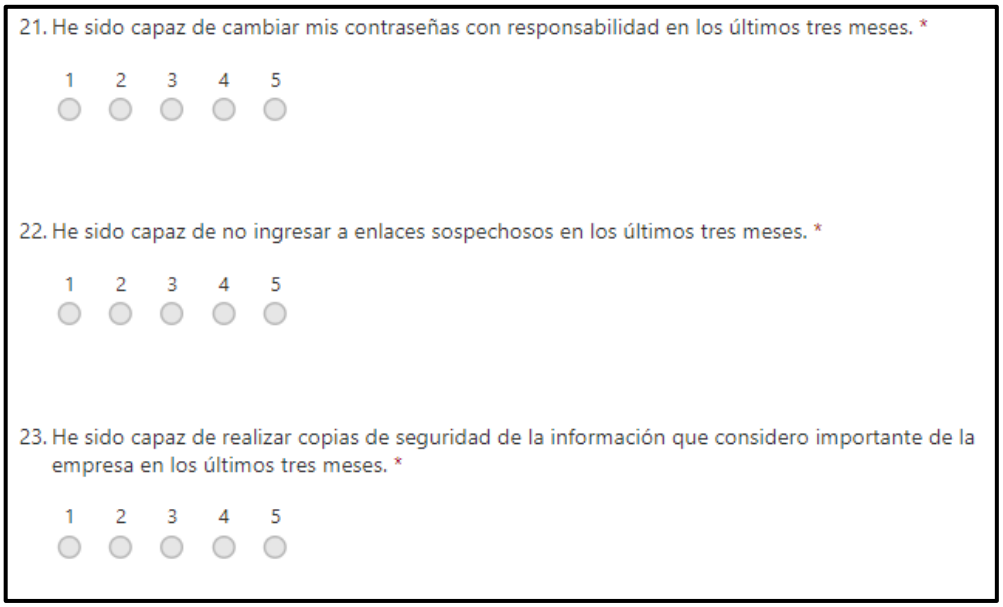
- Preguntas seleccionadas para evaluar el PBC (Pregunta 13, Pregunta 14, Pregunta 15 y Pregunta 16)



- Preguntas para evaluar la intención (Pregunta 17, Pregunta 18, Pregunta 19 y Pregunta 20)

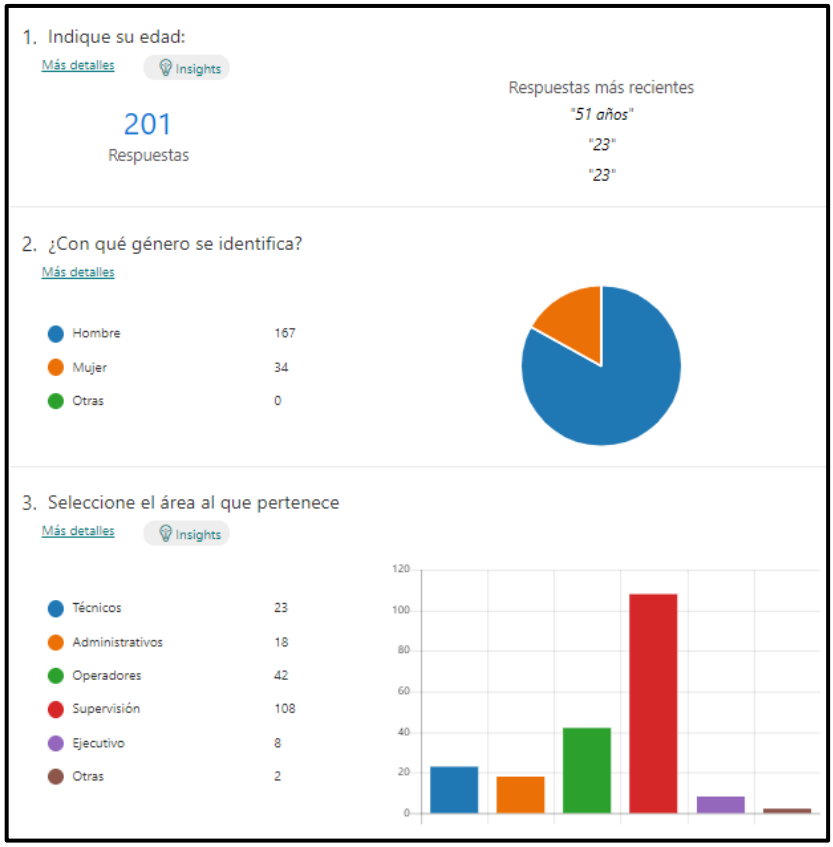


- Preguntas para determinar el comportamiento (Pregunta 21, Pregunta 22, Pregunta 23)



7.2 Resultados de encuesta

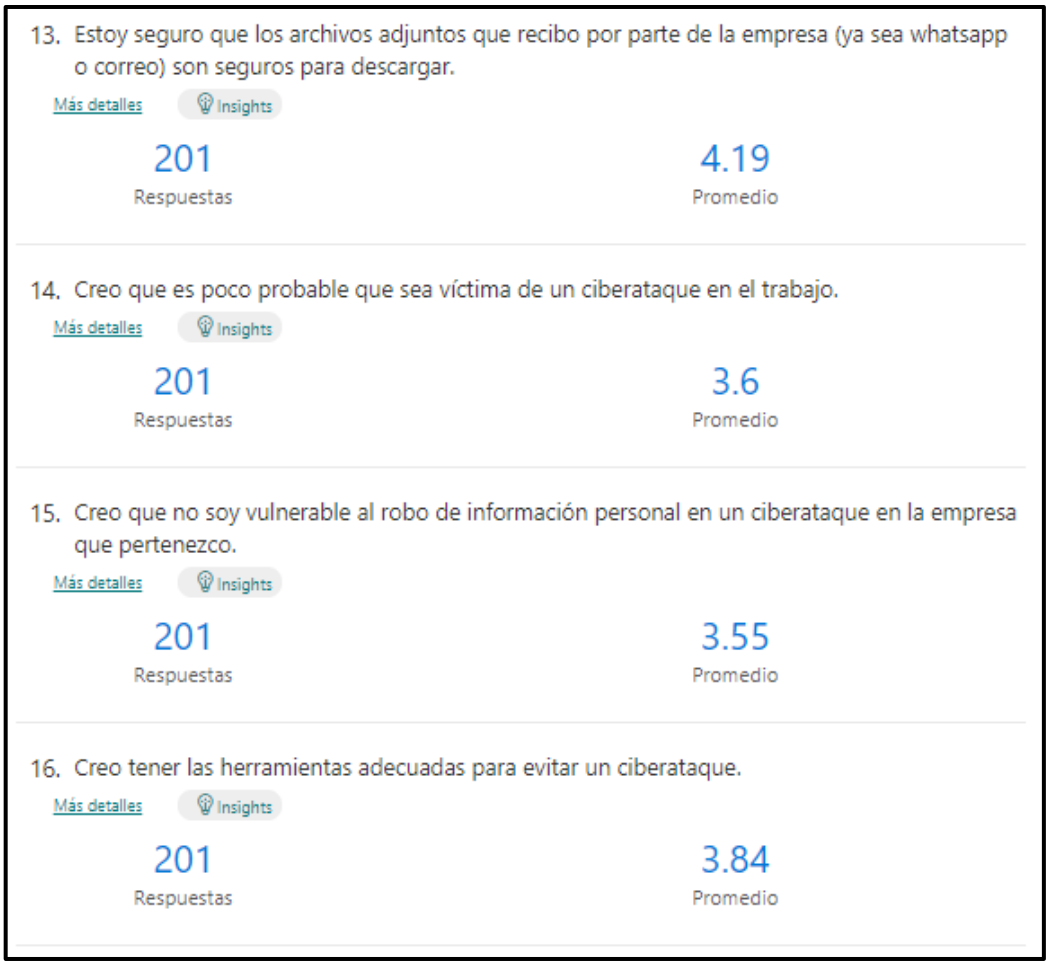
- Respuestas de características de la muestra (Pregunta 1, Pregunta 2 y Pregunta 3)



- Respuestas para evaluar la variable actitud (Pregunta 4, Pregunta 5 y Pregunta 6)

- Respuestas para evaluar la Norma Subjuntiva (Pregunta 7, Pregunta 8 y Pregunta 9)

- Respuestas para evaluar el PBC (Pregunta 13, Pregunta 14, Pregunta 15 y Pregunta 16)

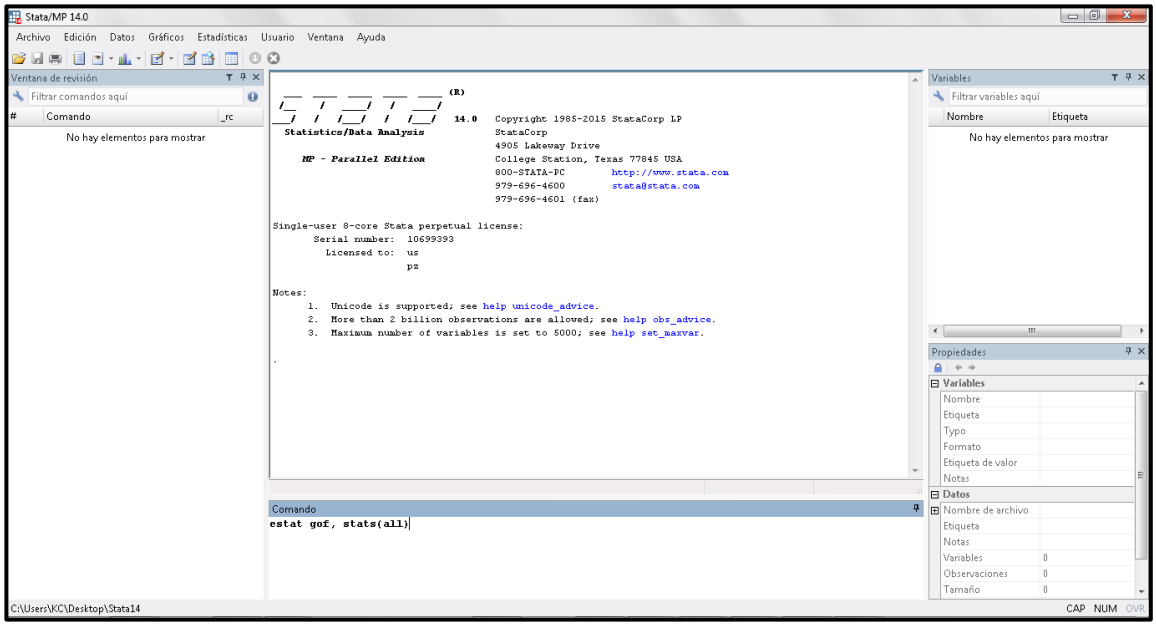


- Respuestas para evaluar la intención (Pregunta 17, Pregunta 18, Pregunta 19 y Pregunta 20)

- Respuestas para determinar el comportamiento (Pregunta 21, Pregunta 22, Pregunta 23)

7.3 Stata/MP14

Interfaz de códigos.



Interfaz para la construcción del modelo.