# Diseño de un instrumento para identificar los comportamientos que puedan interferir potencialmente en la ciberseguridad en el contexto militar.

**Camilo Andrés Quijano Rueda**

Trabajo de grado para optar al título profesional:
**Maestría en Ciberseguridad y Ciberdefensa**

**Escuela Superior de Guerra "General Rafael Reyes Prieto"**
Bogotá D.C., Colombia

2020

MINISTERIO DE DEFENSA NACIONAL
COMANDO GENERAL DE LAS FUERZAS MILITARES
ESCUELA SUPERIOR DE GUERRA "GENERAL RAFAEL REYES PRIETO"



# DISEÑO DE UN INSTRUMENTO PARA IDENTIFICAR LOS COMPORTAMIENTOS QUE PUEDAN INTERFERIR POTENCIALMENTE EN LA CIBERSEGURIDAD EN EL CONTEXTO MILITAR.

AUTOR
MY. QUIJANO RUEDA CAMILO ANDRES

MAESTRIA EN CIBERSEGURIDAD Y CIBERDEFENSA.
MONOGRAFÍA PARA OPTAR AL TITULO DE MAGISTER EN CIBERSEGURIDAD Y CIBERDEFENSA.
BOGOTÁ D.C.
2020.

**Tabla de contenido**

Introducción. ....6
Antecedentes y Conceptos. ....9
Conceptos en ciberseguridad. ....11
Contexto legal en ciberseguridad. ....14
Marco legal colombiano. ....15
Marco legal internacional. ....19
Justificación. ....23
Objetivos. ....26
Objetivo general. ....26
Objetivos específicos. ....26
Pregunta de investigación ....26
Metodología. ....27
Tipo de estudio. ....27
Variables. ....27
Participantes. ....27
Procedimiento. ....28
Consideraciones éticas. ....29
Capítulo 1. Diseño y pilotaje del instrumento. ....30
Marco teórico del estudio del comportamiento. ....30
Perspectiva teórica del estudio del comportamiento social. ....32
Diseño del instrumento. ....37
Resultados de la evaluación de los Instrumentos por expertos. ....38
Pilotaje del instrumento. ....44

Capítulo 2. Características psicométricas del instrumento.....46

Teorías de los test .....46

Escalas de puntuación.....52

Capítulo 3. Análisis técnico del instrumento. .....58

Análisis factorial.....58

Análisis técnico del instrumento.....61

Conclusiones. .....68

Referencias. .....72

APENDICES.....78

**Listado de tablas.**


| | | |
|---|---|---|
| **Tabla 1.** | Normatividad Nacional, | 16 |
| **Tabla 2.** | Iniciativas Nacionales, | 18 |
| **Tabla 3.** | Instrumentos internacionales y normatividad, | 20 |
| **Tabla 3.1.** | Instrumentos internacionales y normatividad, | 22 |
| **Tabla 4.** | Coeficiente de razón de validez de constructo (RVC), | 33 |
| **Tabla 5.** | Ítems resultantes de la evaluación por jueces, | 38 |
| **Tabla 5.** | Ítems por dimensiones, | 39 |
| **Tabla 6.** | KMO and Bartlett's Test, | 55 |

**Listado de figuras.**


| | | |
|---|---|---|
| **Figura 1.** | Estandarized residual, | 57 |
| **Figura 2.** | Summary of 75 measured person, | 59 |
| **Figura 3.** | Summary of 75 measured ítem, | 60 |
| **Figura 4.** | Item estadistic entery-order, | 61 |
| **Figura 5.** | Measure person-map-item, | 63 |

## Introducción.

La presente investigación describe desde una óptica cuantitativa, basada en la investigación científica los elementos que comprenden el desarrollo de una escala de auto informe que permite la caracterización de los comportamientos que pueden ser potencialmente peligrosos para el mantenimiento de la seguridad en el ciberespacio en el contexto militar colombiano. Desde esta perspectiva, se buscó recolectar la mayor cantidad de información posible para comprender el contexto en el cual se desarrolla la investigación y las variables que intervienen en el mismo. Teniendo en cuenta lo anterior, y para intereses de este trabajo es necesario realizar una revisión de la evidencia empírica y teórica que permite la caracterización de ciberespacio y la dimensión ciberseguridad.

Este trabajo fue desarrollado en el marco del proceso de formación de la maestría de ciberseguridad y ciberdefensa de la Escuela Superior de Guerra General Rafael Prieto Reyes. Uno de los principales precursores para el desarrollo de este trabajo es la necesidad de lograr una descripción del proceso metodológico necesario para la construcción de una escala de medición que sea útil en el marco de la investigación científica y que permita cumplir con el objetivo de reconocer y describir las variables que intervienen en el mantenimiento de la ciberseguridad en el ciberespacio. Partiendo de este principio, es necesario resaltar que en adelante se describirán dichos elementos y que como resultado de lo anterior se logrará describir el proceso de investigación adelantado, sus alcances y perspectivas de investigación futura. Así como, los resultados obtenidos tras el pilotaje y aplicación de la escala diseñada en el marco del trabajo de investigación, sin que esto constituya una medida generalizable a toda la población, o represente una última palabra en el marco de la investigación de este constructo, ya que la construcción de este tipo de herramientas requiere de diferentes procesos de validación que permitan su generalización.

De acuerdo con los intereses de esta investigación es necesario empezar por reconocer que, cuidar la información parece ser una necesidad prevalentemente importante a lo largo de la historia del hombre. Desde la antigüedad las acciones orientadas a la defensa y la protección de la información de una sociedad en particular ha sido relevantes. La conceptualización y aplicación de este constructo en diferentes contextos sociales y culturales ha ido modificándose en la medida

en que las necesidades se han ido agudizando (Coz-Fernández & Pastor-Pérez, 2013; Hernández, Cerquera & Vanegas, 2015).

De acuerdo con Deighton y Kornfeld (2013) la sociedad en general con la llegada de los avances tecnológicos comenzó a depender del ciberespacio. Las acciones del estado y los organismos de control, así como las acciones de la fuerza pública y su efectividad, se han visto directamente relacionada con los avances en tecnologías de la información. La forma de comunicación entre los diferentes actores sociales, los negocios y la economía, también se han visto beneficiados por los avances tecnológicos, traspasando fronteras nunca antes imaginadas, por lo que debe comprenderse que la tecnología y como consecuencia la información administrada a través de las plataformas tecnológicas, son una característica propia de la sociedad contemporánea.

Aun cuando en la mayoría de los casos los avances tecnológicos y de comunicación han traído consigo numerosos beneficios, el riesgo y la vulneración de la información se ha ido acelerando del mismo modo. Situación que ha obligado a los organismos de control, los estados y las fuerzas militares alrededor del mundo a generar estrategias que favorezcan la protección y defensa de la información, situación que ha provocado que la legislación a nivel nacional e internacional vaya evolucionada gradualmente (Ministerio de Tecnologías de la información y las Comunicaciones, 2016).

Si bien la legislación parece contrarrestar y generar políticas de acción frente a las amenazas y el riesgo latente de la información en el ciberespacio (Ministerio de Tecnologías de la información y las Comunicaciones, 2016). Las acciones de ciberseguridad, dependen en gran medida de los operadores de dichas acciones, razón por la cual, ha de entenderse que el comportamiento humano comprendido este desde la visión de capacidad de elección del ser humano ante un evento externo, determina en gran medida el efecto causado por las normas y las conductas adoptadas por la sociedad en materia de protección de la información. Desde esta perspectiva, se hace relevante contemplar el comportamiento humano como una variable que interviene en el éxito de las acciones de ciberseguridad.

Estudiar el comportamiento humano parece ser un reto para diferentes disciplinas científicas (Vera, 2003). Esto en la medida en que permite la comprensión de la forma en que las personas interactúan. De acuerdo con diferentes autores como Skinner (1975), Bandura (1974), Bandura y

Walters (1983) y Pellón, (2013) el estudio del comportamiento permite la comprensión de las diferentes variables que intervienen en la forma de actuar e interactuar del ser humano, así como la forma en que se aprenden los comportamientos que son socialmente aceptados en un grupo social determinado, teniendo en cuenta que el comportamiento social es aprendido y modificado de acuerdo a las normas establecidas en un grupo social determinado (Ruíz, Pellón & García, 2006).

Así como se aprenden las conductas sociales aceptadas, existen comportamientos que no son aceptados en un grupo social, los cuales son catalogados como comportamientos antisociales, dotados de intención de daño hacia las personas del grupo, y que en la mayoría de los casos son tipificados como conductas delictivas (Cruz, 2015). Estos comportamientos emitidos por personas con intención de daño parecen afectar diferentes contextos de funcionamiento de las personas a quienes son dirigidos, entre los cuales se encuentra la seguridad de la información que depositan las personas en diferentes recursos tecnológicos, y que pueden alterar el funcionamiento normal de la seguridad cibernética.

De acuerdo con lo anterior, esta investigación tiene como objetivo diseñar una escala de medición que permita: identificar los comportamientos de las personas que trabajan en el contexto militar que pueden interferir en las acciones de ciberseguridad. Dicho objetivo se llevará acabado a través el pilotaje del instrumento diseñado para tal fin. La descripción de los resultados obtenidos y el establecimiento de estrategias eficaces de evaluación que permitan la identificación de las características conductuales, es en consecuencia un resultado esperado por el investigador. Para lo cual como pregunta de investigación se plantea: ¿Cómo se desarrolla una escala de medición que permita identificar los comportamientos de las personas que trabajan en el contexto militar que pueden interferir en las acciones de ciberseguridad?

## Antecedentes y Conceptos.

Las modificaciones en las sociedades e industrias han movilizado a las grandes empresas y sociedades a las dinámicas de manejo de información en línea. Desde el inicio de la humanidad como organización social, conocer los planes o actividades de un pueblo vecino supuso ventajas, que representaban formas de comportamiento, estrategias de supervivencia y modos de relacionarse. Los cambios y avances de la tecnología de la información, han permitido que la sociedad en general use la web como medio de administración de la información y la economía, buscando hacer frente a las dinámicas de la economía global, los cambios culturales y las tendencias de las sociedades actuales.

Por su parte Coz-Fernández y Pastor-Pérez (2013) al igual que Machín y Gazapo (2016 como se cita en Coz-Fernández & Pastor-Pérez, 2013) indican que históricamente los primeros inicios de acciones similares a las propuestas en el marco de la ciberseguridad, se remontan a los comportamientos de culturas milenarias que guardaban su información a través de códigos cifrados. Un ejemplo de ello, es la cultura egipcia en la edad antigua, a partir de la cual se conceptualizó el constructo al cual llamamos en la actualidad criptografía, y que representa un claro ejemplo de acciones orientadas a proteger la información. Sin embargo, sugieren la existencia de métodos de encriptación de información desde la antigüedad.

De acuerdo con el Ministerio de Tecnologías de la información y las Comunicaciones de Colombia (2011) los avances en tecnología, y en organización de los sistemas sociales alrededor del mundo, han motivado un continuo cambio del concepto de ciberseguridad, que se ha empleado, para referirse a las acciones que se desarrollan en el marco de la seguridad de la información.

Desde esta mirada la definición más reciente es la de: conjunto de políticas y recursos, métodos de gestión de riesgo, directrices, acciones, investigación y desarrollo, formación, prácticas idóneas, seguros y tecnologías que son usadas buscando la disponibilidad, integridad, autenticación, confidencialidad y no repudio, con el fin de proteger a los usuarios y los activos de la organización en el Ciberespacio (Ministerio de Tecnologías de la información y las Comunicaciones, 2016), y que tiene sus más significativos antecedentes de riesgo en gobiernos inicialmente europeos, sin desconocer que el continente americano ha sido protagonista de ataques de la misma índole, que al igual que los estados europeos requirieron de la intervención

de entidades internacionales para superar las crisis desencadenadas tras la trasgresión de los mecanismos de seguridad empleados para su protección.

Por su parte Hernández, Cerquera y Vanegas (2015) sugieren que en el contexto mundial la ciberseguridad es un concepto que ha ido avanzando y modificándose de acuerdo con las necesidades sociales y culturales que le han demandado responder a los avances tecnológicos y los modos de operación que ponen en riego la información de relevancia para el estado, organizaciones públicas y privadas, así como la información personal de los usuarios del internet, lo que supone un riesgo generalizado.

Deighton y Kornfeld (2013) señalan que durante el siglo XX los avances en tecnología modificaron significativamente la manera de relacionarse a nivel mundial, favoreciendo que la comunicación de la mano de la tecnología atraviese las fronteras de manera real y directa, como nunca antes se había visto.

Por su parte Cueva, Camino y Ayala (2013) indican que la evolución de las estructuras sociales supuso una alineación generalizada especialmente en la forma de comportarse. De otro lado, Del Pino-Romero y Fajardo (2010) manifiestan que la expresión adecuada y efectiva de las necesidades de los usuarios y la necesidad de las organizaciones e instituciones por responder a dichos requerimientos, motivó avances significativos a través de las tecnologías de la información y las comunicaciones, generando medios de comunicación masivos que permitieron menor inversión de tiempo y mayor efectividad de las personas en sus actividades de la vida diaria en diferentes áreas de funcionamiento como: el trabajo, la educación y los negocios, suponiendo de este modo una modificación en el comportamiento social.

Situación que de acuerdo con Martínez y Jiménez (2006) no fue ajena en las operaciones militares en diferentes contextos mundiales. Razón que ha orientado a las fuerzas armadas a lo largo del mundo a diseñar estrategias que les permitan hacer presencia en el mundo cibernético (Deighton & Kornfeld, 2013). Históricamente se registran casos en Estonia y País, este último sufrió un ataque cibernético en el año 2007 el cual fue catalogado como el ataque más significativo en la historia de la seguridad al ciberespacio, y que afecto de manera considerable diferentes organismos de control del Estado (Ministerio de Tecnologías de la información y las Comunicaciones, 2011). Ahora bien, en el ámbito militar las tecnologías de información y las

comunicaciones han supuesto una innovación en todos los niveles de acción y en el concepto mismo de seguridad (Miguel, 2017).

De acuerdo con la Comisión Europea (2013) las tecnologías de la información y las comunicaciones constituyen actualmente la base del crecimiento económico de las naciones, e impactan en sectores como las finanzas, la salud, la energía y el transporte, entre otros, además de favorecer la comunicación y el intercambio de conocimientos, favorece la integración política y social en el mundo.

Sin embargo, de acuerdo con Díaz del Río (2010 citado en Wegener, 2013) vale la pena mencionar que los avances a nivel tecnológico han traído consigo el desarrollo de una serie de vulnerabilidades que ponen en riesgo la seguridad de la información, sustentada en la incuestionable dependencia de las fuerzas armadas, los organismos de control y el mismo estado al ciberespacio en funciones básicas como el apoyo logístico, el mando y control de las fuerzas, la información de inteligencia en tiempo real o en la información de los campos de batalla, en las comunicaciones, en los sistemas armamentísticos, así como en los sistemas aéreos, marítimos y terrestres (Wegener, 2013).

De acuerdo con lo anterior, es necesario describir que el estudio de este tipo de constructos, como lo es la ciberseguridad es bajo en relación a otras problemáticas relacionadas con el ciberespacio, esto en la medida en que las investigaciones se han ocupado de describir con mayor suficiencia el impacto positivo de la llegada y avance de la tecnología, lo que ha propiciado que el estudio y análisis de otras variables relacionadas con el uso de las tecnologías de información, como es el caso de la seguridad de la información, no hayan sido estudiadas, a lo largo del documento se rescatan las investigaciones más relevantes encontradas y que se desarrollan en concordancia con el objetivo de esta investigación, ahora bien, es necesario reconocer que dichas variables como es el caso del comportamientos en el contexto de la ciberseguridad, no han sido estudiados de manera suficiente para contar con evidencia empírica.

**Conceptos en ciberseguridad.**

La ciberseguridad como se ha mencionado a lo largo de este documento es un continuo de acciones adelantadas por organismos de control del estado o entidades privadas, con la finalidad de preservar la seguridad de la información. Del mismo modo, se ha mencionado que este

concepto se ha modificado de acuerdo a las necesidades sociales de los diferentes contextos en los que se han presentado amenazas contra la seguridad.

En el contexto colombiano la primera definición de ciberseguridad de acuerdo con el Ministerio de Tecnologías de la información y las Comunicaciones (2011) fue como: la capacidad del Estado para minimizar el nivel de riesgo al que están expuestos sus ciudadanos, ante amenazas o incidentes de naturaleza cibernética.

Posterior a esta definición, el Ministerio de Tecnologías de la información y las Comunicaciones (2016) la define como el conjunto de recursos, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión del riesgo, acciones, investigación y desarrollo, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse buscando la disponibilidad, integridad, autenticación, confidencialidad y no repudio, con el fin de proteger a los usuarios y los activos de la organización en el Ciberespacio.

En adelante se mencionarán algunos de los conceptos más relevantes en la materia definidos de este modo por el Ministerio de Tecnologías de la información y las Comunicaciones (2016) desde la perspectiva de la seguridad nacional así:

***Cibercrímen/delito cibernético.*** Este es definido como el conjunto de acciones o actividades ilegales asociadas con el uso de tecnologías de la in formación y las comunicaciones como medio o fin (Ministerio de Tecnologías de la información y las Comunicaciones, 2016).

***Ciberlavado***. Este definido como el uso del ciberespacio en cualquiera de sus formas, con la finalidad de dar apariencia de legalidad a bienes obtenidos ilícitamente u ocultad la ilegalidad de los mismos ante las autoridades (Ministerio de Tecnologías de la información y las Comunicaciones, 2016).

***Ciberseguridad.*** Esta comprende el conjunto de políticas y recursos, métodos de gestión de riesgo, directrices, acciones, investigación y desarrollo, formación, prácticas idóneas, seguros y tecnologías que son usadas buscando la disponibilidad, integridad, autenticación, confidencialidad y no repudio, con el fin de proteger a los usuarios y los activos de la organización en el Ciberespacio (Ministerio de Tecnologías de la información y las Comunicaciones, 2016).

De otro lado se encuentran las definiciones realizadas desde la perspectiva de defensa nacional así:

***Amenaza cibernética.*** Situación potencial que pone en peligro la seguridad cibernética de la población, el territorio y la organización política del estado (Ministerio de Tecnologías de la información y las Comunicaciones, 2016).

***Ataque cibernético.*** Acciones organizada o premeditada realizada por uno o más actores con la finalidad de causar daño o problemas a un sistema a través del ciberespacio (Ministerio de Tecnologías de la información y las Comunicaciones, 2016).

***Ciberdefensa.*** Comprende el uso de las capacidades militares ante las amenazas cibernéticas o ante actos que sean catalogados como hostiles de naturaleza cibernética y que afecten la sociedad, la soberanía nacional, la independencia, la integridad territorial, el orden constitucional y los intereses nacionales (Ministerio de Tecnologías de la información y las Comunicaciones, 2016).

***Ciberespionaje.*** Este se define como el acto o el conjunto de actos realizados sin permiso del dueño de la información que sea catalogada como personal y sensible, con la finalidad de obtener una ventaja personal, económica, política o militar en el ciberespacio a través del uso de técnicas malintencionadas (Ministerio de Tecnologías de la información y las Comunicaciones, 2016).

***Ciberterrorismo.*** Se denomina de este modo el uso del ciberespacio, como fin o como medio, con el propósito de generar terror o miedo generalizado en la población, nación o estado y desencadenando como consecuencia la violación de la voluntad de las personas (Ministerio de Tecnologías de la información y las Comunicaciones, 2016).

**Contexto legal en ciberseguridad.**

De acuerdo con Manjarrés y Jiménez (2012) las tecnologías de la información y las comunicaciones tomaron fuerza a partir de la década de los 50 con la llegada de la computadora a la sociedad, los avances fueron acelerados y la acogida por diferentes actores sociales fue aumentando en la medida en que se identificaban las cualidades de los ordenadores de aquella época y la proyección a largo plazo, su utilidad y los beneficios que parecían a portar a la sociedad en general.

Sin embargo, a pesar del impacto positivo, en los años 60 en Alemania y Estados Unidos, comenzaron a conocerse informes que reflejaban que los sistemas de información habían sido vulnerados y víctimas de abusos informáticos, en los años 70 se conocieron los primeros estudios empíricos que mostraban resultados de la investigación de delitos informáticos, estos denominados así por los investigadores en la medida en que involucraban conductas delictivas en el contexto de la informática (Manjarrés & Jiménez, 2012).

En el contexto colombiano los avances en la tecnología, la comunicación y las redes, han traído consigo múltiples avances que han permitido el desarrollo de las organizaciones e instituciones en diferentes contextos tanto públicos como privados, así como ventajas en la administración de la información, el acceso y la consulta, lo que aumenta la probabilidad de éxito y productividad esperada por las organizaciones, instituciones y la comunidad en general.

Ahora bien, el fácil acceso a los sistemas de información, y al ciberespacio favorece en primera medida la dependencia de los sistemas de información y la tecnología, limitando el acceso únicamente a las personas que cuenten con los recursos necesarios para acceder a la web, y sumado a ello el aumento de actores que buscan explorar las vulnerabilidades de dichos sistemas de información, lo que representa una amenaza y riesgo para las diversas organizaciones y especialmente para las instituciones que tiene como finalidad defender la seguridad y el estado (Ministerio de Tecnologías de la información y las Comunicaciones, 2011).

De acuerdo con la Redacción Tecnológica de El Tiempo (2011) las investigaciones realizadas por la compañía Norton de Symantec realizadas en diferentes países del mundo incluido Colombia, indicaron que cada segundo 18 personas adultas están siendo víctimas de delitos informáticos en el último año, lo que indica que por lo menos 1.5 millones de personas

usuarios de la red caen en trampas de los Hackers, cifras que pueden ascender a los 556 millones de personas al año, con un impacto económico de pérdidas superiores a los 110 millones de dólares en todo el mundo (Redacción Tecnológica de El Tiempo, 2011).

La misma investigación describe que en Colombia por lo menos el 50 por ciento de los usuarios de redes sociales encuestados han sido víctimas del ciber crimen, y al menos el 20 por ciento han sido suplantados en su perfil personal, así como el 77 por ciento considera haber sido por lo menos una vez en la vida víctima de delitos informáticos (Redacción Tecnológica de El Tiempo, 2011).

**Marco legal colombiano.**

De acuerdo con el Departamento Nacional de Planeación (2011) el Gobierno Nacional lideró un trabajo conjunto durante el año 2011, con diferentes ministerios entre los cuales se encuentran: el Ministerio de Interior y de Justicia, el Ministerio de Relaciones Exteriores, el Ministerio de Defensa Nacional, el Ministerio de Tecnologías de la información y las comunicaciones, el Departamento Administrativo de Seguridad, el Departamento Nacional de Planeación y la Fiscalía General de la Nación, a partir del cual se logró determinar que el estado colombiano no cuenta con las herramientas ni la capacidad de enfrentar una amenaza cibernética, aun cuando existen iniciativas gubernamentales y privadas que orientan sus acciones a desarrollar herramientas que favorezcan la ciberseguridad.

Por su parte Fedesarrollo (2014) en su informe anual indica que las pérdidas por delitos informáticos en Colombia ascienden a USD 500 Millones de dólares durante el último año, lo que indica que la infraestructura organizacional de Colombia, presenta vulnerabilidades, que aumentan exponencialmente el riesgo ante la creciente y evolutiva amenaza cibernética.

Por su parte el Ministerio de las Tecnologías y las Comunicaciones (2011), mediante el CONPES 3701 el país y las Fuerzas Militares de Colombia reconocieron que existe una nueva amenaza inminente, a partir de la cual se crea y activa el Comando Conjunto Cibernético (CCOC) y en el contexto de su organización ha establecido los lineamientos directrices y los criterios de nivel operacional que permiten la aplicación del poder militar dentro del quinto dominio de la guerra en todo lo relacionado con ciberseguridad y ciberdefensa, posterior a ello, en 2016 mediante el CONPES 3854 se adopta la gestión del riesgo como núcleo central para la

implementación de manera proactiva, y hace que las fuerzas militares deban fortalecer las capacidades militares en el uso del ciberespacio.

Desde esta perspectiva un caso a resaltar fue el ocurrido durante el primer semestre de 2011, cuando el grupo "hacktivista" autodenominado Anonymous atacó a los portales de la Presidencia de la República, el Senado de la República, Gobierno en Línea y de los Ministerios del Interior y Justicia, Cultura y Defensa, dejando fuera de servicio sus páginas web por varias horas. Este ataque se dio en protesta al Proyecto de Ley "por el cual se regula la responsabilidad por las infracciones al derecho de autor y los derechos conexos en Internet". Este grupo ha atacado indistintamente entidades públicas y privadas, entre las que se cuentan PayPal, el banco suizo Post Finance, MasterCard, Visa y páginas web del gobierno suizo (Ministerio de Tecnologías de la información y las Comunicaciones, 2011).

También se pueden mencionar las denuncias reportadas por los ciudadanos a la Policía Nacional. De enero a diciembre de 2009, con base en la Ley 1273/0912, se atendieron 575 delitos informáticos, que van desde el acceso abusivo a un sistema informático (259) hasta el hurto por medios informáticos y semejantes (247), la interceptación de datos informáticos (17), la violación de datos personales (35), la transferencia no consentida de activos (8), la suplantación de sitios Web (5), el daño informático (3) y la obstaculización ilegítima de un sistema informático (1).

Así mismo, durante el 2010, la cantidad de delitos y contravenciones aumentó en 73% al alcanzar un total de 995 delitos informáticos, siendo el hurto por medios informáticos el incremento más representativo al pasar de 247 a 50213 delitos, equivalentes al 103%. Estas cifras han motivado la implementación reglamentación de un marco legal nacional para combatir dicha problemática.

En adelante se presentan las normativas adelantadas por la legislación colombiana en orden cronológico, tomadas del Conpes 3701 (Concejo Nacional de Política Económica y Social de Colombia, 2011; Ministerio de Tecnologías de la información y las Comunicaciones, 2011).

**Tabla 1.**
*Normatividad Nacional.*

| Legislación | Fecha | Temática |
|---|---|---|
| Ley 527 | 1999 | Define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones. |

| | | |
|---|---|---|
| Ley 599 | 2000 | Expide el Código Penal. En esta se mantuvo la estructura del tipo penal de "violación ilícita de comunicaciones", se creó el bien jurídico de los derechos de autor y se incorporaron algunas conductas relacionadas indirectamente con el delito informático, tales como el ofrecimiento, venta o compra de instrumento apto para interceptar la comunicación privada entre personas. Se tipificó el "Acceso abusivo a un sistema informático", así: "Art. 195. El que abusivamente se introduzca en un sistema informático protegido con medida de seguridad o se mantenga contra la voluntad de quien tiene derecho a excluirlo, incurrirá en multa." |
| Ley 962 | 2005 | A través de la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos. Prevé el incentivo del uso de medios tecnológicos integrados para disminuir los tiempos y costos de realización de los trámites por parte de los administrados. |
| Ley 1150 | 2007 | Por medio de la cual se introducen medidas para la eficiencia y la transparencia en la Ley 80 de 1993 y se dictan otras disposiciones generales sobre la contratación con Recursos Públicos. |
| Ley 1273 | 2009 | Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. |
| Resolución 2258 | 2009 | Comisión de Regulación de Comunicaciones: Sobre seguridad de las redes de los proveedores de redes y servicios de telecomunicaciones. Esta resolución modifica los artículos 22 y 23 de la Resolución CRT 1732 de 2007 y los artículos 1,8 y 2,4 de la Resolución CRT 1740 de 2007. |
| Circular 052 | 2007 | Superintendencia Financiera de Colombia: Fija los requerimientos mínimos de seguridad y calidad en el manejo de información a través de medios y canales de distribución de productos y servicios para clientes y usuarios. |
| CONPES 3701 | 2011 | Lineamientos de política para la Ciberseguridad y Ciberdefensa. |

**Nota:** Tabla adaptada del CONPES 3701 (2011) diseño propio con información basada de la normativa nacional.

De otro lado, el gobierno nacional y diferentes sectores, han unido esfuerzos para el diseño de iniciativas que han permitido la elaboración y reglamentación en el marco nacional, algunas de ellas contenidas en adelante según se describen en el Conpes 3701 (Ministerio de Tecnologías de la información y las Comunicaciones, 2011).

**Tabla 2.**
Iniciativas Nacionales.

| Iniciativa. | Sector. | Alcance de la Iniciativa. |
|---|---|---|
| Modelo de Seguridad de la Información para la Estrategia de Gobierno en Línea | Programa Gobierno en Línea - Ministerio de las Tecnologías de Información y las Comunicaciones | Establece como elementos fundamentales de la seguridad de la información para los Organismos Gubernamentales: 1) La disponibilidad de la información y los servicios. 2) La integridad de la información y los datos. 3) Confidencialidad de la información. |
| Recomendaciones al Gobierno Nacional para la implementación de una Estrategia Nacional de Ciberseguridad | Comisión de Regulación de Telecomunicaciones | 1) Identifica caminos para la disuasión del crimen cibernético 2) recomienda la implementación y desarrollo de marcos jurídicos relacionados con la ciberseguridad que sean consistentes con los parámetros internacionales 3) da recomendaciones para la elaboración de sistemas de respuesta ante incidentes de seguridad en la red, incluyendo la vigilancia, análisis y respuesta a estos incidentes y 4) propone lineamientos para la implementación de una cultura nacional de ciberseguridad que mejore los niveles de protección de la infraestructura crítica de la información en Colombia. |
| CSIRT- CCIT - Centro de coordinación de atención a incidentes de Seguridad Informática Colombiano para proveedores de servicios de Internet (ISP). | Cámara Colombiana de Informática y Telecomunicaciones (CCIT) | Centro de coordinación de atención a incidentes de seguridad informática colombiano, el cual está en contacto directo con los centros de seguridad de sus empresas afiliadas (las más grandes empresas proveedoras de Internet en Colombia). Está en capacidad de coordinar el tratamiento y solución de las solicitudes y denuncias sobre problemas de seguridad informática que sean recibidas. |

**Nota:** Tabla adaptada del CONPES 3701 (2011) diseño propio con información basada de la normativa nacional.

En consecuencia, de las iniciativas y la legislación nacional, el estado colombiano ha venido resaltando la necesidad de la implementación de políticas de ciberseguridad y ciberdefensa, desde el año 2007.

Para dicho fin el Gobierno Nacional, en acompañamiento internacional, especialmente de la Organización de Estados Americanos (OEA) y a través del Comité Interamericano contra el terrorismo (CICTE) organizo desde mayo de 2008 la mesa nacional de dialogo, en el que se encomendó al Ministerio de Defensa Nacional el liderazgo para impulsar e implementar las políticas en seguridad cibernética, así como el diseño de la implementación de estrategias y mecanismos que den respuesta a los incidentes y delitos informáticos que afectan a la nación (Ministerio de Tecnologías de la información y las Comunicaciones, 2011).

Esta solicitud surgió como resultado de un profundo análisis de las particularidades del esquema de seguridad nacional, las capacidades técnicas existentes en el Ministerio de Defensa y un estudio del contexto internacional. El diagnóstico final indicó que el Ministerio de Defensa tenía la mayor capacidad para manejar de manera eficiente y coordinada estos temas (Ministerio de Tecnologías de la información y las Comunicaciones, 2011).

Lo que ha motivado al Ministerio de Defensa Nacional a promover dentro de la agenda nacional en los últimos años el dialogo y la reglamentación e implementación de políticas de ciberseguridad.

**Marco legal internacional.**

Si bien, en el contexto colombiano no se contaba con los organismos de respuesta a incidentes y delitos informáticos, se cuenta con la participación en comisiones internacionales en la región que permiten tomar referencia de las estrategias y mecanismos utilizados por los centros Nacionales de Respuesta Técnica a Incidentes Informáticos (Ministerio de Tecnologías de la información y las Comunicaciones, 2011).

Ahora bien, cabe destacar que el tema de ciberseguridad y ciberdefensa fue incluido en el Plan Nacional de Desarrollo 2010-2014 *Prosperidad para Todos*, como parte del Plan Vive Digital liderado por el Ministerio de Tecnologías de la Información y las Comunicaciones, cuyo fin es impulsar la masificación del uso de internet, para dar un salto hacia la prosperidad democrática. En adelante se presentan las iniciativas internacionales en materia de ciberseguridad. De acuerdo a la investigación realizada por el Ministerio de Tecnologías de la información y las Comunicaciones (2011). En dicha caracterización se presentan los principales instrumentos internacionales diñados.

**Tabla 3.**
*Instrumentos internacionales y normatividad.*

| Instrumento | Año | Materia. |
|---|---|---|
| Convenio sobre Ciberdelincuencia del Consejo de Europa | 2001 | El objetivo principal del convenio es la adopción de una legislación que facilite la prevención de las conductas delictivas y contribuya con herramientas eficientes en materia penal que permitan detectar, investigar y sancionar las conductas antijurídicas. |
| Convenio sobre Ciberdelincuencia del Consejo de Europa (Adaptación | 2004 | El Consejo considera que el delito cibernético exige una política penal común destinada a prevenir la delincuencia en el ciberespacio15 y en particular, hacerlo mediante la adopción de legislación apropiada y el fortalecimiento de la cooperación internacional. Cabe resaltar que si bien el CCC tuvo su origen en el ámbito regional europeo, es un instrumento abierto para su adhesión a todos los países del mundo. |
| Resolución de la Asamblea General de la Organización de los Estados Americanos. | 2004 | Estrategia Integral para combatir las amenazas a la seguridad cibernética: Un enfoque multidimensional y multidisciplinario para la creación de una cultura de la seguridad cibernética.<br>*Estipula tres vías de acción:*<br>-Creación de una Red Hemisférica de Equipos Nacionales de Respuesta a Incidentes de Seguridad de Computadores.<br>-Identificación y adopción de normas técnicas para una arquitectura segura de Internet.<br>-Adopción y/o adecuación de los instrumentos jurídicos necesarios para proteger a los usuarios de Internet y las redes de información de los delincuentes y los grupos delictivos |
| Decisión 587 de la Comunidad Andina | 2004 | Por la cual se establecen los lineamientos de la Política de Seguridad Externa Común Andina. Dentro de los objetivos de dicha política se encuentra el prevenir, combatir y erradicar las nuevas amenazas a la seguridad y cuando corresponda sus interrelaciones, a través de la cooperación y coordinación de acciones orientadas a enfrentar los desafíos que representan dichas amenazas para la Comunidad Andina. |
| Consenso en materia de ciberseguridad de la Unión Internacional | 2005 | Busca la promoción del examen de los conceptos internacionales pertinentes encaminados a fortalecer la seguridad de los sistemas mundiales de información y telecomunicaciones. |

| | | |
|---|---|---|
| de Telecomunicaciones | | |
| Resolución 64/25 | 2009 | La Asamblea General exhorta a los Estados miembros a seguir promoviendo el examen multilateral de las amenazas reales y potenciales en el ámbito de la seguridad de la información y de posibles medidas para limitar las amenazas que surjan en ese ámbito, de manera compatible con la necesidad de preservar la libre circulación de información. |

**Nota:** Tabla adaptada del CONPES 3701 (2011) diseño propio con información basada de la normativa nacional.

De acuerdo con el Ministerio de Tecnologías de la información y las Comunicaciones (2011) es importante reasfaltar que varios países de la región cuentan con equipos de respuesta a los incidentes y delitos informáticos, entre los que se encuentran países como:

- Argentina
- Bahamas
- Brasil
- Canadá
- Chile
- Estados Unidos
- Guatemala
- Paraguay
- Perú
- Surinam
- Uruguay
- Venezuela.

Lo que en el contexto mundial se traduce como la existencia de al menos 55 países con centros de respuesta (Universidad Carnegie Mellón, 2018).

Del mismo modo, en el contexto mundial el implemento de estrategias y mecanismos de ciberseguridad, ha sido implementado por diferentes países. Incorporando nuevas estrategias y capacidades de operación en el desarrollo de estas funciones tal como se muestra a continuación.

**Tabla 3.1.**

*Instrumentos internacionales y normatividad.*

| Gobierno | Año | Acción |
|---|---|---|
| Alemania | 2011 | Creación del centro nacional de ciber defensa. |
| Australia | 2008 | Creó el Centro de Operaciones Cibernéticas que coordina las acciones estatales ante los incidentes ocurridos en el ciberespacio. |
| Canadá | 2010 | Crea el centro Canadiense de Repuesta a Incidentes Cibernéticos (CCIRC), en el mismo año adoptó la Estrategia Canadiense de Seguridad Cibernética. |
| Estados Unidos de América. | 2011 | Creó un Centro de Ciber-Comando Unificado que depende de la Agencia de Seguridad Nacional en el mismo año Adopto la Estrategia Internacional para el Ciberespacio. |
| Estonia. | 2008 | Crea el Centro Internacional de Análisis de Ciber amenazas, en el mismo año adopta la Estrategia Internacional para el Ciberespacio. |
| Francia. | 2011 | Creó la Agencia de Seguridad para las Redes e Información (ANSSI) y adoptada una Estrategia de Defensa y Seguridad de los Sistemas de Información. |
| Colombia | 2011 | Establece a través del Conpes 3701 los lineamientos de política para la Ciberseguridad y Ciberdefensa. |
| Colombia | 2016 | Diseña la política de seguridad digital. |

**Nota:** Tabla adaptada del CONPES 3701 (2011) diseño propio con información basada de la normativa nacional.

## Justificación.

La investigación y los resultados basados en la evidencia científica suponen un elemento crucial para el desarrollo de herramientas generalizables en contextos diferentes a los principalmente afectados, luego las prácticas de réplica de investigación permiten suponen cambios positivos en el desarrollo y mejoramiento de los productos de investigación. Este tipo de trabajos basado en un modelo de investigación, permite la identificación y recolección de información que basada en la experiencia puede ser ajustada con la finalidad de mejorar procesos, delimitar posibles abordajes de problemáticas y aumentar los recursos que sirven como herramientas de diagnóstico y mejora.

La ciberseguridad como acción, ha ido avanzando de manera importante en diferentes escenarios mundiales, el impacto de la tecnología de la información como se ha descrito en los primeros aparados es significativo, las sociedades se han ido modificando en fundación del proceso de adaptación natural que suponen los cambios sociales, económicos y políticos; a consecuencia de la tecnología la sociedad en general se ha ido modificando y basado en ellos, es necesario que se involucren todas las variables relacionadas con el uso de la misma y las afectación que generan en diferentes dimensiones, para este trabajo de investigación es de vital importancia reconocer las variables relacionadas con la afectación que genera el comportamiento en la preservación del objetivo principal de la ciberseguridad, partiendo de la premisa de la ausencia de evidencia empírica en la materia y de la necesidad de aumentar los recursos científicos.

En la experiencia profesional como oficial de las fuerzas militares colombianas y en el ejercicio de la profesión en el contexto de ciberseguridad, se logra reconocer diferentes aspectos que contribuyen al desarrollo de nuevas propuestas y ópticas del ejercicio profesional y técnico, así como la actividad administrativa que derivan las funciones propias del cargo que se desempeñé en dicho contexto. Si bien, la práctica profesional a diario favorece el desarrollo de habilidades que se van poniendo a prueba en cada una de las situaciones en las que se requiere dar respuesta de manera efectiva a las necesidades que demanda la profesión, también se desarrollan nuevas perspectivas del ejercicio profesional, así como intereses que motivan este tipo de investigaciones.

La idea de la propuesta de investigar sobre los comportamientos que pueden interferir en las acciones de ciberseguridad, nace a través, de la observación de los comportamientos adoptados por las personas que trabajan en el contexto militar, desde esta perspectiva, llama la atención la forma en que las personas que trabajan en contexto se perciben dentro del contexto social y cultural en el que ejercen su profesión, con el pasar del tiempo y el ejercicio profesional este tipo de intereses han tomado una relevancia importante, en la medida en que así como existen variables asociadas al desarrollo técnico y de infraestructura, parecen tener un peso también muy relevante la forma en que estos desarrollos son adoptados y utilizados por las personas en el ejercicio profesional. En la práctica los profesionales que trabajan en el contexto militar parecen percibir que el contexto favorece la seguridad en diferentes ámbitos del ejercicio de sus operaciones, sin embargo, las investigaciones sugieren que aun en los contextos más controlados en términos de la seguridad, los delitos informáticos aumentan considerablemente (Forero, 2017).

Este tipo investigaciones sustenta en primer lugar, el interés en el desarrollo de investigaciones en la materia, y en segundo describen una problemática que parece afectar de manera considerable la seguridad de la información, desde esta perspectiva se hace necesario entonces, trabajar en la construcción de herramientas que permitan tener las consideraciones necesarias y adoptar las contingencias que se requieran para que el desarrollo tecnológico prevalezca como una herramienta beneficiosa para el ejercicio profesional y el uso de la sociedad en general, y que el grado de afectación del uso indebido de este tipo de desarrollos pueda ser predecible y controlable.

En la actualidad diferentes disciplinas científicas se han encargado de estudiar y tipificar los delitos informáticos (Cruz, 2015), así como el conjunto de conductas que pueden vulnerar los sistemas de información y la seguridad cibernética. Aun cuando estos esfuerzos han sido valiosos para el desarrollo de sistemas jurídicos que permitan la judicialización de dichos comportamientos, y los esfuerzos realizados por mejorar las estructuras informáticas para disminuir el riesgo y las vulnerabilidades de dichas estructuras, se carece de herramientas que permitan identificar las variables relacionadas al recurso humano, específicamente con su comportamiento, y que puedan ser elemento diferencial para mitigar las acciones que afecten la seguridad, y que puedan favorecer la percepción de seguridad de las personas que trabajan en el contexto militar, y con ello diseñar herramientas sustentadas teórica y empíricamente que

permitan modificar dicha percepción y aumentar las conductas orientadas a favorecer la seguridad (Forero, 2017).

Este tipo de herramientas ofrecen nuevas perspectivas que permitan el abordaje de las problemáticas no solo desde el componente de la infraestructura tecnológica, sino desde la perspectiva del recurso humano, aumentando la posibilidad del trabajo conjunto con otras unidades militares para mejorar las acciones en pro del desarrollo de la cultura de seguridad cibernética. A partir de la formación en el programa de maestría y la experiencia a lo largo de la formación como oficial y en esta oportunidad como investigador, me siento interesado en el desarrollo de herramientas que permitan identificar características asociadas al comportamiento de las personas que trabajan en el contexto militar, especialmente a las personas que pertenecen a la Escuela Superior de Guerra, que puedan interferir en el buen desarrollo de la ciberseguridad, adicionalmente el desarrollo de herramientas que incluyan un trabajo interdisciplinar, y la mejora en las operaciones dentro de las unidades militares en términos de la seguridad informática.

Este tipo de propuestas son factibles en la medida en que se desarrollan en el marco empírico de investigación y sugieren avances de tipo teórico e investigativo, que pueden ser generalizadas y utilizadas en otros contextos militares, aumentando la posibilidad de mejorar los procesos y las operaciones, y en ultimas mitigando la vulneración de la ciberseguridad, además de permitir un impacto en la comunidad militar en general, en la medida en que presentan resultados de investigación aportados por profesionales que se forman dentro de la Escuela Superior de Guerra.

## Objetivos.

### Objetivo general.

- Diseñar un instrumento para identificar los comportamientos de las personas que trabajan en el contexto militar que puedan interferir en las acciones de ciberseguridad.

### Objetivos específicos.

- Desarrollar el módulo de evaluación para la construcción de instrumento para identificar los comportamientos de las personas que trabajan en el contexto militar que puedan interferir en la ciberseguridad.
- Describir las características psicométricas obtenidas en el desarrollo del módulo de evaluación que permitió la construcción de un instrumento para identificar los comportamientos que puedan interferir en la ciberseguridad.
- Establecer el análisis técnico del instrumento como estrategias de evaluación eficaz para la identificación de las características conductuales, que interfieren en la seguridad del ciberespacio en el contexto militar.

### Pregunta de investigación

¿ Cómo desarrollar un instrumento que permita identificar los comportamientos que pueden interferir en las acciones de ciberseguridad?.

## Metodología.

### Tipo de estudio.

Desde el punto de vista metodológico este trabajo se desarrolló desde la perspectiva de la metodología cuantitativa y se encuentra enmarcado en un diseño no experimental con el propósito de describir los comportamientos de las personas que trabajan en el contexto militar que puedan interferir en las acciones de ciberseguridad (Hernández, Fernández & Baptista, 2010).

### Variables.

#### Comportamiento socialmente aceptado.

Conductas que han sido abaladas y/o aceptadas por un grupo social determinado, para intereses de esta investigación se catalogan así: las conductas que estén orientadas al mantenimiento de la ciberseguridad y que están alineadas con los principios de seguridad de la información en la sub especialidad de ciberseguridad y ciberdefensa de las fuerzas militares colombianas.

#### Comportamiento potencialmente peligroso.

Comportamientos que no han sido aceptados por un grupo social determinado, para intereses de esta investigación se catalogan así: los comportamientos que no se cuentan alineados con los principios de seguridad de la información en la sub especialidad de ciberseguridad y ciberdefensa de las fuerzas militares colombianas.

### Participantes.

La investigación se realizó con un grupo poblacional de la escuela superior de guerra de las fuerzas militares colombianas, la cual cuenta con una población total de 350 personas de planta. Mediante el muestreo intencional se escoge una población de 106 participantes. El muestreo intencional permite que el trabajo de investigación se desarrolle asumiendo los lineamientos básicos de selección de la muestra y por lo tanto contar con un número significativo de participantes que puedan representar el universo total de la población. La ecuación aplicada para el muestreo intencional de acuerdo con Hernández, Fernández y Baptista (2010):

$$n = \frac{N2^2\ pq}{d^2\ (N-1) + Z2pq}$$

$$n = \frac{350\ [(3.8)(0.1)]}{0.0025\ (350-1) + [(3.8)(0.1)]} = 106.18$$

**Procedimiento.**

**Primera fase.**

En la primera fase se realizó la construcción del estado del arte y se diseñó el módulo de evaluación, que permitió posteriormente la identificación de las características conductuales que interfieren en la seguridad cibernética en el contexto militar, el desarrollo de esta fase estuvo enmarcado en la consecución de la información necesaria para descripción del marco nacional e internacional en materia de ciberseguridad y ciberdefensa, así como identificar el marco teórico y conceptual desde el cual se abordó el constructo y se desarrolló el proyecto de investigación.

**Segunda fase.**

La consecución y el desarrollo de un proceso de investigación requiere una serie de pasos que permiten en primera medida la compresión del fenómeno de estudio, para posteriormente seleccionar la perspectiva que explique con mayor suficiencia el constructo de investigación y por tanto a partir de este, desarrollar el objetivo principal de la investigación. De acuerdo con esto, en el marco de la segunda fase del proceso de investigación se realizó el proceso de validación de constructo del instrumento de medición construido a partir de la información recolectada y el diseño de módulo de medición de la primera fase del proceso de investigación. Dicho proceso se adelantó a partir del modelo de evaluación de ítems por parte de los jueces expertos en la matería, seleccionados cada uno de manera intencional, con la finalidad de lograr una mayor rigurosidad al proceso de selección de los ítems que serían parte de la versión final del instrumento producto de este proyecto de investigación.

**Tercera fase.**

Posterior al análisis del proceso de evaluación de juicio de expertos, se adelantó el pilotaje de la estrategia de evaluación y se analizaron los resultados obtenidos, de manera que se puedan

construir los parámetros para la implementación de la estrategia de evaluación. Los jueces seleccionados para el desarrollo de esta fase fueron seleccionados de manera intencional de acuerdo con los lineamientos de inclusión determinador para el trabajo de investigación, entre los cuales se encuentran: pertenecer a un área en la que se trabaje directamente o se esté relacionado con la subespecialidad de ciberseguridad, contar con experiencia militar y conocer el contexto en el cual se trabaja (teniendo en cuenta su formación militar), contar con conocimientos en relación a los contenidos del instrumento. De otro lado, para contar con mayor profundidad en el desarrollo de la escala se contó con un juez experto en desarrollo de instrumentos psicométricos, con la finalidad de que se midiese de manera correcta el constructo que ha sido medido con mayor frecuencia en profesiones que estén vinculadas con el estudio de la conducta humana.

**Cuarta fase.**

Finalmente, en la cuarta fase se validó la estrategia de evaluación y se realizara el reporte de investigación a modo de monografía de investigación mostrando cada uno de los procesos adelantados a través de apartados por capítulos que aumenten la compresión del proceso y permitan cumplir con el objetivo del trabajo de investigación.

**Consideraciones éticas.**

Este estudio se clasifica como riesgo mayor al mínimo según los lineamientos de la resolución N° 008430 de 1993 del Ministerio de Salud sobre las normas científicas, técnicas y administrativas para la investigación, enfatizando: Titulo II (de la Investigación en seres humanos) Capítulos I (de los aspectos éticos de la investigación en seres humanos) y Capitulo II (de la investigación en comunidades). Aunque no se espera que realizar el auto-reporte genere algún tipo afectación en los participantes. Todos los participantes firmarán un consentimiento informado antes de iniciar su participación en el estudio, esto a través de las respuestas emitidas por los mismo en la plataforma usada para la aplicación del instrumento, las personas que aceptaron participar en la investigación respondieron a los ítems, aquellas que libremente decidieron no hacerlo abandonaron el cuestionario.

## Capítulo 1. Diseño y pilotaje del instrumento.

La construcción de instrumentos o escalas de medición ha sido un reto asumido por la comunidad académica, como una de las prácticas aplicadas con mayor influencia científica (Hernández, Fernández & Baptista, 2010). Construir una herramienta de medición implica un trabajo único en cada uno de los procesos del diseño del instrumento en la medida en que, representa un esfuerzo por mostrar a través de los resultados una visión objetiva que permite la toma de decisiones, la modificación de procesos y hasta el diagnóstico de una problemática.

Para interés de la presente investigación en este capítulo se presentarán las fases adelantadas para la construcción de una escala diseñada con la finalidad de identificar los comportamientos que puedan interferir potencialmente en la seguridad cibernética en el contexto militar. De acuerdo con lo anterior, la primera fase en la construcción de un instrumento de medición, está orientada a definir el constructo teórico que se pretende medir, para este caso, el constructo es el comportamiento específicamente, los comportamientos que puedan interferir en la ciberseguridad. En adelante se encuentra el marco conceptual que describe dicho constructo. Adicional a ello, se presentarán los elementos psicométricos de la fase de validación de contenido por jueces expertos y la escala que será utilizada en apartados anteriores para las fases de pilotaje y análisis estadístico del instrumento final.

### Marco teórico del estudio del comportamiento.

De acuerdo con Vera (2013) el estudio del comportamiento humano supone un reto para diferentes disciplinas científicas, y el interés por el estudio del mismo, ha dependido en gran medida de los hitos históricos que han representado mayor impacto en la humanidad. Por su parte Guiza (2011) y Pino (2013) manifiestan que algunos ejemplos, suponen que los cambios en la manera de comportarse se han presentado desde la antigüedad tras la organización social, la cual supuso un cambio representativo en la forma de comportarse y relacionarse. Deighton y Kornfeld (2013) describen un escenario más reciente de cambio en la organización social, con la llegada de las tecnologías de la información y las comunicaciones.

Bandura (1974) refiere que estudiar el comportamiento humano permite establecer las diferentes variables que interfieren en la manera de actuar de las personas, y comprender las como el comportamiento es aprendido y mantenido a lo largo del tiempo, especialmente cuando

nos referimos al comportamiento social. Históricamente desde la filosofía, la sociología, la antropología y la economía se ha estudio el comportamiento (Peligero, 1999). Sin embargo, de manera mucho más reciente y con mayor detenimiento a las variables intervinientes de tipo contextual e interno, la psicología del comportamiento se ha ocupado de dicho estudio, permitiendo establecer la forma en que se aprenden los comportamientos, la manera en que se mantienen y las variables que los modifican (Skinner, 1986 como se citó en Pellón, 2013).

Si bien las primeras disciplinas suponen una mirada mucho más ontológica de la conducta humana y el estudio filosófico de la misma; la psicología por su parte, se ha ocupado del estudio de la conducta desde una óptica que permite establecer las variables biológicas (emociones y procesos sensoriales), las variables sociales (procesos de aprendizaje social y variables contextuales) y las variables psicológicas (procesos cognitivos y aprendizajes de patrones de conductas) que interfieren en la comportamiento humana como un todo (Ruíz, Pellón y García, 2008). Sin embargo, el comportamiento humano es directamente observable, no así los procesos psicológicos que se desencadenan antes de la conducta manifiesta (Skinner, 1975) no obstante, el conocimiento de dichos factores es un tema fundamental para la comprensión del mismo.

De acuerdo con Skinner (1986 como se citó en Pellón, 2013) la conducta humana desde la óptica conductista de la psicología, debe ser comprendida como la contingencia entre el ambiente y la conducta, que le permiten a la persona establecer una relación de funcionalidad, es decir la efectividad de la conducta en un determinado contexto de funcionamiento, o ambiente en donde se desarrolla la conducta. El ambiente es el encargado de reforzar el aprendizaje de acuerdo a las consecuencias recibidas por la conducta emitida, las cuales pueden ser positivas o negativas. Para la comprensión de dicha relación, es necesario saber que está es de orden bidireccional, es decir que el comportamiento humano depende tanto de los aprendizajes previos de la persona, como de las variables externas que provienen de su contexto de funcionamiento, quienes actúan como agentes de modificación de la conducta, parta que esta se mantenga a lo largo del tiempo o sea extinguida.

Sin embargo, existen otras apreciaciones científicas que definen el estudio del comportamiento desde diferentes ópticas, algunas de ellas distan de manera significativa a la propuesta inicial sustentada por la corriente conductista de Watson y Skinner (descrita en Pellón, 2013) sino que, por el contrario, introducen variables que no habían sido contempladas en el

estudio inicial. Un ejemplo de ello es la postura del aprendizaje social de la conducta propuesto por Albert Bandura, que incluye una relevancia a los procesos cognitivos, sin sustentar que estos sean los únicos responsables del aprendizaje de los comportamientos sociales, sino protagonistas del proceso de aprendizaje.

**Perspectiva teórica del estudio del comportamiento social.**

Por su parte Bandura (2000) sostiene que el comportamiento de las personas está determinado por los modelos disponibles en su ambiente, en este orden de ideas, el modelamiento, es decir el proceso de observación de la conducta emitida en otros, es el que configuran los patrones de comportamiento estables en el tiempo, pero a diferencia de Skinner (1975), plantea que los reforzamientos no necesariamente tiene que ser directos, sino que por el contrario al observar que las consecuencias del comportamiento en otras personas son reforzadas, se dará el aprendizaje.

Desde esta perspectiva es necesario adoptar el modelo teórico de conceptos y constructos estudiados desde la disciplina psicológica de la conducta social, sin que esto represente una compresión absoluta de los constructos, en la medida en que no es el objetivo principal de la investigación, sino por el contrario con la finalidad de tener una visión global y detallada del estudio del comportamiento humano y a las diferentes variables que interfieren, en procesos tales como la conducta social, que resulta ser un constructo clave para los intereses de esta investigación.

El aprendizaje de la conducta social supone uno de los procesos más complejos de la conducta humana (Bandura, 2000). Aprender un comportamiento requiere de la interacción de diferentes procesos psicológicos, como: la memoria, la emoción, la motivación, la atención, el leguaje y el pensamiento, y de procesos sociales dependientes del contexto de funcionamiento que retroalimentan la conducta y hacen que esta sea mantenida, es decir aprendida (Ruíz, Pellón & García, 2008). Ahora bien, la relevancia del aprendizaje para los intereses de esta investigación, se sustentan en la necesidad de comprender que comportamientos han sido aprendidos socialmente por las personas que trabajan en el contexto militar que puedan afectar el desarrollo exitoso de las acciones de ciberseguridad.

Desde esta perspectiva se realizará una descripción de las diferentes ópticas desde las cuales se estudia y comprende el comportamiento social. Para comenzar, es importante señalar que el aprendizaje de conductas sociales, depende en gran medida de la forma en que dicho comportamiento sea interpretado y las consecuencias del mismo en el contexto social en el cual es manifestado. El comportamiento según Skinner (1975) y Bandura (2000) el primero autor de la psicología comportamental y el segundo autor del aprendizaje social, desde ópticas diferentes, coinciden en que este es aprendido a causa de las consecuencias recibidas por el individuo de manera directa u observadas en otras personas.

Ahora bien, es necesario que comencemos por hablar del comportamiento socialmente aceptado. Este se refiere a la conducta o comportamientos que son aceptados por el contexto social en el cual son manifestados, y que corresponden al comportamiento esperado dentro de un grupo social determinado (Allport, 1975; Bandura, 1977; Worchel, Cooper, Goethals, Olson, 2000). Es importante señalar que los comportamientos socialmente aceptados varían de un contexto social a otro, es decir que los comportamientos sociales aceptados en la sociedad civil pueden diferir de los comportamientos aceptados en el contexto militar, aun cuando estos se desarrollen en un mismo marco cultural y político.

De otro lado encontramos el comportamiento asocial, este tipo de comportamientos no resulta ser dañino para un grupo socialmente determinado, puede o no ser aceptado por el grupo social (Sanabria & Uribe, 2009), y es denominado de este modo en la medida en que quien lo emite carece de interés por las relaciones con otras personas, y depende de la historia de aprendizaje individual (Bandura & Walters, 1983). Por otra parte, se encuentra el denominado comportamiento antisocial, este a diferencia del anterior, está dotado de una intención de daño hacia las otras personas del grupo social (Worchel, Cooper, Goethals & Olson, 2000). En algunos casos este comportamiento es tipificado como delictivo, sin embargo, en otros casos no resulta ser un comportamiento delictivo, aun cuando causa daño a las personas próximas de un grupo social determinado (Cruz, 2015).

El aprendizaje de los comportamientos sociales, sean estos aceptados o no en el grupo social determinado, dependen de diferentes factores subyacentes especialmente al componente contextual (Domjan, 2010). Cuando se pertenece a un grupo social, los comportamientos tienden a parecerse, las prácticas sociales y culturales son relevantes para el establecimiento de los

mismos. Sin embargo, de acuerdo con Pérez (1994) es importante mencionar que la conducta social, implica un proceso altamente complejo, en el que el individuo contrasta sus recursos personales frente a las necesidades demandadas por su contexto.

Por su parte Tarpy (2000) al igual que Bandura (2000) manifiestan que llama la atención, reconocer que de acuerdo a las normas socialmente establecidas en determinado grupo de personas u organización estas modifiquen el comportamiento de las personas y orientes sus acciones hacia el comportamiento aceptado por dicho grupo, aun cuando las características individuales de la persona sean diferenciales (Azjen, 1988; Chance, 2000).

Lo que hace necesario considerar que el estudio social de la conducta tiene una mirada individualista. De acuerdo con Cruz (2015) la individualidad en psicología social es entendida como el estudio de las funciones psicológicas fundamentales de los individuos, sin hacer referencia a los factores sociales que las determinan. Por otro lado, diversos autores definen el individualismo como un conjunto de creencias, valores y prácticas culturales en el que los objetivos individuales predominan sobre los grupales (Allport, 1975; Bandura & Walters, 1983).

Ahora bien, de acuerdo con lo anterior debe señalarse que el medio modifica la conducta, es decir las variables intervinientes desde el contexto en el cual se emiten los comportamientos, son determinantes de la forma en que actúan las personas (Domjan, 2010). Lo que sustente que, con la llegada de las tecnologías de la información y las comunicaciones, la manera relacionarse, aprender y entrenarse en diferentes lugares del mundo se ha modificado. Con mayor frecuencia en lugares en los que la tecnología se ha convertido en una herramienta importante para el desarrollo económico, político y social. Del mismo modo, la tecnología ha influido de manera significativa en la vida de los seres humanos. El internet se ha convertido en el medio de comunicación más efectivo en las relaciones interpersonales, los negocios y el conocimiento.

Si bien, la llegada de las tecnologías de la información, suponen modificaciones en las estructuras y la organización social (Deighton & Kornfeld, 2013), el estudio del comportamiento humano desde una óptica social ha permitido la caracterización de fenómenos sociales en el contexto cibernético (González, 2016), que llaman la atención de la comunidad en general y que han motivado la implementación de diferentes alertas y acciones civiles y gubernamentales en la

materia, desde esta perspectiva, realizaremos una corto recorrido por el estado actual del estudio de los comportamientos antisociales en el contexto cibernético.

Los delitos informáticos parecen ser una de las principales motivaciones de la implementación de acciones en contra de los mismos desde la población en general, hasta las entidades gubernamentales y de control de las naciones. Sin embargo, la revisión realizada en esta investigación muestra un interés marcado de los investigadores, por comprender las conductas antisociales desde una óptica que involucra a la población civil, especialmente a los menores de edad que se ven involucrados en situaciones de abuso y acoso escolar en los cuales los victimarios usan como medio el ciberespacio para atacar a sus víctimas, y que dan lugar a diferentes fenómenos sociales relacionados con esta problemática (Lucio-López & Prieto-Quezada, 2014; González-García, 2015). Las conductas de acoso en el ciberespacio están siendo ampliamente estudiadas, aunque comúnmente siguen confundiéndose los conceptos de ciberacoso en general y el de cyberbullying, como variante específica (Gonzales -García 2015). Dicho aumento de estas conductas se ha dado la medida en que los comportamientos de las nuevas generaciones que tienen lugar en el ciberespacio, y el crecimiento ha sido acelerado y con mayor participación juvenil (Miro, 2012).

Ahora bien, a pesar de dicho interés por parte de los investigadores, vale la pena resaltar que existe poco material investigativo aportado desde la academia que permita la compresión de los comportamientos antisociales en contextos empresariales o gubernamentales. Sin embargo, de acuerdo con el Centro de Innovación en Formación Profesional de Europa (2018) los casos de comportamientos antisociales ejecutados por hackers a importantes empresas suponen un reto para las tecnologías de la información y las comunicaciones en materia de ciberseguridad. En la medida en que los pronósticos de este año no parecen mejorar las cifras de incidentes de seguridad en internet, obligando a las instituciones y empresas a tomar medidas y prepararse frente a los posibles ataques.

Esto sustentando en que la ineficiente gestión de las ciberseguridades en la actual sociedad de consumo, representan un gran impacto de tipo económico, político y social, así como una gran repercusión mediática que genera una situación de desconfianza entre los clientes, accionistas o trabajadores y la población en general. Aunque existe la creencia que las grandes empresas son

las más afectadas por estos ataques, lo cierto es que las pequeñas y medianas empresas son las que suelen ser frecuentes víctimas de estos incidentes; así como la población civil.

Sin embargo, el fácil acceso a los sistemas de información, y al ciberespacio favorece en primera medida la dependencia de los sistemas de información y la tecnología, limitando el acceso únicamente a las personas que cuenten con los recursos necesarios para acceder a la web, y sumado a ello el aumento de actores que buscan explorar las vulnerabilidades de dichos sistemas de información, lo que representa una amenaza y riesgo para las diversas organizaciones y especialmente para las instituciones que tiene como finalidad defender la seguridad y el estado (Ministerio de Tecnologías de la información y las Comunicaciones, 2011).

De acuerdo con la Redacción Tecnológica de El Tiempo (2011) las investigaciones realizadas por la compañía Norton de Symantec realizadas en diferentes países del mundo incluido Colombia, indicaron que cada segundo 18 personas adultas están siendo víctimas de delitos informáticos en el último año, lo que indica que por lo menos 1.5 millones de personas usuarios de la red caen en trampas de los Hackers, cifras que pueden ascender a los 556 millones de personas al año, con un impacto económico de pérdidas superiores a los 110 millones de dólares en todo el mundo (Redacción Tecnológica de El Tiempo, 2011).

La misma investigación describe que en Colombia por lo menos el 50 por ciento de los usuarios de redes sociales encuestados han sido víctimas del cibercrimen, y al menos el 20 por ciento han sido suplantados en su perfil personal, así como el 77 por ciento considera haber sido por lo menos una vez en la vida víctima de delitos informáticos (Redacción Tecnológica de El Tiempo, 2011).

**Diseño del instrumento.**

***Fase 1.*** Inicialmente es necesario revisar y limitar teóricamente la definición de las variables y sus componentes (Hernández, Fernández y Baptista, 2010), en este caso el concepto de comportamiento, basándose en el desarrollo el estado del arte y la evidencia empírica de estudios similares en los cuales ha sido de interés el constructo del comportamiento en ciberdefensa y teniendo en cuenta que no hay un consenso entre las definiciones y las dimensiones, el desarrollo de este instrumento se basó en el modelo de comportamiento social planteado por Bandura (2000).

Teniendo en cuenta el planteamiento teórico de este autor, para intereses de la investigación se describieron los comportamientos que son categorizados dentro del contexto de ciberseguridad como comportamientos potencialmente peligrosos o dañinos, que pueden alterar el curso normal de la ciberseguridad en el contexto militar. Teniendo en cuenta la elaboración del estado de arte se identifican carencias a nivel metodológico y de evidencia empírica en el contexto nacional e internacional en materia investigativa, que no han permitido el diseño de este tipo de instrumento o escalas, razón que hace que este proceso represente un esfuerzo mayor en términos metodológicos e investigativos.

De acuerdo con las características de la población a la cual se le aplicara el instrumento, este está diseñado con la finalidad de medir 23 conductas a través de una escala de medición de falso verdadero, que permite que el evaluado seleccione la opción que le describa en términos conductuales y el ajuste del examinado a las conductas socialmente aceptadas en el marco de la ciberseguridad en el contexto militar colombiano.

Dicha medición se realizó a través de cuatro dimensiones diseñadas dentro del instrumento, la primera (1) orientada a la medición de prácticas de protección de la información a través del uso adecuado de los sistemas y la infraestructura tecnológica, la segunda (2) dimensión diseñada para medir conocimiento de la legislación y normativa en materia de ciberseguridad, la tercera (3) orientada a la medición de prácticas de alojamiento de la información que puedan afectar potencialmente la seguridad de la información y la cuarta (4) diseñada para medir prácticas que pongan en riesgo el acceso a la información.

**Resultados de la evaluación de los Instrumentos por expertos.**

En el marco del desarrollo de instrumentos de medición, se cumplen con diferentes procesos que permiten la consecución del instrumento final de aplicación, entre estos procesos se encuentra la revisión por parte de jueces expertos, diseñada con la finalidad de conseguir la valides del contenido de la escala, dicho procedimiento se realiza de manera intencionada para los intereces de la investigación (Aiken, 2003), lo que quiere decir que se ubican los jueces expertos de acuerdo al nivel de formación y experiencia que corresponda a las finalidades para las que son convocados. Entre las características más relevantes se requería para la selección de los jueces expertos que estos, contaran con la experiencia en el campo de ciberseguridad y ciberdefensa, que refirieron un nivel de formación en profesionales vinculadas con el área de sistemas de información o que su arma correspondiera comunicaciones militares.

Para los intereses de este trabajo de investigación se seleccionaron ocho (8) perfiles profesionales que contaban con la experiencia y manejo de la temática para la cual fue diseñada la escala, las preguntas contendidas en dicho proceso permiten identificar el grado de pertinencia de la ubicación de los ítems dentro de la escala, la corrección gramatical y demás ajustes que correspondan. Entre los jueces expertos se contó con la participación de:

*(1) Javier Ignacio Velásquez Bolívar*

Profesional operación negocios área transmisión y distribución

Adscrito al proyecto de ciberseguridad centinela, 10 años de experiencia en el sector eléctrico

5 años en el Sector Privado.

*(2) Teniente. Alfredo Miranda*

Armada de Perú

Ingeniero de Sistemas con Especialización en Redes.

Director Ciberseguridad Armada de Perú

*(3) Teniente Coronel. Jose Wilfredo Oseguera*

Ejercitó de Honduras

Ingeniero de Sistemas con Especialización en Seguridad Informática

Director Ciberataques Ejército Honduras

***(4) Técnico Segundo. Andrea Tovar***

Fuerza Aérea de Colombia

Ingeniera de Sistemas con Maestría en Educación

Especialista en Seguridad Informática

Suboficial de TICs Escuela Superior de Guerra

***(5) Teniente. Jaimes Bermon Hector***

Oficial de la Fuerza Aérea de Colombia

Ingeniero de Sistemas Especialista en Seguridad Informática

Oficial TICs J-6 Comando General

***(6) Subteniente Noguera Diego***

Oficial de la Fuerza Aérea

Ingeniero de Sistemas

Especialista en Redes Informáticas

***(7) Subteniente. Khristian Morales***

Oficial Fuerza Aérea

Ingeniero de Sistemas

Especialista en Seguridad Informática.

***(8) Teniente de Navío Mónica Burgos.***

Ingeniera de Sistemas, Especialista en redes de computadores.

Oficial de la Armada de Colombia

Jefe del Departamento de Telemática de la Base Naval No.6 ARC Bogotá.

El proceso de revisión por parte de los jueces expertos incluyo la revisión de los siguientes aspectos pertinencia, está definida de acuerdo con o intereses de este trabajo de investigación como el ajuste del ítem en representación del universo total de preguntas posibles. Dicha pertinencia debería corresponder del mismo modo a la dimensión que se pretende evaluar a través de la escala, y de este modo seleccionar los ítems que correspondan a dicha pertinencia y se ajusten al modelo estadístico (Lawshe, 1975) seleccionado para el filtraje y selección de los ítems finales, como resultado del posterior de evaluación por parte de jueces expertos.

El instrumento se diseñó con la finalidad de medir los comportamientos que pueden interferir potencialmente en la seguridad cibernética en el contexto militar en adelante denominado como ESCOM-23. El contenido se ha desarrollado mediante revisión bibliográfica, en la que se incluyen estudios científicos, revisiones teóricas o planteamientos teóricos sobre las acciones que han generado afectación en la seguridad de la información. Una vez realizado dicho proceso de construcción de los ítems mediante la recolección y conocimientos en el marco de ciberseguridad, los ítems de la escala fueron sometidos a validación por jueces expertos seleccionados de acuerdo a los criterios mencionado en el apartado anterior.

Entre las consideraciones revisadas por los expertos se expusieron las cuatro (4) dimensiones diseñadas para la medición del constructo. Para dicho análisis se utilizó la medida de acuerdo de jueces expertos usando el coeficiente de razón de validez de constructo planteado por Lawshe (1975), obteniendo como resultado un acuerdo entre los jueces en términos de pertinencia y no pertinencia de los ítems. Como se describe en la tabla 4.

De acuerdo con el planteamiento de Lawshe (1975) la formula estadística que permite determinar la razón de valides de constructo, se incluye $n_e$ = número de jueces que consideran el ítem válido y N=número total de expertos.

$$RVC = \frac{n_e - N/2}{\mathrm{N}/2}$$

Este índice expresa la comunalidad o traslapo que se origina entre la ejecución en la prueba y la habilidad teórica que se define en el dominio. Tristán (2008) propone que la Razón de Validez de Contenido (RVC) debe ser igual o superior a 0.5823. El análisis estadístico de los ítems incluyó la determinación del índice de homogeneidad.

El RVC oscila entre +1 y -1, siendo las puntuaciones positivas las que indican una mejor validez de contenido. Un índice RVC = 0 indica que la mitad de los expertos han evaluado el ítem como esencial, debiendo eliminarse, por tanto, los ítems con una bajo RVC serán eliminados.

Una vez comprobado el grado de acuerdo de los expertos y, por tanto, los ítems que permanecen y desaparecen de la prueba inicial, el siguiente paso es verificar el grado de acuerdo de los jueces sobre la pertenencia de cada ítem a una de las dimensiones consideradas y se procede a la aplicación de la escala en la fase de pilotaje.

Además de las consideraciones de acuerdo entre los jueces expertos, se tuvieron en cuenta las indicaciones y recomendaciones en materia de gramática, razón por la cual algunos de los reactivos de la escala fueron ajustados para una mejor redacción y por ende una mejor compresión. Obteniendo como resultado los ítems descritos en la tabla 5.

**Tabla 4.**

*Coeficiente de razón de validez de constructo (RVC)*

| | Experto | | | | | | | | *Índices de RVC* | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Ítem | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | *Jueces* | *Pertinente* | *No pertinente* | **RVC** |
| PPI1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 8 | 8 | 0 | 1 |
| PPI2 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 1 | 8 | 7 | 1 | 0,8 |
| CLG3 | 1 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 8 | 7 | 1 | 0,8 |
| CLG4 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 8 | 8 | 0 | 1 |
| PAI5 | 1 | 1 | 1 | 1 | 0 | 1 | 1 | 1 | 8 | 7 | 1 | 0,8 |
| PAI6 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 8 | 8 | 0 | 1 |
| PPI7 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 8 | 8 | 0 | 1 |
| PPI8 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 8 | 8 | 0 | 1 |
| CLG9 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 8 | 7 | 1 | 0,8 |
| CLG10 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 8 | 7 | 1 | 0,8 |
| CLG11 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 1 | 8 | 7 | 1 | 0,8 |
| PPI12 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 1 | 8 | 7 | 1 | 0,8 |
| PRI13 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 8 | 7 | 1 | 0,8 |
| PAI14 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 1 | 8 | 7 | 1 | 0,8 |
| PRI15 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 8 | 8 | 0 | 1 |
| PRI16 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 8 | 8 | 0 | 1 |
| PAI17 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 8 | 8 | 0 | 1 |
| PRI18 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 1 | 8 | 7 | 1 | 0,8 |
| PRI19 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 8 | 7 | 1 | 0,8 |
| PRI20 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 8 | 8 | 0 | 1 |
| PPI21 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 8 | 8 | 0 | 1 |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| PRI22 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 1 | 8 | 7 | 1 | 0,8 |
| PRI23 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 8 | 7 | 1 | 0,8 |

**Nota.** Elaboración propia.

Como se observa en la tabla 4., en general los ítems fueron aceptados en términos de pertinencia por los jueces expertos, lo que represento un nivel de ajuste adecuado para los intereses de la investigación, sin que se requiriera eliminar o desechar alguno de los reactivos.

En términos de las dimensiones a las cuales pertenecen cada uno de los ítems y su ajuste en la misma, se evidencia un acuerdo y las recomendaciones estuvieron orientadas a mantener la estructura de la prueba. Razón que permitió la modificación únicamente términos gramaticales de los ítems 7, 22 y 23 por cuestiones de redacción, en relación a los demás ítems restantes estos fueron aceptados y utilizados para el proceso de pilotaje del instrumento.

**Tabla 5.**

*Ítems resultantes de la evaluación por jueces.*

| | ÍTEM |
|---|---|
| PPI1 | Periódicamente realizo actualizaciones a software y sistemas en mi equipo de trabajo dentro de la institución. |
| PPI2 | Antes de descargar archivos en mi equipo de trabajo realizo un análisis de seguridad independiente del remitente del archivo. |
| CLG3 | Me ajusto a las reglas de firewall dispuestas en su equipo de trabajo dentro de la institución. |
| CLG4 | Me ajusto a los protocolos de seguridad diseñados por la institución para mantener a salvo la información. |
| PAI5 | Uso servicios de alojamiento de información en la nube para guardar información de mi trabajo. |
| PAI6 | Utilizo memorias extraíbles para alojar información de mi trabajo. |
| PPI7 | Descargo aplicaciones y/o programas de en mi equipo de trabajo. |
| PPI8 | Uso equipos fuera de la institución para el envío de documentos o transferencia de información de mi trabajo. |
| CLG9 | Conozco la legislación y/o normativas diseñadas en materia de seguridad de la información. |
| CLG10 | Uso la autenticación como estrategia para proteger la información de mi equipo de trabajo. |
| CLG11 | Actualizo con frecuencia mis claves de acceso en mi equipo de trabajo y correo electrónico. |
| PPI12 | Realizo una copia de seguridad periódica de la información. |
| PRI13 | Pongo en conocimiento de terceros mi dirección de correo electrónico institucional. |

| | |
|---|---|
| PAI14 | Reviso correos electrónicos de remitentes desconocidos. |
| PRI15 | Desde mi equipo de trabajo reviso enlaces recibidos por remitentes desconocidos. |
| PRI16 | Uso contraseñas repetibles o comunes en mi equipo de trabajo. |
| PAI17 | He utilizado servidores externos para enviar información confidencial. |
| PRI18 | Comparto información de acceso con otros usuarios. |
| PRI19 | He olvidado bloquear mi usuario en el equipo cuando me ausento de la oficina. |
| PRI20 | Me he conectado a redes comerciales desde el equipo de trabajo. |
| PPI21 | Utilizo aplicaciones de acceso remoto para trabajar en mi equipo desde otros lugares diferentes a mi oficina. |
| PRI22 | Utilizo las redes sociales en mi equipo de trabajo. |
| PRI23 | Comparto información confidencial de mi trabajo con otros compañeros por medio de redes sociales. |

**Nota.** Elaboración propia.

La estructura de la prueba está terminada en cuatro (4) dimensiones:

- Prácticas de protección de la información a través del uso adecuado de los sistemas y la infraestructura tecnológica. (PPI)
- Conocimiento de la legislación y normativa en materia de ciberseguridad. (CLG)
- Prácticas de alojamiento de la información que puedan afectar potencialmente la seguridad de la información. (PAI)
- Prácticas que pongan en riesgo el acceso a la información. (PRI)

Los ítems correspondientes a cada una de las dimensiones fueron categorizados y denominados con las iniciales de cada una de las dimensiones para facilitar el proceso estadístico y el análisis de resultados, como se presenta en la tabla 6.

**Tabla 5.**

*Ítems por dimensiones.*

| **Prácticas de protección de la información a través del uso adecuado de los sistemas y la infraestructura tecnológica** | |
|---|---|
| PPI1 | Periódicamente realizo actualizaciones a software y sistemas en mi equipo de trabajo dentro de la institución. |
| PPI12 | Realizo una copia de seguridad periódica de la información. |
| PPI2 | Antes de descargar archivos en mi equipo de trabajo realizo un análisis de seguridad independiente del remitente del archivo. |

| | |
|---|---|
| PPI21 | Utilizo aplicaciones de acceso remoto para trabajar en mi equipo desde otros lugares diferentes a mi oficina. |
| PPI7 | Descargo aplicaciones y/o programas de en mi equipo de trabajo. |
| PPI8 | Uso equipos fuera de la institución para el envío de documentos o transferencia de información de mi trabajo. |
| **Conocimiento de la legislación y normativa en materia de ciberseguridad.** | |
| CLG10 | Uso la autenticación como estrategia para proteger la información de mi equipo de trabajo. |
| CLG11 | Actualizo con frecuencia mis claves de acceso en mi equipo de trabajo y correo electrónico. |
| CLG3 | Me ajusto a las reglas de firewall dispuestas en su equipo de trabajo dentro de la institución. |
| CLG4 | Me ajusto a los protocolos de seguridad diseñados por la institución para mantener a salvo la información. |
| CLG9 | Conozco la legislación y/o normativas diseñadas en materia de seguridad de la información. |
| **Prácticas de alojamiento de la información que puedan afectar potencialmente la seguridad de la información.** | |
| PAI14 | Reviso correos electrónicos de remitentes desconocidos. |
| PAI17 | He utilizado servidores externos para enviar información confidencial. |
| PAI5 | Uso servicios de alojamiento de información en la nube para guardar información de mi trabajo. |
| PAI6 | Utilizo memorias extraíbles para alojar información de mi trabajo. |
| **Prácticas que pongan en riesgo el acceso a la información.** | |
| PRI113 | Pongo en conocimiento de terceros mi dirección de correo electrónico institucional. |
| PRI15 | Desde mi equipo de trabajo reviso enlaces recibidos por remitentes desconocidos. |
| PRI16 | Uso contraseñas repetibles o comunes en mi equipo de trabajo. |
| PRI18 | Comparto información de acceso con otros usuarios. |
| PRI19 | He olvidado bloquear mi usuario en el equipo cuando me ausento de la oficina. |
| PRI20 | Me he conectado a redes comerciales desde el equipo de trabajo. |
| PRI22 | Utilizo las redes sociales en mi equipo de trabajo. |
| PRI23 | Comparto información confidencial de mi trabajo con otros compañeros por medio de redes sociales. |

**Nota.** Elaboración propia.

**Pilotaje del instrumento.**

Posterior al proceso de evaluación por parte de los jueces expertos se realizó una prueba piloto al instrumento, aplicándolo a tres personas que trabajan en el contexto militar con la finalidad de identificar si los ítems eran comprensibles para la población. Los participantes del proceso de pilotaje del instrumento no fueron utilizados en el proceso de validación de

instrumento y así lograr cumplir con los fines de la investigación. Los resultados obtenidos en este pilotaje permitieron reconocer el adecuado ajuste de la redacción y la compresión de todos los ítems.

**Procedimiento.**

***Fase 1.*** Se contactaron los participantes del pilotaje por medio de comunicación blackboard, explicando los objetivos de la investigación, y su participación en la prueba piloto del instrumento, permitiendo la participación voluntaria en la investigación.

***Fase 2.*** Se realizó la aplicación de la prueba piloto del instrumento, permitiendo que los participantes de la prueba piloto contestaran cada uno de los reactivos e hicieran los comentarios pertinentes en relación a la compresión y claridad de los mismos.

***Fase 3.*** Se realizó el análisis de los resultados de la prueba piloto encontrando que los participantes reconocían los reactivos como claros, sin encontrar recomendaciones en términos de compresión o redacción.

***Fase 4.*** Finalmente se validaron los ítems en términos de contenido, logrando que los reactivos se ajustaran a los requerimientos en términos de pertinencia, por medio del análisis del coeficiente de razón de valides de constructo y el pilotaje de los reactivos en población con características como las de la muestra, razón que argumento la aplicación del instrumento a una muestra mayor de la población universal en el contexto militar y su posterior validación a través de los procesos estadísticos.

## Capítulo 2. Características psicométricas del instrumento.

### Teorías de los test

La teoría clásica de las pruebas permite asumir que se pueden construir formas paralelas de una prueba, esto hace referencia a la capacidad de medir y evaluar de la misma forma. Se considera que, aunque las formas tengan diferentes preguntas, el hecho de hacer semejantes los índices de dificultad y discriminación de los ítems, garantiza una medición igual con ambas formas (ICFES, 2000), a lo que vamos a llamar confiabilidad.

Es importante resaltar la importancia de la confiabilidad en las pruebas, eso es lo que nos permite generalizar y estandarizar el instrumento de medición, desde el punto de vista de la teoría de generalizabilidad, existe un universo de ítems a partir de los cuales podemos partir usando procedimientos aleatorios y seleccionar diferentes grupos de ellos, lo que le permite al instrumento tener una serie de confiabilidades diferentes, es más, para una misma situación de prueba, los puntajes pueden tener muchos índices de generalizabilidad dependiendo de los factores que afectan el proceso de medición (ICFES, 2000).

De acuerdo con el ICFES (2000) la teoría clásica de los test (TCP) como una forma especial de la teoría de generalizabilidad en la cual se propone que las preguntas de una prueba que no hayan sido seleccionadas desde el universo de ítems, si no, que pretenden ajustarse a él, insiste en la posibilidad de formas paralelas, lo que impide que se acomoden a la noción de un que una prueba tenga más de un índice de generalizabilidad es decir de confiabilidad, por lo tanto se hacen evidentes algunas de las desventajas más centrales de la TCP, la cual se refiere a la estimación del puntaje del universo de preguntas. Se trata de establecer el puntaje del individuo como si este hubiese respondido al universo total de las preguntas, pero como este universo de preguntas es un infinito, se debe estimar un puntaje, lo que asumirá un cierto porcentaje de error.

El desempeño de una persona en una prueba es determinado a partir de la suma del puntaje obtenido de manera individual, es decir, una proporción de respuestas correctas si estas han sido seleccionadas de manera aleatoria del universo, en una estimación insesgada de las preguntas del universo que una persona podría contestar correctamente.

De esta forma es la que se puede conocer de manera objetiva el rendimiento de una persona en una disciplina en particular, medido atraves de un conjunto de ítems obtenido aleatoriamente del universo de preguntas, se esperaría que la persona obtuviera un resultado semejante en cualquiera de estos conjuntos. En este caso hablaríamos de la validez de la prueba, tema que abordaremos más adelante debido a que no es caso del TCT, ya que los ítems se construyen basadas en unos intereses particulares (ICFES, 2000).

De acuerdo con el ICFES (2000) estas mediciones no pueden hacerse sin algún margen de error, ya que estos provienen de diferentes fuentes tales como, las variaciones propias de la aplicación de las pruebas, las diferencias entre las formas de las pruebas, las variaciones de la ejecución de la prueba por parte de los examinados, y otros factores que se desconozcan.

Es necesario citar el ejemplo propuesto por Pardo (2010) para entender los conceptos de "puntaje observado" y "puntaje verdadero"; es decir, supongamos que aplicamos una prueba repetidamente a una misma persona (pensemos que las mediciones son independientes unas de otras y que son idénticas; esto es que la estructura probabilística del experimento no cambia de una aplicación a otra). Podríamos decir que el puntaje de la persona en las diferentes aplicaciones corresponde a su "puntaje observado" mientras que el valor esperado, calculado a partir de estas observaciones lo llamaremos "puntaje verdadero" (ICFES, 2000). El error corresponderá a la diferencia entre el puntaje observado y el puntaje verdadero, así:

$$e_a = x_a - t_a$$

Por otra parte, este error tiene una varianza a la cual se le denota como "Varianza de error examinado a" (ICFES, 2000).

$$S^2\,(E_a)$$

Cuya raíz cuadrada corresponde al "error estándar de la medición para el examinado (ICFES, 2000).

$$S\,(E_a)$$

Que es a su vez una medida de variabilidad de la distribución denotada como:

$$t_a$$

Lo que es un constante denotado así:

$$S(X_a) = S(E_a)$$

Esto permite evidenciar que el error de medición es un índice de la exactitud en la medida, por ello, si el error estándar de la medición tiene una magnitud pequeña significa que el puntaje observado es muy equivalente al puntaje verdadero obtenido, es importante saber que la magnitud está directamente asociada a la escala usada para la medición. De acuerdo con Pardo (2010) la mayoría de las pruebas se enfocan en los resultados de un conjunto de personas y no solo en un resultado individual, dada la población de examinados, cada uno de ellos teniendo un puntaje verdadero, se puede definir una variable $T$ asociada con la distribución de dichos puntajes, asumir una distribución de cierto promedio y una varianza, de esta forma también poder asimilar un puntaje de error ($E$) cuyo promedio será cero (0), y si es cero (o) este puntaje de error en cada persona, se puede inferir que los puntajes observados y los puntajes examinados tendrán una distribución igual en promedio.

Postulando como ecuación básica de la teoría clásica de las pruebas (TCP): el puntaje observado es igual al puntaje verdadero más el puntaje de error (ICFES, 2000).

De lo anterior Pardo (2010) plantea los supuestos básicos de la TCP así:

- El puntaje observado es igual al puntaje verdadero más el puntaje de error: este supuesto permite validar la distribución simétrica de los puntajes obtenidos tras las aplicaciones de los instrumentos.
- El valor esperado del puntaje de error es cero: permite validad la igualdad entre la distribución del promedio del puntaje observado y la distribución del puntaje examinado, siendo ideal que esta relación tenga una diferencia de cero (0).
- La correlación entre los puntajes de error y verdadero es cero: este supuesto soporta la posición del autor al proponer que la diferencia entre el puntaje observado y el puntaje verdadero, esto permitirá demostrar un puntaje de error de cero (0).

- El promedio del puntaje verdadero es igual al promedio del puntaje observado: Se espera que la persona evaluada al ser evaluada con el mismo instrumento de medición en diferentes sesiones obtenga puntajes muy similares, el puntaje verdadero y el puntaje observado tengan una diferencia de cero (0).
- La varianza del puntaje observado es igual a la varianza del puntaje verdadero más la varianza del error: la varianza siendo una medida de dispersión de los datos, permite evidenciar la relación.
- La regresión del puntaje de error en el puntaje verdadero es lineal y con valor constante de cero: este supuesto explica la correlación que mantiene el puntaje de error con el puntaje verdadero, guardando entre si una constante de cero (0).

Todos estos supuestos son de gran relevancia en contextos de una población específica ya que se constituye en un evento condicional, según ICFES (2000).

Ahora abordaremos la medición y evaluación educativa la cual se desarrolla a partir de propuestas de la psicometría, teniendo fundamentos de la teoría general de la medición, en este sentido se puede mencionar como objetivo de la medición, poder medir una variable observada en un sujeto en particular, pero además debe permitir evaluar la validez de la medición. De acuerdo con el ICFES (2000) en el caso de la medición educativa a diferencia de la TCP, no se hace mucho consenso en la definición de las variables más importantes y cuáles de las unidades más convenientes para hacer la medición.

Desde esta perspectiva es mucho más importante tener claridad a la hora de la selección todos los componentes teóricos, conceptúeles y empíricos, la población a la cual se piensa evaluar, y de allí partir para la elaboración de preguntas, formatos y medios de la evaluación. Lo que en este sentido un modelo de medición es una función matemática que relaciona la probabilidad de una respuesta correcta a una pregunta con las características de la persona (habilidad) y las características de la pregunta (dificultad) (Pardo, 2010).

Por tanto, es el modelo de medición debe cumplir con las siguientes condiciones, la persona con habilidad desde una perspectiva psicométrica es aquella que tiene la capacidad de obtener mayor éxito en el ítem, en relación con una persona con habilidad baja. Cualquier persona tiene la capacidad de responder un ítem con menor dificultad que un ítem con dificultad alta.

De acuerdo con Pardo (2010) la consecuencia del cumplimiento de estas condiciones, se evidencia a partir del parámetro habilidad o dificultad, el cual debe ser estimado de manera independiente a los demás parámetros, por lo tanto, es la habilidad de una persona para estimarse independientemente de las preguntas específicas que responda puesto que la habilidad es la misma, esto sin importar si responde a una prueba difícil o fácil.

Estos parámetros antes mencionados permiten formular modelos matemáticos que se puedan usar para una evaluación, y saber que tan apropiada es la observación de la variable cuestionada, durante muchos años la evaluación ha sido abordada desde la perspectiva de la TCT, pero como lo hemos visto una de sus debilidades, es la utilización de índices de los ítems que dependen de un grupo de personas.

Por ello la psicometría ha avanzado hacia un sistema de evaluación mucho más sofisticado, como es el caso de la teoría de respuesta al ítem (TRI), la cual hace dos postulados en primera estancia: (1) la ejecución de una persona en una prueba puede predecirse, explicarse por un conjunto de factores llamados habilidades (ICFES, 2000). Es evidente la importancia que le da esta teoría a las habilidades que tiene cada individuo frente al instrumento de medición, por otra parte (2) la relación entre la ejecución del examinado y las habilidades que la soportan, puede describirse por una función monotónicamente creciente llamada: función característica del ítem o curva característica del ítem (ICC). Esta función hace referencia a que cuando la habilidad de la persona es mayor, la probabilidad de éxito al responder el ítem será equivalentemente mayor.

Desde este punto de vista se pueden hacer evidentes las diferencias entre las dos propuestas (TCT-TRI), ya que el TRI, no hace consideraciones de que pueda justificarse los resultados a partir de los paralelos, entonces de esta manera todos los modelos por mas diversidad tienden a describir por lo menos en un caso el ítem y en otro a la persona.

El modelo de respuesta estocástica de Rasch, describe la probabilidad del éxito de una persona en un ítem como una función de la habilidad de la persona y la dificultad de la pregunta, siendo una aproximación estadística al análisis de las respuestas a una prueba y de otros tipos de observación ordinal (ICFES, 2000). Este análisis propuesto por Rasch, contribuye en gran parte a la medición lineal de las habilidades de la persona y la dificultad de los ítems, y a su vez permite establecer índices de precisión y exactitud de la medición, este modelo mantiene una fuerte

relación con el análisis matemático de los resultados obtenidos en la evaluación, permite por otra parte predecir el comportamiento de la preguntas, pruebas, personas y efectividad.

Establece también la probabilidad de repuesta correcta y poder elaborar la curva característica de la pregunta, y permite establecer la estimación de los parámetros. Por supuesto en el caso del TRI, propone sus supuestos básicos, ya que este validado sobre un modelo matemático, acerca de los datos a los cuales se aplica y especifica las relaciones entre los constructos descritos en el modelo. La dimensionalidad permite asumir a la TRI un conjunto de habilidades que soportan la ejecución del examinado del conjunto de ítems, Las (k) habilidades definen un espacio (k) dimensional, en el cual la localización de cada examinado está determinada por la posición del examinado en cada habilidad (ICFES, 2000).

Por otra parte se postula el supuesto de la independencia local, este supuesto abordado en la evaluación educativa, esperando que el estudiante pueda contestar al ítem sin necesidad de recurrir a información de otros ítems para hacerlo correctamente, en otras palabras el acertar o fallar en una respuesta no debe afectar la capacidad contestar a otro ítem, propone así ves la curva característica del ítem, que había sido ya mencionada, siendo una función matemática que relaciona la probabilidad de éxito en una pregunta con la habilidad medida por el conjunto de ítems que la contienen (Pardo, 2010).

Una vez mencionado todo lo anterior, se hacen invidentes las diferencias, ventajas y desventajas de cada una de las teorías, la TCT, trabaja en función del universo de ítems, haciendo que los resultados obtenidos dependan en gran medida a una forma paralela entre un grupo de personas, mientras la TRI, hace un énfasis muy importante y relevante en las habilidades de la persona frente al ítem y su capacidad de éxito frente a la dificultad de cada constructo. Se puede evidenciar como las dos teorías también hacen uso de modelos matemáticos que permiten validad cada uno de los puntajes obtenidos y asumir una serie de estructuras para la creación, uso y evaluación de instrumentos de medición psicométrica.

Según el ICFES (2000) encontramos un concepto muy importante y relevante para el tema de la medición y la psicometría, la confiabilidad o también llamada fiabilidad hace referencia a la exactitud y precisión que tiene un instrumento de medición psicométrico al ser comparado con otro instrumento que mida los mismos constructos, de este concepto se espera que cuando una

persona sea evaluada por dos pruebas diferentes que midan el mismo constructo obtengan resultados muy similares o iguales.

**Escalas de puntuación.**

La selección de un método de escalamiento se entiende como un proceso por el cual se logran establecer las reglas mediante las cuales se asignarán números a los resultados de la prueba, para esto Gregory (2003) resalta que la construcción de pruebas puede considerarse tanto un arte como una ciencia, ya que aquí se requiere de la creatividad del autor. Gregory (2003) afirma que generalmente el creador de la prueba se vale de estrategias de investigación a la hora de tener una versión preliminar de la prueba, aplicando los reactivos a una muestra de tamaño modesto (en el caso de esta investigación denominado pilotaje), con el objetivo de recolectar una serie de datos y obtener una serie de características iniciales de sus reactivos, a lo que formalmente llamamos análisis de los reactivos. Aquí es el momento en el que se toman decisiones sobre, si los reactivos creados cumplen con su objetivo de medición, o si por algún caso deben modificarse o eliminarse.

Con base a los análisis de reactivos se elaboran hasta tres (3) bosquejos del instrumento de medición entes de su publicación lo que implica que la construcción de pruebas sea un circuito de realimentación que permite hacer las modificaciones necesarias para que el instrumento sea efectivo frente a su objetivo de medición.

Para lograr que todo lo anterior sea posible, es necesario seguir al pie de la letra los pasos postulados por Gregory (2003). Para este trabajo centraremos nuestra atención en la selección del método de escalamiento y profundizaremos en las escalas de puntuación utilizadas para la creación del instrumento objeto de la investigación. Para ello, comenzaremos hablando de selección del método de escalamiento.

De acuerdo con Gregory (2003) el propósito inmediato de un instrumento es poder asignar números a las repuestas en una prueba de modo que el examinador pueda juzgar a partir de estos puntajes a la persona examinada, y así saber si cuenta en mayor o menor proporción con las características de la medida, las reglas con las cuales se asigna el número a la respuesta de una prueba son conocidas como métodos de escalamiento.

Elegir el método que más se adecue en forma óptima a la manera en la que ha conceptuado los rasgos o el rasgo medido por la prueba, con esto no quiere decir que un método es más adecuado o mejor que otro, simplemente, que hay un universo completo de métodos diseñados para suplir las necesidades del examinador, lo que le permitirá elegir el que más se ajuste a su necesidad.

Para poder entender los métodos de escalamiento Gregory (2003) nos recomienda antes entender conceptos básicos y necesarios como lo son los niveles de evaluación. Según Stevens (1946 citado por Gregory, 2003) todos los números extraídos de los instrumentos de medición de cualquier tipo pueden colocarse dentro de una de cuatro categorías jerárquicas, así:

- Nominal.
- Ordinal.
- Intervalo.
- Razón.

Cada una de estas define un nivel de medición. La escala *nominal*, solo permite que los números sirvan como categorías, en las escalas *ordinales*, constituyen una forma de orientación o clasificación, en el caso de *intervalo* esta escala informa acerca de clasificación, pero también provee una medida para estimar las diferencias entre las clasificaciones, en cambio la escala de medida de *razón* tiene todas las características de una escala de intervalo pero posee un punto cero de medida, que es conceptualmente significativo, en la que existiría ausencia total de la característica o el rasgo medido, una vez entendidos los conceptos de los niveles medición podremos entrar en materia de los métodos de escalamiento.

Entre los métodos más representativos de escalamiento en medición encontramos la Escala de Likert, esta escala fue propuesta por Likert en 1932 el cual consiste en asignar de manera sencilla y directa una escala a las actitudes, método que es usado en la actualidad con gran frecuencia, una escala de Likert le presenta a la persona evaluada un listado de cinco opciones de repuesta, ordenadas en un continuo de acuerdo /desacuerdo o en aprobación/desaprobación.

Likert (1932 citado por Gregory, 2003) asigno una puntuación de cinco (5) a esta respuesta extrema uno (1), a la respuesta totalmente opuesta y dos (2), tres (3), y cuatro (4), a las respuestas

intermedias, luego de esta asignación propuso que la puntuación total de la escala se obtiene al sumar las puntuaciones de los reactivos individuales. Por tal razón, la escala de Likert es también conocida como la escala sumatoria. Por otro lado, Aiken (2003) reafirma que este método de escalamiento es el más popular y conocido para la evaluación de actitudes, sin duda alguna se debe a su sencillez y versatilidad.

Otros de los métodos más representativos presentador por Gregory (2003) es la Escala de Guttman, en esta escala las personas que corroboran una afirmación también concuerdan con afirmaciones más leves que tienen que ver con el mismo continuo subyacente Guttman (1944 citado por Gregory, 2003) postula que, cuando el examinado de la persona evaluada es continuo, le es posible reconstruir también la respuesta intermedia, en la escala de Guttman , es muy difícil obtener una escala perfecta que permita llevar una secuencia ordenada de confirmaciones por parte de la persona examinada, esto se debe en gran proporción al error de la medición , aunque es también importante mencionar que la escala de Guttman fue diseñada originalmente para determinar si un conjunto de afirmaciones de actitud es unidimensional, técnica que sea ajusto a muchas necesidades de medición y fue usada por muchos autores de aquel entonces. (Aiken, 2003)

Esta escala según Aiken (2003) aunque un poco menos popular que le modelo de Likert, tiene como objetivo realizar un análisis escalo-gramado, que permite medir si la respuesta frente a un reactivo por parte del examinado afirma aceptar en cierta medida las demás opciones de respuesta de menor valor, ejemplificado como lo menciona Aiken (2003) en la mayoría de pruebas cognoscitivas que presentan esta situación.

Un ejemplo similar a los reactivos usados por la esta escala, podría ser muy secano a "marque en cada grupo las afirmaciones que, a su parecer, lo representan de manera más cercana" (Gregory, 2003, pág. 150), se pide a la persona examinada que marque la opción que más se ajusta, si en algún caso la persona examinada marca una alternativa extrema, casi con toda seguridad coincidiría también con las afirmaciones más leves. Algunos de las posibles opciones de respuesta podrían ser: "en ocasiones me siento triste o afligido", "Con frecuencia me siento triste o afligido", "Me siento triste o afligido en la mayor parte del tiempo", "siempre me siento triste y no puedo tolerarlo" por citar un ejemplo.

En este orden de ideas podríamos hacer un paralelo entre las dos escalas antes mencionadas, por un lado, la escala de Likert permite medir las actitudes de la persona evaluada frente a un reactivo usando un listado de opciones que consta de 5 respuestas, en cambio la escala de Guttman usa un listado similar de opciones de repuesta, pero mide una afirmación de la persona frente al reactivo.

Dentro del proceso de construcción de pruebas encontramos otras escalas de medición que permiten al examinador obtener uno estadísticos y a partir de ellos realizar una interpretación. De acuerdo con Gregory (2003) uno de los estadísticos más conocidos es el percentil, este tipo de escala expresa el porcentaje de personas de la muestra de estandarización que obtuvieron puntuación por debajo de una puntuación natural específica. Es decir, si en un caso extremo el individuo examinado obtiene una puntuación natural que exceda todas las puntuaciones en la muestra de estandarización recibirá un percentil de 100.

Este tipo de estadístico es muy conocido ya que su cálculo es muy sencillo e intuitivamente atractivo para los profesionales de la ciencia, por ende, es muy común que este estadístico sea el más usado para la trasformación de puntuaciones, pero no por ello se deben obviar otros modelos de trasformación que permiten un análisis más profundo una serie de propiedades mucho más efectivas para la interpretación por parte de examinador.

Este proceso de transformación llevado a cabo por el examinador es conocido como la estandarización, procesos que son llevados a cabo en su mayoría con distribuciones normales de los estadísticos, este tipo de distribución más conocida como distribución con propiedades de curva normal o simétricas, una vez los datos siguen este tipo de distribución es mucho más sencillo hacer comparaciones directas y análisis estadísticos, por fortuna la estadística ofrece herramientas que permiten que las puntuaciones con distribuciones asimétricas sean encajadas dentro de la curva normal. Así su comparación es mucho más directa, este proceso es conocido como conversión de los percentiles a puntuaciones estándar normalizadas.

Según Gregory (2003) la obtención de las puntuaciones estándar normalizadas se logra a partir del cálculo inverso, es decir se toman los percentiles obtenidos de la puntuación natural, y se determina su puntuación estándar correspondiente, si este proceso se lleva a cabo con la

totalidad de las puntuaciones obtenidas, la distribución de las puntuaciones estará normalizada y encaja dentro de la curva normal.

Gregory (2003) propone que aunque, los percentiles son el tipo más popular de puntuación transformada, las puntuaciones estándar aportan las propiedades psicométricas más deseadas por el evaluador, el cálculo de la puntuación estándar de un individuo es también conocido como puntuación Z, esta puntuación se halla a partir de la resta de la puntuación normal de la persona examinada a la media del grupo normativo, y después se divide entre la desviación estándar del grupo normativo, este tipo de puntuación posee propiedades psicométricas deseables que mantienen magnitudes relativas de distancia entre los valores sucesivos, encontrados a partir de las puntuaciones naturales.

Por último, Gregory (2003), nos presenta una breve mención de tres transformaciones de puntuaciones naturales que tienen un interés netamente histórico, estas transformaciones son conocidas como escala de estaninas, escala que fue desarrollada en la segunda guerra mundial en los E.U, esta escala permite convertir las puntuaciones naturales en un sistema de puntuaciones de un solo digito que va de 1 a 9, donde 5 es la media de la puntuación estándar y la desviación estándar será de 2. Esta transformación de puntuaciones naturales a estaninas es simple ya que se obtiene a partir de la clasificación de menor a mayor donde por ejemplo si el puntaje obtenido es menor al 4% entonces esta será la estanina 1, si el segundo es del 7% entonces esta será la estanina 2, y así sucesivamente.

Según (Gregory, 2003), la principal ventaja que ofrece este método es que se reduce a la cualidad de un solo digito, aporte que en la segunda guerra mundial era de gran utilidad.

Diferentes autores como Canfield (1951 citado por Gregory, 2003) propuso en su momento una estaca de estaninas de 10 unidades con una media de 5, lo que indicaba que 5 por debajo y 5 por encima de la media, esta escala fue conocida como estanes, por otra parte Guilford y Fruchter (1978) propusieron una escala de 11 unidades conocida como la escala C, pero en realidad este tipo de escalas como lo propuso (Gregory, 2003), solo tienen un impacto histórico debido a que por su ambigüedad no son muy atractivas para los creadores de pruebas.

Otras puntuaciones o transformaciones utilizadas por los examinadores es la propuesta por Aiken (2003) utilizada con frecuencia para medir el CI de desviación, este coeficiente que se obtiene al convertir las puntuaciones naturales en una prueba de inteligencia a una distribución de calificaciones que tienen una medida de 100 y una desviación estándar fija. Aiken (2003) propone unos ejemplos de uso de este coeficiente en la prueba de inteligencia de Stanford-Binet la cual cuenta con una desviación fija de 16; entre otros métodos de puntuación podremos encontrar la transformación de puntuaciones naturales a partir de modelos como el propuesto por la calificación CEEB (Aiken, 2003). Este tipo de calificaciones fueron usadas en principio sobre pruebas publicadas en el Consejo de evaluación de ingreso a la universidad, en donde se determinaba esta calificación tomando como referencia las calificaciones o puntajes Z, y multiplicándolos por 100, después de este producto se sumaban 500, lo que en su momento aplicado a una prueba conocida como SAT (1941), produjo una media de 500 y una desviación estándar de 100, sin embargo Aiken (2003), menciona que posteriormente estas calificaciones obtenidas por los estudiantes de SAT no fueron transformadas de bajo este modelo si no que se buscó garantizar que la unidad de medida de las calificaciones fuera comparada un año vs., el otro año directamente.

Por otra parte, encontramos los baremos, esta herramienta es muy importante y aporta información de gran utilidad al intérprete del instrumento, los baremos estadísticos permiten que las puntuaciones estandarizadas sean clasificadas por grupos que representan una característica psicométrica en común, permitiendo que la estandarización de los puntajes sea eficaz a la hora de analizar los puntajes obtenidos por la persona examinada.

Todo lo anterior hace es de vital importancia para la construcción de la prueba ya que aporta un sin número de herramientas que deben ser usadas por el creador del instrumento para asegurar que los reactivos, las dimensiones y todo el constructo en general cumple el objetivo de medición de la variable que se propuso medir.

## Capítulo 3. Análisis técnico del instrumento.

### Análisis factorial.

Según Burga (2005) fundamentalmente lo que busca el análisis factorial es simplificar la información que nos da la matriz de correlación, para que esta sea más fácil de interpretar, y así poder dar respuesta a un interrogante muy importante, de por qué unas variables se relación más entre sí misma que con otras. La respuesta hipotética es porque existen otras variables, otras dimensiones o factores que explican por qué unos ítems se relacionan más con unos que con otros (Burga, 2005).

De acuerdo con Meneses (2012) los valores obtenidos a partir de KMO, permiten indicar si, las correlaciones parciales entre las variables analizadas son suficientemente pequeñas, lo que se logra contrastando la magnitud de los coeficientes de correlación obtenidos con la magnitud de los coeficientes de correlación parcial, entonces si la correlación de las variables es pequeña el uso del análisis factorial será pertinente.

De acuerdo con lo anterior Meneses (2012) propone que este estadístico puede presentar valores entre .00 y 1.0; algunos autores indican que el valor esperado debe ser mínimo de .60; otros indican que podría ser de .5; Desde la perspectiva de un valor mínimo de .60 se entiende que todo valor obtenido en KMO, que sea < .60 indicará que el análisis factorial (AF) no es recomendado, por el contrario si el valor obtenido esta entre un rango de .60 & .749 entonces las puntuaciones analizadas cumplen con un criterio aceptable para realizar el AF, aquellos valores que sean ≥ .75 señalan que las puntuaciones analizadas cumplen con una satisfacción para realizar el AF, si es .80 Excelente.

**Tabla 6.**
*KMO and Bartlett's Test*

| | | |
|---|---|---|
| Kaiser-Meyer-Olkin Measure of Sampling Adequacy. | | ,444 |
| Bartlett's Test of Sphericity | Approx. Chi-Square | 821,455 |
| | df | 253 |
| | Sig. | ,000 |

Teniendo en cuenta los criterios de análisis propuestos por Meneses (2012) los resultados obtenidos en la prueba KMO para el caso de la escala de comportamientos que pueden interferir

potencialmente en la seguridad cibernética en el contexto militar, muestran que los estadísticos obtenidos en KMO, expuestos en la tabla 6., reflejan una Medida de adecuación muestral de KMO, de .444 lo que permite plantear la no pertinencia de un análisis factorial. La prueba de esfericidad de Bartlett señala un valor de Chi-cuadrado aproximado de 821.455; que para 250 grados de libertad (Gl), tiene un nivel de una significancia de $P < .000$; lo que indica que los puntajes analizados no son adecuados para el Análisis Factorial.

Razón por la cual se toma la decisión de realizar el análisis de unidimencionalidad de Rasch. Según Haties (1985, citado por Burga, 2005), la unidimencionalidad implica que un solo rasgo latente o constructo se encuentre en la base de un conjunto de ítems.

Un instrumento será unidimensional si las respuestas dadas a él son originadas en base a un único atributo. Para Wright y Linacre (1998, Citado por Burga, 2005), afirman que, en la práctica, ningún instrumento puede ser perfectamente unidimensional, lo que se pretende es tener instrumentos que, en esencia evidencien unidimencionalidad. Según Hamebleto (1991, citado por Burga, 2005) un ejemplo puede ser que en muchos factores tales como la ansiedad, motivación, y la velocidad de respuesta tienen un impacto sobre el desempeño de una persona en un conjunto de ítems. Lo fundamental es que un instrumento de medida represente con sus puntuaciones un solo factor dominante.

Según Embretson y Rerise (2000, citado por Burga, 2005), lo que se quiere lograr es que la mayor cantidad de la varianza observada es las respuestas a los ítems sea explicada por un solo atributo latente. De esta forma no es la única manera que se puede entender la unidimencionalidad, por otra parte, según Bejar (1993, citado por Burga, 2005), afirma que la unidimencionalidad no implica necesariamente que las respuestas a un conjunto de ítems se deban a un único proceso psicológico. Bejar (1993, citado por Burga, 2005), pensaba que podía haber un amplio conjunto de procesos psicológicos producidos en dichas respuestas, pero en la medida que los mismos procesos afecten de la misma forma las respuestas a un conjunto de ítems, se podrá sostener que se presenta una unidimencionalidad esencial en dicho instrumento de medida.

Para Wright y Masters (1982; y Stone 1998, citado por Burga, 2005), es importante tener un instrumento unidimensional, debido a que para muchos esto será un requisito indispensable para generar buenas mediadas.

En la teoría clásica de los test TCT, las puntuaciones obtenidas de la aplicación de un instrumento psicométrico siguen un modelo monotónico lineal, es decir, se asume que existe una relación lineal entre el puntaje directo obtenido y el nivel del rasgo o atributo que posee la persona evaluada. Los puntajes directos o puntajes globales provienen de la suma de los puntajes obtenidos en cada uno de los ítems. Según Cuesta (1996, citado por Burga, 2005), el obtener los puntajes globales sumados las calificaciones de cada ítem, presume que se está midiendo con ellos un solo constructo; de lo contrario no habría ningún fundamento que soporte las operaciones realizadas con los ítems.

De la misma manera Stout (1987, citado por Burga, 2005), postulo que, si se pretende medir un nivel en una variable, esta no debe estar continuada por los niveles que posee la persona en otras variables. De esta forma, evaluar la unidimencionalidad es una obligación ya que es muy importante en el desarrollo de un instrumento de medición. Burga (2005) postula que, no existe una única línea metodológica para evaluar la unidimencionalidad, se presentara los aportes del análisis factorial como herramienta para evaluar. Ya que estas herramientas son de suma importancia al momento de estudiar la unidimencionalidad de un conjunto de ítems.

**Figura 1.** *Estandarized residual*

```
TABLE 23.0 BASE DE DATOS ANALISIS INSTRUMENTO.xl ZOU404WS.TXT  Apr 21 2019 17:45
INPUT: 75 PERSON  23 ITEM  REPORTED: 75 PERSON  23 ITEM  2 CATS   MINISTEP 4.4.1
-------------------------------------------------------------------------------

     Table of STANDARDIZED RESIDUAL variance in Eigenvalue units = ITEM information units
                                      Eigenvalue   Observed   Expected
Total raw variance in observations     =     39.6846 100.0%        100.0%
  Raw variance explained by measures   =     16.6846  42.0%         41.0%
    Raw variance explained by persons  =      4.1400  10.4%         10.2%
    Raw Variance explained by items    =     12.5446  31.6%         30.9%
  Raw unexplained variance (total)     =     23.0000  58.0% 100.0%   59.0%
    Unexplned variance in 1st contrast =      3.6928   9.3%  16.1%
    Unexplned variance in 2nd contrast =      2.0243   5.1%   8.8%
    Unexplned variance in 3rd contrast =      1.8361   4.6%   8.0%
    Unexplned variance in 4th contrast =      1.6547   4.2%   7.2%
    Unexplned variance in 5th contrast =      1.5804   4.0%   6.9%
```

**Figura 1.** Estandarized residual, resultado proceso estadístico software Winsteps.

Para identificar si este criterio se cumple, se utiliza la herramienta Winsteps y allí se logra calcular la figura 1; en las cuales encontramos los estadísticos, obtenidos a partir del análisis de 23 variables y 75 sujetos, posibles procesados por la versión de Ministps, una varianza explicada

por la media de 39.68 % (Véase tabla 23.0), este valor obtenido es >.4 para los 23 ítems (Meneses, 2013) sugiere que en este orden de ideas la prueba mide un solo constructo según los criterios de (Crocker &Algina, 1986; Linacre, 2006; Wilson, 2005).

En el caso de la varianza no explicada tiene un valor de 9.3% (Véase figura 1), lo que nos permite inferir nuevamente que la prueba mide un solo constructo ya que no es mayor al 15% según los criterios de (Crocker &Algina, 1986; Linacre, 2006; Wilson, 2005, citado por, Meneses, 2013).

Véase también en la figura 1; que El número de eigenvalues para la varianza residual del primer contraste fue 3.6928, y la razón obtenida por del porcentaje total de la varianza no explicada es de 9.3%, como cumple los anteriores criterios postulados por (Crocker &Algina, 1986; Linacre, 2006; Wilson, 2005, citado por, Meneses, 2013), de un valor máximo de 2, y Reckase (1979) en valor máximo de 3, se concluye que el cuestionario ESCOM-23 es unidimensional.

**Análisis técnico del instrumento.**

En el presente apartado se presentan los resultados del estudio en tres partes: 1. Un análisis descriptivo de las variables sociales y demográficas, 2. El análisis técnico del instrumento y, 3. El análisis de los datos obtenido a través de la aplicación de la prueba ESCOM-23, con 1 para respuestas verdadero y 0 para respuestas falso y analizadas a través del software Winstep 4.01, mediante el Modelo de Rasch (1980; Pardo, 2015).

Según Badenes (2007) el modelo de Rasch ha sido utilizado a través de los años para medir un fenómeno latente, no observable directamente, lo que se logra a partir de una serie de puntuaciones obtenidas de distintos ítems por diferentes individuos. Este modelo fue aplicado por primera vez con el objetivo de medir la inteligencia de los soldados Daneses y ha sido utilizado de manera muy extensa en la psicometría, para medir la inteligencia, las capacidades y los rasgos personales no observables directamente, lo que se denomina una variable latente, en donde a partir de las respuestas de los individuos ante distintas preguntas de un test (ítems).

Este modelo ha sido utilizado en distintos modelos para medir resultados educativos y otros fenómenos del ámbito económico, también, ha sido usado para medir la calidad de servicio ofrecido por las entidades de educación superior, entre otro tipo de medidas, como es el caso de

los conocimientos, las actitudes y los comportamientos. El modelo de Rasch es un modelo en el sentido literal de la palabra, ya que representa el ideal con el que se debería contar para medir los rasgos y características del fenómeno que se pretende caracterizar.

La figura 2 muestra la información básica de los 106 participantes en el estudio. En la columna de los puntajes (RAW SCORE) se muestra la media de 10.0 y S.D 2.9 un puntaje máximo de 16 puntos y un mínimo de 5 puntos. En la columna de las medidas (MEASURE) notamos que los máximos y mínimos fueron estimados en 1.34 y -1.97 logits respectivamente, con una media de -.33 logits y una S.D .83 logits.

En la columna de ajuste interno (INFIT) reporta valores para el MNSQ entre 0.37 y 2.86 con una media de 0.98 lo que indica que existe un buen ajuste interno al modelo, sin embargo, el puntaje máximo 2.86 representa cierto ruido que debe analizarse. En el caso del ajuste externo (OUTFIT) los valores del MNSQ se encuentran comprendidos entre 0.25 y 5.52 con una media de 1.08 lo que indica que de acuerdo con la media en general existe un buen ajuste al modelo, sin embargo, el valor máximo de 5.52 indica que existe un ruido que es sensible de análisis, al igual que en el caso del ajuste interno (INFIT).

**Figura 2.** Summary of 75 measured person.

TABLE 3.1 BASE DE DATOS ANALISIS INSTRUMENTO.xls ZOU978WS.TXT Apr 21 2019 18:11
INPUT: 75 PERSON 23 ITEM REPORTED: 75 PERSON 23 ITEM 2 CATS MINISTEP 4.4.1

SUMMARY OF 75 MEASURED PERSON

| | TOTAL SCORE | COUNT | MEASURE | MODEL S.E. | INFIT MNSQ | INFIT ZSTD | OUTFIT MNSQ | OUTFIT ZSTD |
|---|---|---|---|---|---|---|---|---|
| MEAN | 10.0 | 23.0 | -.33 | .55 | .98 | -.18 | 1.08 | .00 |
| SEM | .3 | .0 | .10 | .00 | .05 | .18 | .12 | .15 |
| P.SD | 2.8 | .0 | .83 | .03 | .46 | 1.59 | 1.01 | 1.28 |
| S.SD | 2.9 | .0 | .83 | .03 | .47 | 1.60 | 1.02 | 1.29 |
| MAX. | 16.0 | 23.0 | 1.34 | .64 | 2.86 | 4.90 | 5.52 | 4.78 |
| MIN. | 5.0 | 23.0 | -1.97 | .52 | .37 | -2.41 | .25 | -1.66 |

| | | | | | |
|---|---|---|---|---|---|
| REAL RMSE | .59 | TRUE SD | .58 | SEPARATION .97 | PERSON RELIABILITY .48 |
| MODEL RMSE | .55 | TRUE SD | .62 | SEPARATION 1.12 | PERSON RELIABILITY .56 |
| S.E. OF PERSON MEAN = .10 | | | | | |

**Figura 1.** Summary of 75 measured person, resultado proceso estadístico software Winsteps.

En la figura 3 se muestra la información básica de los 23 ítems del instrumento. La columna (RAW SCORE) muestra el número de respuestas correctas de los reactivos. La media fue de 32.7 con una S.D de 22.1. El valor máximo fue de 71 y el mínimo de 3 respuestas. En la columna de las medidas notamos que los máximos y mínimos fueron estimados 3.16 y -3.48 logits respectivamente, con una media de 0.00 logits y una S.D. 1.79 logits.

En la columna de ajuste interno (INFIT) los valores del MNSQ se encuentran comprendidos entre .81 y 1.23 con una media de .99. Para el caso del ajuste externo (OUTFIT) los valores del MNSQ se encuentran comprendidos entre 0.52 y 2.27 con una media de 1.08 lo que indica que existe un buen ajuste interno al modelo en el caso de los ítems, del mismo modo que en ajuste externo, sin embargo, el puntaje máximo 2.27 del ajuste externo (OUTFIT) representa un ruido que debe ser analizado.

**Figura 3.** Summary of 75 measured ítem.

SUMMARY OF 23 MEASURED ITEM

| | TOTAL SCORE | COUNT | MEASURE | MODEL S.E. | INFIT MNSQ | INFIT ZSTD | OUTFIT MNSQ | OUTFIT ZSTD |
|---|---|---|---|---|---|---|---|---|
| MEAN | 32.7 | 75.0 | .00 | .33 | .99 | -.09 | 1.08 | .13 |
| SEM | 4.6 | .0 | .37 | .02 | .02 | .18 | .08 | .23 |
| P.SD | 21.6 | .0 | 1.75 | .09 | .10 | .83 | .36 | 1.09 |
| S.SD | 22.1 | .0 | 1.79 | .09 | .10 | .85 | .36 | 1.12 |
| MAX. | 71.0 | 75.0 | 3.16 | .60 | 1.23 | 1.77 | 2.27 | 2.78 |
| MIN. | 3.0 | 75.0 | -3.48 | .25 | .81 | -2.11 | .52 | -1.97 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| REAL RMSE | .35 | TRUE SD | 1.72 | SEPARATION | 4.97 | ITEM | RELIABILITY | .96 |
| MODEL RMSE | .34 | TRUE SD | 1.72 | SEPARATION | 5.05 | ITEM | RELIABILITY | .96 |
| S.E. OF ITEM MEAN = .37 | | | | | | | | |

ITEM RAW SCORE-TO-MEASURE CORRELATION = -.99
Global statistics: please see Table 44.
UMEAN=.0000 USCALE=1.0000

**Figura 3.** Summary of 75 measured item, resultado proceso estadístico software Winsteps.

De acuerdo con Pardo (2010) algunas de las ventajas del modelo de Rasch es que permite analizar el ajuste delos ítems al modelo e identificar el índice de dificultad de cada uno de los ítems, de acuerdo con el modelo la aceptación de ajuste se encuentra entre 0.5 y 1.5, sin embargo, aquellos ítems que no superen 2.0 no introducen ruido que modifique de manera significativa la medida. En la figura 4., se presentan los ítems y el ajuste de los ítems al modelo.

**Figura 4.** Item estadistic entery order.

TABLE 14.1 BASE DE DATOS ANALISIS INSTRUMENTO.xl ZOU978WS.TXT Apr 21 2019 18:11
INPUT: 75 PERSON 23 ITEM REPORTED: 75 PERSON 23 ITEM 2 CATS MINISTEP 4.4.1

PERSON: REAL SEP.: .97 REL.: .48 ... ITEM: REAL SEP.: 4.97 REL.: .96

ITEM STATISTICS: ENTRY ORDER

| ENTRY NUMBER | TOTAL SCORE | TOTAL COUNT | MEASURE | MODEL S.E. | INFIT MNSQ | INFIT ZSTD | OUTFIT MNSQ | OUTFIT ZSTD | PTMEASUR-AL CORR. | PTMEASUR-AL EXP. | EXACT MATCH OBS% | EXACT MATCH EXP% | ITEM |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 42 | 75 | -.62 | .25 | 1.00 | .01 | 1.09 | .80 | .34 | .36 | 66.7 | 66.1 | PPI1 |
| 2 | 57 | 75 | -1.65 | .28 | 1.11 | .78 | 1.15 | .74 | .18 | .30 | 77.3 | 76.2 | PPI2 |
| 3 | 71 | 75 | -3.48 | .52 | 1.07 | .30 | 2.27 | 1.68 | -.08 | .16 | 94.7 | 94.6 | CLG3 |
| 4 | 70 | 75 | -3.23 | .47 | 1.07 | .30 | 1.49 | .94 | .02 | .17 | 93.3 | 93.3 | CLG4 |
| 5 | 23 | 75 | .60 | .27 | .84 | -1.40 | .80 | -1.24 | .54 | .35 | 76.0 | 72.6 | PAI5 |
| 6 | 37 | 75 | -.31 | .25 | .86 | -1.72 | .84 | -1.60 | .53 | .37 | 78.7 | 65.9 | PAI6 |
| 7 | 19 | 75 | .90 | .28 | .93 | -.45 | .89 | -.50 | .42 | .34 | 77.3 | 76.2 | PPI7 |
| 8 | 30 | 75 | .13 | .25 | .81 | -2.11 | .78 | -1.97 | .58 | .37 | 76.0 | 67.7 | PPI8 |
| 9 | 55 | 75 | -1.49 | .28 | 1.23 | 1.77 | 1.64 | 2.78 | -.03 | .31 | 72.0 | 74.0 | CLG9 |
| 10 | 68 | 75 | -2.85 | .41 | 1.01 | .14 | 1.04 | .24 | .18 | .20 | 90.7 | 90.6 | CLG10 |
| 11 | 58 | 75 | -1.73 | .29 | 1.07 | .55 | 1.32 | 1.33 | .17 | .30 | 76.0 | 77.4 | CLG11 |
| 12 | 56 | 75 | -1.57 | .28 | .90 | -.75 | .86 | -.66 | .43 | .31 | 78.7 | 74.9 | PPI12 |
| 13 | 25 | 75 | .46 | .26 | 1.07 | .65 | 1.12 | .82 | .27 | .36 | 69.3 | 70.9 | PRI13 |
| 14 | 8 | 75 | 2.06 | .39 | 1.00 | .07 | 1.05 | .25 | .24 | .25 | 89.3 | 89.3 | PAI14 |
| 15 | 15 | 75 | 1.25 | .31 | .97 | -.11 | .93 | -.21 | .35 | .32 | 82.7 | 80.2 | PRI15 |
| 16 | 13 | 75 | 1.44 | .32 | 1.09 | .51 | 1.43 | 1.41 | .14 | .30 | 82.7 | 82.6 | PRI16 |
| 17 | 9 | 75 | 1.91 | .37 | .99 | .04 | .87 | -.24 | .29 | .26 | 88.0 | 88.0 | PAI17 |
| 18 | 9 | 75 | 1.91 | .37 | .93 | -.22 | 1.19 | .59 | .30 | .26 | 88.0 | 88.0 | PRI18 |
| 19 | 18 | 75 | .99 | .29 | 1.07 | .49 | 1.00 | .07 | .28 | .33 | 73.3 | 77.1 | PRI19 |
| 20 | 23 | 75 | .60 | .27 | .99 | -.06 | .96 | -.17 | .37 | .35 | 70.7 | 72.6 | PRI20 |
| 21 | 24 | 75 | .53 | .27 | .98 | -.16 | .89 | -.66 | .41 | .36 | 68.0 | 71.6 | PPI21 |
| 22 | 18 | 75 | .99 | .29 | .88 | -.81 | .81 | -.88 | .47 | .33 | 81.3 | 77.1 | PRI22 |
| 23 | 3 | 75 | 3.16 | .60 | .92 | .01 | .52 | -.52 | .30 | .16 | 96.0 | 96.0 | PRI23 |
| MEAN | 32.7 | 75.0 | .00 | .33 | .99 | -.1 | 1.08 | .1 | | | 80.3 | 79.3 | |
| P.SD | 21.6 | .0 | 1.75 | .09 | .10 | .8 | .36 | 1.1 | | | 8.6 | 9.1 | |

**Figura 4.** Item estadistic entery order, resultado proceso estadístico software Winsteps.

De acuerdo con lo anterior, el ítem PPI1 con un MEASURE de -.62 un INFIT (ajuste interno) 1.00 y un OUTFIT (ajuste externo) 1.09 introduce ruido a la medida de la prueba, razón que hace relevante su revisión y análisis. Del mismo modo el ítem PPI2 MEASURE de -1.65., un INFIT (ajuste interno) 1.11 y un OUTFIT (ajuste externo) 1.15 representan un ruido en la medida. En el caso del ítem CLG3 y CLG4 con un MEASURE de -3.48 y -3.23 un INFIT (ajuste interno) 1.07 y 1.07, con un OUTFIT (ajuste externo) 2.27 y 1.49 respectivamente representa un desajuste al modelo, razón que indica una revisión de los reactivos y si es el caso la eliminación de los mismos.

Otros reactivos que introducen ruido son los ítems CLG9, CLG10 y CLG11lo que indica que la medida de la dimensión Conocimiento de la legislación y normativa en materia de ciberseguridad, introduce en general una medida de ruido al análisis de la prueba desde el modelo de ajuste interno y externo planteado por Rasch y basado en los criterios de Pardo (2010), razón que demanda una revisión detallada del reactivo y la relación existente con los examinados (personas). Teniendo en cuenta que esta dimensión representa una medida de conocimiento, es necesario identificar el índice de dificultad de los ítems y la capacidad de respuesta de los examinados en relación a la prueba. Es decir, que es probable que el desajuste de los reactivos con el modelo estadístico represente que los examinados (personas) no cuentan con la habilidad o conocimiento en relación a cada uno de los reactivos.

Partiendo del principio planteado por Pardo (2010) las ventajas del modelo de Rasch es que permite analizar el ajuste de los ítems al modelo e identificar el índice de dificultad de cada uno de los ítems, esto a través de la comparación de las personas y los ítems, teniendo en cuenta que juntas variables son medidas en las mismas unidades de análisis (logits).

En la figura 5 se muestra el mapa de personas-ítems medidos en las mismas unidades de análisis, lo que permite determinar el índice de dificultad de los ítems y la habilidad de las personas para responder los ítems, como se puede observar en esta tabla en los polos altos se identifican los ítems y las personas que cuentan con la habilidad para responder esos ítems con un alto índice de dificultad, en el polo bajo, por el contrario se encuentran los reactivos con un bajo índice de dificultad y las personas que logran contestar dichos ítems.

Sin embargo, otra de las propiedades que nos permite identificar este modelo estadístico es la agrupación de los reactivos y las personas de acuerdo al índice de dificultad y la habilidad de las

personas. Esta representación gráfica permite identificar, como las personas no logran contestar los ítems de la dimensión de conocimiento, y a su vez el modelo estadístico nos muestra que dicha respuesta no estuvo determinada por la complejidad de los ítems, sino por la ausencia de la habilidad de las personas.

**Figura 5.** Measure person-map-item

```
TABLE 12.2 BASE DE DATOS ANALISIS INSTRUMENTO.xl ZOUS78WS.TXT  Apr 21 2019 18:11
INPUT: 75 PERSON  23 ITEM  REPORTED: 75 PERSON  23 ITEM  2 CATS   MINISTEP 4.4.1
-----------------------------------------------------------------------------

MEASURE   PERSON - MAP - ITEM
            <more>|<rare>
     4            +
                  |
                  |
                  |T
                  |
                  |
                  |  PRI23
     3            +
                  |
                  |
                  |
                  |
                  |
                  |
     2            +  PAI14
                  |  PAI17  PRI18
                  |S
                  |
                  |  PRI16
              XXXX T|  PRI15
                  |
     1         XXXX  +  PRI19  PRI22
                 X  |  PPI7
                  |
              XXXXX  |  PAI5   PPI21  PRI20
                   S|  PRI13
          XXXXXXXX  |
                  |  PPI8
     0   XXXXXXXXXX  +M
                  |
            XXXXXX M|  PAI6
                  |
          XXXXXXXX  |  PPI1
                  |
    XXXXXXXXXXXX  |
    -1            +
                 S|
        XXXXXXXXX  |
                  |  CLG9
             XXXXX  |  PPI12
                  |S CLG11  PPI2
                  |
    -2          X T+
                  |
                  |
                  |
                  |
                  |
                  |  CLG10
    -3            +
                  |
                  |  CLG4
                  |  CLG3
                  |T
                  |
                  |
    -4            +
              <less>|<freq>
```

## Conclusiones.

El desarrollo de este trabajo de investigación, permitió la construcción de una escala de evaluación de comportamientos que pueden interferir en el mantenimiento de la seguridad en el ciberespacio con un énfasis en el contexto militar colombiano. Dicho recorrido permitió el establecimiento de unidades de análisis que describen los posibles comportamientos relacionados con la problemática de investigación, y la caracterización del estado del arte del estudio de la ciberseguridad desde una perspectiva del talento humano. El desarrollo del estado del arte permitió identificar varias consideraciones que son sensibles de análisis al momento de establecer las conclusiones pertinentes de este trabajo de investigación, en principio reconocer que existe poca evidencia científica en materia de ciberseguridad desde un perspectiva de investigación empírica que tenga como objetivo establecer casualidades entre una y otra variable, por el contrario existe material actualizado suficiente que describe y sustenta la conceptualización del constructo y las variables relacionadas con el mantenimiento de la seguridad tanto desde la perspectiva legal como desde la perspectiva teórica.

De otro lado, los estudios que se han realizado en la materia de comportamiento y su relación con las problemáticas que se presentan en el contexto de la ciber seguridad, son escasos, sobre todo en países latinoamericanos. Situación similar ocurre en el contexto militar en donde se encuentra poca evidencia científica. Ahora bien, se ha investigado en el marco legal la tipificación de las conductas relacionadas con los delitos informáticos. Sin embargo, en el campo de la ciberseguridad exista una ausencia representativa de información que permita comprender la forma en que se han observado los comportamientos del hombre en el uso de las herramientas tecnológicas y el impacto negativo que puede tener el uso indebido de las mismas, más allá del concepto de hacker.

En el desarrollo de este trabajo de investigación, se realizó un recorrido por diferentes perspectivas teóricas que pudiesen explicar con amplitud el impacto del comportamiento humano en diferentes contextos y la forma en que este puede ser interpretado y descrito, teniendo en cuenta que este tipo de constructos de estudio se ha investigado más desde las ciencias que estudian el comportamiento, fue necesario contar con el acompañamiento por parte de uno de los jueces expertos en materia de conducta, y hacer una revisión mucho más profunda en el tema del estudio del comportamiento, encontrando que una de las mejores perspectivas ofrecidas para su

compresión es la psicología del comportamiento social. Que ha sido estudiada desde diferentes perspectivas y disciplinas. Si bien la principal disciplina científica ocupada del estudio del comportamiento ha sido la psicología, otras disciplinas como es el caso de la administración de personas y las ingenierías en las que se trabaja con el talento humano, no es ajeno al interés de la investigación reconocer constructos desde su perspectiva teórica y comprender la forma en que estos funcionan, así como lograr a través de un proceso de investigación rigurosos la consecución de herramientas que midan este tipo de variables.

Una de las principales conclusiones que se desprenden de la revisión documental realizada para la construcción de dicho marco de referencia teórica, es que la principal teoría que permite una comprensión mucho más amplia y consecuente con los interés planteados para la investigación desarrollada es la propuesta por las teorías sociales del comportamiento, en donde se describe como un comportamiento individual es adoptado por el individuo en un grupo social determinado y cuando un comportamiento es categorizado como un comportamiento potencialmente dañino, situación que se asemeja a la problemática planteada para esta investigación que describe que como en el contexto militar se asumen comportamientos de manera individual que van en contra de los socialmente establecidos por dicho grupo social.

Desde esta óptica, el interés de esta investigación permitió seleccionar este marco de referencia teórica ya que describía con suficiencia el constructo, y a partir de él lograr la consecución de los ítems que permitieron el desarrollo de la escala. Dicho proceso de construcción del instrumento, se adelantó partiendo de la experiencia del investigador en el campo profesional de las fuerzas militares y teniendo en cuenta los lineamientos teóricos del comportamiento social, para de este modo lograr tener ítems que describieron con claridad el objetivo de la medida.

Situación que fue alcanzada y validada a través de la valides de contenido mediante el análisis de los jueces expertos, quienes basándose en sus conocimientos realizaron recomendaciones en cada una de las versiones de los ítems y la consecución de la escala final que fue piloteada en población con las características establecidas para la muestra, en dicho proceso se logró seleccionar los ítems que mostraron ser los indicados para la medida final y el diseño de la estrategia de medida. Una de las conclusiones más importantes en este proceso, fue reconocer la importancia de la aplicación del proceso de evaluación de jueces expertos teniendo en cuenta

las viables que fueron evaluadas este paso en el marco del proceso de investigación constituyó una clave fundamental para la consecución de ítems dotados de claridad, suficiencia y pertinencia.

Posterior al proceso de análisis de resultados de esta primera fase de la construcción y diseño del instrumento a modo de escala de medición en auto informe, se logró concluir que la medida diseñada a través de la escala constituye en primer lugar el resultado de un proceso de investigación riguroso, que represento el análisis de los resultados desde una metodología cuantitativa, a través del cual se lograron reconocer las diferentes consideraciones psicométricas, así consideradas en las teorías de construcción de las pruebas de medición, lo que favoreció la compresión del proceso del proceso de construcción y la metodología para el diseño del mismo.

Posteriormente el análisis de los resultados que aportaron las pruebas piloto y de validación del contenido del instrumento, permitieron determinar que el instrumento mide de manera unidimensional el constructo definido como las conductas que pueden interferir en las acciones de ciberseguridad, sin embargo, también dichas consideraciones psicométricas, permitieron determinar que existen ítems que pueden introducir ruido estadístico al proceso de análisis de los resultados y que deben ser datos sensibles de análisis para futuras investigaciones, así como para el uso del instrumento en poblaciones con otras características sociales o culturales, lo que representan principalmente que este instrumento es válido para medir este tipo de constructos en población que trabaja en el contexto militar, especialmente en la subespecialidad de ciberseguridad y ciberdefensa.

Otra conclusión aportada tras el proceso de análisis de resultados mostró que el instrumento cuenta con características psicométricas que indican su consistencia interna a nivel metodológico y por tanto representan los esfuerzos adelantados en la investigación por describir con amplitud el universo posible de conductas que pueden presentarse en el contexto laboral militar; sin embargo, también permite identificar que este tipo de herramientas no constituye una única forma de medición de dichas conductas, ni los resultados representan la generalidad del universo de personas que trabajan en contexto militar, esto teniendo en cuenta que el principal interés de esta investigación fue el diseño y elaboración del instrumento como una estrategia de medida efectiva que permitiera identificar si existen este tipo de comportamientos en el contexto militar y no la

caracterización de la población que trabaja en el contexto militar en la subespecialidad de ciberseguridad y ciberdefensa.

Por último, este estudio represento un desafío para el desarrollo mismo de la investigación, existieron varios retos a lo largo del desarrollo de la misma, en la medida en que se existe una ausencia significativa de información en materia y que la consecución de la información represento un esfuerzo significativo tanto en su recolección como en su compresión, por lo que los resultados obtenidos permitieron concluir que este tipo de investigaciones además de favorecer la recolección de datos científicos y puntos de referencia para posibles futuras investigaciones, también represento una oportunidad de crecimiento y aprendizaje de principio a fin.

Los resultados obtenidos en esta investigación representan los esfuerzos adelantados a lo largo del proceso de formación del programa de maestría y el interés en la construcción de nuevos horizontes que permitan ampliar la investigación en la materia y favorecer el desarrollo de herramientas de medición que puedan ser aplicables como estrategia efectiva en la identificación de este tipo de variables y como punto de partida lograr saber cómo identificarlas y así cumplir con el objetivo principal de la investigación.

**Referencias.**

Aiken, L. (2003). Glosario. En L. Aiken, Test Psicológicos y Evaluación (págs. 458-475). Mexico: Pearson.

Alcaraz, A. (2011). Cambios producidos por las TICS en la Distribución comercial. *Creatividad y Sociedad.* 15(5), 2-19.

Allport, G.W. (1935). Handbook of social Psichology, p.768-844.

Azjen, I. (1988). Attitudes, personality, and behavior. Homewood, Illinois: Dorsey Press.

Bandura, A. & Walters, R. (1983). Aprendizaje social y desarrollo de la personalidad. Alianza Universidad. Madrid. p. 293.

Bandura, A. & Walters, R.H. (1974). *Aprendizaje social y desarrollo de la personalidad.* Alianza Editorial

Bandura, A. (1977a). Social learning theory. New York: Prentice Hall.

Bandura, A. (1977b), Self-efficacy: Toward a unifying theory of behavioral change. Psychological Review, 84, 191-215.

Bandura, A. (1986) Social foundations of thought and action. A social cognitive theory. Englewood.

Bandura, A. (2000). Social Cognitive Theory: An Agentic Perspective. Stanford, California: Stanford University, Department of Psychology. Consultado el 5 de mayo de 2016, en: https://www.uky.edu/~eushe2/Bandura/Bandura2001ARPr.pdf

Burga, A. (2005). Unidimencionalidad de un instrumento de medición perspectiva factorial. *Ministerio de Educación Universidad Peruana Cayetano Heredia*, 1-21.

Comisión Europea (2013) "Estrategia de ciberseguridad de la Unión Europea: Un ciberespacio abierto, protegido y seguro". Disponible en: http://register.consilium.europa.eu/doc/srv?f=ST+6225+2013+INIT&l=es

Coz-Fernández, J. &Pastor-Pérez, V. (2013). La Conciencia situacional en ciberdefensa. Situational Awareness. (113) 90-92.

Cruz, L. (2015). Especificación de un Modelo de Comportamiento Delictivo. Acta de investigación Psicológica. 5(2), 2028-2046. Disponible en: http://www.psicologia.unam.mx/documentos/pdf/actas_ip/2015/articulos_b/Acta_Inv._Psicol._2015_5(2)_2028_2046_Especificacion_de_un_Modelo_del_Comportamiento_Delictivo.pdf

Cueva, R. A., Camino, J. R., y Ayala, V. M. M. (2013). Conducta del consumidor: estrategias y políticas aplicadas al marketing. Editorial Esic.

Chance, P. (2001). Aprendizaje y conducta. Tercera Edición, México: Manual Moderno.

Deighton, J. & Kornfeld, L. (2013). Amazon, Apple, Facebook and Google. *Harvard Business School. 514(7),* 1-19.

Del Pine Romero, C., y Fajardo, E. G. (2010). Internet y los nuevos consumidores: el nuevo modelo publicitario. Talos: Cuadernos de comunicación e innovación, (82), 55-64.

Departamento Nacional de Planeación. (14 de julio del 2011). Documento CONPES 3701. Lineamientos de política para ciberseguridad y ciberdefensa. Disponible en: http://www.mintic.gov.co/portal/604/articles3510_documento.pdf

Díaz del Río, Juan J. (2010), "La ciberseguridad en el ámbito militar", en Ministerio de Defensa, *Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio*, Cuadernos de Estrategia, 149, 217-256.

Domjan, M. (2010). Principios de aprendizaje y conducta. México: Thomson.

Fedesarrollo. (2014). Avances y retos de la defensa digital en Colombia. Disponible en: http://www.fedesarrollo.org.co/wp-content/uploads/TICNoviembre-2014_Web.pdf

Fernández, R. (2014). Actitudes y Comportamiento Social. Tesis Doctoral. Universitat Jaume I. Disponible en: http://repositori.uji.es/xmlui/bitstream/handle/10234/106155/TFG_2014_FERNANDEZ%20GARCIA.pdf?sequence=1&isAllowed=y

Forero, A.M. (2017). El Ejército Nacional de Colombia y sus heridas: una aproximación a las narrativas militares de dolor y desilusión. *Antípoda. Revista de Antropología y Arqueología* 29: 41-61. Doi: https://dx.doi.org/10.7440/antipoda29.2017.02

Garay, C. & Ramírez, E. (2017). Los factores estratégicos de Colombia en seguridad y su influencia en el posicionamiento regional en el postconflicto. En Ramírez, E. (2017). *Desafíos para la seguridad y defensa nacional de Colombia: Teoría y praxis*. Ediciones Escuela Superior de Guerra, Colombia, Estudios Superiores, 407 – 459.

González, M. M. (2008). El Análisis de Reactivos con Modelo de Rasch. *Universidad de Sonora,* 1-110.

Gregory, R. (2001). Validez y desarrollo de pruebas. En R. Gregory, Evaluación Psicológica, Historia, principios y aplicaciones (págs. 118-166). Mexico D.F: Manual Moderno.

Gregory, R. (2003). Construcción de Pruebas. En R. Gregory, *Evaluación Psicológica. Historia, Principios y Aplicaciones* (págs. 143-167). Mexico: Manual Moderno.

Guiza, M. (2011). Trabajo colaborativo en la Web. Tesis Doctoral. Universidad de les elles Balears. Recuperado de: http://www.tdx.cat/bitstream/handle/10803/59037/tmge1de1.pdf;jsessionid=B8777CD7E96B552EE2FA4C37233DADEC?sequence=1

Hernández, L., Cerquera, J. & Vanegas, J. (2015). Riesgos presentes en los ciberataques: un análisis a partir de las herramientas de auditoria forense. Pensamiento Republicano, 3(2). 57-76.

Hernández, S. R., Fernández, C. C., & Baptista, L. P. (2010). Metodología de la Investigación. México: McGraw Hill.

Llorens, T. A., Gil, P. L., Vidal Abarca, G. E., Giménez, T. M., Lloriá, A. M., & Pérez, R. G. (2011). Prueba de Competencia Lectora para Educación Secundaria. Universidad de Valencia y Universidad Nacional de Educación a Distancia, 808-817.

Malaver, F., & Vargas, M. (2005). Políticas y avances en la ciencia, la tecnología y la innovación en Colombia 1990-2005. *Cuadernos de Administración, 18* (30), 39-7

Manjarrés, I. & Jiménez F. (2012). Caracterización de los delitos informáticos en Colombia. *Pensamiento Americano,* 71-82.

Meneses Báez, A. L. (2013). Cuestionario de estrategias para la escritura de ensayos argumentativos. Acta Colombiana de Psicología, 137-148.

Meneses Báez, A. L. (2013). Cuestionario de estrategias para la escritura de ensayos argumentativos. *Acta Colombiana de Psicología*, 137-148.

Meneses, B. A. (2012). Guía para la interpretación resultados de cálculo análisis factorial MECP y por rotación de factores Varimax. *Universidad Catolica de Colombia*, 1-9.

Miguel, J. (2017). La integración del ciberespacio en el ámbito militar. *Grupo de estudios en seguridad internacional Universidad de Granada. Despoblé en http://www.seguridadinternacional.es/?q=es/content/la-integraci%C3%B3n-del-ciberespacio-en-el-%C3%A1mbito-militar*

Milenos, J. R. (1977). Principios de análisis conductual. México: Trillas.

Ministerio de Tecnologías de la información y las Comunicaciones, (2011). CONPES 3701.

Ministerio de Tecnologías de la información y las Comunicaciones, (2016). CONPES 3854.

MINSALUD. (4 de octubre de 1993). Resolución Nª 008430 de 1993. (M. d. Social, Ed.) Recuperado el 27 de abril de 2014, de Ministerio de Salud: http://www.unisabana.edu.co/fileadmin/Documentos/Investigacion/comite_de_etica/Res__8430_1993_-_Salud.pdf

Morales Vallejo, P. (2013). El Análisis Factorial en la construcción e interpretación de test, escalas y cuestionarios. Facultad de Ciencias Humanas y Sociales, *Universidad Pontificia Comillas*, Madrid, 1-46.

Morales, F (2000). Individualismo y psicología social. *Revista de psicología general y aplicada.* 53(2). 223-239

Niño, Y. (2015). Importancia de la implementación del concepto de ciberseguridad organizacional en las organizaciones tipo Pymes. Tesis de Maestría. Universidad Militar Nueva Granada.

Peligero, F. La antropología filosófica y la economía. *Anuario de filosofía, psicología y sociología. 2, 17-26. Disponible en: https://acceda.ulpgc.es:8443/bitstream/10553/3521/1/0237190_01999_0001.pdf*

Pellón, R. (2013). Watson, Skinner y algunas disputas dentro del conductismo. Revista Colombiana de Psicología, 22(2), 389-399.

Pérez, A. (1994). Psicología del Aprendizaje. Bogotá: Fondo Nacional Universitario.

Pino, E. (2013). *La dimensión social de la Universidad del Siglo XXI.* Tesis Doctoral. Universidad Complutense de Madrid. Recuperado de: http://eprints.ucm.es/22393/1/T34660.pdf

PISA. (2006). Marco de la evaluación. Conocimientos y habilidades en Ciencias, Matemáticas y Lectura. OCDE, 47-72.

Redacción Tecnológica de El Tiempo. (2011). Cada segundo hay 18 víctimas de Ciber-delitos. El Tiempo.

Ruíz, G. Pellón, R. & García, A (2006). Análisis experimental de la conducta en España. *Revistas Científicas de América Latina, el Caribe, España y Portugal*. 24, 71-103 Disponible en: http://redalyc.uaemex.mx/src/inicio/ArtPdfRed.jsp?iCve=79902408

Sanabria, A., & Uribe, A. (2009). Conductas antisociales y delictivas en adolescentes infractores y no infractores. *Pensamiento Psicológico, 6* (13), 203-217.

SEP. (2011). Habilidades Lectoras. Secretaria de Educación Pública Mexico, 1-6.

Skinner, B. F. (1975). ¿Son necesarias las teorías del aprendizaje? En B. F. Skinner (Ed.), *Registro acumulativo* (p. 77-111). Barcelona: Fontanela.

Tarpy, R.M. (2000). Aprendizaje: teorías e investigación contemporáneas del aprendizaje. Mexico D.F., México: Mc Graw Hill.

Vera, J. (2003). Desarrollo y comportamiento humano en el siglo XXI: Agenda Pendiente. *Tópicos de la comunicación. Despoblé en: http://www.psicom.uson.mx/topicos/4/historia.htm*

Wegener, H. (2013), "Los riesgos económicos de la ciberguerra", en IEEE, *La inteligencia económica en un mundo globalizado, Cuadernos de Estrategia*, 162, 177- 224.

Worchel, S., Cooper, J., Goethals, G. & Olson, J. (2000). Psicología Social. México: Thompson.

# APENDICES.

ESCALA DE COMPORTAMIENTOS POTENCIALMENTE PELIGROSOS EN MATERIA DE CIBERSEGURIDAD EN EL CONTEXTO MILITAR.

My. Quijano Rueda Camilo Andres.

FORMATO DE EVALUACIÓN POR JUECES

INSTRUCCIONES

Apreciado Evaluador(a):

Agradecemos su colaboración. En esta ocasión le solicitamos nos apoye con la evaluación de una (1) escala compuesta por 23 ítems diseñados con la finalidad de identificar los comportamientos de las personas que trabajan en el contexto militar que puedan interferir en las acciones de ciberseguridad. Para efectos de su evaluación en relación a la escala en cada ítem encontrará un cuadro donde podrá consignar las observaciones generales, posteriormente encontrará un formato con los ítems que corresponden a cada una de las categorías. Los criterios para la evaluación de los ítems son: pertinencia (P) – suficiencia (S) – claridad (C) – corrección gramatical (G). Asigne un valor de 1 si considera pertinente y 0 sino no considera la pertinencia, para cada uno de los criterios, teniendo en cuenta que 0 significa que no cumple con el criterio y que 1cumple de forma satisfactoria con el criterio. Para cada ítem tendrá un espacio que le permitirá realizar las observaciones que considere pertinentes.

Agradezco de ante mano su colaboración y pronta respuesta, dado que este paso es clave para el éxito de la investigación.

My. Quijano Rueda Camilo Andres.
Investigador Maestría en Ciberseguridad y Ciberdefensa.

Nombre: _____ Institución: _____

Nivel de formación: _____ Área de trabajo: _____

ESCALA DE COMPORTAMIENTOS POTENCIALMENTE PELIGROSOS EN MATERIA DE CIBERSEGURIDAD EN EL CONTEXTO MILITAR.

*Es una escala compuesta por 23 ítems. Tipo de escala: dicotómica (SI – NO).* Asigne un valor de 1 si considera pertinente y 0 sino no considera la pertinencia, para cada uno de los criterios, teniendo en cuenta que 0 significa que no cumple con el criterio y que 1cumple de forma satisfactoria con el criterio.

| ÍTEM | Pertinencia | Suficiencia | Claridad | Gramática | Observaciones |
|---|---|---|---|---|---|
| Periódicamente realizo actualizaciones a software y sistemas en mi equipo de trabajo dentro de la institución. | | | | | |
| Antes de descargar archivos en mi equipo de trabajo realizo un análisis de seguridad independiente del remitente del archivo. | | | | | |
| Me ajusto a las reglas de firewall dispuestas en su equipo de trabajo dentro de la institución. | | | | | |
| Me ajusto a los protocolos de seguridad diseñados por la institución para mantener a salvo la información. | | | | | |
| Uso servicios de alojamiento de información en la nube para guardar información de mi trabajo. | | | | | |
| Utilizo memorias extraíbles para alojar información de mi trabajo. | | | | | |
| Descargo aplicaciones y/o programas de en mi equipo de trabajo para uso diario. | | | | | |
| Uso equipos fuera de la institución para el envío de documentos o transferencia de información de mi trabajo. | | | | | |
| Conozco la legislación y/o normativas diseñadas en materia de seguridad de la información. | | | | | |
| Uso la autenticación como estrategia para proteger la información de mi equipo de trabajo. | | | | | |

| | | | | | |
|---|---|---|---|---|---|
| Actualizo con frecuencia mis claves de acceso en mi equipo de trabajo y correo electrónico. | | | | | |
| Realizo una copia de seguridad periódica de la información. | | | | | |
| Pongo en conocimiento de terceros mi dirección de correo electrónico institucional. | | | | | |
| Reviso correos electrónicos de remitentes desconocidos. | | | | | |
| Desde mi equipo de trabajo reviso enlaces recibidos por remitentes desconocidos. | | | | | |
| Uso contraseñas repetibles o comunes en mi equipo de trabajo. | | | | | |
| He utilizado servidores externos para enviar información confidencial. | | | | | |
| Comparto información de acceso con otros usuarios. | | | | | |
| He olvidado bloquear mi usuario en el equipo cuando me ausento de la oficina. | | | | | |
| Me he conectado a redes comerciales desde el equipo de trabajo. | | | | | |
| Utilizo aplicación de acceso remoto para trabajar en mi equipo desde otros lugares diferentes a mi oficina. | | | | | |
| Utilizo las redes sociales en mi equipo de trabajo. | | | | | |
| Comporto información confidencial de mi trabajo con otros compañeros por medio de redes sociales. | | | | | |

## ESCALA DE COMPORTAMIENTOS POTENCIALMENTE PELIGROSOS EN MATERIA DE CIBERSEGURIDAD EN EL CONTEXTO MILITAR.

**Instrucción:** a continuación, encontrará unos ítems que describen acciones que son realizadas con frecuencia por personas que trabajan en el contexto de la ciberseguridad y la ciberdefensa, teniendo en cuenta estas descripciones, seleccione **V** (verdadero) **F**(falso) según esto le describa.

| | | |
|---|---|---|
| Periódicamente realizo actualizaciones a software y sistemas en mi equipo de trabajo dentro de la institución. | V | F |
| Antes de descargar archivos en mi equipo de trabajo realizo un análisis de seguridad independiente del remitente del archivo. | V | F |
| Me ajusto a las reglas de firewall dispuestas en su equipo de trabajo dentro de la institución. | V | F |
| Me ajusto a los protocolos de seguridad diseñados por la institución para mantener a salvo la información. | V | F |
| Uso servicios de alojamiento de información en la nube para guardar información de mi trabajo. | V | F |
| Utilizo memorias extraíbles para alojar información de mi trabajo. | V | F |
| Descargo aplicaciones y/o programas de en mi equipo de trabajo para uso diario. | V | F |
| Uso equipos fuera de la institución para el envío de documentos o transferencia de información de mi trabajo. | V | F |
| Conozco la legislación y/o normativas diseñadas en materia de seguridad de la información. | V | F |
| Uso la autenticación como estrategia para proteger la información de mi equipo de trabajo. | V | F |
| Actualizo con frecuencia mis claves de acceso en mi equipo de trabajo y correo electrónico. | V | F |
| Realizo una copia de seguridad periódica de la información. | V | F |
| Pongo en conocimiento de terceros mi dirección de correo electrónico institucional. | V | F |
| Reviso correos electrónicos de remitentes desconocidos. | V | F |
| Desde mi equipo de trabajo reviso enlaces recibidos por remitentes desconocidos. | V | F |
| Uso contraseñas repetibles o comunes en mi equipo de trabajo. | V | F |
| He utilizado servidores externos para enviar información confidencial. | V | F |
| Comparto información de acceso con otros usuarios. | V | F |
| He olvidado bloquear mi usuario en el equipo cuando me ausento de la oficina. | V | F |
| Me he conectado a redes comerciales desde el equipo de trabajo. | V | F |
| Utilizo aplicación de acceso remoto para trabajar en mi equipo desde otros lugares diferentes a mi oficina. | V | F |
| Utilizo las redes sociales en mi equipo de trabajo. | V | F |
| Comparto información confidencial de mi trabajo con otros compañeros por medio de redes sociales. | V | F |

MATRIZ DE JUECES EXPERTOS.

| | Experto | | | | | | | | Índices de RVC | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **ÍTEM** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **Jueces** | **Pertinente** | **No pertinente** | **RVC** |
| Periódicamente realizo actualizaciones a software y sistemas en mi equipo de trabajo dentro de la institución. | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 8 | 8 | 0 | 1,0 |
| Antes de descargar archivos en mi equipo de trabajo realizo un análisis de seguridad independiente del remitente del archivo. | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 1 | 8 | 7 | 1 | 0,8 |
| Me ajusto a las reglas de firewall dispuestas en su equipo de trabajo dentro de la institución. | 1 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 8 | 7 | 1 | 0,8 |
| Me ajusto a los protocolos de seguridad diseñados por la institución para mantener a salvo la información. | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 8 | 8 | 0 | 1,0 |
| Uso servicios de alojamiento de información en la nube para guardar información de mi trabajo. | 1 | 1 | 1 | 1 | 0 | 1 | 1 | 1 | 8 | 7 | 1 | 0,8 |
| Utilizo memorias extraíbles para alojar información de mi trabajo. | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 8 | 8 | 0 | 1,0 |
| Descargo aplicaciones y/o programas de en mi equipo de trabajo para uso diario. | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 8 | 8 | 0 | 1,0 |
| Uso equipos fuera de la institución para el envío de documentos o transferencia de información de mi trabajo. | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 8 | 8 | 0 | 1,0 |
| Conozco la legislación y/o normativas diseñadas en materia de seguridad de la información. | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 8 | 7 | 1 | 0,8 |
| Uso la autenticación como estrategia para proteger la información de mi equipo de trabajo. | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 8 | 7 | 1 | 0,8 |
| Actualizo con frecuencia mis claves de acceso en mi equipo de trabajo y correo electrónico. | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 1 | 8 | 7 | 1 | 0,8 |
| Realizo una copia de seguridad periódica de la información. | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 1 | 8 | 7 | 1 | 0,8 |
| Pongo en conocimiento de terceros mi dirección de correo electrónico institucional. | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 8 | 7 | 1 | 0,8 |
| Reviso correos electrónicos de remitentes desconocidos. | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 1 | 8 | 7 | 1 | 0,8 |
| Desde mi equipo de trabajo reviso enlaces recibidos por remitentes desconocidos. | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 8 | 8 | 0 | 1,0 |
| Uso contraseñas repetibles o comunes en mi equipo de trabajo. | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 8 | 8 | 0 | 1,0 |
| He utilizado servidores externos para enviar información confidencial. | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 8 | 8 | 0 | 1,0 |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Comparto información de acceso con otros usuarios. | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 1 | 8 | 7 | 1 | 0,8 |
| He olvidado bloquear mi usuario en el equipo cuando me ausento de la oficina. | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 8 | 7 | 1 | 0,8 |
| Me he conectado a redes comerciales desde el equipo de trabajo. | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 8 | 8 | 0 | 1,0 |
| Utilizo aplicación de acceso remoto para trabajar en mi equipo desde otros lugares diferentes a mi oficina. | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 8 | 8 | 0 | 1,0 |
| Utilizo las redes sociales en mi equipo de trabajo. | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 1 | 8 | 7 | 1 | 0,8 |
| Comparto información confidencial de mi trabajo con otros compañeros por medio de redes sociales. | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 8 | 7 | 1 | 0,8 |