Factores que influencian la conducta de seguridad de la informática:
Un estudio transcultural

Resumen

Las violaciones de datos de alto perfil como Equifax, Yahoo, Facebook y Uber no solo afectan la confianza y lealtad de los clientes, sino que también causan pérdidas de reputación y financieras a gran escala, así como riesgos operativos. En consecuencia, los nuevos requisitos regulatorios y de cumplimiento, como el Reglamento General de Protección de Datos (GDPR), Ley de privacidad del consumidor de California (CCPA) y el Departamento de Servicios Financieros de Nueva York, Parte 500, exigen controles de seguridad de la información complejos y difíciles de implementar para garantizar la confidencialidad, integridad y disponibilidad de los datos de clientes y empleados. Los académicos están de acuerdo en que es necesario realizar más investigaciones para identificar los factores y antecedentes que influyen en las mejores prácticas de seguridad, privacidad y cumplimiento de políticas, y procesos de auditoría para las organizaciones. Esta investigación quiere contribuir al cuerpo teórico de conocimiento mediante el examen de factores culturales y de comportamiento que podrían conducir a una implementación efectiva del programa de gestión de riesgos de seguridad de los sistemas de información. También quiere proporcionar una mejor comprensión de cómo la cultura afecta la intención de cumplir con las políticas de seguridad de información entre diferentes naciones. Del mismo modo, quiere validar los constructos tomados de PMT y Hofstede, e identificar cómo éstos afectan la efectividad de la implementación del programa de gestión de riesgos de sistemas de información. Finalmente, esperamos que los resultados sustenten o rechacen constructos tomados de la literatura.

Palabras claves: Hofstede, Teoría de la motivación de la protección, ciberseguridad, políticas de cumplimiento, privacidad, manejo de riesgo

Introducción

La ciberseguridad se ha convertido en un desafío primordial para las organizaciones y empresas de todos los sectores debido a la creciente complejidad de los sistemas y redes de tecnología de la información, y por la creciente demanda de servicios de *software* (Yoo et al., 2018; Bahl & Wali, 2014). En específico, y según el informe de investigaciones de violación de datos de Verizon

(2017; 2018), las industrias financieras, bancarias, de seguros, de salud y gubernamentales están dentro de los cinco primeros puestos para convertirse en los objetivos principales de los delincuentes cibernéticos. Estas industrias son objetivos primarios debido a los beneficios monetarios que los ciberdelincuentes pueden obtener y los efectos perjudiciales que pueden crear mediante el robo, venta y divulgación de información personal no pública (NPPI por sus siglas en ingles) a través del mercado negro en la Internet (Verizon 2017; Verizon, 2018; Safa et al., 2015; Safa & Von Solms, 2016). Por otra parte, los hackers están desarrollando tácticas, técnicas y procedimientos más sofisticados que potencialmente podrían poner en riesgo todo tipo de redes corporativas, así como sus infraestructuras tecnológicas. Los hackers también han estado explotando las vulnerabilidades conocidas y desconocidas de los sistemas operativos y de las aplicaciones, sin dejar rastros de ninguna actividad maliciosa. Esa es la razón de que cuando los profesionales especializados en la seguridad de la información finalmente descubren estas actividades, en la mayoría de los casos, es demasiado tarde para recuperarse de esas violaciones de seguridad y fuga de datos.

La ciberdelincuencia está adoptando continuamente nuevas formas y nuevos métodos, como robo de datos o falsificación, sabotaje informático o ciberespionaje y manejo inadecuado de la información de la empresa por parte de socios comerciales, proveedores y empleados (Yoo et al., 2018; Verizon, 2017; Verizon, 2018). Estos riesgos han crecido hasta un punto en el que las violaciones de seguridad informáticas y fuga de datos son inevitables. Es sólo cuestión de tiempo el que sean *hackeados*, si es que las empresas no los descubren con antelación.

Las mejoras en tecnologías existentes y emergentes, como computación en la nube, Internet de las cosas (IoT), aprendizaje automático (ML) e inteligencia artificial (AI) (p. ej., *botnets*, *Chatbots* y asistentes digitales), son avances tecnológicos que se han vuelto más maduros y ampliamente utilizados. Esto permite a las empresas administrar y procesar una gran cantidad de datos, desde una diversa variedad de dispositivos conectados en línea en todo el mundo, así como tomar decisiones empresariales más rápidas, inteligentes y mejor informadas (Crespo-Perez & Ojeda-Castro, 2017; Safa et al., 2015). Del mismo modo, el empleo de nuevos y más exigentes requisitos regulatorios, creó un ambiente de preocupación dentro de la gestión de nivel *C-suite* de las

empresas sobre la importancia de estar en cumplimiento, con el fin de proteger sus activos primarios, sus clientes y los datos de los empleados (Johnston, & Perfil Warkentin, 2010).

De acuerdo con la revisión de la literatura y expertos en ciberseguridad, una tendencia hacia ataques cibernéticos cada vez más sofisticados continuará en un futuro próximo (Rocha-flores & Ekstedt, 2016; Yoo et al., 2018). Las industrias de servicios financieros y bancarios, componentes vitales de la infraestructura de la nación, siguen siendo un objetivo primordial para los ciberdelincuentes. Cabe señalar que las industrias de salud, gobierno, Retail, alojamiento y educación también están dentro de los más atractivos para perpetrar ciberataques (Verizon, 2017; Verizon, 2018).

Para mitigar los riesgos que las nuevas tendencias y adoptar tecnologías que pueden aportar a la organización, los profesionales y expertos de la seguridad de la información, así como también investigadores, han identificado factores que pueden ayudar dentro del cambiante espacio cibernético. La mayoría de los profesionales están implementando todo tipo de contramedidas tecnológicas para mitigar o reducir con éxito los riesgos cibernéticos dentro de sus empresas. Sin embargo, la revisión de la literatura muestra repetidamente que las contramedidas tecnológicas no son suficientes contra la enorme diversidad de ataques y vectores de amenazas de los ciberdelincuentes (Gratian et al., 2018; Rocha-flores & Ekstedt, 2016; Kim et al., 2014; Johnston, & Perfil Warkentin, 2010; Safa et al., 2015). Uno puede tener todas las tecnologías de seguridad que rodean y protegen el objetivo de ataques cibernéticos maliciosos externos, pero una simple vulnerabilidad, como no tener las actualizaciones, puede ser explotada por códigos de *software* maliciosos. Inclusive, una ejecución no intencionada por un usuario interno, podría ser suficiente para que la seguridad de la red de una empresa se vea comprometida. Esta explotación podría conducir a todo tipo de riesgos de seguridad como exponer información privada y confidencial de clientes y empleados, secretos comerciales, estrategias militares o instalaciones secretas, entre muchos otros.

Los estudiosos y los profesionales de la seguridad han señalado que los empleados de una empresa son el eslabón más débil en la seguridad de la información (Gratian et al., 2018; Moon et al., 2018; Balozian et al., 2017; Bulgurcu et al., 2010; Johnston, & Perfil Warkentin, 2010), a pesar de que

tienen la intención de cumplir con las políticas de seguridad de la información institucional y los requisitos reglamentarios. Del mismo modo, han reconocido que éstos empleados son a su vez, grandes activos para mitigar el riesgo cibernético (Burns et al., 2017; Shropshire et al., 2015; Bulgurcu et al., 2010). Dado que los empleados que cumplen con las reglas y regulaciones de seguridad de la información de la organización son una pieza importante e inteligente para fortalecer los programas de seguridad de la información, entender su comportamiento hacia el cumplimiento es crucial para las organizaciones que quieren aprovechar su capital humano (Moon et al., 2018; Bulgurcu et al., 2010; Johnston, & Perfil Warkentin, 2010).

En estudios recientes, los investigadores han estado interesados en identificar los factores humanos teóricamente arraigados que potencialmente podrían modificar comportamientos desviados, con el fin de hacer que los empleados cumplan exitosamente con las políticas de seguridad de la información de la organización (Gratian et al., 2018; Moon et al., 2018; Mwagwabi, McGill & Dixon, 2018; Balozian et al., 2017; Rocha-flores, & Ekstedt, 2016; Johnston, & Perfil Warkentin, 2010; Ifinedo, 2012). Más concretamente, las actitudes, los valores y las creencias, el miedo, las normas, los patrones de comportamiento y los rasgos culturales han estado captando la atención de los investigadores, ya que hallazgos recientes señalan que la falta humana de cumplimiento de la seguridad, comportamiento de violación, mal uso de la tecnología, falta de conciencia, apatía y la resistencia, están entre las principales razones para las violaciones de seguridad y fuga de datos de una organización (Balozian et al., 2017; Moon et al., 2018; Johnston, & Perfil Warkentin, 2010; Ifinedo, 2012). Asimismo, los humanos se han convertido en una pieza importante en la efectividad de la seguridad de la información (Moon et al., 2018; Gratian et al., 2018; Bulgurcu et al., 2010; Johnston, & Perfil Warkentin, 2010), aunque los resultados todavía son mixtos e inconclusos.

Es bien sabido entre los académicos y expertos en seguridad de la información que la tecnología no es el único factor para tener en cuenta al implementar medidas preventivas de seguridad, defensivas y detectivescas, asegurando así el entorno tecnológico (Moon et al., 2018; Rocha-flores, & Ekstedt, 2016). Los comportamientos e intenciones de los usuarios también deben ser ponderados como una parte importante del campo de la seguridad de la información (Ifinedo, 2012; Safa et al., 2015). La cultura es otro factor poderoso estudiado a largo plazo para dar forma a la intención del comportamiento humano (Dincelli, 2018; Menard et al., 2018; Dinev et al., 2008).

El comportamiento de seguridad de la información deficiente de los empleados se ha encontrado como una de las principales oportunidades en este dominio (Dincelli, 2018; Moon et al., 2018; Rocha-flores, & Ekstedt, 2016; Gratian et al., 2018; Balozian et al., 2017; Shropshire et al., 2015; Safa et al., 2015). El estudio propuesto se esfuerza para reducir el riesgo del comportamiento del usuario, considerando los factores organizacionales y culturales en este campo. Pretendemos evaluar cómo estos factores afectan al cumplimiento de las políticas de seguridad de la información, específicamente en la industria financiera. Presentamos varias hipótesis a probar y esperamos que exista una tendencia entre las dimensiones interculturales y el comportamiento de la intención del individuo.

Revisión de Literatura

Antecedentes teóricos

Esta investigación se basa fundamentalmente en la teoría de la motivación de la protección (PMT) de Rogers (1975; 1983) y en la teoría de las dimensiones culturales de Hofstede (1983; 1991). De la PMT, estamos centrados principalmente en los constructos de autoeficacia, la evaluación de amenazas y el temor a las amenazas. Por otro lado, para las dimensiones culturales nacionales de Hofstede, estamos interesados específicamente en los constructos individualismo-colectivismo, evitación de incertidumbre, distancia de poder y en la orientación a largo/corto plazo. Estamos interesados en estas dos teorías debido a los resultados significativos encontrados en la investigación del comportamiento de la intención individual desde que se propusieron originalmente.

Dimensiones conductuales

La teoría de la motivación de la protección (PMT) es una de las teorías explicativas más poderosas para predecir la intención de los usuarios de participar en acciones protectoras (Anderson & Agarwal, 2010; Floyd et al., 2000; Rogers, 1983; Rogers, 1975). La información sobre las amenazas desempeña un papel importante en la cognición del riesgo. La evaluación de amenazas y de afrontamiento son dos componentes principales de esta teoría. La evaluación de amenazas se relaciona con la valoración de los usuarios del nivel de riesgo, que resulta de tener una manera descuidada en términos de seguridad de la información (Floyd et al., 2000; Rogers, 1983; Rogers, 1975). Este riesgo puede amenazar la integridad, la confidencialidad y la disponibilidad de la

información. La vulnerabilidad percibida y la gravedad del riesgo son dos secciones importantes de la evaluación de amenazas.

La autoeficacia se refiere a las habilidades y capacidades de los usuarios para hacer frente o realizar el comportamiento recomendado (Floyd et al., 2000; Rogers, 1983; Rogers, 1975). En el contexto de este estudio, se refiere al comportamiento del usuario de tal manera que se minimice el riesgo de violación de la seguridad de la información. Los investigadores anteriores han aplicado la PMT con el fin de mostrar cómo el cumplimiento de las políticas de seguridad de la información organizacional redujo el riesgo de comportamiento de los usuarios (Safa et al., 2015; Bulgurcu et al., 2010; Anderson & Agarwal, 2010). Nuestro estudio utiliza esta teoría para mostrar que, si los usuarios piensan antes de tomar cualquier acción, en las consecuencias de sus actos en términos de seguridad de la información, y consideraran el nivel de daño y costo que podría significar, se comportarán más cuidadosamente.

Las evaluaciones de amenazas incluyen evaluaciones del individuo en términos de cuán perjudicial es la amenaza (gravedad de la amenaza), la probabilidad de que el individuo sea vulnerable a la amenaza (susceptibilidad a las amenazas) y cualquier beneficio extrínseco o intrínseco que se logre al comportarse de una manera maladaptativa (Floyd et al., 2000; Rogers, 1983, 1975). Investigaciones anteriores han demostrado que las percepciones de la gravedad y susceptibilidad de las amenazas están positivamente correlacionadas con el comportamiento adaptativo, mientras que los beneficios intrínsecos y extrínsecos reducen las percepciones de las amenazas y minimizan la probabilidad de que una persona realice un comportamiento adaptativo (Floyd et al., 2000; Rogers, 1983, 1975).

Tras una evaluación de la amenaza, un individuo llevará a cabo una evaluación del mecanismo de afrontamiento sugerido. En este proceso, el individuo mide la eficacia de la respuesta recomendada (eficacia de respuesta), su confianza en la capacidad de realizar correctamente la respuesta recomendada (autoeficacia) y la cantidad de tiempo, dinero o esfuerzo necesario para realizar la respuesta recomendada (costo de respuesta) (Floyd et al., 2000; Rogers, 1983, 1975). La eficacia de la respuesta y la autoeficacia han demostrado efectos positivos en el rendimiento de las

respuestas recomendadas, mientras que el costo de respuesta tiene un impacto negativo en los comportamientos adaptativos (Floyd et al., 2000; Rogers, 1983, 1975).

Las dimensiones culturales

La cultura se ha definido como una programación colectiva de la mente que distingue a los miembros de un grupo o categoría de personas de otros (Hofstede, 1983). Esta definición implica que los patrones de pensamiento, sentimiento y potencial, actuando sobre diversos índices de desarrollo de ciberseguridad, se ven afectados por la cultura. Por lo tanto, la cultura nacional se refiere a la actitud general, los sistemas de creencias, los valores y las tradiciones peculiares de una nación (Hofstede, 1983). Esto implica que el desarrollo de la ciberseguridad en todos los niveles de la sociedad depende en gran medida de cómo esa sociedad vea el tema de la seguridad y su actitud hacia ella. La conceptualización más popular de la cultura entre los investigadores es el marco cultural de Hofstede. A pesar de las críticas por su metodología para validar los datos, habiendo confiado en las entrevistas de los empleados de IBM y planteando preguntas sobre la extensión de sus hallazgos a la cultura nacional, el marco ha sido ampliamente validado por miles de estudios. También constituye la base de la mayor parte de la investigación de dimensiones culturales con respecto a estudios comparados transculturales.

La extensa investigación de Hofstede ha sido la obra más celebrada en el campo de la cultura nacional (Hofstede, 1983). Analizando los datos obtenidos a través de 116,000 cuestionarios, de los cuales más de 60,000 personas respondieron de más de 50 países durante el período 1967-1978, Hofstede identificó cuatro dimensiones bipolares; distancia de poder (PD), individualismo/colectivismo (I/C), evasión de incertidumbre (UA) y masculinidad/feminidad (M/F) (Hofstede, 1983). Esto se convirtió en la base para la caracterización de la cultura para cada país. El quinto elemento, la orientación a largo/corto plazo, se introdujo después de un estudio posterior, en un esfuerzo por captar la incertidumbre de la cultura Asiática (Minkov & Hofstede, 2010).

A medida que las organizaciones continúan expandiendo sus operaciones en nuevas regiones de todo el mundo y reclutan personal local, se vuelve fundamental entender cómo las normas culturales nacionales pueden influir en las percepciones a nivel individual de las intenciones de

comportamiento seguras. Como se mencionó anteriormente, en la investigación de Hofstede (1983) sobre las dimensiones culturales, individualismo-colectivismo fue identificado como una diferencia cultural, especialmente cuando se comparan culturas occidentales y orientales. En general, las personas en las culturas occidentales poseen una visión del mundo individualista, mientras que las de los países orientales son típicamente colectivistas (Hovav & D'Arcy, 2012; Minkov & Hofstede, 2010). Esta diferencia cultural debe proporcionar información adicional sobre cómo se toman las decisiones sobre el cumplimiento de las directrices de política de seguridad. Las dimensiones culturales también han demostrado influir en el cumplimiento de las políticas de seguridad de las personas (Hovav & D'Arcy, 2012).

La dimensión individual versus colectivismo expresa el grado con que una sociedad refuerza el logro individual o colectivo y la relación interpersonal (Hofstede, 1983). La cultura del individualismo se ocupa del derecho a la intimidad y prefiere el uso de la comunicación electrónica, ya que es más orientada a la tecnología que la cultura colectivista. Por su parte, la cultura colectivista prefiere la comunicación cara a cara para establecer un marco social estrechamente unido, en el que los individuos esperan que su grupo los cuide a cambio de una lealtad incuestionable.

Distancia de poder explica el deseo social de jerarquías y la aceptación de la distribución del poder entre individuos e instituciones dentro de esa cultura. Una cultura que ocupa un lugar alto en la distancia de poder tolera mucha desigualdad, mientras que las culturas de baja potencia no apoyan la desigualdad, sino que apoyan la independencia de dichos miembros para expresar su opinión (Hofstede, 1983). Por lo tanto, es razonable esperar menos uso de la información en la cultura de alta distancia de poder y menos necesidad de protección contra los ciberataques.

La dimensión evitación de incertidumbre aborda la tolerancia de la sociedad a la ambigüedad y la incertidumbre. Una sociedad con baja tolerancia a la incertidumbre tendrá un índice elevado de elusión de la incertidumbre y se caracterizará por la intolerancia, la evasión del riesgo y la necesidad emocional de amplias legislaciones, incluso cuando no se obedezcan (Hofstede, 1983). Por lo tanto, esta dimensión es relevante ya que las políticas, normas y control son factores importantes en el desarrollo de la ciberseguridad.

Para la dimensión de masculinidad versus feminidad, según Hofstede (1983), la masculinidad es sinónimo de preferencia en la sociedad por el logro, asertividad y éxito material; mientras que la feminidad expresa la preferencia por la relación, la modestia y el cuidado para los débiles. Es una cultura orientada a los resultados que se ocupa más de los hechos que de los sentimientos. El uso de la tecnología, por lo tanto, garantiza la entrega de resultados, que es una de las preocupaciones de una cultura masculina. Debido a la falta de hallazgos significativos y la correlación de no existencia en la literatura de cumplimiento de políticas, vamos a excluir esta dimensión de nuestro estudio.

Por último, la dimensión de largo/corto plazo expresa la medida en que una cultura orienta a sus miembros a aceptar un objetivo a largo plazo centrado en el futuro, frente al respeto por la tradición y las orientaciones a corto plazo, que enfatiza la pasado y el presente (Minkov & Hofstede, 2010). Esta cultura establece objetivos a largo plazo y estrategias, mecanismo que representa uno de los índices más significativos de la ciberseguridad.

Las diferencias interculturales entre los empleados dentro de las organizaciones son también factores importantes que podrían tener un impacto en la seguridad de la información (Hovav & D'Arcy, 2012; Dinev et al., 2008). A medida que aumentaba la interconectividad global, también lo hacían las complejidades y los desafíos de mantener la seguridad de la información. En este estudio, las diferencias culturales en las intenciones de comportamiento para actuar con seguridad se estudian examinando los vínculos entre el individualismo-colectivismo, evitación de incertidumbre, distancia de poder y el comportamiento largo y seguro, en el contexto del cumplimiento normativo de la seguridad de la información.

El marco conceptual propuesto muestra que, en una cultura de seguridad, la autoeficacia, la evaluación de amenazas, el temor a la amenaza, el individualismo-colectivismo, la elusión de la incertidumbre, la distancia de poder y la orientación a largo/corto plazo podrían influir en la actitud hacia tener un método cuidadoso, en términos de comportamiento de intención de seguridad de la información. Influir positivamente en la intención de cumplir con directivas de seguridad de información organizativa podrían afectar al rendimiento de seguridad organizacional.

Marco de estudio

Para nuestro estudio, proponemos un modelo teórico extraído de la teoría de motivación de protección (PMT) y la dimensión de cultura nacional de Hofstede. La figura 1 presenta el modelo y sus relaciones hipotetizadas asociadas. En el modelo propuesto, representamos la autoeficacia, la evaluación de amenazas y el temor a la amenaza, componentes del PMT, como antecedentes que influyen en la intención del individuo de cumplir. PMT asume que las intenciones de comportamiento predicen la conducta protectora (Rogers, 1983; 1975), por lo tanto, su variable dependiente es una medida de las intenciones del comportamiento. Del mismo modo, representamos al individualismo-colectivismo, la evitación de incertidumbre, la distancia de poder, y la dimensión a largo/corto plazo, como variables de influencia directa a la intención del individuo de cumplir con las políticas de seguridad de la información.

Desarrollo de Hipótesis Principales

Sobre la base de la revisión bibliográfica presentada en este trabajo, se han formulado las siguientes hipótesis:

- H_1: La autoeficacia está relacionada positivamente con el comportamiento de la intención de cumplimiento de políticas de seguridad de información.
- H_2: La evaluación de amenazas está positivamente relacionada con el comportamiento de intención de cumplimiento de políticas de seguridad de información.
- H_3: El miedo a la amenaza está positivamente relacionado con el comportamiento de intención de cumplimiento de políticas de seguridad de información.
- H_{4a}: El individualismo está relacionado negativamente con el comportamiento de intención de cumplimiento de políticas de seguridad de información.
- H_{4b}: El colectivismo está positivamente relacionado con el comportamiento de intención de cumplimiento de políticas de seguridad de información.
- H_5: La evasión de incertidumbre está positivamente relacionada con el comportamiento de intención de cumplimiento de políticas de seguridad de información.
- H_6: La distancia de poder está positivamente relacionada con la actitud de los empleados hacia el comportamiento de intención de cumplimiento de políticas de seguridad de información.

- H_7: La orientación a largo/corto plazo está positivamente relacionada con la actitud de los empleados hacia el comportamiento de intención de cumplimiento de políticas de seguridad de información.
- H_8: La intención de cumplir con las políticas de seguridad de información conduce hacia una implementación efectiva de un programa de gestión de riesgos de seguridad de la información.

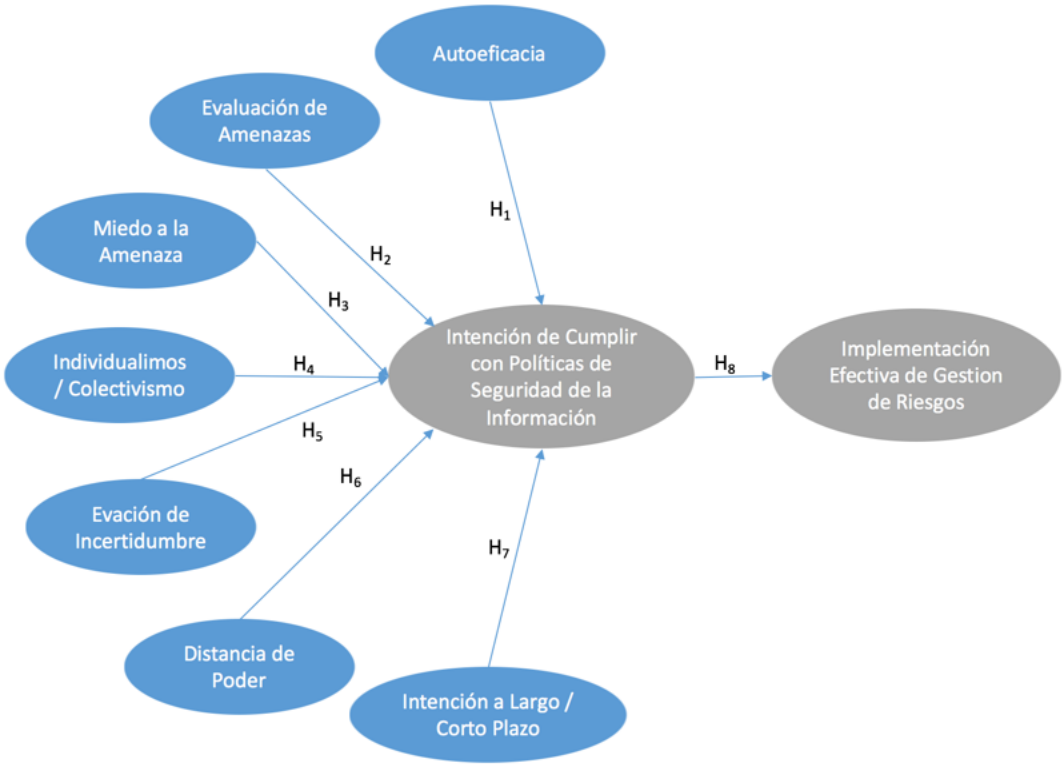

Figura 1. Marco conceptual propuesto

Fuente: Elaboración propia

Metodología

Diseño de investigación

El diseño de la investigación para este estudio será uno cuantitativo no experimental. Se medirán múltiples variables independientes y dependientes, asegurando que ninguna variación intencional tenga lugar. Del mismo modo, la relación entre las variables será del tipo correlacional-causal, donde las causas y efectos ya ocurrieron, o se están produciendo durante el progreso del estudio, y la persona que está llevando a cabo la investigación observa y los informa (Hernández et al.,

2015). Establecer este tipo de relación ayudará al investigador a describir las variables y analizar su influencia en un momento en el tiempo.

Población

Un foro de la industria de servicios financieros ubicado en los Estados Unidos proporcionará una muestra global de sus miembros profesionales, de distintas industrias financieras y sectores bancarios. Entre los miembros, identificaremos varios roles y puestos clave cuyas responsabilidades son garantizar el cumplimiento de las políticas de seguridad de la información y las mejores prácticas de seguridad, y salvaguardar la confidencialidad, integridad y disponibilidad de los datos de sus clientes y de los empleados para las empresas en las que trabajan. Del mismo modo, deben estar a cargo de la gobernanza y la aplicación de contramedidas que funcionan como la primera y segunda líneas de defensa contra las amenazas cibernéticas y riesgos de seguridad de la información ante ciberataques.

Diseño de la muestra

La muestra consistirá en toda la membresía de un foro del centro de seguridad y análisis de la información de los servicios financieros (FS-ISAC). Entre los miembros de este foro se encuentran jefes de seguridad de la información (CISO), directores de tecnología (CTO), directores de riesgos (CRO) y profesionales de seguridad de información, entre otros gerentes de nivel ejecutivo. También incluiría a otros profesionales tales como contadores, oficiales de tecnología de la información y personal de seguridad de la información. Enviaremos una invitación por correo electrónico a más de 7,000 de los miembros profesionales para crear una población de muestras diversa (industria financiera y sectores bancarios). La encuesta también se publicará en varias redes sociales profesionales, con meta-palabras como infosec, contabilidad, ciberseguridad, banca y finanzas, para obtener una muestra más grande y variada.

Discusión del instrumento

Se desarrollará un cuestionario para las variables y elementos identificados y seleccionados de la revisión de literatura. Este cuestionario se utilizará para recopilar datos de forma estructurada y cuantificable, para establecer el empirismo de esta investigación. Este instrumento se dividirá en tres partes. La primera sección será una captura de la información demográfica de la empresa:

nombre, región geográfica, industria y/o sector al que pertenece, tamaño (número de empleados), ubicaciones dentro y/o fuera de los Estados Unidos de América y tipos de servicios y/o productos ofrecidos, entre otros. La segunda parte de la encuesta recogerá los datos demográficos de los empleados: rango de edad, rol/posición, años de experiencia profesional y educación (grado académico y/o certificaciones profesionales), nacionalidad, grupo étnico y estatus migratorio, entre otros. Por último, la tercera sección medirá y validará los constructos del marco conceptual propuesto en esta investigación.

Para mantener la validez y confiabilidad de los instrumentos utilizados en estudios anteriores, la escala Likert de cinco puntos se utilizará para representar valores de datos ordinales que van desde en desacuerdo (1) a totalmente de acuerdo (5). Una vez que todos los datos son recopilados, purificados, normalizados y homogeneizados, realizaremos varios análisis estadísticos, utilizando el paquete estadístico de IBM para el programa de ciencias sociales (SPSS).

Recopilación de datos

El investigador recopilará los datos mediante la administración de una encuesta basada en la *web*, que se considera apropiada ya que nuestros encuestados serán empleados que utilicen los recursos de tecnología de la información de sus organizaciones y tienen acceso a Internet (D'Arcy & Lowry, 2017; Hovav, & D'Arcy 2012; Bulgurcu et al., 2010). La encuesta se enviará por correo electrónico y se publicará en varios foros y redes sociales profesionales. También será administrado en persona dentro de múltiples conferencias de seguridad de la información y/o cumbres alrededor de Estados Unidos y Puerto Rico.

Análisis de datos

Para establecer el empirismo dentro de esta investigación, se utilizarán varios métodos y técnicas estadísticas avanzadas. Entre ellos se encuentran los siguientes: coeficiente alfa de Cronbach, análisis de factores y correlación, y múltiples regresiones lineales (o PLS). Los análisis también incluirán estadísticas inferenciales y descriptivas.

El análisis factorial nos dice cómo establecer la evidencia de validez de los constructos que se están midiendo (Hernández et al., 2015). Según Hernández et al. (2015), este método muestra

cuántas dimensiones constituyen una variable y qué elemento componen cada dimensión. Es una técnica estadística que se utiliza para descubrir la estructura interna de un número relativamente grande de variables. En nuestro caso, podemos utilizarlo para simplificar la información dada por una matriz de correlaciones con la intención de tener una interpretación mejor y más fácil (Hernández et al., 2015).

Para este estudio, podemos utilizar el método de consistencia interna conocido como el coeficiente alfa de Cronbach, que oscila entre cero (0) y uno (1), para calcular la confiabilidad del cuestionario o instrumento a utilizar. Según Sekaran (2003), cuanto más se acerque el alfa de Cronbach a uno, mayor será el grado de confiabilidad de la consistencia interna del instrumento. Esto significa que un coeficiente superior a 0.90 indica que el instrumento es altamente fiable; entre 0.89 y 0.80, que es bueno; entre 0.79 y 0.70, que el instrumento es aceptable; entre 0.60 y 0.69 es débil; y entre 0.59 y 0.50, el cuestionario es deficiente. Si es inferior a 0.50, el instrumento es de baja confiabilidad y no es aceptable para llevar a cabo la investigación (George & Mallery, 2009)

El análisis de correlación se puede utilizar para determinar la correlación entre las variables de la investigación. Este método mide el grado o nivel de correlación en el que las variables están relacionadas entre sí. Por ejemplo, uno puede hacer uso del coeficiente de correlación de Pearson, que tiene como objetivo proporcionar una medida numérica del nivel de correlación entre dos variables, si ambas variables son cuantitativas. Según Hair et al (2013), el índice indica una dependencia entre las dos variables denominadas relación directa: cuando uno aumenta, el otro también lo hace en proporción constante. La correlación de rangos puede variar de cero a uno y el valor más alto será el nivel de correlación más alto.

La regresión lineal múltiple es un método para analizar el efecto de dos o más variables independientes en una dependiente (Hair et al., 2013). Es una extensión de la regresión lineal, sólo que con un mayor número de variables independientes. En otras palabras, se utiliza para predecir el valor de una variable dependiente, cuando el valor y la influencia de las variables independientes contenidas en el análisis son conocidas (Hernández et al., 2015). Para este método, la distribución de los datos debe incluir la normalidad, la independencia, la homogeneidad y la linealidad (Hair et al., 2015;). Por ejemplo, si queremos conocer el efecto de las variables a) autoeficacia, b)

evaluación de amenazas, c) miedo a la amenaza, d) individualismo-colectivismo, e) evitación de incertidumbre, f) distancia de poder y e) orientación a largo/corto plazo sobre la variable intención de cumplir con el ISP, el método de regresión múltiple podría ser adecuado para aplicar a los datos recopilados. Sin embargo, si la distribución de datos no es normal u homogénea, se recomienda utilizar otro método de análisis, como multivariado, para analizar múltiples variables independientes y dependientes (Hair et al., 2013; Hair et al., 2015).

Hallazgos

Dentro de esta investigación, los autores esperan correlaciones positivas entre factores culturales y humanos, lo que puede conducir a la mitigación de riesgos de seguridad de la información para reducir los ciberataques. Del mismo modo, esperamos hallazgos significativos entre las relaciones en la integración de varios constructos de la motivación de la protección y la teoría de Hofstede sobre la intención del comportamiento del individuo, para aclarar el cumplimiento de la política de seguridad de información en organizaciones entre naciones. Por último, esperamos resultados confirmatorios entre variables independientes y dependientes para sostener y/o rechazar constructos tomados de la literatura consultada.

Discusión y conclusiones

Los ciberataques están creciendo vertiginosamente y tácticas más sofisticadas de *hacking*, técnicas y procedimientos, representan desafíos más novedosos y complejos para las organizaciones y los profesionales de seguridad de la información. Vulnerabilidades descubiertas recientemente como Spectre y Meltdown, están generando todo tipo de preocupaciones y pánico a nivel mundial. Además, la fuga de datos de alto perfil como Equifax, Yahoo, Facebook, Home Depot y Uber están afectando la confianza y lealtad de los clientes, representando pérdida de reputación y financiera a gran escala y riesgos operacionales.

Por otro lado, los comportamientos desviados de los usuarios, la inconsciencia, el mal uso, la apatía y la resistencia suelen ser las razones principales de las infracciones de seguridad. Del mismo modo, el comportamiento de seguridad de la información deficiente de los usuarios y la falta de apoyo de la alta gerencia organizacional, están entre los principales problemas en el dominio de seguridad de la información. Por lo tanto, este estudio intenta reunir las dimensiones culturales

Hofstede y la PMT en el marco conceptual propuesto, en un esfuerzo por reducir el riesgo de comportamientos desviados de los usuarios, así como para aumentar el apoyo a la gestión en este ámbito.

Implicaciones académicas y prácticas

Este estudio ayudará a establecer un modelo teórico con el propósito de evaluar los factores que influyen en la implementación de un programa eficaz de gestión de riesgos de seguridad de la información. Del mismo modo, su objetivo es validar si varios o algunas de los constructos tomados de la revisión de la literatura son sostenidos o rechazados. También busca probar y expandir la teoría de la motivación de la protección con el fin de identificar las variables predictoras y moderadoras, y sus respectivas correlaciones y efectos. Por último, contribuirá a identificar la influencia de las dimensiones de la cultura nacional en la actitud de los empleados y, por ende, su comportamiento hacia la intención de cumplir con las políticas de seguridad de la información.

Desde el punto de vista práctico, este estudio ayudará a las empresas a comprender mejor cuáles son los factores más importantes e influyentes al implementar un programa de gestión de riesgos para la seguridad de la información. También servirá como guía de implementación de gestión de riesgos a la planificación de nuevas iniciativas y adopciones tecnológicas, así como una referencia en el desarrollo de nuevas políticas de ciberseguridad, estándares y directrices. La comprensión de estos factores y su correlación podría proporcionar a los gerentes una mayor percepción y dirigirlos para desarrollar e implementar un programa de gestión de riesgos de seguridad de la información más eficaz y holístico. Asimismo, este estudio reforzará la importancia de establecer una cultura de seguridad a través de las instituciones. Por último, busca proporcionar información a las empresas sobre cómo estos factores influyentes afectan el rendimiento de la seguridad de la información de la organización.

Contribuciones

Esta investigación quiere contribuir al cuerpo teórico del conocimiento examinando las intenciones del comportamiento del individuo, y los factores culturales que podrían conducir hacia una implementación efectiva del programa de gestión de riesgos de seguridad de los sistemas de

información. También quiere proporcionar una mejor comprensión de cómo las dimensiones culturales tienen un impacto en la intención del individuo de cumplir con las políticas de seguridad de información entre naciones.

Referencias bibliográficas

Anderson CL, Agarwal R (2010) Practicing safe computing: a multimedia empirical examination of home computer user security behavioral intentions. MIS Q 34(3):613–643

Bahl, S., & Wali, O. P. (2014). Perceived significance of information security governance to predict the information security service quality in software service industry. Information Management & Computer Security, 22(1), 2–23. http://doi.org/10.1108/IMCS-01-2013-0002

Balozian, P., Leidner, D., & Warkentin, M. (2017). Managers' and Employees' Differing Responses to Security Approaches. Journal of Computer Information Systems, 1–14. http://doi.org/10.1080/08874417.2017.1318687

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. MIS Quarterly, 34(3), 523–548. http://doi.org/10.1093/bja/aeq366

Burns, A. J., Roberts, T. L., Posey, C., Bennett, R. J., & Courtney, J. F. (2017). Intentions to Comply Versus Intentions to Protect: A VIE Theory Approach to Understanding the Influence of Insiders' Awareness of Organizational SETA Efforts. Decision Sciences, 0(0). http://doi.org/10.1111/deci.12304

Crespo-Perez, G., & Ojeda-Castro, A. (2017). Convergence of Cloud Computing, Internet Of Things, And Machine Learning: The Future Of Decision Support Systems. International Journal of Scientific & Technology Research, 6(7). http://doi.org/10.1109/ICITST.2016.7856729

D'Arcy, J., & Lowry, P. B. (2017). Cognitive-affective drivers of employees' daily compliance with information security policies: A multilevel, longitudinal study. Information Systems Journal, (September 2016), 1–27. http://doi.org/10.1111/isj.12173

Dincelli, E. (2018). The Role of National Culture in Shaping Information Security and Privacy Behaviors. World Scientific Book Chapters, 47-68.

Dinev, T., Goo, J., Hu, Q., and Nam, K. 2008. "User Behavior Towards Protective Information Technologies: The Role of National Cultural Differences," Information Systems Journal

(19:4), pp. 391-412.

Floyd DL, Prentice-Dunn S, Rogers RW. A Meta-Analysis of Research on Protection Motivation Theory. J Appl Soc Psychol 2000; 30: 407–29.

George, D. and P. Mallery (2009). SPSS for Windows step by step: A simple guide and reference 16.0 update Boston, Pearson Education, Inc.

Gratian, M., Bandi, S., Cukier, M., Dykstra, J., & Ginther, A. (2018). Correlating human traits and cyber security behavior intentions. Computers & Security, 73, 345–358

Hair, J. F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2013). A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM). Thousand Oaks: Sage.

Hair, J.F., Celsi, M., Money, A., Samouel, P. y Page, M. (2015). Essentials of Business Research Methods, M.E. Sharpe

Hernandez, R.; Fernandez, C. y Baptista, P. (2015). Metodología de la Investigación, McGraw Hill.

Hofstede, G. (1983). The cultural relativity of organizational practices and theories. Journal of international business studies, 14(2), 75-89.

Hovav, A., & D'Arcy, J. (2012). Applying an extended model of deterrence across cultures: An investigation of information systems misuse in the US and South Korea. Information & Management, 49(2), 99-110.

Ifinedo P. Understanding information systems security policy compliance: an integration of the theory of planned behavior and the protection motivation theory. Computer Securirty 2012; 31(1):83–95. http://dx.doi.org/10.1016/j.cose.2011 .10.007.

Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: an empirical study. MIS quarterly, 549-566.

Kim, S. H., Yang, K. H., & Park, S. (2014). An Integrative Behavioral Model of Information Security Policy Compliance. The Scientific World Journal, 2014, 1–12. https://doi.org/10.1155/2014/463870

Menard, P., Warkentin, M., & Lowry, P. B. (2018). The impact of collectivism and psychological ownership on protection motivation: A cross-cultural examination. Computers and Security, 75, 147–166. https://doi.org/10.1016/j.cose.2018.01.020

Minkov M. and Hofstede G. (2010) Hofstede's Fifth Dimension: New Evidence from the World Values Survey Journal of Cross-Cultural Psychology 43(1) 314.

Moon, Y. J., Choi, M., & Armstrong, D. J. (2018). The impact of relational leadership and social alignment on information security system effectiveness in Korean governmental organizations. International Journal of Information Management, 40(August 2017), 54–66. http://doi.org/10.1016/j.ijinfomgt.2018.01.001

Mwagwabi, F., McGill, T., & Dixon, M. (2018). Short-term and long-term effects of fear appeals in improving compliance with password guidelines. Communications of the Association for Information Systems, 42(1), 147–182

Rocha Flores, W., & Ekstedt, M. (2016). Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. Computers and Security, 59, 26–44. http://doi.org/10.1016/j.cose.2016.01.004

Rogers RW. A Protection Motivation Theory of Fear Appeals and Attitude Change. J Psychol 1975; 91: 93–114.

Rogers RW. Cognitive and Physiological Processes in Fear Appeals and Attitude Change: A Revised Theory of Protected Motivation. In: Cacioppo JT, Petty RE, editors. Soc. Psychophysiol. A Source., New York: The Guilford Press; 1983, p. 153–76.

Safa, N. S., & Von Solms, R. (2016). An information security knowledge sharing model in organizations. Computers in Human Behavior, 57, 442–451. http://doi.org/10.1016/j.chb.2015.12.037

Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behavior formation in organizations. Computers and Security, 53, 65–78. http://doi.org/10.1016/j.cose.2015.05.012.

Sekaran, U. (2003). Research Methods for Business: A Skill Building Approach, J. W. Sons.

Shropshire, J., Warkentin, M., & Sharma, S. (2015). Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. Computers and Security, 49, 177–191. http://doi.org/10.1016/j.cose.2015.01.002

Verizon. (2017). 2017 Verizon Data Breach Investigations Report, 10th edition, 1-74.

Verizon. (2018). 2018 Verizon Data Breach Investigations Report, 11th edition, 1-68.

Yoo, C. W., Sanders, G. L., & Cerveny, R. P. (2018). Exploring the influence of flow and psychological ownership on security education, training and awareness effectiveness and security compliance. Decision Support Systems, (July 2017), 0–1. http://doi.org/10.1016/j.dss.2018.02.009