Yura: Relaciones internacionales

Departamento de Ciencias Económicas, Administrativas y de Comercio

Revista electrónica ISSN: 1390-938x

N° 20: Octubre - diciembre 2019

Modelo de Creencia de Salud: Investigación aplicada en el sector corporativo ante el ciber delito pp. 137-163

Manobanda Mora, Melissa Jamileth

Universidad de las Fuerzas Armadas, sede Sangolquí

Sangolquí, Ecuador

Av. Gral. Rumiñahui s/n, EC170501.

mjmanobanda1@espe.edu.ec

Modelo de Creencia de Salud: Investigación aplicada en el sector corporativo ante el ciber delito

Manobanda Mora, Melissa Jamileth
Universidad de las Fuerzas Armadas
melissa.jamileth.mm@gmail.com

Resumen

La siguiente investigación tiene como base el comprender la percepción del entorno de seguridad digital de las empresas en la República del Ecuador. El Modelo de Creencia de Salud diseñado presenta un conjunto de dimensiones que explican la manera de como la cultura organizacional se percibe ante los ataques digitales propios del ciberdelito, convertidos en un mal social, donde los gerentes y colaboradores deben mostrar interés en estrategias competentes en la era digital. Para el análisis de la investigación se realizó un cuestionario que aborda las características propias de cada dimensión revisados a través de la investigación y que fueron analizados con ayuda de parámetros estadísticos como análisis de frecuencias, correlación de variables y análisis de correspondencias.

Palabras clave
Modelo de Creencia de Salud, ciber- delito, cultura organizacional.

Abstract

The following research was based on understanding the perception of the digital security environment of companies in the Republic of Ecuador. The Health Belief Model designed presents a set of dimensions that explain the way how the organizational culture is perceiving the digital attacks own of the cybercrime, a social evil, where the managers and collaborators must show interest in adapting their strategies in the digital age.

The analysis research was conducted a questionnaire that addresses the characteristics of each dimension reviewed through investigation and were analyzed with the help of statistical parameters such as frequencies analysis, correlation, and analysis of correspondences

Keywords

Health belief model, cyber-crime, organizational culture.

La línea de tiempo tanto de la humanidad como de la guerra se vincula históricamente. El hombre no es un gladiador por excelencia más bien ha buscado incesantemente la superación de sus debilidades por necesidad de existencia desde la era primitiva, lo cierto es que, la violencia de grupos humanos documenta hostilidad en la diversidad de culturas (Álvarez, 2007). Debido a la pertenencia por hechos de descendencia y nacimiento, connotaciones morales, tradiciones y la manera común de ser y vivir originan la nación, "este concepto de nación conduce al ser humano a la consecución del bienestar colectivo, al fortalecimiento de sus instituciones, a la defensa de su territorio y valores" (Salcedo, 2006), creando fundamentos de estudio como la seguridad.

> "La Doctrina de Seguridad Nacional - DSN es un cuerpo de enseñanza derivado de supuestas verdades, principios, normas y valores que un Estado, a través de sus propias experiencias o las de otros Estados y de conformidad con su Constitución Política y con las realidades del país, considera que debe llevar a la práctica para garantizar el desarrollo integral del hombre y de la colectividad nacional, preservándolos de interferencias a perturbaciones sustanciales de cualquier origen" (Humanos de la Organización de las Naciones Unidas, 1976).

Debido a un desarrollo integral, la mención colectiva, el individuo y su inserción necesitan ser estudiados bajo una teoría sistémica asociada con aspectos multidimensionales. La seguridad es deudora de la Teoría de Redes, rica en la tradición antropológica cultural (Scott, 1991). Las redes sociales son importantes porque explican como funcionan los mercados, como las organizaciones solucionan problemas o como cambia la sociedad. Existe sincronía entre una población compuesta por individuos diferentes y su relevancia no es estudiar las partes que forman un sistema complejo sino las interacciones entre todos sus elementos y las redes que forman (Mitchell Clyde, 1969).

Dentro de esta teoría, la escuela antropológica de Manchester explica que : primero, la insistencia en el conflicto más que en la cohesión como factor del mantenimiento y la transformación del grupo y, segundo, en consecuencia la visión de la estructura como redes relacionales analizables por técnicas específicas y como conceptos sociológicos basados en la Teoría del Conflicto (Lozares, 1996), que son funciones de la sociedad o una organización y cada participante individual y sus grupos se esfuerzan para maximizar sus beneficios, cual inevitablemente contribuye al cambio social, político y revoluciones. Si el conflicto deriva en reacciones de seguridad de parte de aquel que lo resiste, en la época contemporánea con

la revolución digital a tomado matices que hacen tener la necesidad de plantear esquemas de seguridad bajo el concepto de ciberespacio.

En el año 2018, el comunicado de prensa de la Unión Internacional de Telecomunicaciones - ITU, con la Comisión de Banda Ancha para el Desarrollo Sostenible y el Foro Económico Mundial, dan a conocer sus metas para el año 2025: 1) todos los países deben disponer de un plan o estrategia de banda ancha financiada, o incluir la banda ancha en sus definiciones de acceso y servicio 2) el porcentaje de microempresa, pequeñas y medianas empresas desconectadas debe haberse reducido un 50% por sector, y finalmente, 3) 40% de la población mundial debe utilizar servicios financieros digitales (Telecomunicaciones, 2018).

El interés de los organismos mundiales en áreas financieras, económicas, productivas…; hacia la inserción de la tecnología disruptiva (Fernández y Valle, 2018) busca denotar el conveniente aprendizaje de los actores, las relaciones estructurales y causalidad en la innovación inclusiva en las organizaciones (Martínez, Dutrénit, Gras, y Tecuanhuey, 2018). Con ello se provee también ciertos resultados indeseables de las actividades tecnológicas como lo son: el cibercrimen, ciberdelito o ciberdelincuencia que se describen como la forma genérica de aspectos ilícitos, como extorsiones, crimen, abuso, entre otras, perpetradas con ayuda de las tecnologías (Subijana, 2008) y ante el compromiso de estas actividades, es conveniente el fomentar condiciones mínimas de seguridad, beneficiosas desde *el usuario* y las autoridades reguladoras (Bitar, 2014).

Más allá de estas alternativas insatisfactorias, la seguridad informática, no es más que una variante de la seguridad en general, y por lo tanto, cabe destacar la importancia del factor humano en la mayoría de las fallas de seguridad informáticas (Martin, 2015) “En esta situación, la sensibilización y formación de los usuarios a procedimientos básicos de seguridad informática parece la opción que podría potencialmente dar mejores resultados, por un esfuerzo reducido” (Martin, 2015, pág. 16).

El internet y sus usuarios.

El Internet es conocido como una de las tecnologías más disruptivas del mercado (Manyika, Dobbs, Chui, y Bughin, 2013) a tal punto que integra los objetos físicos de la sociedad en la red, de forma que, transforma las actividades de las organizaciones y sociedad (Rosemann, 2014). Desde 1990, el creciente uso de internet la convierte hasta la actual línea de tiempo como lugar o espacio intangible de comercialización e interacción social. El glosario

informático ha incorporado una definición de este espacio como -ciberespacio" (Gubern, 2000).

Desde una concepción de la cultura digital en su integridad operativa, material, simbólica y organizativa, se derivan importantes consecuencias para el planteamiento y la comprensión de las implicaciones culturales de las innovaciones tecnológicas (Pierre, 2007). En base a lo expuesto por Pierre, define a la ciber cultura como "como el conjunto de los sistemas culturales surgidos en conjunción con las tecnologías de información y comunicación digitales"; se trata pues de "la cultura propia de las sociedades en las que las tecnologías digitales configuran decisivamente las formas dominantes tanto de información, comunicación y conocimiento como de investigación, producción, organización y administración (Lopera, 2012). Así, la cibercultura es "el conjunto de las técnicas (materiales e intelectuales), de las prácticas, de las actitudes, de los modos de pensamiento y de los valores que se desarrollan conjuntamente en el crecimiento" (Pierre, 2007, pág. 1). El ciberespacio, como la versión binaria del "mundo real" es al unísono con la ciber cultura, el espacio de relaciones por excelencia; resignifica fundamentalmente las díadas sujeto-mundo, sujeto-conocimiento y sujeto-sujeto (Ramirez, 2016).

El comportamiento de los usuarios de esta tecnología difiere su forma de uso según la educación de quien se involucra; quienes lo usen en respuesta al comercio electrónico y quienes lo hacen con propósitos de comunicación (Cano y Baena, 2015). En consecuencia, la regulación para su uso obliga a que el plan de un estado se interese en tres pilares que convergen esta área: la seguridad como condición, la institucionalidad como medio, y el desarrollo como objetivo (Sancho, 2017). En materia de seguridad cibernética, en América Latina, se presenta una agudeza en el uso de internet, pues posee infraestructuras propias con usos económicos vinculados al ciberespacio, por ende, el riesgo cibernético es un factor definitivo para incluir entre las variables de una evaluación de riesgo integral.

La ciber victimización responde a las consecuencias económicas y personales extensas para los usuarios de Internet, así como consecuencias negativas para las economías y la infraestructura cibernética. (Dodel y Mesch, 2017). Para los usuarios individuales, los impactos directos incluyen amenazas a sus activos digitales (dispositivos, sub - rendimiento de redes y software), acceso forzado a información privada y uso no autorizado de sus activos financieros (Clough, 2010). El entorno organizacional debe manejar las problemáticas de seguridad vinculadas a usos "tradicionales" de la tecnología (Martin, 2015), pero también a otros relativamente nuevos del ciberespacio que tienen impactos

notables, directamente o vía efectos mosaico sobre su actividad. *Véase* Los factores de Riesgo y la competencia de autores de crimen, el gobierno y el sector privado que presenta la tabla 1.

Tabla1.
Factores de riesgo en ciberespacio.

Autoría	**Gobierno**	**Sector privado**
Ataques patrocinados por otros Estados	Espionaje ataques contra infraestructuras críticas, amenazas persistentes avanzadas	Espionaje ataques con infraestructura críticas, APT
Ataques patrocinados por privados	Espionaje	Espionaje
Terroristas, de extremismo político o ideológico.	Ataques contra redes de sistemas; contra servicios de internet; infección con malware, ataques contra redes, sistemas o servicios de terceros	Ataques contra redes de sistemas; ataques contra servicios de internet; infección con malware, ataques contra redes, sistemas o servicios de terceros
Hacktivista	Robo y publicación de información clasificada o sensible, ataques contra las redes y sistemas, ataques contra servicios de internet, ataques contra redes, sistemas o servicios de terceros	Robo y publicación de información clasificada o sensible, ataques contra las redes y sistemas, ataques contra servicios de internet, ataques contra redes, sistemas o servicios de terceros
Crimen organizado	Espionaje	Robo de identidad digital y fraude
Ataques de bajo perfil	Ataques contra las redes y sistemas, ataques contra servicios de internet, infección con malware, ataques contra redes, sistemas o servicios de terceros	Ataques contra las redes y sistemas, ataques contra servicios de internet, infección con malware, ataques contra redes, sistemas o servicios de

		terceros
Ataques de personal con accesos privilegiados (Insiders)	Espionaje, ataques contra infraestructuras críticas, ataques contra las redes, sistemas o servicios de terceros, robo y publicación de información clasificada o sensible, APT - amenazas avanzada persistente	Espionaje, ataques contra infraestructuras críticas, ataques contra las redes, sistemas o servicios de terceros, robo y publicación de información clasificada o sensible, APT - amenazas avanzada persistente

Nota: Recuperada de (Sancho, 2017)

Una línea base de investigación que refleje las determinantes de conductas de seguridad cibernética que se evalúan a través del modelo de creencias de salud como predictor de una conducta protectora con medidas de valor, permiten conformar estrategias de acción en base a los comportamientos de empleados y sociedad en general, desde este punto, se provee *diagnosticar variables de conducta en los empleados que determinan conductas de seguridad cibernética en las empresas a través del MCS con el propósito fomentar una cultura organizacional con bases en la seguridad interconectada para las empresas y también para el entorno que la conforman.*

Materiales y Métodos

Modelo de Creencia de Salud.

La psicología cognitiva ha intentado explicar el ocurrir de la conducta protectora de la salud con varios modelos; Modelo de Creencia de Salud (Becker, 1974), Teoría de la Utilidad Subjetiva Esperada Edwards (Edwards, 1954), Teoría de la Motivación para la Protección (Rogers, 1975), Teoría de la Acción Razonada Ajzen (Ajzen y Fishbein, 1980), Teoría de la autosuficiencia (Bandura, 1977). El primer modelo se ha convertido hasta la fecha en el más usado con mayor número de investigaciones generadas, pero también con resultados de estudios opuestos por la no correlación hacia los comportamientos de salud. Sin embargo, es el modelo sistemáticamente más usado y citado para exponer las acciones de prevención de enfermedades, respuesta de síntomas, y a enfermedades, asi como otros diversos patrones comportamentales con efectos de salud (Cabrera, Tascón, y Lucumí, 2001).

La motivación de un estudio a través del Modelo de Creencia de Salud permite entender la razón de conductas como la prevención, evitación, y la respuesta a síntomas, intentando relacionar estos puntos a la exposición de virus y formas de ataques o infecciones para efectuar los ciber delitos, asi también intentando entender las secuelas por infecciones a los puntos terminales de las empresas, o llámese también computadoras o dispositivos. La conducta del modelo está determinada por dos variables: a) El valor que se atribuye a una meta y b) la probabilidad de existir esa meta ante los esfuerzos que demande (Maiman y Becker, 1974) el equivalente se refleja al deseo de un usuario de internet o internauta que labora en una empresa de no ser infectado y el creer en actividades y hábitos correspondientes a evitar o restaurar su seguridad.

La *susceptibilidad, la severidad, los beneficios y las barreras percibidas* son dimensiones que constan en el Modelo de Creencias de Salud – MDS. Rosenstock (1996), esclarece las dimensiones para el modelo:

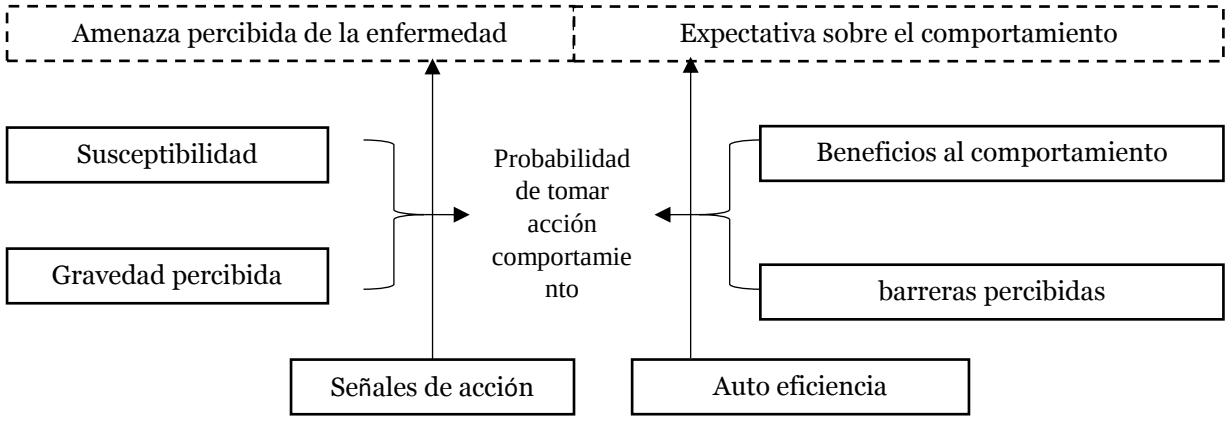

Figura 1. The Health Belief Model as a predictor of health preventive behavior. Basado en (Rosenstock I. , 1974)

Percepción de susceptibilidad. - La susceptibilidad percibida ante un determinado problema de salud, es la dimensión que valora cómo los sujetos varían en la percepción de la propia vulnerabilidad a enfermar. Se refiere fundamentalmente a la percepción subjetiva que tiene cada ser humano sobre el riesgo de caer enfermo (Rosenstock M. , 1996, pág. 47). En el entorno organizacional se postula el conocer la vulnerabilidad que el trabajador cree tener en la organización en la que trabaja. Se relaciona este punto al grado en el que un trabajador concibe los ataques informáticos y exposición de virus en los entornos organizacionales de otras empresas y en su propia organización.

Conductas de seguridad informática se relacionan con la creencia en la susceptibilidad personal por infección de un virus y la posibilidad a que ese virus afecte la información o la infección refiera a canales espías (Liang & Xue, 2010).

Percepción de gravedad. - La *severidad o gravedad percibida* se describe como la dimensión a la probabilidad de contraer tipológicamente un padecimiento o no tratar de alguna forma con el padecimiento. Dimensión que contemplan dos tipos de consecuencias de la pérdida de la salud; médico clínicas (muerte, incapacidad o dolor), y consecuencias sociales (pérdida de relaciones sociales, los efectos sobre la capacidad laboral del sujeto o sobre sus relaciones familiares, etc.) (Moreno & Gil, 2003).

Los medios relacionales a la primera son la perdida de información, extorsión, encryptos y al segundo tipo corresponden los males sociales, pues son sujetos de exposición documental, motivación a la sustanciación del crimen organizado y el mal concepto al uso de procesos digitales (compras en línea). MgGuire afirma que (2013) “la vulnerabilidad de los usuarios móviles y de internet a malware, los intentos de phishing y el robo de identidades tienen

consecuencias negativas no únicamente en el usuario, los daños son considerables en la infraestructura digital y la economía nacional." (pág. 75) Esta dimensión recupera las fases cognitivas referentes hacia la posibilidad de no ser atacado, el serlo y el peligro inminente de haber sido infectado o afectado por riesgos propios de ciber delincuencia.

Dimensiones de susceptibilidad y gravedad avalan conductas que deben favorecer al sujeto a denotar conductas saludables, sin embargo, ambas no contemplan totalmente dichas conductas hasta que considere una efectiva respuesta por adoptar una conducta propia ante los índices e estas dimensiones (De Roux, 1994).

Beneficios percibidos. - El sujeto debe percibir *efectividad relativa o beneficios a conductas* de salud que se practiquen. Esto nos lleva a entender los beneficios que se perciben del comportamiento preventivo. "Asumiendo que las creencias del sujeto respecto a los cursos de acción que dispone están influidas por las normas e incluso presiones del grupo social al que pertenece" (Rosenstock I. , 1974, págs. 328-334).

Un ejemplo al que se debe referir es el tomar medidas preventivas contra la amenaza. El internauta debe creer que un software antivirus puede protegerlo ante amenazas (Lee, Larose, y Rifon, 2008). A ello también se analiza si el antivirus es el único medio por el cual un trabajador cree tener seguridad, reconocimiento a posibles ataques y seguridad de información personal.

Barreras percibidas. - Aspectos contradictorios de la conducta de salud beneficiosa, funcionarían como barreras para la acción que encadenan las anteriores dimensiones (Moreno y Gil, 2003, pág. 95). El sujeto puede reflexionar un determinado curso de acción como realmente efectivo para enfrentarse a un trastorno de salud o "ataque", pero, al mismo tiempo, puede verlo como costoso, desagradable o doloroso; siendo barreras para la acción de las dimensiones del modelo (Moreno y Gil, 2003, pág. 96).

Para este punto, las variables sociodemográficas son influyentes en los comportamientos tales como la edad, nivel de educación y la frecuencia de uso de herramientas digitales.

Señales para la acción. - Para desencadenar el proceso en la toma de decisiones, existen los conocidos estímulos o señales de para la acción (Janz y Becker, 1984). La intensidad necesaria de una de estas claves para desencadenar la conducta puede variar de sujeto a sujeto, e incluso en el mismo sujeto dependiendo de sus niveles de susceptibilidad y del grado de severidad percibida (Moreno y Gil, 2003). En el MCS estas señales asumen un entorno externo (experiencias previas) e interno (conductas preventivas), la intensidad de ambas serán

determinantes a la hora de evaluar los comportamientos preventivos en sus dimensiones. Para entender el resultado final, el modelo considera varias opciones que representan diferentes valores de las dimensiones y que se reflejarán en forma de conductas distintas frente a la salud y/o la enfermedad.

En conclusión, el modelo funciona de manera lógica contemplando un hipotético análisis interior de costes, beneficios para el sujeto en el curso y acción de sus actividades, quien sopesaría la efectividad de la acción a tomar, así como los posibles costes de tomarla (Janz y Becker, 1984).

Considerando que existe un conceso que las amenazas de seguridad cibernética son motivo de preocupación y las consecuencias de los delitos se miden en millones de dólares (Anderson & R, 2010) "y considerando también la adopción de medidas preventivas y de protección, paralelo al comportamiento del modelo en mención, es la razón por la cual la ciencias psicológicas y sociales participan más en la contextualización y el estudio de la seguridad cibernética" (Dodel & Giustavo, 2016).

La motivación de entender cómo y hacia donde los hábitos de empleados en las empresas están siendo dirigidos permiten contextualizar los índices de exposición al crimen cibernético de las empresas y la cultura preventiva que está construyendo el sector empresarial, también el tener una línea base para las prontas estrategias que las actividades comerciales demandaran y con ello está implícito el ámbito de seguridad de una empresa y la información que maneja.

Los datos obtenidos fueron recabados al personal de afiliados de un total de 243 empresas estableciendo medidas de valor a los componentes del Modelo de Creencia de Salud; explicados en la tabla 2.

Tabla 2

Dimensiones al Modelo de Creencia de Salud considerando infecciones informáticas y ciber delitos

Componente	Dimensiones
Comportamiento preventivo	Antivirus o antimalware considerados principales contramedidas de seguridad cibernética (Choi, 2008).
Susceptibilidad percibida	Vulnerabilidad relativa percibida para sí mismo y hacia una persona (Harris y Guten, 1979).

Gravedad percibida	Evaluación del conocimiento ante amenazas digitales tienen consecuencias en las unidades atacadas y afectan negativamente al usuario (Liang y Xue, 2010).
Beneficios percibidos	Creencia en la eficacia del comportamiento digital de protección contra amenazas digitales. (Lee, Larose, y Rifon, 2008)
Barreras percibidas	Costos al participar en una conducta definida.
Experiencias previas	Los usuarios podrían no están conscientes de la presencia de malware. (Yar, 2013) Percepción a errores de software o información perdida debido a un virus informático. (Holt y Turner, 2012)
Auto eficiencia	Ámbitos de la seguridad cibernética que fue puesta en práctica como una forma de autoevaluación respecto a la capacidad para proteger sus ordenadores personales. (Rhee, Kim, y Ryu, 2009)
Estatus socio demográfico	Variables sociológicas tradicionales y acercamientos a dispositivos digitales.

Nota: Elaboración propia

Mediante las encuestas se conoció la opinión o valoración del sujeto seleccionado en la muestra habiendo aplicado como herramienta de investigación, el cuestionario. A partir de los componentes y dimensiones se elabora un cuestionario que resumen la tendencia más relevante hacia variables para la construcción de interpretaciones con preguntas que revelen el perfil del encuestado y su frecuencia en el uso de dispositivos digitales, también se estructuró preguntas a responder en una escala de Likert siendo 1 - *Muy fácil* y 5 *Muy difícil* cuyo índice de confiabilidad fue aceptable para la aplicación (α de Cronbach 0,800) y finalmente preguntas dicotómicas que evalúan el comportamiento preventivo y experiencias previas.

La pregunta central para la investigación de este estudio fue: ¿Cuáles son los principales determinantes de las conductas preventivas de seguridad cibernética?

Diseño muestral

El alcance del estudio es de interés descriptivo – correlacional ya que "busca especificar propiedades, características y rasgos importantes del fenómeno que se analiza además que se describe tendencias de la población y el hecho de saber que dos variables se relacionan aporta más explicación" (Sampieri, 2010, págs. 92-94). Se especifican en las participaciones, las características y los perfiles de empleados en las organizaciones a las que está dirigido el estudio revelando los principales determinantes de las conductas preventivas de la seguridad cibernética y lo razonable que es el Modelo de Salud como predictor a la adopción de estas conductas a personas que laboren en el entorno de las empresas.

El proceso desarrollado es especialmente cualitativo pero apoyado parcialmente en variables cuantitativas que responden a los componentes del modelo propiciando construcciones e interpretaciones de los datos revelados (Galeano, 2004).

La técnica de investigación a aplicarse es la encuesta, para lograr comprender con información directa desde ámbitos y áreas de la cultura organizacional.

Tamaño de la muestra

Para el muestreo se seleccionó a la población que representa al número de afiliados al Instituto Ecuatoriano de Seguridad Social-IESS con un nivel de confianza del 95% y margen de error del 5%, la población objetivo cuenta con la participación del personal afiliado según provincia de Pichincha perteneciente a la República del Ecuador (35.17%) es un total de 1.033.790 empleados (INEC, 2018) siendo el número correspondiente a la muestra, 385 afiliados al IESS. Se considero también el analizar el sector corporativo para conocer la intencionalidad cognitiva en ciber seguridad a la que el personal se expone por parte de las empresas, este punto, como parte de los estímulos o señales que el modelo de la investigación participa. Se planteo realizar el diagnostico al personal afiliado según la forma institucional respecto al porcentaje de personal afiliado a la seguridad social, como lo especifica la tabla 3:

Tabla 3.

Porcentaje de afiliados asociados al número de encuestas.

Forma institucional	Porcentaje Ecuador	Numero de encuestas
Sociedad con fines de lucro	43,50%	168
Institución Pública	19,17%	74
Persona Natural no obligado a llevar contabilidad	18,48%	71

Persona Natural obligado a llevar contabilidad	8,70%	34
Sociedad sin fines de lucro	4,84%	18
Empresa Pública	2,28%	8
Régimen simplificado RISE	1,93%	7
Economía Popular y Solidaria	1,10%	5

Fuente: Elaboración propia.

Resultados

La tabla 4 presenta las características del perfil del encuestado y una descripción resumida de los datos. La participación por géneros fue casi equitativa (49.5% masculino). El nivel de educación de los encuestados se encontró en un 75.4% en el tercer nivel académico y las edades correspondientes fueron de 32 años con una desviación estándar de 11.17 años.

En cuanto a la cotidianidad de uso de internet, el promedio de años que los encuestados llevan haciendo uso de internet es de 12 años (DS 5.84 años) y la frecuencia con la que ha venido trabajando en un dispositivo conectado a la red según la escala de Likert aplicada es frecuente (índice de 4.45/5).

Tabla 4.
Estadísticos descriptivos

Dimensiones	N	Suma	Media	Desviación estándar	Varianza
Edad	398	12904	32,42	11,175	124,889
Tiempo uso de internet	397	5111	12,87	5,843	34,146
Frecuencia de uso de internet y dispositivos digitales	398	1771	4,45	,940	,883
Crimen cibernético afecte a las organizaciones	398	1044	2,62	1,057	1,117
Crimen cibernético afecte a su empresa	398	1093	2,75	1,130	1,278
Posibilidad a que alguien use su tarjeta de crédito sin su consentimiento	398	1314	3,30	1,187	1,410
Posibilidad de perder información debido a un virus.	398	1097	2,76	1,124	1,263
Posibilidad de perder información almacenada en un dispositivo y que tomen beneficio de esta	398	1039	2,61	1,107	1,226
Nivel de reconocimiento a correos falsos y o paginas inseguras a pagos en línea	398	1281	3,22	1,168	1,365
Posibilidad a que tomen control remoto/distancia o presencial de su computadora para des beneficiarla/o	398	1295	3,25	1,085	1,177

Posibilidad que alguien cree una cuenta en Facebook falsa de usted	398	1092	2,74	1,246	1,551
Disponibilidad de costo para protegerse	398	1028	2,58	1,082	1,171
Tiempo que dispone para prevención	398	1218	3,06	1,058	1,120
Costo que asume para la prevención	398	1310	3,29	,979	,958

Nota: Elaboración propia.

La tabla 5 entregó resultados de interacción entre las categorías de evaluación de forma independiente, demostrando que las variables por si solas interactúan de forma moderada para estudiar la dimensión a la que corresponden. Los datos analizados consideran la significación de la herramienta debido a que el estudio de correlaciones de la misma población en un posterior caso de estudio tendrá resultados serán consistentes y la probabilidad al cambio es o%.

Las dimensiones de susceptibilidad y severidad percibida son las dimensiones con mayor relación en cómo interactúan las categorías. La relación en la susceptibilidad a ataques en otras organizaciones y ataques en su propia empresa corresponde a una correlación de Pearson modera (0.672 r – ,000 sig), demostrando que los entornos empresariales existe una relación recíproca entre estas dos categorías pertenecientes a una misma dimensión; también existe el caso de la severidad percibida por colaboradores pues perder información almacenada en un dispositivo y reconocer a correos falsos y/o paginas inseguras a pagos en línea se relacionan en esta categoría en la misma dimensión.

Tabla 5.

Correlaciones entre variables

Dimensiones	Susceptibilidad		Severidad			Beneficios			Barreras	
Categorías	1	2	3	4	5	6	7	8	9	10
1. Crimen cibernético afecte a las organizaciones	1	.672 r .000sig	.255 r .000sig	.393 .000sig	.449 .000sig	.185 r .000sig	.273 r .000sig	-.060 r .231sig	.135 r .007sig	.241 r .000sig
2.Crimen cibernético afecte a su empresa		1	.335 r .000sig	.407 r .000sig	.488 r .000sig	.246 r .000sig	373 r .000sig	-.061 r .228sig	.196 r .000sig	.218 r .000sig

3.Posibilidad a que alguien use su tarjeta de crédito sin su asenso	1	.606 r .000sig.	.444 r .000sig	.254 r .000sig	.482 r .000sig	-.179 r .000sig	.186 r .000sig	.043 r .390sig
4. Posibilidad de perder información almacenada en un dispositivo y que tomen beneficio de esta		1	.679 r .000sig	.211 r .000sig	.561 r .000sig	-.164 r .001sig	.207 r .000sig	.142 r .000sig
5. Nivel de reconocimiento a correos falsos y o paginas inseguras a pagos en línea			1	.208 r .000sig	.458 r .000sig	-.085 .089sig	.136 r .007sig	.188 r .000sig
6. Posibilidad a que tomen control remoto/distancia o presencial de su computadora para des beneficiarla/o				1	.312 r .000sig	.065 r .199sig	.368 r .000sig	.236 r .000sig
7. Posibilidad que alguien cree una cuenta en Facebook falsa de usted					1	-.097 .000sig	.256 r .000sig	.142 r .005sig
8. Seguridad en claves.						1	.123 r .014sig	.150 .003sig
9. Tiempo que dispone para prevención							1	.414 r .000sig
10. Costo que asume para la prevención								1

Nota : Elaboración propia.

La tabla 6 establece una correlación alta y significativa entre las categorías de las dimensiones del Modelo de Creencia de Salud denotando valores que favorecen a su explicación; en tanto se aprecia que los crímenes cibernéticos tanto internos (,908** r; sig. ,000) como externos (,920**r; sig. ,000) se relacionan altamente a la susceptibilidad de seguridad a la que un empleado concibe en su trabajo y en las empresas en general; de igual forma sucede en las amenazas que deben confrontar ya sea con implicaciones a extorsión en tarjetas de crédito (0,816**r - sig. 0,000), reconocer correos falsos (,828**; sig. ,000) y el que tomen

información de su computadora (0,897** - sig. ,000); las dimensiones de las barreras y los beneficios también demuestran estar relacionadas con las sus respectivas categorías.

Tabla 6

Correlaciones entre Variables- Dimensión

Dimensiones	Susceptibilidad	Amenaza	Beneficios	Barreras
1. Crimen cibernético afecte a las organizaciones	,908**	,429**	,199**	,224**
	,000	,000	,000	,000
2.Crimen cibernético afecte a su empresa	,920**	,482**	,281**	,246**
	,000	,000	,000	,000
3.Posibilidad a que alguien use su tarjeta de crédito sin su consentimiento	,324**	,816**	,272**	,135**
	,000	,000	,000	,007
4. Posibilidad de perder información almacenada en un dispositivo y que tomen beneficio de esta	,438**	,897**	,297**	,207**
	,000	,000	,000	,000
5. Nivel de reconocimiento a correos falsos y o paginas inseguras a pagos en línea	,513**	,828**	,289**	,193**
	,000	,000	,000	,000
6. Posibilidad a que tomen control remoto/distancia o presencial de su computadora para des beneficiarla/o	,237**	,266**	,724**	,358**
	,000	,000	,000	,000
7. Posibilidad que alguien cree una cuenta en Facebook falsa de usted	,355**	,591**	,606**	,236**
	,000	,000	,000	,000
8. Seguridad en claves	-,066	-,170**	,554**	,163**
	,189	,001	,000	,001
9. Tiempo que dispone para prevención	,182**	,209**	,393**	,837**
	,000	,000	,000	,000
10. Costo que asume para la prevención	,251**	,145**	,281**	,845**
	,000	,004	,000	,000

Nota: Elaboración propia.

En la *tabla 7*, entregó resultados de un analisis de correspondencia donde se considera la dimensión auto eficiencia de los encuestados hacia los males cibernéticos y explica bajo un analisis de correspondencias con un valor significativo al estudio (.000sig) definiendo la existencia de una relación de los atributos conceptualizados en una escala de Likert (1- 5; muy fácil – muy difícil) y las dimensiones prestadas por el modelo en el plano del valor que se atribuye a una meta y el plano de lograr esta meta al creer en actividades y hábitos correspondientes a evitar o restaurar su seguridad, es decir, autosuficiencia. La inercia de los datos se puede reflejar en solo dos dimensiones pues acumula la información necesaria para

las posteriores interpretaciones (acumulado de 98.9%). La correlación de las dimensiones es de -0.047

Tabla 7.
Análisis de correspondencias del MCS analizando el comportamiento y la auto eficiencia.

Dimensión	Valor singular	Inercia	Chi cuadrado	Sig.	Proporción de inercia		Valor singular de confianza	
					Contabilizado para	Acumulado	Desviación estándar	Correlación 2
1	,156	,024			,766	,766	,014	-,047
2	,084	,007			,222	,989	,015	
3	,016	,000			,008	,997		
4	,010	,000			,003	1,000		
Total		,032	139,230	,000[a]	1,000	1,000		
a. 16 grados de libertad								

Nota: Elaboración propia.

La *tabla número 8* explica de qué manera los datos aportan en la explicación de las correspondencias y el analisis de datos en las dimensiones del gráfico. De la *tabla 9* correspondencias por filas generales, el atributo *Fácil* aporta mayormente a la dimensión 1 (0,319) y el *Muy difícil* a la segunda dimensión *(0.661)*; de la *tabla 10* de correspondencias por columna la dimensión del modelo Auto eficiencia tiene aportes mayormente significativos en las dimensiones 1 (0,471) y 2 (0,368) de las correspondencias.

Tabla 8.
Tabla de correspondencias

Atributo	Dimensiones					
	Susceptibilidad	Amenaza	Beneficios	Barreras	Auto eficiencia	Margen activo
Muy fácil	103	139	112	84	12	450
Fácil	288	347	307	250	75	1267
Neutral	207	308	316	233	134	1198
Difícil	153	271	299	172	139	1034
Muy difícil	45	124	160	57	38	424
Margen activo	796	1189	1194	796	398	4373

Nota: Elaboración propia.

Tabla 9.
Puntos de fila generales

Atributo	Masa	Puntuación en dimensión		Inercia	Contribución				
					Del punto en la inercia de dimensión		De la dimensión en la inercia del punto		
		1	2		1	2	1	2	Total
Muy fácil	,103	-,599	-,309	,007	,237	,117	,865	,124	,989
Fácil	,290	-,415	,040	,008	,319	,005	,990	,005	,995
Neutral	,274	,128	,225	,002	,029	,165	,355	,590	,944
Difícil	,236	,421	,136	,007	,268	,052	,932	,052	,984
Muy difícil	,097	,487	-,757	,008	,147	,661	,433	,565	,998
Total, activo	1,000			,032	1,000	1,000			

a. Normalización simétrica

Fuente: Elaboración propia.

Tabla 10.
Puntos de columna generales

Dimensiones	Masa	Puntuación en dimensión		Inercia	Contribución				
					Del punto en la inercia de dimensión		De la dimensión en la inercia del punto		
		1	2		1	2	1	2	Total
Susceptibilidad	,182	-,550	,192	,009	,352	,079	,933	,061	,994
Amenaza	,272	-,072	-,170	,001	,009	,093	,223	,677	,901
Beneficios	,273	,267	-,318	,005	,125	,327	,563	,429	,993
Barreras	,182	-,193	,247	,002	,044	,132	,495	,436	,932
Auto eficiencia	,091	,899	,583	,014	,471	,368	,814	,185	,999
Total activo	1,000			,032	1,000	1,000			

a. Normalización simétrica

Fuente: Elaboración propia.

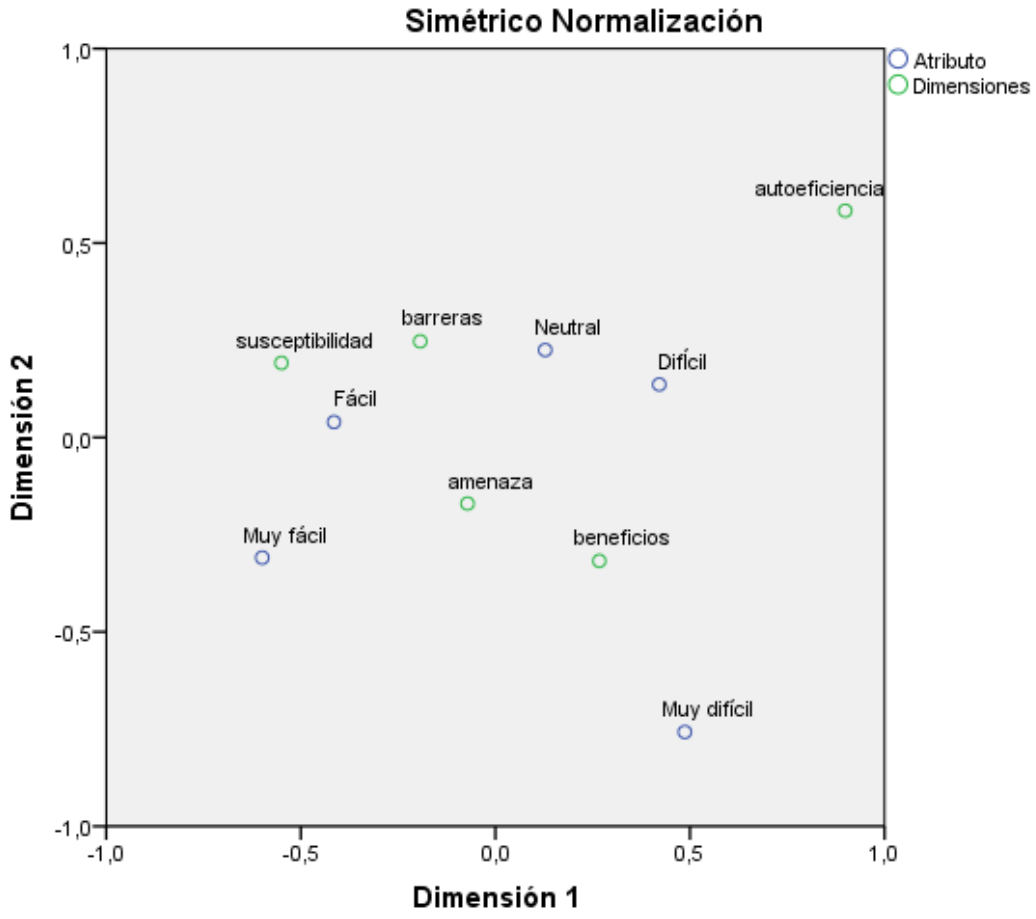

Figura 2

Dimensiones de las correspondencias.

En la *tabla 11* del analisis del Analisis de correspondencias del MCS analizando el comportamiento sin la consideración de la dimensiones del modelo de *auto eficiencia* , entregó resultados de un analisis de correspondencia de un valor significativo al estudio (.000sig) definiendo la existencia de una relación de los atributos conceptualizados en una escala de Likert (1- 5; muy fácil – muy difícil) y las dimensiones prestadas por el modelo en el plano del valor que se atribuye a una meta donde la correlación de las dimensiones es de es positiva de con un valor de Pearson de (0.014).

Tabla 11

Analisis de correspondencias del MCS analizando el comportamiento sin auto eficiencia.

Dimensión	**Chi cuadrado**	**Sig.**	**Proporción de inercia**		**Valor singular de confianza**	
			Contabilizado para	**Acumulado**	**Desviación estándar**	**Correlación 2**
1			,926	,926	,015	,014
2			,068	,994	,016	
3			,006	1,000		

Total	70,627	,000[a]	1,000	1,000		

Fuente: Elaboración propia.

Discusión

Las victimas con experiencias previas en ciber delitos corresponden el 19% de los encuestado, pues, ha experimentado extorciones con su tarjeta de crédito, y un 68.6% ha experimentado fallas de software o problemas en sus dispositivos digitales. Estos porcentajes aclaran comportamientos posteriores de estimulación preventiva interna considerada dentro del modelo. Por otro lado, el 62% de encuestados conoce de víctimas cercanas a estos delitos y el 14.8% ha sentido amenazas respecto al uso ilegal de información y cuentas personales. Estos dos últimos porcentajes corresponderían a la estimulación externa en el comportamiento preventivo.

Sobre la *susceptibilidad percibida*, los encuestados asumen ligeramente que es más fácil que una empresa ajena sea expuesta a un ataque por virus y que esta afecte a las computadoras o empresa respecto a su misma empresa. En términos generales, el empleado de una empresa siente que es fácil ser atacado por algún virus (índice promedio de 2.94/5) según la escala de Likert aplicada, los valores tanto del índice de suma y todas las variables individuales fueron sesgadas hacia valores más altos.

El índice por *severidad percibida* fue de 2.89/5, describiendo que los encuestados no se sienten amenazados mayormente por los delitos de la web y en contraste a este valor se evidencia en relación hacia una *disposición para la protección* de sus actividades que arroja índices muy bajos, es decir, la disponibilidad en cuanto tiempo, costo y esfuerzos es nula según el índice que se le confiere (muy deficiente 1.21/5).

Los beneficios de una actividad de prevención más básica y comúnmente aceptada para actividades en la web es la instalación de antivirus, otras medidas también implican medidas de seguridad para evitar el acceder cuentas con información valiosa. Los encuestados asumieron que solo el 63.4% de ellos usa un antivirus y el 7.5% usa otros medios de seguridad. El 17.6% de los encuestados es indiferente a la seguridad informática.

Los valores de la población en entornos empresariales ante amenazas percibidas a la enfermedad de ciber-delito son altas, pese a esta percepción, sus hábitos para una prevención o expectativa a mejorar la situación actual en términos de vulnerabilidad o exposición, es considerada como difícil. De modo que el modelo de creencia a la salud digital es susceptible al ciberdelito fácilmente, indiferente al riesgo o severidad que alguien use su tarjeta de crédito y se beneficie de ella sin su consentimiento, no adoptando conductas beneficiosas en su navegación como tiempo y costo, permitir inquirir que el nivel de auto - eficiencia es indiferente.

Las contribuciones de las dimensiones del *Grafico 3* determinaron que la población percibe como difícil el crear hábitos y actividades que le permitan estar protegidos de males en sus computadoras y el uso de internet, es decir, se vio susceptible y amenazado en su entorno; barreas como costo y tiempo le hacen percibir indiferencia a la seguridad cibernética. La correlación de las dimensiones es negativa pudiendo ser las injerencias de mayor susceptibilidad, menor auto eficiencia para responder a estos males. Tal injerencia es refutable pero la auto eficiencia se ajusta no solo a señales de acción sino también a las barreras percibidas.

De tal manera en respuesta a la Hipótesis plateada ¿Es el Modelo de Creencia de Salud un predictor razonable de la adopción de conductas preventivas ciber-seguridad para los usuarios de Internet? La relevancia de los datos analizados se presenta cuando considerada la significación de la herramienta debido a que el estudio de correlaciones de la misma población en un posterior caso de estudio tendrá resultados que serán consistentes y la probabilidad al cambio es o%, establecido así por el Modelo General lineal.

Lista de referencias

Álvarez, A. (2007). La seguridad desde los clásicos y su influencia en la Doctrina. *Historia de la seguridad*, 1-10.

Anderson, C., & R, A. (2010). Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions . *Management Information Systems Research Center,*, 23.

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

Becker, M. (1974). The health belief model and illness behavior. *Health Education Monographs*, 2.

Bitar, S. (2014). Las tendencias mundiales y el futuro de América. *CEPAL. Serie de Gestión Pública*, 3-8.

Choi, K. S. (2008). Computer crime victimization and integrated theory: An empirical assesment. *International Journal of Cyber Criminology*, 333.

Clough, J. (2010). Principles of cybercrime. Principles of Cybercrime. *Cambrige University Press*.

De Roux, G. I. (1994). La prevención de comportamiento de riesgos y la promición de estilos de vida saludable en el desarrollo de salud. *Educación Médica y Salud*, 226.

Dodel, M., & Giustavo, M. (2016). Las computadoras en el comportamiento humano. *El Sevier*, 2.

Edwards, W. (1954). The theory of decision making. *Psychological Bulletin*, 51.

Galeano, M. E. (2004). *Estrategias de investigación social cualitativa: el giro en la mirada.* Medellín, Colombia: La Carreta.

Gubern, R. (2000). El eros electrónico. *Taurus*, 41-47.

Humanos de la Organización de las Naciones Unidas. (1976). *Revista de las Fuerzas Armadas*, 83.

INEC, I. N. (Octubre de 2018). *Directorio de empresas y establecimientos 2017.* Obtenido de Ecuador en Cifras: http://www.ecuadorencifras.gob.ec

Liang, H., & Xue, Y. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association for Information*, 394-410.

Lopera, H. (2012). Los estudios de la cibercultura. *Research Gates*, 9-11.

Lozares, C. (1996). La teoria de redes sociales. *Universitat Autbnoma de Barcelona*, 103-126.

M McGuire, S. D. (2013). Cybercrime a review of the evidence. *Home Office Research Report*, 75.

Martin, P.-E. (2015). Inseguridad cibernética en América Latina: Líneas de reflexión para la evaluación de riesgos. *Instituto Español de Estudios Estrategicos*, 5-9.

Martin, P.-E. (2015). Inseguridad Cibernética en América Latina: Líneas de reflexión para la evaluación de riesgos. *Instituto Español de Estudios Estrategicos* , 79.

Mitchell Clyde, J. (1969). The Concept and Use of Social Networks. *Analyses of Personal Relationships in Central African Towns*, 1-50.

Moreno, E., & Gil, J. (2003). El Modelo de Creencias de Salud: Revisión Teórica, Consideración Crítica y Propuesta Alternativa. I: Hacia un Análisis Funcional de las Creencias en Salud. *nternational Journal of Psychology and Psychological Therapy*, 91-109.

Ojeda, J., Jiménez, P., Quintana, A., Crespo, G., & Viteri, M. (2015). Protocolo de investigación. (U. d. ESPE, Ed.) *Yura: Relaciones internacionales, 5*(1), 1 - 20.

Pierre, L. (2007). *CIBERCULTURA: Informe al consejo de Europa.* Barcelona: Anthropos Editorial.

Ramirez, S. (2016). CIBER-HUMANIDAD. *Research Gates*, 1.

Rogers, R. (1975). A protection motivation theory of fear appeals and attitude change. *Journal of Psychology*, 91.

Rosemann, M. (2014). The Internet of Things – New digital capital in the hand of customers. *Business Transformation Journal*, 6-15.

Rosenstock, I. (1974). Historical origins of the health belief model. *Health Education Monographs*, 328-335.

Rosenstock, M. (1996). The health belief model and preventive health behavior. *Health Education Monographs*, 2.

Salcedo, A. (2006). La Seguridad Social en la Fuerza Armada Nacional.

Sampieri, R. (2010). *Metodologia de la Investigacion.* México: McGRAW - HILL.

Sancho, C. (2017). Ciberseguridad. Presentación del dossier. *Revista Latinoamerica de Estudios de Seguridad*(20), 8-15.

Scott, J. (1991). Social Network Analysis. *Newbury Park*.

Subijana, I. J. (2008). El ciberterrorismo: Una perspectiva legal y judicial. *Eguzkilore*, 169-188.

Telecomunicaciones, U. I. (23 de Enero de 2018). *La Comisión de la Banda Ancha para el Desarrollo Sostenible lanza metas de 2025 para "Conectar la otra mitad"*. Obtenido de [Comunicado de prensa]: https://www.itu.int/es/mediacentre/Pages/2018-PR01.aspx

Yar, M. (2013). Cybercrime and society. *Sage*.