

**UNIVERSIDAD PERUANA UNIÓN**  
FACULTAD DE INGENIERÍA Y ARQUITECTURA  
Escuela Profesional de Ingeniería de Sistemas



*Una Institución Adventista*

**Métodos de apoyo a la concientización del factor humano al  
implementar un sistema de gestión de seguridad de la  
información en una organización**

Por:

Moisés Pinedo Torres

Asesor:

Ing. John Clark Santa María Pinedo

**Tarapoto, diciembre de 2019**

## DECLARACIÓN JURADA DE AUTORÍA DE TRABAJO DE INVESTIGACIÓN

Ing. John Clark Santa María Pinedo, de la Facultad de Ingeniería y Arquitectura, Escuela Profesional de Ingeniería de Sistemas, de la Universidad Peruana Unión.

### **DECLARO:**

Que el presente informe de investigación titulado: "Métodos de apoyo a la concientización del factor humano al implementar un sistema de gestión de seguridad de la información en una organización" constituye la memoria que presenta el estudiante Pinedo Torres Moisés; para aspirar al Grado Académico de Bachiller en Ingeniería de Sistemas, cuyo trabajo de investigación ha sido realizado en la Universidad Peruana Unión bajo mi dirección.

Las opiniones y declaraciones en este informe son de entera responsabilidad del autor, sin comprometer a la institución.

Y estando de acuerdo, firmo la presente constancia en Morales, a los 02 días del mes de diciembre del año 2019.

Asesor

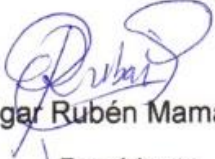
Ing. John Clark Santa María Pinedo

Métodos de apoyo a la concientización del factor humano al implementar un sistema de Gestión de seguridad de la información en una organización

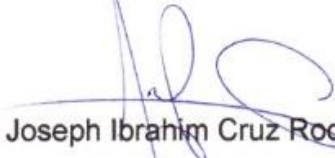
## TRABAJO DE INVESTIGACIÓN

Presentado para optar el Grado de Bachiller en Ingeniería de Sistemas

### JURADO CALIFICADOR

  
Dr. Edgar Rubén Mamani Apaza  
Presidente

  
Mg. Danny Lévano Rodríguez  
Secretario

  
Mg. Joseph Ibrahim Cruz Rodríguez  
Vocal

  
Ing. John Clark Santa María Pinedo  
Asesor

Tarapoto, 02 diciembre de 2019

## Resumen

Este artículo tiene como objetivo explorar y mostrar métodos eficientes que tienen efecto positivo en la conciencia del factor humano para la implantación con éxito de un Sistema de Gestión de Seguridad de la Información. El Intercambio de información sobre los conocimientos de seguridad, la colaboración de seguridad de la información, el comportamiento de atención consciente y el cumplimiento con las políticas de la información de organizaciones y procedimientos son metodologías que aumentan el nivel de conciencia con respecto a la seguridad de información en el factor humano, permitiéndoles entender que juegan un papel importante con la seguridad de la información dentro de una organización. A través de la revisión sistemática de la literatura se concluye que existen métodos que ayudan a la concientización del factor humano a implementar exitosamente un sistema de gestión de seguridad de la información.

**Palabras clave:** Seguridad de la Información, Comportamiento humano, Colaboración, SGSI, ISKS, ISC, ISCCB, CISOP

## Abstract

This article aims to explore and show efficient methods that have a positive effect on the awareness of the human factor for the successful implementation of an Information Security Management System. The Exchange of information on security knowledge, information security collaboration, conscious attention behavior and compliance with the information policies of organizations and procedures are methodologies that increase the level of awareness regarding the security of information on the human factor, allowing them to understand that they play an important role with information security within an organization. Through the systematic review of the literature, it is concluded that there are methods that help raise awareness of the human factor to successfully implement an information security management system.

**Keywords:** Information Security, Human behavior, Collaboration, ISMS, ISKS, ISC, ISCCB, CISOP

## I. Metodología

Se realizó una búsqueda sistemática y un análisis narrativo utilizando las siguientes palabras clave: seguridad de la información, SGSI, information security, cultura organizacional, factores humanos; así como también se hizo un filtro de búsqueda desde el año 2014 hasta el 2019, priorizando los resultados a reportes científicos, artículos científicos, reportes científicos. Los registros obtenidos estaban entre 1 a 65 registros tras la combinación entre estas palabras. Para la ubicación de los artículos científicos, se realizó una búsqueda bibliográfica en varias bases de datos como ScienceDirect, IEEE Xplore y EBSCO Discovery Service.

## II. INTRODUCCIÓN

A medida que internet se ha convertido en un producto integrado en la vida humana, las tecnologías de información y comunicación se han convertido en algo esencial para las organizaciones para seguir manteniendo sus altos niveles de productividad. Al mismo tiempo la adopción de estas tecnologías viene con una serie de vulnerabilidades, y por lo tanto nuevas amenazas hacia la confidencialidad y la integridad de los datos organizacionales y personales [1]. Estos problemas de vulnerabilidades son ahora de gran preocupación para las organizaciones ya que en estos últimos años se registraron varios ataques cibernéticos y los famosos phishing [2], [3]. Una encuesta realizada por la Identity Theft Resource Center [4] encontraron que el número de violaciones de datos en los Estados Unidos (US) aumentó en un 8,1% 2014 hasta el 2015, y el costo de la ciberdelincuencia en los EE.UU es aproximadamente \$ 100 mil millones al año [5].

Sin embargo, Fumell y Clarke señalan que algunos estudios coinciden en que las personas son el eslabón más débil en la protección del sistema de gestión de seguridad de la información [1] [6]. Así mismo, el estado global de las encuestas de información de seguridad han informado de que los empleados son las fuente más frecuentes de las brechas de seguridad de la información [7]. Del mismo modo, IBM Global Technology Services reportó un informe reciente de unos estudios realizados sobre las violaciones cibernéticos relaciona al error humano como un factor en el 95% de los incidentes de la seguridad de información en las organizaciones [1].

Arachchilage & Love en investigaciones anteriores han demostrado que la conciencia de seguridad de la información en los empleados es fundamental para los riesgos asociados a las brechas de seguridad de la información [8]. Por lo tanto, la concientización del factor humano en las organizaciones debe ser propicio para la protección de la información de un contexto de seguridad de la información [9]. Esto ayudará a minimizar el riesgo de incidentes causados por los empleados ya sea por negligencia, error o ataques maliciosos deliberados en el tratamiento de la información confidencial o personal [10],[11].

En este sentido, este artículo tiene como objetivo principal explorar y mostrar los métodos eficientes que tienen efecto positivo en la conciencia del factor humano para la implementación de un Sistema de Información de Seguridad de la Información exitosamente. En la parte de desarrollo o revisión se presentarán cuatro métodos importantes para la concientización, el intercambio de información sobre los conocimientos de seguridad (ISKS), la colaboración hacia la seguridad de la información (ISC), La seguridad de la información como un comportamiento de atención consciente (ISCCB) y el cumplimiento con las políticas de seguridad de la información de organizaciones y procedimientos (CISOP).

### III. DESARROLLO

#### **Métodos de apoyo para la concientización del factor humano para Implementar un SGSI**

Los métodos a mencionar fueron aplicados en varias organizaciones en Malasia, organizaciones cuyas actividades principalmente estaban en el ámbito de la banca, los seguros, el comercio electrónico y la educación. Los participantes en la sección de educación eran empleados de una universidad gubernamental muy reconocida y de muy buena reputación en Malasia, estas organizaciones establecieron políticas y procedimientos de seguridad de la información, de tal manera que todos los empleados deben seguir estas políticas y procedimientos. Los participantes estaban familiarizados con la importancia de la seguridad de la información. Las respuestas de las preguntas se basaron en una escala de Likert de cinco puntos (1-totalmente en desacuerdo a 5-totalmente de acuerdo). Después que analizaron los datos del instrumento aplicado, llegaron a la conclusión que los métodos a mencionar tuvieron un efecto significativo con respecto al apoyo para la concientización del factor humano para implementar un Sistema de Gestión de Seguridad de la Información.

#### **El Intercambio de información sobre los conocimientos de seguridad (ISKS)**

El intercambio de conocimientos juega un rol muy importante en el ámbito de la seguridad de la información, debido a su efecto positivo en la conciencia en el factor humano con relación a la seguridad de la información [12], [13], [14]. Los hackers utilizan nuevos métodos para poder ingresar a grandes ordenadores o sistemas que son muy robustos para sus propios beneficios [15]. Recientemente, Kim et al mencionaron que los hackers desarrollaron un sitio web falso de una organización muy conocida y pidieron a los usuarios descargar software antivirus gratuito desde su página web, muchos usuarios descargaron el software antivirus de estos sitios web falsos y perdieron su información privada [6]. Víctimas de Ingeniería social y phishing son otros ejemplos de error de los usuarios en el dominio de la conducta de seguridad de la información [16], [17].

En este entorno mostrado, el conocimiento efectivo y el intercambio de información entre los usuarios de seguridad [18], no solo aumentan el nivel de conciencia como un enfoque eficaz, sino que también reduce los costos de la seguridad de la información en las organizaciones [19],[20]. La mayoría de profesionales en seguridad de la información más de una vez quizás pasaron con problemas similares en este ámbito pudiendo haber ganado mucha experiencia si quizás hubiesen intercambiado conocimientos con otros profesionales en el mismo ámbito [21] [22].

KwangWook & Ravichandran [23], investigaron el efecto de intercambio de conocimientos de seguridad de la información en la comunidad virtual, y su efecto en la reducción de riesgos, mencionando que existe un bajo nivel de disposición de parte de los miembros y que deberían de compartir sus conocimientos con los demás ya que esta es una barrera muy importante en la seguridad de la información. Los obstáculos para el intercambio de conocimientos en el factor humano es la confianza en la propiedad de los conocimientos, el peligro de perder el empleo, la falta de familiaridad con el compañero de trabajo, la actitud individual y la desconfianza [23], [24].



Las organizaciones deben establecer un entorno adecuado, incentivar y motivar para que los usuarios intercambien conocimientos de seguridad de la Información[22]. Por ejemplo, el Centro de Ciberseguridad Industrial creó un juego que ayudó como herramienta profesional de concientización para trabajadores y directivos en algunas organizaciones [25]. Por lo tanto, el intercambio de información sobre los conocimientos de seguridad (ISKS) es un aspecto importante en el enfoque del factor humano para asegurar los activos de información.

### **La colaboración de seguridad de la información (ISC)**

Woodland, RH & Hutton, MS mencionan que la colaboración es trabajar juntos con el fin de lograr un solo objetivo y este objetivo puede ser la salvaguarda de la información de una organización. Ahora, la colaboración de seguridad de la información es la agrupación de las contribuciones del factor humano contra los incidentes de seguridad de la información[6].

La colaboración de seguridad de la información ha sido reconocido, como un enfoque necesario para mitigar el riesgo de fallos en las organizaciones [12]. Así mismo se le considera como imprescindible en términos de una buena documentación, proporciona una línea de tiempos para las actividades y un conjunto de pruebas para el manejo de incidentes[23]. La colaboración de seguridad de la información permite al factor humano entender y ampliar su información sobre las violaciones de seguridad de la información [23]. La colaboración es el objetivo principal en muchos estudios relacionados al aprendizaje, la salud, control de proyectos, organización, empresa y así sucesivamente, el beneficio de la colaboración es que ayuda a aumentar la experiencia en el factor humano así como también ayuda a mejorar la toma de decisiones dentro de la organización [26] [27]. El compromiso, la comunicación, la confianza, la coordinación, la cultura de colaboración, la supervisión y la concentración en las habilidades técnicas son barreras para la colaboración de seguridad de la información [6], [28]. Para poder llevar a cabo las actividades referentes a la seguridad de la información con éxito, el factor humano debe cooperar, coordinar y colaborar con los demás [29], en respuesta a incidencias de seguridad, el desarrollo de las políticas, informar violaciones de la seguridad y el intercambio de conocimiento en el ámbito de la seguridad de la información son ejemplos claros de colaboración de seguridad de la información. Sin embargo, existe una escasez de investigación sobre la formación de la colaboración de seguridad de la información en las organizaciones [12].

### **El comportamiento de atención consciente (ISCCB)**

El comportamiento de atención consciente es reconocido eficaz y eficientemente contra el enfoque de ingeniería social y phishing ya que ayuda a las demás metodologías con mitigar las brechas de seguridad de la información [6]. Por ejemplo, cada día los hackers se dirigen a las personas, en lugar de los ordenadores, con el fin de crear una brecha, es por ello que el comportamiento de atención consciente entra a contrarrestar estos tipos de ataques creativos [30], [18]. “El comportamiento de atención consciente significa que los usuarios piensan en las consecuencias de sus actos en términos de seguridad de la información cuando trabajan con un sistema” [12], [31], [32]. El factor humano considera a la seguridad de la información como un obstáculo cuando no hay adecuada respuesta a sus incidentes cibernéticos [33], [27], se sienten con muchas dificultades cuando el personal de TI implementa un sistema de seguridad de la información en sus áreas, malinterpretan y tratan de anular los controles de seguridad, mostrando un comportamiento que pone en riesgo a la organización [12], [34], [35]. Los investigadores dicen que este tipo de personas que muestra un comportamiento negligente, son de mucha amenaza dentro de una organización siendo el principal problema referente a la seguridad de la información [36].

Sin embargo, también existe una escasa investigación sobre la formación del comportamiento de seguridad de la información. A partir de lo mencionado, está de más decir que el comportamiento de atención consciente hacia la seguridad de la información (ISCCB) en el factor humano está en un estado que se debe trabajar cada día en las organizaciones, también está claro que tanto ISC y ISKS cumplen un rol principal en el logro de ISCCB [12], [37].

Cumplimiento con las políticas de la información de organizaciones y procedimientos (CISOP)

Warkentin et al hasta ahora no se ha encontrado una definición única, hemos descrito cumplimiento de un empleado con prácticas de protección de datos de una organización como la intención y la voluntad de actuar conforme a las normas y reglamentos establecidos en las políticas de seguridad de la información [38].

Muchos investigadores de seguridad de la información examinaron métodos para poder identificar a los empleados que hacen un mal uso de la información y de esta manera encontrar mejoras para el cumplimiento de las políticas de la información [39], haciendo uso de hábitos y teorías de motivación [38], [40]. Otros investigadores muestran la importancia del desarrollo de política de seguridad, la conciencia [41], el cumplimiento y la aplicación de mejores prácticas como base para medir la seguridad de la información [42], [43].

Las amenazas internas por parte de los empleados siguen afectando a las organizaciones, los piratas informáticos utilizan aplicaciones engañosas, como la desfragmentación falsa de o escáneres de antivirus falsos [44]. Todo este tipo de aplicaciones falsas reportan problemas que no existen y sugieren la descarga del software libre en lo cual el empleado no debería descargar el software, más bien debería de reportar este tipos de incidencias a los expertos de seguridad de la información [45], [46]. Las políticas y procedimientos de la seguridad de la información de la organización prohíben la descarga de software de sitios web maliciosos [17], [47]. Por lo tanto, el cumplimiento de las políticas y procedimientos de seguridad de la información (CISOP) es un enfoque eficaz y de mucha importancia dentro de las organizaciones [48] [49] [50]. Es importante que todos ISKS, ISC, ISCCB y CISOP contribuyen colectivamente para abordar el aspecto humano en la obtención de los activos de información en las empresas.



#### **IV. CONCLUSIONES**

Existen métodos que ayuda a la concientización del factor humano para implementar exitosamente un sistema de gestión de seguridad de la Información. Métodos que contribuye a reducir el costo de la seguridad en una organización, que aumenta la experiencia de cooperación y coordinación entre los demás empleados, que influye directamente que el empleado piense en las consecuencias de sus actos en términos de seguridad al hacer uso de las tecnologías y que tenga el hábito de verificar y reportar dichos incidentes maliciosos de parte de cualquier acto malicioso en un tiempo que pueda ser identificado y controlado. Este estudio sugiere a las organizaciones que quieran implementar un sistema de gestión de seguridad de la información que deben antes considerar la importancia de la concientización del factor humano haciendo usos de las metodologías mencionadas, ya que tiene ventajas positivas hacia la seguridad de la información.

## V. REFERENCIAS

- [1] K. Parsons, D. Calic, M. Pattinson, M. Butavicius, A. McCormac, and T. Zwaans, "The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies," *Comput. Secur.*, vol. 66, pp. 40–51, May 2017.
- [2] K. Dae-Wook, P. Yan, and J. Zhang, "Detecting fake anti-virus software distribution webpages," *Comput. Secur.*, vol. 49, pp. 95–106, Mar. 2015.
- [3] D. D. Caputo, S. L. Pfleeger, J. D. Freeman, and M. E. Johnson, "Going spear phishing: exploring embedded training and awareness," *IEEE Secur. Priv.*, vol. 12, no. 1, pp. 28–38, Jan. 2014.
- [4] G. Rafael-Samillan and E. Castillo-Oviedo, "Auditoría Informática usando las Normas Cobit en el Centro de Sistemas de Información del Hospital Regional Docen Las Mercedes de Chiclayo – 2016," Universidad Nacional Pedro Ruiz Gallo, 2017.
- [5] J. Rooheart, "Cyber Crime to Reach \$2 Trillion By 2019 - business.com," 2017. [Online]. Available: <https://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#685c38a63a91>. [Accessed: 28-May-2019].
- [6] N. Sohrabi-Safa, M. Sookhak, R. Von Solms, S. Furnell, N. Abdul-Ghani, and T. Herawan, "Information security conscious care behaviour formation in organizations," *Comput. Secur.*, vol. 53, pp. 65–78, Sep. 2015.
- [7] Price Waterhouse Coopers, "Information Security Breaches Survey 2015," 2015.
- [8] N. Sohrabi-Safa and R. Von-Solms, "An information security knowledge sharing model in organizations," *Comput. Human Behav.*, vol. 57, pp. 442–451, Apr. 2016.
- [9] J. Shibchurn and X. Yan, "Information disclosure on social networking sites: An intrinsic-extrinsic motivation perspective," *Comput. Human Behav.*, vol. 44, pp. 103–117, Mar. 2015.
- [10] A. Da Veiga and N. Martins, "Information security culture and information protection culture: A validated assessment instrument," *Comput. Law Secur. Rev.*, vol. 31, no. 2, pp. 243–256, Apr. 2015.
- [11] H. Haqaf and M. Koyuncu, "Understanding key skills for information security managers," *Int. J. Inf. Manage.*, vol. 43, pp. 165–172, Dec. 2018.
- [12] N. Sohrabi-Safa, R. Von-Solms, and L. Fitcher, "Human aspects of information security in organisations," *Comput. Fraud Secur.*, vol. 2016, no. 2, pp. 15–18, Feb. 2016.
- [13] K. Phudphad, B. Watanapa, W. Krathu, and S. Funilkul, "Rankings of the security factors of human resources information system (HRIS) influencing the open climate of work: Using analytic hierarchy process (AHP)," in *Procedia Computer Science*, 2017, vol. 111, pp. 287–293.
- [14] A. McCormac, T. Zwaans, K. Parsons, D. Calic, M. Butavicius, and M. Pattinson, "Individual differences and information security awareness," *Comput. Human Behav.*, vol. 69, pp. 151–156, Apr. 2017.
- [15] J. Hepler, "A good thing isn't always a good thing: Dispositional attitudes predict non-normative judgments," *Pers. Individ. Dif.*, vol. 75, pp. 59–63, Mar. 2015.
- [16] K. M. Parsons, E. Young, M. A. Butavicius, A. McCormac, M. R. Pattinson, and C. Jerram, "The influence of organizational information security culture on information security decision making," *J. Cogn. Eng. Decis. Mak.*, vol. 9, no. 2, pp. 117–129, Jun. 2015.

- [17] R. Torten, C. Reaiche, and S. Boyle, "The impact of security awareness on information technology professionals' behavior," *Comput. Secur.*, vol. 79, pp. 68–79, Nov. 2018.
- [18] W. Rocha Flores, E. Antonsen, and M. Ekstedt, "Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture," *Comput. Secur.*, vol. 43, pp. 90–110, Jun. 2014.
- [19] E. H. Park, J. Kim, and Y. S. Park, "The role of information security learning and individual factors in disclosing patients' health information," *Comput. Secur.*, vol. 65, pp. 64–76, Mar. 2017.
- [20] D. Dang-Pham, S. Pittayachawan, and V. Bruno, "Why employees share information security advice? Exploring the contributing factors and structural patterns of security advice sharing in the workplace," *Comput. Human Behav.*, vol. 67, pp. 196–206, Feb. 2017.
- [21] A. Akhunzada *et al.*, "Man-At-The-End attacks: Analysis, taxonomy, human aspects, motivation and future directions," *Journal of Network and Computer Applications*, vol. 48. Academic Press, pp. 44–57, 01-Feb-2015.
- [22] E. Metalidou, C. Marinagi, P. Trivellas, N. Eberhagen, C. Skourlas, and G. Giannakopoulos, "The Human Factor of Information Security: Unintentional Damage Perspective," *Procedia - Soc. Behav. Sci.*, vol. 147, pp. 424–428, Aug. 2014.
- [23] N. Sohrabi-Safa, R. Von-Solms, and S. Furnell, "Information security policy compliance model in organizations," *Comput. Secur.*, vol. 56, pp. 1–13, Feb. 2016.
- [24] M. E. Lo-Giudice, "Datos empresariales, protección en la actual sociedad de la información: Una visión Argentina," no. 17, 2017.
- [25] J. Abadia-Correa, L. Ortiz-Paez, and N. Peña-Castiblanco, "Desarrollo de un Juego Formativo para Aportar a la Concienciación en Ciberseguridad al Personal de la Escuela Militar de Aviación (Emavi) 'Marco Fidel Suárez' de la Fuerza Aérea Colombiana en la ciudad de Cali," *Cienc. y Pod. Aéreo*, vol. 12, no. 1, p. 264, 2017.
- [26] A. Alhogail, "Design and validation of information security culture framework," *Comput. Human Behav.*, vol. 49, pp. 567–575, Aug. 2015.
- [27] J. Shropshire, M. Warkentin, and S. Sharma, "Personality, attitudes, and intentions: Predicting initial adoption of information security behavior," *Comput. Secur.*, vol. 49, pp. 177–191, Mar. 2015.
- [28] A. Tamjidyamcholo, M. S. Bin-Baba, N. L. Mohd-Shuib, and V. A. Rohani, "Evaluation model for knowledge sharing in information security professional virtual community," *Comput. Secur.*, vol. 43, pp. 19–34, Jun. 2014.
- [29] J. Webb, A. Ahmad, S. B. Maynard, and G. Shanks, "A situation awareness model for information security risk management," *Comput. Secur.*, vol. 44, pp. 1–15, Jul. 2014.
- [30] N. Ben-Asher and C. Gonzalez, "Effects of cyber security knowledge on attack detection," *Comput. Human Behav.*, vol. 48, pp. 51–61, Jul. 2015.
- [31] I. Hwang and O. Cha, "Examining technostress creators and role stress as potential threats to employees' information security compliance," *Comput. Human Behav.*, vol. 81, pp. 282–293, Apr. 2018.
- [32] S. Egelman, M. Harbach, and E. Peer, "Behavior ever follows intention?," *Conf. Hum. Factors Comput. Syst. - Proc.*, pp. 5257–5261, 2016.

- [33] S. Egelman and E. Peer, "Scaling the security wall," *Proc. 33rd Annu. ACM Conf. Hum. Factors Comput. Syst. - CHI '15*, pp. 2873–2882, 2015.
- [34] A. Tsohou, M. Karyda, and S. Kokolakis, "Analyzing the role of cognitive and cultural biases in the internalization of information security policies: Recommendations for information security awareness programs," *Comput. Secur.*, vol. 52, pp. 128–141, Jul. 2015.
- [35] A. Yazdanmehr and J. Wang, "Employees' information security policy compliance: A norm activation perspective," *Decis. Support Syst.*, vol. 92, pp. 36–46, Dec. 2016.
- [36] T. Galba, K. Solic, and I. Lukic, "An information security and privacy self-assessment ( ISPSA ) tool for internet users," *Acta Polytech. Hungarica*, vol. 12, no. 7, pp. 149–162, 2015.
- [37] G. Öütçü, Ö. M. Testik, and O. Chouseinoglou, "Analysis of personal information security behavior and awareness," *Comput. Secur.*, vol. 56, pp. 83–93, Feb. 2016.
- [38] H. N. Chua, S. F. Wong, Y. C. Low, and Y. Chang, "Impact of employees' demographic characteristics on the awareness and compliance of information security policy in organizations," *Telemat. Informatics*, vol. 35, no. 6, pp. 1770–1780, Sep. 2018.
- [39] J. R. Altamirano-Yupanqui and S. Bayona-Oré, "Políticas de Seguridad de la Información: Revisión sistemática de las teorías que explican su cumplimiento," *RISTI - Rev. Iber. Sist. e Tecnol. Inf.*, vol. 2017, no. 25, pp. 112–134, Dec. 2017.
- [40] G. Dhillon, R. Syed, and F. de Sá-Soares, "Information security concerns in IT outsourcing: Identifying (in) congruence between clients and vendors," *Inf. Manag.*, vol. 54, no. 4, pp. 452–464, Jun. 2017.
- [41] W. Wei-tsong and H. Ya-Pei, "Motivations of employees' knowledge sharing behaviors: A self-determination perspective," *Inf. Organ.*, vol. 25, no. 1, pp. 1–26, Jan. 2015.
- [42] S. V. Flowerday and T. Tuyikeze, "Information security policy development and implementation: The what, how and who," *Comput. Secur.*, vol. 61, pp. 169–183, Aug. 2016.
- [43] B. Ngoqo and S. V. Flowerday, "Information Security Behaviour Profiling Framework (ISBPF) for student mobile phone users," *Comput. Secur.*, vol. 53, pp. 132–142, Sep. 2015.
- [44] M. R. Fazlida and J. Said, "Information Security: Risk, Governance and Implementation Setback," *Procedia Econ. Financ.*, vol. 28, pp. 243–248, Jan. 2015.
- [45] M. Kiss, G. Breda, and L. Muha, "Information security aspects of Industry 4.0," *Procedia Manuf.*, vol. 32, pp. 848–855, Jan. 2019.
- [46] M. A. Alnatheer, "Information security culture critical success factors," *Proc. - 12th Int. Conf. Inf. Technol. New Gener. ITNG 2015*, pp. 731–735, Apr. 2015.
- [47] Y. "Andy" Wu and C. S. Saunders, "Governing the fiduciary relationship in information security services," *Decis. Support Syst.*, vol. 92, pp. 57–67, Dec. 2016.
- [48] R. L. Valdivia-Málaga, "Propuesta de formulación de las estrategias de tecnologías de la información y comunicación de SENCICO basado en el proceso de Planeación Estratégica de Tecnologías de la Información y Comunicación (PETIC), de la metodología COBIT en marco del plan strat," UCSM, 2016.

[49] P. Ifinedo, "Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition," *Inf. Manag.*, vol. 51, no. 1, pp. 69-79, Jan. 2014.

[50] P. Ifinedo, "Critical Times for Organizations: What Should Be Done to Curb Workers' Noncompliance With IS Security Policy Guidelines?," *Inf. Syst. Manag.*, vol. 33, no. 1, pp. 30-41, Jan. 2016.