RECIBIDO: 29-12-2022 | ENVIADO A PARES: 03-04-2023 | APROBADO POR PARES: 14-05-2023 | ACEPTADO: 28-06-2023 | PP. 39 - 50

Modelo de evaluación de seguridad de la información en centros de datos

Information Security Assessment Model for Data Centers

Karen Estacio Corozo
Instituto Superior Tecnológico ARGOS, Ecuador
k_estacio@tecnologicoargos.edu.ec
https://orcid.org/0000-0002-6394-2455

Revista Cumbres Vol.9 Nº1

Versión electrónica ISSN 1390-3365
http://investigacion.utmachala.edu.ec/revistas/index.php/Cumbres
http://doi.org/10.48190/cumbres.v9n1a3

RESUMEN

La seguridad de la información (SI) ha pasado de utilizarse netamente para fines de protección de datos clasificados del gobierno en cuestiones militares, a convertirse en un bien de vital importancia para las organizaciones de cualquier sector económico. El objetivo del presente estudio es elaborar un modelo que permita evaluar el nivel de cumplimiento de la SI en centros de datos. Para esto, se analizaron los controles de los estándares ISO27002 y NIST 800-53 r5 que aplican al objetivo mencionado, con los controles seleccionados se obtuvo un instrumento que consta de 80 ítems, distribuidos en Aspectos Organizativos de seguridad de la Información (9), Control de Accesos (20), Seguridad Física y Ambiental (28), Seguridad Operativa (14), Seguridad en Telecomunicaciones (9).

Por otra parte, para evaluar el nivel de pertinencia de implementación de cada control seleccionado conforme a la escala y estructura de cada organización se tomó como referencia el estudio "Una metodología de múltiples perspectivas para la evaluación de la Madurez de seguridad de centros de datos", donde se realizan 2 análisis (tradicional y contextual) con el objetivo de personalizar el instrumento a las necesidades de la organización considerando la ponderación y relevancia que el auditado o evaluado le asigna a cada control. Con los resultados obtenidos se analizarán ambas perspectivas y su relación de pertinencia para la empresa donde se aplicará el instrumento, dado que el auditado otorgará la relevancia a los controles y evitar brechas en la seguridad de la información.

Palabras clave: seguridad de información, ISO 27000, NIST 800-53 centro de datos.

ABSTRACT

The importance of information security (IS) has evolved from being solely used for the protection of classified government data in military matters to becoming a vital asset for organizations in any economic sector. The objective of this study is to develop a model that allows for the assessment of IS compliance in data centers. To achieve this, the controls from ISO27002 and NIST 800-53 r5 standards applicable to the mentioned objective were analyzed. From the selected controls, an instrument consisting of 80 items was obtained, distributed across Organizational Aspects of Information Security (9), Access Control (20), Physical and Environmental Security (28), Operational Security (14), and Telecommunications Security (9).

Furthermore, to evaluate the level of implementation relevance for each selected control in accordance with the organization's scale and structure, the study "A Methodology of Multiple Perspectives for Data Center Securi-

ty Maturity Assessment" was referenced. This study performs two analyses (traditional and contextual) with the aim of customizing the instrument to the organization's needs, considering the weighting and relevance assigned to each control by the auditee or evaluated party. The obtained results will be analyzed from both perspectives, assessing their relevance to the company where the instrument will be applied. This approach allows the auditee to assign importance to the controls and prevent any information security gaps.

Keywords: Security information, ISO 27000, NIST 800-53, data center.

INTRODUCCIÓN

La evolución de la tecnología y la falta de conocimiento para mitigar los riesgos de ataques han generado innumerables amenazas que aprovechan las vulnerabilidades de las empresas para materializar riesgos y generar un impacto negativo en las organizaciones (Cholez et al., 2014). La evolución de la tecnología y la falta de conocimiento para mitigar los riesgos de ataques han generado innumerables amenazas que aprovechan las vulnerabilidades de las empresas para materializar riesgos y generar un impacto negativo en las organizaciones (Vroom et al., 2004).

La importancia de una gestión eficaz de la seguridad de las tecnologías de información (TI) desde una perspectiva económica ha aumentado en los últimos años debido a la creciente frecuencia de los ataques informáticos y al coste de las infracciones de seguridad (Bulgurcu et al., 2010; Cavusoglu et al., 2004).

Las organizaciones maduras en seguridad definen sistemáticamente los objetivos de seguridad de información (SI), los medios para lograrlos y los controles para mantenerlos. La madurez y cumplimiento de la SI depende no solo de los aspectos técnicos, sino también de la participación humana en todo el proceso y en la gestión operativa (Lima et al., 2017). Como mencionan Knapp y Ferrante (2012) las políticas internas de seguridad de la información incluyen los controles internos de SI para prevenir y detectar incidentes de seguridad, existe una brecha relacionada a los empleados que no los cumplen, los factores podrían moderar la relación entre el cumplimiento de la política y el logro de los objetivos de seguridad de la organización o podría influir en la consecución de los objetivos de seguridad de la organización directamente (Cram et al., 2017).

La gerencia que gestiona la seguridad de la información en una organización tiene como principal desafío lograr los objetivos generales que incluyen: salvaguardar la información confidencial, crítica y propietaria del acceso,

divulgación o modificación no autorizados, proteger los sistemas de información y dar soporte a los recursos informáticos. contra pérdida, daño y destrucción (Hong et al., 2003).

Un centro de datos (DC) es un lugar crítico para las empresas ya que alberga los activos más importantes, por lo que cuenta con características físicas, de refrigeración, redundancia y protección con el objetivo de albergar todo el equipamiento tecnológico de la empresa, brindando seguridad y confiabilidad, todas estas condiciones garantizar el correcto funcionamiento de la red de datos. Una incursión ilegal por parte de personal no autorizado en un centro de datos puede comprometer la seguridad de los datos y las contraseñas de los usuarios y causar daños maliciosos a la red, causando graves perturbaciones en los sistemas de procesamiento y comunicación (Galvan, 2013).

La SI garantiza la confidencialidad, disponibilidad e integridad (CDI) de la información, lo que implica la aplicación y administración de controles adecuados que involucran la consideración de una amplia gama de amenazas y minimizar las consecuencias de los incidentes de SI (27001:2022, 2022). Una adecuada gama de controles de seguridad es una combinación adecuada de condiciones físicas, técnicas y controles de seguridad operacional. Esto ayudará a una organización a continuar construyendo relaciones de confianza con sus clientes, proveedores y otros socios comerciales (Posthumus et al., 2004; Veiga et al., 2010).

El propósito de esta investigación es elaborar un modelo que sirva como herramienta guía para evaluar la SI en los centros de datos, con el componente novedoso de adaptación a la necesidad de cada empresa considerando sus necesidades y alcance de infraestructura tecnológica.

MATERIALES Y MÉTODOS

En esta investigación, se llevó a cabo una revisión sistemática de la literatura relacionada con estudios previos sobre SI en centros de datos y ciberseguridad de infraestructura tecnológica. En la Tabla 1 se proporciona un detalle de los estudios previos, así como los estándares seleccionados por los autores utilizados en cada uno de ellos para la selección de políticas, procedimientos, lineamientos, recursos y actividades asociadas a la implementación de controles de SI. Estos controles son gestionados colectivamente con el objetivo de fortalecer la seguridad de la información, permitiendo recomendaciones e implementaciones de controles de seguridad en cumplimiento de confidencialidad, disponibilidad e integridad de la información, de ahora en adelante, llamado CDI por sus siglas, en la tabla 2 se detallan los estándares seleccionados y su breve contenido.

ISO/IEC 27002:2022 – Seguridad de la información, ciberseguridad y protección de la privacidad — Controles de seguridad de la información, propor-

ciona un conjunto de referencia de controles genéricos de seguridad de la información, cuenta con 93 controles distribuidos de la siguiente forma: 37 controles organizacionales, 8 controles de personas, 14 controles físicos y 34 controles tecnológicos (ISOTools, 2022).

El Instituto Nacional de Estándares y Tecnología (NIST), en su publicación especial 800-53, ofrece un catálogo exhaustivo de controles de seguridad y privacidad diseñados para sistemas de información federales y organizaciones del sector privado en los Estados Unidos. El objetivo principal de estos controles es salvaguardar los activos y las operaciones de la organización a través de la garantía de CDI de la información (NIST, 2022). Es importante destacar que NIST 800-53 ha evolucionado para incluir controles relacionados con la computación en la nube, además de incorporar controles provenientes del estándar ISO 27002, así como de otros marcos tanto gubernamentales como no gubernamentales. (Duncan et al., 2014).
Tabla 1. Revisión de la literatura

Tabla 1. Revisión de la literatura

PUBLICACIÓN	METODOLOGÍA
On Developing Information Security Management System (ISMS) Framework for ISO 27001-based Data Center (Achmadi et al., 2018).	Selección de controles del estándar ISO 27002 para construir un SGSI
Improving the quality of information security management systems with ISO27000 (Gillies, 2011).	Una guía para simplificar el proceso para obtener la certificación ISO27001, con beneficios significativos para alcanzar la madurez de SI.
A High-Level Comparison between the NIST Cyber Security Framework and the ISO 27001 Information Security Standard (Prameet, 2020).	Análisis comparativo y ventajas de implementar los controles de SI del estándar ISO27002 y el marco regulatorio NIST 800-53
A security review of local government using NIST CSF: a case study (Ibrahim et al., 2018).	Herramienta para evaluar la el riesgo de ciberseguridad utilizando los controles del marco NIST 800-53
Automation of Security and Privacy Controls for Efficient tInformation Security Management	Aplicación de herramientas para la automatización de la gestión de los controles del marco NIST 800-53 mejorando la eficiencia en la seguridad y privacidad de la información dentro de las organizaciones.
Information System Risk Scenario Using COBIT 5 for Risk And NIST SP 800-30 Rev. 1 A Case Study (Supriyadi et al., 2018).	Caso de estudio donde se creó un escenario de riesgo aplicando COBIT 5 y posterior se aplicó análisis de riesgos de SI, utilizando los controles del marco NIST 800-53

Ambos estándares, ISO 27001 (controles del estándar ISO 27002) y NIST 800-53, son ampliamente reconocidos y muy completos en la industria de la seguridad de la información. El estándar ISO 27001 proporciona una estructura para establecer, implementar, mantener y mejorar continuamente un Sistema de Gestión de la Seguridad de la Información (SGSI) en una organización. Por otro lado, el estándar ISO 27002 ofrece un conjunto de controles para la gestión de la seguridad de la información. Al utilizar ambos estándares de manera conjunta, es posible establecer un modelo sólido y efectivo, que integre los controles adecuados para proteger la información de la organización.

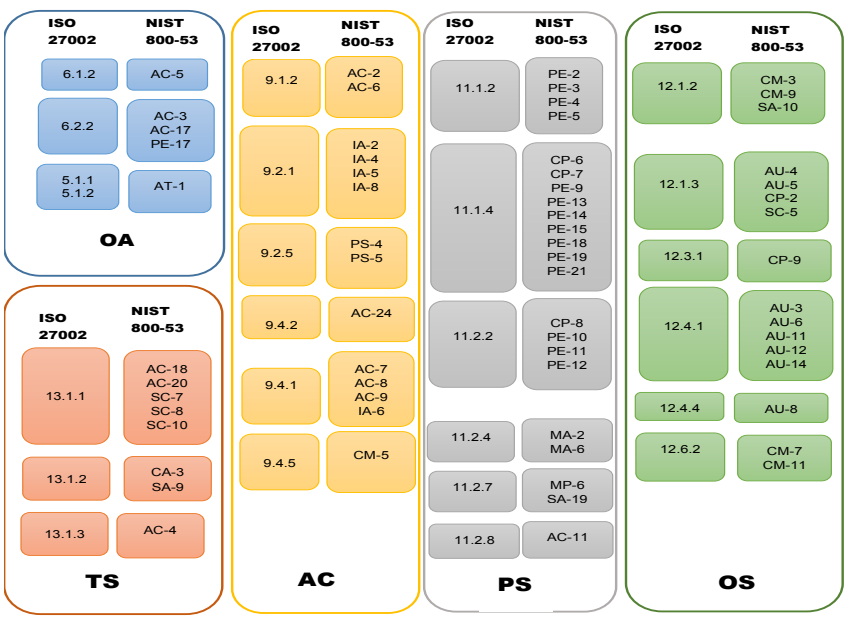
Tabla 2. Estándares de seguridad de información

STANDARD	CONTENIDO	CDI
NIST 800-53	Proporciona un catálogo de controles de seguridad y privacidad.	Si
ISO 27001:2022	Directrices para la selección, implementación y gestión de los controles del SGSI	Si

RESULTADOS

Una vez seleccionados los estándares antes mencionados que cumplen con CDI se realizó un análisis comparativo entre NIST 800-53 e ISO 27000 con el objetivo de aprovechar la complementariedad de los estándares, seleccionando 80 controles que se consideraron más adecuados, identificando la superposición y la convergencia de los controles propuestos en ambos estándares. (Hong et al., 2003). Esto permite identificar los puntos en común y las diferencias clave entre los enfoques, permitiendo una mejor selección y adaptación de los controles específicos a las necesidades de una organización para garantizar el cumplimiento normativo, mejorar la eficiencia y aprender de las mejores prácticas propuestas en ambos marcos de referencia. La figura 1 contoine de forma abreviada los controles selecionados y su clasificación.

Figura 1. Detalle de controles de SI para evaluar en centros de datos



Los criterios de selección de controles de SI a modo general fueron relevancia para la organización en el cumplimiento de sus objetivos de negocio, cumplimiento normativo en conforme a requisitos regulatorios, mejores prácticas de SI, evaluación de riesgos, recursos disponibles y adaptabilidad y flexibilidad. En la tabla 3 en la columna de cláusulas se detalla de forma específica los criterios que se consideraron relevantes para el objetivo del estudio, enfocados a un centro de datos que alberga la información como activo principal.

Tabla 3. Modelo guía para evaluar la SI en centros de datos

CLAUSULA	CONTROLES	ITEMS	TOTAL
Aspectos organizativos de la seguridad de la información (OA)	Segregación de tareas (ST)	4	9
	Telecomunicaciones (TT)	3	
	Políticas y procedimientos de sensibilización y formación (PA)	2	
Control de acceso (AC)	Control de acceso a redes y servicios asociados (AN)	3	20
	Gestión de altas/bajas en el registro de usuarios (MU)	5	
	Revisión de los derechos de acceso de los usuarios (UA)	3	
	Restricción de acceso to información (RA)	2	
	Procedimientos de inicio de sesión seguros (SP)	5	
	Control de acceso al código fuente de los programas (CC)	2	
Seguridad física y ambiental (PS)	Controles de acceso físico (HC)	5	28
	Protección contra amenazas externas y ambientales (PE)	10	
	Servicios de suministro (SS)	5	
	Mantenimiento de equipo (EM)	3	
	Eliminación segura o reutilización de equipos (SD)	3	
	Equipo de usuario desatendido (UE)	2	
Seguridad Operacional (OS)	Gestión del cambio (CH)	4	14
	Gestión de capacidad (CM)	5	
	Copia de seguridad de la información (IB)	4	
	Registro de eventos (EL)	2	
	Sincronización de reloj (CS)	6	
	Gestión de vulnerabilidades técnicas (GV)	4	
Seguridad en Telecomunicaciones (TS)	Controles de red (NC)	5	9
	Mecanismos de seguridad asociados a los servicios de red (NS)	3	
	Segregación de red (SN)	1	

El modelo de adaptación y cumplimento en CDI de SI se presenta como una herramienta de evaluación del desempeño en proteger de información como activo fundamental en las organizaciones conforme a su infraestructura tecnológica y modelo de negocio (Ghaffari et al., 2018). Para la elaboración del presente artículo se agregó el componente novedoso de ajustar el instrumento de evaluación a la necesidad de cada organización, otorgando un grado de pertinencia e importancia a cada control presente en la rúbrica, para estos fines se utilizó la propuesta del artículo - A Multi-Perspective Methodology for Evaluating the Security Maturity of Data Centers- (Lima et al., 2017), donde los autores mencionan tres perspectivas de análisis para conocer el punto de vista del evaluado (personal encargado de la infraestructura tecnológica en una organización) y el evaluador (personal interno o externo encargado del validad el cumplimiento de SI):

Análisis tradicional. Mediante la obtención de evidencia tangible e intangible del cumplimiento de los controles de SI seleccionados. Así mismo, la evidencia física está conformada por documentación de políticas, procedimientos y contratos, la evidencia intangible puede ser registros de archivo y código fuente.

Se utilizará una escala de 0 a 4 para clasificar el nivel de cumplimiento del control de seguridad: 0 – sin evidencia; 1 - no aplicado; 2 - implementado parcialmente; 3 -ampliamente implementado; 4 - totalmente implementado. Usaremos la fórmula 1, para determinar el nivel de cumplimiento, donde n es el número de controles de seguridad analizados, Evi es el nivel de evidencia del control de seguridad, MaxEV (el valor máximo en la evidencia 4), y n es el número de controles analizados (80 controles detallados en la Tabla 3).

$$\bar{X} = \frac{\sum_1^n Ev_i}{MaxEv} \qquad (1)$$

Análisis contextual. Introduce el concepto de perspectiva de la organización, que es el nivel de importancia que la organización atribuye a cada uno de los 80 controles de SI que fueron seleccionado en el modelo propuesto. Asimismo, considera las particularidades de cada organización con el fin de lograr la personalización y utilidad del instrumento en cada entidad. A diferencia del análisis anterior, se utilizará la tabla 4, la escala de Likert (1932), para ponderar el nivel de importancia y pertinencia que la organización atribuye a cada control.

$$\bar{X} = \frac{\sum_1^n Ev_i xCWixOWi}{\sum_1^n 4xCWixOWi} \qquad (2)$$

Tabla 4. Nivel de importancia que la organización atribuye a cada control de seguridad.

NIVEL	GRADO DE PERTINENCIA
1	Totalmente en desacuerdo: El control no tiene relevancia para la organización
2	Parcialmente en desacuerdo: El control de seguridad es parcialmente irrelevante
3	Indeciso: existen dudas sobre si el control de seguridad es relevante para la organización
4	Parcialmente de acuerdo: El control de seguridad es parcialmente relevante para la organización

Como resultado el instrumento puede llegar ser una herramienta valiosa para mitigar la
incertidumbre acerca de la implementación en cumplimiento de SI dentro de la empresa referente a su infraestructura tecnológica específicamente centro de datos y detectar si los controles de SI a ser evaluados son de relevancia para la compañía, al realizar los 2 análisis se obtendrá el resultado de cada perspectiva mediante la comparación de los controles de SI implementados y gestionados y se valorará el grado de implemenetación conforme a lo detallado en la tabla 5 en una escala de 0 a 4, desde no administrado hasta totalmente administrado.

Tabla 5. Interpretación de resultados de nivel de cumplimiento de la seguridad de los centros de datos.

NIVEL DE CUMPLIMIENTO	GRADO DE IMPLEMENTACIÓN	CONTROLES ATENDIDOS
0	No implementado	0-19%
1	Parcialmente implementado	20-39%
2	Ampliamente implementado	40-59%
3	Parcialmente implementado	50-79%
4	Totalmente implementado	80-100%

A modo de conclusión se desarrolló un modelo para validar el cumplimiento de los 80 controles de SI seleccionados mediante un análisis comparativo entre las normas internacionales ISO/IEC 27002:2013 y NIST 800-53 quinta revisión. La SI ha generado controversia debido a preocupaciones sobre la privacidad, el equilibrio entre seguridad, accesibilidad, y la creciente sofisticación de las amenazas cibernéticas. Estos debates son un reflejo de la importancia y la complejidad de proteger la información en un mundo cada vez más digitalizado. En el presente estudió se seleccionaron 80 controles de SI que servirán como modelo de evaluación de seguridad en cumplimiento de CDI, la selección partió desde el análisis de las normas internacionales ISO/IEC 27002:2013 y NIST 800-53 quinta revisión.

Complementando al análisis del cumplimiento de SI el componente innovador del presente estudio es la personalización del instrumento a las necesidades y escala de cada organización que cuente con un centro de datos

como infraestructura tecnológica para la gestión de la información, dicho componente es la evaluación del nivel de cumplimiento y pertinencia de cada control seleccionado en el modelo propuesto desde la perspectiva del evaluador y el evaluado en un proceso de validación de cumplimiento, por lo tanto, se han considerado tres tipos de análisis tradicional y contextual, teniendo en cuenta las necesidades específicas de la empresa en relación con el enfoque holístico y generalizado recomendado por los estándares internacionales y normas de SI, al encontrar un equilibrio adecuado entre la seguridad y la usabilidad es un punto de discusión constante, la eficacia de las medidas de seguridad existentes y la necesidad de adoptar enfoques más robustos y proactivos para proteger la información sensible.

Los resultados obtenidos permitirán comprender la relación entre las perspectivas del evaluado y el evaluador, demostrando la pertinencia y necesidad de implementar los 80 controles seleccionados en la propuesta de medición dentro de la organización. Esto proporcionará una visión clara del estado de cumplimiento y la efectividad de los controles de seguridad de la información en la empresa, así como identificar posibles áreas de mejora y acciones correctivas necesarias. En última instancia, este modelo de validación y evaluación contribuirá a fortalecer la seguridad de la información en la organización, proporcionando una base sólida para la toma de decisiones e implementación de mejoras continuas en la gestión de la seguridad de la información.

En cuanto a futuras investigaciones, se propone la ejecución del modelo para evaluar el nivel de cumplimiento de gestión de la seguridad de la información en centros de datos de pequeñas y grandes organizaciones, para tomar una referencia desde diferentes perspectivas de referencia, modelo de negocio y necesidades de la organización que garanticen la CDI de la información, brindando como oportunidad de mejora la implementación de los controles de SI del presente estudio.

REFERENCIAS BIBLIOGRÁFICAS

27001:2022, I. (29 de Diciembre de 2022). *Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. https://www.iso.org/standard/82875.html

Achmadi, D., Suryanto, Y., & Ramli, K. (2018). On Developing Information Security Management System (ISMS) Framework for ISO 27001-based Data Center. *2018 International Workshop on Big Data and Information Security (IWBIS)*, 149-157. doi:10.1109/IWBIS.2018.8471700

Arshpreet, K., Zavarsky, P., & Swar, B. (2021). Automation of Security and

Privacy Controls for Efficient Information Security Management. *2021 2nd International Conference on Secure Cyber Computing and Communications (ICSCCC)*. doi:10.1109/ICSCCC51823.2021.9478126

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. doi:10.2307/25750690

Cavusoglu, H., Mishra, B. K., & Raghunathan, S. (2004). The effect of Internet security breach announcements on market value: Capital market reactions for breached firms and Internet security developers. *International Journal of Electronic Commerce, 9*(1), 69-104. doi:10.1080/10864415.2004.11044320

Cholez, H., & Girard, F. (2014). Maturity assessment and process improvement for information security management in small and medium enterprises. *Journal of Software-Evolution and Process, 26*, 496-503. doi:10.1002/smr.1609

Cram, W. A., Proudfoot, J., & D'Arcy, J. (18 de Julio de 2017). Organizational information security policies: a review and research framework. *European Journal of Information Systems*, 605–641. doi:10.1057/s41303-017-0059-9

Duncan, B., & Whittington, M. (2014). Compliance with standards, assurance and audit: Does this equal security? *Proceedings of the 7th International Conference on Security of Information and Networks*, 77-84. doi:10.1145/2659651.2659711

Galvan, V. (2013). *Datacenter una mirada por dentro.* Tucumán: Ediciones Índigo. doi:10.13140/RG.2.1.3434.8401

Ghaffari, F., & Abouzar, A. (2018). A New Adaptive Cyber-security Capability Maturity Model. *9th International Symposium on Telecommunications*, 298-304. doi:10.1109/ISTEL.2018.8661018

Gillies, A. (2011). Improving the quality of information security management systems with ISO27000. *The TQM Journal, 23*(4), 367-376. doi:10.1108/17542731111139455

Hong, K., Chi, Y., Chao, L., & Tang, J. (2003). An integrated system theory of information security management. *Information Management y Computer Security, 11*(5), 243-448. doi:10.1108/09685220310500153

Ibrahim, A., Craig, V., McAteer, I., & Chaudhry, J. (2018). A security review of local government using NIST CSF: a case study. *The Journal of Supercomputing, 74*, 5171–5186. doi:10.1007/s11227-018-2479-2

ISOTools. (29 de Diciembre de 2022). Obtenido de https://www.isotools.org/2022/07/22/nueva-iso-iec-270022022-cambios-con-respecto-a-la-version-de-2013/#:~:text=Las%2014%20cl%C3%A1usulas%20se%20cambian,eliminado%20(eliminaci%C3%B3n%20de%20activos).

Kerstetter, K. (29 de Diciembre de 2022). *Compliance Versus Risk: Why Choosing the Right Approach is So Important*. Obtenido de Isaca: https://www.isaca.org/en/resources/news-and-trends/isaca-now-blog/2021/compliance-versus-risk-why-choosing-the-right-approach-is-so-important

Knapp, K., & Ferrante, C. (2012). Policy awareness, enforcement and maintenance: Critical to information security effectiveness in organizations. *Journal of Management Policy and Practice, 13*(5), 66–80. Obtenido de http://www.na-businesspress.com/JMPP/KnappKJ_Web13_5_.pdf

Likert, R. (1932). *A technique for the measurement of attitudes.* R. S. WOODIYORTE.

Lima, M., Lima, R., & Lins, F. (2017). A Multi-Perspective Methodology for Evaluating the Security Maturity of Data Centers. *2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*. doi:10.1109/SMC.2017.8122775

NIST. (29 de Diciembre de 2022). *Special Publication 800-53 Revision 5: Security and Privacy Controlsfor Information Systems and Organizations*. Obtenido de https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

Posthumus, S., & Solms, R. (2004). A framework for the governance of information security. *Computers & Security, 23*, 638-646. doi:10.1016/j.cose.2004.10.006

Prameet, R. (2020). *2020 National Conference on Emerging Trends on Sustainable Technology and Engineering Applications (NCETSTEA)*. doi:10.1109/NCETSTEA48365.2020.9119914

Supriyadi, Y., & Hardani, C. (2018). Information System Risk Scenario Using COBIT 5 for Risk And NIST SP 800-30 Rev. 1 A Case Study. *2018 3rd International Conference on Information Technology, Information System and Electrical Engineering (ICITISEE)*. doi:10.1109/ICITISEE.2018.8721034

Veiga, & Eloff. (2010). A framework and assessment instrument for information security culture. *computers & security*, 196–207. doi:10.1016/j.cose.2009.09.002

Vroom, C., & Rossouw, v. S. (2004). Towards information security behavioural compliance. *Elsevier Computers & Security, 23*, 191-198. doi:10.1016/j.cose.2004.01.012