

**Modelo del efecto económico de la implementación de un framework de seguridad de la información para las organizaciones en Colombia.**

**Juan Carlos Serna Agudelo**


**Asesoras:  
Aixa Villamizar  
Silvana Vallejo**

**Maestría en Gestión de Tecnologías de la Información  
Facultad de Ingenierías  
Tecnológico de Antioquía**

## Resumen

El uso creciente de Tecnologías de Información en las empresas trae consigo una serie de amenazas en contra de la seguridad de la información, que demandan la aplicación de buenas prácticas de ciberseguridad y estas acciones no siempre son valoradas por la alta dirección o se desconocen sus implicaciones.

El presente proyecto pretende proponer un modelo que evidencie el efecto económico de implementar un framework de ciberseguridad en una organización colombiana, justificando de manera explícita su inversión. La investigación se apoya de estudios previos realizados en países desarrollados y donde la ciberseguridad es un componente incluido en los modelos económicos que describen la productividad de las empresas; así como también de una metodología para estimar riesgos en términos de costos. El desarrollo del trabajo puede agruparse en tres fases generales donde inicialmente se realiza un mapeo sistemático de la literatura científica relacionada con modelos económicos y métodos desarrollados previamente, luego se hace extensivo el análisis de estos trabajos para definir un modelo adaptado al contexto empresarial colombiano y finalmente se somete a evaluación el modelo, por medio de la técnica del grupo focal que determine su viabilidad en entornos académicos o empresariales. Con esta herramienta se espera potencializar el uso de los frameworks de ciberseguridad, aumentando el margen de protección ante ataques cibernéticos y pérdidas de información.

	REPOSITORIO INSTITUCIONAL DE INVESTIGACIÓN	Código: FO-INV-02
		Versión: 01
		Fecha de Aprobación: Febrero 07 de 2017
		Página 3 de 6

COPIA CONTROLADA

## Bibliografía

Abreu, J. (2012). Hipótesis, método & diseño de investigación (hypothesis, method & research design). *Daena: International Journal of Good Conscience*, 7(2), 187–197.

Ahmed, E. M. (2021). Modelling Information and Communications Technology Cyber Security Externalities Spillover Effects on Sustainable Economic Growth. *Journal of the Knowledge Economy*, 12(1), 412–430. <https://doi.org/10.1007/s13132-020-00627-3>

Alahmari, A. A., & Duncan, R. A. (2021). Towards Cybersecurity Risk Management Investment: A Proposed Encouragement Factors Framework for SMEs. *2021 IEEE International Conference on Computing, ICOCO 2021*, 115–121. <https://doi.org/10.1109/ICOCO53166.2021.9673554>

Anderson, R. (2001). Why information security is hard - An economic perspective. *Proceedings - Annual Computer Security Applications Conference, ACSAC, 2001-January*, 358–365. <https://doi.org/10.1109/ACSAC.2001.991552>

Anderson, R., & Moore, T. (2009). Information security: Where computer science, economics and psychology meet. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 367(1898), 2717–2727. <https://doi.org/10.1098/rsta.2009.0027>

Banegas, J. I., Quinché, R. G., Diaz, R. F., & Zaquinaula, F. A. (2016). Systematic Literature Review: SQL Injection in Web Applications. *Latin American Journal of Computing*, 3(2), 8.


Bojanc, R., Jerman-Blažič, B., & Tekavčič, M. (2012). Managing the investment in information security technology by use of a quantitative modeling. *Information Processing & Management*, 48(6), 1031–1052. <https://doi.org/https://doi.org/10.1016/j.ipm.2012.01.001>

Díaz, M. R. O., & Rangel, P. E. S. (2020). National challenges for cybersecurity on a global level: An analysis for Colombia. *Revista Criminalidad*. [http://www.scielo.org.co/scielo.php?pid=S1794-31082020000200199&script=sci\\_abstract&tlng=en](http://www.scielo.org.co/scielo.php?pid=S1794-31082020000200199&script=sci_abstract&tlng=en)

Ezhei, M., & Tork Ladani, B. (2017). Information sharing vs. privacy: A game theoretic analysis. *Expert Systems with Applications*, 88, 327–337. <https://doi.org/10.1016/j.eswa.2017.06.042>


Fedele, A., & Roner, C. (2022). Dangerous games: A literature review on cybersecurity investments. *Journal of Economic Surveys*, 36(1), 157–187. <https://doi.org/10.1111/joes.12456>

Guerrero-Narváez, S., Niño-Zambrano, M., Riobamba-Calvache, D.-J., & Ramírez-González, G.-A. (2018). Test bed of semantic interaction of smart objects in the web of things. *Future Internet*, 10(5). <https://doi.org/10.3390/fi10050042>

	REPOSITORIO INSTITUCIONAL DE INVESTIGACIÓN	Código: FO-INV-02
		Versión: 01
		Fecha de Aprobación: Febrero 07 de 2017
		Página 4 de 6


COPIA CONTROLADA

- Huang, C. D., Behara, R. S., & Goo, J. (2014). Optimal information security investment in a Healthcare Information Exchange: An economic analysis. *Decision Support Systems*, 61(1), 1–11. <https://doi.org/10.1016/j.dss.2013.10.011>
- Iannacone, M. D., & Bridges, R. A. (2020). Quantifiable & comparable evaluations of cyber defensive capabilities: A survey & novel, unified approach. *Computers & Security*, 96, 101907. <https://doi.org/https://doi.org/10.1016/j.cose.2020.101907>
- Jeong, C. Y., Lee, S.-Y. T., & Lim, J.-H. (2019). Information security breaches and IT security investments: Impacts on competitors. *Information & Management*, 56(5), 681–695. <https://doi.org/https://doi.org/10.1016/j.im.2018.11.003>
- Kamiya, S., Kang, J.-K., Kim, J., Milidonis, A., & Stulz, R. M. (2021). Risk management, firm reputation, and the impact of successful cyberattacks on target firms. *Journal of Financial Economics*, 139(3), 719–749. <https://doi.org/https://doi.org/10.1016/j.jfineco.2019.05.019>
- Kissoon, T. (2020). Optimum spending on cybersecurity measures. *Transforming Government: People, Process and Policy*, 14(3), 417–431. <https://doi.org/10.1108/TG-11-2019-0112>
- Kurii, Y., & Opirskyy, I. (2022). Analysis and Comparison of the NIST SP 800-53 and ISO/IEC 27001:2013. *CEUR Workshop Proceedings*, 3288, 21–32. <https://www.scopus.com/inward/record.uri?eid=2-s2.0-85143792195&partnerID=40&md5=6672f25624c8d26cff9b20cedaa8d232>
- Mella, O. (2000). Grupos focales (“Focus groups”). Técnica de investigación cualitativa. *Documento de Trabajo*, 3.
- Mendoza-Moreno, M., González-Serrano, C., & Pino, F. J. (2013). Focus group como proceso en ingeniería de software: una experiencia desde la práctica. *Dyna*, 80(181), 51–60.
- Miaoui, Y., & Boudriga, N. (2019). Enterprise security investment through time when facing different types of vulnerabilities. *Information Systems Frontiers*, 21(2), 261–300. <https://doi.org/10.1007/s10796-017-9745-3>
- Nagurney, A., & Nagurney, L. S. (2015). A game theory model of cybersecurity investments with information asymmetry. *NETNOMICS: Economic Research and Electronic Networking*, 16(1–2), 127–148. <https://doi.org/10.1007/s11066-015-9094-7>
- Onwubiko, C., & Onwubiko, A. (2019). Cyber kpi for return on security investment. *2019 International Conference on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA)*, 1–8.
- Panou, A., Ntantogian, C., & Xenakis, C. (2017). RiSKi: A framework for modeling cyber threats to estimate risk for data breach insurance. *ACM International Conference Proceeding Series, Part F132523*. <https://doi.org/10.1145/3139367.3139426>

	REPOSITORIO INSTITUCIONAL DE INVESTIGACIÓN	Código: FO-INV-02
		Versión: 01
		Fecha de Aprobación: Febrero 07 de 2017
		Página 5 de 6

COPIA CONTROLADA

- Paul, J. A., & Zhang, M. (2021). Decision support model for cybersecurity risk planning: A two-stage stochastic programming framework featuring firms, government, and attacker. *European Journal of Operational Research*, 291(1), 349–364. <https://doi.org/10.1016/j.ejor.2020.09.013>
- Rashid, Z., Noor, U., & Altmann, J. (2021). Economic model for evaluating the value creation through information sharing within the cybersecurity information sharing ecosystem. *Future Generation Computer Systems*, 124, 436–466. <https://doi.org/10.1016/j.future.2021.05.033>
- Rivera, C. A. (2020). Modelo para medir el retorno sobre la inversión en seguridad informática y de la información-ROSI. *Publicaciones e Investigación*, 14(3).
- Roy, P. P. (2020). A High-Level Comparison between the NIST Cyber Security Framework and the ISO 27001 Information Security Standard. *2020 National Conference on Emerging Trends on Sustainable Technology and Engineering Applications, NCETSTEA 2020*. <https://doi.org/10.1109/NCETSTEA48365.2020.9119914>
- Rudas, J. S., Gómez, L. M., & Toro, A. O. (2013). Revisión sistemática de literatura. Caso de estudio: Modelamiento de un par deslizante con fines de predecir desgaste. *Prospectiva*, 11(1), 50–58.
- Schilling, A., & Werners, B. (2015). Optimal information security expenditures considering budget constraints. *Pacific Asia Conference on Information Systems, PACIS 2015 - Proceedings*. <https://www.scopus.com/inward/record.uri?eid=2-s2.0-85011024539&partnerID=40&md5=45602e3470140f27013a253c6b52a88d>
- Taherdoost, H. (2022). Understanding Cybersecurity Frameworks and Information Security Standards—A Review and Comprehensive Overview. *Electronics*, 11(14), 2181.
- Tosh, D., Sengupta, S., Kamhoua, C. A., & Kwiat, K. A. (2018). Establishing evolutionary game models for CYber security information EXchange (CYBEX). *Journal of Computer and System Sciences*, 98, 27–52. <https://doi.org/https://doi.org/10.1016/j.jcss.2016.08.005>
- Weishäupl, E., Yasasin, E., & Schryen, G. (2015). A multi-Theoretical literature review on information security investments using the resource-based view and the organizational learning theory. *2015 International Conference on Information Systems: Exploring the Information Frontier, ICIS 2015*. <https://www.scopus.com/inward/record.uri?eid=2-s2.0-85126603063&partnerID=40&md5=01e728bc68f1617459291cb267d49d31>
- Weishäupl, E., Yasasin, E., & Schryen, G. (2018). Information security investments: An exploratory multiple case study on decision-making, evaluation and learning. *Computers and Security*, 77, 807–823. <https://doi.org/10.1016/j.cose.2018.02.001>
- Woods, D. W., & Simpson, A. C. (2018). Towards Integrating Insurance Data into Information Security Investment Decision Making. *2018 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA)*, 1–6. <https://doi.org/10.1109/CyberSA.2018.8551375>

	REPOSITORIO INSTITUCIONAL DE INVESTIGACIÓN	Código: FO-INV-02
		Versión: 01
		Fecha de Aprobación: Febrero 07 de 2017
		Página 6 de 6

COPIA CONTROLADA

- Xu, L., Li, Y., & Fu, J. (2019). Cybersecurity investment allocation for a multi-branch firm: Modeling and optimization. *Mathematics*, 7(7). <https://doi.org/10.3390/math7070587>
- Yaqoob, T., Arshad, A., Abbas, H., Amjad, M. F., & Shafqat, N. (2019). Framework for Calculating Return on Security Investment (ROSI) for Security-Oriented Organizations. *Future Generation Computer Systems*, 95, 754–763. <https://doi.org/https://doi.org/10.1016/j.future.2018.12.033>
- Forbes (2021). Empresas colombianas prevén duplicar sus inversiones en IA en los próximos cuatro años. (29 de agosto de 2022). Recuperado de: <https://forbes.co/2021/08/17/tecnologia/empresas-colombianas-preven-duplicar-sus-inversiones-en-ia-en-los-proximos-cuatro-anos/>
- Tiempo, C., 2022. La ciberdelincuencia no segmenta: todos somos vulnerables. [online] Portafolio.co. Available at: <<https://www.portafolio.co/opinion/otros-columnistas-1/ciberdelincuencia-colombia-perdidas-anuales-155222>> [Accessed 6 September 2022].
- Tiempo, C., 2022. Cifras de ciberseguridad en Colombia prenden alarmas al cierre de 2020. [online] Portafolio.co. Available at: <<https://www.portafolio.co/tendencias/cifras-de-ciberseguridad-en-colombia-prenden-alarmas-al-cierre-del-2020-547412>> [Accessed 6 September 2022].
- Sagar, R., 2022. Top Cybersecurity Budgets Around The World. [online] Analytics India Magazine. Available at: <<https://analyticsindiamag.com/top-cybersecurity-budgets-around-the-world/>> [Accessed 7 September 2022].
- S.A.S., E., 2022. Condiciones del mercado de ciberseguridad colombiano atraen a nuevos jugadores. [online] Diario La República. Available at: <<https://www.larepublica.co/empresas/condiciones-del-mercado-de-ciberseguridad-colombiano-atraen-a-nuevos-jugadores-3324669>> [Accessed 9 September 2022].
- Etek.com. 2022. Ataques de Ciberseguridad aumentan en el 2022 – etek. [online] Available at: <<https://etek.com/es/ataques-de-ciberseguridad-aumentan-en-el-2022/>> [Accessed 9 September 2022].
- Modelo de Seguridad - Fortalecimiento TI. (s. f.). <https://www.mintic.gov.co/gestion-ti/Seguridad-TI/Modelo-de-Seguridad/>