METHODOLOGY BASED ON THE NIST CYBERSECURITY FRAMEWORK AS A PROPOSAL FOR CYBERSECURITY MANAGEMENT IN GOVERNMENT ORGANIZATIONS

Maurice Frayssinet Delgado
Graduate University School - EUPG - Federico Villarreal National University, (Peru).
E-mail: mfrayssinet@gmail.com ORCID: https://orcid.org/0000-0001-6223-2577

Doris Esenarro
Specialized Institute for Ecosystems and Natural Resources Research (INERN).
Graduate University School - EUPG - Federico Villarreal National University, (Peru).
E-mail: desenarro@unfv.edu.pe ORCID: https://orcid.org/0000-0002-7186-9614

Francisco Fernando Juárez Regalado
Graduate University School - EUPG - Federico Villarreal National University,
Universidad Tecnológica del Perú-UTP, (Peru).
E-mail: ffjuarezr@hotmail.com ORCID: https://orcid.org/0000-0002-3942-7832

Mónica Díaz Reátegui
Graduate University School - EUPG - Federico Villarreal National University.
Universidad Norbert Wiener, (Peru).
E-mail: monicdre@yahoo.com ORCID: https://orcid.org/0000-0003-4506-7383

Recepción: 29/04/2021 **Aceptación:** 18/06/2021 **Publicación:** 29/06/2021

Citación sugerida:
Frayssinet, M., Esenarro, D., Juárez, F. F., y Díaz, M. (2021). Methodology based on the NIST cybersecurity framework as a proposal for cybersecurity management in government organizations. *3C TIC. Cuadernos de desarrollo aplicados a las TIC, 10*(2), 123-141. https://doi.org/10.17993/3ctic.2021.102.123-141

ABSTRACT

This research aims to propose the use of the methodology based on the NIST Framework for adequate management of cybersecurity in government organizations within the framework of the delivery of digital services. Many government organizations have been managing cybersecurity without a defined process; this generates that the management is deficient and without indicators. Concerning whether they are implementing the methodology based on the NIST cybersecurity framework", shows that 36.8% of respondents present a level in disagreement, 31.6% (6) an undecided level, 15.8% (3) a level of agreement, 10.5% (2) a level totally in disagreement and 5.3% (1) a level totally in agreement. Meanwhile, the variable "The management of cybersecurity" shows that 36.8% (7) of the Ministries surveyed present a level in disagreement; 36.8% (7) an undecided level, 15.8% (3) a level of agreement, and 10.5% (2) a level totally in disagreement In conclusion: It has been shown that the use of the methodology based on the NIST cybersecurity framework influences cybersecurity management in government organizations and it is clear that they are currently not using it which causes a relatively poor level of leadership in the implementation of security measures concerning cybersecurity management.

KEYWORDS

Methodology, Nist Cybersecurity Framework, Cybersecurity, Management.

https://doi.org/10.17993/3ctic.2021.102.123-141

1. INTRODUCTION

New information technologies have been developing more and more, giving rise to more significant interaction of the internet the person, which causes a large volume of information within cyberspace, such fact has led to the emergence of digital threats, which cause adverse effects on the lives of people and many institutions, being victims of information theft. Often cybercriminals can not be identified by the authorities, so States have to adapt their structures and use regulatory frameworks, strategies, or cybersecurity policies (Nagurney & Shukla, 2017). In the region, it is possible to highlight that there are already ten countries with a national cybersecurity policy or strategy. Recently, the Dominican Republic and Guatemala joined the list integrated by Colombia, Trinidad and Tobago, Jamaica, Panama, Chile, Costa Rica, Mexico, and Paraguay (Alvarez, 2018). In the case of Peru, it could be said that it is a country with insufficient awareness in terms of digital security, risks, and protection, being one of the countries that have legislated the least in terms of cyber defense and cybersecurity, i.e., there are no national security strategies. Therefore, there is a need to take protective measures against malicious attacks within both the public and private sectors (Montes, 2020).

In a comparison made in the Cybersecurity Report 2020, it can be observed that in Peru, there was no progress since 2016 in terms of Cyber Security Policy and Strategy (National Cyber Security Strategy, Critical Infrastructure Protection). Likewise, there is no difference in Cyber Security Training, Capacity Building, and Skills (Awareness Raising, Framework for Training, Framework for Professional Training). Furthermore, no changes in Legal and Regulatory Frameworks (Criminal Justice System) were visualized. Finally, no progress in Standards, Organizations, and Technologies (Standards Compliance, Internet Infrastructure Resilience, Responsible Disclosure) (Cybersecurity Observatory in Latin America and the Caribbean, 2020).

To date, after the increase of digital processes due to the state of a health emergency, it is worrying the amount of sensitive information that is handled online and see that many of the institutions, both public and private, do not have a policy or strategy to help neutralize the loss or deterioration of information,

https://doi.org/10.17993/3ctic.2021.102.123-141

also unauthorized access by cybercriminals, which steal the essential knowledge of the institutions (León, 2021). It is worth mentioning that, in these times, all organizations require and demand the use of technologies, but many of them do not know how to handle it; as far as cybersecurity is concerned, this means that they do not have a methodology for the detection of incidents. This is the reason for the great concern about the risks to which government institutions and citizens are exposed (Santos, 2020). Cybersecurity has a value; today, we express it in the concept of digital trust, an approach that allows citizens, in general, to feel confident to use digital technologies and services (Presidency of the Council of Ministers. Government of Peru, 2018).

When the standards or methodologies that exist for adequate protection of technology are not respected and mismanaged, we find its weak point, which causes cybersecurity breaches to be created that compromise the confidentiality, integrity, or availability of technological assets.

NIST framework methodology

The Framework provides a common language for understanding, managing, and expressing cybersecurity risk for internal and external stakeholders. It can help identify and prioritize actions to reduce cybersecurity risk and align policy, business, and technology approaches to manage cybersecurity risk. It can also be used to manage cybersecurity risk across all parts of an organization or can be focused on the delivery of critical services within one part of the organization. Different types of entities, including sector coordination structures, associations, and organizations, can use the Framework for other purposes, including the creation of Common Profiles. The NIST framework, a set of activities and deliverables for a guide to assess organizational IT security, consists of 3 parts:

- 05 High-level functions.
- 23 Categories, which cover technical aspects, people and processes, with a focus on results.
- 108 Subcategories, which are based on results, to create or improve a cybersecurity program.

https://doi.org/10.17993/3ctic.2021.102.123-141

It is worth mentioning that it is a tool for cybersecurity risk management, which fits any type of organization. In addition, it can be used as a key part of your systematic process, which does not replace existing processes. Rather, it determines gaps and improves them, optimizing costs and results (National Institute of Standards and Technology, 2018; Wallis, 2018; Almagro, 2019).

Table 1. NIST Framework methodology categories.

Function Identifier	Function	Category Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Source: own elaboration.

The NIST Framework has five functions: Identify, Protect, Detect, Detect, Respond, and Recover; in each of these functions, you can see the framework categories that group strategies for managing cybersecurity in an organization (Gomez, 2019).

https://doi.org/10.17993/3ctic.2021.102.123-141

Cybersecurity

In essence, cybersecurity is dedicated to protecting everything that is safeguarded in the intangible medium of cyberspace, sensitive information concerning operating systems, media, national plans, innovations, and strategic infrastructure. For example, for criminals and terrorists, the connectivity of industrial control systems presents windows of opportunity for the attack at points where the impact on a nation's power is most significant, highlighting the dangers posed by cyber-attacks on critical infrastructure for public welfare economic development. Therefore, achieving cybersecurity is a joint work between government, private initiative, and citizens (García, 2019).

Cybersecurity is effective when cyberspace is considered reliable, secure, and flexible. Its primary objective was to prevent an attack from being carried out successfully. Currently, its goals are to prevent, detect, respond and recover. Most security professionals consider that it is impossible to avoid all attacks; that is why there must be planning and preparation that involves methods of detection and prevention of seizures (Leiva, 2015; ITU, 2018; Watson, 2019).

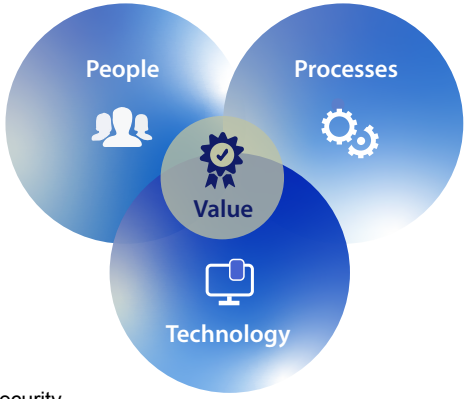

Figure 1. Three components of Cybersecurity.
Source: own elaboration.

Cybersecurity must contemplate the three components for its proper management, the focus on people that must be trained, the processes that must be written, defined, and implemented, and finally, the

https://doi.org/10.17993/3ctic.2021.102.123-141

necessary technology to implement the technical controls. All three are interrelated and must be managed (Fadrell Grupo Tecnológico, 2020; Vilcarromero & Vilchez, 2018).

Defining a digital security strategy is necessary, identifying vulnerabilities and protecting against cyber-attacks. To do so, the following actions are defined:

- Perform backups (backups) of information and confirm the restoration process.
- Update information technology systems.
- Raise employee awareness of the importance of cybersecurity.
- Control the information environment.
- Layered defense to reduce risk (Fadrell Grupo Tecnológico, 2020).

Management

Management is generally defined as a social process and by the actors that embody it (Clegg, 2005; Déry, 2010). As a social process, management brings together the set of management devices that are implemented to make an organization effective and efficient. While effectiveness refers to achieving the objectives set, efficiency refers to optimizing the means about the aim. As many management specialists have shown, this distinction is not neutral in implementing management practices, with some managers favoring effectiveness and others essentially favoring efficiency.

2. METHOD

The Experimental Research design has been selected since it handles variables of the cause-effect type. The independent variable is of interest to the researcher because the hypothesized variable (X) is one of the causes that produce the supposed effect.

https://doi.org/10.17993/3ctic.2021.102.123-141

3. RESULTS

In this research, a survey was conducted to 19 government organizations, where questions were posed about the current state of cybersecurity management with a scale to be used:

Level 0= Strongly disagree.

Level 1= Disagree.

Level 2= Undecided.

Level 3= Agree.

Level 4= Strongly agree.

The following results were obtained:

Table 2. Dimension: Nist Framework Phases.

		Frequency	Percentage	Valid Percentage	Cumulative Percentage
Valid	Strongly Disagree	2	10,5	10,5	10,5
	Disagree	7	36,8	36,8	47,4
	Undecided	6	31,6	31,6	78,9
	Agree	4	21,1	21,1	100,0
	Total	19	100,0	100,0	

Source: own elaboration.

Table 2 shows the information protection processes and procedures that have been established in the organization.

https://doi.org/10.17993/3ctic.2021.102.123-141

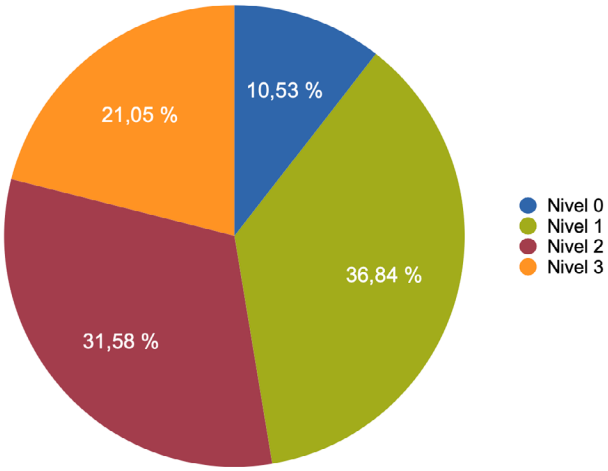

Figure 2. Dimension: phases of Nist Framework.
Source: own elaboration.

Figure 2 shows that protection processes and procedures were established in the organization.

According to Table 2 and Figure 2, 36.84% of the government organizations present a level of disagreement on establishing processes and procedures for information protection in the organizations. In the Nist Framework Phases dimension, 31.58% of the respondents were undecided, 21.05% agreed, and 10.53% disagreed.

Table 3. Dimension: Nist Framework Phases.

		Frequency	Percentage	Valid Percentage	Cumulative Percentage
Valid	Strongly Disagree	3	15,8	15,8	15,8
	Disagree	4	21,1	21,1	36,8
	Undecided	7	36,8	36,8	73,7
	Agree	4	21,1	21,1	94,7
	Strongly Agree	1	5,3	5,3	100,0
	Total	19	100,0	100,0	

Source: own elaboration.

In Table 3, the procedures have been implemented for intrusion detection in the organization.

https://doi.org/10.17993/3ctic.2021.102.123-141

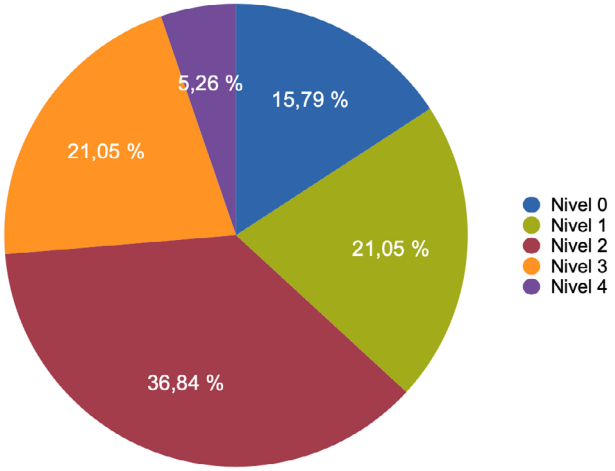

Figure 3. Dimension: Phases of Nist Framework.
Source: own elaboration.

From Figure 3, it can be deduced that procedures for intrusion detection have been implemented in the organization.

According to Table 3 and Figure 3, 36.84% of the government organizations present an undecided level about implementing procedures for intrusion detection in the organizations. In the Nist Framework Phases dimension, 21.05% disagreed and agreed; 15.79% disagreed, and 5.26% agreed.

Table 4. Dimension: Incident Level.

		Frequency	Percentage	Valid Percentage	Cumulative Percentage
Valid	Strongly Disagree	1	5,3	5,3	5,3
	Disagree	8	42,1	42,1	47,4
	Undecided	7	36,8	36,8	84,2
	Agree	2	10,5	10,5	94,7
	Strongly Agree	1	5,3	5,3	100,0
	Total	19	100,0	100,0	

Source: own elaboration.

In Table 4, a plan for incident management has been implemented.

https://doi.org/10.17993/3ctic.2021.102.123-141

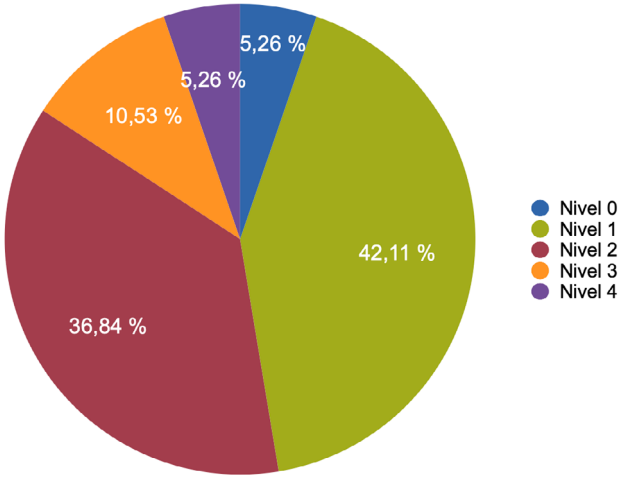

Figure 4. Dimension: Incident level.
Source: own elaboration.

In Figure 4, a plan for incident management has been implemented.

According to Table 4 and Figure 4, 42.11% of the government organizations present a level of Disagree on implementing a plan for incident management in the organizations. Incident Level Dimension, 36.84% an undecided level; 10.53% an agreed level and 5.26% a disagree level; decide on the deck.

Table 5. Dimension: Incident Level.

		Frequency	Percentage	Valid Percentage	Cumulative Percentage
Valid	Strongly Disagree	4	21,1	21,1	21,1
	Disagree	4	21,1	21,1	42,1
	Undecided	8	42,1	42,1	84,2
	Agree	2	10,5	10,5	94,7
	Strongly Agree	1	5,3	5,3	100,0
	Total	19	100,0	100,0	

Source: own elaboration.

In Table 5, a plan has been implemented for communication between areas involved in an incident.

https://doi.org/10.17993/3ctic.2021.102.123-141

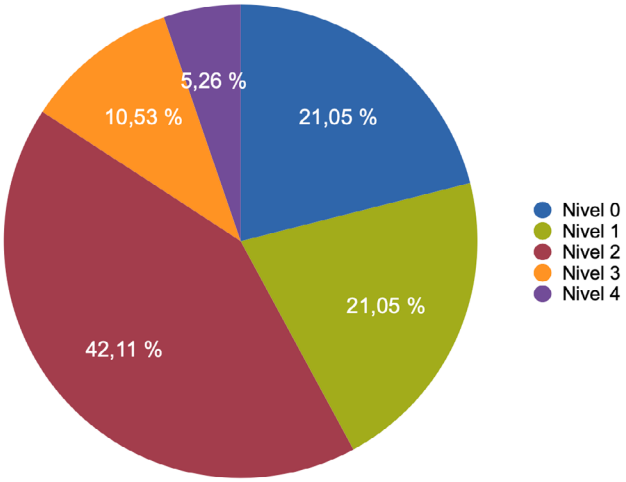

Figure 5. Dimension: Incident level.
Source: own elaboration.

In Figure 5, the implementation of a plan for communication between areas involved in an incident.

According to Table 5 and Figure 5, 42.11% of the government organizations present an undecided level on implementing a plan for communication between areas involved before an incident in the organizations. 21.05% disagreed and disagreed; 10.53% agreed, and 5.26% agreed.

Table 6. Capabilities.

		Frequency	Percentage	Valid Percentage	Cumulative Percentage
Valid	Strongly Disagree	5	26,3	26,3	26,3
	Disagree	4	21,1	21,1	47,4
	Undecided	7	36,8	36,8	84,2
	Agree	1	5,3	5,3	89,5
	Strongly Agree	2	10,5	10,5	100,0
	Total	19	100,0	100,0	

Source: own elaboration.

The Table 6 show all personnel are trained and informed.

https://doi.org/10.17993/3ctic.2021.102.123-141

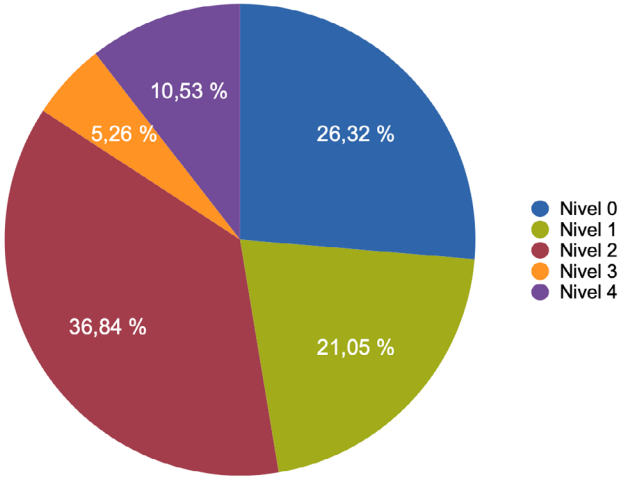

Figure 6. Capabilities.
Source: own elaboration.

Figure 6 shows that all personnel is informed.

According to Table 6 and Figure 6, 36.84% of the government organizations present an undecided level about the training and education of all personnel in the organizations. In the Capabilities dimension, 26.32% disagree; 21.05% disagree; 10.53% totally agree, and 5.26% agree.

Table 7. Dimension: Capabilities.

		Frequency	Percentage	Valid Percentage	Cumulative Percentage
Valid	Strongly Disagree	6	31,6	31,6	31,6
	Disagree	5	26,3	26,3	57,9
	Undecided	6	31,6	31,6	89,5
	Agree	2	10,5	10,5	100,0
	Total	19	100,0	100,0	

Source: own elaboration.

The Table 7 show there is training in cybersecurity issues.

https://doi.org/10.17993/3ctic.2021.102.123-141

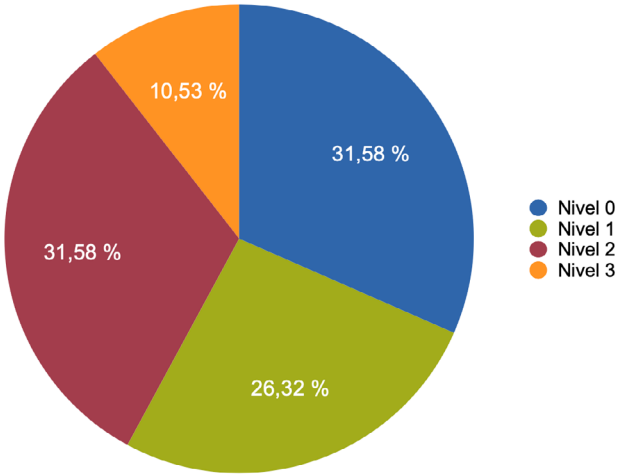

Figure 7. Dimension: capabilities.
Source: own elaboration.

Figure 7 shows that there is training in cybersecurity issues.

According to Table 7 and Figure 7, 31.58% of government organizations present a disagree and uncertain status on training in cybersecurity issues in organizations. In the Capabilities dimension, 26.32% disagreed, and 10.53% strongly agreed.

Concerning the general statistical hypothesis, we have the following results:

Hi: using the methodology based on the NIST framework does influence cybersecurity management in government organizations.

Ho: using the methodology based on the NIST framework does not influence cybersecurity management in government organizations.

https://doi.org/10.17993/3ctic.2021.102.123-141

Table 8. Chi-square tests of the methodology based on the NIST framework and the management of cybersecurity in government organizations.

	Value	gl	Asymptotic significance (bilateral)
Pearson's Chi-square	34,392a	12	,433
Likelihood ratio	35,706	12	,303
Linear by linear association	14,651	1	,208
N of Valid cases	19		
a.; four boxes (66.7%) have expected a count of less than 5. The minimum expected count is 54.			

Source: own elaboration.

According to Table 6, when the chi-square statistic was applied, a correlation coefficient value (p) of 0.433 was obtained. As the (p) value is less than the significance level ($\alpha = 0.5$), it allows us to have sufficient evidence to accept the alternative research hypothesis and reject the null hypothesis. Therefore, the use of the methodology based on the NIST framework influences cybersecurity management in government organizations.

4. DISCUSSION

According to Alvarez, in the region, there are already ten countries with a national cybersecurity policy or strategy; however, Peru is not among them; this can be evidenced in the lack of proper cybersecurity management that is evident in this study. Santos (2020) also speaks of the great concern for the risks to which government institutions and citizens are exposed; in this sense, I reaffirm that it is only a concern, but it has not yet been transferred to the implementation of effective measures to manage cybersecurity.

5. CONCLUSIONS

It was observed that most government organizations do not have formalized cybersecurity, since they do not have incident statistics; this is due to poor management by untrained personnel.

https://doi.org/10.17993/3ctic.2021.102.123-141

It has been shown that there is an influence between the use of the methodology based on the NIST framework and cybersecurity management in government organizations obtaining. As a result, Pearson's chi-square = 0.433.

It is recommended that government organizations adopt the NIST cybersecurity Framework methodology to measure cybersecurity improvement and management.

REFERENCES

Almagro, L. (2019). NIST Cybersecurity Framework (CSF) / A comprehensive approach to cybersecurity. *White paper series, Issue 5.* http://www.itsd.gov.vc/itsd/images/pdf_documents/OAS_AWS_NIST_Cybersecurity_Framework_CSF_ENG.pdf

Alvarez, D. (2018). Cybersecurity in Latin America and cyber defense in Chile. *Chilean journal of law and technology, 7*(1). https://rchdt.uchile.cl/index.php/RCHDT/article/view/50416

Ayala, C., & Lopez, E. (2019). *Design and implementation of ISO 27035 (information security incident management) for the service platform area of a Peruvian state entity.* http://repositorio.utp.edu.pe/handle/UTP/2477

Clegg, S. R. (2005). *Managing and Organizations: an introduction to theory and practice*. SAGE.

Cybersecurity Observatory in Latin America and the Caribbean. (2020). *CYBERSECURITY: Risks, progress and the way forward in Latin America and the Caribbean.* USA. https://observatoriociberseguridad.org/

Dammert, L., & Núñez, C. (2019). Facing cyber threats: national cybersecurity strategies in the Southern Cone. *Security, Science & Defense, 5*(5), 107-129. http://35.190.156.69/index.php/rscd/article/view/99

https://doi.org/10.17993/3ctic.2021.102.123-141

Déry, R. (2010). *Les perspectives de Management.* JFD Éditions.

Dominguez, D. (2020). National cyber security system in the face of cyber attacks as a threat to National Security. *Journal of Defense Science and Research, 1*(2), 43-48. http://recide.caen.edu.pe/index.php/Recide/article/view/11/18

Fadrell Grupo Tecnológico. (2020). *Cybersecurity pie chart*. http://www.fadrell.com/ciberseguridad-defensa-en-capas-para-reducir-el-riesgo/grafica-circular-ciberseguridad/

Fernández, D., & Martínez, G. (2018). *Cybersecurity, cyberspace and cybercrime.* Thomson Reuters Aranzadi.

García, A. (2019). *Cybersecurity Why is it important for everyone?* Siglo XXI Editores Mexico.

García, O. (2019). *Information Security Governance Model for the Office of the Comptroller General of the Republic of Colombia*. https://bdigital.uexternado.edu.co/handle/001/1895

Gómez, Á. (2019). *Designing an enterprise cybersecurity program based on the NIST framework.* https://hdl.handle.net/10953.1/11905

Gomez, G. (2019). *What is the U.S. NIST Cybersecurity Framework?* https://www.esan.edu.pe/conexion/actualidad/2019/04/30/que-es-el-cybersecurity-framework-de-nist-de-los-estados-unidos/

International ISO/IEC Standard 27000. (2018). *Information technology-Security techniques-Information security management systems-Information security management systems-Overview and vocabulary.* Switzerland.

ITU. (2018). *Global Cybersecurity Index (GCI)*. ITU Publications. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

https://doi.org/10.17993/3ctic.2021.102.123-141

Leiva, E. (2015). National cybersecurity strategies: comparative study based on top-down approach from a global to a local vision. *Latin American Journal of Software Engineering, 3*(4), 161-17. https://doi.org/10.18294/relais.2015.161-176

León, J. (2021). Cybersecurity and personal data protection in Peru. *Advocatus*, (039), 15-21.

Martinez, N. (2019). *Cybersecurity and operational risk in organizations*. https://repositorio.comillas.edu/xmlui/handle/11531/42317

Montes, J. (2020). Integrated cybersecurity strategies for strengthening homeland security. *Journal of Defense Science and Research, 1*(4), 36-48. http://recide.caen.edu.pe/index.php/Recide/article/view/29

Nagurney, A., & Shukla, S. (2017). Multiform models of cybersecurity investment competition vs. cooperation and network vulnerability. *European Journal of Operational Research, 260*(2), 588-600. https://doi.org/10.1016/j.ejor.2016.12.034

National Institute of Standards and Technology. (2018). *Framework for improving cybersecurity in critical infrastructure.* https://www.nist.gov/system/files/documents/2018/12/10/frameworkesmell-rev_20181102mn_clean.pdf

Poma, A., & Vargas, R. (2019). Problematic in Cybersecurity as protection of computer systems and social networks in Peru and the World. *Revista SCIÉNDO, 22*(4), 275-282. https://revistas.unitru.edu.pe/index.php/SCIENDO/article/view/2692

Presidency of the Council of Ministers. Government of Peru. (2018). *Legislative Decree No. 1412: Legislative Decree approving the Digital Government Law.* https://www.gob.pe/institucion/pcm/normas-legales/289706-1412

https://doi.org/10.17993/3ctic.2021.102.123-141

Rios, J. (2018). *Digital certification and efficient administrative management in Peruvian State Institutions.* http://repositorio.unfv.edu.pe/bitstream/handle/UNFV/2476/RIOS%20BARRIOS%20JUAN%20CARLOS%20HUGO%20-MAESTRIA.pdf?sequence=1&isAllowed=y

Santos, Z. (2020). *From the documented public service to the digital public service*. https://cader.sunarp.gob.pe/repositorio/cader/cader2019/jornadas/jornada1/docs/01D.pdf

Tates, C., & Recalde, L. (2019). Cybersecurity in Ecuador, a proposal for Organization. *Journal of Security and Defense Sciences, IV*(7), 156-169. http://geo1.espe.edu.ec/wp-content/uploads/2019/03/7art12.pdf

Vila, G. (2019). *Cyberattacks as threats to infrastructures and resources.* Estrategia Magazine. https://www.gub.uy/ministerio-defensa-nacional/sites/ministerio-defensa-nacional/files/2020-03/Revista_Estrategia_6.pdf#page=24

Vilcarromero, L., & Vilchez, E. (2018). *Proposal for the implementation of a cybersecurity management model for the security operations center (SOC) of a telecommunications company*. https://repositorioacademico.upc.edu.pe/handle/10757/624832

Villamil, W. (2019). *Risk management in government entities in Colombia.* http://35.227.45.16/bitstream/handle/20.500.12277/6351/Gestion%20de%20Riesgos%20en%20Entidades%20del%20Gobierno.pdf?sequence=1&isAllowed=y

Wallis, A. (2018). *What is Information Security? Why it's Important, Job Outlook and Mo*re. https://www.snhu.edu/about-us/newsroom/2018/06/what-is-information-security

Watson, M. (2019). *The top 4 cybersecurity frameworks*. https://www.itgovernanceusa.com/blog/top-4-cybersecurity-frameworks

https://doi.org/10.17993/3ctic.2021.102.123-141