Journal of Applied Research and Technology

www.jart.icat.unam.mx

Journal of Applied Research and Technology 22 (2024) 284-294

Original

The importance of cyber protection in the power grid in the face of an uncertain future

G. Silva Atencio[a]* • M. Umaña Ramírez[b]

[a]*Universidad Latinoamericana de Ciencia y Tecnología (ULACIT), San José, Costa Rica*
[b]*Universidad Católica de El Salvador (UNICAES), Santa Ana, El Salvador*

Received 09 13 2023; accepted 11 08 2023
Available 04 30 2024

Abstract: In the digital era, cybersecurity is transforming the behavior of human beings in the correct use of technology, regulations, and it has become a critical element in business strategy, thus giving rise to the present research, which identified the current situation of associated companies in the process of generation, transmission, distribution and public lighting of electricity in Costa Rica, in the field of cybersecurity, with particular emphasis on the identification, analysis and evaluation of policies, standards, procedures, controls, regulations and infrastructure in the sector. The study approach was quantitative, descriptive, and exploratory, based on a sample of experts in information security, where a survey was used for data collection. In the findings obtained, personnel with the technical knowledge to deal with a computer incident were observed. Still, from the business perspective, the need for institutional guidelines and country strategy to protect the electrical network was recognized. In conclusion, there is a latent risk in the infrastructure of the national power grid, evidenced by the lack of a clear national strategy that establishes a roadmap to protect the sector against a cyber-attack.

Keywords: cybersecurity, power grid, hacker, vulnerability

*Corresponding author.
E-mail address: gsilvaa468@ulacit.ed.cr (G. Silva Atencio).
Peer Review under the responsibility of Universidad Nacional Autónoma de México.

1. Introduction

Cybersecurity in electrical infrastructure is a topic of global attention and concern. Cyberspace is a fierce and empirical field dominated by a common denominator; there are no rules, good or bad, moral, or immoral; they are subjective criteria that vary according to the latitude and longitude where they are addressed.

The current context of cybersecurity goes beyond just safeguarding the pillars of information technologies: availability, integrity, and confidentiality. In little more than a decade, humanity has witnessed human losses, corruption in the democracy of several countries, and fraud in the leading economies of the planet. The above was achieved with resources such as a computer and Internet connection, the same that any elementary school student would have at home; malicious actors use technology to damage and jeopardize what today's society has built in the last century (Congressional Digest, 2019).

The critical infrastructure of the planet is at risk. Industries such as hydrocarbons, electricity, transportation, telecommunications, health, and food are vulnerable to a cyber-attack (Zuluaga, 2020). In the Costa Rican framework, the monopolistic economic model in the electricity industry identifies the Instituto Costarricense de Electricidad (ICE), the Compañía Nacional de Fuerza y Luz (CNFL) and the Empresa de los Servicios Públicos de Heredia (ESPH) as the central governmental institutions in charge of bringing electricity service to the more than 5 million inhabitants of Costa Rica.

Cybersecurity in the country's electricity industry is a little explored and scarce field of information, being a complex discipline that, among many skills, requires much dedication to understand the why of things to find computer gaps to ensure that unauthorized persons enter critical systems.

Costa Rica has government institutions that ensure national security and others that guarantee the use of technology as an engine of development for the country. It is essential that, as a country, joint efforts are created to identify the current challenges of the cybersecurity strategy. When placing current policies, the responsible institutions use international standards as a reference, which is an excellent starting point to make an objective situational assessment, allowing to establish the backbone of this research.

Today's technological challenges are complex. Public and private sector awareness is essential; this is the only way to move into the future. Some demographics like Costa Rica's, such as the European Union, the Middle East, and Latin America, show that, with intersectoral interest, situations that would be devastating for the population and the economy can be prevented. For this reason, the study obtained the following results:

1. To assess current policies in Costa Rican cybersecurity in electricity supply.
2. To clarify which is the body in charge of risk mitigation in the event of a cyber-attack on the national electric infrastructure.
3. To objectively demonstrate the national strategy for protecting the electric power supply to the Costa Rican population.

Also, the research seeks to be a reference to understand the national position concerning the current cyber threat exposure. In addition, it can be a source of information to propose a comprehensive cybernetic policy for all sectors of the economy. From the above, the question arises: What is the current situation of the Costa Rican electricity industry in the face of a possible cyber-attack? How has the country prepared itself to guarantee the electricity service's continuity and mitigate the population's associated risks?

To achieve the study's objective, a bibliometric review was conducted in different scientific databases and on official websites. In this case, publications from 2011, 2012, and 2013 were considered to know the actual situation only three years after the first event, cataloged by the international cybersecurity community as the genesis of attacks on primary infrastructure. Additionally, recent sources in the years 2019, 2020, and 2021 were reviewed in conjunction with regulations developed by the National Security Agency (NSA), Department of Homeland Security (DHS), and practical manuals on the portal of the Cybersecurity and Infrastructure Security Agency (CISA).

After the bibliometric review, we proceeded to the collection and analysis of data from critical actors in cybersecurity in Costa Rica, being the participating experts the primary source of information in the study, where, based on the findings, it was complemented with a complementary review of the literature, to generate a discussion; and develop the most relevant conclusions in the national power grid and its integration into the cyberspace.

2. Materials and methods

The study had a quantitative approach, as it is tested a hypothesis based on numerical measurement and statistical analysis to establish patterns of behaviors and test theories (Dzul, 2020), along with the development of the investigated object, seeking regularities and relationships between the components of the study (Creswell & Poth, 2018). Additionally, a descriptive subcategory was established, which sought to identify the properties and characteristics of the phenomenon related to the main strategies for protecting electrical infrastructure in Costa Rica (Creswell & Poth, 2018). Also, to model the factors to be considered in the information security strategies of a country, an exploratory type subcategory was taken into account to detail each element involved (Rockmore, 2005).

For this purpose, a sample of 100 information security professionals with proven knowledge, experience, and expertise in cybersecurity in Costa Rica for 2022 was selected. The sample size was determined using the finite population model since the open database of expert professionals in the area was known at the time of the study, thanks to the information provided by the Colegio de Profesionales en Informática y Computación (CPIC) in Costa Rica (de Haro, 2017).

The data collection instrument was a mixed survey (open and closed questions) to learn about the perspectives on the topic of study (Hernández-Sampieri & Mendoza, 2020). Therefore, e-mail was established as a means of contact, mainly because of the participants' advantages in time, cost, and ease of being answered at any time. Then, a 5-point Likert scale was used for the closed questions, allowing a valuation ranging from disagree (1) to agree (5) concerning the statements presented and an open question to collect complementary data for the research.

Subsequently, data analysis was performed to test the hypothesis. Marino (2014) states that the hypothesis is the assumption of the investigated object, being the assumption for the study the following:

> "The national electrical infrastructure has an information security management system, which protects mission-critical services against a cyber-attack."

They sought to determine the current situation of the technological infrastructure in Costa Rica in the face of a possible cyber-attack affecting business continuity in the primary services of the Costa Rican state and to be able to promote the necessary preventive and corrective actions to avoid damage to the image and investment in the country (Baggott & Santos, 2020; Rusco, 2021).

3. Theoretical framework

Today, the exponential advance that technology has had given rise to the question of whether modern civilization is building a better future or, on the contrary, is destroying what has been made in the last 100 years; the reality is that, as of 2021, cyber threats cost the global economy close to 6 trillion dollars (Middaugh, 2021).

Pernik et al. (2016) explain in their study the division of cyber security tasks and responsibilities between different agencies and describe their mandate, duties, and competencies, and the coordination among them. It depicts political and strategic management grants, operational cyber security capabilities and cyber incident management, military cyber defense, and cyber aspects of crisis prevention and crisis management. It also offers a summary of the national information society setting and e-government initiatives and the national cyber security strategy objectives to clarify the context for the organizational approach in a particular nation. The result is a series of country chapters outlining national cyber security management structures by the government. This is a roadmap for the future of cybersecurity in different countries.

At the country level, Soni (2020) explains that Artificial intelligence is generally an associate of humans that apply problem-solving techniques and learning to understand activities' high levels in operation of the human-inspired elements, decision-making, and emotional cycle. As opposed to human intelligence, artificial intelligence is machine-based intelligence. Based on research evaluating the challenges related to artificial intelligence for cybersecurity in the United States. The study proposes an innovative solution for Artificial Intelligence in cybersecurity in the United States of America (USA).

Based on Tvaronavičienė et al. (2020), the cyber security management of critical energy infrastructure in national cybersecurity strategies: cases of USA, United Kingdom (UK), France, Estonia and Lithuania are very insightful. The progress made in cybersecurity in these past years has been tremendous, and the implementation of newer strategies has brought exciting results all over the globe. However, the full implementation of cybersecurity presents a challenge to many countries, especially if considered Critical Infrastructure Protection (CIP), which is still one of the areas with the most gaps in terms of cybersecurity. The previous research explains what the first five countries by cybersecurity level according to the Global Cybersecurity Index (GCI) 2018, in the UK, USA, France, Estonia, and Lithuania, will be evaluated for their solutions in terms of Critical Infrastructure Protection. The results will show the practical accuracy of the index and will shed light on the various approaches to Critical Infrastructure Protection.

Maroto (2009) states that cyber espionage and cybersecurity are violent in the 21st century. These are new forms of warfare and pose strategic studies for states. At the national level, the Gobierno de México (2017) has attempted to create "The National Cybersecurity Strategy" using a study that establishes the vision of the Mexican State in the matter based on the recognition of:

1. Information and Communication Technologies (ICT) is important as a factor in Mexico's political, social, and economic development, with the understanding that more individuals are connected to the Internet and that both private and public organizations develop their activities in cyberspace.
2. The risks associated with using technologies and the growing number of cybercrimes.
3. The need for a general culture of cybersecurity.
4. The increase in risks, threats, and sophisticated computer attacks.
5. The global nature of cyberspace and the concurrence of different sovereignties and legal frameworks.

All the above makes it difficult to treat the issue of cybersecurity as an isolated case for one country.

In June 2010, engineers at the Natanz nuclear power plant informed their antivirus provider, located in Belarus, about an anomalous operation in their equipment since they were constantly restarting, causing a malfunction in the plant's systems (Lindsay, 2013). Now, international standards demand that for atomic power generators, a physical recognition of what happened is performed, the finding in this plant of a malfunction in the centrifuges responsible for enriching uranium (Scholtz et al., 2018). However, months after replacing all the equipment, the devices were utterly unusable (Englert, 2013). In a second event, the same plant reported the destruction of 1000 centrifuges involved in generating nuclear materials. Several months later, Symantec engineers determined that malicious software explicitly targeted this industrial equipment, specifically the Siemens Programmable Logic Controllers (PLC), hardware, and software parts in the Iranian centrifuges. This attack reached more than 6 continents in a matter of days (Falliere et al., 2011; Krzykowski, 2021).

The Stuxnet plant marked a before and after in protecting assets through cybersecurity policies; months after day zero, countries in Asia, Europe, and America began a fierce dispute to dominate cyberspace. The conflicts resulted from several malicious actors who tried to replicate or create new attacks from the first (Unsal et al., 2021). In today's society, the term hacker is usually used negatively. Graves (2007), describes it as:

A person who steals information by entering private systems is not authorized to enter, stealing data for commercial, personal, financial, and other purposes, using technical knowledge and technological tools to achieve his goals.

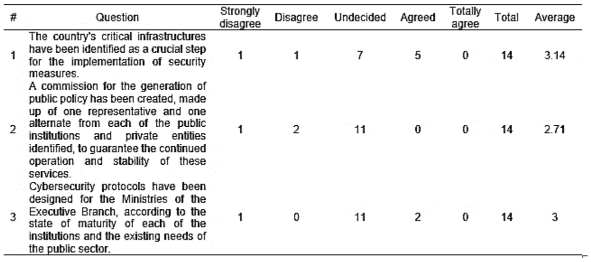
However, in recent years, the negative connotation has evolved; according to Graves (2007), new government-sponsored actors have emerged who are currently responsible for attacks on primary infrastructure in countries such as the USA, Estonia, Ukraine, and electoral frauds in several democracies around the world. In addition, they are directly responsible for the most significant espionage case documented in recent history (SolarWinds case, 2020) and the fuel shortage on the east coast of the United States (Colina Pipeline case, 2021), even creating a business term known as Ransomware as a Service (RaaS), representing one of the most complex challenges of modern computing (Tweneboah-Koduah & Prasad, 2020).

In the Costa Rican context, being one of the smallest countries in the world does not guarantee that a cybersecurity incident will not affect the electrical infrastructure. The Ministry of Science, Technology and Telecommunications (MICITT), in its report on the National Cybersecurity Strategy (ENC) of Costa Rica, Chapter 5: Strategic Framework for cybersecurity, specifically in the specific objective no. 5 on the protection of critical infrastructure, proposes the following No. 5 on the protection of critical infrastructure, offers the next: "Promote mechanisms for the identification and protection of critical infrastructure, as well as the creation of specific public policies, as a crucial step to prevent and mitigate cybersecurity incidents aimed at damaging or discontinuing sensitive operations," together with this objective, the following lines of action are proposed (MICITT, 2023):

1. We are identifying the country's critical infrastructures as a crucial step for implementing security measures.
2. Create a commission for the generation of public policy made up of a representative and an alternate from each of the public institutions and private entities identified to guarantee the continuous operation and stability of these services.

However, four years after the launching of the ENC, the results in the 2021 review are alarming, giving rise to the research question: What is the current situation of the Costa Rican electricity industry in the face of a possible cyber-attack? How has the country prepared itself to guarantee the continuity of the electricity service and mitigate the risks associated with the national population? To better understand the ENC's current position, it is necessary to talk about the details. In its original 2017 version led by the MICITT, it had the participation of personnel from the Organization of American States (OAS) and representatives from all sectors, so it is documented in the final report, while in 2021, the validation was carried out through 25 surveys to members (private and public) of the Costa Rican society. Table 1 shows the results of the survey (MICITT, 2023).

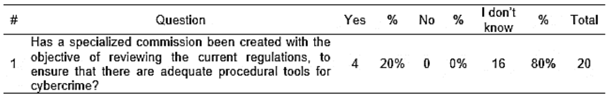
Table 1. Results of the strategic line: Identification and classification of critical infrastructure.



#	Question	Strongly disagree	Disagree	Undecided	Agreed	Totally agree	Total	Average
1	The country's critical infrastructures have been identified as a crucial step for the implementation of security measures.	1	1	7	5	0	14	3.14
2	A commission for the generation of public policy has been created, made up of one representative and one alternate from each of the public institutions and private entities identified, to guarantee the continued operation and stability of these services.	1	2	11	0	0	14	2.71
3	Cybersecurity protocols have been designed for the Ministries of the Executive Branch, according to the state of maturity of each of the institutions and the existing needs of the public sector.	1	0	11	2	0	14	3

Beyond such a discouraging result, the time lost is worrying. Technology does not stand still, and, therefore, neither do new threats. Costa Rica is currently seen as one of the largest technology hubs in Latin America. Some companies such as Intel, IBM, Microsoft, Hewlett Packard, Amazon, and McKinsey, among other large multinational companies, have bet on investing in this country (Smith, 2018). Unfortunately, at the national level, there are no solid efforts to guarantee a safe investment from a security perspective in the electrical infrastructure (Organismo de Investigación Judicial [OIJ], 2022). Table 2 reflects the progress in legal regulations in the face of attacks on technological infrastructure.

Table 2. Costa Rican legal situation to criminalize computer crimes.



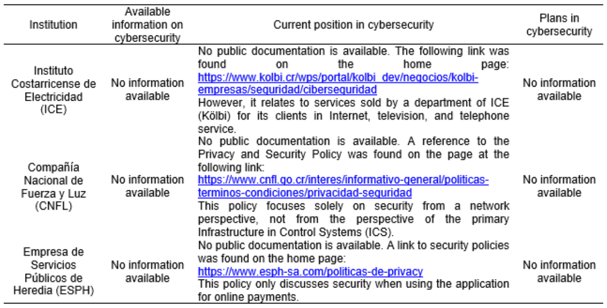
#	Question	Yes	%	No	%	I don't know	%	Total
1	Has a specialized commission been created with the objective of reviewing the current regulations, to ensure that there are adequate procedural tools for cybercrime?	4	20%	0	0%	16	80%	20

The MICITT is the regulatory body for technology in Costa Rica; in this ministry, Costa Rica consolidates all strategic decisions that set the country's course in cybersecurity issues. According to the Public Services Regulatory Authority (ARESEP, 2022):

Electricity service is provided to the population through a network, from generation, transmission, distribution, and public lighting. Electricity service is provided by eight companies authorized by law, according to their geographic coverage: ICE (rural areas throughout the country), CNFL (San José), ESPH (Heredia), Junta Administrativa del Servicio Eléctrico Municipal de Cartago (JASEC) (Cartago), Coopeguanacaste (Guanacaste), Coopealfaroruiz (Alfaro Ruiz), Coopesantos (Zona de los Santos) and Coopelesca (San Carlos), with ARESEP being the entity in charge of regulating the provision of this service, the conditions under which it is provided and the definition of tariffs.

For research purposes, the following institutions were considered: ICE, CNFL, and ESPH to analyze cybersecurity policies in the country's electrical infrastructure. In addition, the web portal of each institution and its links were used as a basis (see Table 3).

Table 3. Review of current policies for the protection of the national electrical infrastructure.



Institution	Available information on cybersecurity	Current position in cybersecurity	Plans in cybersecurity
Instituto Costarricense de Electricidad (ICE)	No information available	No public documentation is available. The following link was found on the home page: https://www.kolbi.cr/wps/portal/kolbi_dev/negocios/kolbi-empresas/seguridad/ciberseguridad However, it relates to services sold by a department of ICE (Kölbi) for its clients in Internet, television, and telephone service.	No information available
Compañía Nacional de Fuerza y Luz (CNFL)	No information available	No public documentation is available. A reference to the Privacy and Security Policy was found on the page at the following link: https://www.cnfl.go.cr/interes/informativo-general/politicas-terminos-condiciones/privacidad-seguridad This policy focuses solely on security from a network perspective, not from the perspective of the primary Infrastructure in Control Systems (ICS).	No information available
Empresa de Servicios Públicos de Heredia (ESPH)	No information available	No public documentation is available. A link to security policies was found on the home page: https://www.esph-sa.com/politicas-de-privacy This policy only discusses security when using the application for online payments.	No information available

In 2012, the Computer Security Incident Response Center for Costa Rica (CSIRT-CR) was created; this department of the MICITT was formalized through the norm 37052: Improvements in Cybersecurity for the Public sector of the Costa Rican State, where it is granted the powers conferred for this activity, through the political Constitution, being its primary functions the following (MICITT, 2022):

1. Promote at the national level actions that allow for the general improvement of cyber and information security.
2. Support administrative and judicial authorities in appropriate cases for investigating and prosecuting perpetrators of cyber and computer crimes.
3. Coordinate, at the national level, actions that allow for the general improvement of cyber and information security.
4. To promote and ensure the establishment of contingency plans to secure information and communication technologies in the public sector.
5. Promote the development and implementation of national policies and strategies in information and communication technology security among public and private entities.

An important aspect to highlight is that none of the activities conducted by the CSIRT-CR has a degree of specialization or direct involvement in the security of Costa Rica's electrical infrastructure.

All the above allows us to understand the current Costa Rican cybersecurity situation in the national power grid, allowing us to establish the starting point for the research field study.

4. Analysis of results

Once the literature review was completed, we analyzed the data collected in the survey sent to the experts. Figure 1 shows descriptive information on the level of knowledge of the participants.

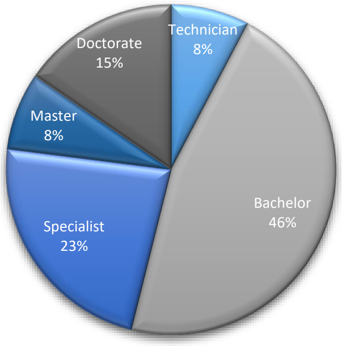


Figure 1. Academic grade level.

As can be seen in Figure 1, 92% of the interviewees have a level of education and knowledge in cybersecurity for each of the institutions where they work, indicating competencies associated with the field of information security. Figure 2 shows the roles and responsibilities of the people participating in the study.

69% of the interviewees have a role associated with Information Technology Security Management as a component of the institutional strategic plan. However, 31% of the participants need clarification about the role and responsibility in the institution to which they belong, this being a relevant risk that can trigger a vulnerability. Parker and Brown (2019), Peslak and Hunsin-ger (2019) agree that to avoid the level of exposure to a threat, it is necessary to determine the specific and general competencies expected from cybersecurity for each of the collaborators to reduce the probability and impact of an IT incident.

Then, the participants' knowledge level of existing policies and procedures for managing an information security system in the electricity industry is analyzed (see Figure 3).

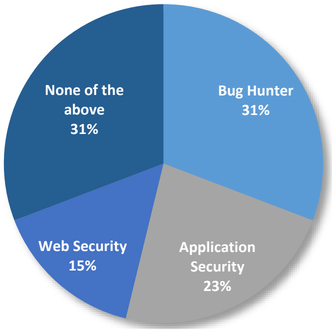


Figure 2. Current job functions.

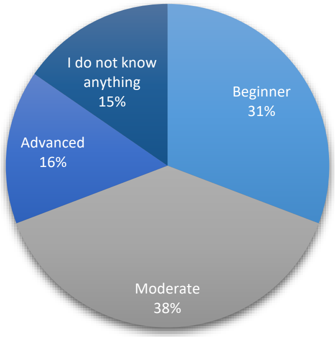


Figure 3. Level of knowledge of the security management system for the protection of the electric power infrastructure.

As shown in Figure 3, 16% of the respondents mentioned the existence of policies and procedures for information security management in the technological and electrical infrastructure. However, 46% of the participants were unaware of any standards or guidelines, while 38% thought that some initiative existed but needed to be made aware of its location or use.

Additionally, 100% of the participants agreed that the institutions of the electricity sector in Costa Rica do not have a robust policy, standard, guideline, or procedure that would allow them to face a cyber-attack on the national electricity grid, even mentioning that they lack a roadmap with specific plans for risk assessment in a timely and preventive manner. However, the professionals interviewed argue that they have the necessary technical knowledge to safeguard the national electric infrastructure but need more support and call for preventive action by the electric utilities. Coronado et al, (2014), Tirumala et al. (2019) mention that a fundamental element to secure infrastructure, data, and collaborators in business environments is necessary to develop a cybersecurity risk management plan, as it allows for establishing the roadmap to avoid Information Technology (IT) incidents. Figure 4 shows the results corresponding to the respondents' perception of their knowledge of cybersecurity public policies.

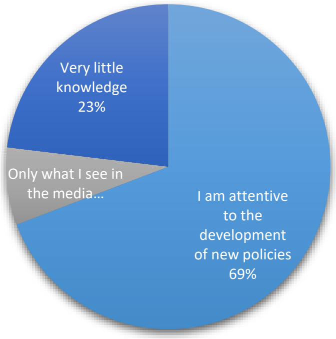


Figure 4. Knowledge of cybersecurity public policies.

The perception of the experts (69.2%) is that Costa Rica needs to catch up in cybersecurity. Fortunately, not everything is negative since the experts express in the same percentage (69.2%) the willingness to participate in a national initiative for the promotion, encouragement, and development of a national information security management plan and, in general, a comprehensive solution to respond to a possible cyber-attack to the electrical infrastructure.

Finally, the experts agreed, through the open question, on the initial actions to follow in the roadmap for the establishment of a cybersecurity policy in the electricity sector, the diagnosis being the following:

In the short term:

1. Creation of an intersectoral unit specialized in cybersecurity.
2. Involvement of personnel in all ranks of the companies of interest in constant training.
3. Schematization of the components of the current systems.
4. Establishment of more efficient controls in the administration of devices.
5. Policies for selection, recruitment, and evaluation of personnel to promote leaders in cybersecurity initiatives.
6. Promotion of agreements with countries that have implemented security in critical infrastructure.
7. Training and education of professionals interested in supporting the public sector.

In the medium term:

1. Implementation of policies and procedures based on international standards.
2. We are strengthening the layers of defense in international cybernetic networks.

3. Creation of an Incident Response Center (CIRT) for real-time analysis.
4. Enforce industrial security through standards such as operational technology security.

In the long term:

1. Investment in artificial intelligence for task automation.
2. Design and implementation of advanced monitoring systems.
3. Boost vulnerability scanning as a prevention measure.
4. Creation of vulnerability testing policies for infrastructure security, data, and collaborators.

5. Discussion

The research objective was to explore the degree to which the experts interviewed agreed and for which purpose the proposed assumption was tested using the correlation coefficient model. Alzina (2004) suggests that correlation models are mathematical indicators that provide information on the degree, intensity, and direction of the relationship between variables, where, if two variables are in the same order, there is a relationship that we will call optimistic. Its intensity will be reflected in the coefficient that adopts a value between 0 and 1, with the value closest to 1 representing greater intensity in the relationship.

This type of non-parametric test represents a method of testing the hypothesis associated with populations of quantitative data when there are doubts about whether the assumptions for the population distribution are (Levin & Levin, 2001), this being the scenario of the study since the degree of agreement between the interviewees was determined, based on their perception and opinion, the more significant the difference in the average ranges, the greater the agreement between the interviewees, and the more equal the middle degrees, the lower the agreement.

Given the above, the nonparametric test of interest for the research was Spearman's rank correlation test between two variables. Kendall and Smith (1939) indicate that Spearman's bivariate correlation coefficient measures the degree of relationship between several variables. Therefore, it is used to evaluate hypotheses of non-association between two populations. It is assumed that the n pairs of observations (x_i, y_i) are randomly selected and, therefore, the hypothesis of no association between the populations implies a random assignment of the n ranks in each sample. Each random allocation (for the two models) represents a sampling point associated with the experiment, and a subscript value can be calculated for each. Figure 5 presents the rejection region for a two-tailed (bilateral) test.

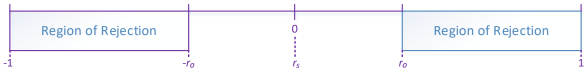


Figure 5. Rejection region for two-tailed tests.

Suppose the alternative hypothesis (H_a) is that the correlation between x and y is positive. In that case, the null hypothesis (H_0) is rejected for large positive values of r_s, the upper tail of Figure 5. Similarly, if one seeks to evaluate that the correlation is negative, H_0 is rejected for large negative values of r_s, lower tail of Figure 5. Thus, a null hypothesis of no association is posed against the alternative of an association between the ranks (two-tailed test) or positive (or negative). For a two-tailed test, H_0 is rejected if $r_s \le r_0$ or if $r_s \ge -r_0$, these reflect the test statistics for an upper or lower tail respectively, Table 4 presents the interpretation of the correlation coefficient.

Table 4. Interpretation of the correlation coefficient.

Coefficient	Interpretation
From 0 to 0.20	Correlation practically null
From 0.21 to 0.40	Low correlation
From 0.41 to 0.70	Moderate correlation
From 0.71 to 0.90	High correlation
From 0.91 to 1	Very high correlation

Table 5 summarizes the most significant negative or positive correlations, in general terms, according to Alzina (2004) classification, ranging from null to low correlations. For their interpretation, we proceed to review the positive correlations since these constitute the interest of the research, as the main findings in the relationships between dependent and independent variables.

Table 5. Results of Spearman's correlations in dependent variables.

Dependent Variable		Hypothesis Testing Model Spearman's Rho	Independent Variables	
			Level of knowledge of the security management system for the protection of the electric power infrastructure	Knowledge in cybersecurity public policies
Question	The national electricity infrastructure has an information security management system in place to protect mission-critical services against a possible cyber-attack	Correlation Coefficient	0.154	0.121
		(Bilateral) Sig.	0.02	0.14
		N	100	100

From the dependent variable, the interpretation of the positive associations with the independent variables is performed, where the p-value associated with the statistic to contrast the null hypothesis obtained was 0.154 and 0.121, respectively, being this result very small; therefore, the interrelation between the variables is almost null, and the hypothesis can be rejected.

Undoubtedly, the hypothesis test ratifies the results obtained, evidencing a high exposure to cyber-attacks in the national electricity system without an information security policy. Krkoleva-Mateska et al. (2021) mention that the lack of implementations, maintenance, and updates of technologies in the electricity system exponentially increases the risk of a possible cyber-attack, thus becoming the critical path of the industry.

Coffey et al. (2018) mention that the implementation of Supervisory Control And Data Acquisition (SCADA) or Industrial Control Systems (ICS) in industrial systems allows preventive management of the network, but when consulting experts, 46.2% possessed essential or no knowledge about the use of this operational technology. This is fully compatible with the results of the research.

Given the increase in global cyber-attacks, many countries are making significant investments to protect their infrastructure, as is the case of the United States of America, which allocated a budget of 20 billion dollars for cybersecurity in 2022 (Legg, 2021). In contrast to the national context, Costa Rica gave $11 million to the MICITT Field (Hacienda, 2021) to protect against cyber-attacks through the CSIRT-CR.

Additionally, it is necessary to promote the continuous training of professionals in new tactics, techniques, and procedures. Glantz et al. (2016) mention that it is necessary to maintain updated knowledge experiences and create expertise for offensive and defensive teams to ensure the protection of confidentiality, integrity, and availability of infrastructure, data, and people. In the findings, 69.3% of the participants knew the area; however, according to data from the National Security Agency, there is a gap of 1700 cybersecurity professionals in Costa Rica at the end of 2021 (Marks, 2021). Additionally, participants have roles and responsibilities associated with cybersecurity tasks in their jobs but need a Costa Rican state guideline in this area, involving public-private partnerships, to achieve a commitment with suppliers (Lee et al., 2022).

Finally, there are currently case studies, lessons learned and best practices in the industry that are constantly updating the area of information security, such as the National Institute of Standards and Technology (NIST), which provides a clear roadmap for the design, planning and implementation of a security management model in electrical infrastructure; specifically, the NIST reference structure is Framework and Roadmap for Smart Grid Interoperability Standards (Gopstein et al., 2021), which can serve as a basis for the national electricity industry in the development of an information security management plan.

6. Conclusions and recommendations

In the Costa Rican context, the Internet is one of the fundamental tools for the country's development. However, without the proper strategy, it can become a deadly attack vector for the national electrical infrastructure and an imminent risk for the Costa Rican economy.

The research conducted determined that companies in the electricity sector in Costa Rica do not have a mechanism for action and response to a cyber-attack on their infrastructure, coupled with the lack of robust policies and plans for mitigation in the event of a possible materialization of the risk (Szabó, 2021).

In 2012, Costa Rica joined the international movement to protect cyber infrastructure by creating the CSIRT-CR Department, an entity under the tutelage of the MICITT. On paper, this department oversees the national response to cybersecurity events; however, in practice, this goal has yet to be fully achieved since, when analyzing the objectives, none addresses the national electrical infrastructure. In other words, receiving a cyber-attack on the national critical infrastructure would be devastating since Costa Rica does not have a specialized entity to deal with this threat.

In summary, the study evaluated whether the Costa Rican government's current cybersecurity policies adequately counteract an attack on the electrical infrastructure. The above could be demonstrated with data and evidence through the expert judgment of the interviewees, in conjunction with the literature review of standards, policies, guidelines, processes, and procedures to establish a national cybersecurity strategy. However, it is essential to highlight the impetus of MICITT in developing a national cybersecurity strategy that was updated in 2023. Still, with clear legislation, the plan highlights promising practices in general for the country.

The above confirms the hypothesis since the Costa Rican government needs to consider critical actors of the national population to create a robust and comprehensive security strategy, along with policies and regulations that could mitigate a materialization of risk in the electrical infrastructure. The study did not find a direct relationship between the lack of policies in the field of information security and the investment of foreign companies in Costa Rica; however, investors review the economic situation of countries, as well as the risk assessments of international entities in different industries and sectors before investing in an economy. Therefore, not having a robust cybersecurity policy in energy is not a favorable variable for developing and attracting foreign investment to the country.

Among the main recommendations because of this study is the development of a roadmap for the establishment of the information security plan for the national electricity sector with the following axes:

1. Electrical components. Mapping of generators, transformers, switches, circuit protection, transmission, and distribution lines.
2. Digital component. Mapping of information and communication systems that allow the monitoring and control of all network devices.
3. Control component. Map all control systems, protection circuits, and synchronization systems critical to safety, operational efficiency, and performance.
4. Integration with feedstock. Electricity generation will depend heavily on other sources that are unrelated. This is the case with hydrocarbon-based fuels and natural gas pipelines, both critical to power generation.
5. Regulatory component. Review the relevant legislation for each country before starting any implementation steps.
6. Solution integration. You are likely to find multiple pieces of equipment within a plant, and not all of them will oversee the power plant. It is essential to know these types of equipment and to be clear about their capabilities and operation.
7. Vulnerability analysis. For the safeguarding of the infrastructure, it is fundamental to evaluate it. Attack simulations must be conducted to adjust, correct, and improve the previously established processes.
8. Constant training. The weakest link in any security system is the end user. This last step is critical to ensure that the other seven steps are successful.

7. Future research lines

The practical implications of the results obtained lead to a change of approach to using technologies in security strategies. Therefore, it will become an instrument of the country's plan to ensure the success or failure of the future rulers of a given society. Thus, the study's results will serve as input for interested institutions, as a guide for promoting a strategy based on information security, and to understand technology's role in safeguarding infrastructure, data, and collaborators.

It is important to note that you can have very technical personnel and are prepared for specializations. However, as a nation-state, the national strategy does not exist, or you need to prepare for war because you are working on islands. This prepares a state with clear public policies, which can become state policies for national security.

The implications from the theoretical perspective contemplate the development of research works in the academy that include additional elements in the existing relationship between cybersecurity processes and procedures in the electric industry and the resilient role of regulatory institutions in the digital era. Hence, the future lines of research are varied since the topic of study is very recent, broad, and with infinite ramifications.

Conflict of interest

The authors have no conflict of interest to declare.

Acknowledgments

The authors would like to thank all those involved in the work who made it possible to achieve the objectives of the research study.

Funding

The authors received no specific funding for this work.

References

Alzina, R. B. (2004). Metodología de la investigación educativa (Vol. 1). Editorial La Muralla.

Autoridad Reguladora de los Servicios Públicos [ARESEP]. (2022). Electricidad. Retrieved from https://aresep.go.cr/

Baggott, S. S., & Santos, J. R. (2020). A risk analysis framework for cyber security and critical infrastructure protection of the US electric power grid. *Risk analysis*, *40*(9), 1744-1761. https://doi.org/10.1111/risa.13511

Coffey, K., Smith, R., Maglaras, L., & Janicke, H. (2018). Vulnerability analysis of network scanning on SCADA systems. *Security and Communication Networks*, *2018*. https://doi.org/10.1155/2018/3794603

Congressional-Digest. (2019). *Power Grid: Federal Jurisdiction and Issues for Debate*. Cybersecurity and the U.S. Power Grid. https://congressionaldigest.com/issue/u-s-energy-infrastructure/cybersecurity-and-the-u-s-power-grid/

Coronado, A. J., & Wong, T. L. (2014). Healthcare cybersecurity risk management: Keys to an effective plan. *Biomedical instrumentation & technology*, *48*(s1), 26-30. https://doi.org/10.2345/0899-8205-48.s1.26

Creswell, J. W., & Poth, C. N. (2016). Qualitative inquiry and research design: Choosing among five approaches. Sage publications.

de Haro, J. (2017). Programación y Estadística con R: Fundamentos de Programación y Técnicas para el análisis Exploratorio, Contraste de Hipótesis y Aprendizaje Automático. Retrieved from

Dzul, E., M. (2020). Los enfoques de la investigación científica. Retrieved from https://repository.uaeh.edu.mx/bitstream/handle/123456789/14905

Englert, M. (2013). Cyber meets nuclear-Stuxnet and the cyberattacks on Iranian centrifuges. *Verhandlungen der Deutschen Physikalischen Gesellschaft*. Retrieved from https://www.osti.gov/etdeweb/biblio/22294125

Englert, M. (2013). Cyber meets nuclear-Stuxnet and the cyberattacks on Iranian centrifuges. Verhandlungen der Deutschen Physikalischen Gesellschaft.

Falliere, N., Murchu, L. O., & Chien, E. (2011). W32. stuxnet dossier. white paper, Symantec Corp., Security Response 5. Retrieved from https://archive.org/details/w32_stuxnet_dossier

Glantz, C., Somasundaram, S., Mylrea, M., Underhill, R., & Nicholls, A. (2016). Evaluating the maturity of cybersecurity programs for building control systems. US Department of Energy Office of Scientific and Technical Information.

Gobierno de México. (2017). Estrategia Nacional de Ciberseguridad. Retrieved from https://openresearch-repository.anu.edu.au/bitstream/1885/277212/1/MexCyber_4.pdf

Gopstein, A., Nguyen, C., O'Fallon, C., Hastings, N., & Wollman, D. (2021). NIST framework and roadmap for smart grid interoperability standards, release 4.0. Gaithersburg, MD, USA: Department of Commerce. National Institute of Standards and Technology.

Graves, K. (2007). Ceh: Official certified ethical hacker review guide: Exam 312-50. John Wiley & Sons.

Hacienda (2021). Proyecto de Ley de Presupuesto Nacional 2021, Pre*supuesto Ciudadano*. Retrieved from https://www.hacienda.go.cr/docs/03-FolletoCiudadano21.pdf

Hernández-Sampieri, R., & Mendoza, C. (2020). Metodología de la investigación: las rutas cuantitativa, cualitativa y mixta.

Kendall, M. G., & Smith, B. B. (1939). The problem of m rankings. The annals of mathematical statistics, 10(3), 275-287.

Krkoleva-Mateska, A., Krstevski, P., & Borozan, S. (2021). Overview and Improvement of Procedures and Practices of Electricity Transmission System Operators in South East Europe to Mitigate Cybersecurity Threats. *Systems*, *9*(2), 39. https://doi.org/10.3390/systems9020039

Krzykowski, M. (2021). Legal Aspects of Cybersecurity in the Energy Sector—Current State and Latest Proposals of Legislative Changes by the EU. *Energies*, *14*(23), 7836. https://doi.org/10.3390/en14237836

Lee, M., Kwon, H., & Yoon, H. (2022). Compliance-Driven Cybersecurity Planning Based on Formalized Attack Patterns for Instrumentation and Control Systems of Nuclear Power Plants. *Security and Communication Networks*, *2022*, 1-13. https://doi.org/10.1155/2022/4714899

Legg, J. (2021, 21 de octubre). *Council Post: Confronting The Shortage Of Cybersecurity Professionals*. Forbes. https://www.forbes.com/sites/forbesbusinesscouncil/2021/10/21/confronting-the-shortage-of-cybersecurity-professionals/?sh=79b31b78b9ba

Levin, J., & Levin, W. (2001). Fundamentos de estadística en la investigación social. *México, Oxford*. Retrieved from https://idoc.pub/documents/levin-fundamentos-de-estadistica-546gwkzo3wn8

Lindsay, J. R. (2013). Stuxnet and the limits of cyber warfare. *Security Studies*, *22*(3), 365-404. https://doi.org/10.1080/09636412.2013.816122

Marks, J. (2021, 2 de agosto). *Analysis | The Cybersecurity 202: The government's facing a severe shortage of cyber workers when it needs them the most*. Washington Post. https://www.washingtonpost.com/politics/2021/08/02/cybersecurity-202-governments-facing-severe-shortage-cyber-workers-when-it-needs-them-most/

Marino, J. J. A. L., Jiménez, I. F., & Jiménez, R. F. (2014). La hipótesis: un vínculo para la investigación. Xikua: Boletín Informativo de la Escuela Superior de Tlahuelilpan, 2(4).

Maroto, J. P. (2009). El ciberespionaje y la ciberseguridad. In La violencia del siglo XXI. Nuevas dimensiones de la guerra (pp. 45-76). Instituto Español de Estudios Estratégicos.

MICITT. (2022). Centro de Respuesta de Incidentes de Seguridad Informática (CSIRT-CR) Retrieved from https://www.micitt.go.cr/gobierno-digital/ciberseguridad

MICITT. (2023). Estrategia Nacional de Ciberseguridad de Costa Rica.

Middaugh, D. J. (2021). Cybersecurity Attacks during a Pandemic: It Is Not Just IT's Job!. Medsurg Nursing, 30(1), 65-66.

Organismo de Investigación Judicial, [OIJ]. (2022). *Planes y Operaciones*. Organismo de Investigación Judicial. https://sitiooij.poder-judicial.go.cr/index.php/oficinas/oficina-de-planes-y-operaciones

Parker, A., & Brown, I. (2019). Skills requirements for cyber security professionals: a content analysis of job descriptions in South Africa. In *Information Security: 17th International Conference, ISSA 2018, Pretoria, South Africa, August 15–16, 2018, Revised Selected Papers 17* (pp. 176-192). Springer International Publishing. https://doi.org/10.1007/978-3-030-11407-7_13

Pernik, P., Wojtkowiak, J., & Verschoor-Kirss, A. (2016). National cyber security organisation: United States. NATO Cooperative Cyber Defence Centre of Excellence.

Peslak, A., & Hunsinger, D. S. (2019). What is cybersecurity and what cybersecurity skills are employers seeking? *Issues in Information Systems, 20*(2). https://doi.org/10.48009/2_iis_2019_62-72

Rockmore, T. (2005). On constructivist epistemology.

Rusco, F. (2021). Electricity grid cybersecurity: DOE Needs to Ensure Its Plans Fully Address Risks to Distribution Systems. Retrieved from https://www.gao.gov/products/gao-21-81

Scholtz, J., Franklin, L., Ashok, A., LeBlanc, K., Bonebrake, C., Andersen, E., & Cassiadoro, M. (2018). Employing a user-centered design process for cybersecurity awareness in the power grid. *Journal of Human Performance in Extreme Environments, 14*(1), 4. https://doi.org/10.7771/2327-2937.1094

Smith, D. C. (2018). Enhancing cybersecurity in the energy sector: a critical priority. *Journal of Energy & Natural Resources Law*, *36*(4), 373-380. https://doi.org/10.1080/02646811.2018.1516362

Soni, V. D. (2020). Challenges and Solution for Artificial Intelligence in Cybersecurity of the USA. *Available at SSRN 3624487*. https://dx.doi.org/10.2139/ssrn.3624487

Szabó, Z. (2021). Cybersecurity issues in power systems. In Proceedings of FIKUSZ Symposium for Young Researchers (pp. 241-251). Óbuda University Keleti Károly Faculty of Economics.

Tirumala, S. S., Valluri, M. R., & Babu, G. A. (2019). A survey on cybersecurity awareness concerns, practices and conceptual measures. In *2019 International Conference on Computer Communication and Informatics (ICCCI)* (pp. 1-6). IEEE. https://doi.org/10.1109/ICCCI.2019.8821951

Tvaronavičienė, M.; Plėta, T.; Casa, S. D.; Latvys, J. 2020. Cyber security management of critical energy infrastructure in national cybersecurity strategies: cases of USA, UK, France, Estonia and Lithuania, I*nsights into Regional Development 2*(4): 802-813. https://doi.org/10.9770/IRD.2020.2.4(6)

Tweneboah-Koduah, S., & Prasad, R. (2020). The Threats of Infrastructure Obsolescence to Smart Grid: A Case Study. *Wireless Personal Communications, 114*(2), 1025-1043. https://doi.org/10.1007/s11277-020-07406-y

Unsal, D., Ustun, T., Hussain, S., & Onen, A. (2021). Enhancing Cybersecurity in Smart Grids: False Data Injection and Its Mitigation. *Energies,* *14*(9), 2657. https://doi.org/10.3390/en14092657

Zuluaga, D. (2020). Cybersecurity for Centralized and Distributed Power Generation at ISAGEN. *Ingeniería y Ciencias, 16*(32), 171-194. https://doi.org/10.17230/ingciencia.16.32.8