Chapter 1

Definition and Impact of Digital Transformation and Cibersecurity*

DOI: https://doi.org/10.25062/9786287818064.01

Lucas Adolfo Giraldo Ríos

Escuela Superior de Guerra "General Rafael Reyes Prieto"

Abstract: This chapter discusses strategic forecasting and foresight. The former involves anticipating plausible future scenarios, while the latter identifies emerging trends. It highlights the need for strategies that promote cybersecurity awareness for a solid organizational culture in information security. It concludes that promoting this culture strengthens organizational resilience to cyber threats.

Keywords: cybersecurity; awareness raising; organizational culture; strategy; forecasting; foresight

* Book chapter resulting from the research project *Disruptive Technologies, Logistics, and National Security and Defense in Cyberspace* conducted by the Cyberspace, Technology, and Innovation research group of Escuela Superior de Guerra "General Rafael Reyes Prieto," categorized C by the Ministry of Science, Technology and Innovation (MinCiencias) and registered under code COL0181179. The points of view and results of this chapter belong to the authors and do not necessarily reflect those of the participating institutions.

Lucas Adolfo Giraldo Ríos
PhD candidate in Engineering, Industry and Organizations, Universidad Nacional de Colombia. Master's in Technology-Based Business Management, Universidad Antonio de Nebrija, Spain. Master's in Innovation, Universidad EAN, Colombia. Specialization in Business Financial Management, Universidad de Medellín, Colombia. Bachelor's in Business Management, Universidad de Antioquia, Colombia.
https://orcid.org/0000-0002-9947-7882 - Contacto: **lucas.giraldo@esdeg.edu.co**

APA Citation: Giraldo Ríos, L. A. (2025). Definition and Impact of Digital Transformation and Cybersecurity. In M. E. Realpe Díaz & A. M. González González (Eds.), *Disruptive Technologies, Logistics, and National Security and Defense in Cyberspace* (pp. 15-42). Sello Editorial ESDEG. https://doi.org/10.25062/9786287818064.01

DISRUPTIVE TECHNOLOGIES, LOGISTICS, AND NATIONAL SECURITY AND DEFENSE IN CYBERSPACE
Print ISBN: 978-628-7818-05-7
Digital ISBN: 978-628-7818-06-4
DOI: https://doi.org/10.25062/9786287818064

Cybersecurity and Cyber Defense Collection
Sello Editorial ESDEG
Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia
2025

Introduction

Technological convergence, where information flows are becoming more frequent every day, marks the advent of the digital revolution due to the interconnected world in which we are, with instant, permanent, and updated information. All this has produced a change in computer systems and the demand for security as a challenge that organizations and individuals face daily.

Protecting information is one of the most prominent concerns organizations have today. Due to globalization and the Internet of Things (IoT), more and more public and private entities face new threats and risks. Thus, the security policies implemented or the technological investment companies make are not enough to counteract this scourge; the personnel working in the institutions and representing the weakest link in information security must be considered.

Organizations must take a resilient position in the face of cybersecurity problems, i.e., they must anticipate the threats and risks that arise since they are becoming more varied and widespread. This makes it difficult to protect information assets and forces organizations to change their perspective regarding how to act upon it in a dynamic and uncertain world.

Information security must be incorporated into corporate strategies and tactical plans that understand an organization's business model. This understanding allows an organization to anticipate future challenges and support decision-making regarding cybersecurity issues.

This chapter offers an overview of the key concepts and ideas about strategic forecasting and foresight, the importance of raising awareness of cybersecurity in organizations, and the use of perspective to achieve an organizational culture in cybersecurity.

Strategic Forecasting and Foresight

Forecasting has long been used to describe how governments prepare for and address long-term problems. *Technology foresight* began to be used in the 1990s in Europe, although later, other countries began to address it as a policy relating to science, technology, and innovation systems (Miles, 2010).

Irvine and Martin's studies highlighted *forecasting* as the popular way to describe broad research and innovation curricula for future developments (Miles, 2010). In many cases, forecasting is conducted to anticipate the main social and future challenges, managing to support decision-making not only because it identifies technological changes but also because it involves the relevant stakeholders that will generate knowledge and innovation.

According to Könnölä et al. (2010), forecasting activities have tended to shift from focusing on positivist and rationalist technologies to recognizing broader concerns spanning the entire innovation system, taking into account social approaches, such as sustainability, security, and information society.

On the other hand, foresight plays a definitive role in organizations' decision-making since it allows organizations to prepare for the future. It identifies both promising technological paths and different stakeholders interested in anticipating and creating common actions that involve preparing for and confronting what is coming (Könnölä et al., 2010).

Foresight is thus recognized as a systematic, participatory process of brainstorming ideas that can be used in the long term for current and future decision-making and allows for strategic planning that meets organizations' objectives.

Due to the social challenges that arise every day due to technological convergence, IoT, and the digital economy, among others, research results are needed to support specific situations in decision-making. Therefore, it is necessary to consider data and studies, as they serve as a guide to prepare us to face future science, technology, and innovation challenges and make better decisions (Könnölä et al., 2010, p. 3).

Experience in the use of foresight and perspective in countries such as Japan, the Netherlands, the USA, Spain, and the United Kingdom demonstrates that their systematic incorporation in science and technology processes has improved strategies and served as a guide for decision-making in implementing policies in both public and private organizations. This reveals the importance of foresight for an organization since the studies in this regard make it possible to minimize many risks brought by technology and digitalization and, generally, achieve information security, which is one of the challenges of organizations (Miles, 2010, pp. 7–8).

Regarding cybersecurity awareness, foresight is required to predict the future since new risks and threats arise daily and as a tool that allows organizations to be resilient against challenges and implement better strategies.

Likewise, information insecurity will continue to be an imminent problem for governments due to connectivity and the need to be permanently informed, so the challenges will continue to be huge for researchers and those in charge of the security of information assets.

Strategic Foresight: Importance for the Future of Organizations

Organizations increasingly use strategic foresight because it gives them a vision of the future and allows for continuous improvement in processes to counteract the risks and threats that a lack of foresight may cause.

Companies should consider the strategy as a whole and begin to implement or correct it gradually, depending on their pace of adaptation. According to Mintzberg et al. (1998), ten schools categorize the strategy into three main groups. The first, known as *prescriptive,* focuses on formulating strategies before considering their conception. The second group, comprised of six schools, describes procedures, prioritizes content and positioning, and transforms the strategy into something different, systematic, and formal. Finally, the school of knowledge emerges, which seeks to use the tools of cognitive psychology to understand the strategist's mind.

One of the strategy's main objectives is to resolve the significant challenges and problems that may arise in organizations in the future. This does not mean that by implementing or modifying a strategy, we are already exempt from a threat or danger; instead, many possible risks are minimized. Following Mintzberg et al. (1998), "A strategy moderates the ability to respond to changes and modifications in the environment; that is, it is a fundamental element that forces you to go straight and does not allow you to look away" (p. 4).

To implement a good strategy, we must, however, review its importance for organizations. For this reason, Mintzberg et al. (1998) describe the role of strategy and its advantages in four points: 1) as guidance, since it serves as a compass for an organization; 2) as a concentration of efforts, since it allows the concentration of activities; 3) as meaning to the organization, since it distinguishes it from the others, and 4) as a source of coherence, since it helps to understand the environment and with this the implementation of actions that respond to it.

Therefore, when implementing strategies, organizations must consider them as a whole, not at their convenience or as best suited to the organization. For the school of culture and spirit, strategies are unique perspectives from a person's point of view or organizational culture and, therefore, each one is different; that is, they cannot be compared with other strategies since these are derived and born from personal adaptation processes and are the result of individual creative efforts (Mintzberg et al., 1998).

Strategies for a Culture of Information Security

This section explores the essence of cybersecurity and digital transformation: the organizational culture surrounding information security. According to Beaver (2018), adequate security is not simply a matter of tools and technology but also attitudes, behaviors, and awareness within the organization. Here is where strategies to foster a safety culture become crucial (Spafford, 2006).

The organizational culture of information security (COSI, by its Spanish acronym) is a relevant issue that allows companies to increase their resistance to cyberattacks. Although it is a topic that must be studied, public and private companies still need to give it the relevance it requires (Cano, 2016).

The organizational culture works toward protecting information, which ceases to be just another resource for companies and becomes a vital strategic asset for decision-making. Cybersecurity is a risk management problem and must be addressed from a strategic, economic, and reactive perspective. It must involve all organization members and be a cross-cutting process for all areas of the entity. Protecting the assets of entities from cybercrimes is not an option, but rather a key element for the development of an organization (Organization of American States [OAS], 2017).

According to Sechin (as cited in Cano, 2015), "An organizational culture is built from what people believe, what persons do, and what individuals see." To build a culture of information security, it is necessary to study people's behavior since this reflects how they act on security issues, the responsibility with which they face them, and, in many cases, the level of knowledge they have regarding cybersecurity. This analysis seeks to coordinate the relationship between people and information, the responsibility that each person has from the role they play in this asset, and the value it has for the strategic and missional fulfillment of each entity, seeking not only compliance with strategies and regulations implemented by the company but also ownership for the protection of information.

It is known that when prospective strategies are implemented for an organization concerning information security, these cannot be addressed 100 % since new threats and risks emerge every day due to technological evolution and their convergence. Here is where information security managers begin to assess "which risks to avoid, which to accept, and which to mitigate or transfer through insurance, as well as specific plans associated with each approach" (OAS, 2017, p. 24). Once these aspects are analyzed in terms of the cost-benefit they can generate for the company, it is good to make this decision. Based on the above, some strategies that support the culture of information cybersecurity are described below.

Importance of Information Security

Information security is essential in any organization to ensure the protection of confidential data and avoid potential financial loss or reputational damage. In the Information Age, when information is exposed to various risks and threats, such as data theft or cyberattacks, it is crucial to have adequate security strategies and measures. Information is a valuable asset that can provide competitive advantages, so its protection becomes a priority to ensure business continuity. Implementing security policies and procedures, as well as staff training and awareness, are crucial to achieving an influential information security culture. In addition, it is important to continually evaluate and improve the security system to adapt to technological changes and new threats that may arise.

Identification of Risks and Vulnerabilities

Identifying risks and vulnerabilities is a fundamental step to achieving an influential information security culture. This process allows us to identify the possible dangers our organization is exposed to and the weaknesses in our systems and processes that malicious actors could exploit. To carry out this task, both internal and external risk assessments must be conducted to detect possible threats and vulnerabilities. Security analysis tools and techniques like penetration testing and vulnerability scans can also help us identify potential system gaps. Once the risks and vulnerabilities have been identified, the necessary measures can be implemented to mitigate them and guarantee the protection of an organization's information (Cando, 2024; Castillo, 2023).

Development of Security Policies and Procedures

Developing security policies and procedures is critical to establishing an organization's strong information security culture. These policies must be designed comprehensively and consider all relevant aspects, such as the classification of information, access and protection of assets, password management, and security in the use of mobile devices. Furthermore, the procedures must be clear and detailed, specifying the technical and operational actions necessary to guarantee information security. These documents must be communicated and distributed to all members of the organization, who must commit to complying with the established policies and procedures. In addition, a periodic review and update process of these policies and procedures must be established to ensure they align with new threats and changes in the security environment (Montalbán et al., 2020; Muñoz, 2021; Valencia, 2021).

Staff Training and Awareness

Staff training and awareness are fundamental aspects of achieving a culture of information security. It is vital to provide all employees with adequate training on computer security issues, including basic concepts of data protection, secure password management, prevention of cyberattacks, and good practices in using technological systems and resources. Besides, it is important to raise awareness about the rights and responsibilities of staff regarding information security, promoting the relevance of maintaining data confidentiality, integrity, and availability. To ensure adherence to these measures, regular and updated training programs must be carried out, including periodic assessments to measure the level of knowledge and promote continuous improvement in the safety culture (Arpi & Cajamarca, 2023; Barcia, 2023; Fong & Bayona, 2022).

Evaluation and Continuous Improvement of the Security System

The evaluation and continuous improvement of the information security system are essential to guarantee its effectiveness and efficiency over time. To do this, it is necessary to perform periodic audits to identify possible failures or weaknesses in the system. These audits must be performed internally and externally by professionals with experience in information security. Internationally recognized standards, e.g., ISO 27001, must be followed to assess compliance with the controls and security measures implemented. Furthermore, it is important to consider emerging threats and vulnerabilities and adapt the security system accordingly. For continuous improvement, indicators and metrics must be established to measure the system's effectiveness and take corrective actions when deviations are detected. It is also advisable to conduct security drills and tests regularly to evaluate the response capacity and detect possible areas for improvement. In summary, the evaluation and continuous improvement of the information security system is an essential process to maintain the protection of assets and guarantee the confidentiality, integrity, and availability of information (Bedoya & Patiño, 2023; Sánchez et al., 2023; Sepúlveda & Medina, 2024).

Finally, individuals are fundamental for the success of organizational safety culture programs since each one plays a role that contributes positively or negatively to the organization. This is why awareness-raising programs are important for companies since they reduce the risks and vulnerabilities that entities may suffer.

Philosophy of Cybercrime

Cybercrime is a criminal activity carried out in the digital sphere, using information and communications technologies as tools to commit crimes (Saín, 2018). These crimes may include the theft of personal or financial data, forgery of identities, unauthorized access to computer systems, and dissemination of illegal content. Cybercrime is characterized by its global nature, since it can be perpetrated from anywhere in the world, and by its capacity to cause large-scale damage both at the individual and societal levels.

Cybercrime has several characteristics that distinguish it from other types of crimes. First, it is committed covertly, taking advantage of the relative anonymity that the internet provides. Second, cybercrime is highly sophisticated, requiring specialized information technology knowledge and advanced technical skills. Third, cybercrime is a constantly evolving phenomenon, with cybercriminals adapting their methods and techniques to circumvent security measures. Finally, cybercrime can have an almost unlimited global reach since the internet allows criminals to operate in different countries and attack people worldwide (Incibe-Cert, 2020).

Cybercrime has a significant impact on society on multiple levels. At an individual level, it can cause personal and financial data loss and deterioration of online privacy and security. At the enterprise level, cybercrime can result in security breaches, loss of customers, and damage to the reputation of organizations. At the societal level, cybercrime can affect trust in institutions, undermine the digital economy, and generate significant costs for governments and citizens (Cano, 2011). Furthermore, cybercrime can contribute to the spread of misinformation, widening the digital divide and exacerbating inequality. Therefore, it is important to address cybercrime effectively to protect individuals and safeguard the well-being of society as a whole.

The philosophy of cybercrime analyzes and reflects on the fundamental aspects related to this criminal phenomenon. Different elements are addressed, such as the origin and evolution of cybercrime, the motivations of cybercriminals, the ethics and morals involved in these practices, and the philosophical implications arising from this type of crime (Creese et al., 2020). With a critical and reflective approach, we seek to understand the ethical, moral, and philosophical dimensions of cybercrime and its influence on today's society (Sáinz, 2016).

The fight against cybercrime faces constant challenges due to rapid technological advancement and the sophistication of the techniques used by cybercriminals. The increased connectivity and the digitalization of various areas of society provide new opportunities to commit online crimes. Cybercriminals are constantly adapting, improving their techniques, and exploiting emerging vulnerabilities. Moreover, anonymity and the lack of a single jurisdiction make it difficult to chase and capture those responsible (Saín, 2018). Other challenges include a lack of cybersecurity awareness and training in various sectors, the shortage of cybersecurity experts, and the need for financial resources to combat cybercrime effectively. Overcoming these challenges requires a collective response and constant adaptation to new threats and scenarios to fight them.

With the development of the internet, favorable conditions have been created for those who pursue personal interests at the expense of network users. The effects have common characteristics, such as a serial killer environment and low levels of harassment. Crime can be committed anywhere in the world with internet access. It can affect organizations or individuals anywhere, giving criminals a high-impact, easy-to-implement, anonymous level of risk, efficiency, and effectiveness. In some cases, the perpetrator does not need in-depth knowledge to commit a cybercrime. In this regard, the World Economic Forum lists infrastructure failures, cyberattacks, and fraud or data theft (which involves the theft of personal data) as the top ten global threats (World Economic Forum [WEF], 2013).

Cybersecurity Challenges

Cyber threats are constantly evolving and represent an increasing challenge to digital security. The attack techniques used by cybercriminals are increasingly sophisticated and can affect both individuals and organizations (Incibe-Cert, 2020). Some of the most common cyber threats include phishing, malware, ransomware, and denial of service attacks. These attacks can have devastating consequences, including the loss of sensitive data, theft of personal or financial information, and damage to a company's reputation. To address these threats, it is essential to have adequate security measures in place, such as antivirus software, two-factor authentication, and cybersecurity education, to ensure the protection of digital systems and data (Mijares, 2020).

Vulnerabilities in digital infrastructures pose a significant cybersecurity challenge. These vulnerabilities can arise for various reasons, such as using obsolete or outdated systems, lack of security patches, inadequate implementation of protective actions, and unawareness of cyber threats. Additionally, digital infrastructures are often interconnected, meaning that the vulnerability of one system can affect other systems. This highlights the importance of implementing robust and up-to-date security measures at all layers of the digital infrastructure, from servers and networks to end devices (Pérez et al., 2012). It is also crucial to conduct periodic vulnerability assessments and make corrections to mitigate risks and strengthen security in digital infrastructures.

Data protection strategies play a fundamental role in cybersecurity. To ensure information security, it is essential to implement measures such as data encryption, firewalls and intrusion detection systems, and robust password policies. In addition, it is necessary to make regular backups and have an incident response plan that allows us to act quickly and effectively in the event of any eventuality. Other strategies include network segmentation, two-factor authentication, and constant user activity monitoring. Implementing identity and access management tools can also help prevent unauthorized system access. In summary, having a comprehensive data protection strategy is essential to mitigate risks and protect information from potential cyberattacks (IT Trends, 2019).

The role of governments in cybersecurity is fundamental to protect and guarantee the security of citizens and organizations against cyber threats. Governments are responsible for establishing and enforcing laws and regulations that promote the protection of information systems and data privacy. In addition, they must encourage cooperation and collaboration between the public and private sectors, facilitating information exchange and developing good cybersecurity practices (Ibarra & Igartua, 2018). Governments must also invest in the education and training of cybersecurity professionals to prepare them for new technological challenges and promote the research and development of advanced technologies and tools that can help prevent and detect cyberattacks. In short, the role of governments in cybersecurity is essential to protect society and foster a safe and trustworthy digital environment (Evans & Farrell, 2020).

Cybersecurity education and awareness are critical in protecting individuals and organizations from cyber threats. Through educational programs and awareness campaigns, we seek to inform people about how they can be victims of cyberattacks and how they can prevent them. These programs include teaching safe practices in using the internet, email, and social media and promoting the importance of keeping operating systems and security software up-to-date. The risks associated with using weak passwords and sharing personal information online should also be highlighted. Cybersecurity awareness also extends to companies, encouraging the implementation of internal security policies and staff training and creating an organizational culture that prioritizes the protection of digital information (Deloitte et al., 2013). Some examples of these challenges are:

Advances and Policies in the United States

Various initiatives and legislation have been implemented in the USA to address cybersecurity challenges. A notable example is the Modernization of Research and Innovation Infrastructure Act (MIIRIA), which includes provisions to strengthen cybersecurity at federally funded research and development institutions. The National Cybersecurity Strategy, launched in 2018, also establishes a comprehensive framework to protect critical infrastructure and strengthen the country's cyber resilience.

Advances and Policies in the European Union

The EU has taken a coordinated approach to improving regional cybersecurity. The General Data Protection Regulation (GDPR), implemented in 2018, sets rigorous standards for protecting personal data and forces organizations to take proactive measures to ensure data security. Furthermore, the EU Cybersecurity Strategy, launched in 2013 and updated in 2020, promotes cooperation between Member States and the private sector to address cyber threats effectively.

Advances and Policies in China

China has established several regulations and laws to strengthen its cybersecurity position. For example, the Cybersecurity Law of the People's Republic of China, implemented in 2017, establishes requirements to protect critical infrastructure and regulate the handling of personal data. Additionally, China's National Information Security Action Plan, launched in 2019, sets out goals and measures to improve cybersecurity in the country.

Advances and Policies in Japan

Japan has developed a series of initiatives to strengthen its cybersecurity capacity. Japan's Cybersecurity Strategy, launched in 2015 and updated in 2020, establishes objectives and measures to protect critical infrastructure and promote collaboration among the Government, the private sector, and academia. Additionally, Japan's Act on the Protection of Personal Information, enacted in 2005 and amended in 2015, establishes standards for the secure handling of personal data.

Advances and Policies in Australia

Australia has introduced several initiatives to strengthen its cybersecurity capacity. For example, the Australian Government launched the Australian Cybersecurity Strategy in 2020, which includes significant investments in cybersecurity infrastructure and cyber defense capabilities. Australia's Notifiable Data Breaches scheme, implemented in 2018, also requires organizations to notify authorities and affected individuals during a data security breach.

Weak Links

Nowadays, cybersecurity has become an issue of vital importance for organizations. In addition to protecting confidential company information and customer data, cybersecurity also plays a critical role in protecting against external threats. The increasing dependence on technology in the business environment has increased organizations' vulnerability to cyberattacks, highlighting the need to implement appropriate security measures. A lack of cybersecurity can have devastating consequences, such as theft of sensitive information, disruption of business processes, and loss of customer trust. Therefore, organizations must recognize the importance of investing in cybersecurity to protect their assets and maintain business continuity.

Organizations face several common cybersecurity threats. One is phishing, in which attackers try to obtain confidential information by posing as trusted entities. There are also malware attacks, which can infect the organization's systems and compromise data integrity. Another type of threat is ransomware, in which cybercriminals block access to files and demand a ransom for their release. Additionally, brute force attacks are common, using programs that attempt to guess passwords to access systems or accounts. Finally, organizations should also be concerned about denial-of-service attacks, where an attempt is made to overload a website or service to make it inaccessible to legitimate users. Organizations must be prepared and take preventive measures to mitigate these threats and protect their systems and data.

Several factors can weaken cybersecurity in organizations. One of them is the absence of cybersecurity awareness and training on the part of employees. Workers often ignore good security practices or fall into phishing traps and other attacks. Another factor is the need to update the systems and applications used. If organizations do not install the latest security patches and updates, they leave vulnerabilities exposed to attacks. Additionally, the lack of clear and consistently applied security policies and procedures can weaken an organization's cyber protection. Establishing security rules and guidelines and ensuring compliance is necessary to avoid security breaches. In brief, ignorance, a lack of updates, and the absence of clear policies weaken cybersecurity in organizations.

Weak links in organizations' cybersecurity can have serious consequences. One of the main repercussions is the risk of suffering a cyberattack. Hackers can use these vulnerabilities to infiltrate the system and access sensitive information. This can result in the theft of data, such as passwords, credit card numbers, or personal information of customers and employees. Weak links can also facilitate the spread of malware, which can impact system performance and cause financial damage. On the other hand, organizations that do not adequately manage information security can face serious legal consequences and reputational damage in the event of data breaches. In short, weak links in cybersecurity are a severe threat that can have financial, legal, and reputational repercussions for organizations.

To improve cybersecurity in organizations, adopting a series of measures and solutions is essential. First of all, it is advisable to implement a continuous network monitoring system in order to detect any suspicious activity or intrusion attempt. Second, there should be a cybersecurity education and awareness program in place, providing training to all organization members so that they understand threats and how to respond to them. Third, it is necessary to establish clear and rigorous password management policies, encouraging strong and periodically updated passwords. Another critical measure is the implementation of two-factor authentication systems, which provide an additional layer of protection. Finally, it would be best to have a response plan for security incidents, which allows a quick and efficient reaction to possible attacks or security breaches. These improvements and solutions are essential to strengthen organizations' cybersecurity and protect data and systems integrity.

Cyber Resilience and Cybersecurity Awareness

In today's world, where technology and interconnectivity play an increasingly important role in our society, *cyber resilience* and *cybersecurity awareness* are two fundamental concepts. In this chapter, both terms are analyzed in detail, exploring their importance and the strategies that can be implemented to strengthen security in the digital environment. In addition, we examine the available tools and technologies that can contribute to cyber resilience, as well as the conclusions reached after the study. This work aims to provide solid knowledge on such relevant topics and encourage greater awareness regarding cybersecurity.

Importance of Cyber Resilience

Cyber resilience is a fundamental aspect of today's cybersecurity. It refers to an organization's ability to resist, adapt, and recover from cyber incidents and attacks. It is essential to ensure business continuity and protect confidential information. Cyber resilience is vital because it allows us to reduce risks and mitigate the possible negative consequences of a cyberattack. Besides, it guarantees the ability to respond quickly and efficiently to potential incidents, thus minimizing the impact on an organization. Implementing cyber resilience strategies strengthens system security and maintains the trust of customers and business partners.

Cybersecurity Awareness Strategies

Cybersecurity awareness strategies are essential to educate and make people aware of the risks and threats in the digital world. One of the most effective strategies is to carry out training and training programs that provide practical knowledge about good computer security practices. These programs may include talks, workshops, and courses that address topics such as secure password use, identifying suspicious emails and links, and protecting personal information. Another essential strategy is the creation of awareness campaigns that reach a broad audience through the media, social media, and other dissemination channels. These campaigns can use clear and direct messages to inform about risks and promote responsible use of technology. Cyberattack simulations can also be implemented to evaluate response capacity and raise awareness of the importance of staying alert to potential threats. In short, cybersecurity awareness strategies are essential to foster a culture of security in society and reduce the incidence of cyberattacks.

In conclusion, cyber resilience is vital today, where cyberattacks are increasingly frequent and sophisticated. Cybersecurity awareness strategies are essential to protect organizations from possible threats and minimize risks. Furthermore, using appropriate tools and technologies to strengthen cyber resilience is crucial. These tools may include intrusion detection and prevention systems, data encryption, and backup and recovery systems. Organizations must invest in training and constant updating to be prepared for any contingency. Cyber resilience is not only about resisting and recovering from attacks but also about learning from them and improving security in the future.

Public-Private Cooperation in Cybersecurity and Culture

Cooperation between the public and private sectors in cybersecurity is vital due to the growing challenges of protecting information and digital systems. Both sectors possess unique knowledge and resources that, when combined, can significantly strengthen cybersecurity defenses. The public sector has experts in policy and regulatory frameworks, while the private sector brings expertise in technology and adaptability. Additionally, collaboration enables timely sharing of threat and vulnerability information, facilitating early detection and response to security incidents. The public and private sectors can effectively address cybersecurity challenges and protect critical data and systems by working together.

Collaboration between the public and private sectors in cybersecurity has numerous benefits. Firstly, it combines both sectors' experience and knowledge, enabling us to address computer security challenges more effectively. Secondly, this collaboration promotes interoperability and information exchange among organizations, allowing for a faster and more coordinated response to cyber threats. Thirdly, public-private partnership in cybersecurity strengthens the protection of critical infrastructures by pooling resources, technologies, and good practices. Finally, this collaboration can boost economic development by encouraging innovation and job creation in the field of cybersecurity.

One of the main challenges in cybersecurity cooperation is the need for more mutual trust between the public and private sectors. There is a reluctance on the part of private companies to share sensitive information with government authorities for fear of data leaks or being used against them. On the other hand, public institutions may need more support in acting due to legal and bureaucratic restrictions. The lack of common standards and protocols also makes communication and collaboration between both sectors difficult. The rapid evolution of information and communication technologies represents a constant challenge as cyber threats and vulnerabilities evolve quickly and complexly. Therefore, overcoming these challenges and promoting new forms of cooperation in cybersecurity that allow for an effective and coordinated response to digital threats is necessary.

Promoting a culture of cybersecurity is essential to protect information and maintain security in the digital sphere. To this end, it is necessary to make people aware of the risks and good practices in cybersecurity. This involves providing cybersecurity training and education at the individual and organizational levels. Organizations should implement awareness programs that include the importance of strong passwords, phishing detection and prevention, and adequate protection of sensitive data. Furthermore, it is essential to foster a general culture of cybersecurity in society, promoting responsibility and the safe use of digital technologies.

Taking action is essential to promote cooperation and a cybersecurity culture. First of all, it is necessary to encourage cybersecurity training for both the public and private sectors, with the aim of having specialized personnel aware of the risks. Likewise, awareness-raising programs should be established aimed at society in general so that citizens are informed and adopt safe practices in their digital lives. It is important to facilitate collaboration and the exchange of information between both parties by creating cooperation platforms and networks. These platforms will help share good practices, knowledge, and security alerts in an agile and effective way. Lastly, incentives and recognition should be established for those organizations and companies that demonstrate a significant commitment to cybersecurity and foster a culture of information protection. All these measures will strengthen cooperation and cybersecurity culture in the public and private spheres.

Experiences and Appropriate Practices

This section presents various successful experiences in the field of cybersecurity. Actual cases are addressed in which companies and institutions have implemented adequate measures to protect their digital infrastructure and safeguard their data confidentiality, integrity, and availability. It analyzes how these organizations have managed to confront cyber threats and strengthen their security by adopting advanced technologies, implementing robust security policies, training staff, and collaborating with cybersecurity experts. In addition, this section highlights the benefits obtained from these successful experiences at the information protection, reputation, and customer trust levels. Likewise, it explores the challenges and obstacles faced during the implementation process, as well as the lessons learned that may be useful for other organizations interested in improving their digital security (Goundar et al., 2021; Pérez et al., 2018; Vial, 2019).

In the sphere of digital transformation, it is vital to follow a series of recommended practices to ensure success and maximize the benefits of this process. First, it is essential to establish a clear and defined strategy that sets the objectives and goals to be achieved with digital transformation. It is also necessary to have the support and leadership of the management team to ensure the involvement of all organization members (Schmitt, 2018). Another important aspect is to thoroughly analyze existing processes and systems, identifying areas for improvement and possible obstacles that may arise during the transformation process. It is also advisable to use technological tools and innovative solutions that facilitate the automation and optimization of processes. Finally, it is crucial to have a training and education plan in new technologies and digital skills to ensure that all organization members are prepared to adapt to changes and make the most of the opportunities offered by digital transformation (Patiño, 2018; Teslia et al., 2016).

The implementation of cybersecurity poses a series of challenges and risks that are important to take into account. Firstly, one of the main challenges is the adaptability and constant updating of security measures. Technological advances and new cyber threats demand that organizations constantly stay aware of changes and update their security systems effectively. Another challenge relates to the need for cybersecurity awareness and education. Many employees need to learn to recognize and avoid cyberattacks, which can put company security at risk. Cybersecurity implementation can also face technical challenges, such as integrating different systems and managing data securely. It is essential to address these challenges and risks with practical strategies and prioritize the protection of organizations' digital infrastructure.

Commercial Technologies for Cybersecurity

In today's digital world, cybersecurity has become an unavoidable priority for companies and governments. With cyberattacks on the rise, the demand for advanced technologies and robust solutions to protect systems and data is higher than ever. The commercial technologies used nowadays in cybersecurity, according to Palo Alto Networks (2023), include:

Authentication and Identity Management

Technologies Used

Multi-factor authentication (MFA)—essential technology that adds layers of security by requiring multiple forms of verification before granting user access. Usage example: Financial institutions use MFA to protect user accounts by combining passwords with a temporary code sent to a user's mobile device.

Identity and access management (IAM)—solutions such as Okta or Microsoft Azure Active Directory allow organizations to manage and monitor user identities and access different corporate resources. Usage example: Companies implement IAM to ensure only authorized employees can access critical systems and sensitive data.

Encryption

Technologies Used

Encryption of data at rest and in transit—using algorithms such as AES and RSA to encrypt data, ensuring that information is inaccessible during transfer or storage. Usage example: Cloud storage services use encryption to protect user data stored on their servers.

Network Security

Technologies Used

Next-generation firewalls and intrusion prevention systems (IPS)—tools like Cisco Firepower or Palo Alto Networks monitor network traffic and block suspicious activity. Usage example: Organizations use IPS to detect and prevent automated attacks and other network threats.

Virtual private network (VPN)—allows users to establish a secure, encrypted connection to a corporate network from a remote location. Usage example: During remote work, employees use a VPN to access internal company resources securely.

Security Analysis and Incident Response

Technologies Used

Extended detection and response (XDR) tools—platforms such as SentinelOne or CrowdStrike provide complete visibility across endpoints, networks, and servers, facilitating rapid threat detection and automated response. Usage example: Technology companies deploy XDR to detect anomalous behavior in real time and respond to security incidents in an automated manner.

Emerging Technologies: Their Impact on Cybersecurity for Digital Transformation

Artificial Intelligence in Cybersecurity

Artificial intelligence (AI) transforms cybersecurity, offering new ways to detect and respond to threats in real time. AI can analyze large volumes of data to identify suspicious patterns and behaviors, enabling faster and more accurate threat detection than traditional methods. Additionally, AI systems are used to automate responses to security incidents, reducing the burden on cybersecurity teams and improving the effectiveness of responses (Morgan, 2021).

Internet of Things

The Internet of Things (IoT) represents a significant challenge for cybersecurity due to the large number and diversity of connected devices, many of which need to be designed with security as a priority. This increases the attack surface and exposes unique vulnerabilities in corporate and consumer networks. Cybersecurity technologies for IoT must address everything from device security to network protection and transmitted data, ensuring the integrity of increasingly interconnected systems (Weber, 2023).

Cloud Computing

Cloud computing has allowed companies to scale resources and improve efficiency, but it has also introduced new cybersecurity risks, such as misconfiguration of cloud environments that can expose sensitive data. Cloud security solutions, such as web application firewalls and identity and access management tools, are crucial to protecting data hosted on cloud services (Jackson, 2022).

Big Data and Cybersecurity

Big data offers significant opportunities to improve cybersecurity by analyzing massive data sets to detect anomalies and attack trends. However, it also poses challenges in protecting and managing these large volumes of data. Emerging big data technologies require robust security measures, including advanced encryption and specific solutions for large-scale data protection (Thompson, 2023).

To illustrate the concepts described, we present some diagrams explaining each emerging technology mentioned and their impact on cybersecurity for digital transformation. These diagrams include details on AI, IoT, cloud computing, and big data, each highlighting how these technologies strengthen security in a digital environment. The description and use of each one are presented in Table 1.

Table 1. *Description and Use of Emerging Technologies in Digital Transformation*

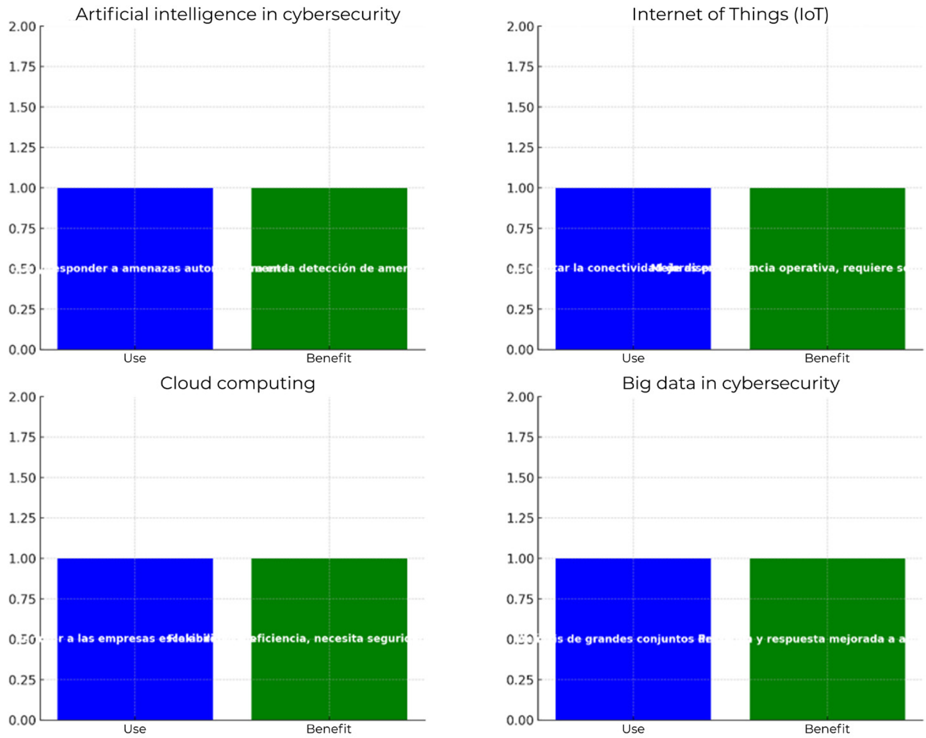
Technology	Use	Benefit
AI in cybersecurity	Automatically detects and responds to threats by analyzing large volumes of data to identify anomalous behavior patterns	Improves speed and accuracy in threat detection
IoT	Increases device connectivity but increases the attack surface due to the diversity and number of connected devices	Improves operational efficiency but requires robust security measures to protect corporate and consumer networks
Cloud computing	Allows companies to scale resources and improve efficiencies but also introduces new risks, such as misconfiguration that can expose sensitive data	Flexibility and efficiency with the need to implement specific security solutions for the cloud

Big data	Analyzes extensive data sets to detect threats and anomalies, addressing challenges to protect and manage that data	Improved ability to anticipate and respond to cyber threats by identifying trends from large volumes of information

Source: Own elaboration.

Figure 1 shows the impact of emerging cybersecurity technologies on digital transformation. Each diagram highlights the main application and benefit of the following technologies: 1) AI in cybersecurity: used to automatically detect and respond to threats, improving the speed and accuracy of detection; 2) IoT: increases device connectivity, requiring robust security measures to protect expanded networks; 3) cloud computing: allows companies to scale resources, needing specific security solutions to protect data in cloud environments, and 4) big data in cybersecurity: uses the analysis of large volumes of data to detect trends and threats, improving forecasting and response capacity.

Figure 1. *Diagrams of the Impact of Emerging Technologies on Cybersecurity*



Source: Own elaboration.

The diagrams in Figure 1 use bars to represent two main categories: "use" and "benefit" of each technology. The function of each axis in the diagrams is as follows:

X-axis (horizontal)—represents the categories compared for each technology. In this case, the X-axis has two categories labeled "use" and "benefit." These categories describe how each technology is used in cybersecurity and what primary benefit it brings.

Y-axis (vertical)—shows a measurement scale for the compared values. In the diagrams provided, the Y-axis does not represent a traditional quantitative scale but is used more as a method to organize information visually. The bars are the same height since they aim to highlight the textual information within them, not measure quantities.

Each bar in the diagram is colored differently to distinguish between the use and benefit of each technology. The information in the bars provides specific details on how each technology is applied in the cybersecurity context and the benefits it offers. This helps to visually understand the contribution of each technology to digital security in the digital transformation era.

Conclusions

Foresight studies are essential for making policies and strategies that minimize the risks that may arise in organizations and allow better decisions to be made in the future. To achieve this, interactive work must be conducted in which all stakeholders are involved, futuristic projects are built, and existing processes are improved.

Cybersecurity awareness is an ongoing activity that should begin at the primary education level and involve all citizens. This will undoubtedly benefit people and the workplace, thus creating a cyber-resilient nation.

The use of strategic foresight is the best option for entities to be prepared for future changes, both social, political, and economic, and to be able to respond to them. That is, the formulation of strategic plans allows companies to respond resiliently to possible changes that may arise. The above does not mean that strategic foresight will solve the future, but it will allow us to minimize many risks and threats that an organization may suffer.

This is where the generation of knowledge and innovation plays a vital role in cybersecurity forecasting and the integration of all the actors involved so that this planning leads to improvements in processes and, in the case of cybersecurity, serves as a guide to minimizing the risks and threats that emerging technologies bring with them.

The construction of an entity with these particularities poses apparent challenges. First, management must provide specialized resources, such as public communication, cybersecurity, and legal advice. Second, it requires making and implementing agreements. Lastly, adequate investment is needed to ensure the success of this company.

Despite the challenges involved, the long-term benefits of this initiative are evident. An example of this is the approach adopted by the European Union to promote investment in R&D&i within the framework of Horizon 2020. There are several public-private partnerships (PPP), especially in cybersecurity, to direct investment toward the interests and needs of production sectors.

Nonetheless, individual knowledge of cybersecurity is not enough. People must engage effectively with their companies and nations. In the workplace, companies and organizations must provide employees with a sense of belonging, job security, group identity, and even a shared purpose, in addition to offering added values beyond direct financial remuneration. At the national level, it is essential to inform citizens that their cybersecurity contributes to national security.

In conclusion, to improve our global cybersecurity culture, it is essential to 1) take into account the human factor, 2) have the institutional support and resources necessary to implement the required plans and coordinate them with state interests, and 3) bring together all stakeholders in a public-private partnership to define the most appropriate work strategies that guarantee success.

Digital transformation and cybersecurity will continue to evolve in the future as technologies advance and cyber threats become more sophisticated. Organizations must adapt to new trends and challenges to protect their digital infrastructure. Two critical areas in this evolution are artificial intelligence (AI) and machine learning (ML) in digital security. AI and ML enable cybersecurity solutions to be more proactive and efficient by detecting and mitigating threats in real time. These technologies can analyze large amounts of data in an automated manner, identifying patterns and anomalies to anticipate future attacks. Their application to digital security will be fundamental in the fight against cybercriminals.

Artificial Intelligence and Machine Learning in Digital Security

Artificial intelligence (AI) and machine learning (ML) have revolutionized digital security. These technologies allow cybersecurity systems to learn and adapt autonomously without constant human intervention. AI and ML analyze real-time data, identify anomalous patterns and behaviors, and generate alerts for potential threats. Additionally, they can predict and anticipate future attacks, providing greater protection in a constantly evolving cyber environment. These advanced capabilities make AI and ML essential tools for digital security, enabling early detection and rapid response to threats.

Internet of Things and Its Impact on Cybersecurity

IoT is a trend in digital transformation that is producing a significant impact on cybersecurity. With the increasing interconnection of devices and systems, the need arises to protect computer equipment and everyday objects that are part of daily life. IoT devices are exposed to cyber threats, such as unauthorized access, data interception, or remote tampering. Appropriate security measures such as data encryption, strong authentication, and network segmentation must be implemented to mitigate these risks. Furthermore, monitoring and managing the security of IoT devices becomes essential to ensure a secure and reliable digital transformation in a connected environment.

The cybersecurity technologies discussed are critical to protecting critical infrastructure and valuable data in today's digital environment. Proper implementation can mean the difference between security and vulnerability in the ever-evolving threat landscape.

References

Arpi-Saquipay, W. A., & Cajamarca-Criollo, O. A. (2023). Análisis de riesgos de seguridad de la información en una Institución de Educación Superior en Ecuador, basado en la Norma ISO 27002 Anexo A dominio 7. *MQRInvestigar, 7*(3), 2793-2808. https://doi.org/10.56048/MQR20225.7.3.2023.2793-2808

Banco Interamericano de Desarrollo. (2020). *Ciberseguridad: Riesgos, avances y el camino a seguir en América Latina y el Caribe.* Banco Interamericano de Desarrollo; Organización de Estados Americanos. https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf

Barcia Baque, G. A. (2023). *Implementación del estándar ISO/IEC 27001 para la seguridad de la información en la Unidad Educativa Fiscal Cultura Machalilla* [Bachelor's thesis, Universidad Estatal del Sur de Manabí]. Repositorio UNESUM. https://repositorio.unesum.edu.ec/bitstream/53000/5917/1/BARCIA%20BAQUE%20GABRIEL%20ALEXANDER.pdf

Bedoya Velásquez, J. E., & Patiño Castrillón, J. I. (2023). *Plan estratégico para la identificación de riesgos y vulnerabilidades en la seguridad de la información de los datos personales en una empresa* [Bachelor's thesis, Tecnológico de Antioquia]. Repositorio TDEA. https://n9.cl/25ntkg

Cando Cando, E. D. (2024). *Propuesta de mejora de seguridad de la información digital a desarrollarse en el centro de mediación Online Dispute Resolution Quito-Rumipamba, Ecuador* [Master's thesis, Escuela de Posgrados Newman]. Repositorio EPNEWMAN. https://repositorio.epnewman.edu.pe/bitstream/handle/20.500.12892/929/rev_trabajo_obtencion_de_grado_edwin_daniel_cando_cando_epnewman_invest_aplicada.pdf?sequence=1&isAllowed=y

Cano, J. (2011). Ciberseguridad y ciberdefensa: Dos tendencias emergentes en un contexto global. *Sistemas,* (119), 4-7. https://acis.org.co/archivos/Revista/119/Editorial.pdf

Cano, J. (2015, 13 de diciembre). Cultura organizacional de seguridad de la información. Más allá de las implementaciones tecnológicas. https://insecurityit.blogspot.com/2015/12/cultura-organizacional-de-seguridad-de.html

Cano. J. (2016). Modelo de madurez de cultura organizacional de seguridad de la información: Una visión desde el pensamiento sistémico. In P. Ll. Ferrer Gomila & M. F. Hinarejos Campos, *Actas de la XIV Reunión Española sobre Criptología y Seguridad de la Información* (pp. 24-29). https://www.researchgate.net/publication/309717795_Modelo_de_madurez_de_cultura_organizacional_de_seguridad_de_la_informacion_Una_vision_desde_el_pensamiento_sistemico-cibernetico

Castillo Accarapi, W. (2023). *Sistema de gestión de la seguridad de la información utilizando la metodología Magerit en las redes informáticas de la Empresa Electronic Mihaba* [Bachelor's thesis, Universidad Andina Néstor Cáceres Velásquez]. Repositorio UANCV. https://repositorio.uancv.edu.pe/server/api/core/bitstreams/3142acc5-a69d-4fb8-8109-8705189e6ec0/content

Cisco. (2023). *Cisco Firepower.* https://www.cisco.com/

Evans, M., & Farrell, P. (2020). Barriers to integrating Building Information Modelling (BIM) and lean construction practices on construction mega-projects: A Delphi study. *Benchmarking: An International Journal, 28*(2), 652-669. https://doi.org/10.1108/BIJ-04-2020-0169

Fong, N., & Bayona-Oré, S. (2022). Consideraciones para el cumplimiento de la política de seguridad de la información. *Revista Ibérica de Sistemas e Tecnologias de Informação,* (E51), 528-539.

Fundación Telefónica. (2016). *Ciberseguridad, la protección de la información en un mundo digital*. Planeta.

Goundar, S., Avanija, J., Sunitha, G., Madhavi, K. R., & Bhushan, S. B. (2021). *Innovations in the Industrial Internet of Things (IIoT) and Smart Factory.* IGI Global.

Ibarra, D., Ganzarain, J., & Igartua, J. I. (2018). Business model innovation through industry 4.0: A review. *Procedia Manufacturing,* (22), 4-10. https://doi.org/10.1016/j.promfg.2018.03.002

Instituto Nacional de Ciberseguridad [INCIBE-CERT]. (2020). Incibe-Cert. https://www.incibe-cert.es/

itTrends. (2019, 29 de marzo). Crecen los ataques cibernéticos, especialmente los destinados a Lot. IT https://www.ittrends.es/seguridad/2019/03/crecen-los-ataques-ciberneticos-especialmente-los-destinados-a-io

Könnölä, T., Scapolo, F., Desruelle, P., & Mu, R. (2010). Foresight tackling societal challenges and implications on policy-making. *Futures, 43*(3), 252-264. https://doi.org/10.1016/j.futures.2010.11.004

Microsoft. (2023). *Azure Active Directory.* https://azure.microsoft.com/en-us/services/active-directory/

Mijares, V. M. (2020). Filling the structural gap: Geopolitical links explaining the South American Defense Council. *Colombia Internacional,* (101), 3-28. https://journals.openedition.org/colombiaint/4185

Miles, I. (2010). The development of technology foresight: A review. *Technological Forecasting and Social Change, 77*(9), 1448-1456. https://doi.org/10.1016/j.techfore.2010.07.016

Mintzberg, J. L., Lampel, J., & Ahlstrand, B. (1998). La estrategia y el elefante: una síntesis de las más célebres escuelas de estrategia, concebida para aplicar lo mejor de cada una. *Gestión, 3*(4), 24-34. http://planuba.orientaronline.com.ar/wp-content/uploads/2009/09/02b-mintzberg-la-estrategia-y-el-elefante.pdf

Mitrovic, Z., Taylor, W., Mymoena, S., Claassen, W., & Wesso, H. (2013). E-social Astuteness skills for ICT-supported equitable prosperity and a capable developmental state in South Africa. *International Journal of Education and Development Using Information and Communication Technology, 9*(3), 103-123. https://files.eric.ed.gov/fulltext/EJ1071374.pdf

Muñoz Campuzano, P. S. (2021). Modelos de seguridad para prevenir riesgos de ataques informáticos: Una revisión sistemática. [Bachelor's thesis, Universidad Politécnica Salesiana]. Repositorio UPS. https://dspace.ups.edu.ec/bitstream/123456789/20932/1/UPS-GT003373.pdf

Observatorio de la Seguridad de la Información [INTECO]. (2012). *Estudio sobre la seguridad de los sistemas de monitorización y control de procesos e infraestructuras* (SCADA). INTECO. https://www.aguasresiduales.info/revista/libros/estudio-sobre-la-seguridad-de-los-sistemas-de-monitorizacion-y-control-de-procesos-e-infraestructuras-scada

Okta. (2023). Okta Identity Cloud. https://www.okta.com

Organization of American States [OAS]. (2017). Why a cyber-risk oversight? En *Cyber-Risk oversight handbook for corporate boards* (p. 4). OEA. https://www.oas.org/en/sms/cicte/docs/ENG-Cyber-Risk-Oversight-Handbook-for-Corporate-Boards.pdf

Palo Alto Networks. (2023). Next-Generation Firewalls. https://www.paloaltonetworks.com/

Patiño Mazo, E. (2018). Planeación estratégica de mercadeo y relaciones de transferencia en el ecosistema digital. *Espacios, 39*(50), 13-27. https://www.revistaespacios.com/a18v39n50/a18v39n50p13.pdf

Pérez Zúñiga, R., Mercado Lozano, P., Martínez García, M., Mena Hernández, E., & Partida Ibarra, J. A. (2018). La sociedad del conocimiento y la sociedad de la información como la piedra angular en la innovación tecnológica educativa. *Revista Iberoamericana para la Investigación y el Desarrollo Educativo, 8*(16), 847-70. https://www.scielo.org.mx/scielo.php?pid=S2007-74672018000100847&script=sci_arttext

Rosales Montalbán, E. A., Martelo Gómez, R. J., & Franco Borré, D. A. (2020). Diseño de un sistema de gestión de seguridad de la información para el proceso administrativo de la infraestructura tecnológica de instituciones académicas basado en Magerit. *Aglala, 11*(1), 227-245. https://revistas.uninunez.edu.co/index.php/aglala/article/view/1579

Sain, G. (2018). La estrategia gubernamental frente al cibercrimen: La importancia de las políticas preventivas. En *Cibercrimen y delitos informáticos: Los nuevos tipos penales en la era de internet* (pp. 7-32). Erreius. https://www.pensamientopenal.com.ar/system/files/2018/09/doctrina46963.pdf

Sáinz Peña, R. M. (2016). Ciberseguridad, la protección de la información en un mundo digital. *Revista TELOS.* https://n9.cl/n5bry

Sánchez Holguín, A. del M., Imán Sánchez, A. N. K., Chocan Sosa, E. A., Barreto Espinoza, K. L., & Torres Ruiz, M. I. (2023). *Propuesta de mejora de los servicios del taller R&T a través de un análisis de procesos aplicando metodologías de mejora continua* [Final project, Universidad de Piura]. Repositorio UDEP. https://pirhua.udep.edu.pe/backend/api/core/bitstreams/b2a30486-9b67-46dc-b341-3499a699d2d3/content

Schmitt, U. (2018). Rationalizing a personalized conceptualization for the digital transition and sustainability of knowledge management using the SVIDT Method. *Sustainability, 10*(3), 839. https://doi.org/10.3390/su10030839

Sepúlveda Marciales, C. M., & Medina Ulloa, O. L. (2024). *Desarrollo de un sistema tutorial inteligente para la implementación del modelo de medición de madurez y territorios inteligentes para Colombia (MMMCTIC)* [Bachelor's tesis, Universidad Santo Tomás]. https://n9.cl/4udig

Teslia, I., Yehorchenkov, N., Iegorchenkov, O., Kataieva, Y. (2016). Enterprise information planning - A new class of systems in information technologies of higher educational institutions of Ukraine. *Eastern-European Journal of Enterprise Technologies, 4*(2), 11-23. https://journals.uran.ua/eejet/article/view/74857

Valencia Duque, F. J. (2021). *Sistema de gestión de seguridad de la información basado en la familia de normas ISO/IEC 27000.* Universidad Nacional de Colombia. https://repositorio.unal.edu.co/bitstream/handle/unal/80158/9789587946017.pdf?sequence=2&isAllowed=y

Vial, Gregory. (2019). Understanding digital transformation: A review and a research agenda. *Journal of Strategic Information Systems, 28*(2), 118-44. https://n9.cl/3rlun

World Economic Forum. (2013). *Global Risks 2013* (8th ed.). World Economic Forum. http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2013.pdf