ISSN 2007-9737

Cyber Hygiene in Smart Metering Systems

Juan C. Olivares-Rojas[1], Enrique Reyes-Archundia[1], José A. Gutiérrez-Gnecchi[1],
Ismael Molina-Moreno[1], Arturo Méndez-Patiño[1], Jaime Cerda-Jacobo[2]

[1] Tecnológico Nacional de México / I. T. de Morelia,
División de Estudios de Posgrado e Investigación, Morelia,
Mexico

[2] Universidad Michoacana de San Nicolás de Hidalgo,
Facultad de Ingeniería Eléctrica, Morelia,
Mexico

{juan.or, enrique.ra, jose.gg3, ismael.mm, arturo.mp}@morelia.tecnm.mx,
jaime.cerda@umich.mmx

Abstract. One of the fundamental components of smart cities is the smart grid characterized by various information and operational technologies that guarantee reliable and clean energy supply. For this reason, they are a fundamental pillar for achieving sustainability in the world in which we live. Despite the enormous advantages of the smart grid, it has quite a few challenges; one that has been fundamental in recent years is cybersecurity. The traditional approach to address cybersecurity issues generally does not consider the human factor as the main component. Recently, the concept of cyber hygiene has emerged, where the social and human aspect is fundamental since in the same similarity with traditional hygiene, the fact of carrying out personal care practices can contribute to improving people's health, in this sense, having better personal cybersecurity practices will allow for better cybersecurity performance of systems. This work shows the implementation of cyber hygiene in the context of smart grid, showing a methodology to carry it out and applying it in the context of smart metering systems. The results show that the proposed method can successfully be used in the smart grid and can be applied to other contexts.

Keywords. Cybersecurity, cyber hygiene, internet of things, smart grid, smart meters.

1 Introduction

Cyber Hygiene is a novel concept. There is not a unique definition [1], but most authors consider it as an analogy with daily hygiene. For instance, the idea of washing hands and teeth could improve personal health. In the cybersecurity context, cyber hygiene pretends to enhance the protection of all information systems through the implementation of security controls and its monitoring by all the users participating in the information processes.

Nowadays, cybersecurity is an important issue due to the Digital Transformation (DX) carried out by the Information Technologies (IT), Operational Technologies (OT), and Consumer Technologies (CT) of the Fourth Industrial Revolution (4IR).

One of the most critical challenges is guaranteed the protection of data generated for all these technologies. Notably, DX has improved most of the daily human activities, particularly the cities that have been converted into smart cities considering the pillar of sustainability: society, technology, economics and environment. For this reason, cybersecurity is a very important aspect of technology and sustainability [2].

One of the cornerstones of smart cities is the energy systems, and the power grid is not the exception. The power grid has converted to Smart Grid (SG) with new opportunities, which has facilitated the grid operation and produces a reliable and cheaper electrical energy supply. Still, the grid inherits the challenges of most of these 4IR technologies, include cybersecurity [3].

SG is considered as vital technology such as resistance to climate change and environmental damage, global health, food security and

doi: 10.13053/CyS-27-2-3894

agricultural development, education, human rights, gender equality, and water. SG, as critical infrastructure, requires cybersecurity for its protection [4].

At present, there are a lot of works focused on achieving cybersecurity for SG. Still, there is a lack of works focusing on cyber hygiene, which considers the human factor as a vital element to protect SG assets.

The authors of this paper find cyber hygiene as a critical factor to improve cybersecurity in SG, and other Internet of Things (IoT) domains due to personal protection actions of all actors in all SG operations could strengthen the protection of the SG.

The participation of all actors is essential to guarantee cybersecurity in any domain. For instance, public health is not only necessary; the personal hygiene of each person also is required the participation of other actors like the government because the community needs some public services such as street cleaning, picking up trash, among others.

These public services are required for healthcare. In the same context, electrical energy supply is a public service provided by utilities. The cybersecurity of the SG results of the cyber hygiene of all actor participates in the generation, transmission, distribution, and consumption of electrical energy.

This paper presents a practical cyber hygiene methodology for SG. The implementation of this methodology was tested in the Smart Metering System (SMS) domain due to the complex implementation in all SG domains. This paper can contribute to improving the cybersecurity operations in SG through the use of methodological cyber hygiene practices and policies.

This paper is organized as follows. Section 2 shows a review of cybersecurity and cyber hygiene concepts. Section 3 shows the proposed cyber hygiene methodology and its implementation is shown in Section 4. The results of testing the proposed methodology are discussed in section 4 while Section 5 shows the final conclusions.

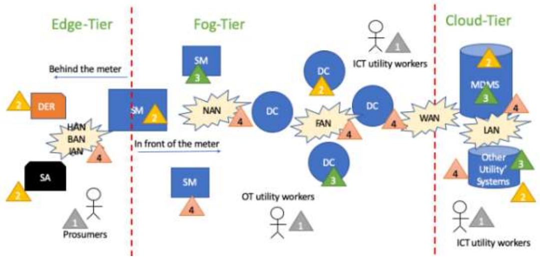

Fig. 1. SMS Architecture based in IoT and EFCDA

2 State of the Art

2.1 Smart Grids

One of the main SG applications is the Smart Metering System (SMS), which is composed of a set of technologies to measure the consumption/production of electrical energy and report this data to billing systems in the utilities. The SMS allows end-users to check their consumption/production patterns and facilitate the process of energy use to achieve better sustainability use of electrical energy [5].

The most critical components of SMS are the Smart Meters (SM), Communication Networks (CN), the Measurement Data Management System (MDMS), and other utilities' information systems and applications [6].

There are other essential components such as Appliances (A), Smart Appliances (SA), Distributed Energy Resources (DER), Data Concentrators (DC), Display Information Devices and Applications, among others. The most implemented architecture of SMS is the Advanced Metering Infrastructure (AMI) [7].

AMI defines a work of interoperability among the SMS components. The SMS is a complex system due to the vast diversity of components. For instance, CN are diverse and forms different tiers according to its geographical location.

Behind the meter exist a CN composed by SA and DER which communicate with SM, this network is called Home Area Network (HAN) if the SG is at home, Building Area Network (BAN) whether in a Building, or Industrial Area Network in an industry. In front of the meter exists others CN according the distance and components which are

Table 1. Risk examples in SG

Risk	Threat	Vulnerabilities
Power Outages	Remote On/Off Switch	Bad network configuration to remote shell
Disruption, System compromises	Cloning SM	Weak alarm report when a SM is changed
Hijack or Brick Meter/DCs	Remotely Update	Incorrect privileges for remote users

Table 2. Examples of risk impacts in SG

Risk	Impact	Estimation
Power Outages	Disconnect a house, build or industry.	Low
Disruption, System compromises	The client consumption/productions readings are not correct and cannot billing correctly.	High
Hijack or Brick Meter/DCs	The SM is hijacked and it is no availability to the utility.	Medium

Table 3. Threat Evolution

Threats	Solutions
Virus (the 1990s)	Anti-virus defense and firewall
Worms (the 2000s)	Intrusion detection and prevention systems
Botnets (late 2000 to present),	Reputation, DLP, firewalls with application recognition
Advanced Persistent Attacks (APT, currently)	Visibility and context strategy.

interconnect. The CN formed by SMs and one DC is called Neighbor Area Network (NAN).

The interconnection between other DCs is called Field Area Network (FAN), and the last interconnection between main DC with the utility's data center is called WAN (Wide Area Network). Also, in the data center exists interconnection between different utility servers form a Local Area Network (LAN).

The main applications of SMS not only include data measuring and reporting to visualizing in web and mobile applications. The utilities can connect and disconnect clients automatically via SM. The SM can publish some alarms and events and also check some security aspects like tampering and fraud detection.

The first SM appeared more than 15 years ago and actually more of them are obsolete. At the moment, the next generation of SM are appearing and bringing new applications to the end-users like data analytics, power quality, among others. One example of these new SM is SMETS2 [8].

The SM is the cornerstone of SMS. SM is an embedded system capable of measure energy consumption/production with CN. These capabilities to communicate data through CN make the SM as an IoT device. Right now, other IoT devices are integrated to SM in the form of Intelligent Electronics Devices (IED). The cybersecurity of SM is very important and also its cyber hygiene, and those are vital for cybersecurity in SMS and SG.

In general, IoT is considered as part of a Cyber-Physical Systems (CPS) [9]. The four components of a CPS are People, Processes, Data, and Objects. The four elements are so essential, but all begins with people. Human factor is vital in CPS and it is a key factor in cybersecurity through cyber hygiene [10].

On the other hand, in IoT and other domains, new computational paradigms have appearing trying to improve the performance of the systems. One of these new paradigms is the Edge-Fog-Cloud Distributed Architecture (EFCDA). This novel paradigm allows the partition of the computation capabilities in different tiers according to each device and where the data is needed is closer [11].

Figure 1 shows the implementation of SMS as an IoT and EFCDA. The three tiers of EFCDA are showed. Note that triangles represent one of the four crucial components of CPS: 1. People, 2. Objects, 3. Data, and 4. Processes.

2.2 Introduction to Cybersecurity in Smart Grids

Cybersecurity is the combination of various technologies, processes, and controls that are designed to eliminate risks of cyberattacks [12]. The consequences of a security breach are diverse. The significant effects are ruined reputation, vandalism, theft, loss of income, intellectual property damaged, among others.

The use of IoT devices, embedded systems, and other cyber physical systems have increased the risk of cyberattacks [13].

One main component of the Smart Cities is the cyber-physical systems. The cybersecurity of any systems is given by the cybersecurity of the least element of its architecture; in this case, all the objects in the cities both physical and virtual, including humans [14].

SMs are not just for billing, and hackers can steal, manipulate, and disrupt it. There is the possibility to bring down the SG through hacking Supervisory Control and Data Acquisition (SCADA) and SMs. The SG is a centrally managed distributed network of millions of devices ready to be hijacked. Traditionally, the cybersecurity in SG has been focused on SCADA systems because the protection of the most significant assets is vital due to the decentralization of SG [15].

SCADA systems are present in the generation, transmission, and distribution processes in the utilities. The customer process is as crucial as the other processes. The cybersecurity must be improved in the customer process. The most important customer processes are related to SMS.

Another way to classify the SG for better understanding is through voltage. SG can be divided in High-Voltage (bulk generation and transmission), Medium-Voltage (Distribution), and Low-Voltage (Consumer). Cybersecurity solutions focused on the low-voltage grid are becoming more important. These allow energy suppliers to recognize whether a lack of cybercriminal activity on the low-voltage grid is real or simply that information gathering attacks are going unnoticed.

Recently two aspects have been taken an important role in SG cybersecurity: communications [16] and sensors [17]. In addition, communications and sensors are vital in any sustainable city. For this reason, it is very important to strengthen cybersecurity in telecommunications and sensor devices.

The cybersecurity concepts are well expressed in the John McCumber's Cybersecurity Skills Cube (CSC) [18]. CSC is composed of three parts: cybersecurity principles (confidentiality, integrity, and availability), information states (transmission, storage, and processing), and countermeasures (technology, policies and practices, and people).

Table 4. Example of cybersecurity policies in SG

Policies	Countermeasures / Best Practices
Analyze all income and outcome network packages	Keep the firewall
Use antivirus and antispyware	
Use unique passwords for each online account.	Use a keychain software to store and retrieval passwords
Use a strong password (do not use dictionary words or names in any language, don't use common misspellings in dictionary words, do not use team names or accounts, if possible, use special characters such as ¡@ # $% & * (), and use a password with ten or more characters)	Implement password accounting where a new password is created
Restrict remote access to privilege account	Configure remote access software to don´t allow root or admin accounts connect directly to the services.

The cybersecurity principles well-known as CIA (Confidentiality, Integrity, and Availability) are the basis of data protection. The most important thing in our time is the data. In the SG utilities, users, and other participants provide data. The data is present on computing devices, operation data, online information, user identity, financial data, among others.

The data is represented in three states: 1. Storage is the static data saved in files, databases and other storage mechanisms; 2. Transmission, who is the data transmitted through CN, and finally, 3. Processing, where the data is processed inside the microprocessors via algorithms implement into the software.

SG operational data is time-sensitive and different in each layer: edge, fog, and cloud. It varies from microseconds in substations and up to seconds and even minutes in SM at the consumers' premises as well as substations.

The data is protected through a set of countermeasures or controls such as technologies, policies and practices, and people. Traditionally the IT personnel focused on cybersecurity on technologies. Still, in the last decade, with the use of security and IT governance frameworks, the cybersecurity roles have been changed to policies and practices. Some works has been showed the important of human factors in cybersecurity and cyber hygiene [19].

Data confidentiality is related to personal information. Data are classified according to confidentiality in maximum secrecy, secrets, confidential records, and restricted. In SG, the confidentiality and privacy of the data are paramount. Clients are responsible of its personal and sensitive data; also, the utility is responsible of the personal data of its clients.

Examples of personal data in SG are data consumptions/production records through the time, number of credit cards, financial history, among others.

Data integrity is regarding to quality, accuracy, and validity of the data; while data availability is related to services that are continuously working all the time. The availability of SMS is so vital for the SG operation. The availability of SMS data and services are affected by natural disasters, equipment failures, cyberattacks like Denial of Service (DoS), among others.

A good cybersecurity design implies and availability target of 99.999%, which it represents less than 5.26 minutes per year unavailability. This requires the implementation and monitoring of countermeasures such as Authentication, Authorization and Accounting (AAA).

An example of a AAA is using a credit card in the billing process. Authentication refers to who it is. Authorization refers how much can the customer can spend.

Audit refers how customers spent the money. Authentication requires that all users identify themselves with something they know (password), something they have (card), and something they are (fingerprint).

Authorization is regarding to the privileges in the systems derived to the authentication process. Audit is crucial to understand the user's actions and to stablish a base line of their activities.

Table 5. STRIDE Threats and Security Objectives

STRIDE Threats	Security Objectives
Spoofing	Authenticity
Tampering	Integrity
Repudiation	Non-repudiation
Information Disclosure	Confidentiality
Denial of Service	Availability
Elevation of Privilege	Authorization

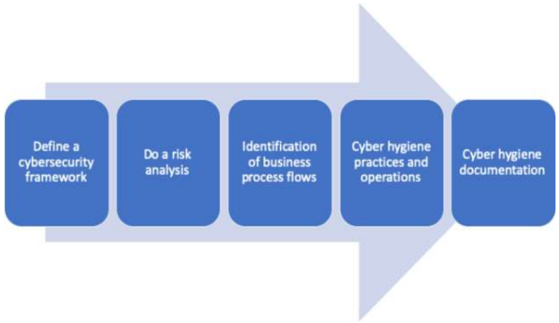
Define a cybersecurity framework
Do a risk analysis
Identification of business process flows
Cyber hygiene practices and operations
Cyber hygiene documentation

Fig. 2. A methodology for Cyber Hygiene in SG

Cybersecurity is expressed in terms of risk. The risk is a probability of a cybersecurity event occurrence. The risk of an asset is related to the increase of threats and the presence of vulnerabilities. The damage of a risk is measured by its impact. Threats are linked to external factors, while vulnerabilities refer to internal factor (weakness).

Risk as a probability is expressed in a percentage between 0 to 100%, where nothing is 0% insecure nor 100% secure. The risks cannot be eliminated but it can be mitigated, reducing the probabilities to occur. The risks are mitigated through using countermeasures and implemented security controls.

Table 1 shows three examples of risk in SG, while Table 2 shows the impacts and estimation of this risks. The risk estimation is shown at section 2.4.

For hackers and malicious people making cyberattacks, trying to obtain sensitive data that represents more revenues. External threats can be foreign people such as cybercriminals, hackers, hacktivists, terrorists, state sponsorship, and fans. Internal threats can be employees and former employees, personnel outsourcing, and reliable partners.

Table 3 shows the evolution of threats through the time. The reader can note that the threats are more specialized in the recent years and the solutions must reached them.

Other threats are human errors, hardware failures, sabotage, and software errors, among others. On the contrary, some examples of vulnerabilities are buffer overflow, inputs not validated, race conditions, weaknesses in security practices, access control problems, among others.

A kind of vulnerability is produced by malware such as spyware, adware, bot, ransomware, scareware, rootkit, virus, trojans, worms, Man in the Middle (MitM), and Man in the Mobile (MitMo). Some cyberintruders could be decrypted WiFi passwords through some cyberattacks such as social engineering, brute force attacks, and network monitoring.

Social engineering is probably the most significant threat that cyber hygiene can be solved. There are different types of social engineering attacks such as pretext, follow-up, something for something (quid pro quo), and the most important: Phishing [20]. Some social engineering tactics are authority, bullying, urgency, familiarity, and trust.

In most cases, the countermeasures and cyber cybersecurity controls depend of cybersecurity policies. The policies are related on how the assets could be protected to guarantee cybersecurity.

The implementation of these policies implies the use of best practices and countermeasures. Table 4 shows some examples of cybersecurity policies and countermeasures to implement it in SG.

Diverse authors have been focused on creating cybersecurity frameworks for SG. For example, [21] is shown a framework to detect cyber threats in the energy sector, but still, there is a lack of using social and human factors to prevent cyber risks.

2.3 Introduction to Cyber Hygiene in SG

The average user does not measure the full consequences of ignoring basic cyber hygiene. Administrators see no financial return on cybersecurity solutions. Software developers are rewarded for faster software and new features, but not for making code more secure.

The incentives to make the right decisions are always misaligned [22]. In general, for end-user some good cyber hygiene practice is do not share too much on social media, email, and web browser privacy, although, cyber hygiene is more complex.

Table 6. Risk Score for each cybersecurity premise

Value	Score
High	3
Medium	2
Low	1

Table 7. Total score for risk assessment of an asset

Total Score	Value
7-9	High
5-6	Medium
3-4	Low

Some example of cyber hygiene practices in SG are conduct a risk assessment, create a security policy, human resources security measures, make and test backup copies, keep patches and security updates, implement access controls, periodically review the response to incidents, use analysis and monitoring tools, inform users of any cybersecurity incidents, encrypt data, make equipment maintenance, update OS, planning to avoid disasters, systems monitoring, checking systems, among others.

There is consensus to consider the need to consider behaviors throughout IoT lifecycles, and SG is not an exception. Through this, key user behaviors can be identified when using SG devices. Besides, it is capable of identifying critical threats that can, for example, place sensitive information or risky behaviors that guide users to the risk of a successful attack.

Cyber hygiene helps establish expert consensus regarding key malicious threats in SG, critical protective behaviors to safeguard SG environments, and risky essential user behavior that helps cyber health of SG cybersecurity environments [23].

Some cyber hygiene operations are detecting computers infected with malware, detect suspicious network activity, identify irregular authentication attempts, describe and understand inbound and outbound traffic, provide summary information including trends, statistics, and counts, provide quick and usable access to statistics and metrics, and correspondence of events in all relevant data sources.

User awareness and necessary training to understand and implement good cyber hygiene practices in SG. A culture of knowledge of cybersecurity must be established in the utilities. Cybersecurity and cyber hygiene recognition program depend on the environment of the organization, and the threat level [24].

The cybersecurity and cyber hygiene training program must incorporate all the employees include the new ones. The modality could be In-person or online training. It is recommendable use tools such as Cyber Range [25].

Some tools for incident detection and prevention are SIEM (Security Information Management and Events), and DLP (Data Loss Prevention) could be used as cyber hygiene tools. There is a lack of cyber hygiene tools to check and verify the own cyber hygiene practices of each actor.

Legal issues of cybersecurity and cyber hygiene, such as personal legal matters, corporate legal matters, and International law are imperative in SG. Another critical aspect to consider is the ethical issues in cybersecurity and cyber hygiene, for example, personal ethical issues and corporate ethical issues.

The next steps must be followed for employees and any person trying to avoid any legal and ethical issues. If the answers are no, the process ends 1. Is it legal? 2. Does this comply with our code of ethics, policies, and principles? 3. Am I sure that this will not cause loss or damage to our companies and their shareholders? 4. Would it be okay if everyone did it?

2.4 Cybersecurity, IT Governance and Risk Management Frameworks

There is a lack of cyber hygiene frameworks, but fortunately, there are a lot of frameworks to guarantee cybersecurity.

Some frameworks are derived of best practices of industry and IT Governance. Other relevant frameworks are related with risk manager. This section describes a review of the essential frameworks necessary to define a cyber hygiene methodology.

In the United States, the National Institute of Standards and Technologies (NIST), Center give some cybersecurity guidelines for computer security resources, Department of Homeland Security (NSA), Guides for security settings, and the common criteria standard [26].

The NIST Cyber Security Framework [27] is one of the most important frameworks for the SG, and it is composed of the following steps: identity, protect, detect, respond, and recover. In addition, NIST has other Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 [28], which is composed of three parts: the core, tiers, and profile.

ISO 27000 [29] is one of the most implement cybersecurity frameworks worldwide, and it is very suitable to implement in SG. ISO 27000 standard defines twelve cybersecurity domains: 1. Risk assessment, 2. Security policy, 3. Organization of computer security, 4. Asset management, 5. Security of human resources, 6. Physical and environmental security, 7. Operations and Communications Administration, 8. Acquisition, development, and maintenance of computer systems, 9. Access control, 10. Management of computer security incidents, 11. Business continuity management, and 12. Compliance.

Other best practice and IT governance frameworks are the Control Objectives for Information and related Technology (COBIT) [30], the Information Technology Infrastructure Library (ITIL) [31], the Mexican Norm for Cybersecurity and IT Governance (MAAGTICSI in Spanish acronym) [32], among others.

The National Initiative for Cybersecurity Education (NICE) defines the National Cybersecurity Workforce Framework [33] consist of the following steps operate and maintain, protect and defend, investigate, collect and operate, analyze, supervision and development, and dispose of safely.

A useful framework for risk management is STRIDE (Spoofing Identity, Tampering with Data, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege) proposed by Microsoft [34]. STRIDE could improve the cybersecurity of diverse security objects that are shown in Table 5.

Other useful risk assessment methodology proposed by Microsoft is DREAD (Damage, Reproducibility, Exploitability, Affected Users, and Discoverability) [35].

Table 8. Risk analysis in SMS at the edge layer

Asset	Value	Threat	Vulnerability	Confidentiality	Integrity	Availability	Controls	Delay Response	Remedy	Risk
Smart Meter		Conservative population organizations against the placement of new technologies		High Only authorized persons	High The physical meter and all the information that is captured and stored	High Available to everyone involved	Monitoring of correct operation and physical integrity of the device	Minutes	Operators and new SM must be available 24/7	9 High
		Computer theft (malicious people)					Security in the placement of SM and some warning control when they are stolen	Seconds		
			Electronic fault (software) in the SM				Fault detection and warning circuitry, or fault detection software	Minutes		
Information display platforms and interfaces	High	Hacking in the system, page data.		High Only producers and consumers should know the information.	High Data not modifiable in any way	High Present the information in every way to the user, since the producer knows it without problems	Algorithm or software that provides certain security such as Firewall, antivirus, among others.	minutes	Backups Cipher all data. IT staff must be available 24/7.	9 High
Smart Appliances	High		Damage to circuitry that controls each appliance (Possibility of loss of information, Costs of circuitry)	High Storage of information and its permanence so as not to lose it.	High It must at least remain integrated without alterations.	Medium At least for a certain time to be able to keep the information when a fault occurs	Availability of variety to consumer options	minutes	Operators, new SM and electronic components must be available 24/7	8 High
		Factory setting that is following standards and does not violate a standard by each manufacturer of the smart appliance					creation but there are standards and that easy connection or interaction between SM	minutes	Never use default/factory settings	
Life of the smart meter	High	Damage due to the passage of time (building materials)		As much as the producer as the consumer can notice this	High	Low (high price)	Development of SM with long service life	minutes	SM materials and operators must be available 24/7	7 High
			Deficiency in element quality				Desirable: various suppliers	minutes		
		Population rejection	Loss in promotional expenses				Development of tests for demonstration of energy saving	days	Show the benefits of the use of SM	

Table 9. Risk analysis in SMS at the fog layer

Asset	Value (Impact)	Threat	Vulnerability	Confidentiality	Integrity	Availability	Controls	Delay Response	Remedy	Risk
RF (microwaves, wireless)	High		A little demonstration of whether or not SM cause RF damage to people. Everything is interconnected through RF: home appliances, smart meters, concentrators, and this creates a considerable increase in RF exposure. In addition to that, it seems not to be within the proper levels of microwatts of power.	Low The information should be accessible to the public and RF experts to demonstrate that it does not cause damage.	High It should be accurate and concise RF information that does not cause damage and with expert evaluation.	High It should be accurate and concise RF information that does not cause damage and expert evaluation.	Scientific demonstrations that RF emitted by SM do not cause damage to human body cells.	Seconds	RF links redundancy must be available 24/7	7 High
		Again the rejection of the population for fear of damage to health.	Little demonstration that does not cause damage to the body.				Dialogue with the population and with the government where the placement of smart meters can be made mandatory.	Days	Implement a healthcare campaigns	
Communication Network (wired such as optical fiber)	High	Temporary weather where the physical network crosses	Travel long distances for the evaluation and collection of consumption data	High	High	Low Only people belonging to the company to make corrections of damages of the Network	Damage Monitoring Systems	Seconds	Wired links redundancy must be available 24/7	7 High
Data Concentrators	High	Weather conditions can produce bad DC operation	The DC are not well located	High	High	High	System Monitoring	Seconds	DC redundancy is required all the tome	9 High

The cybersecurity baselines are a useful guideline for beginning policies and practices. The Microsoft Baseline Security Analyzer (MBSA) [36] defines the following recommendations missing security updates, administrator accounts, simple or nonexistent blank passwords, firewall settings, incorrect security settings, management settings, unnecessary services, network exchanges, security event audit, status of temporary user accounts.

Table 10. Risk analysis in SMS at the cloud layer

Asset	Value (Impact)	Threat	Vulnerability	Confidentiality	Integrity	Availability	Controls	Delay Response	Remedy	Risk
Metering Data Management System (Server)	High	Attacks of bad-intentioned people		High Only certain people with authorization	High No modification	Low Only people with certain tasks assigned by the producing company	Authenticity systems of people who can access	Seconds	IT and CERT staff must be available all the time	7 High
Information (Household data)	High	People or companies (malicious people who want the information for their personal use)		High (Only the user and the producer should have access to it)	High (should not be modifiable under any circumstances)	High (the client should access it easily)	Security in every way: in training, in transfer and storage	Seconds	Data redundancy and backups must be available 24/7	9 High
			A malfunction in the protection in algorithms, computer systems, or someone (person) that damages the system on purpose.				Physical security where information and digital security are stored	Seconds	Physical security staff must be available all the time	

Another organization which define cybersecurity baseline for Web and Mobile apps is the Open Web Application Security Project (OWASP) [37].

The OWASP Application Vulnerabilities are username enumeration, weak passwords, account lockout, lack of multi-factor authentication, insecure third-party components. The most popular exploits are firmware replacement, cloning, DoS, extraction of security parameters.

In addition, OWASP provide mobile applications most widely exposed vulnerabilities such as insecure communication, insecure data storage, insecure authentication, improper platform usage, insufficient cryptography, among others.

The OWASP Web and Cloud Application Vulnerabilities are injection, XML external entities (XXE), sensitive data exposure, broken access control, broken authentication, among others.

The Common Vulnerability Scoring System (CVSS) is a risk assessment framework [38]. CVSS is composed of the following parts. 1. Metric Group: Base Metric Group (Exploitability metrics [Attack Vectors, Attack Complexity, Privileges Required, User Interaction, Scope], Impact metrics [Confidentiality impact, Integrity impact, Availability Impact, Scope]), 2. Temporal Metric Group (Exploit Code Maturity, Remediation Level, Report Confidence), 3. Environmental Metric Group (Modified Base Metrics, Confidentiality Requirement, Integrity Requirement, and Availability Requirement).

Besides, the NIST defines the Risk Management Framework (RMF) [39] composed of the following activities Risk Identification, Risk Assessment (Score, Weight, Prioritize risk), Risk Response Planning (Determine risk response, Plan actions), Response Implementation (Implement risk response), Monitor and Assess Results (Continuous risk monitoring and response evaluation).

3 Methodology

The proposed methodology to carry out cyber hygiene practices in SG is composed of the following steps: Define a cybersecurity framework, Do a risk analysis, Identification of business process flows, and their relevance in cybersecurity and cyber hygiene, cyber hygiene practices and operations, and cyber hygiene documentation. Figure 2 shows in graphical way the proposed methodology. Following all the steps of the proposed methodology are shown.

3.1 Define Cybersecurity Framework

For the development of good cyber hygiene, it is necessary to have an adequate Information Security Management System (ISMS). The cybersecurity and IT governance frameworks are described in Section 2.4.

3.2 Do a Risk Analysis

The fundamental part of an ISMS is risk analysis, where each asset determines each main cybersecurity risk. It is necessary to evaluate the internal and external factors of the organization of each asset for developing a risk analysis. As well as the roles of those involved in the process Traditionally, risk analysis has focused on the threats and vulnerabilities part of information assets but has not considered business processes and related activities.

There are a lot of risk management and assessment frameworks (see Section 2.4). The authors define a simple risk analysis methodology to evaluate assets based on the three basic premises of cybersecurity: CIA reviewing the impact that each of them can cause. This risk methodology is optional and can be replaced by others. Bellow the simple risk management framework is shown. Table 6 shows how a score is assigned for each CIA security premises.

The different types of countermeasures and controls could mitigate risks or the absence of them must help to increase the risk.

For each asset, the threats, vulnerabilities, countermeasures and impacts are considering determining the risk for each CIA premises. The weighting results are given as the sum of the score of each premise. Table 7 shows the total score for risk assessment of an asset.

Risk management is so important but most important is Supply Chain Risk Management. The authors proposed a variation of Model Business Canvas (MBC) [40] composed of the following activities: Key associations, Key activities, Key resources, Value propositions, Cost structure, Customer Relations, Channels, Customer follow-up, Recurring income. All this process could be helping to identify, analyze, and assess risks.

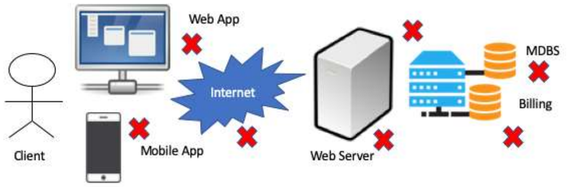

Fig. 3. Scenario 1: General connection using web or mobile apps

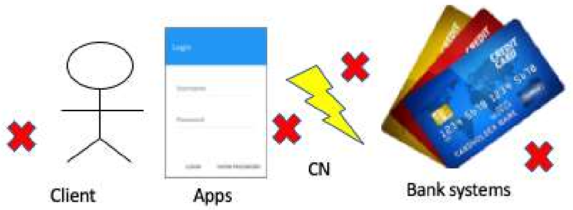

Fig. 4. Scenario 1.1 Login in apps to pay to the bill

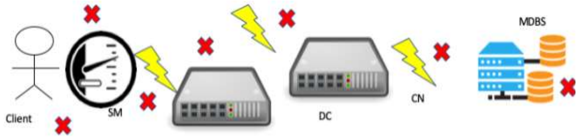

Fig. 5. Scenario 2 Data communication between SM and the utility

3.3 Identification of Business Process Flows and Their Relevance in Cybersecurity and Cyber Hygiene

In addition to risk analysis, it is necessary to visualize the resulting processes to determine risk factors and identify actors that allow them to carry out their activities. The previous steps using MBC could help in this process.

The most important thing in this part is the definition of set scenarios because we can identify, actors (people), processes, data, and objects used. This can help to determine other risks not shown in the risk management process.

Table 11. Cyber hygiene policies and operations for SG

Policy	Operation	Frequency
Defend the perimeter (build a castle)	Implement a Firewall Review firewall rules Implement a Demilitarized Zone (DMZ)	Daily
Secure communication extreme to extreme	Encrypt all communication	In each transaction
Security "Always on"	Update firmware of SG devices. Software updates and patches	In each update
Authenticate always	Using Two Factors Architecture (2FA)	In each login application
Training all the employees	War gamming and simulation	Semesterly
Business continuity	Implement and check a continuity and response emergency plans. Backup and restore data.	Daily
Use strong cybersecurity solutions	Implement hardware appliances cybersecurity Monitoring the correct functionality of the cybersecurity appliances	Daily
Security design	Avoid default password. Do not use UPnP: Universal Plug and Play. Reduce remote communication at minimum possible. Implement physical security.	Daily
AAA Always	Implements Access Controls: Mandatory, Discretional, and Attribute-Based Check the permission related.	Daily
Strong wired and wireless CN	Implement Intrusion Detection systems (IDS) Verify rules and patterns of an IDS Using anti-malware software and check updates	Daily
Strong password	Using phrases instead password Check the long of password and its components (upper and lower cases, digits, special symbols, etc.)	Daily
Make data confidentiality	Delete data Check data permissions	Daily
Fault tolerance	Backups. Redundancy in servers (mirroring), applications and CN. Verify the correct functionality of the redundant assets	Daily
Control Account	Identify and reduce the number of privileged accounts. Apply the principle of least privilege. Establish a process for revocation of rights when employees leave or change jobs. Delete shared accounts with passwords that do not expire. Record all user activity. Generate alerts for unusual behavior.	Daily
Data integrity always	Avoid tampering. Check sensors and other electrical and electronics components	Daily
Audit and certification	Audit by third parties Achieve cybersecurity certifications	Each certification

3.4 Cyber Hygiene Practices and Operations

The next step in the proposed methodology is definition of polices and operations for cyber hygiene.

In this part, it is very important to define in what frequency should it be done the operations? And should it be done manually or automatically?

3.5 Cyber Hygiene Documentation

The last step in the methodology is to document all the incidents that occurred during the cyber hygiene operations. The recommend format to report the cybersecurity events must content Incident date, Short description of the incident, Number of victims, the impact (what was taken) and the most important, how activities I must be

Table 12. Cyber hygiene operations logs

Date	Short description	No. victims	Impact	Activities to do
09/01/2020	A SM was inactive due to DoS	1	The SM was inactive 5 minutes	Check the firewall rules of the network and mainly SM firewall.
14/01/2020	A current sensor failure	1	The SM was not registered correctly the current, consumption and production readings.	Check the business continuity plan on how to work with sensor failures

Table 13. Results of testing the proposed cyber hygiene methodology

Group	1st time incident	1st time training	2nd time incident	2nd time training
1	13	0	8	20 hours
2	7	30 hours	6	0

done in ones cyber hygiene operations to reduce this risk soon.

4 Testing the Methodology

Since the SG domain is extensive, the proposed methodology has been focused on the Smart Metering Systems area. A school laboratory of SMS was used to test the methodology. This SMS is composed of 9 SMs, 3 DCs, wired and wireless CN, MDMS server and diverse A, SA and DER.

In the cyber hygiene operations, 14 people work across the SMS infrastructure in a 30-day period. The methodology was tested twice with two groups of seven participants.

The first group was not training with the method the first time while the second group was training with the proposed methodology. The second time only the first group was training.

4.1 Using a Cybersecurity framework

The authors used the MAAGTIC framework due to is the official norm in Mexico, and our principal client in the future is the Mexican utility CFE (acronym in Spanish of Federal Electricity Commission).

4.2 Implementing a Risk Analysis

The authors used their own simple methodology for risk management to do the risk analysis. Table 8, 9, and 10 show an example of the risk analysis in SMS through Edge, Fog, and Cloud layers.

The parameters used in the risk analysis are Asset, Value (Impact), Threat, Vulnerability, Confidentiality, Integrity, Availability, Controls, and Risk. These parameters are common in risk analysis. Additionally, are include Delay Response and Remedy. The last two parameters express the time delay in response to a contingency and the action that must be implemented after contingence.

4.3 Identification of Business Pprocess Flows and Their Relevance in Cyber Hygiene

The primary business process flows used in the practical case for testing are describing below.

Scenario 1. The user/client reviews their consumption and billing history through the Web or mobile application. Others consist of displaying visual information.

Figure 3 shows the general case of this scenario. The readers can note all the failures points such as mobile and web apps (the responsible are the utility's programmers), the Internet and other CN (responsible utility's network administrators), web server, MDBS, and Billing (responsible utility's sysadmin). The cyber hygiene operations in scenario one is related on each role of responsibility. For instance, programmers must be review and audit source code and must do pentesting. Network admin must check firewall and router configurations. Sysadmin must check https and SSL certificates, check database integrity in MDBS and Billing databases, and do pen testing in all Webservices and API interconnections.

A variation of scenario 1 implies that clients can pay their electricity consumption. For this subcase, clients must be authenticated in the web or mobile apps. The customer number and password will be required to access the apps, so it will be necessary for the user to build a secure and robust password, periodically the password must be changed in addition to not sharing it. Also, clients must store and protect their credit card information.

These activities are examples of cyber hygiene operations that clients must be done.

Figure 4 shows the scenario 1.1. Note that cyber hygiene roles are client, apps programmers, network administrators and bank systems administrators. Clients' cyber hygiene are described in the paragraph above. Programmer must be implemented auditing in login process and notify any inconsistency. Also, programmers must implement a correct interconnection with bank systems. The bank systems programmers and IT personnel must protect the credit card information and store transaction safely.

Oher important scenario in SMS is data communication between SM, DC, and MDBS. Scenario 2 refers to consumption/production readings and events and alarms notification between. This scenario is shown in Figure 5. Note that there are five failure points: client, SM, CN, DC, and MDBS.

The role of the client is checking the physical security of its SM. If the SM is broken or there are some electrical or electronics components altered, the client must communicate these classes of events to the utility. The SM and DC must be checked physical and logical cybersecurity for the OT employees' utility.

The OT must report any inconsistency of physical components. Also, IT employees' utility must check all the logical control such as encrypted data, firmware updates patched, embedded database backups, among others. The cyber hygiene operations in CN must be checked by the network administrators' utility monitoring traffic, implementing perimetral security, among others. In addition, OT employees' utility must check the physical cybersecurity of the means of communication like antennas, access points, and wired means.

Finally, sysadmin must check the cyber hygiene of MBDS doing operations like backups, checking data integrity, and check and monitor all the transactions between SM and DC with the MDBS.

4.4 Cyber Hygiene Policies and Operations

The authors made a literature review of the principal works form cyber hygiene cybersecurity [41-44] and general cybersecurity best practices to determine policies and operations of cyber hygiene. The list of policies and operation are shown in Table 11.

4.5 Cyber Hygiene Documentation

Table 12 shows the cyber hygiene documentation and logs registered in the testing process.

5 Results and Discussion

The implementation of the methodology particularly, in the cyber hygiene operations were highly time consume due to most of the operations are required daily. Even though the seven participants were a useful experience due to the learning process and verify in the second test period were less cybersecurity incidents.

For the fourteen participants, the methodology was clear and quick to implement. The risk analysis was made by the participation of all participants in the testing.

The cyber hygiene operations were shuffled across all participants every day. At the end of each test period, all the participators did all the cyber hygiene operations. Table XIII shows the general results of testing the proposed methodology.

The readers can note that group two has fewer incidents because they receive training in the proposed cyber hygiene methodology.

The second time, group one was training in the methodology, and they required less time because they have known most of the mistakes in the cybersecurity operation practices. In addition, the number of incidents were reduced using the methodology in each group. In general terms, all the participants are ready to work with this methodology. The unique suggestion is trying to divide the operations in different roles according to the number of participants.

The participants are very motivated to improve cybersecurity through their daily cyber hygiene routines. This aspect is crucial in cybersecurity in SG and Smart Cities.

The tests applied to the proposed methodology show that it is feasible to implement cyber hygiene operations and policies in SG through a methodological way trying to guarantee cybersecurity objectives in SG.

6 Conclusions

Cyber hygiene operations are vital to guarantee cybersecurity in SG. Cyber hygiene implies the use of the human factor as a crucial component to improving cybersecurity. In the literature, exists works related to cybersecurity and even less work focused on cyber hygiene in SG. This paper presents a methodology to implement cyber hygiene in SG. The methodology was tested with a practical case in SMS, and the result obtained shows that it is feasible its implementation in SG domains. The social participation in the daily cyber hygiene routines of each participant can contribute to improving the cybersecurity in the fields of SG and Smart Cities in a sustainable way.

References

1. **Vishwanath, A., Neo, L. S., Goh, P., Lee, S., Khader, M., Ong, G., Chin, J. (2020).** Cyber hygiene: The concept, its measure, and its initial tests. Decision Support Systems, Vol. 128, DOI: 10.1016/j.dss.2019.113160.
2. **Nathali, B., Khan, M., Han, K. (2018).** Towards sustainable smart cities: A review of trends, architectures, components, and open challenges in smart cities. Sustainable Cities and Society, Vol. 38, pp. 697–713. DOI: 10.1016/j.scs.2018.01.053.
3. **Leszczyna, R. (2018).** A review of standards with cybersecurity requirements for smart grid. Computers & Security, Vol. 77, pp. 262–276. DOI: 10.1016/j.cose.2018.03.011.
4. **Braun, T., Fung, B. C. M., Iqbal, F., Shah, B. (2018).** Security and privacy challenges in smart cities. Sustainable Cities and Society, Vol. 39, pp. 499–507. DOI: 10.1016/j.scs.2018.02.039.
5. **Marah, R., Hibaoui, A. E. (2018).** Algorithms for smart grid management. Sustainable Cities and Society, Vol. 38, pp. 627–635. DOI: 10.1016/j.scs.2018.01.041.
6. **Dileep, G. (2020).** A survey on smart grid technologies and applications. Renewable Energy, Vol. 146, pp. 2589–2625. DOI: 10.1016/j.renene.2019.08.092.
7. **Van-Aubel, P., Poll, E. (2019).** Smart metering in the Netherlands: What, how, and why. International Journal of Electrical Power & Energy Systems, Vol. 109, pp. 719–725. DOI: 10.1016/j.ijepes.2019.01.001.
8. **Department of Energy & Climate Change (2018).** Smart metering implementation programme: Progress report 2018, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/767128/smart-meter-progress-report-2018.pdf.
9. **Modeste, K. (2019).** Current standards for cyber-hygiene in industrial control system environments. In: Rieger, C., Ray, I., Zhu, Q., Haney, M. (eds) Industrial Control Systems Security and Resiliency, Advances in Information Security, Springer, Cham, Vol. 75. DOI: 10.1007/978-3-030-18214-4.
10. **Cain, A. A., Edwards, M. E., Still, J. D. (2018).** An exploratory study of cyber hygiene behaviors and knowledge. Journal of Information Security and Applications, Vol. 42, pp. 36–45. DOI: 10.1016/j.jisa.2018.08.002.
11. **Parikh, S., Dave, D., Patel, R., Doshi, N. (2019).** Security and privacy issues in cloud, fog and edge computing. Procedia Computer Science, Vol. 160, pp. 734–739. DOI: 10.1016/j.procs.2019.11.018.

12. **Laufs, J., Borrion, H., Bradford, B. (2020).** Security and the smart city: A systematic review. Sustainable Cities and Society, Vol. 55. DOI: 10.1016/j.scs.2020.102023.

13. **Ande, R., Adebisi, B., Hammoudeh, M., Saleem, J. (2020).** Internet of things: evolution and technologies from a security perspective. Sustainable Cities and Society, Vol. 54. DOI: 10.1016/j.scs.2019.101728.

14. **Habibzadeh, H., Nussbaum, B. H., Anjomshoa, F., Kantarci, B., Soyata, T. (2019).** A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities. Sustainable Cities and Society, Vol. 50. DOI: 10.1016/j.scs.2019.101660.

15. **Gunduz, M. Z., Das, R. (2020).** Cyber-security on smart grid: Threats and potential solutions. Computer Networks, Vol. 169. DOI: 10.1016/ j.comnet.2019.107094.

16. **Ferrag, M. A., Maglaras, L. A., Janicke, H., Jiang, J., Shu, L. (2018).** A systematic review of data protection and privacy preservation schemes for smart grid communications. Sustainable Cities and Society, Vol. 38, pp. 806–835. DOI: 10.1016/j.scs.2017.12.041.

17. **Abujubbeh, M., Al-Turjman, F., Fahrioglu, M. (2019).** Software-defined wireless sensor networks in smart grids: An overview. Sustainable Cities and Society, Vol. 51. DOI: 10.1016/j.scs.2019.101754.

18. **Ratchford, M. (2018).** BYOD: A security policy evaluation model. Advances in Intelligent Systems and Computing, Vol. 558. DOI: 10.1007/978-3-319-54978-1_30.

19. **Such, J. M., Ciholas, P., Rashid, A., Vidler, J., Seabrook, T. (2019).** Basic cyber hygiene: does it work?, Computer, Vol. 52, No. 4, pp. 21–31. DOI: 10.1109/MC.2018.2888766.

20. **Facetti, D. (2018).** Staying clean: cyber hygine & social engineering with scada & industrial control systems. A Thesis for the Degree Master of Science in Homeland Security, Sand Diego State University, https://digitallibrary.sdsu.edu/islandora/object/sdsu%3A22145.

21. **Leszczyna, R., Wróbel, M. R. (2019).** Threat intelligence platform for the energy sector. Software: Practice & Experience, Vol. 49, pp. 1225–1254. DOI: 10.1002/spe.2705

22. **European Union Agency for Cybersecurity ENISA (2017).** Review of cyber hygiene practices. https://www.enisa.europa.eu/publications/cyber-hygiene.

23. **Oravec, J. (2017).** Emerging cyber hygiene practices for the Internet of Things (IoT): Professional issues in consulting clients and educating users on IoT privacy and security. In IEEE International Professional Communication Conference (ProComm), pp. 1–5. DOI: 10.1109/ipcc.2017.8013965.

24. **Neigel, A., Claypoole, V. L., Waldfogle, G. E., Acharya, S., Hancock, G. M. (2020).** Holistic cyber hygiene education: Accounting for the human factors. Computers & Security, Vol. 92. DOI: 10.1016/j.cose.2020.101731.

25. **Yamin, M. M., Katt, B., Gkioulos, V. (2020).** Cyber ranges and security testbeds: Scenarios, functions, tools and architecture. Computers & Security, Vol. 88. DOI: 10.1016/ j.cose.2019.101636.

26. **Kallberg, J. (2012).** The common criteria meets realpolitik: Trust, alliances, and potential betrayal. IEEE Security & Privacy, Vol. 10, No. 4, pp. 50–53, DOI: 10.1109/ MSP.2012.29.

27. **Ibrahim, A., Valli, C., McAteer, I., Chaudhry, J. (2018).** A security review of local government using NIST CSF: A case study. Journal of Supercomputing, Vol. 74, pp. 5171–5186. DOI: 10.1007/s11227-018-2479-2.

28. **Khou, S., Mailloux, L. O., Pecarina, J. M., Mcevilley, M. (2017).** A customizable framework for prioritizing systems security engineering processes, activities, and tasks. IEEE Access, Vol. 5, pp. 12878–12894, DOI: 10.1109/ACCESS.2017.2714979.

29. **Mirtsch, M., Kinne, J., Blind, K. (2020).** Exploring the adoption of the international information security management system standard ISO/IEC 27001: A Web Mining-Based Analysis. IEEE Transactions on Engineering Management, Vol. 68, No. 1, pp. 27–100. DOI: 10.1109/TEM.2020.2977815.

30. **Amorim, A., Mira da Silva, M., Pereira, R., Gonçalves, M. (2020).** Using agile

methodologies for adopting COBIT. Information Systems, Vol. 101, DOI: 10.1016/ j.is.2020.101496.

31. **Orta, E., Ruiz, M. (2019).** Met4ITIL: A process management and simulation-based method for implementing ITIL. Computer Standards & Interfaces, Vol. 61, pp. 1–19, DOI: 10.1016/j.cs i.2018.01.006.
32. **Mexico National Intelligence Center (2020).** Administrative manual of general application in the areas of information communication and information technologies, and in the information security (MAAGTICSI) [Spanish]. https://www.gob.mx/cni/documentos/manual-administrativo-de-aplicacion-general-en-materia-de-tecnologias-de-la-informacion.
33. **Alsmadi, I. (2020).** The NICE cyber security framework. DOI: 10.1007/978-3-030-41987-5.
34. **Anwar M. N., Nazir, M., Ansari, A. M. (2020).** Modeling security threats for smart cities: A STRIDE-based approach. Lecture Notes in Civil Engineering, Vol. 58. DOI: 10.1007/978-981-15-2545-2_33.
35. **Naagas M. A., Palaoag, T. D. (2018).** A threat-driven approach to modeling a campus network security. Proceedings of the 6th International Conference on Communications and Broadband Networking (ICCBN 2018), Association for Computing Machinery, New York, NY, USA, pp. 6–12. DOI: 10.1145/31930 92.3193096.
36. **Pattanavichai, S. (2017).** Comparison for network security scanner tools between GFI LanGuard and Microsoft Baseline Security Analyzer (MBSA). 15th International Conference on ICT and Knowledge Engineering (ICT&KE), Bangkok, pp. 1–7. DOI: 10.1109/ICTKE.2017.8259628.
37. **Kritikos, K., Magoutis, K., Papoutsakis, M., Ioannidis, S. (2019).** A survey on vulnerability assessment tools and databases for cloud-based web applications. Array, Vol. 3–4. DOI: 10.1016/j.array.2019.100011.
38. **Tao, W., Yuqing, Z., Bo, Z., Jing, L., Yunxiang, Y., Jing, G. (2020).** A novel improved system based on CVSS. Lecture Notes in Electrical Engineering, Vol. 517, pp. 1015–1021. DOI: 10.1007/978-981-13-6508-9_123.
39. **Johnson, L., (2020).** Security controls evaluation, testing, and assessment handbook. Chapter 5, Risk Management Framework, (Second Edition), Academic Press, pp. 31–41. DOI: 10.1016/B978-0-12-818427-1.00005-7.
40. **Brunner, M., Wolfartsberger, J. (2020).** Virtual reality enriched business model canvas building blocks for enhancing customer retention. Procedia Manufacturing, Vol. 42, pp. 154–157. DOI: 10.1016/j.promfg.2020.02.062.
41. **Panda, S., Panaousis, E., Loukas, G., Laoudias, C. (2020).** Optimizing investments in cyber hygiene for protecting healthcare users. In: Di Pierro, A., Malacaria, P., Nagarajan, R. (eds) From Lambda Calculus to Cybersecurity Through Program Analysis, Lecture Notes in Computer Science, Vol. 12065, pp. 268–291. DOI: 10.1007/978-3-030-41103-9_11.
42. **Maennel K., Mäses, S., Maennel, O. (2018).** Cyber hygiene: The big picture. Lecture Notes in Computer Science, Vol. 11252, pp. 291–305. DOI: 10.1007/978-3-030-03638-6_18.
43. **Shrestha, M., Johansen, C., Noll, J., Roverso, D. (2020).** A Methodology for security classification applied to smart grid infrastructures. International Journal of Critical Infrastructure Protection, Vol. 28. DOI: 10.1016/j.ijcip.2020.100342.

Article received on 25/01/2021; accepted on 09/01/2023.
Corresponding author is Juan C. Olivares-Rojas.