IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received January 15, 2021, accepted January 25, 2021, date of publication February 2, 2021, date of current version February 11, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3056491

Proposal and Validation of a Standard Protection Profile for Homologation of Commercial Videoconferencing Equipment

ARIANE C. B. FLORENTINO[1], SANDERSON CÉSAR MACÊDO BARBALHO[1], AND RAPHAEL CARLOS SANTOS MACHADO[2]

[1]Post-Graduation Program in Mechatronic Systems, Department of Production Engineering, University of Brasilia, Brasilia 70910-900, Brazil
[2]Department of Information Systems, Federal Fluminense University, Niterói 24220-900, Brazil

Corresponding author: Sanderson César Macêdo Barbalho (sandersoncesar@unb.br)

ABSTRACT In the present work, we propose and validate a Common Criteria Standard Protection Profile (sPP) for videoconferencing equipment. The research presents the definition and analysis of the homologation system used to validate the standard protection profile, focusing on its application focused in a large Brazilian financial company. We address the main points to consider in the acquisition and current use of this product: reasonable information security assumptions, technical standards, recommendations, and international best cybersecurity practices. As a result, we have developed a Standard Protection Profile identifying the information security risks involved and the minimum parameters required in those systems acquired and used for Government environments. This paper also presents all tests performed to validate the proposed sPP. As the application is critical, involving sensitive data, our results can also foster less risky conditions in the myriad situations caused by the COVID pandemic.

INDEX TERMS Banking, common criteria, cyber defense, homologation, mechatronic product, security, videoconferencing.

I. INTRODUCTION

Information Technology (IT) is critical for most businesses and services these days [1]. As we depend on Information Technologies, it has become increasingly important to guarantee their security protection. Businesses and services use digital technologies based on assumptions of the availability of information and the integrity, reliability, and confidentiality of computer systems. Achieving an adequate security level involves a holistic approach that should address processes, people, and technologies. We address the technology element in the present work. Our focus is on guaranteeing that mechatronics systems for videoconferencing meet adequate security requirements. More precisely, we consider defining security requirements and assessing the satisfaction of those requirements by video conference products which are increasingly important in the current business environment constrained by the SARS-CoV-2 outbreak [74]. The Covid-19 pandemic has accelerated the digitalization of relationships, both personal and professional, since it has restricted people's face-to-face activities due to the lockdown, social distancing, and confinement imposed by the disease. More and more cases of invasions of virtual conferences, data theft, and the hijacking of public and private databases have occurred since the virus spread throughout the world. As a solution to mitigate information security risks in virtual meetings made possible by videoconferencing equipment, we propose a set of security requirements organized according to the so-called Common Criteria Standard. Common Criteria (CC) is a mature standard for the security of software products that have been developed since the beginning of the twenty-first century [50], [54], [56]. The Common Criteria Standard addresses a vital security attack vector, namely, the security threats and vulnerabilities embedded in software products [60], [65], [68].

Nowadays, much sensitive information transits via videoconferencing systems, both in private and public administration, including federal public administration (FPA). In the present work, we address the security aspects of such systems. We develop a Common Criteria Standard Protection Profile,

The associate editor coordinating the review of this manuscript and approving it for publication was Francesco Tedesco.

a complete, non-cloud-based solution for the homologation of in-house systems supplied for high-sensitivity applications, and have validated it by analyzing an entire video conference system applied in the largest Brazilian bank. Unlike cloud-based providers, these in-house solutions are mechatronic applications that use a set of cameras and hardware for gathering the whole context in a meeting room. A mechatronic background was the starting point for the present analysis, although we have focused on software-based features as basic functionalities for security analysis. We also delimit our work on cybersecurity's technological aspect based on the understanding that social and behavioral issues must be taken into account in a more general cybersecurity framework [75].

The second section of this article addresses the theoretical review. Cyber defense, mechatronics, and videoconferencing concepts are discussed. Section 3 presents the methodology used. The fourth section deals with the standard protection profile (sPP) and its test results. Section five offers our discussion, and the final section sets out the conclusions.

II. THEORETICAL BACKGROUND

Our theoretical review was based on the field of interest that motivated our research. First, we researched important aspects of Brazilian information security initiatives and searched the SCOPUS database looking for other countries' experiences. Second, we did another SCOPUS search combining the threads ''information security,'' ''cybersecurity,'' ''common criteria,'' and ''protection profile'' in pairs to identify articles related to our research interest. This literature analysis section also presents the research's theoretical framework, our critical views, and the decisions made for subsequent research development stages.

A. CYBERSECURITY IN BRAZIL

Cyber defense is closely related to information security (IS), and it deals with cyberspace's aspects in an offensive, defensive, or exploratory approach. For military planning, defense includes identifying harmful information, capturing intelligence data, and protecting information systems. Initially, this approach dealt with security in military applications, but it is now present in civil sectors [48] in which companies are establishing policies for employee data protection [66].

To develop protective measures and mitigate attacks in the cybernetic field, besides considering the risk posed to national sovereignty, in 2009, the Brazilian Army established a Strategic Defense of Cyber Security Policy that included several actions at the operational and strategic levels [2]. The creation of a Cyber Defense Command was one of those actions.

Among the essential elements of the Cyber Defense Command are the National School of Cyber Defense (ENaDCiber) and the Homologation and Certification System for Cyber Defense in Products and Services (SHCDCiber). ENaDCiber is responsible for training human resources and enabling and developing multidisciplinary scientific research focused on integrating corporate and academic civilians [2].

SHCDCiber is ''a Brazilian System of Metrology, Standardization and Industrial Quality for Security and Defense of Cyber-physical systems, directly linked to the Ministry of Defense, and indirectly to the National System of Metrology, Standardization and Industrial Quality - SINMETRO'' [4]. Other Latin American countries have also started to establish actions for cybersecurity [62], [64], [77].

The proposal presented in this paper is part of the Brazilian effort in that direction; a first attempt to build specific requirements for Brazilian critical infrastructures. As such infra-structure is increasingly cyber-physical [47], a mechatronic-based approach is vital for analyzing them [4], [69].

B. INFORMATION SECURITY AND THE COMMON CRITERIA STANDARD

Information Security (IS) is the set of devices for protection against the (accidental or intentional) misuse of information by people internal or external to the organization [9]. The most significant IS parameters are integrity, confidentiality, availability, authenticity, and non-repudiation. This research considered these aspects, which are the basis of the Information Security Policy (POSIC) of the Brazilian FPA entity considered here, which is aligned with the supplementary regulations IN 01, 02, and 03 of the Institutional Security Office - Department of Information and Communications Security, of the Presidency of the Republic of Brazil [42], [43], [79], [80], [81]. Several studies have been carried out to develop and test methodologies for evaluating information systems, particularly those concerning security.

Silva [10] proposed a system for evaluating security in equivalent information systems (cloud and in-house e-mail services) using a multi-criteria methodology to support MACBETH (Measuring Attractiveness by Categorical Based Evolution Technique) decision making. The method used discarded acceptable practices and norms such as COBIT, ISO, and others. That author considered the effort required to apply these control standards and found them to be overly generic and that they failed to consider organizations' specificities. The evaluation criteria proposed by [10] were based on a review of the scientific literature and existing acceptable practices and validation through interviews with those responsible for Security in Portuguese organizations (clients, suppliers, and security specialists). The evaluation object was the e-mail service, and Microsoft Office 365 presented itself as the e-mail service in the cloud.

Ohtoshi [11] has made a comparative analysis of several international standards and acceptable practices in information systems security, describing the main tools and methodologies of analysis and product risk management. The author concludes by demonstrating the trend to convergence and integration among the methods.

Martins and Santos [12] also used the central norms and security standards to create guidelines. From that point on, they presented a proposal for a methodology to

implement an information security management system (ISMS) to guarantee a networked computing environment. Since then, this kind of application has been discussed [54] for single and mixed networks. The methodology used in [12] was a case study in an environmental protection company (predominantly private capital). As a result, the ISMS was implemented in the company, considering the particularities of its business. Ferreira and Shinoda [61] evaluated an Intrusion Detection System (IDS) in a typical wi-fi network. Mukhanov *et al.* [59] consider the possible use of PP for avoiding new classes of network attacks on SDN switches and controllers, which can involve data and control components because of the isolation of the controller from the circulation of messages in the control plane. Deb and Roy [67] report the use of the Common Vulnerability Scoring System (CVSS) to identify component vulnerability to SDN components.

Reinhard and Jung [55] present a protection profile for the remote electronic voting system POLYAS in Germany and its validation. The proposed PP presents a list of mandatory security objectives that are essential requirements for small electronic voting systems and assumptions about the environment in which the voting system needs to be used. According to the Korean Data Privacy Act, Lee *et al.* [58] derive the security functions of a privacy protection system based on the Common Criteria. Companies face threats of personal data leakage from employees using a personal computer, so it is not only an individual privacy problem. The whole PP is presented, but no tests of existing systems using it are presented.

D'ornellas and Kroll [13] analyzed the process of risk assessment focused on the strategic management of information security in general. They verified that there are different methodologies to evaluate the risks, highlighting the TAG's Risk Assessment Process, OCTAVE - Operationally Critical Threat, Asset, Vulnerability Evaluation, and AS/NZS 4360: 2004. As a result of that evaluation information, security management in the respective corporation was optimized.

Fontoura, Konzen, and Nunes [14] used ISO/IEC 27005 as a basis for associating security standards to facilitate the preparation of the standard process and provide a greater guarantee of the use of recommended market practices. Santos and Filho [15] used ABNT NBR ISO / IEC 27001: 2006 and 27002: 2005 standards, in addition to 27005: 2008, to verify the adherence of an information security management system (ISMS) to the criteria defined in those regulations.

Amaral *et al.* [16] proposed a risk assessment methodology based on Six Sigma, consolidating a non-validated information security policy in a hospital institution. Eloff and Solms [17] offered a combination of certification and computer systems evaluation, considering security aspects based on BS7799. At the same time, Trček [18] presented a proposal for a multidisciplinary framework for managing security in information systems, integrating human interactions, man-machine interfaces, physical security, organizational aspects, and legislation.

Trček [18] and Akalp *et al.* [19] used statistical analysis to assess IS management systems' security threats and risks. While the first work only presents the framework but does not validate it, the second uses a case study in small and medium-sized Turkish companies to validate the proposal. Catota *et al.* [77] propose using Computer Security Incident Response Teams (CSIRT) and information sharing to improve the Ecuadorian financial sector's cybersecurity capabilities.

Farn *et al.* [20] present a case study and suggest a five-level certification of a ''Communication and Information Security Protection System'' aligned with government regulation covering existing office policies in Taiwan.

The comparative analysis of some management security standards for information systems was studied by Sipponen and Willison [21], adopting them to validate the market's acceptable practices. At the same time, Tashi and Outi-Hélie [22] sought to analyze the evaluation metrics for security standards following ISO 17799: 2005 and ISO 27001 standards.

The work of Broderick [23] and Kadobayashi and Takahashi [24] both present the use of international security standards and best practices to propose an IS system. The former author used the alignment to specific Control Objectives for Information and related Technology-COBIT to analyze ISMS security standards and regulations. In turn, the latter work proposes a reference ontology focused on operational cybersecurity information. Disso *et al.* [25] also studied cybersecurity, specifically cybersecurity management analysis, in industrial control systems. Martins and Oliveira [70] analyze the new industrial scenario for industry 4.0 applications where even power electronic systems are demanded to exchange sensing and control data, thus presenting cyber vulnerabilities. Fabrício *et al.* [71] propose an IoT system for automatizing production lines in automotive companies. Bouk *et al.* [72] study cyberattacks and security challenges faced by the vehicular cyber-physical systems (VCPS) using European and North American standards and frameworks for security in industrial control systems, unlike Kadobayashi and Takahashi [24], who used guidance from the US, Japanese, and South Korean security operations centers.

Dlamini *et al.* [26] review the literature on information security by researching the main threats, issues addressed, and research trends in this field. Sharp [56] presents CC appliance examples for secure application systems, such as a Point-of-Sale (POS) system, a wind turbine park monitoring and control system, and a secure workflow system. All these systems were specified to achieve CC assurance level EAL3. The research goal was to evaluate how exactly the CC can be applied to support the design tasks. Despite that, the author does not present validation data for the specified CC classes. Löhr *et al.* [57] present a protection profile for highly guaranteed security kernels for trusted computing features such as trusted boot, sealing, and trusted channels reaching an EAL5 level according to the German Federal Office for Information Security (BSI).

Bartsch [49] proposed a protection profile for the Gateway of a Smart Metering System. Sikora [51] discusses a whole architecture for a protection profile EAL-4 and a technical directive (TR) for the communication unit of an intelligent measurement system in Germany. Stegelmann and Kesdogan [52] study privacy in a smart measuring system and suggest a k-anonymity service that reduces the trust needed in service providers in a scalable and secure way. Thiel *et al.* [53] proposed a Measuring Instruments Directive (MID) for the already developed Protection Profile for Smart Meter Gateways, also part of the German effort for making smart grids feasible. Machado *et al.* [63] proposed a methodology for cybersecurity maturity levels in smart grids, taking into account assets, threats, and impacts in a SCADA (Supervisory Control and Data Acquisition) System. Fernández and Rodriguez [64] analyzed the Chilean requirements for a national smart grid system.

In the field of evaluation and certification of IT equipment, the work closest to the research carried out here was the proposed methodology for desktop computer certification presented by Coelho and Silva [27]. Using its ontology and according to international standards and fair marketplace, those authors used a laboratory for simulating real conditions of security threats in desktop utilization for validation steps.

The research efforts of Hou and Yu [28] and Fernandez-Saavedra *et al.* [29] are also close to the work carried out here since they used Common Criteria to evaluate information systems security. Hou and You [28] evaluated the use of Radio Frequency Identification (RFID) technology in a medical-hospital environment. Simultaneously, [29] assessed a biometric system, and both used literature review and best market practices for gathering the assessment criteria.

A current research effort has set out to improve security research utilizing blockchain technology [73], commonly present in cryptocurrencies, smart contracts, and data security. Blockchain technology can change the whole security strategy and architecture, but it is not yet considered a sufficiently consolidated research field for discussing information security.

C. SUMMARY AND DECISION ABOUT INFORMATION SECURITY STANDARDS

The discussion about information security in scientific literature shows a search for the foundation of cybersecurity systems and an effort to develop tools and methodologies for product homologation [12], [13], [14], [18], [21]–[24], [77]. Moreover, national systems and private companies have invested in such an effort as they could and should be expected to do [19], [66], [61]. A similar effort is in course in the Brazilian Government, as already mentioned [2], [4].

There are several internationally accepted approaches to evaluating and certification of IT products and systems, each with its evaluation criteria. The following can be highlighted: TCSEC – Trusted Computer System Evaluation Criteria (Orange book): an approach specifically focused on software. It has seven rating levels (A1, B3, B2, B1, C2, C1 or D); ITSEC - Information Technology Security Evaluation Criteria (E0, E1, E2, E3, E4, E5, and E6 levels); CC - Common Criteria (Evaluation Assurance Levels - EAL - from EAL1, the lowest level, to EAL7, the highest level).

Among the internationally accepted approaches to evaluation and certification of IT products and systems, the CC was chosen for this research due to the following characteristics [30]:

- It considers other aspects of security in the protection of assets (e.g., risk of human activities) beyond confidentiality, integrity, and availability;
- It can be used as a guide for the development, evaluation, and acquisition of IT products that have security features;
- The evaluation process determines a level of confidence reached for security features, helping consumers to define whether IT products meet their security needs;
- It is a generic framework with sufficient flexibility for evaluating security requirements. That is, it can be used in several IT products;
- It enables comparison of independent security assessment results as it presents standard requirements related to the security aspect of IT products (hardware, software, or firmware).

As presented in our literature analysis, CC has also been widely used for information security in companies and academia [27]–[29], [49], [51], [53], [35], [56]–[58]. Institutions in the United States and Europe [36] already consider this critical assessment of security requirements in their products, especially in systems regarded as essential infrastructure (e. g. data communication links in aviation systems, satellite communication).

An example of this is the case study of FAA Telecom [37] in the USA. In this study, the Federal Aviation Administration Telecommunications Infrastructure (FTI/FAA) project provides an example of a service contract that uses the CC. FTI delivers integrated voice, data, and video telecommunications services in the United States, with connectivity to Hawaii and Alaska's territories. FTI requirements are expressed in terms of service classes and service interfaces. In this specific case, the supplier is required to demonstrate the EAL3 level [38].

Another example of actions in this direction is seen in the PP of [45], accredited by the National Information Assurance Partnership (NIAP). Through a public-private partnership, IT products are evaluated under Common Criteria. In this way, the products are validated against the security requirements required by the US national security system (following National Security Agency – NSA), in addition to being able to be used by the remaining 30 countries participating in the Common Criteria Recognition Arrangement (CCRA), among them Australia, Canada, and Germany.

III. MATERIALS AND METHODS

The present work proposes using the Common Criteria (CC) framework to identify information security risks and the

minimum parameters required in video conferencing equipment to mitigate them, taking into account the manufacture, acquisition, and use of the equipment. We validate the proposed model by applying it to equipment that is in use in a financial company.

This work began with quantitative bibliographical research focused on cybersecurity for critical systems and information security, as already mentioned. A second step was a documentary analysis of norms related to cyber defense and information security for Federal Public Administration in Brazil and recommendations of the best practices in the area. The bibliographic research also enabled the evaluation of case studies and accompaniment of state of the art on the same theme as this work, worldwide.

We also searched for the Brazilian Government's public procurement records [31], which refer to the technical characteristics and market standards commonly used in videoconferencing equipment. Moreover, the equipment datasheet [8] and guidelines for the use of unified communications products [32]–[35] were also analyzed, in addition to the Brazilian FPA entity's POSIC.

Afterward, we analyzed the videoconference product with a mechatronic system background [7] to consider the required TOE (Target of Evaluation). We paid particular attention to cyber defense principles. At that stage, the security requirements, which were part of the sPP, were identified. The TOE considered in this search is the same for the default protection profile (sPP), for the base protection profile (BPP), and the protection profile module (PPM), according to the definitions set out in [30].

Then followed the study and application of the Common Criteria standard to prepare the proposal for videoconferencing equipment approval and certification. To that end, the following materials were used: a) Videoconferencing equipment model TE 30, from the manufacturer Huawei, in firmware version TEX0 V500R002C00SPCb00 Release 2.0.b00 Mar. 6, 2017; b) Cisco Jabber UC version 11.11 application – an application used as personal communicator installed on a desktop computer with the Windows 7 Professional 64-bit operating system, 3.00 GHz i5 processor and 4.00 Gb RAM; and c) a LAN, providing Internet access to the desktop computer and TOE.

The observations of the events were subjected to the Chi-squared test (x^2) to verify the hypotheses and possible correlations among them. We chose that test because it involved nominal variables with five independent samples [39].

The events observed in this work satisfy the following requirements for the Chi-squared test: events are independent, presenting randomly selected items; observations are frequencies or counts and belong to only one category of the event; the sample of observations is relatively large, with few groups and at least five observations for each event [25].

The formula used in the calculation of the tests, proposed by Karl Pearson, was:

$$x^2 = \sum [(o - e)^2/e] \tag{1}$$

where:

o = the observed frequency for each class

e = the expected frequency for that class

Since (o-e) = deviation (d), the formula can also be written as $x^2 = \sum (d^2/e)$. It is important to note that the deviation is the difference between the frequencies observed and expected in a class. When these frequencies are very close, the value of x^2 is small. Likewise, when the difference is large, the deviation d is too, making x^2 assume high values.

The following hypotheses were tested [39]:

- Null hypothesis (H_0): the observed frequencies are not different from those expected; that is, there is no difference between the frequencies (counts) of the groups. Therefore, there is no relationship between the groups studied.
- Alternative hypothesis (H_a): The observed frequencies are different from those expected, so there is a difference between the frequencies. That is, there is an association between the groups.

We use two statistics: calculated x^2, the expected frequency (e) and tabulated x^2, the observed frequency (o). The hypotheses are decided by comparing the values of calculated x^2 and tabulated x^2:

- If calculated $x^2 \geq$ tabulated x^2: Reject H_0;
- If calculated x^2 is $<$ tabulated x^2: H_0 is accepted.

In a controlled environment, a data network was set up, simulating the TOE operating environment. The videoconferencing equipment was configured according to the POSIC used in a specific FPA financial organization. The next step was to simulate the terminal conditions by making and receiving videoconference calls to verify whether the TOE met the sPP's related security requirements. The parameters considered in the security requirements were treated as variables. We carried out tests of the requirements to validate the sPP developed, verifying that the auditable events related to the Standard Protection Profile developed were present in the TOE. In this work, references to the protection profile (PP), are understood to be references to the standard protection profile (sPP). The sPP can readily be considered a Base Protection Profile (BPP) and serve as the basis for the corresponding Protection Profile Module (PPM).

IV. DEVELOPMENT

According to [5], mechatronic products combine mechanics with electronics and information technology to compose a functional interaction and a spatial integration of components, modules, products and systems. Cyber-physical Systems (CPS), as conceptualized by the National Institute of Standards and Technology (NIST) [47], seem like

mechatronic products for purposes of functional and spatial analysis.

In comparison with a non-mechatronic product that requires a similar level of effort in its development, it has the following characteristics in cyber-physical systems: greater efficiency, accuracy, reliability, flexibility, functionality, safety, and "environmental friendliness", being low cost and less mechanically complicated [6].

The concept of CPS combines physical and cybernetic space. It can be adapted to several applications, extrapolating specific domains (for example, smart cities and energy systems) that imply essential considerations in their projects. CPS in networks can incorporate third-party infrastructure devices involving trust issues (certificates, registration, access, etc.). CPS is designed to interact with the physical world in which aspects such as reliability, resilience, information security, privacy, and confidentiality are critical. They also bring together functional, business, human, trustworthiness, timing, data, boundaries, composability, and lifecycle elements [47]. Resilience is a particularly highlighted issue in the current literature [72], [78], especially in the financial sector [78].

Considering mechatronics as a coordinated architecture of electronics and mechanics, we have the power to explain several products [7], including videoconferencing equipment. This kind of equipment is a mechatronic product typology that is quite critical in information security despite not having a high degree of automation. It is composed of: a codec element (decoder of voice and audio); microphone(s); monitor(s)/television(s); video camera(s) and documents camera (optional), as shown in Fig. 1. The study analyzed a Huawei TE30 solution.

It is essential to highlight that the web-based or cloud-based distance meeting solutions - such as Zoom, Microsoft Teams, Skype, and Google Meet - have become increasingly common. Despite this, they cannot be considered when we need to meet high-security standards. In such models, there is a third-party providing infrastructure that includes communication channels and services. We claim that to achieve increased security standards, one must have recourse to videoconferencing models that use specific communication protocols and require dedicated equipment for its participants. In this solution, using such increased security videoconferencing models, the client companies control all the necessary infrastructure, with exclusive servers to manage the data flow and even dedicated communication channels, increasing the security level in the information traffic end-to-end. There is also a type of teleconference where participants interact only through audio and transmission via streaming (u broadcast), in which communication occurs by diffusion from conference servers. In this work, the videoconferencing equipment analysis was chosen over the other technological solutions, considering that this is the technological solution used by the respective Brazilian financial institution, in addition to the possibility of the certification of the hardware involved.

FIGURE 1. Typical video conferencing equipment - Huawei TE30 [8].

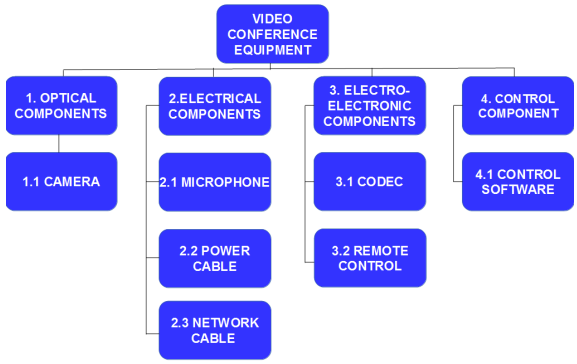


FIGURE 2. Product Structure of Videoconferencing Equipment.

A. EQUIPMENT ANALYSIS

After the quantitative bibliographical research, we started the documentary analysis and concurrently studied the videoconference equipment in a mechatronic systems perspective (according to Fig. 2).

Structurally, the equipment is divided among optical, electrical, electronics, and control components. The camera is the optical component. Network and power cables, in addition to the microphone, are considered electrical components. The electronic components bring together the codec (encoder/decoder) and the remote control, while the control software is the control component (Fig. 2).

Functionally (Fig. 3), the mechatronic product has two central systems: the power supply and the control system. The dashed line represents the energy flow between the components and the systems. The continuous lines represent the equipment's essential operation, connecting the microphones and the camera directly with the power and network cables. The control software is guided by the remote control and directs the microphone, codec, and camera; the codec processes video and audio signals received from the camera and the microphone and sends them to the monitor.

Fig. 4 represents the installation scheme for videoconferencing equipment in an operational environment. Our case's evaluation target includes the control hardware and software, as discussed in the functional structure represented in Fig. 3. The Registration Server and the administration console need to be present in the same IT environment in which the TOE operates.

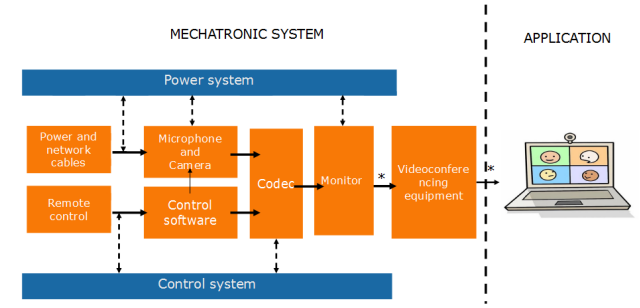


FIGURE 3. Functional Structure of the Videoconferencing Equipment. Adapted from Barbalho (2016).

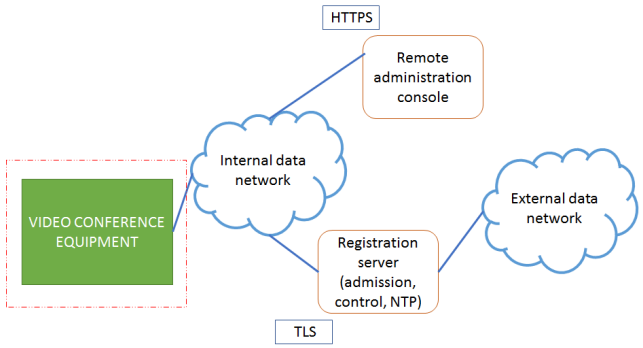


FIGURE 4. Videoconferencing equipment installation.

The TOE is connected through the internal (reliable) data network via TLS to a registry server that acts in several ways: (1) performing the admission and control of the equipment; (2) allowing its administration and registration to enable the videoconference connections through the specification of the SIP or H.323 ports (according to the protocol used); (3) other properties, such as identification and bandwidth to be used, and the NTP server controls configurations for time and date.

As the TOE is a device connected to the telecommunication network, its operating environment is also considered the security environment in which it is inserted and must meet a minimum amount of security requirements, according to the organization's information security policy (POSIC).

In that way, the TOE will be exposed to the same threats and security features as the data network and any other network device, as the following paragraphs explain.

B. THREATS, REQUIREMENTS, AND PROTECTION PROFILE ACCORDING TO CC STANDARD

Threats and assumptions were addressed in this research, insofar as they relate to the TOE, directly or indirectly, referring to the physical and logical environments that constrain TOE utilization. That is a good market practice adopted by security administrators, also recommended by standards NBR 27001: 2006 [33], NBR 27002: 2005 [40], NBR 27005: 2008 [41], IN 01, 02 and 03 [79]–[81], Complementary Norms 07 [42] and 17 [43], from the Office of Institutional Security of the Presidency of the Republic (GSIPR), and finally in international standards such as the Common Criteria.

The threats considered in this research relate to external threats and unauthorized attempts to access and modify data and other critical network traffic, such as bank transaction data and personal information. The sensitivity of the information exchanged through the videoconference equipment depends on the evaluation of each institution. In the specific case of the Brazilian FPA entity, the POSIC of the institution in question, in line with its mission and strategic planning, also considers information and network incident treatments, risk and continuity management, audit and compliance, and access controls.

We organized the security threats to be considered for videoconference equipment according to the CC families [30], as follow:

1) FAU – Family Security Audit – Security audit/traceability (T.UNDETECTED_ACTIVITY);

2) FCS – Family Cryptographic Support – Failed Cryptography (T.WEAK_CRYPTOGRAPHY);

3) FIA/ FTA – Family Identification and Authentication/ Family TOE Access - Undue access (physical/logical) (T. UNAUTHORIZED_ADMINISTRATOR_ACCESS/ T. PASSWORD_CRACKING);

4) FPT – Family Protection of the TSF (TOE Security Functionality) – Security functionality of TOE (T.SECURITY_FUNCTIONALITY_FAILURE);

5) FTP – Family Trusted Path/Channels (T.UNTRUSTED_COMMUNICATION_CHANNELS).

The following assumptions relate to the security requirements used in the development of the TOE and the essential conditions of the environment in which it must be used [30]. These are supported as best practices in most network device sPPs, besides being security requirements considered in the POSIC of the Brazilian FPA entity in question:

- physical protection (OE.PHYSICAL);
- data traffic protection (OE.NO_THRU_TRAFFIC_PROTECTION);
- administrator access through secure credentials (OE.TRUSTED_ADMIN/OE.ADMIN_CREDENTIALS_SECURE);
- firmware updates regarding network elements (OE.UPDATES).

Considering that the equipment embeds critical data and the necessities of users from Federal Public Administration, the following security features were included in the sPP in alignment with [31], [46]:

- encryption support;
- identification and authentication;
- security audit;
- protection of TOE security settings;
- access control;
- use of reliable channels.

Taking into account the respective threats and the evaluation of the principal researcher of this work, who worked

directly as an information security analyst at the Brazilian FPA entity, the specified security requirements were: the ability to have auditable/traceable activities; active cryptography; authentication and registration in gatekeeper; support for protocols H.460.18 and H.460.19; authentication and identification of users; protection against improper access. These requirements are listed in Table 1 with an appropriate description.

TABLE 1. Security requirements of TOE [31], [32], [34].

Component	Required	Use / Description of proposal for the TOE
Authentication and registration in gatekeeper	Yes	The IT environment where the TOE is inserted must provide it with its registration and authentication in the H.323 and SIP protocols simultaneously.
Support for protocols H.460.18 and H.460.19	Yes	The IT environment where the TOE is inserted must provide support for the H.460.18 and H.460.19 protocols, allowing the transparent crossing of firewalls in the communications established by the TOE.
Ability to have audited / traceable activities	Yes	The TOE must allow logging with its activities, enabling traceability and security auditing.
Active cryptography	Yes	The TOE must have active encryption in its communications, mitigating the risk that unauthorized parties will intercept its audio and video traffic.
Authentication and identification of users	Yes	The TOE must have management users with different access levels, authenticating and identifying all administrative console access.
Protection against improper access	Yes	The TOE must protect against improper access (physical and logical). Physical access refers to its safekeeping and use in a room kept safe from unauthorized users. Logical access, however, refers to the use of users and credentials to access the administrative console.

Based on the requirements, threats, assumptions, and information security policies described above, an sPP was defined according to the Common Criteria framework [30].

The security requirements (listed in Tables 1 and 2) in the sPP developed here were listed in the GSI/PR market best practices and supplementary Brazilian government standards. They are present in the Brazilian FPA entity's POSIC and in international security standards. Such requirements are often used in the acquisition and use of videoconferencing equipment for FPA.

Table 2 lists the developed sPP's 25 functional requirements, the proposed auditable events related to each one, and the expected information for event registration. Such requirements were also listed considering the experience of one of the researchers who worked as an information security analyst directly with this kind of equipment in the Brazilian FPA entity studied.

Some of the auditable events can be classified into three audit levels, as desired by the environmental security administrator: minimum, basic, or detailed. Other events still require the date and time when they occurred. Such information is treated as additional to their record, according to statements in column three of Table 2.

V. TESTING AND DISCUSSION

A. TEST SETUP

For sPP validation, the following events cover the 25 requirements considered and were reproduced in the TOE to verify its adherence to the developed sPP. Five simulations for each one of the identified events were carried out:

1) turning on, off, and restarting the TOE;

2) starting, holding, and ending video conferencing calls;

3) Administrative console login and logout (individually, if the system allows an individual login);

4) changing security settings (enabling/disabling encryption, enabling/disabling the H460 protocol), keeping a record of the user who made the change and the changed values;

5) resetting/changing administrative login passwords (individually, if the system allows an individual login).

All these events were tested according to the logic scheme depicted in Fig. 5.

After the events had been reproduced, logs were collected in the TOE to verify whether the equipment contained the sPP requirements stated in Table 2. The logs were recorded in XML (eXtensible Markup Language) format, as shown in fig. 6.

As shown in Fig. 7, it is possible to query the logs in the log file by informing the desired period, the level, and the category of the audited event.

The TOE was structurally tested, according to EAL 3, involving analysis of its documentation in addition to the methodologically performed functional tests. Thus, a moderate level of security assurance was thoroughly investigated in the TOE, considering several security assumptions of the TOE environment, according to the POSIC of the Brazilian FPA entity, dispensing significant reengineering of the evaluated object.

B. TEST RESULTS

All events proposed were performed 30 times, according to Table 3. As can be seen, no event had non-occurrence cases, which means that all requested actions performed as expected.

The results found that the TOE met most of the requirements: of the 25 requirements established (Table 2), only eight were not fully satisfied. That is, the sPP had 68% approval in its parameters. The overall results are presented in Table 4. The next paragraphs explain the requirements not met or partially complied with in our sPP.

The FAU_GEN.1.1 and FAU_GEN.1.2 requirements were met partially, while the FAU_GEN.2 parameter was not fully met since there were no individual users to log into the TOE console and make changes to their configuration. There is only the administrative user, which is unique. In real

TABLE 2. Standard Protection Profile developed: Functional requirements and auditable events. Based on [30].

Security requirement		Auditable Event	Expected information for event registration
Family Security Audit Data Generation – FAU_GEN	**1.1. FAU_GEN.1.1**	TOE connection, shutdown, and restart	Required audit level (minimum/ basic/ detailed)
		Call start, hold and end	Required audit level (minimum/ basic/ detailed)
		Administrative console login and logout	Required audit level (minimum/ basic/ detailed)
		Security settings change	Required audit level (minimum/ basic/ detailed)
		Administrative login password reset/change	Required audit level: (minimum/ basic/ detailed)
	1.2. FAU_GEN.1.2	TOE connection, shutdown, and restart	Date, time, type of event, and outcome (success or failure)
		Call start, hold and end	Date, time, type of event, and outcome (success or failure)
		Administrative console login and logout	Date, time, type of event, and outcome (success or failure)
		Security settings change	Date, time, type of event, and outcome (success or failure)
		Administrative login password reset/change	Date, time, type of event, and outcome (success or failure)
	1.3. FAU_GEN.2	TOE connection, shutdown, and restart	Individual user responsible for the event
		Call start, hold and end	Individual user responsible for the event
		Administrative console login and logout	Individual user responsible for the event
		Security settings change	Individual user responsible for the event
		Administrative login password reset/change	Individual user responsible for the event
Family Cryptographic Support_ Cryptographic Operation – FCS_COP	**1.4.FCS_COP.1**	Communica-tions Encryption activation	Success / failure; cryptographic operation mode
Family Identification and Authentication - Authentication Failures - FIA_AFL	**1.5.FIA_AFL.1**	Administrative console login and logout	Number of unsuccessful login attempts; actions to be taken

TABLE 2. *(Contiuned.)* Standard Protection Profile developed: Functional requirements and auditable events. Based on [30].

Family Identification and Authentication - Family User Attribute Definition - FIA_ATD	**1.6.FIA_ATD.1**	Administrative console login and logout	List of security attributes for each user type
Family Identification and Authentication - Family Specification of Secrets – FIA_SOS	**1.7.FIA_SOS.1**	Administrative login password reset/change	TSF rejection of any tested password (minimum); rejection or acceptance of any tested password (basic); identification of changes to quality metrics adopted (detailed)
	1.8.FIA_SOS.2		
Family Identification and Authentication - Family User Authentication – FIA_UAU	**1.9.FIA_UAU.1**	Administrative console login and logout	Failure to use the authentication mechanism (minimum); use of the authentication mechanism (basic); actions performed by the TSF before user authentication
	1.10. FIA_UAU.2	Security settings change	Failure to use the authentication mechanism (minimum); use of the authentication mechanism (basic)
	1.11. FIA_UAU.3	Administrative console login and logout	TSF detection of authentication data forged by any TSF user, and prevention of or authentication data copied from another TSF user
	1.12. FIA_UAU.4	Administrative console login and logout	The TSF must prevent the reuse of authentication data related to the authentication mechanism used in it
	1.13. FIA_UAU.5	Security settings change	Failure to use the authentication mechanism (minimum); use of the authentication mechanism (basic)
		Video-conferencing calls, start, hold and end	Final result of authentication in the gatekeeper, with date and time (minimum); development of each activated mechanism - call attempt / on-call/call termination (basic)
	1.14. FIA_UAU.6	Security settings change	Reauthentication failure (minimum); all attempts at reauthentication (basic)
	1.15. FIA_UAU.7	Administrative console login and logout	The TSF must provide message feedback to the user while the authentication is in progress.
Family TOE Access - Family Limitation on Multiple Concurrent Sessions – FTA_MCS	**1.16. FTA_MCS.1**	Administrative console login and logout	The TSF must restrict the maximum number of concurrent sessions that belong to the same user. It shall enforce, by default, a limit to sessions per user.

TABLE 2. *(Continued.)* **Standard Protection Profile developed: Functional requirements and auditable events. Based on [30].**

Family TOE Access - Family Limitation on Multiple Concurrent Sessions – FTA_MCS	**1.16. FTA_MCS.1**	Administrative console login and logout	The TSF must restrict the maximum number of concurrent sessions that belong to the same user. It shall enforce, by default, a limit to sessions per user.
	1.17.FTA_MCS.2	Administrative console login and logout	Rejection of a new session due to the limitation of multiple concurrent sessions (minimum); capture of the number of simultaneous user sessions (basic)
Family TOE Access - Family Session Locking and Termination – FTA_SSL	**1.18.FTA_SSL.1**	Administrative console login and logout	The TSF shall lock an interactive session after a certain time interval of user inactivity, and it shall require, before unlocking the session, a new login from the administrative console
	1.19.FTA_SSL.2	Administrative console login and logout	Locking of the session by the respective user after a new login
	1.20.FTA_SSL.3	Administrative console login and logout	Ending of the session by the locking mechanism after a certain time interval of user inactivity
	1.21. FTA_SSL.4	Administrative console login and logout	Ending of user session by the respective user
Family Protection of the TSF - TOE Security Functionality/ Family Fail Secure – FPT_FLS	**1.22. FPT_FLS.1**	TOE connection, shutdown, and restart	Failure occurrence
		Video-conferencing calls start, hold, and end	
Family Protection of the TSF - TOE Security Functionality/ Family Testing of External Entities – FPT_TEE	**1.23. FPT_TEE.1**	Security settings change	The TSF must test the connection with the NTP server and with the gatekeeper whenever there are alterations to the equipment's security configurations
	1.24. FPT_TEE.2	Video-conferencing calls start, hold, and end	Information on the gatekeeper and the NTP server if test failed, the equipment must return the message and seek a connection with the secondary servers
Family Trusted Path/Channels – Trusted Path - FTP_TRP	**1.25. FTP_TRP.1**	Video-conferencing calls start, hold and end	H.460 protocol enablement

TABLE 3. **Events SEARCH and occurrences.**

	Occurrence	Non-occurrence
Turning on, off, and restarting the TOE	30	0
Starting, holding, and ending video conferencing calls	30	0
Administrative console login and logout	30	0
Changing security settings	30	0
Resetting / changing administrative login passwords	30	0

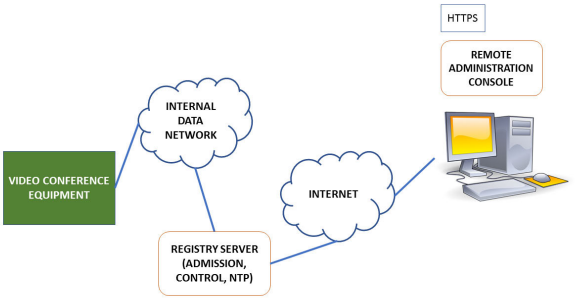


FIGURE 5. **The logical schema for analyzing the system.**

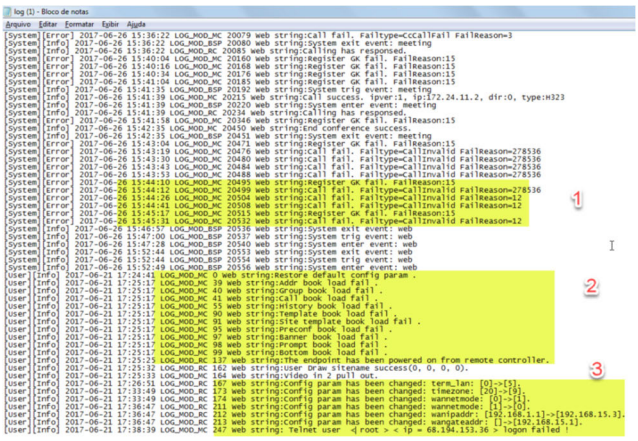


FIGURE 6. **XML file query: server registration failed (highlighted in 1); reset and change security settings (highlighted in 2 and 3).**

situations, it must be done by individual users, enabling traceability in audits. Besides, not all events have three levels of the criticality of recording information. The audit levels exhibited are information, error, critical. It is not possible to change these levels as the TOE does not allow it. It is only possible to consult them, as determined by the manufacturer.

The FIA_AFL.1 parameter was not fully met since logging in, and out does not show the information on the number of unsuccessful login attempts or the basic actions to be taken in these cases.

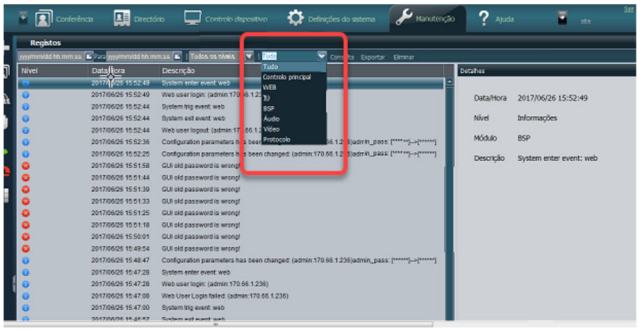


FIGURE 7. Querying Records in MAINTENANCE > RECORDS.

Note: o11 = observed of class 1; e11 = expected of class 1...										
										Totals
o11 =	30	o12 =	30	o13 =	30	o14 =	30	o15 =	30	150
o21 =	0	o22 =	0	o23 =	0	o24 =	0	o25 =	0	0
Totals	30		30		30		30		30	150
Calculation of expected										
e11 =	30	e12 =	30	e13 =	30	e14 =	30	e15 =	30	
e21 =	0	e22 =	0	e23 =	0	e24 =	0	e25 =	0	
Calculation of partial chi with correction										
(|o11-e11|-0,5)²	0,0083	(|o12-e12|-0,5)²	0,0083	(|o13-e13|-0,5)²	0,0083	(|o14-e14|-0,5)²	0,0083	(|o15-e15|-0,5)²	0,0083	
(|o21-e21|-0,5)²	0,0000	(|o22-e22|-0,5)²	0,0000	(|o23-e23|-0,5)²	0,0000	(|o24-e24|-0,5)²	0,0000	(|o25-e25|-0,5)²	0,0000	
Chi square value =			0,0417							

FIGURE 8. Chi-squared test with Yates correction.

The FIA_ATD.1 requirement was not met because there is no definition of access levels for users. The FIA_SOS.1 and FIA_SOS.2 conditions were not met because when resetting/changing administrative login passwords, no quality metric was adopted for password registration.

The FIA_UAU.2 parameters were not met because, when changing the security settings, only the login password change option required new user credentials.

C. STATISTICAL ANALYSIS

The five events surveyed are arranged in Table 3, while the observations made are placed in the columns. Each event was observed thirty times, enabling the creation of a historical series, according to the recommended experiment planning techniques [44] previously explained in section 3.

The more analyses performed on the data set, the higher the likelihood of the results having a high significance index. Thus, thirty (30) observations were collected from each of the 5 (five) events, forming a sample of 150 (one hundred and fifty) elements.

To verify whether there is a relation between the observed events, we used the Chi-squared statistical test, in contingency tables, with Yates correction, according to the calculations displayed in Fig. 8.

After the correction had been applied, $x^2 = 0.0417$ that is, x^2 continued smaller than x_c^2(which was 9.488 in the Chi-squared table, considering 4 degrees of freedom and a confidence interval of 90%), confirming the acceptance of the H_0 hypothesis. The deviations are due to a random chance, and there are no associations between the events.

So, at the end of the verification of the TOE adherence to the developed PP, it was statistically verified through the Chi-squared test that there are no correlations among the security requirements. As no association was identified among the results of each security requirement, their specific tests were independent, and the proposed PP was validated.

D. DISCUSSION

The following security principles in information and communications systems have been met in this TOE assessment: integrity, availability, authenticity, and non-repudiation. Confidentiality can be affected since the requirements not met in the TOE are directly related to the identification, authorization, and authentication of the users.

The results of applying the proposed model to a real case validate the protection profile developed, using POSIC-based security parameters of an FPA entity, as explained in this article's previous items. The obtained results were genuine and authentic.

The profile elaborated in this work is related to the VoIP PP [45] as the TOE considered in the present study presents the technology solution's functionalities. According to the CC, the Evaluation Assurance Level (EAL) of this profile is regarded as three since the evaluation meets the security requirements contemplated in this package. It would be essential to raise this level from EAL4 to EAL7 since more parameters and security requirements would be tested. For increasing the PP to EAL4, it would be necessary to analyze the TOE design. For this research, studying TOE design was not required because we wished to produce relevant analysis for the companies' user side. However, to advance this type of project, it would be possible to gather data from design issues and move to CC EAL 4.

The standard Protection Profile (standard PP) developed in this work is an implementation-independent statement [30] of a specific group of users' security needs for the TOE in question. It can be used for the preparation of the corresponding Protection Profile Configuration (PPC), unfolding it in Base Protection Profile (BPP) and Protection Profile Module (PPM).

It is impossible to eliminate bank phishing attacks, malware, personal data theft, infection of connected devices, leakage of personal and corporate information, or ransomware in Information Security. We need to mitigate it. The primary attacks are mitigated by taking into account IT solutions' compliance with the information security requirements contained in the institutions' POSIC, which is periodically evaluated, reviewed, and updated in Brazilian FPA. Once the simple verification of security requirements does not guarantee the security of information in the virtual product or service, in our case, videoconferencing meetings, a procedure such as the proposal we have made must be periodically run to test the cybersecurity of the company. An EAL 3 can be achieved by our practice. IT technicians must understand each security instruction's role and how the proposed test toolkit described here is related to mitigating cyber risks. A training procedure is demanded and is the next step of this research effort to investigate the possibility of automating the test procedures as current practice in the company.

TABLE 4. Verified Events and results.

	Turning on, off, and restarting the TOE	Starting, holding, and ending video-conferencing calls	Administrative console login and logout	Changing security settings	Resetting/changing administrative login passwords
1.1.FAU_GEN.1.1	BSP module - Audit level: information about turning-on, off, and restarting the TOE. It is not possible to configure the audit levels	Module: Main control - Audit levels: information (start/end), error (failure, reported when unregistered and a call was initiated). It is not possible to configure the audit levels	Module: WEB - Audit level: information (in case of success), error (in case of failure). It is not possible to configure the audit levels	Module: BSP - Audit level: security settings information (active encryption or not, H460 protocol active or not). It is not possible to configure the audit levels	Module: BSP - Audit level: information (if changes are successful), error (if the change is unsuccessful). It is not possible to configure the audit levels
1.2.FAU_GEN.1.2	OK, output as expected	OK, output as expected	OK, output as expected	OK, output as expected	OK, output as expected
1.3. FAU_GEN.2	OK, output as expected, but the administrative user is a single one since there are no individual users	OK, output as expected, but the administrative user is a single one since there are no individual users	OK, output as expected, but the administrative user is a single one since there are no individual users	OK, output as expected, but the administrative user is a single one since there are no individual users	OK, output as expected, but the administrative user is a single one since there are no individual users
1.4.FCS_COP.1	Not applicable	Not applicable	Not applicable	Success / failure; cryptographic operation mode	Not applicable
1.5.FIA_AFL.1	Not applicable	Not applicable	Module: WEB - There is a record of all unsuccessful login attempts, but there is no information about the number of times or the basic actions to be taken	Not applicable	Not applicable
1.6.FIA_ATD.1	Not applicable	Not applicable	There is no definition of access levels for users; that is, access to TOE security administrative settings is performed only by the administrator user	Not applicable	Not applicable
1.7.FIA_SOS.1	Not applicable	Not applicable	Not applicable	Not applicable	There is only rejection by the TSF when the old password, needing to be changed to the new password, is reported wrongly. The only criticism made is regarding the minimum number of characters, which must be 5. There is no quality metric adopted for the registration of the password
1.8.FIA_SOS.2	Not applicable	Not applicable	Not applicable	Not applicable	
1.9.FIA_UAU.1	Not applicable	Not applicable	OK, output as expected. There is a record of unsuccessful login at the administrative console, and the TSF only allows actions on the console to be performed after the administrator login	Not applicable	Not applicable

TABLE 4. *(Continued.)* **Verified Events and results.**

1.10.FIA_UAU.2	Not applicable	Not applicable	Not applicable	After the administrative login, only the options for changing the login password require new user accreditation	Not applicable
1.11.FIA_UAU.3	Not applicable	Not applicable	Not applicable	OK, output as expected. The password used in the login credential is displayed with asterisk "*" signs, as many as the characters entered	Not applicable
1.12.FIA_UAU.4	Not applicable	Not applicable	Not applicable	OK, output as expected. The administrator user's single sign-on occurs	Not applicable
1.13.FIA_UAU.5	OK, output as expected. TOE records log with information of success and failure of the authentication record in the gatekeeper server, date and time; the log records call attempt, in-call, and call-termination TOE information	Not applicable	Not applicable	OK, output as expected. The final result of administrator user authentication is recorded	Not applicable
1.14.FIA_UAU.6	Not applicable	Not applicable	Not applicable	OK, output as expected. TOE records failures in user re-authentication, in addition to all re-authentication attempts	Not applicable
1.15.FIA_UAU.7	Not applicable	Not applicable	Not applicable	OK, output as expected. The only information returned to the user upon incorrect login is "Username or password error."	Not applicable
1.16.FTA_MCS.1	Not applicable	Not applicable	Not applicable	OK, output as expected. There is simultaneous login control from more than one administrator to the administrative console	Not applicable
1.17.FTA_MCS.2	Not applicable	Not applicable	OK, output as expected. TOE rejects a new session due to the limitation of multiple concurrent sessions. However, the number of simultaneous sessions of the administrator user does not occur	Not applicable	Not applicable
1.18.FTA_SSL.1	Not applicable	Not applicable	OK, output as expected. TSF is expected to lock the interactive session after 5 minutes of user inactivity in the administrative console	Not applicable	Not applicable

TABLE 4. *(Contiuned.)* **Verified Events and results.**

1.19.FTA_SSL.2	Not applicable	Not applicable	OK, output as expected. The user cannot lock his session, except for inactivity, when he is logged out of the console, which requires him to log back into the console to continue his session	Not applicable	Not applicable
1.20.FTA_SSL.3	Not applicable	Not applicable	OK, output as expected. TOE records administrator logout via lockout mechanism	Not applicable	Not applicable
1.21.FTA_SSL.4	Not applicable	Not applicable	OK, output as expected. TOE records user logout	Not applicable	Not applicable
1.22.FPT_FLS.1	OK, output as expected	OK, output as expected	Not applicable	Not applicable	Not applicable
1.23.FPT_TEE.1	Not applicable	Not applicable	Not applicable	OK, output as expected, but there is no time server test. After adding your data, the time is automatically displayed	Not applicable
1.24.FPT_TEE.2	Not applicable	OK, output as expected, but there is no registration test at the gatekeeper. After the inclusion of your information, the TOE already attempts to connect to the same	Not applicable	Not applicable	Not applicable
1.25.FTP_TRP.1	Not applicable	OK, output as expected. TOE records the activation and deactivation of the H.460 protocol in its log	Not applicable	Not applicable	Not applicable

The previous research works proposing CC-based information security [27]–[29], [35], [37], [38], [49], [51], [53], [56], [57], [58] report reaching EAL 3, just as we did. Our research brings one more CC application to the set of desktop computer certification [27] applications: Radio Frequency Identification (RFID) technology [28], biometric system [29], smart meters [49], [51], integrated voice, data, and video communications [37], [38], boots, sealing, and IT channels [57], Point-of-Sale (POS) systems, wind turbine park systems, and a secure workflow [56], personal computer [58], electronic voting system [55], SDN switches and controllers [59]. Only [51], [57] report having reached EAL 4 or 5. Still, in general, the authors did not present all classes, constructs, and test procedures to reach the mentioned security class, unlike our proposal, which is fully presented here.

Our proposal is on the user's side, a more common situation than those reported by [51], [57], whose authors could assess the German companies to analyze and propose TOE design changes. In practice, the SARS-CoV-2 pandemic brings online videoconferencing platforms to the center of business, education, and medicine (telemedicine) [74]. IT professionals cannot rely on procedural security, such as ITIL, COBIT, MPS.BR or DevSecOps approaches alone. Attacks like SQL Injection, brute force, DoS (Denial of Service), DDoS (Distributed Denial of Service), phishing, or man-in-the-middle URL handling need to be mitigated along with backdoor, spoofing, DMA (Direct Memory Access), and eavesdropping, just to name a few. Their analysis should advance to some inspection and tests, such as those proposed here. Suppliers could be requested to alter their project configurations or release their IT solutions. Such actions are currently

restricted to certain corporations worldwide and only carried out in the countries where the suppliers have their head offices.

Some business and daily life practices which the SARS-CoV-2 pandemic has brought in will probably persist, provided they cost less and become smarter and more comfortable. In this new context, security proposals such as those presented here will be increasingly necessary.

VI. CONCLUSION

The requirements used in the sPP developed in this work considered the security parameters defined in the POSIC of the FPA entity, a financial institution subject to strong market and security regulations, despite being a public bank. For study purposes, this research considered this specific group of users' needs and the associated acceptable market practices.

The use of Common Criteria to evaluate video conferencing equipment aligns with current practices, and it is an internationally recognized and much-used standard nowadays. It has great potential for evaluating and analyzing the information and communications security of cyber-physical systems.

The proposed sPP can also evaluate other video conferencing equipment from various manufacturers, as the security requirements listed in this profile are ordinary and generic to such equipment. It can also be used to determine mandatory security requirements for manufacturers or providers of videoconferencing systems.

Situations that involve specialized techniques are outside the scope of the CC, such as controlling magnetic emissions generated by the use of cell phones in the same physical space as the videoconferencing equipment or actions addressing support and administrative issues like user instructions and handling procedures. Security criteria relevant to managerial practices like physical access control and individual permissions are not directly related to IT security features.

The mechatronic functions of the TOE were not evaluated in this work. Only software functions were listed in the profile. There would be differences if the former were assessed since the TOE mechatronics questions pertain directly to the product's mechanical and electronic functioning constituent elements. Its implementation reflects significant changes in information security. It will be a new endeavor but demanding a lot of research on integrating physical systems in the proposed sPP and probably preparing the respective PPM.

For the ''active cryptography'' requirement, the study considered the use of encryption in all communications; that is, there was no investigation of more detailed aspects such as whether asymmetric or symmetric keys, algorithms, or cryptographic systems could be used. Future updates of the profile developed in this work may include such elements in implementing requirements for testing.

Applying the sPP in the TOE can be considered an important activity since the conditions listed in the profile must be reproduced in the same conditions in which they were identified. That may not always be possible due to difficulties in reproducing the operating environment.

The maturity of the CC and the awareness of North American and European managers have led institutions in the United States and Europe [38] to consider this vital assessment of security requirements in their products, especially in systems regarded as critical infrastructure (links of data communication in aviation systems, satellite communication, energy generation or telecom infrastructure).

The kind of application presented here demonstrates sPP-based security analysis feasibility in situations where IT equipment is not custom-designed or manufactured but only implemented and adapted for use. New endeavors could include other vital technologies, such as data centers for security evaluation on the user side.

Future work will also be carried out in the sense of customizing and apply this protection profile to the context of web-based videoconference solutions, which are used mainly because of the COVID-19 outbreak. This kind of information, which must transit via videoconference media, cloud, or standalone, is an open research area and will be the focus of our work's next steps.

REFERENCES

[1] C. C. Junior, *Sistemas Integrados de Gestão—ERP: Uma Abordagem Gerencial*, 4th ed. Curitiba, Brazil: Ibpex, 2011.
[2] L. Padilha. Defesa Cibernética. Notícias EPEX. Brasil. Accessed: Dec. 13, 2015. [Online]. Available: http://www.epex.eb.mil.br/index.php/projetos/defesacibernetica.html
[3] Brasil. *CBSI—Comunidade Brasileira de Sistemas de Informação*. Accessed: Dec. 2014. [Online]. Available: http://www.cbsi.net.br/2014/12/guerra-cibernetica-eua-x-coreia-do.html#.Vm3W5L_26r4
[4] A. C. B. Reis, R. C. F. Miranda, S. B. S. Monteiro, and S. C. M. Barbalho, ''Diagnóstico dos processos de homologação e certificação de produtos de natureza cibernética: Perspectivas para a construção de um sistema nacional,'' *Revista Produção Online*, vol. 18, no. 2, pp. 424–453, 2018.
[5] J. Buur and M. M. Andreasen, ''A theoretical approach to mechatronics design,'' Tech. Univ. Denmark, Lyngby, Denmark, 1990, p. 174. Accessed: Jan. 2015. [Online]. Available: https://orbit.dtu.dk/en/publications/a-theoretical-approach-to-mechatronics-design
[6] C. W. de Silva and S. Behbahani, ''A design paradigm for mechatronic systems,'' *Mechatronics*, vol. 23, no. 8, pp. 960–966, Dec. 2012. Accessed: Dec. 2015, doi: 10.1016/j.mechatronics.2012.08.004.
[7] S. C. M. Barbalho, *Modelo de Referência Para o Desenvolvimento de Produtos Mecatrônicos: Conceitos e Aplicações*, 1st ed. Saarbrücken, Germany: Novas Edições Acadêmicas, 2016.
[8] *AV-iQ*. Accessed: Jul. 2017. [Online]. Available: http://www.av-iq.com/avcat/ctl1642/index.cfm?manufacturer=huawei-enterprise-usa&product=te40-720p30-w-p-02
[9] W. Stallings, *Network Security Essentials: Applications and Standards*, 2nd ed. Upper Saddle River, NJ, USA: Prentice-Hall, 2003.
[10] M. J. C. F. T. Silva, *Avaliação da Segurança de Sistemas de Informação Usando uma Abordagem Multicritério*. Lisboa, Portugal: Técnico Lisboa-Engenharia Informática e de Computadores, 2014.
[11] P. H. Ohtoshi, ''Análise comparativa de metodologias de gestão e de análise de riscos sob a ótica da norma ABNT NBR ISO/IEC 27005,'' Dept. Comput. Sci., Inst. Exact Sci., Gestão da Segurança da Informação e Comunicações-Série Segurança da Informação, Faculdade de Ciência da Informação, Univ. Brasília, Brasília, Brazil, 2008, vol. 1.
[12] A. B. Martins and C. A. S. Santos, ''A methodology to implement an information security management system,'' *J. Inf. Syst. Technol. Manage.*, vol. 2, no. 2, pp. 121–136, 2005. Accessed: Sep. 2016. [Online]. Available: http://www.scielo.br/scielo.php?script=sci_arttext&pid=S1807-17752005000200002
[13] M. C. D'ornellas and K. Kroll, ''O gerenciamento estratégico da segurança da informação,'' in *Proc. Simpósio Brasileiro de Pesquisa Operacional-Pesquisa Operacional na Gestão do Conhecimento*, Porto Seguro, Brazil, 2009, p. 61.

[14] L. M. Fontoura, M. P. Konzen, and R. C. Nunes, "Gestão de riscos de segurança da informação baseada na norma ISO/IEC 27005 usando padrões de segurança," in *Proc. Simpósio de Excelência em Gestão e Tecnologia (SEGET)*, Resende, Brazil, 2012, p. 9.

[15] R. B. Filho and V. O. Santos, "Um modelo de sistema de gestão da segurança da informação baseado nas normas ABNT NBR ISO/IEC 27001:2006, 27002:2005 e 27005:2008," *Revista Telecomunicações*, vol. 15, no. 1, pp. 1–6, 2013.

[16] E. M. H. Amaral, R. C. Nunes, M. A. F. Oliveira, S. N. Pereira, and E. Zen, "Uma metodologia de gestão de segurança da informação direcionada a riscos baseado na abordagem Seis Sigma," in *Proc. Encontro Nacional de Engenharia de Produção*, Rio de Janeiro, Brazil, 2008, p. 22.

[17] M. M. Eloff and S. H. von Solms, "Information security management: An approach to combine process certification and product evaluation," *Comput. Secur.*, vol. 19, no. 8, pp. 698–709, Dec. 2000.

[18] D. Tréek, "An integral framework for information systems security management," *Comput. Secur.*, vol. 22, no. 4, pp. 337–360, 2003. Accessed: Sep. 2016. [Online]. Available: http://www.isy.vcu.edu/~gdhillon/Old2/teaching/Spring07-VCU-790-GlobalConseq/temp/An%20integral%20framework%20for%20information%20systems%20security%20management.pdf

[19] E. Yeniman Yildirim, G. Akalp, S. Aytac, and N. Bayram, "Factors influencing information security management in small- and medium-sized enterprises: A case study from Turkey," *Int. J. Inf. Manage.*, vol. 31, no. 4, pp. 360–365, Aug. 2011.

[20] A. Ren-Wei Fung, K.-J. Farn, and A. C. Lin, "Paper: A study on the certification of the information security management systems," *Comput. Standards Interfaces*, vol. 25, no. 5, pp. 447–461, Sep. 2003.

[21] M. Siponen and R. Willison, "Information security management standards: Problems and solutions," *Inf. Manage.*, vol. 46, no. 5, pp. 267–270, Jun. 2009, doi: 10.1016/j.im.2008.12.007.

[22] I. Tashi and S. Ghernaouti-Helie, "Efficient security measurements and metrics for risk assessment," in *Proc. 3rd Int. Conf. Internet Monitor. Protection*, vol. 1, Jun. 2008, pp. 131–138. Accessed: Sep. 2016, doi: 10.1109/ICIMP.2008.34.

[23] J. S. Broderick, "ISMS, security standards and security regulations," *Inf. Secur.*, vol. 11, no. 1, pp. 26–31, 2006.

[24] T. Takahashi and Y. Kadobayashi, "Reference ontology for cybersecurity operational information," *Comput. J.*, vol. 58, no. 10, pp. 2297–2392, Oct. 2015. Accessed: Apr. 2016, doi: 10.1093/comjnl/bxu101.

[25] J. F. P. Disso, K. Jones, D. Hutchison, and D. Prince, "A survey of cyber security management in industrial control systems," *Int. J. Crit. Infrastruct. Protection*, vol. 9, pp. 52–80, Jun. 2015.

[26] M. T. Dlamini, J. H. P. Eloff, and M. M. Eloff, "Information security: The moving target," *Comput. Secur.*, vol. 28, nos. 3–4, pp. 189–198, May 2009.

[27] M. P. Coelho and R. M. Silva, "Trustiness certification of information technology equipment," *Int. J. Comput. Sci. Netw. Secur.*, vol. 13, no. 12, pp. 35–42, 2013.

[28] Y.-C. Yu and T.-W. Hou, "Utilize common criteria methodology for secure ubiquitous healthcare environment," *J. Med. Syst.*, vol. 36, no. 3, pp. 1689–1696, Jun. 2012, doi: 10.1007/s10916-010-9629-2.

[29] B. Fernandez-Saavedra, R. Sanchez-Reillo, J. Liu-Jimenez, and O. Miguel-Hurtado, "Evaluation of biometric system performance in the context of common criteria," *Inf. Sci.*, vol. 245, pp. 240–254, Oct. 2013.

[30] *Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, Version 3.1, Revision 5*, document CCMB-2017-04-001, 2017.

[31] Ministry of Planning, Development and Management, Brazil. (Mar. 2015). *Edital Pregão Eletrônico Para Registro de Preços*. Accessed: Oct. 2016. [Online]. Available: http://www.planejamento.gov.br/acesso-a-informacao/licitacoes-e-contratos/licitacoes/pregao/2015/paginas/pregao-eletronico-no-03-2015-central-de-compras-e-contratacoes

[32] Cisco Systems Inc, San Jose, CA, USA. (2015). *Cisco Unified Communications Manager Security Target, Version 1.0*. Accessed: Sep. 2016. [Online]. Available: https://www.commoncriteriaportal.org/files/../st_vid10646-st.pdf

[33] *Tecnologia da Informação - Técnicas de Segurança—Sistemas de Gestão de Segurança da Informação—Requisitos, NBR 27001:2006*, 1st ed., ABNT, Rio de Janeiro, Brazil, 2006.

[34] Ministry of Planning, Budget and Management, Brasília, Brazil. (2015). *E-PING Padrões de Interoperabilidade de Governo Eletrônico—Documento Referência*. Accessed: Oct. 2016. [Online]. Available: http://eping.governoeletronico.gov.br

[35] *Dispõe Sobre Comunicação de Dados e Serviços de Tecnologia da Informação,* Portaria Interministerial, Ministry Planning, Budget Manage., Diário Oficial da União, Brazil, May 2014, no. 141, sec. 1, p. 83.

[36] M. Lisi. (2013). Security in Large, Strategic and Complex Systems. Università degli Studi CampusBio-Medico di Roma, Rome, Italy. Accessed: Nov. 17, 2013. [Online]. Available: https://www.slideshare.net/MarcoLisi/homeland-security2013-lisivo3

[37] D. Herrmann and S. Keith, "Application of common criteria to telecom services: A case study," *Comput. Secur. J.*, vol. 17, pp. 21–28, Spring 2001. Accessed: Nov. 2017. [Online]. Available: https://www.researchgate.net/publication/248543258_Application_of_Common_Criteria_to_Telecomm_Services_A_Case_Study

[38] N. Mead. (2013). The Common Criteria. Carnegie Mellon University, USA. Accessed: Nov. 2017. [Online]. Available: https://www.us-cert.gov/bsi/articles/best-practices/requirements-engineering/the-common-criteria

[39] F. Conti. (2011). Biometria—Qui Quadrado. UFPA, Belém, PA, Brazil. Accessed: Jul. 2017. [Online]. Available: http://ufpa.br/dicas/biome/bioqui.htm

[40] *Tecnologia da Informação—Técnicas de Segurança—Código de Prática Para a Gestão da Segurança da Informação, NBR 27002:2005*, 2nd ed., ABNT, Rio de Janeiro, Brazil, 2005.

[41] *Tecnologia da Informação—Técnicas de Segurança—Gestão de Riscos de Segurança da Informação, NBR 27005:2008*, 1st ed., ABNT, Rio de Janeiro, Brazil, 2008.

[42] Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República, Brasília, DF, Brazil. (2010). *Estabelece as Diretrizes para Implementação de Controles de Acesso Relativos à Segurança da Informação e Comunicações; nos órgãos e entidades da Administração Pública Federal; direta e indireta—APF, Norma Complementar 07/IN01/DSIC/GSIPR, DSIC/GSIPR*. Accessed: Mar. 2015. [Online]. Available: http://dsic.planalto.gov.br

[43] Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República, Brasília, DF, Brazil. (2013). *Estabelece Diretrizes nos Contextos de Atuação e Adequações Para Profissionais da Área de Segurança da Informação e Comunicações (SIC) nos Órgãos e Entidades da Administração Pública Federal (APF), Norma Complementar 17/IN01/DSIC/GSIPR, DSIC/GSIPR*. Accessed: Mar. 2015. [Online]. Available: http://dsic.planalto.gov.br

[44] M. M. Reis. Conceitos Elementares de Estatística. Universidade Federal de Santa Catarina, Santa Catarina, Brazil. Accessed: Jul. 2017. [Online]. Available: http://www.inf.ufsc.br/~marcelo.menezes.reis/intro.html

[45] NIAP, USA. (2014). *Protection Profile for Voice Over IP (VoIP) Applications, Version 1.3*. Accessed: Sep. 2017. [Online]. Available: https://www.niap-ccevs.org/Profile/Info.cfm?id=

[46] L. Brown and W. Stallings, *Segurança de Computadores: Princípios e Práticas*, 2nd ed. Amsterdam, The Netherlands: Elsevier, 2014.

[47] NIST-National Institute of Standards and Technology, USA. (2015). *Draft—Framework for Cyber-Physical Systems, Release 0.8*. Accessed: Jun. 2018. [Online]. Available: https://pages.nist.gov/cpspwg/library/

[48] W. Al-Ahmad, "A detailed strategy for managing corporation cyber war security," *Int. J. Cyber-Secur. Digit. Forensics*, vol. 2, no. 4, pp. 1–9, Dec. 2013. Accessed: Jun. 2020. [Online]. Available: http://sdiwc.net/digital-library/a-detailed-strategy-for-managing-corporation-cyber-war-security

[49] M. Bartsch, "Smart metering, Common Criteria and European privacy needs," in *Securing Electronic Business Processes*, H. Reimer, N. Pohlmann, and W. Schneider, Eds. Wiesbaden, Germany: Springer, Dec. 2012, pp. 116–127, doi: 10.1007/978-3-658-00333-3_12.

[50] R. V. Solms and H. V. D. Haar, "From trusted information security controls to a trusted information security environment," in *Information Security for Global Information Infrastructures* (IFIP International Federation for Information Processing), S. Qing *et al.*, Eds. Beijing, China: Kluwer, 2000, pp. 29–36.

[51] A. Sikora, "Architecture and development of secure communication solutions for smart grid applications," *J. Commun.*, vol. 8, no. 8, pp. 490–496, Aug. 2013.

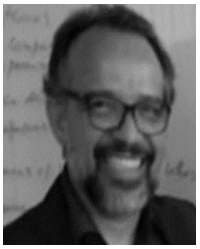
[52] M. Stegelmann and D. Kesdogan, "GridPriv: A smart metering architecture offering k-anonymity," in *Proc. IEEE 11th Int. Conf. Trust, Secur. Privacy Comput. Commun.*, Jun. 2012, pp. 419–426.

[53] F. Thiel, V. Hartmann, U. Grottker, and D. Richter, "IT security standards and legal metrology—Transfer and validation," in *Proc. EPJ Web Conf.*, vol. 77, Aug. 2014, pp. 1–6.

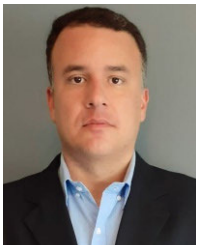
[54] K. Rannenberg and G. Iachello, "Protection profiles for remailer mixes. Do the new evaluation criteria help?" in *Proc. 16th Annu. Comput. Secur. Appl. Conf. (ACSAC)*, Jan. 2000, pp. 107–118.

[55] K. Reinhard and W. Jung, "Compliance of POLYAS with the BSI protection profile—Basic requirements for remote electronic voting systems," in *E-Voting and Identity* (Lecture Notes in Computer Science), vol. 4896, A. Alkassar and M. Volkamer, Eds. Berlin, Germany: Springer-Verlag, 2007, pp. 62–75.
[56] R. Sharp, "Report: CC-based design of secure application systems," in *Engineering Secure Software and Systems* (Lecture Notes in Computer Science), vol. 5429, F. Massacci, S. T. Redwine, Jr., and N. Zannone, Eds. Berlin, Germany: Springer-Verlag, 2009, pp. 111–121.
[57] H. Löhr, A. Sadeghi, C. Stüble, M. Weber, and M. Winandy, "Modeling trusted computing support in a protection profile for high assurance security kernels," in *Trusted Computing* (Lecture Notes in Computer Science), vol. 5471, L. Chen, C. J. Mitchell, and A. Martin, Eds. Berlin, Germany: Springer-Verlag, 2009, pp. 45–62.
[58] H. Lee, K. Lee, and D. Won, "Protection profile of personal information security system: Designing a secure personal information security system," in *Proc. Int. Joint Conf. IEEE TrustCom-11/IEEE ICESS-11/FCST-11*, Changsha, China, Nov. 2011, pp. 806–811.
[59] A. Mukhanov, A. Petukhov, and P. Pilugin, "Common Criteria and software-defined network (SDN) security," in *Proc. Int. Sci. Tech. Conf. Mod. Comput. Netw. Technol. (MoNeTeC)*, Moscow, Russia, 2018, pp. 1–6.
[60] M. Bender Perotoni, R. Menna Barreto, and S. Koch Manfrin, "Cyber-attacks based in electromagnetic effects," *IEEE Latin Amer. Trans.*, vol. 14, no. 6, pp. 2838–2845, Jun. 2016, doi: 10.1109/TLA.2016.7555262.
[61] E. W. Tavares Ferreira and A. Akira Shinoda, "The development and evaluation of a dataset for testing of IDS for wireless networks," *IEEE Latin Amer. Trans.*, vol. 14, no. 1, pp. 404–410, Jan. 2016, doi: 10.1109/TLA.2016.7430108.
[62] F. Flores, R. Paredes, and F. Meza, "Procedures for mitigating cybersecurity risk in a chilean government ministry," *IEEE Latin Amer. Trans.*, vol. 14, no. 6, pp. 2947–2950, Jun. 2016, doi: 10.1109/TLA.2016.7555280.
[63] T. G. Machado, A. A. Mota, L. T. M. Mota, M. F. H. Carvalho, and C. C. Pezzuto, "Methodology for identifying the cybersecurity maturity level of smart grids," *IEEE Latin Amer. Trans.*, vol. 14, no. 11, pp. 4512–4519, Nov. 2016, doi: 10.1109/TLA.2016.7795822.
[64] W. Fernandez and A. Rodriguez, "Analysis of the regulatory requirements for the smart grid in chile," *IEEE Latin Amer. Trans.*, vol. 15, no. 1, pp. 13–20, Jan. 2017, doi: 10.1109/TLA.2017.7827883.
[65] K. Regis Pires Cavalcanti, E. Viana, and F. Antonio Aires Lins, "An integrated solution for the improvement of the mobile devices security based on the Android platform," *IEEE Latin Amer. Trans.*, vol. 15, no. 11, pp. 2171–2176, Nov. 2017, doi: 10.1109/TLA.2017.8070423.
[66] J. G. dos Santos, A. Cappellozza, and A. L. Albertin, "Antecedents of perceived benefits of compliance towards organizational data protection policies," *IEEE Latin Amer. Trans.*, vol. 16, no. 3, pp. 891–896, Mar. 2018, doi: 10.1109/TLA.2018.8358670.
[67] R. Deb and S. Roy, "Common vulnerability scoring system for SDN environment," *Int. J. Eng. Adv. Technol.*, vol. 8, no. 6, pp. 4022–4029, Aug. 2019, doi: 10.35940/ijeat.F9302.088619.
[68] B. Parra, M. Vegetti, and H. Leone, "Advances in the application of ontologies in the area of digital forensic electronic mail," *IEEE Latin Amer. Trans.*, vol. 17, no. 10, pp. 1694–1705, Oct. 2019, doi: 10.1109/TLA.2019.8986448.
[69] S. C. M. Barbalho and H. Rozenfeld. "Modelo de referência para o processo de desenvolvimento de produtos mecatrônicos (MRM): Validação e resultados de uso," *Gestão Produção*, vol. 20, pp. 162–179, 2013, doi: 10.1590/S0104-530X2013000100012.
[70] T. Martins and S. V. G. Oliveira, "Cybersecurity in the power electronics," *IEEE Latin Amer. Trans.*, vol. 17, no. 8, pp. 1300–1308, Aug. 2019, doi: 10.1109/TLA.2019.8932339.
[71] M. A. Fabrício, F. H. Behrens, and D. Bianchini, "Monitoring of industrial electrical equipment using IoT," *IEEE Latin Amer. Trans.*, vol. 18, no. 8, pp. 1425–1432, Aug. 2020, doi: 10.1109/TLA.2020.9111678.
[72] S. H. Bouk, S. H. Ahmed, R. Hussain, and Y. Eun, "Named data networking's intrinsic cyber-resilience for vehicular CPS," *IEEE Access*, vol. 6, pp. 60570–60585, 2018, doi: 10.1109/ACCESS.2018.2875890.
[73] S. Rouhani and R. Deters, "Security, performance, and applications of smart contracts: A systematic survey," *IEEE Access*, vol. 7, pp. 50759–50779, 2019, doi: 10.1109/ACCESS.2019.2911031.
[74] S. Hakak, W. Z. Khan, M. Imran, K.-K.-R. Choo, and M. Shoaib, "Have you been a victim of COVID-19-Related cyber incidents? Survey, taxonomy, and mitigation strategies," *IEEE Access*, vol. 8, pp. 124134–124144, 2020, doi: 10.1109/ACCESS.2020.3006172.
[75] R. A. Maalem Lahcen, B. Caulkins, R. Mohapatra, and M. Kumar, "Review and insight on the behavioral aspects of cybersecurity," *Cybersecurity*, vol. 3, no. 1, p. 10, Dec. 2020, doi: 10.1186/s42400-020-00050-w.
[76] A. Khraisat, I. Gondal, P. Vamplew, and J. Kamruzzaman, "Survey of intrusion detection systems: Techniques, datasets, and challenges," *Cybersecurity*, vol. 2, no. 1, p. 20, 2019, doi: 10.1186/s42400-019-0038-7.
[77] F. E. Catota, M. G. Morgan, and D. C. Sicker, "Cybersecurity incident response capabilities in the Ecuadorian financial sector," *J. Cybersecur.*, vol. 4, no. 1, pp. 1–20, Jan. 2018, doi: 10.1093/cybsec/tyy002.
[78] B. Dupont, "The cyber-resilience of financial institutions: Significance and applicability," *J. Cybersecur.*, vol. 5, no. 1, pp. 1–17, Jan. 2019, doi: 10.1093/cybsec/tyz013.
[79] Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República, Brasília, DF, Brazil. (2008). *Disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, Direta e Indireta, e dá Outras Providências, Instrução Normativa GSI/PR no 1, DSIC/GSIPR*. Accessed: Mar. 2015. [Online]. Available: http://dsic.planalto.gov.br
[80] Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República, Brasília, DF, Brazil. (2013). *Dispõe Sobre o Credenciamento de Segurança Para o Tratamento de Informação Classificada, em Qualquer Grau de Sigilo, no Âmbito do Poder Executivo Federal, Instrução Normativa GSI/PR no 2, DSIC/GSIPR*. Accessed: Mar. 2015. [Online]. Available: http://dsic.planalto.gov.br
[81] Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República, Brasília, DF, Brazil. (2013). *Dispõe Sobre os Parâmetros e Padrões Mínimos dos Recursos Criptográficos Baseados em Algoritmos de Estado Para Criptografia da Informação Classificada no Âmbito do Poder Executivo Federal, Instrução Normativa GSI/PR no 3, DSIC/GSIPR*. Accessed: Mar. 2015. [Online]. Available: http://dsic.planalto.gov.br

ARIANE C. B. FLORENTINO was born in São Paulo, Brazil, in 1982. She received the Technologist's degree in sequential course in telecommunications systems from the University of Vale do Paraíba (UNIVAP) in 2003, and the bachelor's degree in electrical engineering from ETEP Faculties in 2010, both in São José dos Campos, São Paulo, Brazil, and the master's degree in mechanical engineering from the Federal University of Brasília in 2017. Her current research interests are applications of information security management and cyber-defense problems. She has received also the specialization in information security management from the University of Brasilia, Brazil, in 2014.



SANDERSON CÉSAR MACÊDO BARBALHO received the bachelor's degree in electrical engineering and the master's degree in operations management from the Federal University of Rio Grande do Norte, Natal, Brazil, and the Ph.D. degree in new product development from the University of Sao Paulo, Brazil, in 2006. He is currently a Professor with the University of Brasilia, Brazil, and a former Project Management Professional (PMP) with the Project Management Institute.



RAPHAEL CARLOS SANTOS MACHADO received the Ph.D. degree in systems and computer engineering from COPPE/UFRJ, in 2010. He is currently a Researcher with Inmetro and a Professor with Federal Fluminense University (UFF). He has a research productivity scholarship from CNPq since 2013 and a Young Scientist from the State of RJ since 2015, having published more than a hundred scientific articles in the areas of information security, code analysis, obfuscation, software incorruptibility, watermarks, cryptography, computational complexity, combinatory mathematics, and graph theory.